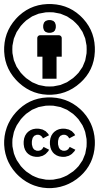
# THE OPEN LOGIC TEXT

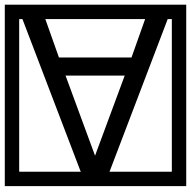
Complete Build (brazilian / pt)

**Projeto Open Logic**

Revision: 51c2271 (main)
2026-07-12



*The Open Logic Text* do Projeto Open Logic está licenciado sob a Licença Creative Commons Atribuição 4.0 Internacional.



# Sobre o Open Logic Project

O *Open Logic Text* é um livro-texto colaborativo de código aberto de metalógica formal e métodos formais, começando em um nível intermediário (ou seja, após um curso introdutório de lógica formal). Embora voltado a um público não matemático (em particular, estudantes de filosofia e ciência da computação), é rigoroso.

A cobertura de alguns tópicos atualmente incluídos pode ainda não estar completa, e muitas seções ainda exigem revisão substancial. Planejamos expandir o texto para cobrir mais tópicos no futuro. Também planejamos adicionar recursos ao texto, como um glossário, uma lista de leituras complementares, notas históricas, imagens, melhores explicações, seções que explicam a relevância dos resultados para filosofia, ciência da computação e matemática, e mais problemas e exemplos. Se você encontrar um erro ou tiver uma sugestão, informe a equipe do projeto.

O projeto opera no espírito do código aberto. O texto não só está disponível gratuitamente; fornecemos o código-fonte LaTeX sob a licença Creative Commons Atribuição, que dá a qualquer pessoa o direito de baixar, usar, modificar, reorganizar, converter e redistribuir nosso trabalho, desde que deem o devido crédito. Consulte o site do Open Logic Project em openlogic-project.org para informações adicionais.

# Sumário

**Sobre o Open Logic Project** **1**

**I Teoria Ingênua dos Conjuntos** **15**

**1 Conjuntos** **17**
1.1 Extensionalidade . . . 17
1.2 Subconjuntos e conjuntos potência . . . 18
1.3 Alguns Conjuntos Importantes . . . 19
1.4 Uniões e Interseções . . . 20
1.5 Pares, Tuplas, Produtos Cartesianos . . . 24
1.6 Paradoxo de Russell . . . 25
Problemas . . . 26

**2 Relações** **28**
2.1 Relações como Conjuntos . . . 28
2.2 Reflexões Filosóficas . . . 30
2.3 Propriedades Especiais das Relações . . . 31
2.4 Relações de Equivalência . . . 32
2.5 Ordens . . . 33
2.6 Grafos . . . 35
2.7 Árvores . . . 36
2.8 Operações sobre Relações . . . 38
Problemas . . . 39

**3 Funções** **40**
3.1 Noções Básicas . . . 40
3.2 Tipos de Funções . . . 42
3.3 Funções como Relações . . . 44
3.4 Inversas de Funções . . . 45
3.5 Composição de Funções . . . 47
3.6 Funções Parciais . . . 48
Problemas . . . 49

**4 O Tamanho dos Conjuntos** **50**
4.1 Introdução . . . 50
4.2 Enumerações e Conjuntos Enumeráveis . . . 50
4.3 Método do Zigue-Zague de Cantor . . . 54
4.4 Funções de Pareamento e Códigos . . . 56
4.5 Uma Função de Emparelhamento Alternativa . . . 56
4.6 Conjuntos Não enumeráveis . . . 58
4.7 Redução . . . 61
4.8 Equinumerosidade . . . 62
4.9 Conjuntos de Tamanhos Diferentes e o Teorema de Cantor . . . 64
4.10 A Noção de Tamanho e Schröder-Bernstein . . . 65
4.11 Enumerações e Conjuntos Enumeráveis . . . 66
4.12 Conjuntos Não Enumeráveis . . . 68
4.13 Redução . . . 70
Problemas . . . 71

**5 Aritmetização** **75**
5.1 De $\mathbb{N}$ para $\mathbb{Z}$ . . . 75
5.2 De $\mathbb{Z}$ para $\mathbb{Q}$ . . . 77
5.3 A Reta Real . . . 78
5.4 De $\mathbb{Q}$ para $\mathbb{R}$ . . . 80
5.5 Algumas Reflexões Filosóficas . . . 81
5.6 Anéis e Corpos Ordenados . . . 83
5.7 Apêndice: os Reais como Sequências de Cauchy . . . 86
Problemas . . . 90

**6 Conjuntos Infinitos** **91**
6.1 Hotel de Hilbert . . . 91
6.2 Álgebras de Dedekind . . . 92
6.3 Indução Aritmética . . . 94
6.4 "Prova" de Dedekind . . . 95
6.5 Apêndice: Provando Schröder-Bernstein . . . 97

**II Propositional Logic** **99**

**7 Syntax and Semantics** **101**

**8 Sistemas de Derivação** **102**
8.1 Introdução . . . 102
8.2 O Cálculo de Sequentes . . . 104
8.3 Dedução Natural . . . 105
8.4 Tableaux . . . 106
8.5 Dedução Axiomática . . . 107

**9 O Cálculo de Sequentes** **109**
9.1 Regras e Derivações . . . 109
9.2 Regras Proposicionais . . . 110
9.3 Regras Estruturais . . . 111
9.4 Derivações . . . 112
9.5 Exemplos de Derivações . . . 113
9.6 Noções da Teoria da Prova . . . 117
9.7 Derivabilidade e Consistência . . . 119
9.8 Derivabilidade e os Conectivos Proposicionais . . . 120
9.9 Correção . . . 121
Problemas . . . 126

**10 Dedução Natural** **128**
10.1 Regras e Derivações . . . 128
10.2 Regras Proposicionais . . . 129
10.3 Derivações . . . 130
10.4 Exemplos de Derivações . . . 131
10.5 Noções da Teoria da Prova . . . 135
10.6 Derivabilidade e Consistência . . . 137
10.7 Derivabilidade e os Conectivos Proposicionais . . . 138
10.8 Correção . . . 140
Problemas . . . 143

**11 Tableaux** **145**

**12 Axiomatic Derivações** **146**

**13 O Teorema da Completude** **147**
13.1 Introdução . . . 147
13.2 Esboço da Prova . . . 148
13.3 Conjuntos Consistentes Completos de Sentenças . . . 149
13.4 Lema de Lindenbaum . . . 150
13.5 Construção de um Modelo . . . 151
13.6 O Teorema da Completude . . . 152
13.7 O Teorema da Compacidade . . . 153
13.8 Uma Prova Direta do Teorema da Compacidade . . . 154
Problemas . . . 154

**III Lógica de Primeira Ordem** **156**

**14 Introdução à Lógica de Primeira Ordem** **158**
14.1 Lógica de Primeira Ordem . . . 158
14.2 Sintaxe . . . 159
14.3 Fórmulas . . . 160

14.4 Satisfação . . . 161
14.5 Sentenças . . . 163
14.6 Noções Semânticas . . . 164
14.7 Substituição . . . 165
14.8 Modelos e Teorias . . . 166
14.9 Correção e Completude . . . 167

**15 Sintaxe da Lógica de Primeira Ordem** **169**
15.1 Introdução . . . 169
15.2 Linguagens de Primeira Ordem . . . 169
15.3 Termos e Fórmulas . . . 171
15.4 Leitura Única . . . 174
15.5 Operador principal de uma Fórmula . . . 177
15.6 Subfórmulas . . . 178
15.7 Sequências de Formação . . . 179
15.8 Variáveis Livres e Sentenças . . . 183
15.9 Substituição . . . 184
Problemas . . . 186

**16 Semântica da Lógica de Primeira Ordem** **187**
16.1 Introdução . . . 187
16.2 Estruturas para Linguagens de Primeira Ordem . . . 188
16.3 Estruturas Cobertas para Linguagens de Primeira Ordem . . . 189
16.4 Satisfação de a Fórmula em a Estrutura . . . 190
16.5 Atribuições de Variáveis . . . 195
16.6 Extensionalidade . . . 198
16.7 Noções Semânticas . . . 199
Problemas . . . 201

**17 Teorias e Seus Modelos** **203**
17.1 Introdução . . . 203
17.2 Expressando Propriedades de Estruturas . . . 205
17.3 Exemplos de Teorias de Primeira Ordem . . . 206
17.4 Expressando Relações em a Estrutura . . . 208
17.5 A Teoria dos Conjuntos . . . 209
17.6 Expressando o Tamanho de Estruturas . . . 212
Problemas . . . 213

**18 Sistemas de Derivação** **215**
18.1 Introdução . . . 215
18.2 O Cálculo de Sequentes . . . 217
18.3 Dedução Natural . . . 218
18.4 Tableaux . . . 219
18.5 Dedução Axiomática . . . 220

**19 O Cálculo de Sequentes** **222**
19.1 Regras e Derivações . . . 222
19.2 Regras Proposicionais . . . 223
19.3 Regras de Quantificadores . . . 224
19.4 Regras Estruturais . . . 225
19.5 Derivações . . . 226
19.6 Exemplos de Derivações . . . 228
19.7 Derivações com Quantificadores . . . 231
19.8 Noções da Teoria da Prova . . . 232
19.9 Derivabilidade e Consistência . . . 234
19.10 Derivabilidade e os Conectivos Proposicionais . . . 236
19.11 Derivabilidade e os Quantificadores . . . 237
19.12 Correção . . . 238
19.13 Derivações com Predicado de identidade . . . 243
19.14 Correção com Predicado de identidade . . . 244
Problemas . . . 244

**20 Dedução Natural** **247**
20.1 Regras e Derivações . . . 247
20.2 Regras Proposicionais . . . 248
20.3 Regras de Quantificadores . . . 249
20.4 Derivações . . . 250
20.5 Exemplos de Derivações . . . 252
20.6 Derivações com Quantificadores . . . 256
20.7 Noções da Teoria da Prova . . . 259
20.8 Derivabilidade e Consistência . . . 261
20.9 Derivabilidade e os Conectivos Proposicionais . . . 263
20.10 Derivabilidade e os Quantificadores . . . 264
20.11 Correção . . . 264
20.12 Derivações com Predicado de identidade . . . 269
20.13 Correção com Predicado de identidade . . . 270
Problemas . . . 271

**21 Tableaux** **273**

**22 Axiomatic Derivações** **274**

**23 O Teorema da Completude** **275**
23.1 Introdução . . . 275
23.2 Esboço da Prova . . . 276
23.3 Conjuntos Consistentes Completos de Sentenças . . . 279
23.4 Expansão de Henkin . . . 280
23.5 Lema de Lindenbaum . . . 282
23.6 Construção de um Modelo . . . 283

23.7 Identidade . . . . . 285
23.8 O Teorema da Completude . . . . . 288
23.9 O Teorema da Compacidade . . . . . 288
23.10 Uma Prova Direta do Teorema da Compacidade . . . . . 291
23.11 O Teorema de Löwenheim–Skolem . . . . . 292
Problemas . . . . . 293

**24 Além da lógica de primeira ordem** **294**
24.1 Visão Geral . . . . . 294
24.2 Lógica de Múltiplas Ordenações . . . . . 295
24.3 Lógica de Segunda Ordem . . . . . 296
24.4 Lógica de Ordem Superior . . . . . 300
24.5 Lógica Intuicionista . . . . . 303
24.6 Lógicas Modais . . . . . 307
24.7 Outras Lógicas . . . . . 308

**IV Model Theory** **310**

**25 Basics of Model Theory** **312**

**26 Models of Arithmetic** **313**

**27 The Interpolation Theorem** **314**

**28 Lindström's Theorem** **315**

**V Computability** **316**

**29 Recursive Functions** **318**

**30 Computability Theory** **319**

**VI Máquinas de Turing** **320**

**31 Computações de Máquinas de Turing** **321**
31.1 Introdução . . . . . 321
31.2 Representando Máquinas de Turing . . . . . 323
31.3 Máquinas de Turing . . . . . 327
31.4 Configurações e Computações . . . . . 328
31.5 Representação Unária de Números . . . . . 330
31.6 Estados de Parada . . . . . 332
31.7 Máquinas Disciplinadas . . . . . 333
31.8 Combinando Máquinas de Turing . . . . . 334

31.9 Variantes de Máquinas de Turing . . . . . 337
31.10 A Tese de Church–Turing . . . . . 339
Problemas . . . . . 340

**32 Indecidibilidade** **343**
32.1 Introdução . . . . . 343
32.2 Enumerando Máquinas de Turing . . . . . 345
32.3 Máquinas de Turing Universais . . . . . 347
32.4 O Problema da Parada . . . . . 349
32.5 O Problema da Decisão . . . . . 351
32.6 Representando Máquinas de Turing . . . . . 352
32.7 Verificando a Representação . . . . . 355
32.8 O Problema da Decisão é Insolúvel . . . . . 360
32.9 Teorema de Trakhtenbrot . . . . . 361
Problemas . . . . . 364

**VII Incompleteness** **366**

**33 Introduction to Incompleteness** **368**

**34 Arithmetization of Syntax** **369**

**35 Representability in Q** **370**

**36 Theories and Computability** **371**

**37 Incompleteness and Provability** **372**

**VIII Second-order Logic** **373**

**38 Syntax and Semantics** **375**

**39 Metatheory of Second-order Logic** **376**

**40 Second-order Logic and Set Theory** **377**

**IX The Lambda Calculus** **378**

**41 Introduction** **380**

**42 Syntax** **381**

**43 The Church–Rosser Property** **382**

**44 Lambda Definability** **383**

**X Many-valued Logic** **384**

**45 Syntax and Semantics** **386**

**46 Three-valued Logics** **387**

**47 Infinite-valued Logics** **388**

**48 Sequent Calculus** **389**

**XI Normal Modal Logics** **390**

**49 Syntax and Semantics** **392**

**50 Frame Definability** **393**

**51 Axiomatic Derivações** **394**

**52 Completeness and Canonical Models** **395**

**53 Filtrations and Decidability** **396**

**54 Modal Tableaux** **397**

**55 Modal Sequent Calculus** **398**

**XII Applied Modal Logic** **399**

**56 Temporal Logics** **401**

**57 Epistemic Logics** **402**

**XIII Intuitionistic Logic** **403**

**58 Introduction** **404**

**59 Semantics** **405**

**60 Soundness and Completeness** **406**

**61 Intuitionistic Tableaux** **407**

**62 Propositions as Types** **408**

**XIV Counterfactuals** **409**

**63 Introduction** **410**

**64 Minimal Change Semantics** **411**

**XV Set Theory** **412**

**65 A Concepção Iterativa** **413**
65.1 Extensionalidade . . . . . 413
65.2 Paradoxo de Russell (de novo) . . . . . 413
65.3 Predicativo e Impredicativo . . . . . 415
65.4 A Abordagem Cumulativa-Iterativa . . . . . 416
65.5 Urelementos ou Não? . . . . . 418
65.6 Apêndice: Lei Básica V de Frege . . . . . 419

**66 Passos rumo a Z** **421**
66.1 A história com mais pormenor . . . . . 421
66.2 Separação . . . . . 421
66.3 União . . . . . 423
66.4 Pares . . . . . 424
66.5 Conjuntos potência . . . . . 424
66.6 Infinito . . . . . 425
66.7 $\mathbf{Z}^-$: um marco . . . . . 427
66.8 A escolher os números naturais . . . . . 428
66.9 Apêndice: Fechamento, compreensão e interseção . . . . . 429
Problemas . . . . . 430

**67 Ordinais** **431**
67.1 Introdução . . . . . 431
67.2 A Ideia Geral de um Ordinal . . . . . 431
67.3 Boas Ordenações . . . . . 432
67.4 Isomorfismos de Ordem . . . . . 433
67.5 Construção de Von Neumann . . . . . 435
67.6 Propriedades Básicas dos Ordinais . . . . . 436
67.7 Substituição . . . . . 438
67.8 $\mathbf{ZF}^-$: um marco . . . . . 440
67.9 Ordinais como Tipos de Ordem . . . . . 440
67.10 Ordinais Sucessores e Limites . . . . . 441
Problemas . . . . . 442

**68 Estágios e postos** **443**
68.1 Definindo os estágios como os $V_\alpha$ . . . 443
68.2 Teorema(s) de recursão transfinita . . . 444
68.3 Propriedades básicas dos estágios . . . 446
68.4 Fundação . . . 447
68.5 **Z** e **ZF**: um marco . . . 448
68.6 Posto . . . 449
Problemas . . . 451

**69 Substituição** **452**
69.1 Introdução . . . 452
69.2 A Força da Substituição . . . 452
69.3 Considerações Extrínsecas . . . 453
69.4 Limitação de Tamanho . . . 455
69.5 Substituição e "Infinito Absoluto" . . . 456
69.6 Substituição e Reflexão . . . 458
69.7 Apêndice: Resultados sobre Substituição . . . 459
69.8 Apêndice: Axiomatizabilidade finita . . . 462
Problemas . . . 463

**70 Aritmética Ordinal** **464**
70.1 Introdução . . . 464
70.2 Adição Ordinal . . . 464
70.3 Usando Adição Ordinal . . . 467
70.4 Multiplicação Ordinal . . . 469
70.5 Exponenciação Ordinal . . . 470
Problemas . . . 471

**71 Cardinais** **472**
71.1 Princípio de Cantor . . . 472
71.2 Cardinais como Ordinais . . . 473
71.3 **ZFC**: um marco . . . 474
71.4 Finito, Enumerável, Não Enumerável . . . 475
71.5 Apêndice: Princípio de Hume . . . 477

**72 Aritmética Cardinal** **480**
72.1 Definindo as Operações Básicas . . . 480
72.2 Simplificando Adição e Multiplicação . . . 482
72.3 Algumas Simplificações . . . 483
72.4 A Hipótese do Contínuo . . . 484
72.5 Pontos Fixos de $\aleph$ . . . 486
Problemas . . . 489

**73 Escolha** **490**

73.1 Introdução . . . . . 490
73.2 O Truque de Tarski–Scott . . . . . 490
73.3 Comparabilidade e Lema de Hartogs . . . . . 491
73.4 O Problema da Boa Ordenação . . . . . 492
73.5 Escolha Enumerável . . . . . 494
73.6 Considerações Intrínsecas sobre a Escolha . . . . . 496
73.7 Paradoxo de Banach–Tarski . . . . . 497
73.8 Apêndice: Paradoxo de Vitali . . . . . 499
Problemas . . . . . 503

**XVI Methods** **504**

**74 Provas** **506**
74.1 Introdução . . . . . 506
74.2 Começando uma Prova . . . . . 507
74.3 Usando Definições . . . . . 508
74.4 Padrões de Inferência . . . . . 509
74.5 Um Exemplo . . . . . 515
74.6 Outro Exemplo . . . . . 519
74.7 Prova por Contradição . . . . . 520
74.8 Lendo Provas . . . . . 524
74.9 Não Consigo Fazer Isso! . . . . . 525
74.10 Outros Recursos . . . . . 526
Problemas . . . . . 527

**75 Indução** **528**
75.1 Introdução . . . . . 528
75.2 Indução em $\mathbb{N}$ . . . . . 529
75.3 Indução Forte . . . . . 531
75.4 Definições Indutivas . . . . . 532
75.5 Indução Estrutural . . . . . 534
75.6 Relações e Funções . . . . . 536
Problemas . . . . . 539

**XVII History** **540**

**76 Biografias** **541**
76.1 Georg Cantor . . . . . 541
76.2 Alonzo Church . . . . . 542
76.3 Gerhard Gentzen . . . . . 543
76.4 Kurt Gödel . . . . . 544
76.5 Emmy Noether . . . . . 545

76.6 Bertrand Russell . . . . . 547
76.7 Alfred Tarski . . . . . 548
76.8 Alan Turing . . . . . 549
76.9 Ernst Zermelo . . . . . 551

**77 História e Mitologia da Teoria dos Conjuntos** **553**
77.1 Infinitesimais e Diferenciação . . . . . 553
77.2 Definição Rigorosa de Limites . . . . . 555
77.3 Patologias . . . . . 556
77.4 Mais Mito do que História? . . . . . 558
77.5 Cantor na Reta e no Plano . . . . . 559
77.6 Apêndice: Curvas Preenchedoras de Espaço de Hilbert . . . . . 560

**XVIIIReference** **563**

**78 O Alfabeto Grego** **565**

**79 The Fraktur Alphabet** **566**

**Créditos das Imagens** **566**

**Referências Bibliográficas** **568**

This file loads all content included in the Open Logic Project. Editorial notes like this, if displayed, indicate that the file was compiled without any thought to how this material will be presented. If you can read this, it is probably *not advisable* to teach or study from this PDF.

The Open Logic Project provides many mechanisms by which a text can be generate which is more appropriate for teaching or self-study. For instance, by default, the text will make all logical operators primitives and carry out all cases for all operators in proofs. But it is much better to leave some of these cases as exercises. The Open Logic Project is also a work in progress. In an effort to stimulate collaboration and improvement, material is included even if it is only in draft form, is missing exercises, etc. A PDF produced for a course will exclude these sections.

To find PDFs more suitable for teaching and studying, have a look at the sample courses available on the OLP website. To make your own, you might start from the sample driver file or look at the sources of the derived textbooks for more fancy and advanced examples.

# Parte I

# Teoria Ingênua dos Conjuntos

The material in this part is an introduction to basic naive set theory. With the inclusion of Tim Button's Teoria dos Conjuntos Aberta, this also covers the construction of number systems, and discussion of infinity, which are not required for the logical parts of the OLP.

# Capítulo 1

# Conjuntos

## 1.1 Extensionalidade

Um *conjunto* é uma coleção de objetos, considerada como um único objeto. Os objetos que compõem o conjunto chamam-se *elementos* ou *membros* do conjunto. Se $x$ é um membro de um conjunto $A$, escrevemos $x \in A$; caso contrário, escrevemos $x \notin A$. O conjunto que não tem membros chama-se o *conjunto vazio* e denota-se "$\varnothing$".

Não importa como *especificamos* o conjunto, ou como *ordenamos* os seus membros, ou mesmo quantas *vezes* contamos os seus membros. Só importa quais são os seus membros. Codificamos isto no princípio seguinte.

**Definição 1.1 (Extensionalidade).** Se $A$ e $B$ são conjuntos, então $A = B$ se e só se todo membro de $A$ é também um membro de $B$, e vice-versa.

A extensionalidade autoriza certa notação. Em geral, quando temos objetos $a_1, \ldots, a_n$, então $\{a_1, \ldots, a_n\}$ é *o* conjunto cujos membros são $a_1, \ldots, a_n$. Enfatizamos a palavra "*o*", pois a extensionalidade nos diz que só pode haver *um* tal conjunto. De fato, a extensionalidade também autoriza o seguinte:

$$\{a, a, b\} = \{a, b\} = \{b, a\}.$$

Isto traduz a ideia de que, quando consideramos conjuntos, não nos importa a ordem dos seus membros, nem quantas vezes são especificados.

**Exemplo 1.2.** Sempre que temos vários objetos, podemos reuni-los num conjunto. O conjunto dos irmãos de Richard, por exemplo, é um conjunto que contém uma pessoa, e podemos escrevê-lo como $S = \{\text{Ruth}\}$. O conjunto dos inteiros positivos menores que 4 é $\{1, 2, 3\}$, mas também se pode escrever como $\{3, 2, 1\}$ ou mesmo como $\{1, 2, 1, 2, 3\}$. São todos o mesmo conjunto, pela extensionalidade. De fato, todo membro de $\{1, 2, 3\}$ é também um membro de $\{3, 2, 1\}$ (e de $\{1, 2, 1, 2, 3\}$), e vice-versa.

Com frequência especificaremos um conjunto por alguma propriedade que os seus membros compartilham. Usaremos a seguinte notação abreviada para isso: $\{x : \varphi(x)\}$, onde $\varphi(x)$ representa a propriedade que $x$ tem de satisfazer para ser contado entre os membros do conjunto.

**Exemplo 1.3.** No nosso exemplo, também poderíamos ter especificado $S$ como

$$S = \{x : x \text{ é irmão de Richard}\}.$$

**Exemplo 1.4.** Diz-se que um número é *perfeito* se e só se for igual à soma dos seus divisores próprios (isto é, números que o dividem sem resto mas não são iguais ao próprio número). Por exemplo, 6 é perfeito porque os seus divisores próprios são 1, 2, e 3, e $6 = 1 + 2 + 3$. De fato, 6 é o único inteiro positivo menor que 10 que é perfeito. Assim, usando a extensionalidade, podemos dizer:

$$\{6\} = \{x : x \text{ é perfeito e } 0 \leq x \leq 10\}$$

Lemos a notação à direita como "o conjunto dos $x$ tais que $x$ é perfeito e $0 \leq x \leq 10$". A identidade aqui confirma que, quando consideramos conjuntos, não nos importa como são especificados. E, mais em geral, a extensionalidade garante que há sempre apenas um conjunto dos $x$ tais que $\varphi(x)$. Logo, a extensionalidade justifica chamar a $\{x : \varphi(x)\}$ *o* conjunto dos $x$ tais que $\varphi(x)$.

A extensionalidade nos dá um modo de mostrar que conjuntos são idênticos: para mostrar que $A = B$, mostre que sempre que $x \in A$ então também $x \in B$, e sempre que $y \in B$ então também $y \in A$.

## 1.2 Subconjuntos e conjuntos potência

Com frequência quereremos comparar conjuntos. E um tipo óbvio de comparação que se pode fazer é o seguinte: *tudo o que está num conjunto está também no outro*. Esta situação é suficientemente importante para introduzirmos nova notação.

**Definição 1.5 (Subconjunto).** Se todo membro de um conjunto $A$ é também um membro de $B$, então dizemos que $A$ é um *subconjunto* de $B$, e escrevemos $A \subseteq B$. Se $A$ não é subconjunto de $B$, escrevemos $A \nsubseteq B$. Se $A \subseteq B$ mas $A \neq B$, escrevemos $A \subsetneq B$ e dizemos que $A$ é um *subconjunto próprio* de $B$.

**Exemplo 1.6.** Todo conjunto é subconjunto de si próprio, e $\emptyset$ é subconjunto de todo conjunto. O conjunto dos números naturais pares é subconjunto do conjunto dos números naturais. Também $\{a, b\} \subseteq \{a, b, c\}$. Mas $\{a, b, e\}$ não é subconjunto de $\{a, b, c\}$.

**Exemplo 1.7.** O número 2 é um membro do conjunto dos inteiros, ao passo que o conjunto dos números pares é subconjunto do conjunto dos inteiros. Contudo, um conjunto pode tanto ser um membro quanto subconjunto de algum outro conjunto, por exemplo, $\{0\} \in \{0, \{0\}\}$ e também $\{0\} \subseteq \{0, \{0\}\}$.

A extensionalidade dá um critério de identidade para conjuntos: $A = B$ se e só se todo membro de $A$ é também um membro de $B$ e vice-versa. A definição de "subconjunto" define $A \subseteq B$ precisamente como a primeira metade deste critério: todo membro de $A$ é também um membro de $B$. Claro que a definição também se aplica se trocarmos $A$ e $B$: isto é, $B \subseteq A$ se e só se todo membro de $B$ é também um membro de $A$. E isso, por sua vez, é exatamente a parte "vice-versa" da extensionalidade. Em outras palavras, a extensionalidade implica que conjuntos são iguais se e só se são subconjuntos um do outro.

**Proposição 1.8.** *$A = B$ se e só se $A \subseteq B$ e $B \subseteq A$.*

Agora é também boa ocasião para introduzir mais alguma notação útil. Ao definir quando $A$ é subconjunto de $B$ dissemos que "todo membro de $A$ é $\ldots$," e preenchemos os "$\ldots$" com "um membro de $B$". Mas esta é uma *forma* tão comum de expressão que convém introduzir notação formal para ela.

**Definição 1.9.** $(\forall x \in A)\varphi$ abrevia $\forall x(x \in A \to \varphi)$. Do mesmo modo, $(\exists x \in A)\varphi$ abrevia $\exists x(x \in A \wedge \varphi)$.

Com esta notação, podemos dizer que $A \subseteq B$ se e só se $(\forall x \in A)x \in B$.

Passamos agora a considerar um certo tipo de conjunto: o conjunto de todos os subconjuntos de um dado conjunto.

**Definição 1.10 (Conjunto potência).** O conjunto constituído por todos os subconjuntos de um conjunto $A$ chama-se o *conjunto potência* de $A$, e denota-se $\wp(A)$.

$$\wp(A) = \{B : B \subseteq A\}$$

**Exemplo 1.11.** Quais são todos os subconjuntos possíveis de $\{a, b, c\}$? São: $\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, $\{a, b, c\}$. O conjunto de todos estes subconjuntos é $\wp(\{a, b, c\})$:

$$\wp(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$$

## 1.3 Alguns Conjuntos Importantes

**Exemplo 1.12.** Trabalharemos sobretudo com conjuntos cujos membros são objetos matemáticos. Quatro desses conjuntos são tão importantes que têm

nomes específicos:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$
o conjunto dos números naturais

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$
o conjunto dos números inteiros

$$\mathbb{Q} = \{m/n : m, n \in \mathbb{Z} \text{ e } n \neq 0\}$$
o conjunto dos números racionais

$$\mathbb{R} = (-\infty, \infty)$$
o conjunto dos números reais (o contínuo)

São todos conjuntos *infinitos*, isto é, cada um tem infinitos membros.

À medida que percorremos estes conjuntos, vamos acrescentando *mais* números ao nosso repertório. De fato, deve ficar claro que $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$: afinal, todo número natural é um inteiro; todo inteiro é racional; e todo racional é real. Igualmente, deve ficar claro que $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q}$, pois $-1$ é inteiro mas não natural, e $1/2$ é racional mas não inteiro. É menos óbvio que $\mathbb{Q} \subsetneq \mathbb{R}$, isto é, que há números reais que não são racionais.

Também usaremos por vezes o conjunto dos inteiros positivos $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ e o conjunto que contém apenas os dois primeiros naturais $\mathbb{B} = \{0, 1\}$.

**Exemplo 1.13 (Cadeias).** Outro exemplo interessante é o conjunto $A^*$ das *cadeias finitas* sobre um alfabeto $A$: qualquer sequência finita de elementos de $A$ é uma cadeia sobre $A$. Incluímos a *cadeia vazia* $\Lambda$ entre as cadeias sobre $A$, para todo alfabeto $A$. Por exemplo,

$$\mathbb{B}^* = \{\Lambda, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, 0000, \ldots\}.$$

Se $x = x_1 \ldots x_n \in A^*$ é uma cadeia constituída por $n$ "letras" de $A$, então dizemos que o *comprimento* da cadeia é $n$ e escrevemos $\text{len}(x) = n$.

**Exemplo 1.14 (Sequências infinitas).** Para qualquer conjunto $A$ podemos também considerar o conjunto $A^\omega$ das sequências infinitas de membros de $A$. Uma sequência infinita $a_1 a_2 a_3 a_4 \ldots$ consiste numa lista infinita numa só direção de objetos, cada um dos quais é um membro de $A$.

## 1.4 Uniões e Interseções

Na Seção 1.1, introduzimos definições de conjuntos por abstração, isto é, definições da forma $\{x : \varphi(x)\}$. Aqui invocamos alguma propriedade $\varphi$, e essa propriedade pode mencionar conjuntos que já definimos. Assim, por exemplo, se $A$

e $B$ são conjuntos, o conjunto $\{x : x \in A \vee x \in B\}$ consiste em todos aqueles objetos que são membros de $A$ ou de $B$, isto é, é o conjunto que reúne os membros de $A$ e $B$. Podemos visualizar isto como na Figura 1.1, onde a área realçada indica os membros dos dois conjuntos $A$ e $B$ juntos.

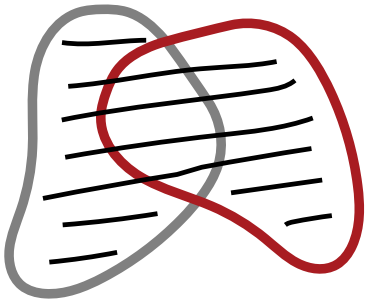


Figura 1.1: A união $A \cup B$ de dois conjuntos é o conjunto dos membros de $A$ juntamente com os de $B$.

Esta operação sobre conjuntos—combiná-los—é muito útil e comum, e por isso damos-lhe um nome formal e um símbolo.

**Definição 1.15 (União).** A *união* de dois conjuntos $A$ e $B$, escrita $A \cup B$, é o conjunto de todas as coisas que são membros de $A$, de $B$, ou de ambos.

$$A \cup B = \{x : x \in A \vee x \in B\}$$

**Exemplo 1.16.** Como a multiplicidade de membros não importa, a união de dois conjuntos que têm um membro em comum contém esse membro apenas uma vez, por exemplo, $\{a, b, c\} \cup \{a, 0, 1\} = \{a, b, c, 0, 1\}$.

A união de um conjunto com um dos seus subconjuntos é simplesmente o conjunto maior: $\{a, b, c\} \cup \{a\} = \{a, b, c\}$.

A união de um conjunto com o conjunto vazio é idêntica ao conjunto: $\{a, b, c\} \cup \emptyset = \{a, b, c\}$.

Também podemos considerar uma operação "dual" à união. É a operação que forma o conjunto de todos os membros que são membros de $A$ e são também membros de $B$. Esta operação chama-se *interseção*, e pode representar-se como na Figura 1.2.

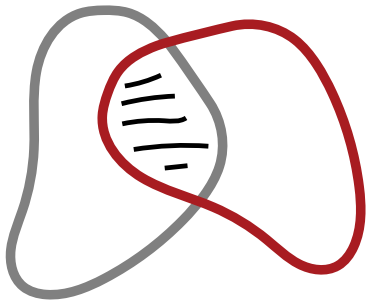


Figura 1.2: A interseção $A \cap B$ de dois conjuntos é o conjunto dos membros que têm em comum.

**Definição 1.17 (Interseção).** A *interseção* de dois conjuntos $A$ e $B$, escrita $A \cap B$, é o conjunto de todas as coisas que são membros de ambos $A$ e $B$.

$$A \cap B = \{x : x \in A \wedge x \in B\}$$

Dois conjuntos dizem-se *disjuntos* se a sua interseção é vazia. Isso significa que não têm membros em comum.

**Exemplo 1.18.** Se dois conjuntos não têm membros em comum, a sua interseção é vazia: $\{a, b, c\} \cap \{0, 1\} = \emptyset$.

Se dois conjuntos têm membros em comum, a sua interseção é o conjunto de todos esses membros: $\{a, b, c\} \cap \{a, b, d\} = \{a, b\}$.

A interseção de um conjunto com um dos seus subconjuntos é simplesmente o conjunto menor: $\{a, b, c\} \cap \{a, b\} = \{a, b\}$.

A interseção de qualquer conjunto com o conjunto vazio é vazia: $\{a, b, c\} \cap \emptyset = \emptyset$.

Também podemos formar a união ou a interseção de mais de dois conjuntos. Uma forma elegante de tratar disso em geral é a seguinte: suponhamos que reunimos num único conjunto todos os conjuntos dos quais queremos formar a união (ou a interseção). Então podemos definir a união de todos os nossos conjuntos originais como o conjunto de todos os objetos que pertencem a pelo menos um membro desse conjunto, e a interseção como o conjunto de todos os objetos que pertencem a todo membro desse conjunto.

**Definição 1.19.** Se $A$ é um conjunto de conjuntos, então $\bigcup A$ é o conjunto dos membros dos membros de $A$:

$$\begin{aligned} \bigcup A &= \{x : x \text{ pertence a um membro de } A\}, \text{ isto é,} \\ &= \{x : \text{existe um } B \in A \text{ tal que } x \in B\} \end{aligned}$$

**Definição 1.20.** Se $A$ é um conjunto de conjuntos, então $\bigcap A$ é o conjunto dos objetos que todos os elementos de $A$ têm em comum:

$$\begin{aligned}\bigcap A &= \{x : x \text{ pertence a todo membro de } A\}, \text{ isto é,}\\ &= \{x : \text{para todo } B \in A, x \in B\}\end{aligned}$$

**Exemplo 1.21.** Suponha $A = \{\{a,b\},\{a,d,e\},\{a,d\}\}$. Então $\bigcup A = \{a,b,d,e\}$ e $\bigcap A = \{a\}$.

Também poderíamos fazer o mesmo para uma sequência de conjuntos $A_1$, $A_2, \ldots$

$$\begin{aligned}\bigcup_i A_i &= \{x : x \text{ pertence a um dos } A_i\}\\ \bigcap_i A_i &= \{x : x \text{ pertence a todos os } A_i\}.\end{aligned}$$

Quando temos um *índice* de conjuntos, isto é, algum conjunto $I$ tal que consideramos $A_i$ para cada $i \in I$, podemos também usar estas abreviaturas:

$$\begin{aligned}\bigcup_{i\in I} A_i &= \bigcup\{A_i : i \in I\}\\ \bigcap_{i\in I} A_i &= \bigcap\{A_i : i \in I\}\end{aligned}$$

Finalmente, podemos querer pensar no conjunto de todos os membros em $A$ que não estão em $B$. Podemos representá-lo como na Figura 1.3.

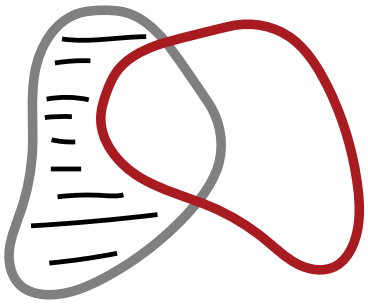


Figura 1.3: A diferença $A \setminus B$ de dois conjuntos é o conjunto dos membros de $A$ que não são também membros de $B$.

**Definição 1.22 (Diferença).** A *diferença* de conjuntos $A \setminus B$ é o conjunto de todos os membros de $A$ que não são também membros de $B$, isto é,

$$A \setminus B = \{x : x \in A \text{ e } x \notin B\}.$$

## 1.5 Pares, Tuplas, Produtos Cartesianos

Da extensionalidade segue-se que os conjuntos não têm ordem entre os seus elementos. Por isso, se queremos representar ordem, usamos *pares ordenados* $\langle x, y\rangle$. Num par não ordenado $\{x, y\}$, a ordem não importa: $\{x, y\} = \{y, x\}$. Num par ordenado, importa: se $x \neq y$, então $\langle x, y\rangle \neq \langle y, x\rangle$.

Como devemos pensar os pares ordenados na teoria dos conjuntos? O essencial é preservar a ideia de que pares ordenados são idênticos se e só se compartilham o mesmo primeiro elemento e o mesmo segundo elemento, isto é:

$$\langle a, b\rangle = \langle c, d\rangle \text{ se e só se } a = c \text{ e } b = d.$$

Podemos definir pares ordenados na teoria dos conjuntos usando a definição de Wiener–Kuratowski.

**Definição 1.23 (Par ordenado).** $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$.

Tendo fixado uma definição de par ordenado, podemos usá-la para definir outros conjuntos. Por exemplo, por vezes queremos sequências ordenadas de mais de dois objetos, p.ex., *triplos* $\langle x, y, z\rangle$, *quádruplos* $\langle x, y, z, u\rangle$, e assim por diante. Podemos pensar nos triplos como pares ordenados especiais, em que o primeiro elemento é ele próprio um par ordenado: $\langle x, y, z\rangle$ é $\langle\langle x, y\rangle, z\rangle$. O mesmo vale para quádruplos: $\langle x, y, z, u\rangle$ é $\langle\langle\langle x, y\rangle, z\rangle, u\rangle$, e assim por diante. Em geral, falamos de *n-tuplas ordenadas* $\langle x_1, \ldots, x_n\rangle$.

Certos conjuntos de pares ordenados, ou outras $n$-tuplas ordenadas, serão úteis.

**Definição 1.24 (Produto cartesiano).** Dados conjuntos $A$ e $B$, o seu *produto cartesiano* $A \times B$ é definido por

$$A \times B = \{\langle x, y\rangle : x \in A \text{ e } y \in B\}.$$

**Exemplo 1.25.** Se $A = \{0, 1\}$, e $B = \{1, a, b\}$, então o seu produto é

$$A \times B = \{\langle 0, 1\rangle, \langle 0, a\rangle, \langle 0, b\rangle, \langle 1, 1\rangle, \langle 1, a\rangle, \langle 1, b\rangle\}.$$

**Exemplo 1.26.** Se $A$ é um conjunto, o produto de $A$ consigo próprio, $A \times A$, também se escreve $A^2$. É o conjunto de *todos* os pares $\langle x, y\rangle$ com $x, y \in A$. O conjunto de todos os triplos $\langle x, y, z\rangle$ é $A^3$, e assim por diante. Podemos dar uma definição recursiva:

$$A^1 = A$$
$$A^{k+1} = A^k \times A$$

**Proposição 1.27.** *Se $A$ tem $n$ membros e $B$ tem $m$ membros, então $A \times B$ tem $n \cdot m$ elementos.*

*Prova.* Para todo membro $x$ em $A$, há $m$ membros da forma $\langle x, y\rangle \in A \times B$. Seja $B_x = \{\langle x, y\rangle : y \in B\}$. Como sempre que $x_1 \neq x_2$, $\langle x_1, y\rangle \neq \langle x_2, y\rangle$, tem-se $B_{x_1} \cap B_{x_2} = \emptyset$. Mas se $A = \{x_1, \ldots, x_n\}$, então $A \times B = B_{x_1} \cup \cdots \cup B_{x_n}$, e portanto tem $n \cdot m$ membros.

Para visualizar isto, dispomos os membros de $A \times B$ numa grade:

$$\begin{array}{rccccc} B_{x_1} = & \{\langle x_1, y_1\rangle & \langle x_1, y_2\rangle & \ldots & \langle x_1, y_m\rangle\} \\ B_{x_2} = & \{\langle x_2, y_1\rangle & \langle x_2, y_2\rangle & \ldots & \langle x_2, y_m\rangle\} \\ \vdots & & \vdots & & \\ B_{x_n} = & \{\langle x_n, y_1\rangle & \langle x_n, y_2\rangle & \ldots & \langle x_n, y_m\rangle\} \end{array}$$

Como os $x_i$ são todos distintos, e os $y_j$ são todos distintos, quaisquer dois pares nesta grade são distintos, e há $n \cdot m$ deles. □

**Exemplo 1.28.** Se $A$ é um conjunto, uma *palavra* sobre $A$ é qualquer sequência de membros de $A$. Uma sequência pode ser vista como uma $n$-tupla de membros de $A$. Por exemplo, se $A = \{a, b, c\}$, então a sequência "*bac*" pode ser vista como o triplo $\langle b, a, c\rangle$. Palavras, isto é, sequências de símbolos, são de importância crucial na ciência da computação. Por convenção, contamos os membros de $A$ como sequências de comprimento 1, e $\emptyset$ como a sequência de comprimento 0. O conjunto de *todas* as palavras sobre $A$ é então

$$A^* = \{\emptyset\} \cup A \cup A^2 \cup A^3 \cup \ldots$$

## 1.6 Paradoxo de Russell

A extensionalidade autoriza a notação $\{x : \varphi(x)\}$, para *o* conjunto dos $x$ tais que $\varphi(x)$. Contudo, tudo o que a extensionalidade *realmente* autoriza é o seguinte pensamento. *Se* há um conjunto cujos membros são exatamente os que satisfazem $\varphi$, *então* há apenas um tal conjunto. Dito de outro modo: fixada alguma $\varphi$, o conjunto $\{x : \varphi(x)\}$ é único, *se existir*.

Mas este condicional é importante! Crucialmente, nem toda propriedade se presta à *compreensão*. Isto é, algumas propriedades *não* definem conjuntos. Se todas definissem, cairíamos em contradições flagrantes. O exemplo mais famoso disso é o Paradoxo de Russell.

Os conjuntos podem ser membros de outros conjuntos—por exemplo, o conjunto potência de um conjunto $A$ é constituído por conjuntos. Por isso faz sentido perguntar ou investigar se um conjunto é um membro de outro conjunto. Pode um conjunto ser membro de si próprio? Nada na ideia de conjunto parece excluir isso. Por exemplo, se *todos* os conjuntos formam uma coleção de objetos, alguém poderia pensar que podem reunir-se num único conjunto—o conjunto de todos os conjuntos. E ele, sendo conjunto, seria um membro do conjunto de todos os conjuntos.

O Paradoxo de Russell surge quando consideramos a propriedade de não ter a si próprio como um membro, de ser *não auto-membro*. E se supusermos que há um conjunto de todos os conjuntos que não têm a si próprios como um membro? Será que

$$R = \{x : x \notin x\}$$

existe? Verifica-se que podemos provar que não.

**Teorema 1.29 (Paradoxo de Russell).** *Não há conjunto* $R = \{x : x \notin x\}$.

*Prova.* Se $R = \{x : x \notin x\}$ existisse, então $R \in R$ se e só se $R \notin R$, o que é uma contradição. □

Vamos percorrer esta prova mais devagar. Se $R$ existe, faz sentido perguntar se $R \in R$ ou não. Suponhamos que de fato $R \in R$. Agora, $R$ foi definido como o conjunto de todos os conjuntos que não são membros de si próprios. Logo, se $R \in R$, então $R$ não tem a propriedade definidora de $R$. Mas só os conjuntos que têm essa propriedade estão em $R$, logo $R$ não pode ser um membro de $R$, isto é, $R \notin R$. Mas $R$ não pode ao mesmo tempo ser e não ser um membro de $R$, logo temos uma contradição.

Como a suposição de que $R \in R$ leva a uma contradição, temos $R \notin R$. Mas isto também leva a uma contradição! Pois se $R \notin R$, então $R$ tem a propriedade definidora de $R$, e assim $R$ seria um membro de $R$, tal como todos os outros conjuntos não auto-membros. E de novo, $R$ não pode ao mesmo tempo não ser e ser um membro de $R$.

Como montar uma teoria dos conjuntos que evite cair no Paradoxo de Russell, isto é, que evite afirmar de modo *inconsistente* que $R = \{x : x \notin x\}$ existe? Teríamos de estabelecer axiomas que nos dêem condições muito precisas para dizer quando os conjuntos existem (e quando não existem).

A teoria dos conjuntos esboçada neste capítulo não faz isso. É *genuinamente ingênua*. Diz apenas que os conjuntos obedecem à extensionalidade e que, se temos alguns conjuntos, podemos formar a sua união, interseção, etc. É possível desenvolver a teoria dos conjuntos com mais rigor do que isto.

## Problemas

**Problema 1.1.** Prove que há no máximo um conjunto vazio, isto é, mostre que se $A$ e $B$ são conjuntos sem membros, então $A = B$.

**Problema 1.2.** Liste todos os subconjuntos de $\{a, b, c, d\}$.

**Problema 1.3.** Mostre que se $A$ tem $n$ membros, então $\wp(A)$ tem $2^n$ membros.

**Problema 1.4.** Prove que se $A \subseteq B$, então $A \cup B = B$.

**Problema 1.5.** Prove rigorosamente que se $A \subseteq B$, então $A \cap B = A$.

**Problema 1.6.** Mostre que se $A$ é um conjunto e $A \in B$, então $A \subseteq \bigcup B$.

**Problema 1.7.** Prove que se $A \subsetneq B$, então $B \setminus A \neq \emptyset$.

**Problema 1.8.** Usando Definição 1.23, prove que $\langle a, b\rangle = \langle c, d\rangle$ se e só se $a = c$ e $b = d$.

**Problema 1.9.** Liste todos os membros de $\{1, 2, 3\}^3$.

**Problema 1.10.** Mostre, por indução em $k$, que para todo $k \geq 1$, se $A$ tem $n$ membros, então $A^k$ tem $n^k$ membros.

# Capítulo 2

# Relações

## 2.1 Relações como Conjuntos

Na Seção 1.3, mencionamos alguns conjuntos importantes: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Sem dúvida que se lembram de algumas relações interessantes entre os membros de alguns destes conjuntos. Por exemplo, cada um destes conjuntos tem uma *relação de ordem* completamente padrão sobre si. Há também a relação *ser idêntico a*, segundo a qual cada objeto só se relaciona consigo próprio e com nenhum outro. Há muitas outras relações interessantes que encontraremos, e ainda mais relações possíveis. Antes de as revermos, contudo, começaremos por observar que podemos ver relações como um tipo especial de conjunto.

Para isso, recordemos duas coisas da Seção 1.5. Primeiro, recordemos a noção de *par ordenado*: dados $a$ e $b$, podemos formar $\langle a, b\rangle$. É importante notar que a ordem dos elementos *importa* aqui. Assim, se $a \neq b$ então $\langle a, b\rangle \neq \langle b, a\rangle$. (Contrastemos isto com pares não ordenados, isto é, conjuntos de 2 elementos, onde $\{a, b\} = \{b, a\}$.) Segundo, recordemos a noção de *produto cartesiano*: se $A$ e $B$ são conjuntos, então podemos formar $A \times B$, o conjunto de todos os pares $\langle x, y\rangle$ com $x \in A$ e $y \in B$. Em particular, $A^2 = A \times A$ é o conjunto de todos os pares ordenados de $A$.

Consideremos agora uma relação particular num conjunto: a relação $<$ no conjunto $\mathbb{N}$ dos números naturais. Seja o conjunto de todos os pares de números $\langle n, m\rangle$ onde $n < m$, isto é,

$$R = \{\langle n, m\rangle : n, m \in \mathbb{N} \text{ e } n < m\}.$$

Há uma ligação estreita entre $n$ ser menor que $m$, e o par $\langle n, m\rangle$ ser membro de $R$, nomeadamente:

$$n < m \text{ se e só se } \langle n, m\rangle \in R.$$

De fato, sem qualquer perda de informação, podemos considerar o conjunto $R$ como *sendo* a relação $<$ em $\mathbb{N}$.

Do mesmo modo podemos construir um subconjunto de $\mathbb{N}^2$ para qualquer relação entre números. Reciprocamente, dado qualquer conjunto de pares de números $S \subseteq \mathbb{N}^2$, há uma relação correspondente entre números, nomeadamente, a relação segundo a qual $n$ se liga a $m$ se e só se $\langle n, m\rangle \in S$. Isto justifica a definição seguinte:

**Definição 2.1 (Relação binária).** Uma *relação binária* num conjunto $A$ é um subconjunto de $A^2$. Se $R \subseteq A^2$ é uma relação binária em $A$ e $x, y \in A$, por vezes escrevemos $Rxy$ (ou $xRy$) para $\langle x, y\rangle \in R$.

**Exemplo 2.2.** O conjunto $\mathbb{N}^2$ dos pares de números naturais pode ser listado numa matriz bidimensional assim:

$$\begin{array}{ccccc}
\langle \mathbf{0},\mathbf{0}\rangle & \langle 0,1\rangle & \langle 0,2\rangle & \langle 0,3\rangle & \dots \\
\langle 1,0\rangle & \langle \mathbf{1},\mathbf{1}\rangle & \langle 1,2\rangle & \langle 1,3\rangle & \dots \\
\langle 2,0\rangle & \langle 2,1\rangle & \langle \mathbf{2},\mathbf{2}\rangle & \langle 2,3\rangle & \dots \\
\langle 3,0\rangle & \langle 3,1\rangle & \langle 3,2\rangle & \langle \mathbf{3},\mathbf{3}\rangle & \dots \\
\vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Colocamos a diagonal, aqui, em negrito, pois o subconjunto de $\mathbb{N}^2$ constituído pelos pares que estão na diagonal, isto é,

$$\{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,2\rangle, \dots\},$$

é a *relação identidade em* $\mathbb{N}$. (Como a relação identidade é popular, definamos $\mathrm{Id}_A = \{\langle x, x\rangle : x \in A\}$ para qualquer conjunto $A$.) O subconjunto de todos os pares acima da diagonal, isto é,

$$L = \{\langle 0,1\rangle, \langle 0,2\rangle, \dots, \langle 1,2\rangle, \langle 1,3\rangle, \dots, \langle 2,3\rangle, \langle 2,4\rangle, \dots\},$$

é a relação *menor que*, isto é, $Lnm$ se e só se $n < m$. O subconjunto dos pares abaixo da diagonal, isto é,

$$G = \{\langle 1,0\rangle, \langle 2,0\rangle, \langle 2,1\rangle, \langle 3,0\rangle, \langle 3,1\rangle, \langle 3,2\rangle, \dots\},$$

é a relação *maior que*, isto é, $Gnm$ se e só se $n > m$. A união de $L$ com $I$, que podemos chamar $K = L \cup I$, é a relação *menor ou igual a*: $Knm$ se e só se $n \leq m$. Do mesmo modo, $H = G \cup I$ é a *relação maior ou igual a*. Estas relações $L$, $G$, $K$, e $H$ são tipos especiais de relações chamadas *ordens*. $L$ e $G$ gozam da propriedade de que nenhum número está em relação $L$ ou $G$ consigo próprio (isto é, para todo $n$, não se verifica nem $Lnn$ nem $Gnn$). Relações com esta propriedade chamam-se *irreflexivas*, e, se também forem ordens, chamam-se *ordens estritas.*

Embora ordens e identidade sejam relações importantes e naturais, convém enfatizar que, segundo a nossa definição, *qualquer* subconjunto de $A^2$ é uma

relação em $A$, por mais artificial ou forçado que pareça. Em particular, $\emptyset$ é uma relação em qualquer conjunto (a *relação vazia*, que nenhum par de elementos satisfaz), e $A^2$ em si é também uma relação em $A$ (uma que todo par de elementos satisfaz), chamada a *relação universal*. Mas também algo como $E = \{\langle n, m\rangle : n > 5 \text{ ou } m \times n \geq 34\}$ conta como relação.

## 2.2 Reflexões Filosóficas

Na Seção 2.1, definimos relações como certos conjuntos. Devemos fazer uma pausa e colocar uma questão filosófica rápida: o que é que tal definição *faz*? É extremamente duvidoso que devamos querer dizer que *descobrimos* fatos metafísicos de identidade; que, por exemplo, a relação de ordem em $\mathbb{N}$ *acabou por ser* o conjunto $R = \{\langle n, m\rangle : n, m \in \mathbb{N} \text{ e } n < m\}$ que definimos na Seção 2.1. Eis três razões para isso.

Primeiro: na Definição 1.23, definimos $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$. Consideremos em vez disso a definição $\|a, b\| = \{\{b\}, \{a, b\}\} = \langle b, a\rangle$. Quando $a \neq b$, temos que $\langle a, b\rangle \neq \|a, b\|$. Mas poderíamos com a mesma facilidade ter tomado $\|a, b\|$ como a nossa definição de par ordenado, em vez de $\langle a, b\rangle$. Ambas as definições teriam funcionado igualmente bem. Assim, temos dois candidatos igualmente bons a "ser" a relação de ordem nos números naturais, nomeadamente:

$$R = \{\langle n, m\rangle : n, m \in \mathbb{N} \text{ e } n < m\}$$
$$S = \{\|n, m\| : n, m \in \mathbb{N} \text{ e } n < m\}.$$

Como $R \neq S$, pela extensionalidade, é claro que não podem *ambos* ser idênticos à relação de ordem em $\mathbb{N}$. Mas seria meramente arbitrário, e por isso um pouco embaraçoso, afirmar que $R$ em vez de $S$ (ou vice-versa) *é* a relação de ordenação, como questão de fato. (Isto é um caso muito simples de um argumento contra o reducionismo em teoria dos conjuntos que Benacerraf tornou famoso em 1965. Voltaremos a ele várias vezes.)

Segundo: se pensamos que *toda* a relação deve ser identificada com um conjunto, então a própria relação de pertinência a conjuntos, $\in$, deveria ser um conjunto particular. De fato, teria de ser o conjunto $\{\langle x, y\rangle : x \in y\}$. Mas será que este conjunto existe? Dado o Paradoxo de Russell, é uma afirmação não trivial que tal conjunto exista. De fato, é possível desenvolver a teoria dos conjuntos de modo rigoroso como teoria axiomática, e essa teoria de fato nega a existência deste conjunto. Logo, mesmo que algumas relações possam ser tratadas como conjuntos, a relação de pertinência a conjuntos terá de ser um caso especial.

Terceiro: quando "identificamos" relações com conjuntos, dissemos que nos permitiríamos escrever $Rxy$ para $\langle x, y\rangle \in R$. Isto está bem, desde que a relação de pertinência, "$\in$", seja tratada *como* um predicado. Mas se pensamos que "$\in$" denota um certo tipo de conjunto, então a expressão "$\langle x, y\rangle \in R$"

consiste apenas em três termos singulares que denotam conjuntos: "$\langle x, y\rangle$", "$\in$", e "$R$". E tal lista de nomes não é mais capaz de exprimir uma proposição do que a sequência sem sentido: "o copo porta-canetas a mesa". De novo, mesmo que algumas relações possam ser tratadas como conjuntos, a relação de pertinência a conjuntos tem de ser um caso especial. (Isto reúne num só argumento uma versão simples do paradoxo do conceito *cavalo* de Frege, e uma objeção célebre que Wittgenstein dirigiu a Russell.)

Então onde nos deixa isto? Bem, não há nada de *errado* em dizermos que as relações nos números são conjuntos. Só temos de compreender o espírito em que tal observação é feita. Não enunciamos um fato metafísico de identidade. Limitamo-nos a notar que, em certos contextos, podemos (e iremos) *tratar* (certas) relações como certos conjuntos.

## 2.3 Propriedades Especiais das Relações

Alguns tipos de relações revelam-se tão comuns que receberam nomes especiais. Por exemplo, $\leq$ e $\subseteq$ relacionam os seus respectivos domínios (digamos, $\mathbb{N}$ no caso de $\leq$ e $\wp(A)$ no caso de $\subseteq$) de modos semelhantes. Para precisar exatamente como estas relações são semelhantes, e como diferem, as categorizamos segundo algumas propriedades especiais que as relações podem ter. Verifica-se que (combinações de) algumas destas propriedades especiais são especialmente importantes: ordens e relações de equivalência.

**Definição 2.3 (Reflexividade).** Uma relação $R \subseteq A^2$ é *reflexiva* se e só se, para todo $x \in A$, $Rxx$.

**Definição 2.4 (Transitividade).** Uma relação $R \subseteq A^2$ é *transitiva* se e só se, sempre que $Rxy$ e $Ryz$, então também $Rxz$.

**Definição 2.5 (Simetria).** Uma relação $R \subseteq A^2$ é *simétrica* se e só se, sempre que $Rxy$, então também $Ryx$.

**Definição 2.6 (Antissimetria).** Uma relação $R \subseteq A^2$ é *antissimétrica* se e só se, sempre que tanto $Rxy$ quanto $Ryx$, então $x = y$ (ou, noutras palavras: se $x \neq y$ então ou $\neg Rxy$ ou $\neg Ryx$).

Numa relação simétrica, $Rxy$ e $Ryx$ verificam-se sempre em conjunto, ou nenhuma se verifica. Numa relação antissimétrica, a única forma de $Rxy$ e $Ryx$ se verificarem em conjunto é que $x = y$. Note-se que isto não *exige* que $Rxy$ e $Ryx$ se verifiquem quando $x = y$, apenas que isso não está excluído. Assim, uma relação antissimétrica pode ser reflexiva, mas não é o caso que toda relação antissimétrica seja reflexiva. Note-se também que ser antissimétrica e ser meramente não simétrica são condições diferentes. De fato, uma relação pode ser ao mesmo tempo simétrica e antissimétrica (por exemplo, a relação identidade o é).

**Definição 2.7 (Conexidade).** Uma relação $R \subseteq A^2$ é *conexa* se para todos $x, y \in A$, se $x \neq y$, então ou $Rxy$ ou $Ryx$.

**Definição 2.8 (Irreflexividade).** Uma relação $R \subseteq A^2$ diz-se *irreflexiva* se, para todo $x \in A$, não $Rxx$.

**Definição 2.9 (Assimetria).** Uma relação $R \subseteq A^2$ diz-se *assimétrica* se para nenhum par $x, y \in A$ se tem tanto $Rxy$ quanto $Ryx$.

Note-se que se $A \neq \emptyset$, então nenhuma relação irreflexiva em $A$ é reflexiva e toda relação assimétrica em $A$ é também antissimétrica. Contudo, há $R \subseteq A^2$ que não são reflexivas nem irreflexivas, e há relações antissimétricas que não são assimétricas.

## 2.4 Relações de Equivalência

A relação identidade num conjunto é reflexiva, simétrica e transitiva. Relações $R$ que têm todas as três destas propriedades são muito comuns.

**Definição 2.10 (Relação de equivalência).** Uma relação $R \subseteq A^2$ que é reflexiva, simétrica e transitiva chama-se uma *relação de equivalência*. Membros $x$ e $y$ de $A$ dizem-se *R-equivalentes* se $Rxy$.

As relações de equivalência dão origem à noção de *classe de equivalência*. Uma relação de equivalência "reparte" o domínio em partições distintas. Dentro de cada partição, todos os objetos estão relacionados uns com os outros; e objetos de partições diferentes não se relacionam entre si. Por vezes, é útil falar destas partições *diretamente*. Para esse fim, introduzimos uma definição:

**Definição 2.11.** Seja $R \subseteq A^2$ uma relação de equivalência. Para cada $x \in A$, a *classe de equivalência* de $x$ em $A$ é o conjunto $[x]_R = \{y \in A : Rxy\}$. O *quociente* de $A$ por $R$ é $A/_R = \{[x]_R : x \in A\}$, isto é, o conjunto destas classes de equivalência.

O resultado seguinte justifica a definição de classe de equivalência, provando que as classes de equivalência são de fato as partições de $A$:

**Proposição 2.12.** *Se $R \subseteq A^2$ é uma relação de equivalência, então $Rxy$ se e só se $[x]_R = [y]_R$.*

*Prova.* Para o sentido da esquerda para a direita, suponhamos $Rxy$, e seja $z \in [x]_R$. Por definição, então, $Rxz$. Como $R$ é uma relação de equivalência, $Ryz$. (Explicando melhor: como $Rxy$ e $R$ é simétrica temos $Ryx$, e como $Rxz$ e $R$ é transitiva temos $Ryz$.) Logo $z \in [y]_R$. Generalizando, $[x]_R \subseteq [y]_R$. Mas de modo perfeitamente análogo, $[y]_R \subseteq [x]_R$. Logo $[x]_R = [y]_R$, pela extensionalidade.

Para o sentido da direita para a esquerda, suponhamos $[x]_R = [y]_R$. Como $R$ é reflexiva, $Ryy$, logo $y \in [y]_R$. Assim também $y \in [x]_R$ pela suposição de que $[x]_R = [y]_R$. Logo $Rxy$. □

**Exemplo 2.13.** Um bom exemplo de relações de equivalência vem da aritmética modular. Para quaisquer $a$, $b$, e $n \in \mathbb{Z}^+$, digamos que $a \equiv_n b$ se e só se dividir $a$ por $n$ dá o mesmo resto que dividir $b$ por $n$. (De modo um pouco mais simbólico: $a \equiv_n b$ se e só se, para algum $k \in \mathbb{Z}$, $a - b = kn$.) Agora, $\equiv_n$ é uma relação de equivalência, para qualquer $n$. E há exatamente $n$ classes de equivalência distintas geradas por $\equiv_n$; isto é, $\mathbb{N}/_{\equiv_n}$ tem $n$ membros. São: o conjunto dos números divisíveis por $n$ sem resto, isto é, $[0]_{\equiv_n}$; o conjunto dos números divisíveis por $n$ com resto 1, isto é, $[1]_{\equiv_n}$; ...; e o conjunto dos números divisíveis por $n$ com resto $n - 1$, isto é, $[n-1]_{\equiv_n}$.

## 2.5 Ordens

Muitas das nossas comparações envolvem descrever certos objetos como sendo "menores que", "iguais a" ou "maiores que" outros objetos, sob algum aspecto. Isso envolve relações de *ordem*. Mas há vários tipos de relação de ordem. Por exemplo, algumas exigem que quaisquer dois objetos sejam comparáveis, outras não. Algumas incluem a identidade (como $\leq$) e outras a excluem (como $<$). Ter aqui uma taxonomia ajuda-nos.

**Definição 2.14 (Pré-ordem).** Uma relação que é ao mesmo tempo reflexiva e transitiva chama-se uma *pré-ordem.*

**Definição 2.15 (Ordem parcial).** Uma pré-ordem que também é antissimétrica chama-se uma *ordem parcial*.

**Definição 2.16 (Ordem linear).** Uma ordem parcial que também é conexa chama-se uma *ordem total* ou *ordem linear.*

**Exemplo 2.17.** Toda ordem linear é também uma ordem parcial, e toda ordem parcial é também uma pré-ordem, mas as implicações recíprocas não valem. A relação universal sobre $A$ é uma pré-ordem, pois é reflexiva e transitiva. Mas, se $A$ tem mais de um membro, a relação universal não é antissimétrica e, portanto, não é uma ordem parcial.

**Exemplo 2.18.** Considere a relação *não mais longa que* $\preccurlyeq$ sobre $\mathbb{B}^*$: $x \preccurlyeq y$ sse $\text{len}(x) \leq \text{len}(y)$. Trata-se de uma pré-ordem (reflexiva e transitiva), e até conexa, mas não é uma ordem parcial, pois não é antissimétrica. Por exemplo, $01 \preccurlyeq 10$ e $10 \preccurlyeq 01$, mas $01 \neq 10$.

**Exemplo 2.19.** Uma ordem parcial importante é a relação $\subseteq$ sobre um conjunto de conjuntos. Em geral não é uma ordem linear: se $a \neq b$ e consideramos $\wp(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$, vemos que $\{a\} \not\subseteq \{b\}$ e $\{a\} \neq \{b\}$ e $\{b\} \not\subseteq \{a\}$.

**Exemplo 2.20.** A relação de *divisibilidade sem resto* nos dá uma ordem parcial que não é linear. Para inteiros $n$ e $m$, escrevemos $n \mid m$ para significar que $n$ divide $m$ (exatamente), isto é, sse existe algum inteiro $k$ tal que $m = kn$. Sobre $\mathbb{N}$, isso é uma ordem parcial, mas não linear: por exemplo, $2 \nmid 3$ e também $3 \nmid 2$. Vista como relação sobre $\mathbb{Z}$, a divisibilidade é apenas uma pré-ordem, pois não é antissimétrica: $1 \mid -1$ e $-1 \mid 1$ mas $1 \neq -1$.

**Exemplo 2.21.** A relação de *extensão* sobre um conjunto de sequências $A^*$ é a seguinte: $s \sqsubseteq s'$ sse $s = \Lambda$ (a sequência vazia), $s = s'$, ou $s = \langle s_1, \ldots, s_n \rangle$ e $s' = \langle s_1, \ldots, s_n, s_{n+1}, \ldots, s_m \rangle$. Se $s \sqsubseteq s'$ dizemos também que $s$ é um *segmento inicial* de $s'$. A relação de extensão sobre $A^*$ é uma ordem parcial, mas não linear, p.ex., se $a \neq b$, então $ab \not\sqsubseteq ba$ e $ba \not\sqsubseteq ab$.

**Definição 2.22 (Ordem estrita).** Uma *ordem estrita* é uma relação irreflexiva, assimétrica e transitiva.

**Definição 2.23 (Ordem linear estrita).** Uma ordem estrita que também é conexa chama-se *ordem total estrita* ou *ordem linear estrita.*

**Exemplo 2.24.** $\leq$ é a ordem linear correspondente à ordem linear estrita $<$. $\subseteq$ é a ordem parcial correspondente à ordem estrita $\subsetneq$.

Qualquer ordem estrita $R$ sobre $A$ pode transformar-se numa ordem parcial adicionando a diagonal $\mathrm{Id}_A$, isto é, adicionando todos os pares $\langle x, x \rangle$. (Isto chama-se o *fecho reflexivo* de $R$.) Reciprocamente, a partir de uma ordem parcial obtém-se uma ordem estrita removendo $\mathrm{Id}_A$. Os dois resultados seguintes tornam isto preciso.

**Proposição 2.25.** *Se $R$ é uma ordem estrita sobre $A$, então $R^+ = R \cup \mathrm{Id}_A$ é uma ordem parcial. Além disso, se $R$ é uma ordem linear estrita, então $R^+$ é uma ordem linear.*

*Prova.* Suponhamos que $R$ é uma ordem estrita, isto é, $R \subseteq A^2$ e $R$ é irreflexiva, assimétrica e transitiva. Seja $R^+ = R \cup \mathrm{Id}_A$. Temos de mostrar que $R^+$ é reflexiva, antissimétrica e transitiva.

$R^+$ é claramente reflexiva, pois $\langle x, x \rangle \in \mathrm{Id}_A \subseteq R^+$ para todo $x \in A$.

Para mostrar que $R^+$ é antissimétrica, suponhamos, para redução ao absurdo, que $R^+xy$ e $R^+yx$ mas $x \neq y$. Como $\langle x, y \rangle \in R \cup \mathrm{Id}_A$, mas $\langle x, y \rangle \notin \mathrm{Id}_A$, temos de ter $\langle x, y \rangle \in R$, isto é, $Rxy$. Do mesmo modo, $Ryx$. Mas isto contradiz a hipótese de que $R$ é assimétrica.

Para estabelecer a transitividade, suponhamos que $R^+xy$ e $R^+yz$. Se tanto $\langle x, y\rangle \in R$ como $\langle y, z\rangle \in R$, então $\langle x, z\rangle \in R$, pois $R$ é transitiva. Caso contrário, ou $\langle x, y\rangle \in \mathrm{Id}_A$, isto é, $x = y$, ou $\langle y, z\rangle \in \mathrm{Id}_A$, isto é, $y = z$. No primeiro caso, temos $R^+yz$ por hipótese, $x = y$, logo $R^+xz$. Analogamente no segundo caso. Em qualquer caso, $R^+xz$; assim, $R^+$ é também transitiva.

Quanto à cláusula "além disso", suponhamos que $R$ é também conexa. Então, para todo $x \neq y$, ou $Rxy$ ou $Ryx$, isto é, ou $\langle x, y\rangle \in R$ ou $\langle y, x\rangle \in R$. Como $R \subseteq R^+$, isto continua a valer para $R^+$, logo $R^+$ é também conexa. □

**Proposição 2.26.** *Se $R$ é uma ordem parcial sobre $A$, então $R^- = R \setminus \mathrm{Id}_A$ é uma ordem estrita. Além disso, se $R$ é uma ordem linear, então $R^-$ é uma ordem linear estrita.*

*Prova.* Deixamos como exercício. □

O resultado simples a seguir estabelece que ordens lineares estritas satisfazem uma propriedade no estilo da extensionalidade:

**Proposição 2.27.** *Se $<$ é uma ordem linear estrita sobre $A$, então:*

$$(\forall a, b \in A)((\forall x \in A)(x < a \leftrightarrow x < b) \to a = b).$$

*Prova.* Suponhamos $(\forall x \in A)(x < a \leftrightarrow x < b)$. Se $a < b$, então $a < a$, o que contradiz o fato de $<$ ser irreflexiva; logo $a \not< b$. De forma totalmente análoga, $b \not< a$. Logo $a = b$, pois $<$ é conexa. □

## 2.6 Grafos

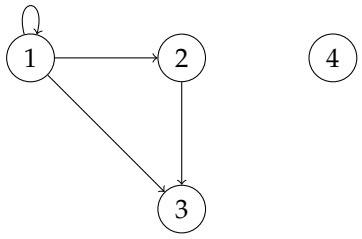
Um *grafo* é um diagrama no qual pontos—chamados "nós" ou "vértices" (plural de "vértice")—são conectados por arestas. Grafos são uma ferramenta onipresente em matemática discreta e em ciência da computação. São incrivelmente úteis para representar e visualizar relações e estruturas, desde coisas concretas como redes de vários tipos até estruturas abstratas como os possíveis resultados de decisões. Existem muitos tipos diferentes de grafos na literatura que diferem, p.ex., quanto a se as arestas são direcionadas ou não, têm rótulos ou não, se pode haver arestas de um nó para o mesmo nó, múltiplas arestas entre os mesmos nós, etc. *Grafos direcionados* têm uma conexão especial com relações.

**Definição 2.28 (Grafo direcionado).** Um *grafo direcionado* $G = \langle V, E\rangle$ é um conjunto de *vértices* $V$ e um conjunto de *arestas* $E \subseteq V^2$.

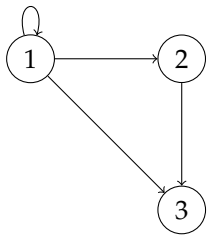
De acordo com nossa definição, um grafo é simplesmente um conjunto junto com uma relação nesse conjunto. Claro, ao falar de grafos, é natural esperar que sejam representados graficamente: podemos desenhar um grafo conectando dois vértices $v_1$ e $v_2$ por uma seta sse $\langle v_1, v_2\rangle \in E$. A única diferença

entre uma relação por si só e um grafo é que um grafo especifica o conjunto de vértices, isto é, um grafo pode ter vértices isolados. O ponto importante, porém, é que toda relação $R$ em um conjunto $X$ pode ser vista como um grafo direcionado $\langle X, R\rangle$, e reciprocamente, um grafo direcionado $\langle V, E\rangle$ pode ser visto como uma relação $E \subseteq V^2$ com o conjunto $V$ explicitamente especificado.

**Exemplo 2.29.** O grafo $\langle V, E\rangle$ com $V = \{1, 2, 3, 4\}$ e $E = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle\}$ se parece com isto:



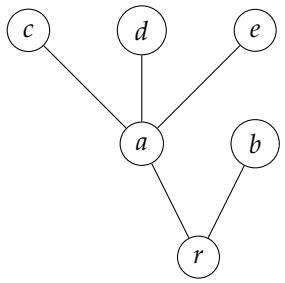

Este é um grafo diferente de $\langle V', E\rangle$ com $V' = \{1, 2, 3\}$, que se parece com isto:




## 2.7 Árvores

Um tipo particular de ordem parcial que desempenha um papel importante em todas as partes da lógica é uma *árvore*. Árvores finitas aparecem em partes elementares da lógica: por exemplo, fórmulas podem ser entendidas em termos de sua decomposição em uma árvore sintática, enquanto derivações em muitos sistemas de derivação também tomam a forma de árvores finitas. Árvores infinitas aparecem já na prova dos teoremas de completude para a lógica proposicional e de primeira ordem, e são usadas em toda a lógica matemática.

O conceito de árvore da teoria dos conjuntos está intimamente relacionado à noção de árvore na teoria dos grafos. Aqui está uma figura de uma árvore (finita):




O nó mais baixo $r$ é a raiz. Todo nó diferente de $r$ tem exatamente um nó pai imediatamente abaixo dele. Podemos pensar na relação em que um nó $x$ está para um nó $y$ se $y$ pode ser alcançado a partir de $x$ seguindo arestas para cima como $x$ sendo um *ancestral* de $y$.

A relação de ancestralidade em uma árvore é uma ordem parcial estrita. Isso motiva a definição teórico-conjuntista. Para enunciá-la, precisamos de dois conceitos. Um *menor elemento* em um conjunto $A$ parcialmente ordenado por $\leq$ é um membro $x \in A$ tal que para todo $y \in A$ temos que $x \leq y$. Um conjunto é *bem ordenado* por $\leq$ se cada um de seus subconjuntos não vazios tem um menor elemento.

**Definição 2.30 (Árvore).** Uma *árvore* é um par $T = \langle A, \leq \rangle$ tal que $A$ é um conjunto e $\leq$ é uma ordem parcial em $A$ com um único menor elemento $r \in A$ (chamado de *raiz*) tal que para todo $x \in A$, o conjunto $\{y : y \leq x\}$ é bem ordenado por $\leq$.

**Definição 2.31 (Sucessores).** Suponha $T = \langle A, \leq \rangle$ é uma árvore. Se $x, y \in A$, $x < y$, e não existe $z \in A$ tal que $x < z < y$, então dizemos que $y$ é um *sucessor* de $x$.

Os sucessores de $x \in A$ também são chamados de seus *filhos*. Se $y$ é um sucessor de $x$, então chamamos $x$ de *predecessor* ou *pai* de $y$.

**Proposição 2.32.** *Se $\langle A, \leq \rangle$ é uma árvore, então todo $x \in A$ diferente da raiz tem no máximo um predecessor.*

*Prova.* Suponha $y_1 < x$ e $y_2 < x$ e $y_1 \neq y_2$. Então $\{y_1, y_2\} \subseteq \{z : z < x\}$. Como $\{z : z < x\}$ é bem ordenado por $\leq$, seu subconjunto $\{y_1, y_2\}$ tem um menor elemento, que obviamente deve ser ou $y_1$ ou $y_2$. Então ou $y_1 \leq y_2$ ou $y_2 \leq y_1$. Supusemos que $y_1 \neq y_2$, então na verdade ou $y_1 < y_2$ ou $y_2 < y_1$. Como supusemos que $y_1 < x$ e $y_2 < x$, temos ainda que ou $y_1 < y_2 < x$ ou $y_2 < y_1 < x$. Então $y_1$ e $y_2$ não podem ambos ser predecessores de $x$. □

**Definição 2.33.** Uma árvore $T = \langle A, \leq \rangle$ é dita *infinita* se $A$ é um conjunto infinito, e *finita* caso contrário. Se $T$ é tal que todo $x \in A$ tem apenas um número finito de sucessores, então dizemos que $T$ é *finitamente ramificada*.

**Definição 2.34 (Ramos).** Dada uma árvore $T = \langle A, \leq \rangle$, um *ramo* de $T$ é uma cadeia maximal em $T$, isto é, um conjunto $B \subseteq A$ tal que para quaisquer $x, y \in B$ ou $x \leq y$ ou $y \leq x$, e para qualquer $z \in X \setminus B$ existe $u \in B$ tal que nem $z \leq u$ nem $u \leq z$. Usamos $[T]$ para denotar o conjunto de todos os ramos de $T$.

**Exemplo 2.35.** Um exemplo clássico de árvore finitamente ramificada é a *árvore binária infinita* de sequências finitas de 0s e 1s, às vezes denotada $\{0,1\}^*$ ou $\mathbb{B}^*$, ordenada pela relação de extensão $\sqsubseteq$ (p.ex., $101 \sqsubseteq 101101$). Como qualquer cadeia binária pode sempre ser estendida adicionando um 0 ou um 1 no final, esta árvore contém infinitos elementos: todo elemento $s$ tem exatamente dois sucessores, $s0$ e $s1$. Sua raiz é a sequência vazia $\Lambda$.

**Exemplo 2.36.** De maneira um pouco mais geral, o conjunto de sequências finitas de números naturais $\mathbb{N}^*$ com a relação de extensão $\sqsubseteq$ também é uma árvore. É obviamente não finitamente ramificada: todo $s \in \mathbb{N}^*$ tem infinitos sucessores $sn$, um para cada $n \in \mathbb{N}$. Todo $A \subseteq \mathbb{N}^*$ que é fechado sob $\sqsubseteq$ é uma *subárvore* de $\mathbb{N}^*$. (Isto é, $A$ é tal que se $s \in A$ e $s' \sqsubseteq s$, então também $s' \in A$.) Todas as árvores finitas podem ser representadas como subárvores finitas de $\mathbb{N}^*$.

**Proposição 2.37 (Lema de Kőnig).** *Se $T = \langle A, \leq \rangle$ é uma árvore infinita finitamente ramificada, então $T$ tem um ramo infinito.*

Um caso especial do Lema de Kőnig amplamente usado em teoria da computabilidade, conhecido como *Lema Fraco de Kőnig*, é o seguinte: qualquer subárvore infinita de $\{0,1\}^*$ tem um ramo infinito.

## 2.8 Operações sobre Relações

É frequentemente útil modificar ou combinar relações. Na Proposição 2.25, consideramos a *união* de relações, que é apenas a união de duas relações vistas como conjuntos de pares. Do mesmo modo, na Proposição 2.26, consideramos a diferença relativa de relações. Eis algumas outras operações que podemos efetuar sobre relações.

**Definição 2.38.** Sejam $R$ e $S$ relações, e $A$ um conjunto qualquer.
A *inversa* de $R$ é $R^{-1} = \{\langle y, x\rangle : \langle x, y\rangle \in R\}$.
O *produto relativo* de $R$ e $S$ é $(R \mid S) = \{\langle x, z\rangle : \exists y(Rxy \wedge Syz)\}$.
A *restrição* de $R$ a $A$ é $R\restriction_A = R \cap A^2$.
A *aplicação* de $R$ a $A$ é $R[A] = \{y : (\exists x \in A)Rxy\}$

**Exemplo 2.39.** Seja $S \subseteq \mathbb{Z}^2$ a relação sucessora sobre $\mathbb{Z}$, isto é, $S = \{\langle x, y\rangle \in \mathbb{Z}^2 : x + 1 = y\}$, de modo que $Sxy$ sse $x + 1 = y$.
$S^{-1}$ é a relação antecessora sobre $\mathbb{Z}$, isto é, $\{\langle x, y\rangle \in \mathbb{Z}^2 : x - 1 = y\}$.
$S \mid S$ é $\{\langle x, y\rangle \in \mathbb{Z}^2 : x + 2 = y\}$

$S\restriction_{\mathbb{N}}$ é a relação sucessora sobre $\mathbb{N}$.
$S[\{1,2,3\}]$ é $\{2,3,4\}$.

**Definição 2.40 (Fecho transitivo).** Seja $R \subseteq A^2$ uma relação binária.

O *fecho transitivo* de $R$ é $R^+ = \bigcup_{0<n\in\mathbb{N}} R^n$, onde definimos recursivamente $R^1 = R$ e $R^{n+1} = R^n \mid R$.

O *fecho reflexivo transitivo* de $R$ é $R^* = R^+ \cup \mathrm{Id}_A$.

**Exemplo 2.41.** Tome a relação sucessora $S \subseteq \mathbb{Z}^2$. $S^2xy$ sse $x+2 = y$, $S^3xy$ sse $x+3 = y$, etc. Logo $S^+xy$ sse $x+n = y$ para algum $n \geq 1$. Em outras palavras, $S^+xy$ sse $x < y$, e $S^*xy$ sse $x \leq y$.

## Problemas

**Problema 2.1.** Liste os membros da relação $\subseteq$ no conjunto $\wp(\{a,b,c\})$.

**Problema 2.2.** Dê exemplos de relações que sejam (a) reflexivas e simétricas mas não transitivas, (b) reflexivas e antissimétricas, (c) antissimétricas, transitivas, mas não reflexivas, e (d) reflexivas, simétricas e transitivas. Não use relações sobre números ou conjuntos.

**Problema 2.3.** Mostre que $\equiv_n$ é uma relação de equivalência, para qualquer $n \in \mathbb{Z}^+$, e que $\mathbb{N}/_{\equiv_n}$ tem exatamente $n$ membros.

**Problema 2.4.** Apresente uma prova da Proposição 2.26.

**Problema 2.5.** Considere a relação menor ou igual a $\leq$ no conjunto $\{1,2,3,4\}$ como um grafo e desenhe o diagrama correspondente.

**Problema 2.6.** Mostre que o fecho transitivo de $R$ é de fato transitivo.

# Capítulo 3

# Funções

## 3.1 Noções Básicas

Uma *função* é um mapa que envia cada membro de um dado conjunto para um membro específico em algum (outro) conjunto dado. Por exemplo, a operação de somar 1 define uma função: cada número $n$ é mapeado para um único número $n + 1$.

Mais em geral, funções podem tomar pares, triplos, etc., como entradas e devolver algum tipo de saída. Muitas funções nos são familiares da aritmética básica. Por exemplo, a adição e a multiplicação são funções. Tomam dois números e devolvem um terceiro.

Neste sentido matemático e abstrato, uma função é uma *caixa preta*: só importa que saída fica associada a que entrada, não o método de calcular a saída.

**Definição 3.1 (Função).** Uma *função* $f\colon A \to B$ é um mapeamento de cada membro de $A$ para um membro de $B$.

Chamamos $A$ de *domínio* de $f$ e $B$ de *contradomínio* de $f$. Os membros de $A$ chamam-se entradas ou *argumentos* de $f$, e o membro de $B$ que fica associado a um argumento $x$ por $f$ chama-se o *valor de* $f$ para o argumento $x$, escrevendo-se $f(x)$.

A *imagem* $\mathrm{Im}(f)$ de $f$ é o subconjunto do contradomínio constituído pelos valores de $f$ para algum argumento; $\mathrm{Im}(f) = \{f(x) : x \in A\}$.

O diagrama na Figura 3.1 pode ajudar a pensar em funções. A elipse à esquerda representa o *domínio* da função; a elipse à direita representa o *contradomínio*; e uma seta aponta de um *argumento* no domínio para o *valor* correspondente no contradomínio.

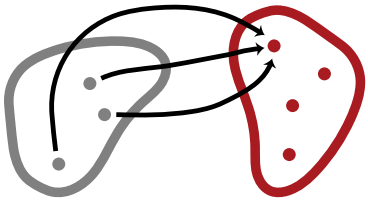


Figura 3.1: Uma função é um mapeamento de cada membro de um conjunto para um membro de outro. Uma seta vai de um argumento no domínio para o valor correspondente no contradomínio.

**Exemplo 3.2.** A multiplicação toma pares de números naturais como entradas e mapeia-os para números naturais como saídas, logo vai de $\mathbb{N} \times \mathbb{N}$ (o domínio) para $\mathbb{N}$ (o contradomínio). Como se vê, a imagem é também $\mathbb{N}$, pois todo $n \in \mathbb{N}$ é $n \times 1$.

**Exemplo 3.3.** A multiplicação é uma função porque associa cada entrada—cada par de números naturais—a uma única saída: $\times : \mathbb{N}^2 \to \mathbb{N}$. Em contraste, mapear um número natural $n$ para um real $x$ tal que $x^2 = n$ não é funcional, pois cada inteiro positivo $n$ tem duas raízes quadradas: $\sqrt{n}$ e $-\sqrt{n}$. Podemos torná-la funcional devolvendo só a raiz quadrada positiva: $\sqrt{\ } : \mathbb{N} \to \mathbb{R}$.

**Exemplo 3.4.** A relação que associa cada aluno de uma turma à sua nota final é uma função—nenhum aluno pode ter duas notas finais diferentes na mesma turma. A relação que associa cada aluno de uma turma aos seus progenitores não é uma função: os alunos podem ter zero, ou dois, ou mais progenitores.

Podemos definir funções especificando de modo preciso qual é o valor da função para cada argumento possível. Formas de o fazer são dar uma fórmula, descrever um método para calcular o valor, ou listar os valores para cada argumento. Como quer que as funções sejam definidas, temos de garantir que, para cada argumento, especificamos um, e apenas um, valor.

**Exemplo 3.5.** Seja $f : \mathbb{N} \to \mathbb{N}$ definida por $f(x) = x + 1$. Esta é uma definição que especifica $f$ como uma função que toma números naturais e devolve números naturais. Diz-nos que, dado um número natural $x$, $f$ devolverá o seu sucessor $x + 1$. Neste caso, o contradomínio $\mathbb{N}$ não é a imagem de $f$, pois o número natural 0 não é sucessor de nenhum número natural. A imagem de $f$ é o conjunto de todos os inteiros positivos, $\mathbb{Z}^+$.

**Exemplo 3.6.** Seja $g : \mathbb{N} \to \mathbb{N}$ definida por $g(x) = x + 2 - 1$. Isto nos diz que $g$ é uma função que toma números naturais e devolve números naturais. Dado um número natural $n$, $g$ devolverá o predecessor do sucessor do sucessor de $n$, isto é, $n + 1$.

Acabamos de considerar duas funções, $f$ e $g$, com *definições* diferentes. Contudo, são a *mesma função*. Afinal, para qualquer número natural $n$, temos $f(n) = n + 1 = n + 2 - 1 = g(n)$. Em outras palavras: as nossas definições de $f$ e $g$ especificam o mesmo mapeamento por meio de equações diferentes. Implicitamente, pois, estamos nos apoiando num princípio de extensionalidade para funções,

$$\text{se } \forall x\, f(x) = g(x), \text{ então } f = g$$

desde que $f$ e $g$ compartilhem o mesmo domínio e contradomínio.

**Exemplo 3.7.** Também podemos definir funções por casos. Por exemplo, poderíamos definir $h\colon \mathbb{N} \to \mathbb{N}$ por

$$h(x) = \begin{cases} \frac{x}{2} & \text{se } x \text{ é par} \\ \frac{x+1}{2} & \text{se } x \text{ é ímpar.} \end{cases}$$

Como todo número natural é par ou ímpar, a saída desta função será sempre um número natural. Basta lembrar que, se se define uma função por casos, cada entrada possível tem de cair em exatamente um caso. Em alguns casos, isto exigirá uma prova de que os casos são exaustivos e exclusivos.

## 3.2 Tipos de Funções

Será útil introduzir uma espécie de taxonomia para alguns dos tipos de funções que encontramos com mais frequência.

Para começar, podemos querer considerar funções com a propriedade de que todo *membro* do contradomínio é um valor da função. Tais funções chamam-se sobrejetivas, e podem ser esquematizadas como na Figura 3.2.

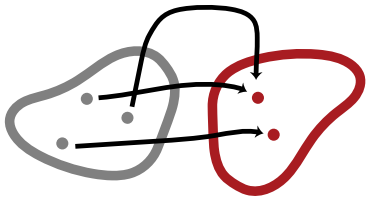


Figura 3.2: Uma função sobrejetiva tem todo membro do contradomínio como valor.

**Definição 3.8 (Função Sobrejetiva).** Uma função $f\colon A \to B$ é *sobrejetiva* se e só se $B$ é também a imagem de $f$, isto é, para todo $y \in B$ existe pelo menos um $x \in A$ tal que $f(x) = y$, ou em símbolos:

$$(\forall y \in B)(\exists x \in A) f(x) = y.$$

Chamamos a tal função uma sobrejeção de $A$ para $B$.

Se quiser mostrar que $f$ é uma sobrejeção, tem de mostrar que todo objeto no contradomínio de $f$ é o valor de $f(x)$ para alguma entrada $x$.

Note-se que qualquer função *induz* uma sobrejeção. Afinal, dada uma função $f\colon A \to B$, seja $f'\colon A \to \mathrm{Im}(f)$ definida por $f'(x) = f(x)$. Como $\mathrm{Im}(f)$ é *definida* como $\{f(x) \in B : x \in A\}$, esta função $f'$ é garantidamente uma sobrejeção

Agora, qualquer função mapeia cada entrada possível para uma única saída. Mas há também funções que nunca mapeiam entradas diferentes para a mesma saída. Tais funções chamam-se injetivas, e podem ser esquematizadas como na Figura 3.3.

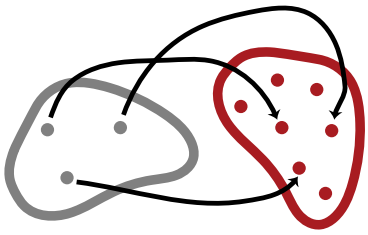


Figura 3.3: Uma função injetiva nunca mapeia dois argumentos diferentes para o mesmo valor.

**Definição 3.9 (Função Injetiva).** Uma função $f\colon A \to B$ é *injetiva* se e só se, para cada $y \in B$, há no máximo um $x \in A$ tal que $f(x) = y$. Chamamos a tal função uma injeção de $A$ para $B$.

Se quiser mostrar que $f$ é uma injeção, tem de mostrar que, para quaisquer membros $x$ e $y$ do domínio de $f$, se $f(x) = f(y)$, então $x = y$.

**Exemplo 3.10.** A função constante $f\colon \mathbb{N} \to \mathbb{N}$ dada por $f(x) = 1$ não é nem injetiva, nem sobrejetiva.

A função identidade $f\colon \mathbb{N} \to \mathbb{N}$ dada por $f(x) = x$ é tanto injetiva quanto sobrejetiva.

A função sucessora $f\colon \mathbb{N} \to \mathbb{N}$ dada por $f(x) = x + 1$ é injetiva mas não sobrejetiva.

A função $f\colon \mathbb{N} \to \mathbb{N}$ definida por:

$$f(x) = \begin{cases} \frac{x}{2} & \text{se } x \text{ é par} \\ \frac{x+1}{2} & \text{se } x \text{ é ímpar.} \end{cases}$$

é sobrejetiva, mas não injetiva.

Muitas vezes, queremos considerar funções que são tanto injetivas como sobrejetivas. Chamamos a tais funções bijetivas. Parecem-se com a função

esquematizada na Figura 3.4. Bijeções são também por vezes chamadas *correspondências biunívocas*, pois associam de modo único elementos do contradomínio a elementos do domínio.

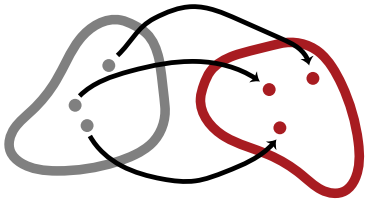


Figura 3.4: Uma função bijetiva associa de modo único os elementos do contradomínio aos do domínio.

**Definição 3.11 (Bijeção).** Uma função $f\colon A \to B$ é *bijetiva* se e só se é tanto sobrejetiva como injetiva. Chamamos a tal função uma bijeção de $A$ para $B$ (ou entre $A$ e $B$).

## 3.3 Funções como Relações

Uma função que mapeia membros de $A$ para membros de $B$ define obviamente uma relação entre $A$ e $B$, nomeadamente a relação que se verifica entre $x$ e $y$ se e só se $f(x) = y$. De fato, podemos até—se nos interessa reduzir os blocos de construção da matemática, por exemplo—*identificar* a função $f$ com esta relação, isto é, com um conjunto de pares. Isto levanta então a questão: que relações definem funções deste modo?

**Definição 3.12 (Gráfico de uma função).** Seja $f\colon A \to B$ uma função. O *gráfico* de $f$ é a relação $R_f \subseteq A \times B$ definida por

$$R_f = \{\langle x, y\rangle : f(x) = y\}.$$

O gráfico de uma função fica unicamente determinado, pela extensionalidade. Além disso, a extensionalidade (sobre conjuntos) justifica de imediato o princípio implícito de extensionalidade para funções, segundo o qual, se $f$ e $g$ compartilham domínio e contradomínio, então são idênticas se coincidem em todos os valores.

Do mesmo modo, se uma relação é "funcional", então é o gráfico de uma função.

**Proposição 3.13.** *Seja $R \subseteq A \times B$ tal que:*

1. *Se $Rxy$ e $Rxz$, então $y = z$; e*
2. *para todo $x \in A$ existe algum $y \in B$ tal que $\langle x, y\rangle \in R$.*

*Então $R$ é o gráfico da função $f\colon A \to B$ definida por $f(x) = y$ se e só se $Rxy$.*

*Prova.* Suponhamos que existe $y$ tal que $Rxy$. Se existisse outro $z \neq y$ tal que $Rxz$, a condição sobre $R$ seria violada. Logo, se existe $y$ tal que $Rxy$, esse $y$ é único, e assim $f$ está bem definida. Obviamente, $R_f = R$. □

Toda função $f\colon A \to B$ tem um gráfico, isto é, uma relação em $A \times B$ definida por $f(x) = y$. Por outro lado, toda relação $R \subseteq A \times B$ com as propriedades dadas na Proposição 3.13 é o gráfico de uma função $f\colon A \to B$. Por causa desta ligação estreita entre funções e os seus gráficos, podemos pensar numa função simplesmente como o seu gráfico. Em outras palavras, funções podem identificar-se com certas relações, isto é, com certos conjuntos de tuplos. Note, contudo, que o espírito desta "identificação" é como na Seção 2.2: não é uma afirmação sobre a metafísica das funções, mas a observação de que é conveniente *tratar* funções como certos conjuntos. Uma razão pela qual isto é tão conveniente é que podemos agora considerar fazer operações semelhantes sobre funções às que fizemos sobre relações (ver Seção 2.8). Em particular:

**Definição 3.14.** Seja $f\colon A \to B$ uma função com $C \subseteq A$.

A *restrição* de $f$ a $C$ é a função $f{\restriction_C}\colon C \to B$ definida por $(f{\restriction_C})(x) = f(x)$ para todo $x \in C$. Em outras palavras, $f{\restriction_C} = \{\langle x, y\rangle \in R_f : x \in C\}$.

A *aplicação* de $f$ a $C$ é $f[C] = \{f(x) : x \in C\}$. Chamamos-lhe também a *imagem* de $C$ por $f$.

Segue-se destas definições que $\mathrm{Im}(f) = f[\mathrm{dom}(f)]$, para qualquer função $f$. Estas noções são exatamente as que se esperaria, dadas as definições na Seção 2.8 e a nossa identificação de funções com relações. Mas outras duas operações—inversas e produtos relativos—exigem um pouco mais de detalhe. Trataremos disso na Seção 3.4 e na Seção 3.5.

## 3.4 Inversas de Funções

Pensamos nas funções como mapas. Uma pergunta natural sobre funções é, pois, se o mapeamento pode ser "invertido". Por exemplo, a função sucessora $f(x) = x + 1$ pode ser invertida, no sentido em que a função $g(y) = y - 1$ "desfaz" o que $f$ faz.

Mas é preciso ter cuidado. Embora a definição de $g$ defina uma função $\mathbb{Z} \to \mathbb{Z}$, não define uma *função* $\mathbb{N} \to \mathbb{N}$, pois $g(0) \notin \mathbb{N}$. Assim, mesmo em casos simples, não é óbvio que uma função possa ser invertida; pode depender do domínio e do contradomínio.

Isto torna-se mais preciso com a noção de inversa de uma função.

**Definição 3.15.** Uma função $g\colon B \to A$ é uma *inversa* de uma função $f\colon A \to B$ se $f(g(y)) = y$ e $g(f(x)) = x$ para todo $x \in A$ e $y \in B$.

Se $f$ tem uma inversa $g$, escrevemos muitas vezes $f^{-1}$ em vez de $g$.

Agora determinaremos quando as funções têm inversas. Um bom candidato a inversa de $f\colon A \to B$ é $g\colon B \to A$ "definida por"

$$g(y) = \text{"o" } x \text{ tal que } f(x) = y.$$

Mas as aspas em "definida por" (e em "o") sugerem que isto não é uma definição. Pelo menos, nem sempre funcionará com total generalidade. Pois, para que esta definição especifique uma função, tem de haver um e apenas um $x$ tal que $f(x) = y$—a saída de $g$ tem de ficar unicamente determinada. Além disso, tem de estar especificada para todo $y \in B$. Se existirem $x_1$ e $x_2 \in A$ com $x_1 \neq x_2$ mas $f(x_1) = f(x_2)$, então $g(y)$ não ficaria unicamente determinada para $y = f(x_1) = f(x_2)$. E se não existir $x$ algum tal que $f(x) = y$, então $g(y)$ nem sequer fica especificada. Em outras palavras, para $g$ estar definida, $f$ tem de ser tanto injetiva quanto sobrejetiva.

Vamos com calma. Dividiremos a questão em duas: dada uma função $f\colon A \to B$, quando existe uma função $g\colon B \to A$ tal que $g(f(x)) = x$? Tal $g$ "desfaz" o que $f$ faz, e chama-se *inversa à esquerda* de $f$. Em segundo lugar, quando existe uma função $h\colon B \to A$ tal que $f(h(y)) = y$? Tal $h$ chama-se *inversa à direita* de $f$—$f$ "desfaz" o que $h$ faz.

**Proposição 3.16.** *Se $f\colon A \to B$ é injetiva, então existe uma* inversa à esquerda *$g\colon B \to A$ de $f$ tal que $g(f(x)) = x$ para todo $x \in A$.*

*Prova.* Suponhamos que $f\colon A \to B$ é injetiva. Consideremos $y \in B$. Se $y \in \operatorname{Im}(f)$, existe $x \in A$ tal que $f(x) = y$. Como $f$ é injetiva, há apenas um tal $x \in A$. Então podemos definir: $g(y) = x$, isto é, $g(y)$ é "o" $x \in A$ tal que $f(x) = y$. Se $y \notin \operatorname{Im}(f)$, podemos mapeá-lo para qualquer $a \in A$. Assim, podemos escolher $a \in A$ e definir $g\colon B \to A$ por:

$$g(y) = \begin{cases} x & \text{se } f(x) = y \\ a & \text{se } y \notin \operatorname{Im}(f). \end{cases}$$

Está definida para todo $y \in B$, pois para cada tal $y \in \operatorname{Im}(f)$ há exatamente um $x \in A$ tal que $f(x) = y$. Por definição, se $y = f(x)$, então $g(y) = x$, isto é, $g(f(x)) = x$. □

**Proposição 3.17.** *Se $f\colon A \to B$ é sobrejetiva, então existe uma* inversa à direita *$h\colon B \to A$ de $f$ tal que $f(h(y)) = y$ para todo $y \in B$.*

*Prova.* Suponhamos que $f\colon A \to B$ é sobrejetiva. Consideremos $y \in B$. Como $f$ é sobrejetiva, existe $x_y \in A$ com $f(x_y) = y$. Então podemos definir: $h(y) = x_y$, isto é, para cada $y \in B$ escolhemos algum $x \in A$ tal que $f(x) = y$; como

$f$ é sobrejetiva há sempre pelo menos um de onde escolher.[1] Por definição, se $x = h(y)$, então $f(x) = y$, isto é, para todo $y \in B$, $f(h(y)) = y$. □

Combinando as ideias da prova anterior, obtemos agora que toda bijeção tem uma inversa, isto é, existe uma única função que é tanto inversa à esquerda quanto à direita de $f$.

**Proposição 3.18.** *Se $f\colon A \to B$ é bijetiva, existe uma função $f^{-1}\colon B \to A$ tal que, para todo $x \in A$, $f^{-1}(f(x)) = x$ e, para todo $y \in B$, $f(f^{-1}(y)) = y$.*

*Prova.* Exercício. □

Há uma forma ligeiramente mais geral de extrair inversas. Vimos na Seção 3.2 que toda função $f$ induz uma sobrejeção $f'\colon A \to \mathrm{Im}(f)$ pondo $f'(x) = f(x)$ para todo $x \in A$. Claramente, se $f$ é injetiva, então $f'$ é bijetiva, logo tem uma inversa única pela Proposição 3.18. Por um pequeno abuso de notação, chamamos por vezes à inversa de $f'$ simplesmente "a inversa de $f$."

**Proposição 3.19.** *Mostre que, se $f\colon A \to B$ tem uma inversa à esquerda $g$ e uma inversa à direita $h$, então $h = g$.*

*Prova.* Exercício. □

**Proposição 3.20.** *Toda função $f$ tem no máximo uma inversa.*

*Prova.* Suponhamos que $g$ e $h$ são ambas inversas de $f$. Então, em particular, $g$ é uma inversa à esquerda de $f$ e $h$ é uma inversa à direita. Pela Proposição 3.19, $g = h$. □

## 3.5 Composição de Funções

Vimos na Seção 3.4 que a inversa $f^{-1}$ de uma bijeção $f$ é ela própria uma função. Outra operação sobre funções é a composição: podemos definir uma nova função compondo duas funções, $f$ e $g$, isto é, aplicando primeiro $f$ e depois $g$. Claro que isto só é possível se as imagens e os domínios forem compatíveis, isto é, a imagem de $f$ tem de ser um subconjunto do domínio de $g$. Esta operação sobre funções é o análogo da operação de produto relativo sobre relações na Seção 2.8.

[1] Como $f$ é sobrejetiva, para todo $y \in B$ o conjunto $\{x : f(x) = y\}$ é não vazio. A nossa definição de $h$ exige que escolhamos um único $x$ em cada um destes conjuntos. Que isto seja sempre possível não é de todo óbvio—a possibilidade de fazer estas escolhas é simplesmente assumida como axioma. Em outras palavras, esta proposição pressupõe o chamado Axioma da Escolha, questão a que voltaremos no Capítulo 73. Contudo, em muitos casos concretos, p.ex., quando $A = \mathbb{N}$ ou é finito, ou quando $f$ é bijetiva, o Axioma da Escolha não é necessário. (No caso em que $f$ é bijetiva, para cada $y \in B$ o conjunto $\{x : f(x) = y\}$ tem exatamente um membro, logo não há escolha a fazer.)

Um diagrama pode ajudar a explicar a ideia de composição. Na Figura 3.5, representamos duas funções $f\colon A \to B$ e $g\colon B \to C$ e a sua composição $(g \circ f)$. A função $(g \circ f)\colon A \to C$ associa cada membro de $A$ a um membro de $C$. Especificamos a que membro de $C$ fica associado um membro de $A$ do seguinte modo: dada uma entrada $x \in A$, aplicamos primeiro a função $f$ a $x$, obtendo algum $f(x) = y \in B$, depois aplicamos a função $g$ a $y$, obtendo algum $g(f(x)) = g(y) = z \in C$.

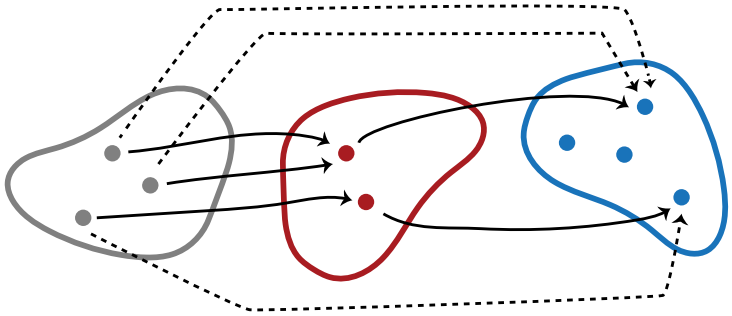


Figura 3.5: A composição $g \circ f$ de duas funções $f$ e $g$.

**Definição 3.21 (Composição).** Sejam $f\colon A \to B$ e $g\colon B \to C$ funções. A *composição* de $f$ com $g$ é $g \circ f\colon A \to C$, onde $(g \circ f)(x) = g(f(x))$.

**Exemplo 3.22.** Consideremos as funções $f(x) = x + 1$, e $g(x) = 2x$. Como $(g \circ f)(x) = g(f(x))$, para cada entrada $x$ deve primeiro tomar-se o sucessor, depois multiplicar o resultado por dois. Logo a composição é dada por $(g \circ f)(x) = 2(x + 1)$.

## 3.6 Funções Parciais

Às vezes é útil relaxar a definição de função de modo que não seja exigido que a saída da função esteja definida para todas as entradas possíveis. Tais mapeamentos são chamados de *funções parciais*.

**Definição 3.23.** Uma *função parcial* $f\colon A \nrightarrow B$ é um mapeamento que associa a cada membro de $A$ no máximo um membro de $B$. Se $f$ associa um membro de $B$ a $x \in A$, dizemos que $f(x)$ está *definido*, e caso contrário *indefinido*. Se $f(x)$ está definido, escrevemos $f(x)\downarrow$, caso contrário $f(x)\uparrow$. O *domínio* de uma função parcial $f$ é o subconjunto de $A$ onde ela está definida, isto é, $\mathrm{dom}(f) = \{x \in A : f(x)\downarrow\}$.

**Exemplo 3.24.** Toda função $f\colon A \to B$ é também uma função parcial. Funções parciais que estão definidas em todo $A$—isto é, o que até agora chamávamos simplesmente de função—também são chamadas de funções *totais*.

**Exemplo 3.25.** A função parcial $f\colon \mathbb{R} \nrightarrow \mathbb{R}$ dada por $f(x) = 1/x$ é indefinida para $x = 0$ e definida em todo o restante.

**Definição 3.26 (Gráfico de uma função parcial).** Seja $f\colon A \nrightarrow B$ uma função parcial. O *gráfico* de $f$ é a relação $R_f \subseteq A \times B$ definida por

$$R_f = \{\langle x, y\rangle : f(x) = y\}.$$

**Proposição 3.27.** *Suponha que $R \subseteq A \times B$ tem a propriedade de que sempre que $Rxy$ e $Rxy'$ então $y = y'$. Então $R$ é o gráfico da função parcial $f\colon A \nrightarrow B$ definida por: se existe um $y$ tal que $Rxy$, então $f(x) = y$, caso contrário $f(x) \uparrow$. Se $R$ também é* serial*, isto é, para cada $x \in A$ existe um $y \in B$ tal que $Rxy$, então $f$ é total.*

*Prova.* Suponha que existe um $y$ tal que $Rxy$. Se existisse outro $y' \neq y$ tal que $Rxy'$, a condição sobre $R$ seria violada. Portanto, se existe um $y$ tal que $Rxy$, esse $y$ é único, e assim $f$ é bem definida. Obviamente, $R_f = R$ e $f$ é total se $R$ é serial. □

## Problemas

**Problema 3.1.** Mostre que, se $f\colon A \to B$ tem uma inversa à esquerda $g$, então $f$ é injetiva.

**Problema 3.2.** Mostre que, se $f\colon A \to B$ tem uma inversa à direita $h$, então $f$ é sobrejetiva.

**Problema 3.3.** Prove Proposição 3.18. Tem de definir $f^{-1}$, mostrar que é uma função, e mostrar que é uma inversa de $f$, isto é, $f^{-1}(f(x)) = x$ e $f(f^{-1}(y)) = y$ para todo $x \in A$ e $y \in B$.

**Problema 3.4.** Prove Proposição 3.19.

**Problema 3.5.** Mostre que, se $f\colon A \to B$ e $g\colon B \to C$ são ambas injetiva, então $g \circ f\colon A \to C$ é injetiva.

**Problema 3.6.** Mostre que, se $f\colon A \to B$ e $g\colon B \to C$ são ambas sobrejetiva, então $g \circ f\colon A \to C$ é sobrejetiva.

**Problema 3.7.** Suponhamos $f\colon A \to B$ e $g\colon B \to C$. Mostre que o gráfico de $g \circ f$ é $R_f \mid R_g$.

**Problema 3.8.** Dada $f\colon A \nrightarrow B$, defina a função parcial $g\colon B \nrightarrow A$ por: para qualquer $y \in B$, se existe um único $x \in A$ tal que $f(x) = y$, então $g(y) = x$; caso contrário $g(y) \uparrow$. Mostre que se $f$ é injetiva, então $g(f(x)) = x$ para todo $x \in \mathrm{dom}(f)$ e $f(g(y)) = y$ para todo $y \in \mathrm{Im}(f)$.

# Capítulo 4

# O Tamanho dos Conjuntos

Este capítulo discute enumerações e conjuntos contáveis e incontáveis. Várias seções vêm em duas versões: uma mais elementar, que toma enumerações como listas, ou sobrejeções de $\mathbb{Z}^+$; e uma mais abstrata que define enumerações como bijeções com $\mathbb{N}$.

## 4.1 Introdução

Quando Georg Cantor desenvolveu a teoria dos conjuntos na década de 1870, um dos seus objetivos era tornar aceitável a ideia de uma coleção infinita—um infinito *atual*, como diriam os medievais. Parte central disto foi o seu tratamento do *tamanho* de conjuntos diferentes. Se $a$, $b$ e $c$ são todos distintos, então o conjunto $\{a, b, c\}$ é intuitivamente *maior* que $\{a, b\}$. Mas e os conjuntos infinitos? Serão todos do mesmo tamanho? Acontece que não.

A primeira ideia importante aqui é a de *enumeração*. Podemos listar qualquer conjunto finito enumerando todos os seus membros. Para alguns conjuntos infinitos, também podemos listar todos os seus membros se permitirmos que a própria lista seja infinita. Tais conjuntos chamam-se enumeráveis. O resultado surpreendente de Cantor, que compreenderemos completamente no fim deste capítulo, foi que alguns conjuntos infinitos *não* são enumeráveis.

## 4.2 Enumerações e Conjuntos Enumeráveis

Esta seção discute enumerações de conjuntos, definindo-as como sobrejeções de $\mathbb{Z}^+$. Faz as coisas devagar, para leitores com pouca formação matemática. Uma versão alternativa, mais concisa, é dada na

Seção 4.11, que define enumerações de outro modo: como bijeções com $\mathbb{N}$ (ou um segmento inicial).

Já demos exemplos de conjuntos listando seus membros. Discutamos agora, de maneira mais geral, como e quando podemos listar os membros de um conjunto, mesmo que esse conjunto seja infinito.

**Definição 4.1 (Enumeração, informalmente).** Informalmente, uma *enumeração* de um conjunto $A$ é uma lista (possivelmente infinita) de membros de $A$ tal que todo membro de $A$ aparece na lista em alguma posição finita. Se $A$ tem uma enumeração, então diz-se que $A$ é *enumerável*.

Alguns pontos sobre enumerações:

1. Contamos como enumerações apenas listas que têm um começo e em que todo membro além do primeiro tem um único membro imediatamente anterior. Em outras palavras, há apenas um número finito de elementos entre o primeiro membro da lista e qualquer outro membro. Em particular, isso significa que todo membro de uma enumeração tem uma posição finita: o primeiro membro tem posição 1, o segundo posição 2, etc.

2. Podemos ter enumerações diferentes do mesmo conjunto $A$ que diferem pela ordem em que os membros aparecem: 4, 1, 25, 16, 9 enumera os (conjunto dos) cinco primeiros quadrados tão bem quanto 1, 4, 9, 16, 25.

3. Enumerações redundantes ainda são enumerações: 1, 1, 2, 2, 3, 3, ... enumera o mesmo conjunto que 1, 2, 3, ....

4. Ordem e redundância *importam* quando especificamos uma enumeração: podemos enumerar os inteiros positivos começando com 1, 2, 3, 1, ..., mas o padrão é mais fácil de ver quando enumerados da maneira padrão como 1, 2, 3, 4, ...

5. Enumerações devem ter um começo: ..., 3, 2, 1 não é uma enumeração dos inteiros positivos porque não tem primeiro membro. Para ver como isso segue da definição informal, pergunte a si mesmo: "em que posição na lista o número 76 aparece?"

6. O seguinte não é uma enumeração dos inteiros positivos: 1, 3, 5, ..., 2, 4, 6, ... O problema é que os números pares ocorrem nas posições $\infty + 1$, $\infty + 2$, $\infty + 3$, em vez de em posições finitas.

7. O conjunto vazio é enumerável: é enumerado pela lista vazia!

**Proposição 4.2.** *Se $A$ tem uma enumeração, tem uma enumeração sem repetições.*

*Prova.* Suponha que $A$ tem uma enumeração $x_1, x_2, \ldots$ em que cada $x_i$ é um membro de $A$. Podemos remover repetições de uma enumeração removendo membros repetidos. Por exemplo, podemos transformar a enumeração em uma nova na qual listamos $x_i$ se ele é um membro de $A$ que não está entre $x_1$, $\ldots$, $x_{i-1}$ ou removemos $x_i$ da lista se já aparece entre $x_1, \ldots, x_{i-1}$. □

O último argumento mostra que, para obter um bom controle sobre enumerações e conjuntos enumeráveis e provar coisas sobre eles, precisamos de uma definição mais precisa. O seguinte a fornece.

**Definição 4.3 (Enumeração, formalmente).** Uma *enumeração* de um conjunto $A \neq \emptyset$ é qualquer função sobrejetiva $f\colon \mathbb{Z}^+ \to A$.

Convençamo-nos de que a definição formal e a definição informal usando uma lista possivelmente infinita são equivalentes. Primeiro, qualquer função sobrejetiva de $\mathbb{Z}^+$ para um conjunto $A$ enumera $A$. Tal função determina uma enumeração conforme definido informalmente acima: a lista $f(1)$, $f(2)$, $f(3)$, .... Como $f$ é sobrejetiva, todo membro de $A$ é garantidamente o valor de $f(n)$ para algum $n \in \mathbb{Z}^+$. Logo, todo membro de $A$ aparece em alguma posição finita na lista. Como a função pode não ser injetiva, a lista pode ser redundante, mas isso é aceitável (como observado acima).

Por outro lado, dada uma lista que enumera todos os membros de $A$, podemos definir uma função sobrejetiva $f\colon \mathbb{Z}^+ \to A$ fazendo $f(n)$ ser o $n$-ésimo membro da lista, ou o último membro da lista se não há $n$-ésimo membro. O único caso em que isso não produz uma função sobrejetiva é quando $A$ é vazio, e portanto a lista é vazia. Assim, toda lista não vazia determina uma função sobrejetiva $f\colon \mathbb{Z}^+ \to A$.

**Definição 4.4.** Um conjunto $A$ é enumerável sse é vazio ou tem uma enumeração.

**Exemplo 4.5.** Uma função que enumera os inteiros positivos ($\mathbb{Z}^+$) é simplesmente a função identidade dada por $f(n) = n$. Uma função que enumera os números naturais $\mathbb{N}$ é a função $g(n) = n - 1$.

**Exemplo 4.6.** As funções $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ e $g\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ dadas por

$$f(n) = 2n \text{ e}$$
$$g(n) = 2n - 1$$

enumeram os inteiros positivos pares e os inteiros positivos ímpares, respectivamente. Contudo, nenhuma das funções é uma enumeração de $\mathbb{Z}^+$, já que nenhuma é sobrejetiva.

**Exemplo 4.7.** A função $f(n) = (-1)^n \lceil \frac{(n-1)}{2} \rceil$ (onde $\lceil x \rceil$ denota a função *teto*, que arredonda $x$ para cima até o inteiro mais próximo) enumera o conjunto

dos inteiros $\mathbb{Z}$. Note como $f$ gera os valores de $\mathbb{Z}$ "saltando" de um lado para outro entre inteiros positivos e negativos:

$$\begin{array}{cccccccc} f(1) & f(2) & f(3) & f(4) & f(5) & f(6) & f(7) & \dots \\ -\lceil \frac{0}{2} \rceil & \lceil \frac{1}{2} \rceil & -\lceil \frac{2}{2} \rceil & \lceil \frac{3}{2} \rceil & -\lceil \frac{4}{2} \rceil & \lceil \frac{5}{2} \rceil & -\lceil \frac{6}{2} \rceil & \dots \\ 0 & 1 & -1 & 2 & -2 & 3 & \dots & \end{array}$$

Você também pode pensar em $f$ como definida por casos da seguinte forma:

$$f(n) = \begin{cases} 0 & \text{se } n = 1 \\ n/2 & \text{se } n \text{ é par} \\ -(n-1)/2 & \text{se } n \text{ é ímpar e} > 1 \end{cases}$$

Embora seja talvez mais natural ao listar os membros de um conjunto começar a contar a partir do 1º membro, os matemáticos gostam de usar os números naturais $\mathbb{N}$ para contar coisas. Eles falam do 0º, 1º, 2º, e assim por diante, membro de uma lista. Correspondentemente, podemos definir uma enumeração como uma função sobrejetiva de $\mathbb{N}$ para $A$. É claro que as duas definições são equivalentes.

**Proposição 4.8.** *Há uma sobrejeção $f\colon \mathbb{Z}^+ \to A$ sse há uma sobrejeção $g\colon \mathbb{N} \to A$.*

*Prova.* Dada uma sobrejeção $f\colon \mathbb{Z}^+ \to A$, podemos definir $g(n) = f(n+1)$ para todo $n \in \mathbb{N}$. É fácil ver que $g\colon \mathbb{N} \to A$ é sobrejetiva. Reciprocamente, dada uma sobrejeção $g\colon \mathbb{N} \to A$, defina $f(n) = g(n-1)$. □

Isso nos dá o seguinte resultado:

**Corolário 4.9.** *Um conjunto $A$ é enumerável sse é vazio ou há uma função sobrejetiva $f\colon \mathbb{N} \to A$.*

Discutimos acima que uma lista de membros de um conjunto $A$ pode ser transformada em uma lista sem repetições. Isso também vale para enumerações, mas é um pouco mais difícil de formular e provar rigorosamente. Qualquer função $f\colon \mathbb{Z}^+ \to A$ deve estar definida para todo $n \in \mathbb{Z}^+$. Se há apenas um número finito de membros em $A$, então claramente não podemos ter uma função definida nos infinitos membros de $\mathbb{Z}^+$ que toma como valores todos os membros de $A$ mas nunca toma o mesmo valor duas vezes. Nesse caso, isto é, no caso em que a lista sem repetições é finita, devemos escolher um domínio diferente para $f$, um com apenas um número finito de membros. Não ter repetições significa que $f$ deve ser injetiva. Como também é sobrejetiva, estamos procurando uma bijeção entre algum conjunto finito $\{1, \dots, n\}$ ou $\mathbb{Z}^+$ e $A$.

**Proposição 4.10.** *Se $f\colon \mathbb{Z}^+ \to A$ é sobrejetiva (isto é, uma enumeração de $A$), há uma bijeção $g\colon Z \to A$ onde $Z$ é $\mathbb{Z}^+$ ou $\{1,\ldots,n\}$ para algum $n \in \mathbb{Z}^+$.*

*Prova.* Definimos a função $g$ recursivamente: seja $g(1) = f(1)$. Se $g(i)$ já foi definido, seja $g(i+1)$ o primeiro valor de $f(1), f(2), \ldots$ que ainda não está entre $g(1), \ldots, g(i)$, se houver um. Se $A$ tem apenas $n$ membros, então $g(1)$, $\ldots, g(n)$ estão todos definidos, e assim definimos uma função $g\colon \{1,\ldots,n\} \to A$. Se $A$ tem infinitos membros, então para qualquer $i$ deve haver um membro de $A$ na enumeração $f(1), f(2), \ldots$, que ainda não está entre $g(1), \ldots, g(i)$. Nesse caso definimos uma função $g\colon \mathbb{Z}^+ \to A$.

A função $g$ é sobrejetiva, já que qualquer elemento de $A$ está entre $f(1)$, $f(2), \ldots$ (pois $f$ é sobrejetiva) e assim eventualmente será um valor de $g(i)$ para algum $i$. Também é injetiva, já que se houvesse $j < i$ tal que $g(j) = g(i)$, então $g(i)$ já estaria entre $g(1), \ldots, g(i-1)$, contrariamente à forma como definimos $g$. □

**Corolário 4.11.** *Um conjunto $A$ é enumerável sse é vazio ou há uma bijeção $f\colon N \to A$ onde $N = \mathbb{N}$ ou $N = \{0,\ldots,n\}$ para algum $n \in \mathbb{N}$.*

*Prova.* $A$ é enumerável sse $A$ é vazio ou há uma sobrejetiva $f\colon \mathbb{Z}^+ \to A$. Pela Proposição 4.10, o último vale sse há uma função bijetiva $f\colon Z \to A$ onde $Z = \mathbb{Z}^+$ ou $Z = \{1,\ldots,n\}$ para algum $n \in \mathbb{Z}^+$. Pelo mesmo argumento da prova da Proposição 4.8, isso por sua vez é o caso sse há uma bijeção $g\colon N \to A$ onde $N = \mathbb{N}$ ou $N = \{0,\ldots,n-1\}$. □

## 4.3 Método do Zigue-Zague de Cantor

Já consideramos algumas enumerações "fáceis". Vejamos algo um pouco mais difícil. Considere-se o conjunto dos pares de números naturais, que definimos na Seção 1.5 assim:

$$\mathbb{N} \times \mathbb{N} = \{\langle n, m\rangle : n, m \in \mathbb{N}\}$$

Podemos organizar estes pares ordenados numa *matriz*, assim:

| | **0** | **1** | **2** | **3** | ... |
|---|---|---|---|---|---|
| **0** | $\langle 0,0\rangle$ | $\langle 0,1\rangle$ | $\langle 0,2\rangle$ | $\langle 0,3\rangle$ | ... |
| **1** | $\langle 1,0\rangle$ | $\langle 1,1\rangle$ | $\langle 1,2\rangle$ | $\langle 1,3\rangle$ | ... |
| **2** | $\langle 2,0\rangle$ | $\langle 2,1\rangle$ | $\langle 2,2\rangle$ | $\langle 2,3\rangle$ | ... |
| **3** | $\langle 3,0\rangle$ | $\langle 3,1\rangle$ | $\langle 3,2\rangle$ | $\langle 3,3\rangle$ | ... |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |

Claramente, cada par ordenado em $\mathbb{N} \times \mathbb{N}$ aparece exatamente uma vez na matriz. Em particular, $\langle n, m\rangle$ aparece na $n$-ésima linha e na $m$-ésima coluna. Mas como organizar os elementos de tal matriz numa lista "unidimensional"?

O padrão na matriz abaixo demonstra uma forma de o fazer (embora haja, claro, muitas outras):

| | **0** | **1** | **2** | **3** | **4** | ... |
|---|---|---|---|---|---|---|
| **0** | 0 | 1 | 3 | 6 | 10 | ... |
| **1** | 2 | 4 | 7 | 11 | ... | ... |
| **2** | 5 | 8 | 12 | ... | ... | ... |
| **3** | 9 | 13 | ... | ... | ... | ... |
| **4** | 14 | ... | ... | ... | ... | ... |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ... | ⋱ |

Este padrão chama-se *método do zigue-zague de Cantor*. Enumera $\mathbb{N} \times \mathbb{N}$ do seguinte modo:

$$\langle 0,0\rangle, \langle 0,1\rangle, \langle 1,0\rangle, \langle 0,2\rangle, \langle 1,1\rangle, \langle 2,0\rangle, \langle 0,3\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 3,0\rangle, \ldots$$

Isto estabelece o seguinte:

**Proposição 4.12.** $\mathbb{N} \times \mathbb{N}$ *é enumerável.*

*Prova.* Seja $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ a função que a cada $k \in \mathbb{N}$ associa o tuplo $\langle n, m\rangle \in \mathbb{N} \times \mathbb{N}$ tal que $k$ é o valor na $n$-ésima linha e $m$-ésima coluna da matriz do zigue-zague de Cantor. □

Esta técnica generaliza-se bem. Por exemplo, podemos usá-la para enumerar o conjunto dos triplos ordenados de números naturais, isto é:

$$\mathbb{N} \times \mathbb{N} \times \mathbb{N} = \{\langle n, m, k\rangle : n, m, k \in \mathbb{N}\}$$

Pensamos em $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ como o produto cartesiano de $\mathbb{N} \times \mathbb{N}$ com $\mathbb{N}$, isto é,

$$\mathbb{N}^3 = (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} = \{\langle\langle n, m\rangle, k\rangle : n, m, k \in \mathbb{N}\}$$

e assim podemos enumerar $\mathbb{N}^3$ com uma matriz rotulando um eixo com a enumeração de $\mathbb{N}$ e o outro com a enumeração de $\mathbb{N}^2$:

| | **0** | **1** | **2** | **3** | ... |
|---|---|---|---|---|---|
| $\langle \mathbf{0}, \mathbf{0}\rangle$ | $\langle 0,0,0\rangle$ | $\langle 0,0,1\rangle$ | $\langle 0,0,2\rangle$ | $\langle 0,0,3\rangle$ | ... |
| $\langle \mathbf{0}, \mathbf{1}\rangle$ | $\langle 0,1,0\rangle$ | $\langle 0,1,1\rangle$ | $\langle 0,1,2\rangle$ | $\langle 0,1,3\rangle$ | ... |
| $\langle \mathbf{1}, \mathbf{0}\rangle$ | $\langle 1,0,0\rangle$ | $\langle 1,0,1\rangle$ | $\langle 1,0,2\rangle$ | $\langle 1,0,3\rangle$ | ... |
| $\langle \mathbf{0}, \mathbf{2}\rangle$ | $\langle 0,2,0\rangle$ | $\langle 0,2,1\rangle$ | $\langle 0,2,2\rangle$ | $\langle 0,2,3\rangle$ | ... |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |

Assim, com um método como o zigue-zague de Cantor, obtemos analogamente uma enumeração de $\mathbb{N}^3$. E podemos continuar, obtendo enumerações de $\mathbb{N}^n$ para qualquer número natural $n$. Logo:

**Proposição 4.13.** $\mathbb{N}^n$ *é enumerável, para todo* $n \in \mathbb{N}$.

## 4.4 Funções de Pareamento e Códigos

O método do zigue-zague de Cantor torna visualmente evidente a enumerabilidade de $\mathbb{N}^n$. Mas vamos concentrar-nos na nossa matriz que representa $\mathbb{N}^2$. Seguindo a linha em zigue-zague na matriz e contando as posições, podemos verificar que $\langle 1,2\rangle$ fica associado ao número 7. Seria útil, contudo, poder calcular isto de modo mais direto. Ou seja, seria útil dispor da *inversa* da enumeração em zigue-zague, $g\colon \mathbb{N}^2 \to \mathbb{N}$, tal que

$$g(\langle 0,0\rangle) = 0,\ g(\langle 0,1\rangle) = 1,\ g(\langle 1,0\rangle) = 2,\ \ldots, g(\langle 1,2\rangle) = 7,\ \ldots$$

Isto permitir-nos-ia calcular exatamente em que posição da enumeração cai $\langle n,m\rangle$.

De fato, podemos definir $g$ diretamente com base em duas observações. Primeiro: se a $n$-ésima linha e a $m$-ésima coluna contêm o valor $v$, então a $(n+1)$-ésima linha e a $(m-1)$-ésima coluna contêm o valor $v+1$. Segundo: a primeira linha da nossa enumeração consiste nos números triangulares, começando por 0, 1, 3, 6, etc. O $k$-ésimo número triangular é a soma dos números naturais $< k$, que se pode calcular como $k(k+1)/2$. Juntando estas duas observações, consideremos a função:

$$g(n,m) = \frac{(n+m+1)(n+m)}{2} + n$$

Escreve-se frequentemente $g(n,m)$ em vez de $g(\langle n,m\rangle)$, já que é mais fácil para os olhos. Isto diz-nos que se determine primeiro o $(n+m)$-ésimo número triangular e depois que lhe somemos $n$. A função preenche a matriz exatamente da maneira que desejamos. Em particular, o par $\langle 1,2\rangle$ é enviado para $\frac{4\times 3}{2} + 1 = 7$.

Esta função $g$ é a *inversa* de uma enumeração de um conjunto de pares. Tais funções chamam-se *funções de emparelhamento*.

**Definição 4.14 (Função de emparelhamento).** Uma função $f\colon A \times B \to \mathbb{N}$ é uma *função de emparelhamento* aritmética se $f$ for injetiva. Dizemos também que $f$ *codifica* $A \times B$, e que $f(x,y)$ é o *código* de $\langle x,y\rangle$.

Podemos usar funções de emparelhamento para codificar, por exemplo, pares de números naturais; ou, em outras palavras, podemos representar cada *par* de elementos por um *único* número. Usando a inversa da função de emparelhamento, podemos *descodificar* o número, isto é, determinar que par representa.

## 4.5 Uma Função de Emparelhamento Alternativa

Há outras enumerações de $\mathbb{N}^2$ que facilitam descobrir quais são suas inversas. Eis uma. Em vez de visualizar a enumeração em uma matriz, comece com a

lista de inteiros positivos associados a espaços (inicialmente) vazios. Imagine preencher esses espaços sucessivamente com pares $\langle n, m\rangle$ da seguinte forma. Começando com os pares que têm 0 na primeira posição (isto é, pares $\langle 0, m\rangle$), coloque o primeiro (isto é, $\langle 0, 0\rangle$) no primeiro espaço vazio, depois pule um espaço vazio, coloque o segundo (isto é, $\langle 0, 2\rangle$) no próximo espaço vazio, pule outro, e assim por diante. O começo (incompleto) de nossa enumeração agora se parece com isto

| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | ... |
|---|---|---|---|---|---|---|---|---|---|---|
| $\langle 0,0\rangle$ | | $\langle 0,1\rangle$ | | $\langle 0,2\rangle$ | | $\langle 0,3\rangle$ | | $\langle 0,4\rangle$ | | ... |

Repita isso com pares $\langle 1, m\rangle$ nos lugares que ainda permanecem vazios, novamente pulando cada outro espaço vazio:

| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | ... |
|---|---|---|---|---|---|---|---|---|---|---|
| $\langle 0,0\rangle$ | $\langle 1,0\rangle$ | $\langle 0,1\rangle$ | | $\langle 0,2\rangle$ | $\langle 1,1\rangle$ | $\langle 0,3\rangle$ | | $\langle 0,4\rangle$ | $\langle 1,2\rangle$ | ... |

Insira pares $\langle 2, m\rangle$, $\langle 2, m\rangle$, etc., da mesma forma. Nossa enumeração completa assim começa assim:

| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | ... |
|---|---|---|---|---|---|---|---|---|---|---|
| $\langle 0,0\rangle$ | $\langle 1,0\rangle$ | $\langle 0,1\rangle$ | $\langle 2,0\rangle$ | $\langle 0,2\rangle$ | $\langle 1,1\rangle$ | $\langle 0,3\rangle$ | $\langle 3,0\rangle$ | $\langle 0,4\rangle$ | $\langle 1,2\rangle$ | ... |

Se numerarmos as células na matriz acima de acordo com essa enumeração, não encontraremos uma linha zigue-zague arrumada, mas este arranjo:

| | **0** | **1** | **2** | **3** | **4** | **5** | ... |
|---|---|---|---|---|---|---|---|
| **0** | 1 | 3 | 5 | 7 | 9 | 11 | ... |
| **1** | 2 | 6 | 10 | 14 | 18 | ... | ... |
| **2** | 4 | 12 | 20 | 28 | ... | ... | ... |
| **3** | 8 | 24 | 40 | ... | ... | ... | ... |
| **4** | 16 | 48 | ... | ... | ... | ... | ... |
| **5** | 32 | ... | ... | ... | ... | ... | ... |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |

Podemos ver que os pares na linha 0 estão nas posições ímpares de nossa enumeração, isto é, o par $\langle 0, m\rangle$ está na posição $2m + 1$; os pares na segunda linha, $\langle 1, m\rangle$, estão em posições cujo número é o dobro de um número ímpar, especificamente, $2 \cdot (2m + 1)$; os pares na terceira linha, $\langle 2, m\rangle$, estão em posições cujo número é quatro vezes um número ímpar, $4 \cdot (2m + 1)$; e assim por diante. Os fatores de $(2m + 1)$ para cada linha, 1, 2, 4, 8, ..., são exatamente as potências de 2: $1 = 2^0$, $2 = 2^1$, $4 = 2^2$, $8 = 2^3$, ... De fato, o expoente relevante é sempre o primeiro membro do par em questão. Assim, para o par $\langle n, m\rangle$ o fator é $2^n$. Isso nos dá a fórmula geral: $2^n \cdot (2m + 1)$. Contudo, isso

é um mapeamento de pares para inteiros *positivos*, isto é, $\langle 0,0\rangle$ tem posição 1. Se quisermos começar na posição 0 devemos subtrair 1 do resultado. Isso nos dá:

**Exemplo 4.15.** A função $h\colon \mathbb{N}^2 \to \mathbb{N}$ dada por

$$h(n,m) = 2^n(2m+1) - 1$$

é uma função de emparelhamento para o conjunto de pares de números naturais $\mathbb{N}^2$.

De acordo com nossa segunda enumeração de $\mathbb{N}^2$, o par $\langle 0,0\rangle$ tem código $h(0,0) = 2^0(2\cdot 0+1)-1 = 0$; $\langle 1,2\rangle$ tem código $2^1\cdot(2\cdot 2+1)-1 = 2\cdot 5-1 = 9$; $\langle 2,6\rangle$ tem código $2^2\cdot(2\cdot 6+1)-1 = 51$.

Às vezes basta codificar pares de números naturais $\mathbb{N}^2$ sem exigir que a codificação seja sobrejetora. Tais codificações têm inversas que são apenas funções parciais.

**Exemplo 4.16.** A função $j\colon \mathbb{N}^2 \to \mathbb{N}^+$ dada por

$$j(n,m) = 2^n 3^m$$

é uma função injetiva $\mathbb{N}^2 \to \mathbb{N}$.

## 4.6 Conjuntos Não enumeráveis

Esta seção prova a não enumerabilidade de $\mathbb{B}^\omega$ e $\wp(\mathbb{Z}^+)$ usando a definição na Seção 4.2. Foi concebida para ser um pouco mais elementar e um pouco mais detalhada que a versão na Seção 4.11

Alguns conjuntos, como o conjunto $\mathbb{Z}^+$ dos inteiros positivos, são infinitos. Até agora vimos exemplos de conjuntos infinitos que eram todos enumerável. Contudo, há também conjuntos infinitos que não têm essa propriedade. Tais conjuntos são chamados de *não enumerável*.

Em primeiro lugar, talvez já seja surpreendente que existam conjuntos não enumerável. Para qualquer conjunto enumerável $A$ há uma função sobrejetiva $f\colon \mathbb{Z}^+ \to A$. Se um conjunto é não enumerável, não há tal função. Isto é, nenhuma função mapeando os infinitos membros de $\mathbb{Z}^+$ para $A$ pode esgotar todo $A$. Assim, há "mais" membros em $A$ do que os infinitos inteiros positivos.

Como se provaria que um conjunto é não enumerável? É preciso mostrar que nenhuma tal função sobrejetora pode existir. Equivalentemente, é preciso mostrar que os elementos de $A$ não podem ser enumerados em uma lista infinita unidirecional. A melhor maneira de fazer isso é mostrar que toda lista

de membros de $A$ deve deixar de fora pelo menos um elemento; ou que nenhuma função $f\colon \mathbb{Z}^+ \to A$ pode ser sobrejetiva. Podemos fazer isso usando o *método diagonal* de Cantor. Dada uma lista de membros de $A$, digamos, $x_1$, $x_2$, ..., construímos outro elemento de $A$ que, por sua construção, não pode estar naquela lista.

Nosso primeiro exemplo é o conjunto $\mathbb{B}^\omega$ de todas as sequências infinitas, sem lacunas, de 0s e 1s.

**Teorema 4.17.** *$\mathbb{B}^\omega$ é não enumerável.*

*Prova.* Suponha, por absurdo, que $\mathbb{B}^\omega$ é enumerável, isto é, suponha que há uma lista $s_1$, $s_2$, $s_3$, $s_4$, ... de todos os membros de $\mathbb{B}^\omega$. Cada um desses $s_i$ é em si uma sequência infinita de 0s e 1s. Chamemos o $j$-ésimo elemento da $i$-ésima sequência nessa lista de $s_i(j)$. Então a $i$-ésima sequência $s_i$ é

$$s_i(1), s_i(2), s_i(3), \ldots$$

Podemos organizar essa lista, e os elementos de cada sequência $s_i$ nela, em uma matriz:

| | 1 | 2 | 3 | 4 | ... |
|---|---|---|---|---|---|
| 1 | $\mathbf{s_1(1)}$ | $s_1(2)$ | $s_1(3)$ | $s_1(4)$ | ... |
| 2 | $s_2(1)$ | $\mathbf{s_2(2)}$ | $s_2(3)$ | $s_2(4)$ | ... |
| 3 | $s_3(1)$ | $s_3(2)$ | $\mathbf{s_3(3)}$ | $s_3(4)$ | ... |
| 4 | $s_4(1)$ | $s_4(2)$ | $s_4(3)$ | $\mathbf{s_4(4)}$ | ... |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |

Os rótulos ao lado indicam o número da sequência na lista $s_1$, $s_2$, ...; os números no topo rotulam os membros das sequências individuais. Por exemplo, $s_1(1)$ é um nome para qualquer número, um 0 ou um 1, que é o primeiro membro na sequência $s_1$, e assim por diante.

Agora construímos uma sequência infinita, $\bar{s}$, de 0s e 1s que não pode estar nessa lista. A definição de $\bar{s}$ dependerá da lista $s_1$, $s_2$, .... Qualquer lista infinita de sequências infinitas de 0s e 1s dá origem a uma sequência infinita $\bar{s}$ que está garantidamente fora da lista.

Para definir $\bar{s}$, especificamos todos os seus membros, isto é, especificamos $\bar{s}(n)$ para todo $n \in \mathbb{Z}^+$. Fazemos isso lendo a diagonal da matriz acima (daí o nome "método diagonal") e depois trocando cada 1 por 0 e cada 0 por 1. De maneira mais abstrata, definimos $\bar{s}(n)$ como 0 ou 1 conforme o $n$-ésimo membro da diagonal, $s_n(n)$, é 1 ou 0.

$$\bar{s}(n) = \begin{cases} 1 & \text{se } s_n(n) = 0 \\ 0 & \text{se } s_n(n) = 1. \end{cases}$$

Se você prefere fórmulas a definições por casos, também pode definir $\bar{s}(n) = 1 - s_n(n)$.

Claramente $\overline{s}$ é uma sequência infinita de 0s e 1s, já que é apenas a sequência espelhada da sequência de 0s e 1s que aparecem na diagonal de nossa matriz. Assim $\overline{s}$ é um membro de $\mathbb{B}^\omega$. Mas não pode estar na lista $s_1, s_2, \ldots$ Por quê?

Não pode ser a primeira sequência na lista, $s_1$, porque difere de $s_1$ no primeiro membro. Seja qual for $s_1(1)$, definimos $\overline{s}(1)$ como o oposto. Não pode ser a segunda sequência na lista, porque $\overline{s}$ difere de $s_2$ no segundo elemento: se $s_2(2)$ é 0, $\overline{s}(2)$ é 1, e vice-versa. E assim por diante.

Mais precisamente: se $\overline{s}$ estivesse na lista, haveria algum $k$ tal que $\overline{s} = s_k$. Duas sequências são idênticas sse concordam em toda posição, isto é, para qualquer $n$, $\overline{s}(n) = s_k(n)$. Em particular, tomando $n = k$ como caso especial, $\overline{s}(k) = s_k(k)$ teria de valer. $s_k(k)$ é 0 ou 1. Se é 0, então $\overline{s}(k)$ deve ser 1—é assim que definimos $\overline{s}$. Mas se $s_k(k) = 1$, de novo por causa da forma como definimos $\overline{s}$, $\overline{s}(k) = 0$. Em ambos os casos $\overline{s}(k) \neq s_k(k)$.

Começamos supondo que há uma lista de membros de $\mathbb{B}^\omega$, $s_1, s_2, \ldots$ A partir dessa lista construímos uma sequência $\overline{s}$ que provamos não poder estar na lista. Mas ela definitivamente é uma sequência de 0s e 1s se todos os $s_i$ são sequências de 0s e 1s, isto é, $\overline{s} \in \mathbb{B}^\omega$. Isso mostra em particular que não pode haver lista de *todos* os membros de $\mathbb{B}^\omega$, já que para qualquer tal lista também poderíamos construir uma sequência $\overline{s}$ garantidamente fora da lista, de modo que a suposição de que há uma lista de todas as sequências em $\mathbb{B}^\omega$ leva a uma contradição. □

Esse método de prova é chamado de "diagonalização" porque usa a diagonal da matriz para definir $\overline{s}$. A diagonalização não precisa envolver a presença de uma matriz: podemos mostrar que conjuntos não são enumerável usando uma ideia semelhante mesmo quando não há matriz nem diagonal propriamente dita.

**Teorema 4.18.** *$\wp(\mathbb{Z}^+)$ não é enumerável.*

*Prova.* Procedemos da mesma forma, mostrando que para toda lista de subconjuntos de $\mathbb{Z}^+$ há um subconjunto de $\mathbb{Z}^+$ que não pode estar na lista. Suponha que a seguinte é uma lista dada de subconjuntos de $\mathbb{Z}^+$:

$$Z_1, Z_2, Z_3, \ldots$$

Agora definimos um conjunto $\overline{Z}$ tal que para qualquer $n \in \mathbb{Z}^+$, $n \in \overline{Z}$ sse $n \notin Z_n$:

$$\overline{Z} = \{n \in \mathbb{Z}^+ : n \notin Z_n\}$$ □

$\overline{Z}$ é claramente um conjunto de inteiros positivos, já que por suposição cada $Z_n$ o é, e assim $\overline{Z} \in \wp(\mathbb{Z}^+)$. Mas $\overline{Z}$ não pode estar na lista. Para mostrar isso, estabeleceremos que para cada $k \in \mathbb{Z}^+$, $\overline{Z} \neq Z_k$.

Seja $k \in \mathbb{Z}^+$ arbitrário. Definimos $\overline{Z}$ de modo que para qualquer $n \in \mathbb{Z}^+$, $n \in \overline{Z}$ sse $n \notin Z_n$. Em particular, tomando $n = k$, $k \in \overline{Z}$ sse $k \notin Z_k$. Mas isso

mostra que $\overline{Z} \neq Z_k$, já que $k$ é um membro de um mas não do outro, e assim $\overline{Z}$ e $Z_k$ têm membros diferentes. Como $k$ foi arbitrário, $\overline{Z}$ não está na lista $Z_1$, $Z_2, \ldots$

A prova precedente não mencionou uma diagonal, mas você pode pensar nela como envolvendo uma diagonal se a imaginar assim: imagine os conjuntos $Z_1$, $Z_2$, ..., escritos em uma matriz, onde cada membro $j \in Z_i$ é listado na $j$-ésima coluna. Digamos que os primeiros quatro conjuntos nessa lista são $\{1, 2, 3, \ldots\}$, $\{2, 4, 6, \ldots\}$, $\{1, 2, 5\}$ e $\{3, 4, 5, \ldots\}$. Então a matriz começaria com

$$\begin{array}{lccccccc}
Z_1 = \{ & \mathbf{1}, & 2, & 3, & 4, & 5, & 6, & \ldots\} \\
Z_2 = \{ & & \mathbf{2}, & & 4, & & 6, & \ldots\} \\
Z_3 = \{ & 1, & 2, & & & 5 & & \} \\
Z_4 = \{ & & & 3, & \mathbf{4}, & 5, & 6, & \ldots\} \\
\vdots & & & & & \ddots & &
\end{array}$$

Então $\overline{Z}$ é o conjunto obtido percorrendo a diagonal, deixando de fora quaisquer números que aparecem ao longo da diagonal e incluindo aqueles $j$ onde a matriz tem uma lacuna na $j$-ésima linha/coluna. No caso acima, deixaríamos de fora 1 e 2, incluiríamos 3, deixaríamos de fora 4, etc.

## 4.7 Redução

> Esta seção prova a não enumerabilidade por redução, correspondendo aos resultados na Seção 4.6. Uma versão alternativa, ligeiramente mais condensada, correspondente aos resultados na Seção 4.12, é fornecida na Seção 4.13.

Mostramos $\wp(\mathbb{Z}^+)$ como não enumerável por um argumento de diagonalização. Já tínhamos uma prova de que $\mathbb{B}^\omega$, o conjunto de todas as sequências infinitas de 0s e 1s, é não enumerável. Eis outra maneira de provar que $\wp(\mathbb{Z}^+)$ é não enumerável: mostre que *se* $\wp(\mathbb{Z}^+)$ *é enumerável, então* $\mathbb{B}^\omega$ *também é enumerável*. Como sabemos que $\mathbb{B}^\omega$ não é enumerável, $\wp(\mathbb{Z}^+)$ também não pode ser. Isso é chamado de *reduzir* um problema a outro—neste caso, reduzimos o problema de enumerar $\mathbb{B}^\omega$ ao problema de enumerar $\wp(\mathbb{Z}^+)$. Uma solução para o último—uma enumeração de $\wp(\mathbb{Z}^+)$—daria uma solução para o primeiro—uma enumeração de $\mathbb{B}^\omega$.

Como reduzimos o problema de enumerar um conjunto $B$ ao de enumerar um conjunto $A$? Fornecemos uma maneira de transformar uma enumeração de $A$ em uma enumeração de $B$. A maneira mais fácil de fazer isso é definir uma função sobrejetiva $f\colon A \to B$. Se $x_1, x_2, \ldots$ enumera $A$, então $f(x_1)$,

$f(x_2), \ldots$ enumeraria $B$. Em nosso caso, procuramos uma função sobrejetora $f\colon \wp(\mathbb{Z}^+) \to \mathbb{B}^\omega$.

*Prova do Teorema 4.18 por redução.* Suponha que $\wp(\mathbb{Z}^+)$ fosse enumerável, e portanto que há uma enumeração dele, $Z_1, Z_2, Z_3, \ldots$

Defina a função $f\colon \wp(\mathbb{Z}^+) \to \mathbb{B}^\omega$ fazendo $f(Z)$ ser a sequência $s_k$ tal que $s_k(n) = 1$ sse $n \in Z$, e $s_k(n) = 0$ caso contrário. Isso define claramente uma função, já que sempre que $Z \subseteq \mathbb{Z}^+$, qualquer $n \in \mathbb{Z}^+$ ou é um membro de $Z$ ou não é. Por exemplo, o conjunto $2\mathbb{Z}^+ = \{2, 4, 6, \ldots\}$ dos pares positivos é mapeado para a sequência $010101\ldots$, o conjunto vazio é mapeado para $0000\ldots$ e o conjunto $\mathbb{Z}^+$ para $1111\ldots$.

Também é sobrejetiva: toda sequência de 0s e 1s corresponde a algum conjunto de inteiros positivos, nomeadamente aquele que tem como membros os inteiros correspondentes às posições onde a sequência tem 1s. Mais precisamente, suponha $s \in \mathbb{B}^\omega$. Defina $Z \subseteq \mathbb{Z}^+$ por:

$$Z = \{n \in \mathbb{Z}^+ : s(n) = 1\}$$

Então $f(Z) = s$, como pode ser verificado consultando a definição de $f$.

Agora considere a lista

$$f(Z_1), f(Z_2), f(Z_3), \ldots$$

Como $f$ é sobrejetiva, todo membro de $\mathbb{B}^\omega$ deve aparecer como valor de $f$ para algum argumento, e assim deve aparecer na lista. Essa lista portanto deve enumerar todo $\mathbb{B}^\omega$.

Assim, se $\wp(\mathbb{Z}^+)$ fosse enumerável, $\mathbb{B}^\omega$ seria enumerável. Mas $\mathbb{B}^\omega$ é não enumerável (Teorema 4.17). Logo $\wp(\mathbb{Z}^+)$ é não enumerável. □

É fácil confundir a direção em que a redução vai. Por exemplo, uma função sobrejetiva $g\colon \mathbb{B}^\omega \to B$ *não* estabelece que $B$ é não enumerável. (Considere $g\colon \mathbb{B}^\omega \to \mathbb{B}$ definida por $g(s) = s(1)$, a função que mapeia uma sequência de 0s e 1s para seu primeiro membro. Ela é sobrejetiva, porque algumas sequências começam com 0 e outras começam com 1. Mas $\mathbb{B}$ é finito.) Note também que a função $f$ deve ser sobrejetiva, caso contrário o argumento não se sustenta: $f(x_1), f(x_2), \ldots$ não estariam garantidos de incluir todos os membros de $B$. Por exemplo,

$$h(n) = \underbrace{000\ldots0}_{n\ 0\text{s}}$$

define uma função $h\colon \mathbb{Z}^+ \to \mathbb{B}^\omega$, mas $\mathbb{Z}^+$ é enumerável.

## 4.8 Equinumerosidade

Temos uma noção intuitiva do "tamanho" dos conjuntos, que funciona bem para conjuntos finitos. E quanto aos infinitos? Se quisermos uma forma formal

de comparar os tamanhos de dois conjuntos de *qualquer* cardinalidade, é boa ideia começar por definir quando dois conjuntos têm o mesmo tamanho. Eis Frege:

> Se um garçom quer ter certeza de que pôs exatamente tantas facas quantos pratos sobre a mesa, não precisa contar nem uns nem outros, se simplesmente puser uma faca à direita de cada prato, de modo que cada faca na mesa fique à direita de algum prato. Os pratos e as facas ficam assim correlacionados de modo único, e de fato por essa mesma relação espacial. (Frege, 1884, § 70)

A intuição central desta passagem traduz-se numa definição formal:

**Definição 4.19.** $A$ é *equinumeroso* a $B$, escrevendo-se $A \approx B$, sse existir uma bijeção $f\colon A \to B$.

**Proposição 4.20.** *A relação de equinumerosidade é uma relação de equivalência.*

*Prova.* É preciso mostrar que a equinumerosidade é reflexiva, simétrica e transitiva. Sejam $A, B$ e $C$ conjuntos.

*Reflexividade.* A aplicação identidade $\mathrm{Id}_A\colon A \to A$, com $\mathrm{Id}_A(x) = x$ para todo $x \in A$, é uma bijeção. Logo $A \approx A$.

*Simetria.* Suponhamos $A \approx B$, isto é, que existe uma bijeção $f\colon A \to B$. Como $f$ é bijetiva, a inversa $f^{-1}$ existe e também é bijetiva. Logo $f^{-1}\colon B \to A$ é uma bijeção, pelo que $B \approx A$.

*Transitividade.* Suponhamos $A \approx B$ e $B \approx C$, isto é, que existem bijeções $f\colon A \to B$ e $g\colon B \to C$. Então a composição $g \circ f\colon A \to C$ é bijetiva, logo $A \approx C$. □

**Proposição 4.21.** *Se $A \approx B$, então $A$ é enumerável se e só se $B$ o é.*

> A prova seguinte usa Definição 4.4 se Seção 4.2 estiver incluída e Definição 4.27 caso contrário.

*Prova.* Suponhamos $A \approx B$, logo existe alguma bijeção $f\colon A \to B$, e suponhamos que $A$ é enumerável. Então ou $A = \emptyset$ ou existe uma função sobrejetiva $g\colon \mathbb{Z}^+ \to A$. Se $A = \emptyset$, então $B = \emptyset$ também (caso contrário existiria um membro $y \in B$ sem $x \in A$ com $g(x) = y$). Se, por outro lado, $g\colon \mathbb{Z}^+ \to A$ for sobrejetiva, então $f \circ g\colon \mathbb{Z}^+ \to B$ é sobrejetiva. De fato, seja $y \in B$. Como $f$ é sobrejetiva, existe $x \in A$ tal que $f(x) = y$. Como $g$ é sobrejetiva, existe $n \in \mathbb{Z}^+$ tal que $g(n) = x$. Logo,

$$(f \circ g)(n) = f(g(n)) = f(x) = y$$

e portanto $f \circ g$ é sobrejetiva. Temos que $f \circ g$ é uma enumeração de $B$, logo $B$ é enumerável.

Se $B$ é enumerável, obtemos que $A$ é enumerável repetindo o argumento com a bijeção $f^{-1}\colon B \to A$ em lugar de $f$. □

## 4.9 Conjuntos de Tamanhos Diferentes e o Teorema de Cantor

Apresentamos uma formulação precisa da ideia de que dois conjuntos têm o mesmo tamanho. Também podemos precisar a ideia de que um conjunto é menor que outro. A nossa definição de "é menor do que (ou equinumeroso)" exigirá, em vez de uma bijeção entre os conjuntos, uma injeção do primeiro para o segundo. Se tal função existir, o tamanho do primeiro conjunto é menor ou igual ao do segundo. Intuitivamente, uma injeção de um conjunto em outro garante que a imagem da função tem pelo menos tantos membros quanto o domínio, pois não há dois membros do domínio que vão parar ao mesmo membro da imagem.

**Definição 4.22.** *$A$ não é maior do que $B$*, escrevendo-se $A \preceq B$, sse existir uma injeção $f\colon A \to B$.

É claro que isto é uma relação reflexiva e transitiva, mas não simétrica (fica como exercício). Podemos ainda introduzir uma noção que diz que um conjunto é (estritamente) menor que outro.

**Definição 4.23.** *$A$ é menor do que $B$*, escrevendo-se $A \prec B$, sse existir uma injeção $f\colon A \to B$ mas não existir bijeção $g\colon A \to B$, isto é, $A \preceq B$ e $A \not\approx B$.

É claro que esta relação é irreflexiva e transitiva. (Também fica como exercício.) Com esta notação, um conjunto $A$ é enumerável sse $A \preceq \mathbb{N}$, e $A$ é não enumerável sse $\mathbb{N} \prec A$. Isto permite reformular o Teorema 4.32 como a observação de que $\mathbb{N} \prec \wp(\mathbb{N})$. De fato, Cantor (1892) provou que este último ponto é *completamente geral*:

**Teorema 4.24 (Cantor).** *$A \prec \wp(A)$, para qualquer conjunto $A$.*

*Prova.* A aplicação $f(x) = \{x\}$ é uma injeção $f\colon A \to \wp(A)$, pois se $x \neq y$, então também $\{x\} \neq \{y\}$ por extensionalidade, logo $f(x) \neq f(y)$. Temos pois $A \preceq \wp(A)$.

Apresentamos a prova longa se Seção 4.6 estiver presente; caso contrário, uma prova mais curta alinhada com a Seção 4.12.

Mostraremos agora que não pode existir função sobrejetiva $g\colon A \to \wp(A)$, quanto mais bijetiva, e portanto que $A \not\approx \wp(A)$. Suponhamos que $g\colon A \to \wp(A)$. Como $g$ é total, todo $x \in A$ é mapeado para um subconjunto $g(x) \subseteq A$. Podemos mostrar que $g$ não pode ser sobrejetora. Para isso, definimos um subconjunto $\overline{A} \subseteq A$ que, por definição, não pode estar no contradomínio de $g$. Seja

$$\overline{A} = \{x \in A : x \notin g(x)\}.$$

Como $g(x)$ está definido para todo $x \in A$, $\overline{A}$ é claramente um subconjunto bem definido de $A$. Mas não pode estar no contradomínio de $g$. Seja $x \in A$ arbitrário; mostramos que $\overline{A} \neq g(x)$. Se $x \in g(x)$, então não satisfaz $x \notin g(x)$, logo, pela definição de $\overline{A}$, temos $x \notin \overline{A}$. Se $x \in \overline{A}$, tem de satisfazer a propriedade definidora de $\overline{A}$, isto é, $x \in A$ e $x \notin g(x)$. Como $x$ era arbitrário, isto mostra que, para cada $x \in A$, $x \in g(x)$ sse $x \notin \overline{A}$, logo $g(x) \neq \overline{A}$. Em outras palavras, $\overline{A}$ não pode estar no contradomínio de $g$, o que contradiz a suposição de que $g$ é sobrejetora. □

É instrutivo comparar a prova do Teorema 4.24 com a do Teorema 4.18. Ali mostramos que, para qualquer lista $Z_1$, $Z_2$, ..., de subconjuntos de $\mathbb{Z}^+$, se pode construir um conjunto $\overline{Z}$ de números garantidamente fora da lista. Estava garantido que não estava na lista porque, para todo $n \in \mathbb{Z}^+$, $n \in Z_n$ sse $n \notin \overline{Z}$. Assim, há sempre algum número que é um membro de um entre $Z_n$ ou $\overline{Z}$ mas não do outro. Seguimos a mesma ideia aqui, exceto que os índices $n$ são agora membros de $A$ em vez de $\mathbb{Z}^+$. O conjunto $\overline{A}$ está definido de modo a diferir de $g(x)$ para cada $x \in A$, porque $x \in g(x)$ sse $x \notin \overline{A}$. De novo, há sempre um membro de $A$ que é um membro de um entre $g(x)$ e $\overline{A}$ mas não do outro. E tal como $\overline{Z}$ portanto não pode estar na lista $Z_1$, $Z_2$, ..., $\overline{A}$ não pode estar no contradomínio de $g$.

É instrutivo comparar a prova do Teorema 4.24 com a do Teorema 4.32. Ali mostramos que, para qualquer lista $N_0$, $N_1$, $N_2$, ..., de subconjuntos de $\mathbb{N}$, podemos construir um conjunto $D$ de números garantidamente fora da lista. Estava garantido que não estava na lista porque $n \in N_n$ sse $n \notin D$, para todo $n \in \mathbb{N}$. Seguimos a mesma ideia aqui, exceto que os índices $n$ são agora membros de $A$ em vez de $\mathbb{N}$. O conjunto $D$ está definido de modo a diferir de $g(x)$ para cada $x \in A$, porque $x \in g(x)$ sse $x \notin D$.

A prova vale também a pena comparar com a do Paradoxo de Russell, Teorema 1.29. De fato, o Teorema de Cantor foi a inspiração para o paradoxo de Russell.

## 4.10 A Noção de Tamanho e Schröder-Bernstein

Eis um pensamento intuitivo: se $A$ não é maior do que $B$ e $B$ não é maior do que $A$, então $A$ e $B$ são equinumerosos. Sejamos honestos: se isto estivesse

*errado*, dificilmente poderíamos justificar que a noção definida de equinumerosidade tem a ver com comparações de "tamanhos" entre conjuntos. Felizmente, o pensamento intuitivo está certo. Isto justifica-se pelo Teorema de Schröder-Bernstein.

**Teorema 4.25 (Schröder-Bernstein).** *Se $A \preceq B$ e $B \preceq A$, então $A \approx B$.*

Em outras palavras, se existir uma injeção de $A$ para $B$ e uma injeção de $B$ para $A$, então existe uma bijeção de $A$ para $B$.

Este resultado é, contudo, realmente bastante *difícil* de provar. De fato, embora Cantor o tivesse enunciado, outros provaram-no.[1] Por agora, pode (e deve) aceitá-lo como verdadeiro.

Felizmente, Schröder-Bernstein é *correto* e legitima pensarmos nas relações que definimos, isto é, $A \approx B$ e $A \preceq B$, como tendo a ver com "tamanho". Além disso, Schröder-Bernstein é muito *útil*. Pode ser difícil imaginar uma bijeção entre dois conjuntos equinumerosos. O Teorema de Schröder-Bernstein permite decompor a comparação em casos em que só precisamos de uma injeção do primeiro para o segundo e vice-versa.

As seções Seção 4.11, Seção 4.12, Seção 4.13 são versões alternativas da Seção 4.2, Seção 4.6, Seção 4.7 de Tim Button para uso em seu texto Open Set Theory. São um pouco mais avançadas e usam uma definição diferente de enumerabilidade mais adequada em um contexto de teoria dos conjuntos (isto é, bijeção com $\mathbb{N}$ ou um segmento inicial, em vez de ser listável ou ser a imagem de uma função sobrejetora de $\mathbb{Z}^+$).

## 4.11 Enumerações e Conjuntos Enumeráveis

Esta seção define enumerações como bijeções com (segmentos iniciais) de $\mathbb{N}$, como se faz em teoria dos conjuntos. Por isso difere ligeiramente das definições em Seção 4.2 e repete os exemplos dessa seção. É também um pouco mais concisa.

Podemos especificar um conjunto finito simplesmente enumerando os seus membros. Fazemo-lo quando definimos um conjunto assim:

$$A = \{a_1, a_2, \ldots, a_n\}.$$

Supondo que os membros $a_1, \ldots, a_n$ são todos distintos, obtemos uma bijeção entre $A$ e os primeiros $n$ números naturais $0, \ldots, n-1$. Reciprocamente, como

[1] Para mais sobre a história, ver por exemplo Potter (2004, pp. 165–6).

todo o conjunto finito tem apenas finitos membros, todo o conjunto finito pode ser posto nessa correspondência. Em outras palavras, se $A$ é finito, existe uma bijeção entre $A$ e $\{0, \ldots, n-1\}$, onde $n$ é o número de membros de $A$.

Se admitirmos certos tipos de conjuntos infinitos, admitiremos também que alguns conjuntos infinitos possam ser enumerados. Podemos precisar isto dizendo que um conjunto infinito é enumerado por uma bijeção entre ele e todo o $\mathbb{N}$.

**Definição 4.26 (Enumeração, no sentido conjuntista).** Uma *enumeração* de um conjunto $A$ é uma bijeção cujo contradomínio é $A$ e cujo domínio é ou um conjunto inicial de números naturais $\{0, 1, \ldots, n\}$ *ou* todo o conjunto dos números naturais $\mathbb{N}$.

Há uma base intuitiva para este uso da palavra *enumeração*. Dizer que enumeramos um conjunto $A$ é dizer que existe uma bijeção $f$ que nos permite *contar* os elementos do conjunto $A$. O elemento de índice 0 é $f(0)$, o de índice 1 é $f(1)$, ...o de índice $n$ é $f(n)$....[2] O raciocínio fica ainda mais claro com o seguinte:

**Definição 4.27.** Um conjunto $A$ é enumerável se e só se $A = \emptyset$ ou existe uma enumeração de $A$. Dizemos que $A$ é não enumerável se e só se $A$ *não* é enumerável.

Logo um conjunto é enumerável se e só se é vazio ou se podemos usar uma enumeração para contar os seus membros.

**Exemplo 4.28.** Uma função que enumera os números naturais é simplesmente a função identidade $\mathrm{Id}_{\mathbb{N}} \colon \mathbb{N} \to \mathbb{N}$ dada por $\mathrm{Id}_{\mathbb{N}}(n) = n$. Uma função que enumera os números naturais *positivos*, $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$, é a função $g(n) = n + 1$, isto é, a função sucessora.

**Exemplo 4.29.** As funções $f \colon \mathbb{N} \to \mathbb{N}$ e $g \colon \mathbb{N} \to \mathbb{N}$ dadas por

$$f(n) = 2n \text{ e}$$
$$g(n) = 2n + 1$$

enumeram, respectivamente, os números naturais pares e os ímpares. Mas nenhuma é sobrejetiva, logo nenhuma é uma enumeração de $\mathbb{N}$.

**Exemplo 4.30.** Seja $\lceil x \rceil$ a função *teto*, que arredonda $x$ por excesso para o inteiro mais próximo. Então a função $f \colon \mathbb{N} \to \mathbb{Z}$ dada por:

$$f(n) = (-1)^n \left\lceil \tfrac{n}{2} \right\rceil$$

[2] Sim, contamos a partir de 0. Claro que também poderíamos começar em 1. Não faria grande diferença. Bastaria substituir $\mathbb{N}$ por $\mathbb{Z}^+$.

enumera o conjunto dos inteiros $\mathbb{Z}$ do seguinte modo:

$$\begin{array}{cccccccc} f(0) & f(1) & f(2) & f(3) & f(4) & f(5) & f(6) & \dots \\ \lceil \frac{0}{2} \rceil & -\lceil \frac{1}{2} \rceil & \lceil \frac{2}{2} \rceil & -\lceil \frac{3}{2} \rceil & \lceil \frac{4}{2} \rceil & -\lceil \frac{5}{2} \rceil & \lceil \frac{6}{2} \rceil & \dots \\ 0 & -1 & 1 & -2 & 2 & -3 & 3 & \dots \end{array}$$

Repare como $f$ gera os valores de $\mathbb{Z}$ "saltitando" entre inteiros positivos e negativos. Também se pode ver $f$ definida por casos assim:

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ -\frac{n+1}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

## 4.12 Conjuntos Não Enumeráveis

Esta seção prova a não enumerabilidade de $\mathbb{B}^\omega$ e de $\wp(\mathbb{N})$ usando as definições na Seção 4.11, isto é, exigindo uma bijeção com $\mathbb{N}$ em vez de uma sobrejeção a partir de $\mathbb{Z}^+$.

O conjunto $\mathbb{N}$ dos números naturais é infinito. Também é trivialmente enumerável. O fato notável, porém, é que existem conjuntos *não enumeráveis*, isto é, conjuntos que não são enumeráveis (ver Definição 4.27).

Isto pode surpreender. Afinal, dizer que $A$ é não enumerável é dizer que *não* existe bijeção $f : \mathbb{N} \to A$; isto é, nenhuma função que mapeie os infinitos membros de $\mathbb{N}$ para $A$ esgota todo $A$. Logo, se $A$ é não enumerável, há "mais" membros em $A$ do que números naturais.

Para provar que um conjunto é não enumerável, é preciso mostrar que não pode existir uma bijeção adequada. A melhor forma é mostrar que qualquer tentativa de enumerar membros de $A$ tem de deixar pelo menos um membro de fora; isto mostra que nenhuma função $f : \mathbb{N} \to A$ é sobrejetiva. Uma estratégia geral para o estabelecer é usar o *método diagonal* de Cantor. Dada uma lista de membros de $A$, digamos $x_1$, $x_2$, ..., construímos outro membro de $A$ que, pela sua construção, não pode estar nessa lista.

Tudo isto compreende-se melhor com um exemplo. O nosso primeiro exemplo é o conjunto $\mathbb{B}^\omega$ de todas as cadeias infinitas de 0s e 1s. (O símbolo '$\mathbb{B}$' significa binário, e podemos pensar nele como o conjunto de dois elementos $\{0, 1\}$.)

**Teorema 4.31.** *$\mathbb{B}^\omega$ é não enumerável.*

*Prova.* Considere-se qualquer enumeração de um subconjunto de $\mathbb{B}^\omega$. Temos então uma lista $s_0$, $s_1$, $s_2$, ... em que cada $s_n$ é uma cadeia infinita de 0s e 1s.

Seja $s_n(m)$ o $m$-ésimo dígito da cadeia $s_n$. Podemos pois pensar na lista como uma matriz, colocando $s_n(m)$ na $n$-ésima linha e $m$-ésima coluna:

| | 0 | 1 | 2 | 3 | ... |
|---|---|---|---|---|---|
| 0 | $\mathbf{s_0(0)}$ | $s_0(1)$ | $s_0(2)$ | $s_0(3)$ | ... |
| 1 | $s_1(0)$ | $\mathbf{s_1(1)}$ | $s_1(2)$ | $s_1(3)$ | ... |
| 2 | $s_2(0)$ | $s_2(1)$ | $\mathbf{s_2(2)}$ | $s_2(3)$ | ... |
| 3 | $s_3(0)$ | $s_3(1)$ | $s_3(2)$ | $\mathbf{s_3(3)}$ | ... |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |

Construiremos agora uma cadeia infinita, $d$, de 0s e 1s que não está nesta lista, especificando cada uma das suas entradas, isto é, $d(n)$ para todo $n \in \mathbb{N}$. Intuitivamente, lemos a diagonal da matriz acima (daí o nome "método diagonal") e trocamos cada 0 por 1 e cada 1 por 0. De modo mais abstrato, definimos $d(n)$ como 0 ou 1 consoante o $n$-ésimo membro da diagonal, $s_n(n)$, seja 1 ou 0, isto é:

$$d(n) = \begin{cases} 1 & \text{se } s_n(n) = 0 \\ 0 & \text{se } s_n(n) = 1 \end{cases}$$

Claramente $d \in \mathbb{B}^\omega$, pois é uma cadeia infinita de 0s e 1s. Mas construímos $d$ de modo que $d(n) \neq s_n(n)$ para qualquer $n \in \mathbb{N}$, isto é, $d$ difere de $s_n$ na sua $n$-ésima entrada. Logo $d \neq s_n$ para qualquer $n \in \mathbb{N}$, pelo que $d$ não pode estar na lista $s_0, s_1, s_2, \ldots$

Mostramos assim que, dada uma enumeração arbitrária de algum subconjunto de $\mathbb{B}^\omega$, ela omite algum membro de $\mathbb{B}^\omega$. Logo não existe enumeração do conjunto $\mathbb{B}^\omega$, isto é, $\mathbb{B}^\omega$ é não enumerável. □

Este método de prova chama-se "diagonalização" porque usa a diagonal da matriz para definir $d$. Contudo, a diagonalização não exige necessariamente uma matriz. De fato, podemos mostrar que um conjunto é não enumerável por uma ideia semelhante mesmo quando não há matriz nem diagonal literal. O resultado seguinte ilustra como.

**Teorema 4.32.** *$\wp(\mathbb{N})$ não é enumerável.*

*Prova.* Procedemos da mesma forma, mostrando que qualquer lista de subconjuntos de $\mathbb{N}$ omite algum subconjunto de $\mathbb{N}$. Suponhamos, pois, que temos uma lista $N_0, N_1, N_2, \ldots$ de subconjuntos de $\mathbb{N}$. Definimos um conjunto $D$ assim: $n \in D$ sse $n \notin N_n$:

$$D = \{n \in \mathbb{N} : n \notin N_n\}$$

Claramente $D \subseteq \mathbb{N}$. Mas $D$ não pode estar na lista: por construção, $n \in D$ sse $n \notin N_n$, logo $D \neq N_n$ para qualquer $n \in \mathbb{N}$. □

A prova precedente não mencionou uma diagonal. Ainda assim, pode pensar-se nela como envolvendo uma diagonal, imaginando os conjuntos $N_0$, $N_1, \ldots$ dispostos numa matriz em que escrevemos $N_n$ na $n$-ésima linha colocando $m$ na $m$-ésima coluna sse $m \in N_n$. Por exemplo, se os primeiros quatro conjuntos da lista são $\{0, 1, 2, \ldots\}$, $\{1, 3, 5, \ldots\}$, $\{0, 1, 4\}$ e $\{2, 3, 4, \ldots\}$, a matriz começaria com

$$\begin{array}{lccccccc}
N_0 = \{ & \mathbf{0}, & 1, & 2, & & & & \ldots\} \\
N_1 = \{ & & \mathbf{1}, & & 3, & & 5, & \ldots\} \\
N_2 = \{ & 0, & 1, & & & 4 & & \} \\
N_3 = \{ & & & 2, & \mathbf{3}, & 4, & & \ldots\} \\
\vdots & & & & & & & \ddots
\end{array}$$

Então $D$ é o conjunto obtido percorrendo a diagonal, pondo $n \in D$ sse $n$ *não* está na diagonal. No caso acima, excluiríamos 0 e 1, incluiríamos 2, excluiríamos 3, etc.

## 4.13 Redução

Esta seção prova a não enumerabilidade por redução, alinhada com os resultados na Seção 4.12. Uma versão alternativa, ligeiramente mais elaborada, alinhada com os resultados na Seção 4.6, encontra-se na Seção 4.7.

Provamos que $\mathbb{B}^\omega$ é não enumerável por um argumento de diagonalização. Usamos um argumento semelhante para mostrar que $\wp(\mathbb{N})$ é não enumerável. Há outra forma de provar que $\wp(\mathbb{N})$ é não enumerável: mostrar que *se* $\wp(\mathbb{N})$ *é enumerável então* $\mathbb{B}^\omega$ *também é enumerável*. Como sabemos que $\mathbb{B}^\omega$ é não enumerável, segue que $\wp(\mathbb{N})$ também o é.

Isto chama-se *reduzir* um problema a outro. Neste caso, reduzimos o problema de enumerar $\mathbb{B}^\omega$ ao problema de enumerar $\wp(\mathbb{N})$. Uma solução para este último—uma enumeração de $\wp(\mathbb{N})$—daria uma solução para o primeiro—uma enumeração de $\mathbb{B}^\omega$.

Para reduzir o problema de enumerar um conjunto $B$ ao de enumerar um conjunto $A$, indicamos uma forma de transformar uma enumeração de $A$ numa enumeração de $B$. A forma mais simples é definir uma sobrejeção $f\colon A \to B$. Se $x_1, x_2, \ldots$ enumeram $A$, então $f(x_1), f(x_2), \ldots$ enumerariam $B$. No nosso caso, procuramos uma sobrejeção $f\colon \wp(\mathbb{N}) \to \mathbb{B}^\omega$.

*Prova do Teorema 4.32 por redução.* Para a redução, suponhamos que $\wp(\mathbb{N})$ é enumerável e portanto que existe uma enumeração $N_1, N_2, N_3, \ldots$

Definimos a função $f\colon \wp(\mathbb{N}) \to \mathbb{B}^\omega$ pondo $f(N)$ igual à cadeia $s_k$ tal que $s_k(n) = 1$ sse $n \in N$, e $s_k(n) = 0$ caso contrário.

Isto define claramente uma função, pois sempre que $N \subseteq \mathbb{N}$, qualquer $n \in \mathbb{N}$ ou é um membro de $N$ ou não é. Por exemplo, o conjunto $2\mathbb{N} = \{2n : n \in \mathbb{N}\} = \{0, 2, 4, 6, \dots\}$ dos naturais pares é mapeado para a cadeia $1010101\dots$; $\emptyset$ é mapeado para $0000\dots$; $\mathbb{N}$ é mapeado para $1111\dots$.

Também é sobrejetiva: toda a cadeia de 0s e 1s corresponde a algum conjunto de números naturais, nomeadamente aquele que tem como membros os naturais nas posições em que a cadeia tem um 1. Com mais precisão, se $s \in \mathbb{B}^\omega$, defina-se $N \subseteq \mathbb{N}$ por:

$$N = \{n \in \mathbb{N} : s(n) = 1\}$$

Então $f(N) = s$, como se verifica consultando a definição de $f$.

Consideremos agora a lista

$$f(N_1), f(N_2), f(N_3), \dots$$

Como $f$ é sobrejetiva, todo o membro de $\mathbb{B}^\omega$ tem de aparecer como valor de $f$ para algum argumento, e portanto na lista. Esta lista teria de enumerar todo $\mathbb{B}^\omega$.

Logo, se $\wp(\mathbb{N})$ fosse enumerável, $\mathbb{B}^\omega$ seria enumerável. Mas $\mathbb{B}^\omega$ é não enumerável (Teorema 4.31). Logo $\wp(\mathbb{N})$ é não enumerável. □

## Problemas

**Problema 4.1.** Defina uma enumeração dos quadrados positivos 1, 4, 9, 16, ...

**Problema 4.2.** Mostre que se $A$ e $B$ são enumeráveis, então $A \cup B$ também é. Para isso, suponha que há funções sobrejetivas $f\colon \mathbb{Z}^+ \to A$ e $g\colon \mathbb{Z}^+ \to B$, e defina uma função sobrejetiva $h\colon \mathbb{Z}^+ \to A \cup B$ e mostre que ela é sobrejetiva. Considere também os casos em que $A$ ou $B = \emptyset$.

**Problema 4.3.** Mostre que se $B \subseteq A$ e $A$ é enumerável, então $B$ também é. Para isso, suponha que há uma função sobrejetiva $f\colon \mathbb{Z}^+ \to A$. Defina uma função sobrejetiva $g\colon \mathbb{Z}^+ \to B$ e mostre que ela é sobrejetiva. O que acontece se $B = \emptyset$?

**Problema 4.4.** Mostre por indução em $n$ que se $A_1, A_2, \dots, A_n$ são todos enumeráveis, então $A_1 \cup \dots \cup A_n$ também é. Você pode assumir o fato de que se dois conjuntos $A$ e $B$ são enumeráveis, então $A \cup B$ também é.

**Problema 4.5.** De acordo com a Definição 4.4, um conjunto $A$ é enumerável sse $A = \emptyset$ ou há uma sobrejetiva $f\colon \mathbb{Z}^+ \to A$. Também é possível definir "conjunto enumerável" precisamente por: um conjunto é enumerável sse há uma função injetiva $g\colon A \to \mathbb{Z}^+$. Mostre que as definições são equivalentes, isto é, mostre que há uma função injetiva $g\colon A \to \mathbb{Z}^+$ sse $A = \emptyset$ ou há uma sobrejetiva $f\colon \mathbb{Z}^+ \to A$.

**Problema 4.6.** Mostre que $(\mathbb{Z}^+)^n$ é enumerável, para todo $n \in \mathbb{N}$.

**Problema 4.7.** Mostre que $(\mathbb{Z}^+)^*$ é enumerável. Pode assumir PROBLEMA 4.6.

**Problema 4.8.** Dê uma enumeração do conjunto de todos os números racionais não negativos.

**Problema 4.9.** Mostre que $\mathbb{Q}$ é enumerável. Recordemos que qualquer número racional se pode escrever como uma fração $z/m$ com $z \in \mathbb{Z}$, $m \in \mathbb{N}^+$.

**Problema 4.10.** Defina uma enumeração de $\mathbb{B}^*$.

**Problema 4.11.** Recordando o curso introdutório de lógica, cada tabela de verdade possível exprime uma função de verdade. Em outras palavras, as funções de verdade são todas as funções de $\mathbb{B}^k \to \mathbb{B}$ para algum $k$. Prove que o conjunto de todas as funções de verdade é enumerável.

**Problema 4.12.** Mostre que o conjunto de todos os subconjuntos finitos de um conjunto infinito enumerável arbitrário é enumerável.

**Problema 4.13.** Um subconjunto de $\mathbb{N}$ diz-se *confinito* sse for o complemento de um conjunto finito; isto é, $A \subseteq \mathbb{N}$ é confinito sse $\mathbb{N} \setminus A$ for finito. Seja $I$ o conjunto cujos membros são exatamente os subconjuntos finitos e confinitos de $\mathbb{N}$. Mostre que $I$ é enumerável.

**Problema 4.14.** Mostre que a união enumerável de conjuntos enumeráveis é enumerável. Isto é, sempre que $A_1, A_2, \ldots$ são conjuntos e cada $A_i$ é enumerável, então a união $\bigcup_{i=1}^{\infty} A_i$ de todos eles também é enumerável. [Nota: isto é difícil!]

**Problema 4.15.** Seja $f\colon A \times B \to \mathbb{N}$ uma função de emparelhamento arbitrária. Mostre que a inversa de $f$ é uma enumeração de $A \times B$.

**Problema 4.16.** Especifique uma função que codifique $\mathbb{N}^3$.

**Problema 4.17.** Mostre que $\wp(\mathbb{N})$ é não enumerável por um argumento diagonal.

**Problema 4.18.** Mostre que o conjunto de funções $f\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ é não enumerável por um argumento diagonal explícito. Isto é, mostre que se $f_1, f_2, \ldots,$ é uma lista de funções e cada $f_i\colon \mathbb{Z}^+ \to \mathbb{Z}^+$, então há alguma $\overline{f}\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ fora dessa lista.

**Problema 4.19.** Mostre que se há uma função injetiva $g\colon B \to A$, e $B$ é não enumerável, então $A$ também é. Faça isso mostrando como você pode usar $g$ para transformar uma enumeração de $A$ em uma de $B$.

**Problema 4.20.** Mostre que o conjunto de todos os *conjuntos de* pares de inteiros positivos é não enumerável por um argumento de redução.

**Problema 4.21.** Mostre que o conjunto $X$ de todas as funções $f\colon \mathbb{N} \to \mathbb{N}$ é não enumerável por um argumento de redução (Dica: dê uma função sobrejetora de $X$ para $\mathbb{B}^\omega$.)

**Problema 4.22.** Mostre que $\mathbb{N}^\omega$, o conjunto de sequências infinitas de números naturais, é não enumerável por um argumento de redução.

**Problema 4.23.** Seja $P$ o conjunto de funções do conjunto dos inteiros positivos para o conjunto $\{0\}$, e seja $Q$ o conjunto de funções *parciais* do conjunto dos inteiros positivos para o conjunto $\{0\}$. Mostre que $P$ é enumerável e $Q$ não é. (Dica: reduza o problema de enumerar $\mathbb{B}^\omega$ a enumerar $Q$).

**Problema 4.24.** Seja $S$ o conjunto de todas as funções sobrejetivas do conjunto dos inteiros positivos para o conjunto $\{0,1\}$, isto é, $S$ consiste de todas as sobrejetivas $f\colon \mathbb{Z}^+ \to \mathbb{B}$. Mostre que $S$ é não enumerável.

**Problema 4.25.** Mostre que o conjunto $\mathbb{R}$ de todos os números reais é não enumerável.

**Problema 4.26.** Mostre que, se $A \approx C$ e $B \approx D$, e $A \cap B = C \cap D = \emptyset$, então $A \cup B \approx C \cup D$.

**Problema 4.27.** Mostre que, se $A$ é infinito e enumerável, então $A \approx \mathbb{N}$.

**Problema 4.28.** Mostre que não pode existir uma injeção $g\colon \wp(A) \to A$, para qualquer conjunto $A$. Sugestão: suponha $g\colon \wp(A) \to A$ injetiva. Considere $D = \{g(B) : B \subseteq A \text{ e } g(B) \notin B\}$. Seja $x = g(D)$. Use o fato de $g$ ser injetiva para obter uma contradição.

**Problema 4.29.** Mostre que um conjunto $A$ é enumerável se e só se $A = \emptyset$ ou existe uma sobrejeção $f\colon \mathbb{N} \to A$. Mostre que $A$ é enumerável se e só se existe uma injeção $g\colon A \to \mathbb{N}$.

**Problema 4.30.** Defina uma enumeração dos quadrados perfeitos 1, 4, 9, 16, ...

**Problema 4.31.** Mostre que se $A$ e $B$ são enumeráveis, então $A \cup B$ também é.

**Problema 4.32.** Mostre por indução em $n$ que se $A_1$, $A_2$, ..., $A_n$ são todos enumeráveis, então $A_1 \cup \cdots \cup A_n$ também é.

**Problema 4.33.** Mostre que o conjunto de todas as funções $f : \mathbb{N} \to \mathbb{N}$ é não enumerável por um argumento diagonal explícito. Isto é, mostre que, se $f_1$, $f_2$, ... é uma lista de funções e cada $f_i : \mathbb{N} \to \mathbb{N}$, então existe alguma $g : \mathbb{N} \to \mathbb{N}$ que não está nesta lista.

**Problema 4.34.** Mostre que, se existir uma função injetiva $g : B \to A$, e $B$ for não enumerável, então $A$ também o é. Faça-o mostrando como pode usar $g$ para transformar uma enumeração de $A$ numa de $B$.

**Problema 4.35.** Mostre que o conjunto $X$ de todas as funções $f : \mathbb{N} \to \mathbb{N}$ é não enumerável por um argumento de redução (Sugestão: dê uma função sobrejetora de $X$ para $\mathbb{B}^\omega$.)

**Problema 4.36.** Mostre que o conjunto de todos os *conjuntos de* pares de números naturais, isto é, $\wp(\mathbb{N} \times \mathbb{N})$, é não enumerável por um argumento de redução.

**Problema 4.37.** Mostre que $\mathbb{N}^\omega$, o conjunto das sequências infinitas de números naturais, é não enumerável por um argumento de redução.

**Problema 4.38.** Seja $S$ o conjunto de todas as sobrejeções de $\mathbb{N}$ para o conjunto $\{0, 1\}$, isto é, $S$ consiste em todas as sobrejeções $f : \mathbb{N} \to \mathbb{B}$. Mostre que $S$ é não enumerável.

**Problema 4.39.** Mostre que o conjunto $\mathbb{R}$ de todos os números reais é não enumerável.

# Capítulo 5

# Aritmetização

O material deste capítulo apresenta a construção dos sistemas numéricos na teoria ingênua dos conjuntos. É retirado do texto *Open Set Theory* de Tim Button.

## 5.1 De $\mathbb{N}$ para $\mathbb{Z}$

Eis duas constatações básicas (no sentido de "ideias que retemos"):

1. Todo inteiro pode escrever-se na forma $n - m$, com $n, m \in \mathbb{N}$.
2. A informação codificada numa expressão $n - m$ pode igualmente codificar-se por um par ordenado $\langle n, m \rangle$.

Já sabemos que os pares ordenados de números naturais são os membros de $\mathbb{N}^2$; estamos a assumir, também, que compreendemos $\mathbb{N}$. Eis uma sugestão ingênua, fundada nestas duas constatações: *tratar os inteiros como pares ordenados de números naturais*.

De fato, esta sugestão é demasiado ingênua. Obviamente, queremos que seja verdade que $0 - 2 = 4 - 6$. Mas, evidentemente, $\langle 0, 2 \rangle \neq \langle 4, 6 \rangle$. Logo, não podemos simplesmente dizer que $\mathbb{N}^2$ é o conjunto dos inteiros.

Generalizando a partir do problema precedente, o que queremos é o seguinte:

$$a - b = c - d \text{ sse } a + d = c + b$$

(Deve ser óbvio que assim é que os inteiros *devem* comportar-se: basta somar $b$ e $d$ a ambos os lados.) A forma fácil de garantir este comportamento é definir uma relação de equivalência entre pares ordenados, $\sim$, do seguinte modo:

$$\langle a, b \rangle \sim \langle c, d \rangle \text{ sse } a + d = c + b$$

Resta-nos mostrar que isto é uma relação de equivalência.

**Proposição 5.1.** *$\sim$ é uma relação de equivalência.*

*Prova.* Há que mostrar que $\sim$ é reflexiva, simétrica e transitiva.

*Reflexividade:* Evidentemente $\langle a, b\rangle \sim \langle a, b\rangle$, pois $a + b = b + a$.

*Simetria:* Suponhamos $\langle a, b\rangle \sim \langle c, d\rangle$, logo $a + d = c + b$. Então $c + b = a + d$, pelo que $\langle c, d\rangle \sim \langle a, b\rangle$.

*Transitividade:* Suponhamos $\langle a, b\rangle \sim \langle c, d\rangle \sim \langle m, n\rangle$. Logo, $a + d = c + b$ e $c + n = m + d$. Assim, $a + d + c + n = c + b + m + d$, e portanto $a + n = m + b$. Logo, $\langle a, b\rangle \sim \langle m, n\rangle$. □

Podemos agora usar esta relação de equivalência para formar classes de equivalência:

**Definição 5.2.** Os inteiros são as classes de equivalência, sob $\sim$, dos pares ordenados de números naturais; isto é, $\mathbb{Z} = \mathbb{N}^2/_\sim$.

Agora, podem surgir várias reações *filosóficas* distintas face a esta definição estipulativa. Antes de as considerarmos, porém, vale a pena continuar com alguns pormenores técnicos.

Tendo dito o que são os inteiros, precisamos de definir funções e relações básicas sobre eles. Escrevamos $[m, n]_\sim$ para a classe de equivalência sob $\sim$ que tem $\langle m, n\rangle$ como um membro.[1] Isto é:

$$[m, n]_\sim = \{\langle a, b\rangle \in \mathbb{N}^2 : \langle a, b\rangle \sim \langle m, n\rangle\}$$

Apresentamos, pois, algumas definições:

$$\begin{aligned}
[a, b]_\sim + [c, d]_\sim &= [a + c, b + d]_\sim \\
[a, b]_\sim \times [c, d]_\sim &= [ac + bd, ad + bc]_\sim \\
[a, b]_\sim \leq [c, d]_\sim &\text{ sse } a + d \leq b + c
\end{aligned}$$

(Como é habitual, uso '$ab$' no sentido de '$(a \times b)$', só para tornar os axiomas mais legíveis.) Há, ainda, que garantir que estas definições se comportam como *devem*. Explicitar o que isto significa, e verificá-lo, é trabalhoso; relegamos os pormenores a Seção 5.6. Em resumo, contudo: tudo funciona!

Resta um último ponto. Construímos os inteiros a partir dos números naturais. Isto significa que os naturais *não são, eles próprios, inteiros*. Voltaremos ao significado filosófico disto na Seção 5.5. Do ponto de vista puramente técnico, porém, precisamos de alguma forma de tratar números naturais *como* inteiros. A ideia é simples: para cada $n \in \mathbb{N}$, estipulamos $n_\mathbb{Z} = [n, 0]_\sim$. Há

[1] Nota: com a notação introduzida na Definição 2.11, escreveríamos $[\langle m, n\rangle]_\sim$ para o mesmo objeto; isso, porém, torna a leitura um pouco mais difícil.

que confirmar que esta definição é bem comportada, isto é, que para quaisquer $m, n \in \mathbb{N}$

$$\begin{aligned}(m+n)_{\mathbb{Z}} &= m_{\mathbb{Z}} + n_{\mathbb{Z}}\\ (m \times n)_{\mathbb{Z}} &= m_{\mathbb{Z}} \times n_{\mathbb{Z}}\\ m \leq n &\leftrightarrow m_{\mathbb{Z}} \leq n_{\mathbb{Z}}\end{aligned}$$

Mas isto é bastante direto. Por exemplo, para mostrar que a segunda condição se verifica, podemos apoiar-nos no comportamento dos naturais e raciocinar assim:

$$\begin{aligned}(m \times n)_{\mathbb{Z}} &= [m \times n, 0]_{\sim}\\ &= [m \times n + 0 \times 0, m \times 0 + 0 \times n]_{\sim}\\ &= [m, 0]_{\sim} \times [n, 0]_{\sim}\\ &= m_{\mathbb{Z}} \times n_{\mathbb{Z}}\end{aligned}$$

Deixamos como exercício confirmar que as outras duas condições se verificam.

## 5.2 De $\mathbb{Z}$ para $\mathbb{Q}$

Acabamos de ver como construir os inteiros a partir dos naturais, usando alguma teoria ingênua dos conjuntos. Veremos agora como construir os racionais a partir dos inteiros, de modo muito semelhante. As constatações iniciais são:

1. Todo racional pode escrever-se na forma $^{i}/_{j}$, onde $i$ e $j$ são inteiros, mas $j$ é diferente de zero.

2. A informação codificada numa expressão $^{i}/_{j}$ pode igualmente codificar-se num par ordenado $\langle i, j\rangle$.

A abordagem óbvia seria pensar nos racionais *como* pares ordenados de $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\})$. Como antes, porém, isso seria um pouco demasiado ingênuo, pois queremos $^{3}/_{2} = {}^{6}/_{4}$, mas $\langle 3, 2\rangle \neq \langle 6, 4\rangle$. Mais geralmente, quereremos o seguinte:

$$^{a}/_{b} = {}^{c}/_{d} \text{ sse } a \times d = b \times c$$

Para obter isto, definimos uma *relação de equivalência* em $\mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\})$ assim:

$$\langle a, b\rangle \backsim \langle c, d\rangle \text{ sse } a \times d = b \times c$$

Há que verificar que isto é uma relação de equivalência. É muito parecido com o caso de $\sim$, e deixamo-lo como exercício. Mas isto permite-nos dizer o seguinte:

**Definição 5.3.** Os racionais são as classes de equivalência, sob $\backsim$, dos pares de inteiros (cujo segundo elemento é não nulo). Isto é, $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0_\mathbb{Z}\}))/\backsim$.

Tal como para os inteiros, queremos também definir algumas operações básicas. Sendo $[i,j]_\backsim$ a classe de equivalência sob $\backsim$ com $\langle i,j\rangle$ como um membro, definimos:

$$[a,b]_\backsim + [c,d]_\backsim = [ad+bc, bd]_\backsim$$
$$[a,b]_\backsim \times [c,d]_\backsim = [ac, bd]_\backsim.$$

Para definir $r \leq s$ nestes racionais, usamos o fato de que $r \leq s$ sse $s - r$ não é negativo, isto é, $r - s$ pode escrever-se como $^i/_j$ com $i$ não negativo e $j$ positivo:

$$[a,b]_\backsim \leq [c,d]_\backsim \text{ sse } [c,d]_\backsim - [a,b]_\backsim = [i_\mathbb{Z}, j_\mathbb{Z}]_\backsim$$

para algum $i \in \mathbb{N}$ e $0 \neq j \in \mathbb{N}$.

Depois há que verificar que estas definições se comportam como *devem*; relegamo-lo a Seção 5.6. Mas de fato comportam-se! Por fim, queremos alguma forma de tratar inteiros *como* racionais; logo, para cada $i \in \mathbb{Z}$, estipulamos $i_\mathbb{Q} = [i, 1_\mathbb{Z}]_\backsim$. De novo, verificamos na Seção 5.6 que tudo isto se comporta corretamente.

## 5.3 A Reta Real

O passo seguinte é mostrar como construir os reais a partir dos racionais. Antes disso, há que perceber o que há de *distintivo* nos reais.

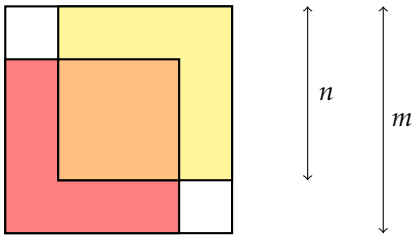
Os reais comportam-se de modo muito parecido com os racionais. (Tecnicamente, ambos são exemplos de *corpos ordenados*; para a definição, ver Definição 5.9.) Agora, se resolveu os exercícios de Capítulo 4, saberá que há estritamente mais reais do que racionais, isto é, que $\mathbb{Q} \prec \mathbb{R}$. Cantor foi o primeiro a provar isto. Há, contudo, cerca de dois milênios e meio que se conhecem números irracionais, isto é, reais que não são racionais. De fato:

**Teorema 5.4.** *$\sqrt{2}$ não é racional, isto é, $\sqrt{2} \notin \mathbb{Q}$*

*Prova.* Suponhamos, por *reductio*, que $\sqrt{2}$ é racional. Então $\sqrt{2} = {}^m/_n$ para alguns números naturais $m$ e $n$. De fato, podemos escolher $m$ e $n$ de modo a que a fração não possa ser mais reduzida. Reorganizando, $m^2 = 2n^2$. A partir daqui, completamos a prova de duas formas:

*Primeiro, geometricamente* (seguindo Tennenbaum).[2] Consideremos estes quadrados:

[2] Esta prova é relatada por Conway (2006).




□

Como $m^2 = 2n^2$, a região em que os dois quadrados de lado $n$ se sobrepõem tem a mesma área que a região que nenhum dos dois quadrados cobre; isto é, a área do quadrado cor de laranja é igual à soma das áreas dos dois quadrados não sombreados. Logo, se o quadrado cor de laranja tem lado $p$ e cada quadrado não sombreado tem lado $q$, então $p^2 = 2q^2$. Mas então $\sqrt{2} = p/q$, com $p < m$, $q < n$ e $p, q \in \mathbb{N}$. Isto contradiz o fato de $m$ e $n$ terem sido escolhidos tão pequenos quanto possível.

*Segundo, formalmente.* Como $m^2 = 2n^2$, segue-se que $m$ é par. (É fácil mostrar que, se $x$ é ímpar, então $x^2$ é ímpar.) Logo $m = 2r$, para algum $r \in \mathbb{N}$. Rearranjando, $2r^2 = n^2$, logo $n$ também é par. Assim $m$ e $n$ são ambos pares, e portanto a fração $m/n$ *pode* ser ainda reduzida. Contradição!

De passagem, esta prova diagramática permite relembrar o material de Seção 77.4. Tennenbaum (1927–2006) era um matemático inequivocamente moderno; mas a prova é inegavelmente bela, completamente rigorosa e apela à intuição geométrica!

Em todo o caso: os reais são "mais extensos" do que os racionais. Nalgum sentido, há "lacunas" nos racionais, e os reais preenchem-nas. Weierstrass apercebeu-se de que isto descreve uma única propriedade dos números reais que os distingue dos racionais, nomeadamente a *propriedade de completude*: *Todo conjunto não vazio de números reais com majorante tem um supremo (menor majorante).*

É fácil ver que os racionais não têm a propriedade de completude. Por exemplo, considere-se o conjunto dos racionais menores que $\sqrt{2}$, isto é:

$$\{p \in \mathbb{Q} : p^2 < 2 \text{ ou } p < 0\}$$

Este conjunto tem um majorante nos racionais; os seus membros são todos menores que 3, por exemplo. Mas qual é o seu supremo? Queremos dizer "$\sqrt{2}$"; contudo, acabamos de ver que $\sqrt{2}$ *não* é racional. E não existe racional mínimo entre os que são estritamente maiores que $\sqrt{2}$. Logo, o conjunto tem majorante, mas não tem supremo. Assim, os racionais não satisfazem a propriedade de completude.

Em contraste, o contínuo "moralmente deveria" ter a propriedade de completude. Não queremos apenas que $\sqrt{2}$ seja um número real; queremos preencher todas as "lacunas" da reta racional. Queremos, ainda, que o próprio contínuo não tenha "lacunas". É exatamente isso que obteremos via completude.

## 5.4 De $\mathbb{Q}$ para $\mathbb{R}$

Em essência, a propriedade de completude mostra que qualquer ponto $\alpha$ da reta real divide essa reta em duas metades de modo perfeito: numa, $\alpha$ é o supremo; noutra, $\alpha$ é o ínfimo. Para *construir* os números reais a partir dos racionais, Dedekind sugeriu que pensássemos nos reais simplesmente como os *cortes* que particionam os racionais. Isto é, identificamos $\sqrt{2}$ com o *corte* que separa os racionais $< \sqrt{2}$ dos racionais $> \sqrt{2}$.

Vamos pôr isto em ordem. Se cortarmos os racionais em duas metades, podemos identificar de modo único a partição que fizemos considerando apenas a metade *inferior*. Sendo precisos, apresentamos a seguinte definição:

**Definição 5.5 (Corte).** Um *corte* $\alpha$ é qualquer segmento inicial próprio não vazio dos racionais sem máximo. Isto é, $\alpha$ é um corte sse:

1. *não vazio, próprio*: $\emptyset \neq \alpha \subsetneq \mathbb{Q}$
2. *inicial*: para todos $p, q \in \mathbb{Q}$: se $p < q \in \alpha$ então $p \in \alpha$
3. *sem máximo*: para todo $p \in \alpha$ existe $q \in \alpha$ tal que $p < q$

Então $\mathbb{R}$ é o conjunto dos cortes.

Podemos pois dizer que $\sqrt{2} = \{p \in \mathbb{Q} : p^2 < 2 \text{ ou } p < 0\}$. Claro que há que verificar que isto *é* de fato um corte, mas relegamo-lo a Seção 5.6.

Como antes, tendo definido certas entidades, precisamos a seguir de definir funções e relações básicas sobre elas. Começamos por uma fácil:

$$\alpha \leq \beta \text{ sse } \alpha \subseteq \beta$$

Esta definição de ordem permite *enunciar* o resultado central, a saber que o conjunto dos cortes tem a propriedade de completude. Por extenso, o enunciado tem esta forma. Se $S$ é um conjunto não vazio de cortes com majorante, então $S$ tem supremo. Com mais pormenor: existe um corte, $\lambda$, que é majorante de $S$, isto é, $(\forall \alpha \in S)\alpha \subseteq \lambda$, e $\lambda$ é o menor tal corte, isto é, $(\forall \beta \in \mathbb{R})((\forall \alpha \in S)\alpha \subseteq \beta \to \lambda \subseteq \beta)$. Segue-se a prova do resultado:

**Teorema 5.6.** *O conjunto dos cortes tem a propriedade de completude.*

*Prova.* Seja $S$ um conjunto não vazio de cortes com majorante. Seja $\lambda = \bigcup S$. Começamos por alegar que $\lambda$ é um corte:

1. Como $S$ tem majorante, pelo menos um corte pertence a $S$, logo $\emptyset \neq \lambda$. Como $S$ é um conjunto de cortes, $\lambda \subseteq \mathbb{Q}$. Como $S$ tem majorante, algum $p \in \mathbb{Q}$ está ausente de todo o corte $\alpha \in S$. Logo $p \notin \lambda$, e portanto $\lambda \subsetneq \mathbb{Q}$.
2. Suponhamos $p < q \in \lambda$. Então existe algum $\alpha \in S$ tal que $q \in \alpha$. Como $\alpha$ é um corte, $p \in \alpha$. Logo $p \in \lambda$.

3. Suponhamos $p \in \lambda$. Então existe algum $\alpha \in S$ tal que $p \in \alpha$. Como $\alpha$ é um corte, existe algum $q \in \alpha$ tal que $p < q$. Logo $q \in \lambda$.

Isto prova a alegação. Além disso, claramente $(\forall \alpha \in S)\alpha \subseteq \bigcup S = \lambda$, isto é, $\lambda$ é majorante de $S$. Suponhamos agora que $\beta \in \mathbb{R}$ também é majorante, isto é, $(\forall \alpha \in S)\alpha \subseteq \beta$. Para qualquer $p \in \mathbb{Q}$, se $p \in \lambda$, então existe $\alpha \in S$ tal que $p \in \alpha$, logo $p \in \beta$. Generalizando, $\lambda \subseteq \beta$. Logo $\lambda$ é o supremo de $S$. □

Temos pois um conjunto de entidades que satisfaz a propriedade de completude. Uma forma de o dizer é: não há "lacunas" nos nossos cortes. (Assim: tomar novos "cortes" de reais, em vez de racionais, não produziria objetos novos interessantes.)

Segue-se a definição de algumas operações sobre os reais. Começamos por embutir os racionais nos reais estipulando $p_{\mathbb{R}} = \{q \in \mathbb{Q} : q < p\}$ para cada $p \in \mathbb{Q}$. Definimos então:

$$\alpha + \beta = \{p + q : p \in \alpha \wedge q \in \beta\}$$
$$\alpha \times \beta = \{p \times q : 0 \leq p \in \alpha \wedge 0 \leq q \in \beta\} \cup 0^{\mathbb{R}} \qquad \text{se } \alpha, \beta \geq 0_{\mathbb{R}}$$

Para tratar os outros casos da multiplicação, definamos primeiro:

$$-\alpha = \{p - q : p < 0 \wedge q \notin \alpha\}$$

e estipulemos:

$$\alpha \times \beta = \begin{cases} -\alpha \times -\beta & \text{se } \alpha < 0_{\mathbb{R}} \text{ e } \beta < 0_{\mathbb{R}} \\ -(-\alpha \times \beta) & \text{se } \alpha < 0_{\mathbb{R}} \text{ e } \beta > 0_{\mathbb{R}} \\ -(\alpha \times -\beta) & \text{se } \alpha > 0_{\mathbb{R}} \text{ e } \beta < 0_{\mathbb{R}} \end{cases}$$

Depois há que verificar que cada uma destas definições produz sempre um corte. E, por fim, há que fazer uma demonstração fácil (mas longa) de que os cortes, assim definidos, se comportam exatamente como devem. Mas relegamos tudo isto a Seção 5.6.

## 5.5 Algumas Reflexões Filosóficas

Quanto aos pormenores técnicos, por ora basta. Mas o que foi que alcançaram?

Bem, de forma pouco contestável, deram-nos uma matemática pura *belíssima*. Além disso, houve conquistas conceptuais profundas. Foi um insight profundo perceber que a propriedade de completude exprime a diferença crucial entre os reais e os racionais. Além disso, a construção explícita dos reais, como cortes de Dedekind, põe o objeto de estudo da análise em bases sólidas. Sabemos que a noção de *corpo ordenado completo* é coerente, pois os cortes formam precisamente um tal corpo.

Todavia, importa também levantar algumas reservas quanto a essas conquistas.

Primeiro, não é claro que pensar os reais em termos de cortes seja *mais* rigoroso do que pensá-los nas suas expansões decimais familiares (eventualmente infinitas). Esta última "construção" dos reais tem alguma semelhança com a construção via sequências de Cauchy; mas, de fato, era, essencialmente, conhecida dos matemáticos desde princípios do século XVII (ver Seção 5.7). O verdadeiro aumento de rigor veio da tomada de consciência de que os reais têm a propriedade de completude; a possibilidade de construir números reais como conjuntos particulares talvez não seja, por si só, tão interessante.

É ainda menos claro que a aritmetização (muito mais fácil) dos inteiros ou dos racionais aumente o rigor nessas áreas. Aqui, vale a pena uma observação simples. Tendo *construído* os inteiros como classes de equivalência de pares ordenados de naturais, e depois construído os racionais como classes de equivalência de pares ordenados de inteiros, e depois construído os reais como conjuntos de racionais, *nos esquecemos de imediato* das construções. Em particular: ninguém quereria *invocar* estas construções no decurso de uma prova matemática (exceto, claro, numa prova de que as construções se comportam como deviam). É muito mais fácil falar de um real diretamente do que falar de algum conjunto de conjuntos de conjuntos de conjuntos de conjuntos de conjuntos de conjuntos de naturais.

O mais duvidoso, porém, é que estas definições nos digam o que os inteiros, racionais ou reais *são*, *do ponto de vista metafísico*. Isto é, é duvidoso que os reais (digamos) *sejam* certos conjuntos (de conjuntos de conjuntos...). A principal barreira a tal visão é que a construção poderia ter sido feita de muitas maneiras diferentes. No caso dos reais, há construções genuinamente diferentes e interessantes (ver Seção 5.7). Mas eis uma forma trivial de obter construções diferentes: como em Seção 2.2, poderíamos ter definido pares ordenados de modo ligeiramente diferente; se tivéssemos usado essa noção alternativa de par ordenado, as nossas construções teriam funcionado exatamente tão bem como funcionaram, mas teríamos acabado com objetos diferentes. Assim, há muitas construções rivais, em teoria dos conjuntos, dos inteiros, racionais e reais. Seria, ademais, arbitrário (e embaraçoso) afirmar que os inteiros (digamos) são *estes* conjuntos, e não *aqueles*. (Como na Seção 2.2, isto é um caso de um argumento tornado célebre por Benacerraf 1965.)

Um outro ponto merece ser levantado: há algo de bastante *estranho* nas nossas construções. Começamos pelos números naturais. Depois, construímos os inteiros e construímos "o 0 dos inteiros", isto é, $[0,0]_\sim$. Mas $0 \neq [0,0]_\sim$. De fato, dadas as nossas construções, *nenhum* natural é um inteiro. Isto parece fortemente contraintuitivo. Na Seção 1.3, afirmamos, sem grande argumento, que $\mathbb{N} \subseteq \mathbb{Q}$. Agora, se as construções nos dissessem exatamente *o que* são os números, esta afirmação seria trivialmente falsa.

Recuando um pouco, onde chegamos? Trabalhando numa teoria ingênua

dos conjuntos e tomando os naturais como dados, podemos *tratar* inteiros, racionais e reais como certos conjuntos. Nesse sentido, podemos *embutir* as teorias destas entidades numa teoria dos conjuntos. Mas a importância filosófica deste embutimento não é assim tão direta.

Claro que isto não é a última palavra! O ponto é apenas este: mostrar que a aritmetização dos reais *é de* profunda significação filosófica exigiria argumento filosófico adicional.

## 5.6 Anéis e Corpos Ordenados

Ao longo deste capítulo, afirmamos que certas definições se comportam "como devem". Neste apêndice técnico, explicitaremos o que queremos dizer com isso e (esboçaremos como) mostrar que as definições se comportam "corretamente".

Na Seção 5.1, definimos adição e multiplicação em $\mathbb{Z}$. Queremos mostrar que, assim definidas, conferem a $\mathbb{Z}$ a estrutura que "quereríamos" que tivesse. Em particular, a estrutura em causa é a de um anel comutativo.

**Definição 5.7.** Um *anel comutativo* é um conjunto $S$, equipado com elementos distintos 0 e 1 e operações $+$ e $\times$, que satisfazem estas oito condições:

| | |
|---|---|
| *Associatividade* | $a + (b + c) = (a + b) + c$ |
| | $(a \times b) \times c = a \times (b \times c)$ |
| *Comutatividade* | $a + b = b + a$ |
| | $a \times b = b \times a$ |
| *Neutros* | $a + 0 = a$ |
| | $a \times 1 = a$ |
| *Simétrico aditivo* | $(\exists b \in S) 0 = a + b$ |
| *Distributividade* | $a \times (b + c) = (a \times b) + (a \times c)$ |

Implicitamente, todas estas fórmulas estão quantificadas universalmente sobre $S$. Note-se que os elementos 0 e 1 aqui não têm de ser os números naturais com o mesmo nome.

Logo, para verificar que os inteiros formam um anel comutativo, basta verificar estas oito condições. Nenhuma é *difícil* de estabelecer, mas o trabalho é um pouco laborioso. Por exemplo, eis como provar *associatividade*, no caso da adição:

*Prova.* Fixemos $i, j, k \in \mathbb{Z}$. Então existem $a_1, b_1, a_2, b_2, a_3, b_3 \in \mathbb{N}$ tais que $i = [a_1, b_1]$ e $j = [a_2, b_2]$ e $k = [a_3, b_3]$. (Por legibilidade, escrevemos "$[x, y]$" em

vez de "$[x, y]_\sim$"; faremos o mesmo ao longo desta secção.) Então:

$$\begin{aligned} i + (j + k) &= [a_1, b_1] + ([a_2, b_2] + [a_3, b_3]) \\ &= [a_1, b_1] + [a_2 + a_3, b_2 + b_3] \\ &= [a_1 + (a_2 + a_3), b_1 + (b_2 + b_3)] \\ &= [(a_1 + a_2) + a_3, (b_1 + b_2) + b_3] \\ &= [a_1 + a_2, b_1 + b_2] + [a_3, b_3] \\ &= ([a_1, b_1] + [a_2, b_2]) + [a_3, b_3] \\ &= (i + j) + k \end{aligned}$$

apoiando-nos livremente no comportamento da adição em $\mathbb{N}$. □

Do mesmo modo, eis uma prova do *simétrico aditivo*:

*Prova.* Fixemos $i \in \mathbb{Z}$, de modo que $i = [a, b]$ para alguns $a, b \in \mathbb{N}$. Seja $j = [b, a] \in \mathbb{Z}$. Apoiando-nos no comportamento dos naturais, $(a + b) + 0 = 0 + (a + b)$, logo $\langle a + b, b + a\rangle \sim_{\mathbb{Z}} \langle 0, 0\rangle$ por definição, e portanto $[a + b, b + a] = [0, 0] = 0_{\mathbb{Z}}$. Assim $i + j = [a, b] + [b, a] = [a + b, b + a] = [0, 0] = 0_{\mathbb{Z}}$. □

E eis uma prova da *distributividade*:

*Prova.* Como acima, fixemos $i = [a_1, b_1]$ e $j = [a_2, b_2]$ e $k = [a_3, b_3]$. Então:

$$\begin{aligned} i \times (j + k) &= [a_1, b_1] \times ([a_2, b_2] + [a_3, b_3]) \\ &= [a_1, b_1] \times [a_2 + a_3, b_2 + b_3] \\ &= [a_1(a_2 + a_3) + b_1(b_2 + b_3), a_1(b_2 + b_3) + b_1(a_2 + a_3)] \\ &= [a_1a_2 + a_1a_3 + b_1b_2 + b_1b_3, a_1b_2 + a_1b_3 + a_2b_1 + a_3b_1] \\ &= [a_1a_2 + b_1b_2, a_1b_2 + a_2b_1] + [a_1a_3 + b_1b_3, a_1b_3 + a_3b_1] \\ &= ([a_1, b_1] \times [a_2, b_2]) + ([a_1, b_1] \times [a_3, b_3]) \\ &= (i \times j) + (i \times k) \end{aligned}$$

□

Deixamos como exercício provar as cinco condições restantes. Tendo feito isso, mostramos que $\mathbb{Z}$ constitui um anel comutativo, isto é, que a adição e a multiplicação (assim definidas) se comportam como devem.

Mas a tarefa não termina. Para além de definir adição e multiplicação em $\mathbb{Z}$, definimos uma relação de ordem, $\leq$, e há que verificar que esta se comporta como deve. Com mais pormenor, há que mostrar que $\mathbb{Z}$ constitui um *anel ordenado*.[3]

[3] Como na Definição 2.16, uma ordem total é uma relação reflexiva, transitiva, antissimétrica e conexa. No contexto de relações de ordem, a conexividade é por vezes chamada *tricotomia*, pois, para quaisquer $a$ e $b$, temos $a \leq b \vee a = b \vee a \geq b$.

**Definição 5.8.** Um *anel ordenado* é um anel comutativo que está também equipado com uma relação de ordem total, $\leq$, tal que:

$$a \leq b \to a + c \leq b + c$$
$$(a \leq b \wedge 0 \leq c) \to a \times c \leq b \times c$$

Como antes, é laborioso mas rotineiro mostrar que $\mathbb{Z}$, tal como construído, é um anel ordenado. Deixamo-lo ao leitor.

Isto trata dos inteiros. Mas agora precisamos de mostrar coisas muito parecidas para os racionais. Em particular, há que mostrar que os racionais formam um *corpo ordenado*, com as nossas definições de $+$, $\times$ e $\leq$:

**Definição 5.9.** Um *corpo ordenado* é um anel ordenado que também satisfaz:

$$\textit{Inverso multiplicativo} \qquad (\forall a \in S \setminus \{0\})(\exists b \in S) a \times b = 1$$

Uma vez mostrado que $\mathbb{Z}$ constitui um anel ordenado, é fácil mas laborioso mostrar que $\mathbb{Q}$ constitui um corpo ordenado.

Tendo tratado dos inteiros e dos racionais, só restam os reais. Em particular, há que mostrar que $\mathbb{R}$ constitui um corpo ordenado *completo*, isto é, um corpo ordenado com a propriedade de completude. Agora, Teorema 5.6 estabeleceu que $\mathbb{R}$ tem a propriedade de completude. Contudo, cumpre ainda percorrer a tediosa verificação de que $\mathbb{R}$ é um corpo ordenado.

Antes de nos lançarmos a *esse* exercício laborioso, há que confirmar algumas coisas mais "imediatas". Por exemplo, precisamos de garantia de que $\alpha + \beta$, tal como definida, é de fato um *corte*, para quaisquer cortes $\alpha$ e $\beta$. Segue-se uma prova desse fato:

*Prova.* Como $\alpha$ e $\beta$ são ambos cortes, $\alpha + \beta = \{p + q : p \in \alpha \wedge q \in \beta\}$ é um subconjunto próprio não vazio de $\mathbb{Q}$. Suponhamos agora $x < p + q$ para alguns $p \in \alpha$ e $q \in \beta$. Então $x - p < q$, logo $x - p \in \beta$, e $x = p + (x - p) \in \alpha + \beta$. Logo $\alpha + \beta$ é um segmento inicial de $\mathbb{Q}$. Finalmente, para qualquer $p + q \in \alpha + \beta$, como $\alpha$ e $\beta$ são cortes, existem $p_1 \in \alpha$ e $q_1 \in \beta$ tais que $p < p_1$ e $q < q_1$; logo $p + q < p_1 + q_1 \in \alpha + \beta$; logo $\alpha + \beta$ não tem máximo. □

Esforços semelhantes permitem verificar que $\alpha - \beta$ e $\alpha \times \beta$ e $\alpha \div \beta$ são cortes (no último caso, ignorando o caso em que $\beta$ é o corte zero). De novo, deixamo-lo ao leitor.

Mas eis um pequeno fio solto a atar. Em Seção 5.4, sugerimos que podemos tomar $\sqrt{2} = \{p \in \mathbb{Q} : p < 0 \text{ ou } p^2 < 2\}$. Mas há que mostrar que este conjunto é de fato um *corte*. Segue-se uma prova desse fato:

*Prova.* Claramente isto é um segmento inicial próprio não vazio dos racionais; basta pois mostrar que não tem máximo. Em particular, basta mostrar que,

sendo $p$ um racional positivo com $p^2 < 2$ e $q = \frac{2p+2}{p+2}$, se tem $p < q$ e $q^2 < 2$. Para ver que $p < q$, basta notar:

$$\begin{aligned} p^2 &< 2 \\ p^2 + 2p &< 2 + 2p \\ p(p+2) &< 2 + 2p \\ p &< \tfrac{2+2p}{p+2} = q \end{aligned}$$

Para ver que $q^2 < 2$, basta notar:

$$\begin{aligned} p^2 &< 2 \\ 2p^2 + 4p + 2 &< p^2 + 4p + 4 \\ 4p^2 + 8p + 4 &< 2(p^2 + 4p + 4) \\ (2p+2)^2 &< 2(p+2)^2 \\ \tfrac{(2p+2)^2}{(p+2)^2} &< 2 \\ q^2 &< 2 \end{aligned}$$

□

## 5.7 Apêndice: os Reais como Sequências de Cauchy

Na Seção 5.4, construímos os reais como cortes de Dedekind. Nesta secção, explicamos uma construção alternativa. Apoia-se na definição, devida a Cauchy, do que hoje chamamos *sequência de Cauchy*; mas o uso desta definição para *construir* os reais deve-se a outros autores do século XIX, nomeadamente Weierstrass, Heine, Méray e Cantor. (Para uma boa história, ver O'Connor and Robertson 2005.)

Antes de chegarmos ao século XIX, vale a pena considerar Simon Stevin (1548–1620). Em resumo, Stevin apercebeu-se de que podemos pensar cada real em termos da sua expansão decimal. Assim, mesmo um número irracional, como $\sqrt{2}$, tem uma expansão decimal agradável, que começa:

$$1.41421356237\ldots$$

É muito fácil modelar expansões decimais na teoria dos conjuntos: basta considerá-las como funções $d\colon \mathbb{N} \to \mathbb{N}$, onde $d(n)$ é o $n$-ésimo algarismo decimal que nos interessa. Depois precisamos de um pequeno ajuste, para tratar a parte do número real que vem antes da vírgula decimal (aqui, apenas 1). Precisaremos também de outro ajuste (uma relação de equivalência) para garantir que, por exemplo, $0.999\ldots = 1$. Mas não é difícil apresentar uma construção perfeitamente rigorosa dos números reais, à maneira de Stevin, dentro da teoria dos conjuntos.

Stevin não é o nosso foco. (Para mais sobre Stevin, ver Katz and Katz 2012.) Mas eis um pensamento estreitamente relacionado. Em vez de tratar diretamente a expansão decimal de $\sqrt{2}$, podemos antes considerar uma *sequência* de aproximações racionais cada vez mais precisas a $\sqrt{2}$, olhando para as expansões cada vez mais precisas:

$$1, 1.4, 1.414, 1.4142, 1.41421, \ldots$$

A ideia de que os reais podem ser considerados via "aproximações cada vez melhores" nos dá a base para outra sequência de insights, semelhante às constatações que retivemos ao construir $\mathbb{Q}$ a partir de $\mathbb{Z}$, ou $\mathbb{Z}$ a partir de $\mathbb{N}$. Os insights básicos são estes:

1. Todo o real pode escrever-se como uma expansão decimal (eventualmente infinita).

2. A informação codificada por uma expansão decimal (eventualmente infinita) pode igualmente codificar-se por uma sequência de números racionais.

3. Uma sequência de números racionais pode pensar-se como uma função de $\mathbb{N}$ para $\mathbb{Q}$; basta definir $f(n)$ como o $n$-ésimo racional na sequência.

Claro que nem *qualquer* função de $\mathbb{N}$ para $\mathbb{Q}$ nos dará um número real. Por exemplo, considere-se esta função:

$$f(n) = \begin{cases} 1 & \text{se } n \text{ é ímpar} \\ 0 & \text{se } n \text{ é par} \end{cases}$$

Essencialmente, a preocupação é que a sequência $0, 1, 0, 1, 0, 1, 0, \ldots$ não parece "convergir" para nenhum real. Logo: para garantir que consideramos sequências que de fato convergem para algum real, precisamos de restringir a atenção a sequências que tenham algum *limite*.

Já encontramos a ideia de limite em Seção 77.2. Mas não podemos usar *exatamente* a mesma definição que ali. A expressão "$(\forall \varepsilon > 0)$" envolvia tacitamente quantificação sobre os números reais; e estávamos a considerar limites de funções nos reais; logo, invocar essa definição seria valer-nos dos números reais — e eram precisamente eles que estávamos a tentar *construir*. Felizmente, podemos trabalhar com uma ideia estreitamente relacionada com a de limite.

**Definição 5.10.** Uma função $f : \mathbb{N} \to \mathbb{Q}$ é uma *sequência de Cauchy* sse, para qualquer $\varepsilon \in \mathbb{Q}$ positivo, se tem $(\exists \ell \in \mathbb{N})(\forall m, n > \ell)|f(m) - f(n)| < \varepsilon$.

A ideia geral de limite é a mesma de antes: se se quer um certo nível de precisão (medido por $\varepsilon$), há uma "região" onde olhar (qualquer entrada maior que $\ell$). E é fácil ver que a nossa sequência 1, 1.4, 1.414, 1.4142, 1.41421… tem

limite: se se quer aproximar $\sqrt{2}$ com erro inferior a $1/10^n$, basta olhar para qualquer entrada depois da $n$-ésima.

O pensamento óbvio seria então dizer que um número real *é* simplesmente qualquer sequência de Cauchy. Mas, como nas construções de $\mathbb{Z}$ e $\mathbb{Q}$, isso seria demasiado ingênuo: para um dado número real, várias sequências de Cauchy diferentes "indicam" esse número. Uma forma simples de ver isto é a seguinte. Dada uma sequência de Cauchy $f$, defina-se $g$ como exatamente a mesma função que $f$, exceto que $g(0) \neq f(0)$. Como as duas sequências coincidem em todo o lado depois do primeiro número, quereremos, em última análise, dizer que têm o mesmo limite, no sentido de Definição 5.10, e portanto devem ser pensadas como "definindo" o mesmo real. Logo, devemos pensar nestas sequências de Cauchy como o mesmo número real.

Consequentemente, voltamos a precisar de definir uma relação de equivalência sobre as sequências de Cauchy, e identificar os números reais com *classes* de equivalência. Precisamos primeiro da ideia de uma função que tende para 0 no limite. Para qualquer função $h : \mathbb{N} \to \mathbb{Q}$, digamos que $h$ *tende para* 0 sse, para qualquer $\varepsilon \in \mathbb{Q}$ positivo, se tem que $(\exists \ell \in \mathbb{N})(\forall n > \ell)|h(n)| < \varepsilon$.[4] Além disso, sendo $f$ e $g$ funções $\mathbb{N} \to \mathbb{Q}$, definamos $(f - g)(n) = f(n) - g(n)$. Definimos agora:

$$f \eqslantless g \text{ sse } (f - g) \text{ tende para } 0.$$

Há que verificar que $\eqslantless$ é uma relação de equivalência; e de fato é. Podemos então, se quisermos, definir os reais como as classes de equivalência, sob $\eqslantless$, de todas as sequências de Cauchy de $\mathbb{N} \to \mathbb{Q}$.

Feito isto, como de costume escrevemos $[f]_{\eqslantless}$ para a classe de equivalência que tem $f$ como um membro. Porém, para manter a legibilidade, no que se segue omitimos o subscrito e escrevemos apenas $[f]$. Estipulamos também que, para cada $q \in \mathbb{Q}$, se tem $q_{\mathbb{R}} = [c_q]$, onde $c_q$ é a função constante $c_q(n) = q$ para todo $n \in \mathbb{N}$. Definimos depois relações e operações básicas sobre os reais, por exemplo:

$$[f] + [g] = [(f + g)]$$
$$[f] \times [g] = [(f \times g)]$$

onde $(f + g)(n) = f(n) + g(n)$ e $(f \times g)(n) = f(n) \times g(n)$. Claro que também há que verificar que cada uma de $(f + g)$, $(f - g)$ e $(f \times g)$ é sequência de Cauchy quando $f$ e $g$ o são; mas o são, e deixamo-lo ao leitor.

Por fim, definimos uma noção de ordem. Dizemos que $[f]$ é *positivo* sse tanto $[f] \neq 0_{\mathbb{Q}}$ como $(\exists \ell \in \mathbb{N})(\forall n > \ell) 0 < f(n)$. Depois dizemos $[f] < [g]$ sse $[(g - f)]$ é positivo. Há que verificar que isto está bem definido (isto é, que não depende da escolha da função "representante" na classe de equivalência). Mas tendo feito isto, é bastante fácil mostrar que obtemos as propriedades algébricas certas; isto é:

[4] Compare-se com a definição de $\lim_{x\to\infty} f(x) = 0$ em Seção 77.2.

**Teorema 5.11.** *As sequências de Cauchy constituem um corpo ordenado.*

*Prova.* Exercício. □

É mais difícil provar que os reais, assim construídos, têm a propriedade de completude, pelo que daremos a prova.

**Teorema 5.12.** *Todo o conjunto não vazio de sequências de Cauchy com majorante tem supremo (menor majorante).*

*Esboço de prova.* Seja $S$ um conjunto não vazio de sequências de Cauchy com majorante. Então existe algum $p \in \mathbb{Q}$ tal que $p_{\mathbb{R}}$ é majorante de $S$. Seja $r \in S$; então existe algum $q \in \mathbb{Q}$ tal que $q_{\mathbb{R}} < r$. Logo, se existe supremo de $S$, este está entre $q_{\mathbb{R}}$ e $p_{\mathbb{R}}$ (inclusive).

Nos aproximaremos do supremo, abordando-o simultaneamente por baixo e por cima. Em particular, definimos duas funções, $f, g \colon \mathbb{N} \to \mathbb{Q}$, com a ideia de que $f$ se irá aproximar do supremo por cima e $g$ por baixo. Começamos por definir:

$$f(0) = p$$
$$g(0) = q$$

Então, sendo $a_n = \frac{f(n)+g(n)}{2}$, definamos:[5]

$$f(n+1) = \begin{cases} a_n & \text{se } (\forall h \in S)[h] \leq (a_n)_{\mathbb{R}} \\ f(n) & \text{caso contrário} \end{cases}$$
$$g(n+1) = \begin{cases} a_n & \text{se } (\exists h \in S)[h] \geq (a_n)_{\mathbb{R}} \\ g(n) & \text{caso contrário} \end{cases}$$

Tanto $f$ como $g$ são sequências de Cauchy. (Isto verifica-se com relativa facilidade, mas deixamo-lo como exercício.) Note-se que a função $(f - g)$ tende para 0, pois a diferença entre $f$ e $g$ reduz-se à metade a cada passo. Logo $[f] = [g]$.

Mostramos primeiro que $[f]$ é majorante de $S$, isto é, que $(\forall h \in S)[h] \leq [f]$. (Invocaremos Teorema 5.11 ao longo do argumento.) Seja $h \in S$ e suponhamos, por *reductio*, que $[f] < [h]$, de modo que $0_{\mathbb{R}} < [(h - f)]$. Como $f$ é uma sequência de Cauchy monotonamente decrescente, existe algum $n \in \mathbb{N}$ tal que $[(c_{f(n)} - f)] < [(h - f)]$. Logo:

$$(f(n))_{\mathbb{R}} = [c_{f(n)}] < [f] + [(h - f)] = [h],$$

o que contradiz o fato de que, por construção, $[h] \leq (f(n))_{\mathbb{R}}$.

[5] Isto é uma definição recursiva. Mas ainda *não* demos qualquer razão para crer que definições recursivas são legítimas.

Mostramos a seguir que $[f] = [g]$ é o supremo de $S$. Seja $j$ qualquer sequência de Cauchy e suponhamos $[j] < [g]$. Raciocinando como acima (usando o fato de $g$ ser *crescente*), existe $n \in \mathbb{N}$ tal que $[j] < (g(n))_{\mathbb{R}}$. Mas, por construção, existe $h \in S$ tal que $(g(n))_{\mathbb{R}} \leq [h]$, logo $[j] < [h]$ e portanto $[j]$ não é majorante de $S$. □

## Problemas

**Problema 5.1.** Mostre que $(m+n)_{\mathbb{Z}} = m_{\mathbb{Z}} + n_{\mathbb{Z}}$ e $m \leq n \leftrightarrow m_{\mathbb{Z}} \leq n_{\mathbb{Z}}$, para quaisquer $m, n \in \mathbb{N}$.

**Problema 5.2.** Mostre que $\backsim$ é uma relação de equivalência.

**Problema 5.3.** Mostre que $(i+j)_{\mathbb{Q}} = i_{\mathbb{Q}} + j_{\mathbb{Q}}$ e $(i \times j)_{\mathbb{Q}} = i_{\mathbb{Q}} \times j_{\mathbb{Q}}$ e $i \leq j \leftrightarrow i_{\mathbb{Q}} \leq j_{\mathbb{Q}}$, para quaisquer $i, j \in \mathbb{Z}$.

**Problema 5.4.** Mostre que $\mathbb{Z}$ é um anel comutativo.

**Problema 5.5.** Mostre que $\mathbb{Z}$ é um anel ordenado.

**Problema 5.6.** Mostre que $\mathbb{Q}$ é um corpo ordenado.

**Problema 5.7.** Mostre que $\mathbb{R}$ é um corpo ordenado.

**Problema 5.8.** Seja $f(n) = 0$ para todo $n$. Seja $g(n) = \frac{1}{(n+1)^2}$. Mostre que ambas são sequências de Cauchy e que o limite de ambas as funções é 0, de modo que também $f \sim_{\mathbb{R}} g$.

**Problema 5.9.** Mostre que as sequências de Cauchy constituem um corpo ordenado.

# Capítulo 6

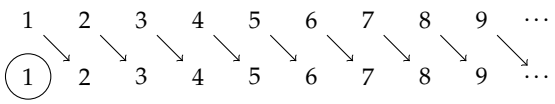
# Conjuntos Infinitos

Este capítulo sobre conjuntos infinitos foi retirado de *Open Set Theory*, de Tim Button.

## 6.1 Hotel de Hilbert

O conjunto dos números naturais é obviamente infinito. Logo, se não quisermos *valer-nos* dos números naturais, o nosso primeiro passo é caracterizar um conjunto infinito em termos que não exijam mencionar os próprios números naturais. Eis uma abordagem agradável, apresentada por Hilbert numa conferência de 1924. Ele nos pede que imaginemos

> [...] um hotel com um número finito de quartos. Todos esses quartos devem estar ocupados por exatamente um hóspede. Se os hóspedes trocam de quarto de algum modo, [mas] de tal forma que cada quarto continua a conter no máximo uma pessoa, então nenhum quarto ficará livre, e o dono do hotel não pode, deste modo, criar um novo lugar para um hóspede que acaba de chegar [...¶...]
>
> Agora estipulamos que o hotel tem infinitos quartos numerados 1, 2, 3, 4, 5, ..., cada um ocupado por exatamente um hóspede. Logo que chega um novo hóspede, o dono só precisa de mudar cada um dos hóspedes antigos para o quarto associado ao número imediatamente superior, e o quarto 1 ficará livre para o recém-chegado.




(publicado em Hilbert 2013, 730; a nossa tradução)

O ponto crucial é que o Hotel de Hilbert tem infinitos quartos; e podemos tomar a sua explicação como definição do que significa dizer isto. De fato, foi esta a abordagem de Dedekind (apresentada aqui, claro, com enorme anacronismo; a definição de Dedekind é de 1888):

**Definição 6.1.** Um conjunto $A$ é *infinito de Dedekind* sse existe uma injeção de $A$ para um subconjunto próprio de $A$. Isto é, existe algum $o \in A$ e uma injeção $f\colon A \to A$ tal que $o \notin \mathrm{Im}(f)$.

## 6.2 Álgebras de Dedekind

Não queremos apenas que os números naturais sejam infinitos; queremos que tenham certas propriedades (algébricas): precisam de comportar-se bem sob adição, multiplicação, e assim por diante.

A ideia de Dedekind foi tomar como primitiva a noção de *função sucessor* e depois caracterizar os números como aqueles que têm as seguintes propriedades:

1. Existe um número, 0, que não é sucessor de nenhum número
   isto é, $0 \notin \mathrm{Im}(s)$
   isto é, $\forall x\, s(x) \neq 0$

2. Números distintos têm sucessores distintos
   isto é, $s$ é uma injeção
   isto é, $\forall x \forall y (s(x) = s(y) \to x = y)$

3. Todo o número se obtém de 0 por aplicações repetidas da função sucessor.

As duas primeiras condições são fáceis de lidar com, usando lógica de primeira ordem (ver acima). Mas não podemos tratar (3) apenas com lógica de primeira ordem. O avanço de Dedekind foi reformular a condição (3), em termos de teoria dos conjuntos, assim:

3′. Os números naturais são o menor conjunto que é *fechado para a função sucessor*: isto é, se aplicarmos $s$ a qualquer membro do conjunto, obtemos outro membro do conjunto.

Mas precisamos de explicitar isto com calma.

**Definição 6.2.** Para qualquer função $f$, o conjunto $X$ é *$f$-fechado* sse $(\forall x \in X) f(x) \in X$. Definimos agora, para qualquer $o$:

$$\mathrm{clo}_f(o) = \bigcap \{X : o \in X \text{ e } X \text{ é } f\text{-fechado}\}$$

Logo $\text{clo}_f(o)$ é a interseção de todos os conjuntos $f$-fechados que têm $o$ como um membro. Intuitivamente, então, $\text{clo}_f(o)$ é o conjunto $f$-fechado *menor* que tem $o$ como um membro. O resultado seguinte torna preciso esse pensamento intuitivo;

**Lema 6.3.** *Para qualquer função $f$ e qualquer $o \in A$:*

1. $o \in \text{clo}_f(o)$; *e*
2. $\text{clo}_f(o)$ *é $f$-fechado; e*
3. *se $X$ é $f$-fechado e $o \in X$, então* $\text{clo}_f(o) \subseteq X$

*Prova.* Note-se que existe pelo menos um conjunto $f$-fechado com $o$ como um membro, nomeadamente $\text{Im}(f) \cup \{o\}$. Logo $\text{clo}_f(o)$, a interseção de *todos* os tais conjuntos, existe. Cumpre agora verificar (1)–(3).

Quanto a (1): $o \in \text{clo}_f(o)$ pois é uma interseção de conjuntos que todos têm $o$ como um membro.

Quanto a (2): suponhamos $x \in \text{clo}_f(o)$. Se $o \in X$ e $X$ é $f$-fechado, então $x \in X$, e agora $f(x) \in X$ pois $X$ é $f$-fechado. Logo $f(x) \in \text{clo}_f(o)$.

Quanto a (3): de modo geral, se $X \in C$ então $\bigcap C \subseteq X$. □

Com isto, podemos dizer:

**Definição 6.4.** Uma *álgebra de Dedekind* é um conjunto $A$ juntamente com uma função $f\colon A \to A$ e algum $o \in A$ tal que:

1. $o \notin \text{Im}(f)$
2. $f$ é uma injeção
3. $A = \text{clo}_f(o)$

Como $A = \text{clo}_f(o)$, o resultado anterior nos diz que $A$ é o menor conjunto $f$-fechado com $o$ como um membro. Claramente uma álgebra de Dedekind é infinita de Dedekind; basta olhar para as cláusulas (1) e (2) da definição. Mas o fato mais relevante é que qualquer conjunto infinito de Dedekind pode ser transformado numa álgebra de Dedekind.

**Teorema 6.5.** *Se existe um conjunto infinito de Dedekind, então existe uma álgebra de Dedekind.*

*Prova.* Seja $D$ infinito de Dedekind. Logo existe uma injeção $g\colon D \to D$ e um elemento $o \in D \setminus \text{Im}(g)$. Seja agora $A = \text{clo}_g(o)$; por Lema 6.3, $A$ existe e $o \in A$. Seja $f = g{\restriction_A}$. Mostraremos que $A, f, o$ formam uma álgebra de Dedekind.

Quanto a (1): $o \notin \text{Im}(g)$ e $\text{Im}(f) \subseteq \text{Im}(g)$, logo $o \notin \text{Im}(f)$.

Quanto a (2): $g$ é injetiva em $D$; logo $f \subseteq g$ tem de ser injetiva.

Quanto a (3): por Lema 6.3, $A$ é $g$-fechado; *a fortiori*, $A$ é $f$-fechado. Logo $\mathrm{clo}_f(o) \subseteq A$ por Lema 6.3. Como também $\mathrm{clo}_f(o)$ é $f$-fechado e $f = g{\restriction_A}$, segue-se que $\mathrm{clo}_f(o)$ é $g$-fechado. Logo $A \subseteq \mathrm{clo}_f(o)$ por Lema 6.3. □

## 6.3 Álgebras de Dedekind e Indução Aritmética

Crucialmente, agora, uma álgebra de Dedekind—de fato, *qualquer* álgebra de Dedekind—servirá como substituto dos números naturais. Isto deve-se à seguinte consequência trivial:

**Teorema 6.6 (Indução aritmética).** *Sejam $N, s, o$ uma álgebra de Dedekind. Então, para qualquer conjunto $X$:*

$$\textit{se } o \in X \textit{ e } (\forall n \in N \cap X)s(n) \in X, \textit{ então } N \subseteq X.$$

*Prova.* Pela definição de álgebra de Dedekind, $N = \mathrm{clo}_s(o)$. Ora, se tanto $o \in X$ como $(\forall n \in N)(n \in X \to s(n) \in X)$, então $N = \mathrm{clo}_s(o) \subseteq X$. □

Como a indução é característica dos números naturais, o ponto é este. Dado qualquer conjunto infinito de Dedekind, podemos formar uma álgebra de Dedekind e usar essa álgebra como substituto dos números naturais.

Admitidamente, Teorema 6.6 formula a indução em termos *de teoria dos conjuntos*. Mas podemos facilmente pôr o princípio em termos mais familiares:

**Corolário 6.7.** *Sejam $N, s, o$ uma álgebra de Dedekind. Então, para qualquer fórmula $\varphi(x)$, que pode ter parâmetros:*

$$\textit{se } \varphi(o) \textit{ e } (\forall n \in N)(\varphi(n) \to \varphi(s(n))), \textit{ então } (\forall n \in N)\varphi(n)$$

*Prova.* Seja $X = \{n \in N : \varphi(n)\}$, e use-se agora Teorema 6.6 □

Neste resultado, falamos de uma fórmula "ter parâmetros". O que isto significa, em traços grosseiros, é que, para quaisquer objetos $c_1, \ldots, c_k$, podemos trabalhar com $\varphi(x, c_1, \ldots, c_k)$. Com mais precisão, podemos enunciar o resultado sem mencionar "parâmetros" do seguinte modo. Para qualquer fórmula $\varphi(x, v_1, \ldots, v_k)$, cujas variáveis livres são todas as exibidas, temos:

$$\begin{aligned}\forall v_1 \ldots \forall v_k((&\varphi(o, v_1, \ldots, v_k) \wedge \\ &(\forall x \in N)(\varphi(x, v_1, \ldots, v_k) \to \varphi(s(x), v_1, \ldots, v_k))) \to \\ &(\forall x \in N)\varphi(x, v_1, \ldots, v_k))\end{aligned}$$

Evidentemente, falar em "ter parâmetros" pode tornar a leitura muito mais fácil. (Na Parte XV, usaremos este expediente com frequência.)

Voltando às álgebras de Dedekind: dada qualquer álgebra de Dedekind, podemos também definir as habituais funções aritméticas de adição, multiplicação

e exponenciação. Isto não é trivial, porém, e envolve a técnica de *definição recursiva*. É uma técnica que introduziremos e justificaremos muito mais tarde, e num contexto bem mais geral. (Os entusiastas podem querer voltar a isto depois de Capítulo 70, ou talvez ler um tratamento alternativo, como Potter 2004, pp. 95–8.) Mas, onde $N, s, o$ formam uma álgebra de Dedekind, acabaremos por poder estipular o seguinte:

$$\begin{array}{lll} a + o = a & a \times o = o & a^o = s(o) \\ a + s(b) = s(a + b) & a \times s(b) = (a \times b) + a & a^{s(b)} = a^b \times a \end{array}$$

e mostrar que estas definições se comportam como se espera.

## 6.4 "Prova" de Dedekind da existência de um conjunto infinito

Neste capítulo, apresentamos um tratamento em teoria dos conjuntos dos números naturais, em termos de álgebras de Dedekind. Em Seção 5.5, refletimos sobre o significado filosófico da aritmetização da análise (entre outras coisas). Cumpre agora refletir sobre o significado do que aqui alcançamos.

Ao longo de Capítulo 5, tomamos os números naturais como dados e os usamos para construir os inteiros, os racionais e os reais, de modo explícito. Neste capítulo, não demos uma construção explícita dos números naturais. Mostramos apenas que, *dado qualquer conjunto infinito de Dedekind*, podemos definir um conjunto que se comportará como queremos que $\mathbb{N}$ se comporte.

Obviamente, pois, não podemos pretender ter respondido a uma questão metafísica, como *quais os objetos que são os números naturais*. Mas isso é bom. Afinal, na Seção 5.5, sublinhamos que estaríamos errados se pensássemos na definição de $\mathbb{R}$ como conjunto de cortes de Dedekind como uma *descoberta*, em vez de uma estipulação conveniente. A observação crucial é que os cortes de Dedekind exemplificam as propriedades matemáticas centrais dos números reais. Assim também aqui: a observação crucial é que *qualquer* álgebra de Dedekind exemplifica as propriedades matemáticas centrais dos números naturais. (De fato, Dedekind insistiu neste ponto ao provar que todas as álgebras de Dedekind são *isomorfas* (1888, Theorems 132–3). Não surpreende, então, que muitos "estruturalistas" contemporâneos cite Dedekind como precursor.)

Além disso, mostramos como embutir a teoria dos números naturais numa teoria ingênua simples dos conjuntos, que ainda permanece bastante informal, mas que (aparentemente) não assume os números naturais como dados. Assim, podemos estar no caminho de realizar o próprio projeto ambicioso de Dedekind, que ele explicou assim:

> Na ciência nada que seja provável deve ser acreditado sem prova. Embora esta exigência pareça razoável, não posso considerá-la satisfeita sequer nos métodos mais recentes de lançar os fundamen-

> tos da ciência mais simples; a saber, aquela parte da lógica que trata da teoria dos números. Ao falar de aritmética (álgebra, análise) como mera parte da lógica, quero insinuar que considero o conceito de número totalmente independente das noções ou intuições de espaço e tempo—que o considero antes um produto imediato das leis puras do pensamento. (Dedekind, 1888, preface)

A ideia audaciosa de Dedekind é esta. Acabamos de mostrar como construir os números naturais usando só (ingenuamente) a teoria dos conjuntos. Em Capítulo 5, vimos como construir os reais dados os números naturais e alguma teoria dos conjuntos. Logo, talvez, "a aritmética (álgebra, análise)" acabe por ser "meramente parte da lógica" (no sentido alargado que Dedekind dá à palavra "lógica").

Essa é a ideia. Mas esperemos um momento. A nossa construção de uma álgebra de Dedekind (o nosso substituto dos números naturais) é condicional à existência de um conjunto infinito de Dedekind. (Basta olhar para trás, para Teorema 6.5.) A menos que a existência de um conjunto infinito de Dedekind possa ser estabelecida via "lógica" ou "as leis puras do pensamento", o projeto estagna.

Então, *pode* a existência de um conjunto infinito de Dedekind ser estabelecida pelas "leis puras do pensamento"? Eis o esforço de Dedekind:

> O meu próprio reino de pensamentos, isto é, a totalidade $S$ de todas as coisas que podem ser objetos do meu pensamento, é infinita. Pois, se $s$ designa um elemento de $S$, então o pensamento $s'$ de que $s$ pode ser objeto do meu pensamento é ele próprio um elemento de $S$. Se considerarmos isto como uma imagem $\varphi(s)$ do elemento $s$, então ... $S$ é infinito de Dedekind, como queríamos ter provado. (Dedekind, 1888, §66)

Isto é algo de espantoso de encontrar no meio de um livro que em grande parte consiste em provas matemáticas altamente rigorosas. Duas observações valem a pena.

Primeiro: esta "prova" mal tem o que hoje reconheceríamos como caráter "matemático". Fala de objetos psicológicos (pensamentos), e apenas de objetos *possíveis*.

Segundo: pelo menos tal como apresentamos as álgebras de Dedekind, esta "prova" tem uma lacuna técnica direta. Se o argumento de Dedekind é bem-sucedido, estabelece só que há infinitas coisas (nomeadamente, infinitos pensamentos). Mas Dedekind também precisa de nos dar uma razão para ver $S$ como um único *conjunto*, com infinitos membros, em vez de pensar em $S$ como *algumas coisas* (no plural).

O fato de Dedekind não ver aqui uma lacuna pode sugerir que o seu uso da palavra "totalidade" não corresponde exatamente ao *nosso* uso da pala-

vra "conjunto".[1] Mas isto não seria demasiado surpreendente. O projeto que perseguimos nos últimos dois capítulos—uma "construção" dos naturais e, a partir deles, uma "construção" dos inteiros, reais e racionais—foi todo ele feito de modo ingênuo. Nos apoiamos neste conjunto, ou naquele conjunto, sempre que precisamos, sem enunciar muitos princípios gerais sobre exatamente que conjuntos existem, e quando. Mas sabemos que precisamos de *alguns* princípios gerais, pois caso contrário caímos no Paradoxo de Russell.

Chegou a hora de superarmos a nossa ingenuidade.

## 6.5 Apêndice: Provando Schröder-Bernstein

Antes de deixarmos a teoria ingênua dos conjuntos, há ainda uma última prova ingênua (mas sofisticada!) a considerar. Trata-se de uma prova de Schröder-Bernstein (Teorema 4.25): se $A \preceq B$ e $B \preceq A$ então $A \approx B$; isto é, dados injeções $f\colon A \to B$ e $g\colon B \to A$, existe uma bijeção $h\colon A \to B$.

Neste capítulo, seguimos a noção dedekindiana de *fechos*. De fato, Dedekind deu uma prova muito elegante de Schröder-Bernstein com esta noção, e aqui a apresentamos. A prova segue de perto Potter (2004, pp. 157–8), se quiser um tratamento ligeiramente diferente mas essencialmente semelhante. Uma breve pesquisa na Internet também convencerá o leitor de que este é um teorema—tal como a irracionalidade de $\sqrt{2}$—para o qual existem *muitas* provas interessantes e distintas.

Usando notação semelhante à de Definição 6.2, seja

$$\mathrm{Clo}_f(B) = \bigcap\{X : B \subseteq X \text{ e } X \text{ é } f\text{-fechado}\}$$

para cada conjunto $B$ e função $f$. Assim definido, $\mathrm{Clo}_f(B)$ é o menor conjunto $f$-fechado que contém $B$, no sentido de que:

**Lema 6.8.** *Para qualquer função $f$, e qualquer $B$:*

1. $B \subseteq \mathrm{Clo}_f(B)$*; e*
2. $\mathrm{Clo}_f(B)$ *é $f$-fechado; e*
3. *se $X$ é $f$-fechado e $B \subseteq X$, então* $\mathrm{Clo}_f(B) \subseteq X$.

*Prova.* Exatamente como no Lema 6.3. □

Precisamos de mais um fato para chegar a Schröder-Bernstein:

**Proposição 6.9.** *Se $A \subseteq B \subseteq C$ e $A \approx C$, então $A \approx B \approx C$.*

[1] De fato, temos outras razões para pensar que não correspondia; ver Potter (2004, p. 23).

*Prova.* Dada uma bijeção $f\colon C \to A$, seja $F = \mathrm{Clo}_f(C \setminus B)$ e defina-se uma função $g$ com domínio $C$ do seguinte modo:

$$g(x) = \begin{cases} f(x) & \text{se } x \in F \\ x & \text{caso contrário} \end{cases}$$

Mostraremos que $g$ é uma bijeção de $C$ para $B$, donde seguirá que $g \circ f^{-1}\colon A \to B$ é uma bijeção, completando a prova.

Primeiro alegamos que, se $x \in F$ mas $y \notin F$, então $g(x) \neq g(y)$. Por reductio, suponhamos o contrário, de modo que $y = g(y) = g(x) = f(x)$. Como $x \in F$ e $F$ é $f$-fechado por Lema 6.8, temos $y = f(x) \in F$, contradição.

Suponhamos agora $g(x) = g(y)$. Então, pelo que precede, $x \in F$ sse $y \in F$. Se $x, y \in F$, então $f(x) = g(x) = g(y) = f(y)$, logo $x = y$ pois $f$ é uma bijeção. Se $x, y \notin F$, então $x = g(x) = g(y) = y$. Logo $g$ é uma injeção.

Resta mostrar que $\mathrm{Im}(g) = B$. Fixemos $x \in B \subseteq C$. Se $x \notin F$, então $g(x) = x$. Se $x \in F$, então $x = f(y)$ para algum $y \in F$, pois caso contrário $F \setminus \{x\}$ seria $f$-fechado e estenderia $C \setminus B$, o que é impossível por Lema 6.8; agora $g(y) = f(y) = x$. □

Finalmente, eis a prova do resultado principal. Recordemos que, dada uma função $h$ e um conjunto $D$, definimos $h[D] = \{h(x) : x \in D\}$.

*Prova de Schröder-Bernstein.* Sejam $f\colon A \to B$ e $g\colon B \to A$ injeções. Como $f[A] \subseteq B$, temos $g[f[A]] \subseteq g[B] \subseteq A$. Além disso, $g \circ f\colon A \to g[f[A]]$ é uma injeção, pois tanto $g$ como $f$ o são; e de fato $g \circ f$ é uma bijeção, apenas pela forma como definimos o seu contradomínio. Logo $g[f[A]] \approx A$, e portanto, por Proposição 6.9, existe uma bijeção $h\colon A \to g[B]$. Além disso, $g^{-1}$ é uma bijeção $g[B] \to B$. Logo $g^{-1} \circ h\colon A \to B$ é uma bijeção. □

# Parte II

# Propositional Logic

This part contains material on classical propositional logic. The first chapter is relatively rudimentary and just lists definitions and results, many proofs are not carried out but are left as exercises. The material on proof systems and the completeness theorem is included from the part on first-order logic, with the "FOL" tag set to false. This leaves out everything related to predicates, terms, and quantifiers, and replaces talk of estruturas $\mathfrak{M}$ with talk about valorações $\mathfrak{v}$.

It is planned to expand this part to include more detail, and to add further topics and results, such as truth-functional completeness.

# Capítulo 7

# Syntax and Semantics

This is a very quick summary of definitions only. It should be expanded to provide a gentle intro to proofs by induction on formulas, with lots more examples.

# Capítulo 8

# Sistemas de Derivação

Este capítulo reúne material geral sobre sistemas de derivação. Um livro-texto que usa um sistema específico pode inserir a seção de introdução mais a seção de panorama relevante no início do capítulo que introduz esse sistema.

## 8.1 Introdução

As lógicas comumente têm tanto uma semântica quanto um sistema de derivação. A semântica trata de conceitos como verdade, satisfatibilidade, validade e consequência. O propósito dos sistemas de derivação é fornecer um método puramente sintático de estabelecer consequência e validade. Eles são puramente sintáticos no sentido de que uma derivação em tal sistema é um objeto sintático finito, geralmente uma sequência (ou outra disposição finita) de sentenças ou fórmulas. Bons sistemas de derivação têm a propriedade de que qualquer sequência ou disposição dada de sentenças ou fórmulas pode ser verificada mecanicamente como "correta".

Os sistemas de derivação mais simples (e historicamente os primeiros) para a lógica de primeira ordem foram *axiomáticos*. Uma sequência de fórmulas conta como uma derivação em tal sistema se cada fórmula individual nela é ou está entre um conjunto fixo de "axiomas" ou segue de fórmulas anteriores na sequência por uma entre um número fixo de "regras de inferência"—e pode ser verificado mecanicamente se uma fórmula é um axioma e se segue corretamente de outras fórmulas por uma das regras de inferência. Sistemas de derivação axiomáticos são fáceis de descrever—e também fáceis de tratar meta-teoricamente—mas as derivações neles são difíceis de ler e entender, e também difíceis de produzir.

Outros sistemas de derivação foram desenvolvidos com o objetivo de facilitar a construção de derivações ou facilitar a compreensão de derivações

uma vez completas. Exemplos são a dedução natural, árvores de verdade, também conhecidas como provas por tableaux, e o cálculo de sequentes. Alguns sistemas de derivação são projetados especialmente com a mecanização em mente; por exemplo, o método da resolução é fácil de implementar em software (mas suas derivações são essencialmente impossíveis de entender). A maioria desses outros sistemas de derivação representa derivações como árvores de fórmulas em vez de sequências. Isso facilita ver quais partes de uma derivação dependem de quais outras partes.

Assim, para uma dada lógica, como a lógica de primeira ordem, os diferentes sistemas de derivação darão diferentes explicações do que significa uma sentença ser um *teorema* e o que significa uma sentença ser derivável a partir de outras. Seja como for feito isso (via derivações axiomáticas, deduções naturais, derivações de sequentes, árvores de verdade, refutações por resolução), queremos que essas relações correspondam às noções semânticas de validade e consequência. Escrevamos $\vdash \varphi$ para "$\varphi$ é um teorema" e "$\Gamma \vdash \varphi$" para "$\varphi$ é derivável de $\Gamma$." Seja como for $\vdash$ definido, queremos que corresponda a $\vDash$, isto é:

1. $\vdash \varphi$ se, e somente se, $\vDash \varphi$
2. $\Gamma \vdash \varphi$ se, e somente se, $\Gamma \vDash \varphi$

A direção "somente se" acima é chamada de *correção*. Um sistema de derivação é correto se a derivabilidade garante consequência (ou validade). Todo sistema de derivação decente tem que ser correto; sistemas de derivação incorretos não são úteis de modo algum. Afinal, o propósito inteiro de uma derivação é fornecer uma garantia sintática de validade ou consequência. Provaremos a correção para os sistemas de derivação que apresentamos.

A direção conversa "se" também é importante: é chamada de *completude*. Um sistema de derivação completo é forte o suficiente para mostrar que $\varphi$ é um teorema sempre que $\varphi$ é válida, e que $\Gamma \vdash \varphi$ sempre que $\Gamma \vDash \varphi$. A completude é mais difícil de estabelecer, e algumas lógicas não têm sistemas de derivação completos. A lógica de primeira ordem tem. Kurt Gödel foi o primeiro a provar a completude para um sistema de derivação da lógica de primeira ordem em sua dissertação de 1929.

Outro conceito ligado aos sistemas de derivação é o de *consistência*. Um conjunto de sentenças é chamado inconsistente se qualquer coisa pode ser derivada dele, e consistente caso contrário. A inconsistência é a contrapartida sintática da insatisfatibilidade: como conjuntos insatisfatíveis, conjuntos inconsistentes de sentenças não fazem boas teorias; são defeituosos de maneira fundamental. Conjuntos consistentes de sentenças podem não ser verdadeiros ou úteis, mas pelo menos passam esse limiar mínimo de utilidade lógica. Para diferentes sistemas de derivação, a definição específica de consistência de conjuntos de sentenças pode diferir, mas como $\vdash$, queremos que a consistência coincida com sua contrapartida semântica, a satisfatibilidade. Queremos que

seja sempre o caso que $\Gamma$ é consistente se, e somente se, é satisfatível. Aqui, a direção "somente se" corresponde à completude (consistência garante satisfatibilidade), e a direção "se" corresponde à correção (satisfatibilidade garante consistência). De fato, para a lógica clássica de primeira ordem, as duas versões de correção e completude são equivalentes.

## 8.2 O Cálculo de Sequentes

Enquanto muitos sistemas de derivação operam com disposições de sentenças, o cálculo de sequentes opera com *sequentes*. Um sequente é uma expressão da forma

$$\varphi_1, \ldots, \varphi_m \Rightarrow \psi_1, \ldots, \psi_m,$$

isto é, um par de sequências de sentenças, separadas pelo símbolo de sequente $\Rightarrow$. Qualquer uma das sequências pode ser vazia. Uma derivação no cálculo de sequentes é uma árvore de sequentes, em que os sequentes mais altos são de uma forma especial (são chamados de "sequentes iniciais" ou "axiomas") e todo outro sequente segue dos sequentes imediatamente acima dele por uma das regras de inferência. As regras de inferência ou manipulam as sentenças nos sequentes (adicionando, removendo ou rearranjando-as à esquerda ou à direita), ou introduzem uma fórmula complexa na conclusão da regra. Por exemplo, a regra $\wedge$L permite a inferência de $\varphi, \Gamma \Rightarrow \Delta$ para $\varphi \wedge \psi, \Gamma \Rightarrow \Delta$, e a $\rightarrow$R permite a inferência de $\varphi, \Gamma \Rightarrow \Delta, \psi$ para $\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi$, para quaisquer $\Gamma$, $\Delta$, $\varphi$ e $\psi$. (Em particular, $\Gamma$ e $\Delta$ podem ser vazios.)

A relação $\vdash$ baseada no cálculo de sequentes é definida da seguinte forma: $\Gamma \vdash \varphi$ se, e somente se, há alguma sequência $\Gamma_0$ tal que toda $\varphi$ em $\Gamma_0$ está em $\Gamma$ e há uma derivação com o sequente $\Gamma_0 \Rightarrow \varphi$ em sua raiz. $\varphi$ é um teorema no cálculo de sequentes se o sequente $\Rightarrow \varphi$ tem uma derivação. Por exemplo, aqui está uma derivação que mostra que $\vdash (\varphi \wedge \psi) \rightarrow \varphi$:

$$\dfrac{\dfrac{\varphi \Rightarrow \varphi}{\varphi \wedge \psi \Rightarrow \varphi}\wedge\text{L}}{\Rightarrow (\varphi \wedge \psi) \rightarrow \varphi}\rightarrow\text{R}$$

Um conjunto $\Gamma$ é inconsistente no cálculo de sequentes se há uma derivação de $\Gamma_0 \Rightarrow$ (em que toda $\varphi \in \Gamma_0$ está em $\Gamma$ e o lado direito do sequente é vazio). Usando a regra WR, qualquer sentença pode ser derivada a partir de um conjunto inconsistente.

O cálculo de sequentes foi inventado na década de 1930 por Gerhard Gentzen. Por causa de seu desenho sistemático e simétrico, é um formalismo muito útil para desenvolver uma teoria de derivações. É relativamente fácil encontrar derivações no cálculo de sequentes, mas essas derivações são frequentemente difíceis de ler e sua conexão com provas às vezes não é fácil de ver. Provou ser uma abordagem muito elegante a sistemas de derivação, no entanto, e muitas lógicas têm sistemas de cálculo de sequentes.

## 8.3 Dedução Natural

A dedução natural é um sistema de derivação destinado a espelhar o raciocínio real (especialmente o tipo de raciocínio regimentado empregado por matemáticos). O raciocínio real procede por vários padrões "naturais". Por exemplo, a prova por casos nos permite estabelecer uma conclusão com base em uma premissa disjuntiva, estabelecendo que a conclusão segue de qualquer um dos disjuntos. A prova indireta nos permite estabelecer uma conclusão mostrando que sua negação leva a uma contradição. A prova condicional estabelece uma afirmação condicional "se ... então ..." mostrando que o consequente segue do antecedente. A dedução natural é uma formalização de algumas dessas inferências naturais. Cada um dos conectivos lógicos e quantificadores vem com duas regras, uma de introdução e uma de eliminação, e cada uma corresponde a um desses padrões de inferência natural. Por exemplo, $\rightarrow$Intro corresponde à prova condicional, e $\vee$Elim à prova por casos. Uma regra particularmente simples é $\wedge$Elim, que permite a inferência de $\varphi \wedge \psi$ para $\varphi$ (ou $\psi$).

Uma característica que distingue a dedução natural de outros sistemas de derivação é o uso de hipóteses. Uma derivação em dedução natural é uma árvore de fórmulas. Uma única fórmula fica na raiz da árvore de fórmulas, e as "folhas" da árvore são fórmulas das quais a conclusão é derivada. Na dedução natural, algumas fórmulas folha desempenham um papel dentro da derivação, mas são "consumidas" quando a derivação atinge a conclusão. Isso corresponde à prática, no raciocínio real, de introduzir hipóteses que só permanecem em vigor por um curto período. Por exemplo, em uma prova por casos, assumimos a verdade de cada um dos disjuntos; na prova condicional, assumimos a verdade do antecedente; na prova indireta, assumimos a verdade da negação da conclusão. Essa maneira de introduzir hipóteses hipotéticas e depois descartá-las a serviço de estabelecer um passo intermediário é uma marca da dedução natural. As fórmulas nas folhas de uma derivação em dedução natural são chamadas de hipóteses, e algumas das regras de inferência podem descarregá-las. Por exemplo, se temos uma derivação de $\psi$ a partir de algumas hipóteses que incluem $\varphi$, então a regra $\rightarrow$Intro nos permite inferir $\varphi \rightarrow \psi$ e descartar qualquer hipótese da forma $\varphi$. (Para acompanhar quais hipóteses são descartadas em quais inferências, rotulamos a inferência e as hipóteses que ela descarta com um número.) As hipóteses que permanecem não descarregadas no final da derivação são, juntas, suficientes para a verdade da conclusão, de modo que uma derivação estabelece que suas hipóteses não descarregadas implicam sua conclusão.

A relação $\Gamma \vdash \varphi$ baseada na dedução natural vale se, e somente se, há uma derivação em que $\varphi$ é a última sentença na árvore, e toda folha que está não descarregada está em $\Gamma$. $\varphi$ é um teorema na dedução natural se, e somente se, há uma derivação em que $\varphi$ é a última sentença e todas as hipóteses são descarregadas. Por exemplo, aqui está uma derivação que mostra que $\vdash (\varphi \wedge$

$\psi) \to \varphi$:

$$\dfrac{\dfrac{[\varphi \wedge \psi]^1}{\varphi}\,\wedge\text{Elim}}{(\varphi \wedge \psi) \to \varphi}\,{}^{1}\,\to\text{Intro}$$

O rótulo 1 indica que a hipótese $\varphi \wedge \psi$ é descarregada na inferência $\to$Intro.

Um conjunto $\Gamma$ é inconsistente se, e somente se, $\Gamma \vdash \bot$ na dedução natural. A regra $\bot_I$ faz com que, a partir de um conjunto inconsistente, qualquer sentença possa ser derivada.

Sistemas de dedução natural foram desenvolvidos por Gerhard Gentzen e Stanisław Jaśkowski na década de 1930, e depois por Dag Prawitz e Frederic Fitch. Porque suas inferências espelham métodos naturais de prova, é favorecida por filósofos. As versões desenvolvidas por Fitch são frequentemente usadas em livros introdutórios de lógica. Na filosofia da lógica, as regras da dedução natural às vezes foram tomadas como dando os significados dos operadores lógicos ("semântica da Teoria da Prova").

## 8.4 Tableaux

Enquanto muitos sistemas de derivação operam com disposições de sentenças, os tableaux operam com fórmulas assinadas. A fórmula assinada é um par consistindo em um sinal de valor de verdade ($\mathbb{T}$ ou $\mathbb{F}$) e a sentença

$$\mathbb{T}\varphi \text{ ou } \mathbb{F}\varphi.$$

A tableau consiste em fórmulas assinadas dispostas em uma árvore ramificada para baixo. Começa com várias *hipóteses* e continua com fórmulas assinadas que resultam de uma das fórmulas assinadas acima dela pela aplicação de uma das regras de inferência. Cada regra nos permite adicionar uma ou mais fórmulas assinadas ao final de um ramo, ou duas fórmulas assinadas lado a lado—neste caso um ramo se divide em dois, com as duas fórmulas assinadas adicionadas formando os finais dos dois ramos.

Uma regra aplicada a uma fórmula assinada complexa resulta na adição de fórmulas assinadas que são sub-fórmulas imediatas. Elas vêm em pares, uma regra para cada um dos dois sinais. Por exemplo, a regra $\wedge\mathbb{T}$ se aplica a $\mathbb{T}\varphi \wedge \psi$, e permite a adição tanto das duas fórmulas assinadas $\mathbb{T}\varphi$ quanto de $\mathbb{T}\psi$ ao final de qualquer ramo que contém $\mathbb{T}\varphi \wedge \psi$, e a regra $\varphi \wedge \psi\mathbb{F}$ permite que um ramo seja dividido adicionando $\mathbb{F}\varphi$ e $\mathbb{F}\psi$ lado a lado. A tableau é fechado se cada um de seus ramos contém um par correspondente de fórmulas assinadas $\mathbb{T}\varphi$ e $\mathbb{F}\varphi$.

A relação $\vdash$ baseada em tableaux é definida da seguinte forma: $\Gamma \vdash \varphi$ se, e somente se, há algum conjunto finito $\Gamma_0 = \{\psi_1, \ldots, \psi_n\} \subseteq \Gamma$ tal que há um tableau fechado para as hipóteses

$$\{\mathbb{F}\varphi, \mathbb{T}\psi_1, \ldots, \mathbb{T}\psi_n\}$$

Por exemplo, aqui está um tableau fechado que mostra que $\vdash (\varphi \wedge \psi) \to \varphi$:

| | | |
|---|---|---|
| 1. | $\mathbb{F}(\varphi \wedge \psi) \to \varphi$ | Assumption |
| 2. | $\mathbb{T}\varphi \wedge \psi$ | $\to\mathbb{F}\,1$ |
| 3. | $\mathbb{F}\varphi$ | $\to\mathbb{F}\,1$ |
| 4. | $\mathbb{T}\varphi$ | $\to\mathbb{T}\,2$ |
| 5. | $\mathbb{T}\psi$ | $\to\mathbb{T}\,2$ |
| | $\otimes$ | |

Um conjunto $\Gamma$ é inconsistente no cálculo de tableau se há um tableau fechado para hipóteses

$$\{\mathbb{T}\psi_1, \ldots, \mathbb{T}\psi_n\}$$

para algum $\psi_i \in \Gamma$.

Os Tableaux foram inventados na década de 1950 independentemente por Evert Beth e Jaakko Hintikka, e simplificados e popularizados por Raymond Smullyan. São muito fáceis de usar, pois construir um tableau é um procedimento muito sistemático. Por causa da natureza sistemática dos tableaux, eles também se prestam à implementação por computador. No entanto, um tableau é frequentemente difícil de ler e sua conexão com provas às vezes não é fácil de ver. A abordagem também é bastante geral, e muitas lógicas diferentes têm sistemas de tableau. Os Tableaux também nos ajudam a encontrar estruturas que satisfazem sentenças (ou conjuntos de sentenças) dadas: se o conjunto é satisfatível, ele não terá um tableau fechado, isto é, qualquer tableau terá um ramo aberto. A estrutura satisfatória pode ser "lida" de um ramo aberto, desde que toda regra que seja possível aplicar tenha sido aplicada naquele ramo. Há também uma conexão muito estreita com o cálculo de sequentes: essencialmente, um tableau fechado é uma derivação condensada no cálculo de sequentes, escrita de cabeça para baixo.

## 8.5 Dedução Axiomática

As derivações axiomáticas são os sistemas de derivação lógicos mais antigos e mais simples. Suas derivações são simplesmente sequências de sentenças. Uma sequência de sentenças conta como uma derivação correta se toda sentença $\varphi$ nela satisfaz uma das seguintes condições:

1. $\varphi$ é um axioma, ou
2. $\varphi$ é um membro de um dado conjunto $\Gamma$ de sentenças, ou
3. $\varphi$ é justificada por uma regra de inferência.

Para ser um axioma, $\varphi$ tem que ter a forma de um entre vários esquemas fixos de sentença. Há muitos conjuntos de esquemas de axiomas que fornecem

um sistema de derivação satisfatório (correto e completo) para a lógica de primeira ordem. Alguns são organizados de acordo com os conectivos que governam, por exemplo, os esquemas

$$\varphi \to (\psi \to \varphi) \qquad \psi \to (\psi \vee \chi) \qquad (\psi \wedge \chi) \to \psi$$

são axiomas comuns que governam $\to$, $\vee$ e $\wedge$. Alguns sistemas de axiomas visam um número mínimo de axiomas. Dependendo dos conectivos tomados como primitivos, é até possível encontrar sistemas de axiomas que consistem em um único axioma.

Uma regra de inferência é uma afirmação condicional que dá uma condição suficiente para que uma sentença em uma derivação seja justificada. O modus ponens é uma regra muito comum desse tipo: diz que se $\varphi$ e $\varphi \to \psi$ já estão justificados, então $\psi$ está justificado. Isso significa que uma linha em uma derivação que contém a sentença $\psi$ está justificada, desde que tanto $\varphi$ quanto $\varphi \to \psi$ (para alguma sentença $\varphi$) apareçam na derivação antes de $\psi$.

A relação $\vdash$ baseada em derivações axiomáticas é definida da seguinte forma: $\Gamma \vdash \varphi$ se, e somente se, há uma derivação com a sentença $\varphi$ como sua última fórmula (e $\Gamma$ é tomado como o conjunto de sentenças nessa derivação que são justificadas por (2) acima). $\varphi$ é um teorema se $\varphi$ tem uma derivação em que $\Gamma$ é vazio, isto é, toda sentença na derivação é justificada por (1) ou (3). Por exemplo, aqui está uma derivação que mostra que $\vdash \varphi \to (\psi \to (\psi \vee \varphi))$:

1. $\psi \to (\psi \vee \varphi)$
2. $(\psi \to (\psi \vee \varphi)) \to (\varphi \to (\psi \to (\psi \vee \varphi)))$
3. $\varphi \to (\psi \to (\psi \vee \varphi))$

A sentença na linha 1 tem a forma do axioma $\varphi \to (\varphi \vee \psi)$ (com os papéis de $\varphi$ e $\psi$ invertidos). A sentença na linha 2 tem a forma do axioma $\varphi \to (\psi \to \varphi)$. Assim, ambas as linhas estão justificadas. A linha 3 é justificada por modus ponens: se a abreviarmos como $\theta$, então a linha 2 tem a forma $\chi \to \theta$, onde $\chi$ é $\psi \to (\psi \vee \varphi)$, isto é, a linha 1.

Um conjunto $\Gamma$ é inconsistente se $\Gamma \vdash \bot$. Um sistema de axiomas completo também provará que $\bot \to \varphi$ para qualquer $\varphi$, e assim, se $\Gamma$ é inconsistente, então $\Gamma \vdash \varphi$ para qualquer $\varphi$.

Sistemas de derivações axiomáticas para lógica foram dados pela primeira vez por Gottlob Frege em sua *Begriffsschrift* de 1879, que por essa razão é frequentemente considerada a primeira obra da lógica moderna. Foram aperfeiçoados em *Principia Mathematica* de Alfred North Whitehead e Bertrand Russell e por David Hilbert e seus alunos na década de 1920. São assim frequentemente chamados de "sistemas de Frege" ou "sistemas de Hilbert". São muito versáteis no sentido de que é frequentemente fácil encontrar um sistema axiomático para uma lógica. Porque as derivações têm uma estrutura muito simples e apenas uma ou duas regras de inferência, também é relativamente fácil provar coisas *sobre* eles. No entanto, são muito difíceis de usar na prática, isto é, é difícil encontrar e escrever provas.

# Capítulo 9

# O Cálculo de Sequentes

Este capítulo apresenta o cálculo de sequentes padrão LK de Gentzen para a lógica clássica de primeira ordem. Ele poderia ter mais exemplos e exercícios. Para incluir ou excluir material relevante ao cálculo de sequentes como sistema de prova, use a tag "prfLK".

## 9.1 Regras e Derivações

Para o que segue, sejam $\Gamma, \Delta, \Pi, \Lambda$ representando sequências finitas de sentenças.

**Definição 9.1 (Sequente).** Um *sequente* é uma expressão da forma

$$\Gamma \Rightarrow \Delta$$

em que $\Gamma$ e $\Delta$ são sequências finitas (possivelmente vazias) de sentenças da linguagem $\mathcal{L}$. $\Gamma$ é chamado de *antecedente*, enquanto $\Delta$ é o *sucedente*.

A ideia intuitiva por trás de um sequente é: se todas as sentenças no antecedente valem, então ao menos uma das sentenças no sucedente vale. Isto é, se $\Gamma = \langle \varphi_1, \ldots, \varphi_m \rangle$ e $\Delta = \langle \psi_1, \ldots, \psi_n \rangle$, então $\Gamma \Rightarrow \Delta$ vale se, e somente se,

$$(\varphi_1 \wedge \cdots \wedge \varphi_m) \rightarrow (\psi_1 \vee \cdots \vee \psi_n)$$

vale. Há dois casos especiais: quando $\Gamma$ é vazio e quando $\Delta$ é vazio. Quando $\Gamma$ é vazio, isto é, $m = 0$, $\Rightarrow \Delta$ vale se, e somente se, $\psi_1 \vee \cdots \vee \psi_n$ vale. Quando $\Delta$ é vazio, isto é, $n = 0$, $\Gamma \Rightarrow$ vale se, e somente se, $\neg(\varphi_1 \wedge \cdots \wedge \varphi_m)$ vale. Dizemos que um sequente é válido se, e somente se, a sentença correspondente é válida.

Se $\Gamma$ é uma sequência de sentenças, escrevemos $\Gamma, \varphi$ para o resultado de acrescentar $\varphi$ à extremidade direita de $\Gamma$ (e $\varphi, \Gamma$ para o resultado de acrescentar $\varphi$ à extremidade esquerda de $\Gamma$). Se $\Delta$ também é uma sequência de sentenças, então $\Gamma, \Delta$ é a concatenação das duas sequências.

**Definição 9.2 (Sequente Inicial).** Um *sequente inicial* é um sequente de uma das seguintes formas:

1. $\varphi \Rightarrow \varphi$
2. $\bot \Rightarrow$

para qualquer sentença $\varphi$ na linguagem.

Derivações no cálculo de sequentes são certas árvores de sequentes, em que os sequentes no topo são sequentes iniciais e, se um sequente está abaixo de um ou dois outros sequentes, ele deve seguir corretamente por uma regra de inferência. As regras para **LK** dividem-se em dois tipos principais: regras *lógicas* e regras *estruturais*. As regras lógicas recebem o nome do operador principal da sentença que contém $\varphi$ e/ou $\psi$ no sequente inferior. Cada uma vem em duas versões, uma para inferir um sequente com a sentença que contém o operador lógico à esquerda, e uma com a sentença à direita.

## 9.2 Regras Proposicionais

**Regras para $\neg$**

$$\frac{\Gamma \Rightarrow \Delta, \varphi}{\neg\varphi, \Gamma \Rightarrow \Delta}\,\neg\mathrm{L} \qquad \frac{\varphi, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\varphi}\,\neg\mathrm{R}$$

**Regras para $\wedge$**

$$\frac{\varphi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}\,\wedge\mathrm{L} \qquad \frac{\psi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}\,\wedge\mathrm{L} \qquad \frac{\Gamma \Rightarrow \Delta, \varphi \qquad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}\,\wedge\mathrm{R}$$

**Regras para $\vee$**

$$\frac{\varphi, \Gamma \Rightarrow \Delta \qquad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta}\,\vee\mathrm{L} \qquad \frac{\Gamma \Rightarrow \Delta, \varphi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}\,\vee\mathrm{R} \qquad \frac{\Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}\,\vee\mathrm{R}$$

### Regras para $\rightarrow$

$$\frac{\Gamma \Rightarrow \Delta, \varphi \qquad \psi, \Pi \Rightarrow \Lambda}{\varphi \rightarrow \psi, \Gamma, \Pi \Rightarrow \Delta, \Lambda} \rightarrow\text{L} \qquad\qquad \frac{\varphi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi} \rightarrow\text{R}$$

## 9.3 Regras Estruturais

Precisamos também de algumas regras que nos permitam reorganizar sentenças nos lados esquerdo e direito de um sequente. Como as regras lógicas exigem que as sentenças na premissa sobre as quais a regra atua estejam ou na extremidade esquerda ou na extremidade direita, precisamos de uma regra de "troca" que nos permita mover sentenças para a posição correta. Às vezes também é importante poder combinar duas sentenças idênticas em uma só, e acrescentar a sentença em qualquer um dos lados.

### Enfraquecimento

$$\frac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\,\text{WL} \qquad\qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi}\,\text{WR}$$

### Contração

$$\frac{\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\,\text{CL} \qquad\qquad \frac{\Gamma \Rightarrow \Delta, \varphi, \varphi}{\Gamma \Rightarrow \Delta, \varphi}\,\text{CR}$$

### Troca

$$\frac{\Gamma, \varphi, \psi, \Pi \Rightarrow \Delta}{\Gamma, \psi, \varphi, \Pi \Rightarrow \Delta}\,\text{XL} \qquad\qquad \frac{\Gamma \Rightarrow \Delta, \varphi, \psi, \Lambda}{\Gamma \Rightarrow \Delta, \psi, \varphi, \Lambda}\,\text{XR}$$

Uma série de inferências de enfraquecimento, contração e troca será frequentemente indicada por linhas de inferência duplas.

A regra a seguir, chamada de "corte", não é estritamente necessária, mas torna muito mais fácil reutilizar e combinar derivações.

$$\frac{\Gamma \Rightarrow \Delta, \varphi \qquad \varphi, \Pi \Rightarrow \Lambda}{\Gamma, \Pi \Rightarrow \Delta, \Lambda}\ \text{Cut}$$

## 9.4 Derivações

Já dissemos como é um sequente inicial e demos as regras de inferência. Derivações no cálculo de sequentes são geradas indutivamente a partir disso: cada derivação ou é um sequente inicial por si só, ou consiste em uma ou duas derivações seguidas de uma inferência.

**Definição 9.3 (LK-derivação).** Uma **LK**-*derivação* de um sequente $S$ é uma árvore finita de sequentes que satisfaz as seguintes condições:

1. Os sequentes no topo da árvore são sequentes iniciais.
2. O sequente na base da árvore é $S$.
3. Todo sequente na árvore exceto $S$ é uma premissa de uma aplicação correta de uma regra de inferência cuja conclusão está diretamente abaixo daquele sequente na árvore.

Dizemos então que $S$ é o *sequente final* da derivação e que $S$ é *derivável em* **LK** (ou **LK**-derivável).

**Exemplo 9.4.** Todo sequente inicial, por exemplo, $\chi \Rightarrow \chi$, é a derivação. Podemos obter uma nova derivação a partir disso aplicando, digamos, a regra WL,

$$\frac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\ \text{WL}$$

A regra, contudo, deve ser geral: podemos substituir o $\varphi$ na regra por qualquer sentença, por exemplo, também por $\theta$. Se a premissa corresponde ao nosso sequente inicial $\chi \Rightarrow \chi$, isso significa que tanto $\Gamma$ quanto $\Delta$ são apenas $\chi$, e a conclusão seria então $\theta, \chi \Rightarrow \chi$. Assim, o seguinte é a derivação:

$$\frac{\chi \Rightarrow \chi}{\theta, \chi \Rightarrow \chi}\ \text{WL}$$

Podemos agora aplicar outra regra, digamos XL, que nos permite trocar duas sentenças à esquerda. Assim, o seguinte também é uma derivação correta:

$$\dfrac{\dfrac{\chi \Rightarrow \chi}{\theta, \chi \Rightarrow \chi}\ \text{WL}}{\chi, \theta \Rightarrow \chi}\ \text{XL}$$

Nesta aplicação da regra, que foi dada como

$$\dfrac{\Gamma, \varphi, \psi, \Pi \Rightarrow \Delta}{\Gamma, \psi, \varphi, \Pi \Rightarrow \Delta,} \text{XL}$$

tanto $\Gamma$ quanto $\Pi$ eram vazios, $\Delta$ é $\chi$, e os papéis de $\varphi$ e $\psi$ são desempenhados por $\theta$ e $\chi$, respectivamente. De modo muito semelhante, vemos também que

$$\dfrac{\theta \Rightarrow \theta}{\chi, \theta \Rightarrow \theta} \text{WL}$$

é a derivação. Agora podemos pegar essas duas derivações e combiná-las usando $\wedge$R. Aquela regra era

$$\dfrac{\Gamma \Rightarrow \Delta, \varphi \qquad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi} \wedge\text{R}$$

No nosso caso, as premissas devem corresponder aos últimos sequentes das derivações que terminam nas premissas. Isso significa que $\Gamma$ é $\chi, \theta$, $\Delta$ é vazio, $\varphi$ é $\chi$ e $\psi$ é $\theta$. Assim, a conclusão, se a inferência for correta, é $\chi, \theta \Rightarrow \chi \wedge \theta$.

$$\dfrac{\dfrac{\dfrac{\chi \Rightarrow \chi}{\theta, \chi \Rightarrow \chi}\text{WL}}{\chi, \theta \Rightarrow \chi}\text{XL} \qquad \dfrac{\theta \Rightarrow \theta}{\chi, \theta \Rightarrow \theta}\text{WL}}{\chi, \theta \Rightarrow \chi \wedge \theta} \wedge\text{R}$$

É claro que também podemos inverter as premissas; então $\varphi$ seria $\theta$ e $\psi$ seria $\chi$.

$$\dfrac{\dfrac{\theta \Rightarrow \theta}{\chi, \theta \Rightarrow \theta}\text{WL} \qquad \dfrac{\dfrac{\chi \Rightarrow \chi}{\theta, \chi \Rightarrow \chi}\text{WL}}{\chi, \theta \Rightarrow \chi}\text{XL}}{\chi, \theta \Rightarrow \theta \wedge \chi} \wedge\text{R}$$

## 9.5 Exemplos de Derivações

**Exemplo 9.5.** Dê uma **LK**-derivação para o sequente $\varphi \wedge \psi \Rightarrow \varphi$.

Começamos escrevendo o sequente final desejado na base da derivação.

$$\dfrac{}{\varphi \wedge \psi \Rightarrow \varphi}$$

Em seguida, precisamos descobrir que tipo de inferência poderia ter um sequente inferior dessa forma. Poderia ser uma regra estrutural, mas é uma boa ideia começar procurando uma regra lógica. O único conectivo lógico que ocorre no sequente inferior é $\wedge$, então procuramos uma regra de $\wedge$ e, como o símbolo $\wedge$ ocorre no antecedente, estamos diante da regra $\wedge$L.

$$\dfrac{}{\varphi \wedge \psi \Rightarrow \varphi} \wedge\text{L}$$

Há duas opções para o que poderia ter sido o sequente superior da inferência $\wedge$L: poderíamos ter um sequente superior $\varphi \Rightarrow \varphi$ ou $\psi \Rightarrow \varphi$. Claramente, $\varphi \Rightarrow \varphi$ é um sequente inicial (o que é bom), enquanto $\psi \Rightarrow \varphi$ não é derivável em geral. Preenchemos o sequente superior:

$$\dfrac{\varphi \Rightarrow \varphi}{\varphi \wedge \psi \Rightarrow \varphi} \wedge\text{L}$$

Agora temos uma **LK**-derivação correta do sequente $\varphi \wedge \psi \Rightarrow \varphi$.

**Exemplo 9.6.** Dê uma **LK**-derivação para o sequente $\neg\varphi \vee \psi \Rightarrow \varphi \to \psi$.

Comece escrevendo o sequente final desejado na base da derivação.

$$\dfrac{}{\neg\varphi \vee \psi \Rightarrow \varphi \to \psi}$$

Para encontrar uma regra lógica que pudesse nos dar esse sequente final, olhamos para os conectivos lógicos no sequente final: $\neg$, $\vee$ e $\to$. No momento, só nos importam $\vee$ e $\to$, porque são operadores principais de sentenças no sequente final, enquanto $\neg$ está dentro do escopo de outro conectivo, de modo que cuidaremos dele depois. Nossas opções de regras lógicas para a inferência final são, portanto, a regra $\vee$L e a regra $\to$R. Poderíamos escolher qualquer uma das regras, na verdade, mas vamos escolher a regra $\to$R (quando não fosse por outro motivo, porque ela nos permite adiar a divisão em dois ramos). De acordo com a forma das inferências $\to$R que podem produzir o sequente inferior, isto deve ser assim:

$$\dfrac{\dfrac{}{\varphi, \neg\varphi \vee \psi \Rightarrow \psi}}{\neg\varphi \vee \psi \Rightarrow \varphi \to \psi} \to\text{R}$$

Se movermos $\neg\varphi \vee \psi$ para a parte externa do antecedente, podemos aplicar a regra $\vee$L. De acordo com o esquema, isto deve se dividir em dois sequentes superiores como segue:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\varphi, \varphi \Rightarrow \psi} \quad \dfrac{}{\psi, \varphi \Rightarrow \psi}}{\neg\varphi \vee \psi, \varphi \Rightarrow \psi} \vee\text{L}}{\varphi, \neg\varphi \vee \psi \Rightarrow \psi} \text{XR}}{\neg\varphi \vee \psi \Rightarrow \varphi \to \psi} \to\text{R}$$

Lembre-se de que estamos tentando subir até sequentes iniciais; parece que estamos bem perto! O ramo direito está a apenas um enfraquecimento e uma troca de um sequente inicial, e então estará pronto:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\varphi, \varphi \Rightarrow \psi} \quad \dfrac{\dfrac{\dfrac{}{\psi \Rightarrow \psi}}{\varphi, \psi \Rightarrow \psi} \text{WL}}{\psi, \varphi \Rightarrow \psi} \text{XL}}{\neg\varphi \vee \psi, \varphi \Rightarrow \psi} \vee\text{L}}{\varphi, \neg\varphi \vee \psi \Rightarrow \psi} \text{XR}}{\neg\varphi \vee \psi \Rightarrow \varphi \to \psi} \to\text{R}$$

Agora, olhando para o ramo esquerdo, o único conectivo lógico em qualquer sentença é o símbolo $\neg$ nas sentenças do antecedente, então estamos diante de uma instância da regra $\neg$L.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \Rightarrow \psi, \varphi}}{\neg\varphi, \varphi \Rightarrow \psi}\neg\text{L} \quad \dfrac{\dfrac{\dfrac{}{\psi \Rightarrow \psi}}{\varphi, \psi \Rightarrow \psi}\text{WL}}{\psi, \varphi \Rightarrow \psi}\text{XL}}{\neg\varphi \vee \psi, \varphi \Rightarrow \psi}\vee\text{L}}{\dfrac{\varphi, \neg\varphi \vee \psi \Rightarrow \psi}{\neg\varphi \vee \psi \Rightarrow \varphi \to \psi}\to\text{R}}\text{XR}$$

De modo semelhante a como finalizamos o ramo direito, estamos a apenas um enfraquecimento e uma troca de finalizar também este ramo esquerdo.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \Rightarrow \varphi}}{\varphi \Rightarrow \varphi, \psi}\text{WR}}{\varphi \Rightarrow \psi, \varphi}\text{XR}}{\neg\varphi, \varphi \Rightarrow \psi}\neg\text{L} \quad \dfrac{\dfrac{\dfrac{}{\psi \Rightarrow \psi}}{\varphi, \psi \Rightarrow \psi}\text{WL}}{\psi, \varphi \Rightarrow \psi}\text{XL}}{\neg\varphi \vee \psi, \varphi \Rightarrow \psi}\vee\text{L}}{\dfrac{\varphi, \neg\varphi \vee \psi \Rightarrow \psi}{\neg\varphi \vee \psi \Rightarrow \varphi \to \psi}\to\text{R}}\text{XR}$$

**Exemplo 9.7.** Dê uma **LK**-derivação do sequente $\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)$

Usando as técnicas acima, começamos escrevendo o sequente final desejado na base.

$$\dfrac{}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}$$

Os conectivos principais disponíveis das sentenças no sequente final são o símbolo $\vee$ e o símbolo $\neg$. Funcionaria aplicar aqui ou a regra $\vee$L ou a regra $\neg$R, mas começamos com a regra $\neg$R porque ela evita, por ora, a divisão em dois ramos:

$$\dfrac{\dfrac{}{\varphi \wedge \psi, \neg\varphi \vee \neg\psi \Rightarrow}}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}\neg\text{R}$$

Agora temos a escolha de olhar para a regra $\wedge$L ou a regra $\vee$L. Vejamos o que acontece quando aplicamos a regra $\wedge$L: temos a escolha de começar com o sequente $\varphi, \neg\varphi \vee \psi \Rightarrow$ ou com o sequente $\psi, \neg\varphi \vee \psi \Rightarrow$ . Como a derivação é simétrica em relação a $\varphi$ e $\psi$, vamos com o primeiro:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi, \neg\varphi \vee \neg\psi \Rightarrow}}{\varphi \wedge \psi, \neg\varphi \vee \neg\psi \Rightarrow}\wedge\text{L}}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}\neg\text{R}$$

Continuando a preencher a derivação, vemos que esbarramos em um problema:

$$\dfrac{\dfrac{\dfrac{\dfrac{\varphi \Rightarrow \varphi}{\neg\varphi, \varphi \Rightarrow}\neg\mathrm{L} \quad \dfrac{\overline{\varphi \Rightarrow \psi}\,?}{\neg\psi, \varphi \Rightarrow}\neg\mathrm{L}}{\neg\varphi \vee \neg\psi, \varphi \Rightarrow}\vee\mathrm{L}}{\varphi, \neg\varphi \vee \neg\psi \Rightarrow}\mathrm{XL}}{\varphi \wedge \psi, \neg\varphi \vee \neg\psi \Rightarrow}\wedge\mathrm{L}}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}\neg\mathrm{R}$$

O topo do ramo direito não pode ser reduzido mais, e ele não pode ser levado, por meio de inferências estruturais, a um sequente inicial, então este não é o caminho certo a tomar. Assim, claramente, foi um erro aplicar a regra $\wedge$L acima. Voltando ao que tínhamos antes e executando a regra $\vee$L em vez disso, obtemos

$$\dfrac{\dfrac{\dfrac{\overline{\neg\varphi, \varphi \wedge \psi \Rightarrow} \quad \overline{\neg\psi, \varphi \wedge \psi \Rightarrow}}{\neg\varphi \vee \neg\psi, \varphi \wedge \psi \Rightarrow}\vee\mathrm{L}}{\varphi \wedge \psi, \neg\varphi \vee \neg\psi \Rightarrow}\mathrm{XL}}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}\neg\mathrm{R}$$

Completando cada ramo como fizemos antes, obtemos

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\varphi \Rightarrow \varphi}{\varphi \wedge \psi \Rightarrow \varphi}\wedge\mathrm{L}}{\neg\varphi, \varphi \wedge \psi \Rightarrow}\neg\mathrm{L} \quad \dfrac{\dfrac{\psi \Rightarrow \psi}{\varphi \wedge \psi \Rightarrow \psi}\wedge\mathrm{L}}{\neg\psi, \varphi \wedge \psi \Rightarrow}\neg\mathrm{L}}{\neg\varphi \vee \neg\psi, \varphi \wedge \psi \Rightarrow}\vee\mathrm{L}}{\varphi \wedge \psi, \neg\varphi \vee \neg\psi \Rightarrow}\mathrm{XL}}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}\neg\mathrm{R}$$

(Poderíamos ter executado as regras de $\wedge$ mais abaixo do que as regras de $\neg$ nesses passos e ainda assim obtido uma derivação correta).

**Exemplo 9.8.** Até agora não usamos a regra de contração, mas às vezes ela é necessária. Eis um exemplo em que isso acontece. Suponha que queiramos provar $\Rightarrow \varphi \vee \neg\varphi$. Aplicar $\vee$R de trás para frente nos daria uma destas duas derivações:

$$\dfrac{\dfrac{\overline{\Rightarrow \varphi}}{\Rightarrow \varphi \vee \neg\varphi}\vee\mathrm{R} \qquad \dfrac{\dfrac{\overline{\varphi \Rightarrow}}{\Rightarrow \neg\varphi}\neg\mathrm{R}}{\Rightarrow \varphi \vee \neg\varphi}\vee\mathrm{R}$$

Nenhuma destas, é claro, termina em um sequente inicial. O truque é perceber que a regra de contração nos permite combinar duas cópias de a sentença em uma só—e quando estamos buscando uma prova, isto é, indo de baixo para cima, podemos manter uma cópia de $\varphi \vee \neg\varphi$ na premissa, por exemplo,

$$\dfrac{\dfrac{\dfrac{}{\Rightarrow \varphi \vee \neg\varphi, \varphi}}{\Rightarrow \varphi \vee \neg\varphi, \varphi \vee \neg\varphi}\,\vee\mathrm{R}}{\Rightarrow \varphi \vee \neg\varphi}\,\mathrm{CR}$$

Agora podemos aplicar $\vee$R uma segunda vez, e também obter $\neg\varphi$, o que leva a uma derivação completa.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \Rightarrow \varphi}}{\Rightarrow \varphi, \neg\varphi}\,\neg\mathrm{R}}{\Rightarrow \varphi, \varphi \vee \neg\varphi}\,\vee\mathrm{R}}{\Rightarrow \varphi \vee \neg\varphi, \varphi}\,\mathrm{XR}}{\Rightarrow \varphi \vee \neg\varphi, \varphi \vee \neg\varphi}\,\vee\mathrm{R}}{\Rightarrow \varphi \vee \neg\varphi}\,\mathrm{CR}$$

Esta seção reúne as definições da relação de demonstrabilidade e de consistência para a dedução natural.

## 9.6 Noções da Teoria da Prova

Assim como definimos uma série de noções semânticas importantes (validade, consequência, satisfatibilidade), definimos agora as *noções da teoria da prova* correspondentes. Elas não são definidas por apelo à satisfação de sentenças em estruturas, mas por apelo à derivabilidade ou à não derivabilidade de certos sequentes. Foi uma descoberta importante que essas noções coincidem. Que elas coincidem é o conteúdo dos teoremas da *correção* e da *completude*.

**Definição 9.9 (Teoremas).** A sentença $\varphi$ é um *teorema* se há a derivação em **LK** do sequente $\Rightarrow \varphi$. Escrevemos $\vdash \varphi$ se $\varphi$ é um teorema e $\nvdash \varphi$ se não é.

**Definição 9.10 (Derivabilidade).** A sentença $\varphi$ é *derivável de* um conjunto de sentenças $\Gamma$, $\Gamma \vdash \varphi$, se, e somente se, há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ e uma sequência $\Gamma_0'$ das sentenças em $\Gamma_0$ tal que **LK** deriva $\Gamma_0' \Rightarrow \varphi$. Se $\varphi$ não é derivável de $\Gamma$, escrevemos $\Gamma \nvdash \varphi$.

Por causa das regras de contração, enfraquecimento e troca, a ordem e o número de sentenças em $\Gamma_0'$ não importam: se um sequente $\Gamma_0' \Rightarrow \varphi$ é derivável, então também o é $\Gamma_0'' \Rightarrow \varphi$ para qualquer $\Gamma_0''$ que contenha as mesmas sentenças que $\Gamma_0'$. Por exemplo, se $\Gamma_0 = \{\psi, \chi\}$, então tanto $\Gamma_0' = \langle \psi, \psi, \chi \rangle$ quanto $\Gamma_0'' = \langle \chi, \chi, \psi \rangle$ são sequências que contêm apenas as sentenças em $\Gamma_0$. Se um sequente contendo uma delas é derivável, o outro também é, por exemplo:

$$\dfrac{\dfrac{\dfrac{\vdots}{\psi, \psi, \chi \Rightarrow \varphi}\,\text{CL}}{\psi, \chi \Rightarrow \varphi}\,\text{XL}}{\chi, \psi \Rightarrow \varphi}\,\text{WL}$$

De agora em diante, diremos que, se $\Gamma_0$ é um conjunto finito de sentenças, então $\Gamma_0 \Rightarrow \varphi$ é qualquer sequente em que o antecedente é uma sequência de sentenças em $\Gamma_0$, e incluiremos tacitamente contrações, trocas e enfraquecimentos se necessário.

**Definição 9.11 (Consistência).** Um conjunto de sentenças $\Gamma$ é *inconsistente* se, e somente se, há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ tal que **LK** deriva $\Gamma_0 \Rightarrow$ . Se $\Gamma$ não é inconsistente, isto é, se para todo $\Gamma_0 \subseteq \Gamma$ finito, **LK** não deriva $\Gamma_0 \Rightarrow$ , dizemos que é *consistente*.

**Proposição 9.12 (Reflexividade).** *Se $\varphi \in \Gamma$, então $\Gamma \vdash \varphi$.*

*Prova.* O sequente inicial $\varphi \Rightarrow \varphi$ é derivável, e $\{\varphi\} \subseteq \Gamma$. □

**Proposição 9.13 (Monotonicidade).** *Se $\Gamma \subseteq \Delta$ e $\Gamma \vdash \varphi$, então $\Delta \vdash \varphi$.*

*Prova.* Suponha $\Gamma \vdash \varphi$, isto é, há um $\Gamma_0 \subseteq \Gamma$ finito tal que $\Gamma_0 \Rightarrow \varphi$ é derivável. Como $\Gamma \subseteq \Delta$, então $\Gamma_0$ também é um subconjunto finito de $\Delta$. A derivação de $\Gamma_0 \Rightarrow \varphi$ mostra, assim, também que $\Delta \vdash \varphi$. □

**Proposição 9.14 (Transitividade).** *Se $\Gamma \vdash \varphi$ e $\{\varphi\} \cup \Delta \vdash \psi$, então $\Gamma \cup \Delta \vdash \psi$.*

*Prova.* Se $\Gamma \vdash \varphi$, há um $\Gamma_0 \subseteq \Gamma$ finito e a derivação $\pi_0$ de $\Gamma_0 \Rightarrow \varphi$. Se $\{\varphi\} \cup \Delta \vdash \psi$, então, para algum subconjunto finito $\Delta_0 \subseteq \Delta$, há a derivação $\pi_1$ de $\varphi, \Delta_0 \Rightarrow \psi$. Considere a seguinte derivação:

$$\dfrac{\begin{array}{cc}\vdots\,\pi_0 & \vdots\,\pi_1\\ \Gamma_0 \Rightarrow \varphi & \varphi, \Delta_0 \Rightarrow \psi\end{array}}{\Gamma_0, \Delta_0 \Rightarrow \psi}\,\text{Cut}$$

Como $\Gamma_0 \cup \Delta_0 \subseteq \Gamma \cup \Delta$, isso mostra $\Gamma \cup \Delta \vdash \psi$. □

Note que isso significa, em particular, que se $\Gamma \vdash \varphi$ e $\varphi \vdash \psi$, então $\Gamma \vdash \psi$. Segue-se também que se $\varphi_1, \ldots, \varphi_n \vdash \psi$ e $\Gamma \vdash \varphi_i$ para cada $i$, então $\Gamma \vdash \psi$.

**Proposição 9.15.** *$\Gamma$ é inconsistente se, e somente se, $\Gamma \vdash \varphi$ para toda sentença $\varphi$.*

*Prova.* Exercício. □

**Proposição 9.16 (Compacidade).** *1. Se $\Gamma \vdash \varphi$, então há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ tal que $\Gamma_0 \vdash \varphi$.*

*2. Se todo subconjunto finito de $\Gamma$ é consistente, então $\Gamma$ é consistente.*

*Prova.* 1. Se $\Gamma \vdash \varphi$, então há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ tal que o sequente $\Gamma_0 \Rightarrow \varphi$ tem a derivação. Consequentemente, $\Gamma_0 \vdash \varphi$.

2. Se $\Gamma$ é inconsistente, há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ tal que **LK** deriva $\Gamma_0 \Rightarrow$ . Mas então $\Gamma_0$ é um subconjunto finito de $\Gamma$ que é inconsistente. □

## 9.7 Derivabilidade e Consistência

Estabeleceremos agora uma série de propriedades da relação de derivabilidade. Elas são interessantes por si mesmas, mas cada uma terá um papel na prova do teorema da completude.

**Proposição 9.17.** *Se $\Gamma \vdash \varphi$ e $\Gamma \cup \{\varphi\}$ é inconsistente, então $\Gamma$ é inconsistente.*

*Prova.* Há $\Gamma_0$ e $\Gamma_1 \subseteq \Gamma$ finitos tais que **LK** deriva $\Gamma_0 \Rightarrow \varphi$ e $\varphi, \Gamma_1 \Rightarrow$ . Seja $\pi_0$ a **LK**-derivação de $\Gamma_0 \Rightarrow \varphi$ e $\pi_1$ a **LK**-derivação de $\Gamma_1, \varphi \Rightarrow$ . Podemos então derivar

$$\dfrac{\begin{array}{cc}\vdots\,\pi_0 & \vdots\,\pi_1\\ \Gamma_0 \Rightarrow \varphi & \varphi, \Gamma_1 \Rightarrow\end{array}}{\Gamma_0, \Gamma_1 \Rightarrow}\ \text{Cut}$$

Como $\Gamma_0 \subseteq \Gamma$ e $\Gamma_1 \subseteq \Gamma$, $\Gamma_0 \cup \Gamma_1 \subseteq \Gamma$; portanto, $\Gamma$ é inconsistente. □

**Proposição 9.18.** *$\Gamma \vdash \varphi$ se, e somente se, $\Gamma \cup \{\neg\varphi\}$ é inconsistente.*

*Prova.* Primeiro, suponha $\Gamma \vdash \varphi$, isto é, há a derivação $\pi_0$ de $\Gamma \Rightarrow \varphi$. Acrescentando uma regra ¬L, obtemos a derivação de $\neg\varphi, \Gamma \Rightarrow$ , isto é, $\Gamma \cup \{\neg\varphi\}$ é inconsistente.

Se $\Gamma \cup \{\neg\varphi\}$ é inconsistente, há a derivação $\pi_1$ de $\neg\varphi, \Gamma \Rightarrow$ . O seguinte é a derivação de $\Gamma \Rightarrow \varphi$:

$$\dfrac{\dfrac{\varphi \Rightarrow \varphi}{\Rightarrow \varphi, \neg\varphi}\,\neg\text{R} \qquad \begin{array}{c}\vdots\,\pi_1\\ \neg\varphi, \Gamma \Rightarrow\end{array}}{\Gamma \Rightarrow \varphi}\ \text{Cut}$$

□

**Proposição 9.19.** *Se $\Gamma \vdash \varphi$ e $\neg\varphi \in \Gamma$, então $\Gamma$ é inconsistente.*

*Prova.* Suponha $\Gamma \vdash \varphi$ e $\neg\varphi \in \Gamma$. Então há a derivação $\pi$ de um sequente $\Gamma_0 \Rightarrow \varphi$. O sequente $\neg\varphi, \Gamma_0 \Rightarrow$ também é derivável:

$$\dfrac{\dfrac{\vdots\,\pi}{\Gamma_0 \Rightarrow \varphi} \qquad \dfrac{\dfrac{\varphi \Rightarrow \varphi}{\neg\varphi, \varphi \Rightarrow}\,\neg\mathrm{L}}{\varphi, \neg\varphi \Rightarrow}\,\mathrm{XL}}{\Gamma_0, \neg\varphi \Rightarrow}\,\mathrm{Cut}$$

Como $\neg\varphi \in \Gamma$ e $\Gamma_0 \subseteq \Gamma$, isso mostra que $\Gamma$ é inconsistente. □

**Proposição 9.20.** *Se $\Gamma \cup \{\varphi\}$ e $\Gamma \cup \{\neg\varphi\}$ são ambos inconsistentes, então $\Gamma$ é inconsistente.*

*Prova.* Há conjuntos finitos $\Gamma_0 \subseteq \Gamma$ e $\Gamma_1 \subseteq \Gamma$ e **LK**-derivações $\pi_0$ e $\pi_1$ de $\varphi, \Gamma_0 \Rightarrow$ e $\neg\varphi, \Gamma_1 \Rightarrow$, respectivamente. Podemos então derivar

$$\dfrac{\dfrac{\vdots\,\pi_0}{\varphi, \Gamma_0 \Rightarrow}}{\Gamma_0 \Rightarrow \neg\varphi}\,\neg\mathrm{R} \qquad \dfrac{\vdots\,\pi_1}{\neg\varphi, \Gamma_1 \Rightarrow}}{\Gamma_0, \Gamma_1 \Rightarrow}\,\mathrm{Cut}$$

Como $\Gamma_0 \subseteq \Gamma$ e $\Gamma_1 \subseteq \Gamma$, $\Gamma_0 \cup \Gamma_1 \subseteq \Gamma$. Portanto, $\Gamma$ é inconsistente. □

## 9.8 Derivabilidade e os Conectivos Proposicionais

Estabelecemos que a relação de derivabilidade $\vdash$ do cálculo de sequentes é forte o suficiente para estabelecer alguns fatos básicos envolvendo os conectivos proposicionais, tais como $\varphi \wedge \psi \vdash \varphi$ e $\varphi, \varphi \to \psi \vdash \psi$ (modus ponens). Esses fatos são necessários para a prova do teorema da completude.

**Proposição 9.21.** *1. Tanto $\varphi \wedge \psi \vdash \varphi$ quanto $\varphi \wedge \psi \vdash \psi$.*

*2. $\varphi, \psi \vdash \varphi \wedge \psi$.*

*Prova.* 1. Ambos os sequentes $\varphi \wedge \psi \Rightarrow \varphi$ e $\varphi \wedge \psi \Rightarrow \psi$ são deriváveis:

$$\dfrac{\varphi \Rightarrow \varphi}{\varphi \wedge \psi \Rightarrow \varphi}\,\wedge\mathrm{L} \qquad \dfrac{\psi \Rightarrow \psi}{\varphi \wedge \psi \Rightarrow \psi}\,\wedge\mathrm{L}$$

2. Eis a derivação do sequente $\varphi, \psi \Rightarrow \varphi \wedge \psi$:

$$\dfrac{\varphi \Rightarrow \varphi \qquad \psi \Rightarrow \psi}{\varphi, \psi \Rightarrow \varphi \wedge \psi}\,\wedge\mathrm{R}$$

□

**Proposição 9.22.** *1. $\varphi \vee \psi, \neg\varphi, \neg\psi$ é inconsistente.*

*2. Tanto $\varphi \vdash \varphi \vee \psi$ quanto $\psi \vdash \varphi \vee \psi$.*

*Prova.* 1. Damos a derivação do sequente $\varphi \vee \psi, \neg\varphi, \neg\psi \Rightarrow$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\varphi \Rightarrow \varphi}{\neg\varphi, \varphi \Rightarrow}\,\neg\mathrm{L}}{\varphi, \neg\varphi, \neg\psi \Rightarrow} \qquad \dfrac{\dfrac{\dfrac{\psi \Rightarrow \psi}{\neg\psi, \psi \Rightarrow}\,\neg\mathrm{L}}{\psi, \neg\varphi, \neg\psi \Rightarrow}}{\varphi \vee \psi, \neg\varphi, \neg\psi \Rightarrow}\,\vee\mathrm{L}$$

(Lembre-se de que linhas de inferência duplas indicam várias inferências de enfraquecimento, contração e troca.)

2. Ambos os sequentes $\varphi \Rightarrow \varphi \vee \psi$ e $\psi \Rightarrow \varphi \vee \psi$ têm derivações:

$$\dfrac{\varphi \Rightarrow \varphi}{\varphi \Rightarrow \varphi \vee \psi}\,\vee\mathrm{R} \qquad \dfrac{\psi \Rightarrow \psi}{\psi \Rightarrow \varphi \vee \psi}\,\vee\mathrm{R}$$ □

**Proposição 9.23.** *1. $\varphi, \varphi \to \psi \vdash \psi$.*

*2. Tanto $\neg\varphi \vdash \varphi \to \psi$ quanto $\psi \vdash \varphi \to \psi$.*

*Prova.* 1. O sequente $\varphi \to \psi, \varphi \Rightarrow \psi$ é derivável:

$$\dfrac{\varphi \Rightarrow \varphi \qquad \psi \Rightarrow \psi}{\varphi \to \psi, \varphi \Rightarrow \psi}\,\to\mathrm{L}$$

2. Ambos os sequentes $\neg\varphi \Rightarrow \varphi \to \psi$ e $\psi \Rightarrow \varphi \to \psi$ são deriváveis:

$$\dfrac{\dfrac{\dfrac{\dfrac{\varphi \Rightarrow \varphi}{\neg\varphi, \varphi \Rightarrow}\,\neg\mathrm{L}}{\varphi, \neg\varphi \Rightarrow}\,\mathrm{XL}}{\varphi, \neg\varphi \Rightarrow \psi}\,\mathrm{WR}}{\neg\varphi \Rightarrow \varphi \to \psi}\,\to\mathrm{R} \qquad \dfrac{\dfrac{\psi \Rightarrow \psi}{\varphi, \psi \Rightarrow \psi}\,\mathrm{WL}}{\psi \Rightarrow \varphi \to \psi}\,\to\mathrm{R}$$ □

## 9.9 Correção

Um sistema de derivação, tal como o cálculo de sequentes, é *correto* se não pode derivar coisas que de fato não valem. A correção é, assim, uma espécie de propriedade de segurança garantida para sistemas de derivação. Dependendo de qual propriedade da teoria da prova está em questão, gostaríamos de saber, por exemplo, que

1. todo $\varphi$ derivável é uma tautologia;

2. se a sentença é derivável de algumas outras, ela também é consequência delas;

3. se um conjunto de sentenças é inconsistente, ele é insatisfatível.

Essas são propriedades importantes de um sistema de derivação. Se alguma delas não vale, o sistema de derivação é deficiente—ele deriva demais. Consequentemente, estabelecer a correção de um sistema de derivação é da máxima importância.

Como todas essas propriedades da teoria da prova são definidas via derivabilidade no cálculo de sequentes de certos sequentes, provar (1)–(3) acima requer provar algo sobre as propriedades semânticas dos sequentes deriváveis. Primeiro definiremos o que significa um sequente ser *válido*, e então mostraremos que todo sequente derivável é válido. (1)–(3) seguem-se então como corolários desse resultado.

**Definição 9.24.** A valoração $\mathfrak{v}$ *satisfaz* um sequente $\Gamma \Rightarrow \Delta$ se, e somente se, ou $\mathfrak{v} \nvDash \varphi$ para algum $\varphi \in \Gamma$ ou $\mathfrak{v} \vDash \varphi$ para algum $\varphi \in \Delta$.

Um sequente é *válido* se, e somente se, toda valoração $\mathfrak{v}$ o satisfaz.

**Teorema 9.25 (Correção).** *Se* **LK** *deriva* $\Theta \Rightarrow \Xi$*, então* $\Theta \Rightarrow \Xi$ *é válido.*

*Prova.* Seja $\pi$ a derivação de $\Theta \Rightarrow \Xi$. Procedemos por indução sobre o número de inferências $n$ em $\pi$.

Se o número de inferências é 0, então $\pi$ consiste apenas em um sequente inicial. Todo sequente inicial $\varphi \Rightarrow \varphi$ é obviamente válido, pois para toda $\mathfrak{v}$, ou $\mathfrak{v} \nvDash \varphi$ ou $\mathfrak{v} \vDash \varphi$.

Se o número de inferências é maior que 0, distinguimos casos de acordo com o tipo da inferência mais inferior. Pela hipótese de indução, podemos supor que as premissas dessa inferência são válidas, já que o número de inferências na derivação de qualquer premissa é menor que $n$.

Primeiro, consideramos as inferências possíveis com apenas uma premissa.

1. A última inferência é um enfraquecimento. Então $\Theta \Rightarrow \Xi$ é $\varphi, \Gamma \Rightarrow \Delta$ (se a última inferência é WL) ou $\Gamma \Rightarrow \Delta, \varphi$ (se é WR), e a derivação termina em uma de

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta\end{array}}{\varphi, \Gamma \Rightarrow \Delta}\ \mathrm{WL} \qquad \dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta\end{array}}{\Gamma \Rightarrow \Delta, \varphi}\ \mathrm{WR}$$

   Pela hipótese de indução, $\Gamma \Rightarrow \Delta$ é válido, isto é, para toda valoração $\mathfrak{v}$, ou há algum $\chi \in \Gamma$ tal que $\mathfrak{v} \nvDash \chi$ ou há algum $\chi \in \Delta$ tal que $\mathfrak{v} \vDash \chi$.

Se $\mathfrak{v} \nvDash \chi$ para algum $\chi \in \Gamma$, então $\chi \in \Theta$ também, já que $\Theta = \varphi, \Gamma$, e assim $\mathfrak{v} \nvDash \chi$ para algum $\chi \in \Theta$. Analogamente, se $\mathfrak{v} \vDash \chi$ para algum $\chi \in \Delta$, como $\chi \in \Xi$, $\mathfrak{v} \vDash \chi$ para algum $\chi \in \Xi$. Consequentemente, $\Theta \Rightarrow \Xi$ é válido.

2. A última inferência é ¬L: Então a premissa da última inferência é $\Gamma \Rightarrow \Delta, \varphi$ e a conclusão é $\neg\varphi, \Gamma \Rightarrow \Delta$, isto é, a derivação termina em

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta, \varphi\end{array}}{\neg\varphi, \Gamma \Rightarrow \Delta}\ \neg\mathrm{L}$$

e $\Theta = \neg\varphi, \Gamma$ enquanto $\Xi = \Delta$.

A hipótese de indução nos diz que $\Gamma \Rightarrow \Delta, \varphi$ é válido, isto é, para toda $\mathfrak{v}$, ou (a) para algum $\chi \in \Gamma$, $\mathfrak{v} \nvDash \chi$, ou (b) para algum $\chi \in \Delta$, $\mathfrak{v} \vDash \chi$, ou (c) $\mathfrak{v} \vDash \varphi$. Queremos mostrar que $\Theta \Rightarrow \Xi$ também é válido. Seja $\mathfrak{v}$ a valoração. Se (a) vale, então há $\chi \in \Gamma$ tal que $\mathfrak{v} \nvDash \chi$, mas $\chi \in \Theta$ também. Se (b) vale, há $\chi \in \Delta$ tal que $\mathfrak{v} \vDash \chi$, mas $\chi \in \Xi$ também. Por fim, se $\mathfrak{v} \vDash \varphi$, então $\mathfrak{v} \nvDash \neg\varphi$. Como $\neg\varphi \in \Theta$, há $\chi \in \Theta$ tal que $\mathfrak{v} \nvDash \chi$. Consequentemente, $\Theta \Rightarrow \Xi$ é válido.

3. A última inferência é ¬R: Exercício.

4. A última inferência é ∧L: Há duas variantes: $\varphi \wedge \psi$ pode ser inferido à esquerda a partir de $\varphi$ ou de $\psi$ no lado esquerdo da premissa. No primeiro caso, $\pi$ termina em

$$\dfrac{\begin{array}{c}\vdots\\ \varphi, \Gamma \Rightarrow \Delta\end{array}}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}\ \wedge\mathrm{L}$$

e $\Theta = \varphi \wedge \psi, \Gamma$ enquanto $\Xi = \Delta$. Considere a valoração $\mathfrak{v}$. Como, pela hipótese de indução, $\varphi, \Gamma \Rightarrow \Delta$ é válido, (a) $\mathfrak{v} \nvDash \varphi$, (b) $\mathfrak{v} \nvDash \chi$ para algum $\chi \in \Gamma$, ou (c) $\mathfrak{v} \vDash \chi$ para algum $\chi \in \Delta$. No caso (a), $\mathfrak{v} \nvDash \varphi \wedge \psi$, então há $\chi \in \Theta$ (a saber, $\varphi \wedge \psi$) tal que $\mathfrak{v} \nvDash \chi$. No caso (b), há $\chi \in \Gamma$ tal que $\mathfrak{v} \nvDash \chi$, e $\chi \in \Theta$ também. No caso (c), há $\chi \in \Delta$ tal que $\mathfrak{v} \vDash \chi$, e $\chi \in \Xi$ também, já que $\Xi = \Delta$. Assim, em cada caso, $\mathfrak{v}$ satisfaz $\varphi \wedge \psi, \Gamma \Rightarrow \Delta$. Como $\mathfrak{v}$ era arbitrário, $\Gamma \Rightarrow \Delta$ é válido. O caso em que $\varphi \wedge \psi$ é inferido a partir de $\psi$ é tratado da mesma forma, mudando $\varphi$ para $\psi$.

5. A última inferência é ∨R: Há duas variantes: $\varphi \vee \psi$ pode ser inferido à direita a partir de $\varphi$ ou de $\psi$ no lado direito da premissa. No primeiro caso, $\pi$ termina em

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta, \varphi\end{array}}{\Gamma \Rightarrow \Delta, \varphi \vee \psi} \vee\mathrm{R}$$

Agora $\Theta = \Gamma$ e $\Xi = \Delta, \varphi \vee \psi$. Considere a valoração $\mathfrak{v}$. Como $\Gamma \Rightarrow \Delta, \varphi$ é válido, (a) $\mathfrak{v} \vDash \varphi$, (b) $\mathfrak{v} \nvDash \chi$ para algum $\chi \in \Gamma$, ou (c) $\mathfrak{v} \vDash \chi$ para algum $\chi \in \Delta$. No caso (a), $\mathfrak{v} \vDash \varphi \vee \psi$. No caso (b), há $\chi \in \Gamma$ tal que $\mathfrak{v} \nvDash \chi$. No caso (c), há $\chi \in \Delta$ tal que $\mathfrak{v} \vDash \chi$. Assim, em cada caso, $\mathfrak{v}$ satisfaz $\Gamma \Rightarrow \Delta, \varphi \vee \psi$, isto é, $\Theta \Rightarrow \Xi$. Como $\mathfrak{v}$ era arbitrário, $\Theta \Rightarrow \Xi$ é válido. O caso em que $\varphi \vee \psi$ é inferido a partir de $\psi$ é tratado da mesma forma, mudando $\varphi$ para $\psi$.

6. A última inferência é $\rightarrow$R: Então $\pi$ termina em

$$\dfrac{\begin{array}{c}\vdots\\ \varphi, \Gamma \Rightarrow \Delta, \psi\end{array}}{\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi} \rightarrow\mathrm{R}$$

Novamente, a hipótese de indução diz que a premissa é válida; queremos mostrar que a conclusão também é válida. Seja $\mathfrak{v}$ arbitrário. Como $\varphi, \Gamma \Rightarrow \Delta, \psi$ é válido, ao menos um dos seguintes casos ocorre: (a) $\mathfrak{v} \nvDash \varphi$, (b) $\mathfrak{v} \vDash \psi$, (c) $\mathfrak{v} \nvDash \chi$ para algum $\chi \in \Gamma$, ou (d) $\mathfrak{v} \vDash \chi$ para algum $\chi \in \Delta$. Nos casos (a) e (b), $\mathfrak{v} \vDash \varphi \rightarrow \psi$ e assim há um $\chi \in \Delta, \varphi \rightarrow \psi$ tal que $\mathfrak{v} \vDash \chi$. No caso (c), para algum $\chi \in \Gamma$, $\mathfrak{v} \nvDash \chi$. No caso (d), para algum $\chi \in \Delta$, $\mathfrak{v} \vDash \chi$. Em cada caso, $\mathfrak{v}$ satisfaz $\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi$. Como $\mathfrak{v}$ era arbitrário, $\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi$ é válido.

Agora consideremos as inferências possíveis com duas premissas.

1. A última inferência é um corte: então $\pi$ termina em

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta, \varphi\end{array} \qquad \begin{array}{c}\vdots\\ \varphi, \Pi \Rightarrow \Lambda\end{array}}{\Gamma, \Pi \Rightarrow \Delta, \Lambda} \mathrm{Cut}$$

Seja $\mathfrak{v}$ a valoração. Pela hipótese de indução, as premissas são válidas, então $\mathfrak{v}$ satisfaz ambas as premissas. Distinguimos dois casos: (a) $\mathfrak{v} \nvDash \varphi$ e (b) $\mathfrak{v} \vDash \varphi$. No caso (a), para que $\mathfrak{v}$ satisfaça a premissa esquerda, ela deve satisfazer $\Gamma \Rightarrow \Delta$. Mas então também satisfaz a conclusão. No caso (b), para que $\mathfrak{v}$ satisfaça a premissa direita, ela deve satisfazer $\Pi \setminus \Lambda$. Novamente, $\mathfrak{v}$ satisfaz a conclusão.

2. A última inferência é $\wedge$R. Então $\pi$ termina em

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ \Gamma \Rightarrow \Delta, \varphi & \Gamma \Rightarrow \Delta, \psi\end{array}}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi} \wedge\text{R}$$

   Considere a valoração $\mathfrak{v}$. Se $\mathfrak{v}$ satisfaz $\Gamma \Rightarrow \Delta$, terminamos. Então suponha que não. Como $\Gamma \Rightarrow \Delta, \varphi$ é válido pela hipótese de indução, $\mathfrak{v} \vDash \varphi$. Analogamente, como $\Gamma \Rightarrow \Delta, \psi$ é válido, $\mathfrak{v} \vDash \psi$. Mas então $\mathfrak{v} \vDash \varphi \wedge \psi$.

3. A última inferência é $\vee$L: Exercício.

4. A última inferência é $\rightarrow$L. Então $\pi$ termina em

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ \Gamma \Rightarrow \Delta, \varphi & \psi, \Pi \Rightarrow \Lambda\end{array}}{\varphi \rightarrow \psi, \Gamma, \Pi \Rightarrow \Delta, \Lambda} \rightarrow\text{L}$$

   Novamente, considere a valoração $\mathfrak{v}$ e suponha que $\mathfrak{v}$ não satisfaça $\Gamma, \Pi \Rightarrow \Delta, \Lambda$. Temos de mostrar que $\mathfrak{v} \nvDash \varphi \rightarrow \psi$. Se $\mathfrak{v}$ não satisfaz $\Gamma, \Pi \Rightarrow \Delta, \Lambda$, não satisfaz nem $\Gamma \Rightarrow \Delta$ nem $\Pi \Rightarrow \Lambda$. Como $\Gamma \Rightarrow \Delta, \varphi$ é válido, temos $\mathfrak{v} \vDash \varphi$. Como $\psi, \Pi \Rightarrow \Lambda$ é válido, temos $\mathfrak{v} \nvDash \psi$. Mas então $\mathfrak{v} \nvDash \varphi \rightarrow \psi$, que é o que queríamos mostrar. □

**Corolário 9.26.** *Se $\vdash \varphi$, então $\varphi$ é uma tautologia.*

**Corolário 9.27.** *Se $\Gamma \vdash \varphi$, então $\Gamma \vDash \varphi$.*

*Prova.* Se $\Gamma \vdash \varphi$, então, para algum subconjunto finito $\Gamma_0 \subseteq \Gamma$, há a derivação de $\Gamma_0 \Rightarrow \varphi$. Por Teorema 9.25, toda valoração $\mathfrak{v}$ ou torna algum $\psi \in \Gamma_0$ falso ou torna $\varphi$ verdadeiro. Logo, se $\mathfrak{v} \vDash \Gamma$, então também $\mathfrak{v} \vDash \varphi$. □

**Corolário 9.28.** *Se $\Gamma$ é satisfatível, então é consistente.*

*Prova.* Provamos a contrapositiva. Suponha que $\Gamma$ não seja consistente. Então há um $\Gamma_0 \subseteq \Gamma$ finito e a derivação de $\Gamma_0 \Rightarrow \quad$. Por Teorema 9.25, $\Gamma_0 \Rightarrow \quad$ é válido. Em outras palavras, para toda valoração $\mathfrak{v}$, há $\chi \in \Gamma_0$ tal que $\mathfrak{v} \nvDash \chi$, e como $\Gamma_0 \subseteq \Gamma$, esse $\chi$ também está em $\Gamma$. Assim, nenhuma $\mathfrak{v}$ satisfaz $\Gamma$, e $\Gamma$ não é satisfatível. □

## Problemas

**Problema 9.1.** Dê derivações dos seguintes sequentes:

1. $\varphi \wedge (\psi \wedge \chi) \Rightarrow (\varphi \wedge \psi) \wedge \chi$.
2. $\varphi \vee (\psi \vee \chi) \Rightarrow (\varphi \vee \psi) \vee \chi$.
3. $\varphi \to (\psi \to \chi) \Rightarrow \psi \to (\varphi \to \chi)$.
4. $\varphi \Rightarrow \neg\neg\varphi$.

**Problema 9.2.** Dê derivações dos seguintes sequentes:

1. $(\varphi \vee \psi) \to \chi \Rightarrow \varphi \to \chi$.
2. $(\varphi \to \chi) \wedge (\psi \to \chi) \Rightarrow (\varphi \vee \psi) \to \chi$.
3. $\Rightarrow \neg(\varphi \wedge \neg\varphi)$.
4. $\psi \to \varphi \Rightarrow \neg\varphi \to \neg\psi$.
5. $\Rightarrow (\varphi \to \neg\varphi) \to \neg\varphi$.
6. $\Rightarrow \neg(\varphi \to \psi) \to \neg\psi$.
7. $\varphi \to \chi \Rightarrow \neg(\varphi \wedge \neg\chi)$.
8. $\varphi \wedge \neg\chi \Rightarrow \neg(\varphi \to \chi)$.
9. $\varphi \vee \psi, \neg\psi \Rightarrow \varphi$.
10. $\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)$.
11. $\Rightarrow (\neg\varphi \wedge \neg\psi) \to \neg(\varphi \vee \psi)$.
12. $\Rightarrow \neg(\varphi \vee \psi) \to (\neg\varphi \wedge \neg\psi)$.

**Problema 9.3.** Dê derivações dos seguintes sequentes:

1. $\neg(\varphi \to \psi) \Rightarrow \varphi$.
2. $\neg(\varphi \wedge \psi) \Rightarrow \neg\varphi \vee \neg\psi$.
3. $\varphi \to \psi \Rightarrow \neg\varphi \vee \psi$.
4. $\Rightarrow \neg\neg\varphi \to \varphi$.
5. $\varphi \to \psi, \neg\varphi \to \psi \Rightarrow \psi$.
6. $(\varphi \wedge \psi) \to \chi \Rightarrow (\varphi \to \chi) \vee (\psi \to \chi)$.
7. $(\varphi \to \psi) \to \varphi \Rightarrow \varphi$.

8. $\Rightarrow (\varphi \to \psi) \vee (\psi \to \chi)$.

(Todos esses requerem a regra CR.)

**Problema 9.4.** Prove Proposição 19.16

**Problema 9.5.** Prove que $\Gamma \vdash \neg\varphi$ se, e somente se, $\Gamma \cup \{\varphi\}$ é inconsistente.

**Problema 9.6.** Complete a prova de Teorema 9.25.

# Capítulo 10

# Dedução Natural

Este capítulo apresenta um sistema de dedução natural no estilo de Gentzen/Prawitz.

Para incluir ou excluir material relevante à dedução natural como sistema de prova, use a tag "prfND".

## 10.1 Regras e Derivações

Sistemas de dedução natural pretendem ser um paralelo próximo do raciocínio informal usado em provas matemáticas (daí serem, de certo modo, "naturais"). Provas em dedução natural começam com hipóteses. Em seguida, aplicam-se regras de inferência. As hipóteses são "descarregadas" pelas regras de inferência $\neg$Intro, $\rightarrow$Intro, e $\vee$Elim, e o rótulo da hipótese descarregada é colocado ao lado da inferência para maior clareza.

**Definição 10.1 (Hipótese).** Uma *hipótese* é qualquer sentença na posição mais alta de qualquer ramo.

Derivações em dedução natural são certas árvores de sentenças, em que as sentenças no topo são hipóteses e, se a sentença está abaixo de um, dois ou três outros sequentes, ela deve seguir corretamente por uma regra de inferência. As sentenças no topo da inferência são chamadas de *premissas* e a sentença abaixo, de *conclusão* da inferência. As regras vêm em pares, uma regra de introdução e uma de eliminação para cada operador lógico. Elas introduzem a operador lógico na conclusão ou removem a operador lógico de uma premissa da regra. Algumas das regras permitem que uma hipótese de certo tipo seja *descarregada*. Para indicar qual hipótese é descarregada por qual inferência, também atribuímos rótulos tanto à hipótese quanto à inferência. Isso é indicado escrevendo-se a hipótese como "$[\varphi]^n$."

É costume considerar regras para todos os operadores lógicos $\wedge$, $\vee$, $\rightarrow$, $\neg$ e $\bot$, mesmo que alguns deles sejam definidos.

## 10.2 Regras Proposicionais

**Regras para $\wedge$**

$$\frac{\varphi \qquad \psi}{\varphi \wedge \psi}\ \wedge\text{Intro} \qquad \frac{\varphi \wedge \psi}{\varphi}\ \wedge\text{Elim} \qquad \frac{\varphi \wedge \psi}{\psi}\ \wedge\text{Elim}$$

**Regras para $\vee$**

$$\frac{\varphi}{\varphi \vee \psi}\ \vee\text{Intro} \qquad \frac{\psi}{\varphi \vee \psi}\ \vee\text{Intro} \qquad {}^{n}\frac{\varphi \vee \psi \qquad \begin{array}{c}[\varphi]^{n}\\ \vdots\\ \chi\end{array} \qquad \begin{array}{c}[\psi]^{n}\\ \vdots\\ \chi\end{array}}{\chi}\ \vee\text{Elim}$$

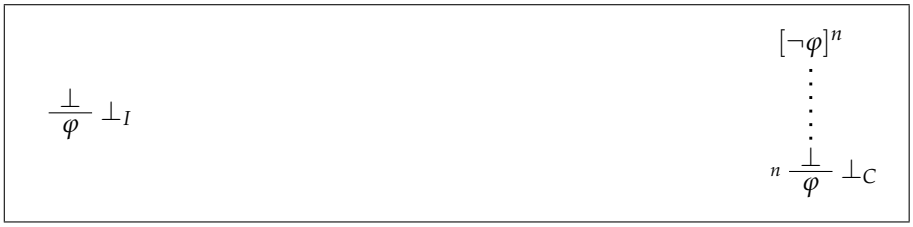
**Regras para $\rightarrow$**

$${}^{n}\frac{\begin{array}{c}[\varphi]^{n}\\ \vdots\\ \psi\end{array}}{\varphi \rightarrow \psi}\ \rightarrow\text{Intro} \qquad \frac{\varphi \rightarrow \psi \qquad \varphi}{\psi}\ \rightarrow\text{Elim}$$

**Regras para $\neg$**

$${}^{n}\frac{\begin{array}{c}[\varphi]^{n}\\ \vdots\\ \bot\end{array}}{\neg\varphi}\ \neg\text{Intro} \qquad \frac{\neg\varphi \qquad \varphi}{\bot}\ \neg\text{Elim}$$

**Regras para $\bot$**




Note que ¬Intro e $\bot_C$ são muito semelhantes: a diferença é que ¬Intro deriva uma sentença negada $\neg\varphi$, mas $\bot_C$, uma sentença positiva $\varphi$.

Sempre que uma regra indica que alguma hipótese pode ser descarregada, nós tomamos isso como uma permissão, mas não uma exigência. Por exemplo, na regra →Intro, podemos descarregar qualquer número de hipóteses da forma $\varphi$ na derivação da premissa $\psi$, inclusive zero.

## 10.3 Derivações

Já dissemos o que é uma hipótese e demos as regras de inferência. Derivações em dedução natural são geradas indutivamente a partir disso: cada derivação ou é uma hipótese por si só, ou consiste em uma, duas ou três derivações seguidas de uma inferência correta.

**Definição 10.2 (Derivação).** A *derivação* de a sentença $\varphi$ a partir de hipóteses $\Gamma$ é uma árvore finita de sentenças que satisfaz as seguintes condições:

1. As sentenças no topo da árvore ou estão em $\Gamma$ ou são descarregadas por uma inferência na árvore.

2. A sentença na base da árvore é $\varphi$.

3. Toda sentença na árvore exceto a sentença $\varphi$ na base é uma premissa de uma aplicação correta de uma regra de inferência cuja conclusão está diretamente abaixo daquela sentença na árvore.

Dizemos então que $\varphi$ é a *conclusão* da derivação e $\Gamma$, suas hipóteses não descarregadas.

Se existe a derivação de $\varphi$ a partir de $\Gamma$, dizemos que $\varphi$ é *derivável* a partir de $\Gamma$, ou, em símbolos: $\Gamma \vdash \varphi$. Se há a derivação de $\varphi$ em que toda hipótese é descarregada, escrevemos $\vdash \varphi$.

**Exemplo 10.3.** Toda hipótese por si só é a derivação. Assim, por exemplo, $\varphi$ por si só é a derivação, e $\psi$ por si só também. Podemos obter uma nova derivação a partir delas aplicando, digamos, a regra ∧Intro,

$$\frac{\varphi \qquad \psi}{\varphi \wedge \psi} \wedge\text{Intro}$$

Essas regras devem ser gerais: podemos substituir o $\varphi$ e $\psi$ nela por quaisquer sentenças, por exemplo, por $\chi$ e $\theta$. Então a conclusão seria $\chi \wedge \theta$, e assim

$$\frac{\chi \qquad \theta}{\chi \wedge \theta} \wedge\text{Intro}$$

é uma derivação correta. É claro que também podemos trocar as hipóteses, de modo que $\theta$ desempenhe o papel de $\varphi$ e $\chi$ o de $\psi$. Assim,

$$\frac{\theta \qquad \chi}{\theta \wedge \chi} \wedge\text{Intro}$$

também é uma derivação correta.

Podemos agora aplicar outra regra, digamos, $\rightarrow$Intro, que nos permite concluir um condicional e nos permite descarregar qualquer hipótese que seja idêntica ao antecedente desse condicional. Assim, ambas as seguintes seriam derivações corretas:

$$1\,\frac{\dfrac{[\chi]^1 \qquad \theta}{\chi \wedge \theta} \wedge\text{Intro}}{\chi \rightarrow (\chi \wedge \theta)} \rightarrow\text{Intro} \qquad 1\,\frac{\dfrac{\chi \qquad [\theta]^1}{\chi \wedge \theta} \wedge\text{Intro}}{\theta \rightarrow (\chi \wedge \theta)} \rightarrow\text{Intro}$$

Elas mostram, respectivamente, que $\theta \vdash \chi \rightarrow (\chi \wedge \theta)$ e $\chi \vdash \theta \rightarrow (\chi \wedge \theta)$.

Lembre-se de que descarregar hipóteses é uma permissão, não uma exigência: não temos de descarregar as hipóteses. Em particular, podemos aplicar uma regra mesmo que as hipóteses não estejam presentes na derivação. Por exemplo, o seguinte é válido, embora não haja hipótese $\varphi$ a ser descarregada:

$$1\,\frac{\psi}{\varphi \rightarrow \psi} \rightarrow\text{Intro}$$

## 10.4 Exemplos de Derivações

**Exemplo 10.4.** Vamos dar a derivação da sentença $(\varphi \wedge \psi) \rightarrow \varphi$.

Começamos escrevendo a conclusão desejada na parte inferior da derivação.

$$\frac{}{(\varphi \wedge \psi) \rightarrow \varphi}$$

Em seguida, precisamos descobrir que tipo de inferência poderia resultar em a sentença desta forma. O operador principal da conclusão é $\rightarrow$, então tentaremos chegar à conclusão usando a regra $\rightarrow$Intro. O melhor é anotar as suposições envolvidas e rotular as regras de inferência conforme avançamos, para que seja fácil ver se todas as suposições foram descarregadas ao final da prova.

$$\dfrac{\begin{array}{c}[\varphi \wedge \psi]^1 \\ \vdots \\ \varphi\end{array}}{(\varphi \wedge \psi) \to \varphi}\ {}^{1}\to\text{Intro}$$

Agora precisamos preencher os passos da suposição $\varphi \wedge \psi$ até $\varphi$. Como só temos um conectivo com o qual lidar, $\wedge$, devemos usar a regra $\wedge$ elim. Isso nos dá a seguinte prova:

$$\dfrac{\dfrac{[\varphi \wedge \psi]^1}{\varphi}\wedge\text{Elim}}{(\varphi \wedge \psi) \to \varphi}\ {}^{1}\to\text{Intro}$$

Agora temos uma derivação correta de $(\varphi \wedge \psi) \to \varphi$.

**Exemplo 10.5.** Agora vamos dar a derivação de $(\neg\varphi \vee \psi) \to (\varphi \to \psi)$.

Começamos escrevendo a conclusão desejada na parte inferior da derivação.

$$\dfrac{}{(\neg\varphi \vee \psi) \to (\varphi \to \psi)}$$

Para encontrar uma regra lógica que possa nos dar esta conclusão, observamos os conectivos lógicos na conclusão: $\neg$, $\vee$ e $\to$. Por enquanto, só nos interessa a primeira ocorrência de $\to$, porque é o operador principal da sentença na conclusão, enquanto $\neg$, $\vee$ e a segunda ocorrência de $\to$ estão dentro do escopo de outro conectivo, então cuidaremos deles depois. Começamos, portanto, com a regra $\to$Intro. Uma aplicação correta deve ser assim:

$$\dfrac{\begin{array}{c}[\neg\varphi \vee \psi]^1 \\ \vdots \\ \varphi \to \psi\end{array}}{(\neg\varphi \vee \psi) \to (\varphi \to \psi)}\ {}^{1}\to\text{Intro}$$

Isso nos deixa com duas possibilidades para continuar. Podemos continuar trabalhando de baixo para cima e procurar outra aplicação da regra $\to$Intro, ou podemos trabalhar de cima para baixo e aplicar a regra $\vee$Elim. Vamos adotar a segunda opção. Usaremos a suposição $\neg\varphi \vee \psi$ como a premissa mais à esquerda de $\vee$Elim. Para uma aplicação válida de $\vee$Elim, as outras duas premissas devem ser idênticas à conclusão $\varphi \to \psi$, mas cada uma pode ser derivada, por sua vez, de outra suposição, a saber, um dos dois disjuntos de $\neg\varphi \vee \psi$. Nossa derivação ficará, então, assim:

$$\dfrac{\dfrac{[\neg\varphi\vee\psi]^1 \qquad \begin{array}{c}[\neg\varphi]^2\\ \vdots\\ \varphi\to\psi\end{array} \qquad \begin{array}{c}[\psi]^2\\ \vdots\\ \varphi\to\psi\end{array}}{\varphi\to\psi}\,\vee\text{Elim}}{(\neg\varphi\vee\psi)\to(\varphi\to\psi)}\,\to\text{Intro}\;{}^{1}\;{}^{2}$$

Em cada um dos dois ramos à direita, queremos derivar $\varphi \to \psi$, o que é melhor feito usando →Intro.

$$\dfrac{\dfrac{[\neg\varphi\vee\psi]^1 \qquad \dfrac{\begin{array}{c}[\neg\varphi]^2,[\varphi]^3\\ \vdots\\ \psi\end{array}}{\varphi\to\psi}\,\to\text{Intro}\;{}^{3} \qquad \dfrac{\begin{array}{c}[\psi]^2,[\varphi]^4\\ \vdots\\ \psi\end{array}}{\varphi\to\psi}\,\to\text{Intro}\;{}^{4}}{\varphi\to\psi}\,\vee\text{Elim}}{(\neg\varphi\vee\psi)\to(\varphi\to\psi)}\,\to\text{Intro}\;{}^{1}\;{}^{2}$$

Nas duas partes que faltam na derivação, precisamos de derivações de $\psi$ a partir de $\neg\varphi$ e $\varphi$ no meio, e a partir de $\varphi$ e $\psi$ à esquerda. Comecemos pelo primeiro caso. $\neg\varphi$ e $\varphi$ são as duas premissas de ¬Elim:

$$\dfrac{\begin{array}{c}\dfrac{[\neg\varphi]^2 \qquad [\varphi]^3}{\bot}\,\neg\text{Elim}\\ \vdots\\ \psi\end{array}}{}$$

Usando $\bot_I$, podemos obter $\psi$ como conclusão e completar o ramo.

$$\dfrac{\dfrac{[\neg\varphi\vee\psi]^1 \qquad \dfrac{\dfrac{\dfrac{[\neg\varphi]^2 \qquad [\varphi]^3}{\bot}\,\bot\text{Intro}}{\psi}\,\bot_I}{\varphi\to\psi}\,\to\text{Intro}\;{}^{3} \qquad \dfrac{\begin{array}{c}[\psi]^2,[\varphi]^4\\ \vdots\\ \psi\end{array}}{\varphi\to\psi}\,\to\text{Intro}\;{}^{4}}{\varphi\to\psi}\,\vee\text{Elim}}{(\neg\varphi\vee\psi)\to(\varphi\to\psi)}\,\to\text{Intro}\;{}^{1}\;{}^{2}$$

Vejamos agora o ramo mais à direita. Aqui é importante perceber que a definição de derivação *permite que hipóteses sejam descarregadas* mas *não exige* que o sejam. Em outras palavras, se pudermos derivar $\psi$ a partir de uma das suposições $\varphi$ e $\psi$ sem usar a outra, tudo bem. E para derivar $\psi$ a partir de $\psi$ é trivial: $\psi$ por si só é tal a derivação, e nenhuma inferência é necessária. Portanto, podemos simplesmente eliminar a suposição $\varphi$.

$$\dfrac{\dfrac{\dfrac{[\neg\varphi]^2 \qquad [\varphi]^3}{\bot}\,\neg\text{Elim}}{\psi}\,\bot_I}{\varphi \to \psi}\,{\scriptstyle 3}\,\to\text{Intro} \qquad \dfrac{[\psi]^2}{\varphi \to \psi}\,\to\text{Intro}}{\varphi \to \psi}\,{\scriptstyle 2}\,\vee\text{Elim}$$
$$\dfrac{\varphi \to \psi}{(\neg\varphi \vee \psi) \to (\varphi \to \psi)}\,{\scriptstyle 1}\,\to\text{Intro}$$

Observe que, na derivação concluída, a inferência $\to$Intro mais à direita na verdade não descarrega nenhuma hipótese.

**Exemplo 10.6.** Até agora não precisamos da regra $\bot_C$. Ela é especial porque nos permite descarregar uma hipótese que não é uma sub-fórmula da conclusão da regra. Está intimamente relacionada à regra $\bot_I$. Na verdade, a regra $\bot_I$ é um caso especial da regra $\bot_C$—existe uma lógica chamada "lógica intuicionista" na qual apenas $\bot_I$ é permitida. A regra $\bot_C$ é um último recurso quando nada mais funciona. Por exemplo, suponha que queiramos derivar $\varphi \vee \neg\varphi$. Nossa estratégia usual seria tentar derivar $\varphi \vee \neg\varphi$ usando $\vee$Intro. Mas isso exigiria derivar $\varphi$ ou $\neg\varphi$ a partir de nenhuma suposição, e isso não pode ser feito. $\bot_C$ ao resgate!

$$\dfrac{\begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1 \\ \vdots \\ \bot\end{array}}{\varphi \vee \neg\varphi}\,{\scriptstyle 1}\,\bot_C$$

Agora procuramos a derivação de $\bot$ a partir de $\neg(\varphi \vee \neg\varphi)$. Como $\bot$ é a conclusão de $\neg$Elim, podemos tentar isso:

$$\dfrac{\dfrac{\begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1 \\ \vdots \\ \neg\varphi\end{array} \qquad \begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1 \\ \vdots \\ \varphi\end{array}}{\bot}\,\neg\text{Elim}}{\varphi \vee \neg\varphi}\,{\scriptstyle 1}\,\bot_C$$

Nossa estratégia para encontrar a derivação de $\neg\varphi$ exige uma aplicação de $\neg$Intro:

$$\dfrac{\dfrac{\begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1, [\varphi]^2 \\ \vdots \\ \bot\end{array}}{\neg\varphi}\,{\scriptstyle 2}\,\neg\text{Intro} \qquad \begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1 \\ \vdots \\ \varphi\end{array}}{\bot}\,\neg\text{Elim}$$
$$\dfrac{\bot}{\varphi \vee \neg\varphi}\,{\scriptstyle 1}\,\bot_C$$

Aqui, podemos obter $\bot$ facilmente aplicando $\neg$Elim à suposição $\neg(\varphi \vee \neg\varphi)$ e a $\varphi \vee \neg\varphi$, que segue da nossa nova suposição $\varphi$ por $\vee$Intro:

$$\dfrac{\dfrac{[\neg(\varphi \vee \neg\varphi)]^1 \qquad \dfrac{[\varphi]^2}{\varphi \vee \neg\varphi}\vee\text{Intro}}{\bot}\neg\text{Elim}}{\dfrac{\bot}{\neg\varphi}\neg\text{Intro}^{2}} \qquad \begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1\\ \vdots\\ \varphi\end{array}}{\dfrac{\bot}{\varphi \vee \neg\varphi}\bot_C}\neg\text{Elim}^{1}$$

No lado direito usamos a mesma estratégia, exceto que obtemos $\varphi$ por $\bot_C$:

$$\dfrac{\dfrac{\dfrac{[\neg(\varphi \vee \neg\varphi)]^1 \qquad \dfrac{[\varphi]^2}{\varphi \vee \neg\varphi}\vee\text{Intro}}{\bot}\neg\text{Elim}}{\dfrac{\bot}{\neg\varphi}\neg\text{Intro}^{2}} \qquad \dfrac{\dfrac{[\neg(\varphi \vee \neg\varphi)]^1 \qquad \dfrac{[\neg\varphi]^3}{\varphi \vee \neg\varphi}\vee\text{Intro}}{\bot}\neg\text{Elim}}{\dfrac{\bot}{\varphi}\bot_C}\neg\text{Elim}^{3}}}{\dfrac{\bot}{\varphi \vee \neg\varphi}\bot_C}\neg\text{Elim}^{1}$$

## 10.5 Noções da Teoria da Prova

Esta seção reúne as definições da relação de demonstrabilidade e de consistência para a dedução natural.

Assim como definimos várias noções semânticas importantes (validade, consequência, satisfatibilidade), agora definimos noções *da Teoria da Prova* correspondentes. Elas não são definidas por apelo à satisfação de sentenças em estruturas, mas por apelo à derivabilidade ou não derivabilidade de certas sentenças a partir de outras. Foi uma descoberta importante que essas noções coincidem. Que coincidem é o conteúdo dos teoremas de *correção* e *completude*.

**Definição 10.7 (Teoremas).** Uma sentença $\varphi$ é um *teorema* se há uma derivação de $\varphi$ em dedução natural na qual todas as hipóteses são descarregadas. Escrevemos $\vdash \varphi$ se $\varphi$ é um teorema e $\nvdash \varphi$ se não o é.

**Definição 10.8 (Derivabilidade).** A sentença $\varphi$ é *derivável de* um conjunto de sentenças $\Gamma$, $\Gamma \vdash \varphi$, se há uma derivação com conclusão $\varphi$ e na qual toda hipótese é ou descarregada ou está em $\Gamma$. Se $\varphi$ não é derivável de $\Gamma$, escrevemos $\Gamma \nvdash \varphi$.

**Definição 10.9 (Consistência).** Um conjunto de sentenças $\Gamma$ é *inconsistente* se, e somente se, $\Gamma \vdash \bot$. Se $\Gamma$ não é inconsistente, isto é, se $\Gamma \nvdash \bot$, dizemos que é *consistente*.

**Proposição 10.10 (Reflexividade).** *Se $\varphi \in \Gamma$, então $\Gamma \vdash \varphi$.*

*Prova.* A hipótese $\varphi$ por si só é uma derivação de $\varphi$ em que toda hipótese não descarregada (isto é, $\varphi$) está em $\Gamma$. □

**Proposição 10.11 (Monotonicidade).** *Se $\Gamma \subseteq \Delta$ e $\Gamma \vdash \varphi$, então $\Delta \vdash \varphi$.*

*Prova.* Qualquer derivação de $\varphi$ a partir de $\Gamma$ é também uma derivação de $\varphi$ a partir de $\Delta$. □

**Proposição 10.12 (Transitividade).** *Se $\Gamma \vdash \varphi$ e $\{\varphi\} \cup \Delta \vdash \psi$, então $\Gamma \cup \Delta \vdash \psi$.*

*Prova.* Se $\Gamma \vdash \varphi$, há uma derivação $\delta_0$ de $\varphi$ com todas as hipóteses não descarregadas em $\Gamma$. Se $\{\varphi\} \cup \Delta \vdash \psi$, então há uma derivação $\delta_1$ de $\psi$ com todas as hipóteses não descarregadas em $\{\varphi\} \cup \Delta$. Considere agora:

$$\dfrac{\dfrac{\begin{array}{c}\Delta, [\varphi]^1 \\ \vdots\,\delta_1 \\ \psi\end{array}}{1\ \varphi \to \psi}\ {\to}\text{Intro} \qquad \begin{array}{c}\Gamma \\ \vdots\,\delta_0 \\ \varphi\end{array}}{\psi}\ {\to}\text{Elim}$$

As hipóteses não descarregadas estão agora todas entre $\Gamma \cup \Delta$, de modo que isto mostra $\Gamma \cup \Delta \vdash \psi$. □

Quando $\Gamma = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$ é um conjunto finito, podemos usar a notação simplificada $\varphi_1, \varphi_2, \ldots, \varphi_k \vdash \psi$ para $\Gamma \vdash \psi$; em particular, $\varphi \vdash \psi$ significa que $\{\varphi\} \vdash \psi$.

Note que se $\Gamma \vdash \varphi$ e $\varphi \vdash \psi$, então $\Gamma \vdash \psi$. Segue também que se $\varphi_1, \ldots, \varphi_n \vdash \psi$ e $\Gamma \vdash \varphi_i$ para cada $i$, então $\Gamma \vdash \psi$.

**Proposição 10.13.** *As seguintes afirmações são equivalentes.*

1. *$\Gamma$ é inconsistente.*
2. *$\Gamma \vdash \varphi$ para toda sentença $\varphi$.*
3. *$\Gamma \vdash \varphi$ e $\Gamma \vdash \neg\varphi$ para alguma sentença $\varphi$.*

*Prova.* Exercício. □

**Proposição 10.14 (Compacidade).**
1. *Se $\Gamma \vdash \varphi$, então há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ tal que $\Gamma_0 \vdash \varphi$.*
2. *Se todo subconjunto finito de $\Gamma$ é consistente, então $\Gamma$ é consistente.*

*Prova.* 1. Se $\Gamma \vdash \varphi$, então há uma derivação $\delta$ de $\varphi$ a partir de $\Gamma$. Seja $\Gamma_0$ o conjunto de hipóteses não descarregadas de $\delta$. Como toda derivação é finita, $\Gamma_0$ só pode conter finitamente muitas sentenças. Assim, $\delta$ é uma derivação de $\varphi$ a partir de um $\Gamma_0$ finito $\subseteq \Gamma$.

2. Isto é a contrapositiva de (1) no caso especial $\varphi \equiv \bot$. □

## 10.6 Derivabilidade e Consistência

Estabeleceremos agora várias propriedades da relação de derivabilidade. Elas são independentemente interessantes, mas cada uma desempenhará um papel na prova do teorema da completude.

**Proposição 10.15.** *Se $\Gamma \vdash \varphi$ e $\Gamma \cup \{\varphi\}$ é inconsistente, então $\Gamma$ é inconsistente.*

*Prova.* Seja a derivação de $\varphi$ a partir de $\Gamma$ igual a $\delta_1$ e a derivação de $\bot$ a partir de $\Gamma \cup \{\varphi\}$ igual a $\delta_2$. Podemos então derivar:

$$\dfrac{\dfrac{\begin{array}{c}\Gamma, [\varphi]^1 \\ \vdots\,\delta_2 \\ \bot\end{array}}{\neg\varphi}\,{}^1\neg\text{Intro} \qquad \begin{array}{c}\Gamma \\ \vdots\,\delta_1 \\ \varphi\end{array}}{\bot}\neg\text{Elim}$$

Na nova derivação, a hipótese $\varphi$ é descarregada, de modo que é uma derivação a partir de $\Gamma$. □

**Proposição 10.16.** *$\Gamma \vdash \varphi$ se, e somente se, $\Gamma \cup \{\neg\varphi\}$ é inconsistente.*

*Prova.* Primeiro suponha que $\Gamma \vdash \varphi$, isto é, há uma derivação $\delta_0$ de $\varphi$ a partir de hipóteses não descarregadas $\Gamma$. Obtemos uma derivação de $\bot$ a partir de $\Gamma \cup \{\neg\varphi\}$ da seguinte forma:

$$\dfrac{\neg\varphi \qquad \begin{array}{c}\Gamma \\ \vdots\,\delta_0 \\ \varphi\end{array}}{\bot}\neg\text{Elim}$$

Agora suponha que $\Gamma \cup \{\neg\varphi\}$ é inconsistente, e seja $\delta_1$ a derivação correspondente de $\bot$ a partir de hipóteses não descarregadas em $\Gamma \cup \{\neg\varphi\}$. Obtemos uma derivação de $\varphi$ apenas a partir de $\Gamma$ usando $\bot_C$:

$$\dfrac{\dfrac{\Gamma, [\neg\varphi]^1}{\vdots\,\delta_1}}{\varphi}\,{}_1\,\bot_C$$

□

**Proposição 10.17.** *Se $\Gamma \vdash \varphi$ e $\neg\varphi \in \Gamma$, então $\Gamma$ é inconsistente.*

*Prova.* Suponha que $\Gamma \vdash \varphi$ e $\neg\varphi \in \Gamma$. Então há uma derivação $\delta$ de $\varphi$ a partir de $\Gamma$. Considere esta aplicação simples da regra ¬Elim:

$$\dfrac{\neg\varphi \qquad \begin{array}{c}\Gamma\\ \vdots\,\delta\\ \varphi\end{array}}{\bot}\,\neg\text{Elim}$$

Como $\neg\varphi \in \Gamma$, todas as hipóteses não descarregadas estão em $\Gamma$; isto mostra que $\Gamma \vdash \bot$. □

**Proposição 10.18.** *Se $\Gamma \cup \{\varphi\}$ e $\Gamma \cup \{\neg\varphi\}$ são ambos inconsistentes, então $\Gamma$ é inconsistente.*

*Prova.* Há derivações $\delta_1$ e $\delta_2$ de $\bot$ a partir de $\Gamma \cup \{\varphi\}$ e de $\bot$ a partir de $\Gamma \cup \{\neg\varphi\}$, respectivamente. Podemos então derivar

$$\dfrac{\dfrac{\dfrac{\Gamma, [\neg\varphi]^2}{\vdots\,\delta_2}}{\bot}}{\neg\neg\varphi}\,{}_2\,\neg\text{Intro} \qquad \dfrac{\dfrac{\dfrac{\Gamma, [\varphi]^1}{\vdots\,\delta_1}}{\bot}}{\neg\varphi}\,{}_1\,\neg\text{Intro}}{\bot}\,\neg\text{Elim}$$

Como as hipóteses $\varphi$ e $\neg\varphi$ são descarregadas, isto é uma derivação de $\bot$ apenas a partir de $\Gamma$. Logo $\Gamma$ é inconsistente. □

## 10.7 Derivabilidade e os Conectivos Proposicionais

Estabelecemos que a relação de derivabilidade $\vdash$ da dedução natural é forte o suficiente para estabelecer alguns fatos básicos envolvendo os conectivos proposicionais, tais como $\varphi \wedge \psi \vdash \varphi$ e $\varphi, \varphi \to \psi \vdash \psi$ (modus ponens). Esses fatos são necessários para a prova do teorema da completude.

**Proposição 10.19.** 1. *Tanto $\varphi \wedge \psi \vdash \varphi$ quanto $\varphi \wedge \psi \vdash \psi$.*

2. *$\varphi, \psi \vdash \varphi \wedge \psi$.*

*Prova.* 1. Podemos derivar ambos:

$$\frac{\varphi \wedge \psi}{\varphi}\,\wedge\text{Elim} \qquad \frac{\varphi \wedge \psi}{\psi}\,\wedge\text{Elim}$$

2. Podemos derivar:

$$\frac{\varphi \qquad \psi}{\varphi \wedge \psi}\,\wedge\text{Intro}$$

□

**Proposição 10.20.** *1. $\varphi \vee \psi, \neg\varphi, \neg\psi$ é inconsistente.*

*2. Tanto $\varphi \vdash \varphi \vee \psi$ quanto $\psi \vdash \varphi \vee \psi$.*

*Prova.* 1. Considere a seguinte derivação:

$$\dfrac{\varphi \vee \psi \qquad \dfrac{\dfrac{\neg\varphi \qquad [\varphi]^1}{\bot}\,\neg\text{Elim} \qquad \dfrac{\neg\psi \qquad [\psi]^1}{\bot}\,\neg\text{Elim}}{\bot}\,\vee\text{Elim}}{\bot}\,1$$

Esta é a derivação de $\bot$ a partir das hipóteses não descarregadas $\varphi \vee \psi$, $\neg\varphi$ e $\neg\psi$.

2. Podemos derivar ambos:

$$\frac{\varphi}{\varphi \vee \psi}\,\vee\text{Intro} \qquad \frac{\psi}{\varphi \vee \psi}\,\vee\text{Intro}$$

□

**Proposição 10.21.** *1. $\varphi, \varphi \to \psi \vdash \psi$.*

*2. Tanto $\neg\varphi \vdash \varphi \to \psi$ quanto $\psi \vdash \varphi \to \psi$.*

*Prova.* 1. Podemos derivar:

$$\frac{\varphi \to \psi \qquad \varphi}{\psi}\,\to\text{Elim}$$

2. Isso é mostrado pelas duas derivações seguintes:

$$\dfrac{\dfrac{\dfrac{\neg\varphi \qquad [\varphi]^1}{\bot}\,\neg\text{Elim}}{\psi}\,\bot_I}{\varphi \to \psi}\,\to\text{Intro}\,1 \qquad \frac{\psi}{\varphi \to \psi}\,\to\text{Intro}$$

Note que $\to$Intro pode, mas não precisa, descarregar a hipótese $\varphi$. □

## 10.8 Correção

Um sistema de derivação, como a dedução natural, é *correto* se não pode derivar coisas que de fato não seguem. A correção é assim uma espécie de propriedade de segurança garantida para sistemas de derivação. Dependendo de qual propriedade da Teoria da Prova está em questão, gostaríamos de saber, por exemplo, que

1. toda sentença derivável é uma tautologia;

2. se uma sentença é derivável a partir de outras, ela também é uma consequência delas;

3. se um conjunto de sentenças é inconsistente, ele é insatisfatível.

Estas são propriedades importantes de um sistema de derivação. Se alguma delas não vale, o sistema de derivação é deficiente—ele deriva demais. Consequentemente, estabelecer a correção de um sistema de derivação é da maior importância.

**Teorema 10.22 (Correção).** *Se $\varphi$ é derivável a partir das hipóteses não descarregadas $\Gamma$, então $\Gamma \vDash \varphi$.*

*Prova.* Seja $\delta$ uma derivação de $\varphi$. Procedemos por indução no número de inferências em $\delta$.

Para a base da indução, mostramos a afirmação quando o número de inferências é 0. Neste caso, $\delta$ consiste apenas de uma única sentença $\varphi$, isto é, uma hipótese. Essa hipótese é não descarregada, pois hipóteses só podem ser descarregadas por inferências, e não há inferências. Assim, qualquer valoração $\mathfrak{v}$ que satisfaz todas as hipóteses não descarregadas da prova também satisfaz $\varphi$.

Agora o passo indutivo. Suponha que $\delta$ contém $n$ inferências. A(s) premissa(s) da inferência mais baixa são derivadas usando sub-derivações, cada uma das quais contém menos de $n$ inferências. Assumimos a hipótese de indução: as premissas da inferência mais baixa seguem das hipóteses não descarregadas das sub-derivações que terminam nessas premissas. Temos que mostrar que a conclusão $\varphi$ segue das hipóteses não descarregadas de toda a prova.

Distinguimos casos de acordo com o tipo da inferência mais baixa. Primeiro, consideramos as possíveis inferências com apenas uma premissa.

1. Suponha que a última inferência é ¬Intro: a derivação tem a forma

$$\dfrac{\begin{array}{c}\Gamma, [\varphi]^n \\ \vdots\,\delta_1 \\ \bot\end{array}}{\neg\varphi}\,{}^{n}\,\neg\text{Intro}$$

Pela hipótese de indução, $\bot$ segue das hipóteses não descarregadas $\Gamma \cup \{\varphi\}$ de $\delta_1$. Considere a valoração $\mathfrak{v}$. Precisamos mostrar que, se $\mathfrak{v} \vDash \Gamma$, então $\mathfrak{v} \vDash \neg\varphi$. Suponha por redução ao absurdo que $\mathfrak{v} \vDash \Gamma$, mas $\mathfrak{v} \nvDash \neg\varphi$, isto é, $\mathfrak{v} \vDash \varphi$. Isto significaria que $\mathfrak{v} \vDash \Gamma \cup \{\varphi\}$. Isto é contrário à nossa hipótese de indução. Logo, $\mathfrak{v} \vDash \neg\varphi$.

2. A última inferência é $\wedge$Elim: há duas variantes: $\varphi$ ou $\psi$ pode ser inferido da premissa $\varphi \wedge \psi$. Considere o primeiro caso. A derivação $\delta$ tem este aspecto:

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots\,\delta_1 \\ \varphi \wedge \psi\end{array}}{\varphi}\,\wedge\text{Elim}$$

Pela hipótese de indução, $\varphi \wedge \psi$ segue das hipóteses não descarregadas $\Gamma$ de $\delta_1$. Considere a estrutura $\mathfrak{v}$. Precisamos mostrar que, se $\mathfrak{v} \vDash \Gamma$, então $\mathfrak{v} \vDash \varphi$. Suponha $\mathfrak{v} \vDash \Gamma$. Pela nossa hipótese de indução ($\Gamma \vDash \varphi \wedge \psi$), sabemos que $\mathfrak{v} \vDash \varphi \wedge \psi$. Por definição, $\mathfrak{v} \vDash \varphi \wedge \psi$ se, e somente se, $\mathfrak{v} \vDash \varphi$ e $\mathfrak{v} \vDash \psi$. (O caso em que $\psi$ é inferido de $\varphi \wedge \psi$ é tratado de forma similar.)

3. A última inferência é $\vee$Intro: há duas variantes: $\varphi \vee \psi$ pode ser inferido da premissa $\varphi$ ou da premissa $\psi$. Considere o primeiro caso. A derivação tem a forma

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots\,\delta_1 \\ \varphi\end{array}}{\varphi \vee \psi}\,\vee\text{Intro}$$

Pela hipótese de indução, $\varphi$ segue das hipóteses não descarregadas $\Gamma$ de $\delta_1$. Considere a valoração $\mathfrak{v}$. Precisamos mostrar que, se $\mathfrak{v} \vDash \Gamma$, então $\mathfrak{v} \vDash \varphi \vee \psi$. Suponha $\mathfrak{v} \vDash \Gamma$; então $\mathfrak{v} \vDash \varphi$, pois $\Gamma \vDash \varphi$ (a hipótese de indução). Logo também deve ser o caso que $\mathfrak{v} \vDash \varphi \vee \psi$. (O caso em que $\varphi \vee \psi$ é inferido de $\psi$ é tratado de forma similar.)

4. A última inferência é $\rightarrow$Intro: $\varphi \rightarrow \psi$ é inferido de uma subprova com hipótese $\varphi$ e conclusão $\psi$, isto é,

$$\dfrac{\begin{array}{c}\Gamma, [\varphi]^n \\ \vdots\,\delta_1 \\ \psi\end{array}}{\varphi \to \psi}\ {}^{n}\!\to\text{Intro}$$

Pela hipótese de indução, $\psi$ segue das hipóteses não descarregadas de $\delta_1$, isto é, $\Gamma \cup \{\varphi\} \vDash \psi$. Considere a valoração $\mathfrak{v}$. As hipóteses não descarregadas de $\delta$ são apenas $\Gamma$, pois $\varphi$ é descartada na última inferência. Precisamos mostrar que $\Gamma \vDash \varphi \to \psi$. Por redução ao absurdo, suponha que para alguma valoração $\mathfrak{v}$, $\mathfrak{v} \vDash \Gamma$ mas $\mathfrak{v} \nvDash \varphi \to \psi$. Assim, $\mathfrak{v} \vDash \varphi$ e $\mathfrak{v} \nvDash \psi$. Mas por hipótese, $\psi$ é uma consequência de $\Gamma \cup \{\varphi\}$, isto é, $\mathfrak{v} \vDash \psi$, o que é uma contradição. Logo, $\Gamma \vDash \varphi \to \psi$.

5. A última inferência é $\bot_I$: aqui, $\delta$ termina em

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots\,\delta_1 \\ \bot\end{array}}{\varphi}\ \bot_I$$

Pela hipótese de indução, $\Gamma \vDash \bot$. Temos que mostrar que $\Gamma \vDash \varphi$. Suponha o contrário; então para algum $\mathfrak{v}$ temos $\mathfrak{v} \vDash \Gamma$ e $\mathfrak{v} \nvDash \varphi$. Mas sempre temos $\mathfrak{v} \nvDash \bot$, de modo que isto significaria que $\Gamma \nvDash \bot$, contrariando a hipótese de indução.

6. A última inferência é $\bot_C$: Exercício.

Agora consideremos as possíveis inferências com várias premissas: $\vee$Elim, $\wedge$Intro, e $\to$Elim.

1. A última inferência é $\wedge$Intro. $\varphi \wedge \psi$ é inferido das premissas $\varphi$ e $\psi$ e $\delta$ tem a forma

$$\dfrac{\begin{array}{cc}\Gamma_1 & \Gamma_2 \\ \vdots\,\delta_1 & \vdots\,\delta_2 \\ \varphi & \psi\end{array}}{\varphi \wedge \psi}\ \wedge\text{Intro}$$

Pela hipótese de indução, $\varphi$ segue das hipóteses não descarregadas $\Gamma_1$ de $\delta_1$ e $\psi$ segue das hipóteses não descarregadas $\Gamma_2$ de $\delta_2$. As hipóteses não descarregadas de $\delta$ são $\Gamma_1 \cup \Gamma_2$, de modo que temos que mostrar que $\Gamma_1 \cup \Gamma_2 \vDash \varphi \wedge \psi$. Considere a valoração $\mathfrak{v}$ com $\mathfrak{v} \vDash \Gamma_1 \cup \Gamma_2$. Como $\mathfrak{v} \vDash \Gamma_1$,

deve ser o caso que $\mathfrak{v} \vDash \varphi$, pois $\Gamma_1 \vDash \varphi$, e como $\mathfrak{v} \vDash \Gamma_2$, $\mathfrak{v} \vDash \psi$, pois $\Gamma_2 \vDash \psi$. Juntas, $\mathfrak{v} \vDash \varphi \wedge \psi$.

2. A última inferência é $\vee$Elim: Exercício.

3. A última inferência é $\rightarrow$Elim. $\psi$ é inferido das premissas $\varphi \rightarrow \psi$ e $\varphi$. A derivação $\delta$ tem este aspecto:

$$\dfrac{\begin{array}{cc} \Gamma_1 & \Gamma_2 \\ \vdots & \vdots \\ \delta_1 & \delta_2 \\ \vdots & \vdots \\ \varphi \rightarrow \psi & \varphi \end{array}}{\psi} \rightarrow\text{Elim}$$

Pela hipótese de indução, $\varphi \rightarrow \psi$ segue das hipóteses não descarregadas $\Gamma_1$ de $\delta_1$ e $\varphi$ segue das hipóteses não descarregadas $\Gamma_2$ de $\delta_2$. Considere a valoração $\mathfrak{v}$. Precisamos mostrar que, se $\mathfrak{v} \vDash \Gamma_1 \cup \Gamma_2$, então $\mathfrak{v} \vDash \psi$. Suponha $\mathfrak{v} \vDash \Gamma_1 \cup \Gamma_2$. Como $\Gamma_1 \vDash \varphi \rightarrow \psi$, $\mathfrak{v} \vDash \varphi \rightarrow \psi$. Como $\Gamma_2 \vDash \varphi$, temos $\mathfrak{v} \vDash \varphi$. Isto significa que $\mathfrak{v} \vDash \psi$ (pois se $\mathfrak{v} \nvDash \psi$, como $\mathfrak{v} \vDash \varphi$, teríamos $\mathfrak{v} \nvDash \varphi \rightarrow \psi$, contradizendo $\mathfrak{v} \vDash \varphi \rightarrow \psi$).

4. A última inferência é $\neg$Elim: Exercício.

□

**Corolário 10.23.** *Se $\vdash \varphi$, então $\varphi$ é uma tautologia.*

**Corolário 10.24.** *Se $\Gamma$ é satisfatível, então é consistente.*

*Prova.* Provamos a contrapositiva. Suponha que $\Gamma$ não é consistente. Então $\Gamma \vdash \bot$, isto é, há uma derivação de $\bot$ a partir de hipóteses não descarregadas em $\Gamma$. Por Teorema 10.22, qualquer valoração $\mathfrak{v}$ que satisfaz $\Gamma$ deve satisfazer $\bot$. Como $\mathfrak{v} \nvDash \bot$ para toda valoração $\mathfrak{v}$, nenhuma $\mathfrak{v}$ pode satisfazer $\Gamma$, isto é, $\Gamma$ não é satisfatível. □

## Problemas

**Problema 10.1.** Dê derivações que mostrem o seguinte:

1. $\varphi \wedge (\psi \wedge \chi) \vdash (\varphi \wedge \psi) \wedge \chi$.
2. $\varphi \vee (\psi \vee \chi) \vdash (\varphi \vee \psi) \vee \chi$.
3. $\varphi \rightarrow (\psi \rightarrow \chi) \vdash \psi \rightarrow (\varphi \rightarrow \chi)$.
4. $\varphi \vdash \neg\neg\varphi$.

**Problema 10.2.** Dê derivações que mostrem o seguinte:

1. $(\varphi \vee \psi) \to \chi \vdash \varphi \to \chi$.
2. $(\varphi \to \chi) \wedge (\psi \to \chi) \vdash (\varphi \vee \psi) \to \chi$.
3. $\vdash \neg(\varphi \wedge \neg\varphi)$.
4. $\psi \to \varphi \vdash \neg\varphi \to \neg\psi$.
5. $\vdash (\varphi \to \neg\varphi) \to \neg\varphi$.
6. $\vdash \neg(\varphi \to \psi) \to \neg\psi$.
7. $\varphi \to \chi \vdash \neg(\varphi \wedge \neg\chi)$.
8. $\varphi \wedge \neg\chi \vdash \neg(\varphi \to \chi)$.
9. $\varphi \vee \psi, \neg\psi \vdash \varphi$.
10. $\neg\varphi \vee \neg\psi \vdash \neg(\varphi \wedge \psi)$.
11. $\vdash (\neg\varphi \wedge \neg\psi) \to \neg(\varphi \vee \psi)$.
12. $\vdash \neg(\varphi \vee \psi) \to (\neg\varphi \wedge \neg\psi)$.

**Problema 10.3.** Dê derivações que mostrem o seguinte:

1. $\neg(\varphi \to \psi) \vdash \varphi$.
2. $\neg(\varphi \wedge \psi) \vdash \neg\varphi \vee \neg\psi$.
3. $\varphi \to \psi \vdash \neg\varphi \vee \psi$.
4. $\vdash \neg\neg\varphi \to \varphi$.
5. $\varphi \to \psi, \neg\varphi \to \psi \vdash \psi$.
6. $(\varphi \wedge \psi) \to \chi \vdash (\varphi \to \chi) \vee (\psi \to \chi)$.
7. $(\varphi \to \psi) \to \varphi \vdash \varphi$.
8. $\vdash (\varphi \to \psi) \vee (\psi \to \chi)$.

(Todos exigem a regra $\bot_C$ .)

**Problema 10.4.** Prove Proposição 10.13

**Problema 10.5.** Prove que $\Gamma \vdash \neg\varphi$ se, e somente se, $\Gamma \cup \{\varphi\}$ é inconsistente.

**Problema 10.6.** Complete a prova de Teorema 10.22.

# Capítulo 11

# Tableaux

This chapter presents a signed analytic tableaux system.
To include or exclude material relevant to natural deduction as a proof system, use the “prfTab” tag.

# Capítulo 12

# Axiomatic Derivações

No effort has been made yet to ensure that the material in this chapter respects various tags indicating which connectives and quantifiers are primitive or defined: all are assumed to be primitive, except $\leftrightarrow$ which is assumed to be defined. If the FOL tag is true, we produce a version with quantifiers, otherwise without.

# Capítulo 13

# O Teorema da Completude

## 13.1 Introdução

O teorema da completude é um dos resultados mais fundamentais sobre lógica. Ele vem em duas formulações, cuja equivalência iremos provar. Em sua primeira formulação, ele diz algo fundamental sobre a relação entre consequência semântica e nosso sistema de derivação: se a sentença $\varphi$ segue de algumas sentenças $\Gamma$, então também existe a derivação que estabelece $\Gamma \vdash \varphi$. Assim, o sistema de derivação é tão forte quanto pode possivelmente ser sem provar coisas que de fato não se seguem.

Em sua segunda formulação, ele pode ser enunciado como um resultado de existência de modelo: todo conjunto consistente de sentenças é satisfatível. A consistência é uma noção da teoria da prova: ela diz que nosso sistema de derivação é incapaz de produzir certas derivações. Mas quem garante que, só porque não há derivações de um certo tipo a partir de $\Gamma$, está garantido que existe valoração $\mathfrak{v}$ com $\mathfrak{v} \vDash \Gamma$? Antes de o teorema da completude ser provado pela primeira vez — na verdade, antes de termos os sistemas de derivação que temos hoje — o grande matemático alemão David Hilbert defendia a visão de que a consistência das teorias matemáticas garante a existência dos objetos de que elas tratam. Ele colocou isso da seguinte forma em uma carta a Gottlob Frege:

> Se os axiomas dados arbitrariamente não se contradizem uns aos outros com todas as suas consequências, então eles são verdadeiros e as coisas definidas pelos axiomas existem. Este é para mim o critério de verdade e existência.

Frege discordou veementemente. A segunda formulação do teorema da completude mostra que Hilbert estava certo pelo menos no sentido de que, se os axiomas são consistentes, então existe *alguma* valoração que os torna todos verdadeiros.

Estas não são as únicas razões pelas quais o teorema da completude — ou melhor, sua prova — é importante. Ele tem uma série de consequências importantes, algumas das quais discutiremos separadamente. Por exemplo, como toda derivação que mostra $\Gamma \vdash \varphi$ é finita e, portanto, só pode usar uma quantidade finita das sentenças em $\Gamma$, segue do teorema da completude que, se $\varphi$ é uma consequência de $\Gamma$, então já é uma consequência de um subconjunto finito de $\Gamma$. Isso é chamado de *compacidade*. Equivalentemente, se todo subconjunto finito de $\Gamma$ é consistente, então o próprio $\Gamma$ deve ser consistente.

Embora o teorema da compacidade decorra do teorema da completude pelo desvio através de derivações, também é possível usar a *prova do* teorema da completude para estabelecê-lo diretamente. Pois o que a prova faz é tomar um conjunto de sentenças com uma certa propriedade — a consistência — e construir a estrutura a partir desse conjunto que possui certas propriedades (neste caso, que ela satisfaz o conjunto). Quase exatamente a mesma construção pode ser usada para estabelecer a compacidade diretamente, partindo de conjuntos "finitamente satisfatíveis" de sentenças em vez de conjuntos consistentes.

## 13.2 Esboço da Prova

A prova do teorema da completude é um pouco complexa e, em uma primeira leitura, é fácil se perder. Então, vamos esboçar a prova. O primeiro passo é uma mudança de perspectiva, que nos permite enxergar um caminho para uma prova. Quando a completude é pensada como "sempre que $\Gamma \vDash \varphi$ então $\Gamma \vdash \varphi$", pode ser difícil até mesmo ter uma ideia: pois, para mostrar que $\Gamma \vdash \varphi$, temos que encontrar a derivação, e não parece que a hipótese de que $\Gamma \vDash \varphi$ nos ajude nisso de alguma forma. Para alguns sistemas de prova, é possível construir diretamente a derivação, mas adotaremos uma abordagem um pouco diferente. A mudança de perspectiva necessária é esta: a completude também pode ser formulada como: "se $\Gamma$ é consistente, então é satisfatível". Talvez possamos usar a informação em $\Gamma$ juntamente com a hipótese de que ela é consistente para construir a valoração que satisfaça toda fórmula em $\Gamma$. Afinal, sabemos que tipo de valoração estamos procurando: uma que seja como $\Gamma$ a descreve!

Se $\Gamma$ contém apenas variáveis proposicionais, é fácil construir um modelo para ele. Tudo o que temos a fazer é apresentar a valoração $\mathfrak{v}$ tal que $\mathfrak{v} \vDash p$ para todo $p \in \Gamma$. Bem, faça $\mathfrak{v}(p) = \mathbb{T}$ se e somente se $p \in \Gamma$.

Agora suponha que $\Gamma$ contenha alguma fórmula $\neg\psi$, com $\psi$ atômica. Poderíamos temer que a construção de $\mathfrak{v}$ interfira na possibilidade de tornar $\neg\psi$ verdadeira. Mas é aqui que entra a consistência de $\Gamma$: se $\neg\psi \in \Gamma$, então $\psi \notin \Gamma$, caso contrário $\Gamma$ seria inconsistente. E se $\psi \notin \Gamma$, então, de acordo com nossa construção de $\mathfrak{v}$, $\mathfrak{v} \nvDash \psi$, logo $\mathfrak{v} \vDash \neg\psi$. Até aqui, tudo bem.

E se $\Gamma$ contiver fórmulas complexas, não atômicas? Digamos que ele con-

tenha $\varphi \wedge \psi$. Para tornar isso verdadeiro, devemos proceder como se tanto $\varphi$ quanto $\psi$ estivessem em $\Gamma$. E se $\varphi \vee \psi \in \Gamma$, então teremos que tornar pelo menos um deles verdadeiro, isto é, proceder como se um deles estivesse em $\Gamma$.

Isso sugere a seguinte ideia: adicionamos fórmulas adicionais a $\Gamma$ de modo a (a) manter o conjunto resultante consistente e (b) garantir que, para toda sentença $\varphi$ atômica possível, ou $\varphi$ está no conjunto resultante, ou $\neg\varphi$ está, e (c) tais que, sempre que $\varphi \wedge \psi$ está no conjunto, então tanto $\varphi$ quanto $\psi$ também estão; se $\varphi \vee \psi$ está no conjunto, pelo menos um dentre $\varphi$ ou $\psi$ também está, etc. Continuamos fazendo isso (potencialmente para sempre). Chame o conjunto de todas as fórmulas assim adicionadas de $\Gamma^*$. Então a nossa construção acima nos forneceria a valoração $\mathfrak{v}$ para a qual poderíamos provar, por indução, que ela satisfaz todas as sentenças em $\Gamma^*$ e, portanto, também todas as sentenças em $\Gamma$, já que $\Gamma \subseteq \Gamma^*$. Acontece que garantir (a) e (b) é suficiente. Um conjunto de sentenças para o qual (b) vale é chamado de *completo*. Assim, nossa tarefa será estender o conjunto consistente $\Gamma$ a um conjunto consistente e completo $\Gamma^*$.

Então, aqui está o que faremos. Primeiro investigamos as propriedades dos conjuntos consistentes completos; em particular, provamos que um conjunto consistente completo contém $\varphi \wedge \psi$ se e somente se contém tanto $\varphi$ quanto $\psi$, contém $\varphi \vee \psi$ se e somente se contém pelo menos um deles, etc. (Proposição 13.2). Em seguida, tomaremos o conjunto consistente $\Gamma$ e mostraremos que ele pode ser estendido a um conjunto consistente e completo $\Gamma^*$ (Lema 13.3). Este conjunto $\Gamma^*$ é o que usaremos para definir nossa valoração $\mathfrak{v}(\Gamma^*)$. A valoração é determinada pelas variáveis proposicionais em $\Gamma^*$ (Definição 13.4). Usaremos as propriedades dos conjuntos consistentes completos para mostrar que, de fato, $\mathfrak{v}(\Gamma^*) \vDash \varphi$ se e somente se $\varphi \in \Gamma^*$ (Lema 13.5) e, portanto, em particular, $\mathfrak{v}(\Gamma^*) \vDash \Gamma$.

## 13.3 Conjuntos Consistentes Completos de Sentenças

**Definição 13.1 (Conjunto completo).** Um conjunto $\Gamma$ de sentenças é *completo* se e somente se, para qualquer sentença $\varphi$, ou $\varphi \in \Gamma$ ou $\neg\varphi \in \Gamma$.

Conjuntos completos de sentenças não deixam questões sem resposta. Para qualquer sentença $\varphi$, $\Gamma$ "diz" se $\varphi$ é verdadeira ou falsa. A importância dos conjuntos completos estende-se para além da prova do teorema da completude. Uma teoria que é completa e axiomatizável, por exemplo, é sempre decidível.

Conjuntos consistentes completos são importantes na prova de completude já que podemos garantir que todo conjunto consistente de sentenças $\Gamma$ está contido em um conjunto consistente completo $\Gamma^*$. Um conjunto consistente completo contém, para cada sentença $\varphi$, ou $\varphi$ ou sua negação $\neg\varphi$, mas não ambas. Isso é verdade em particular para variáveis proposicionais, de modo que, a partir de um conjunto consistente completo, podemos construir

a valoração onde a valor de verdade atribuído às variáveis proposicionais é definida de acordo com quais variáveis proposicionais estão em $\Gamma^*$. Pode-se então mostrar que esta valoração torna verdadeiras todas as sentenças em $\Gamma^*$ (e, portanto, também todas aquelas em $\Gamma$). A prova deste último fato requer que $\neg\varphi \in \Gamma^*$ se e somente se $\varphi \notin \Gamma^*$, $(\varphi \vee \psi) \in \Gamma^*$ se e somente se $\varphi \in \Gamma^*$ ou $\psi \in \Gamma^*$, etc.

No que se segue, usaremos com frequência, de modo tácito, as propriedades de reflexividade, monotonicidade e transitividade de $\vdash$ (ver Seções 9.6 e 10.5 e **????**).

**Proposição 13.2.** *Suponha que $\Gamma$ seja completo e consistente. Então:*

1. *Se $\Gamma \vdash \varphi$, então $\varphi \in \Gamma$.*
2. *$\varphi \wedge \psi \in \Gamma$ se e somente se $\varphi \in \Gamma$ e $\psi \in \Gamma$.*
3. *$\varphi \vee \psi \in \Gamma$ se e somente se $\varphi \in \Gamma$ ou $\psi \in \Gamma$.*
4. *$\varphi \to \psi \in \Gamma$ se e somente se $\varphi \notin \Gamma$ ou $\psi \in \Gamma$.*

*Prova.* Suponhamos, para tudo o que se segue, que $\Gamma$ seja completo e consistente.

1. Se $\Gamma \vdash \varphi$, então $\varphi \in \Gamma$.

   Suponha que $\Gamma \vdash \varphi$. Suponha, ao contrário, que $\varphi \notin \Gamma$. Como $\Gamma$ é completo, $\neg\varphi \in \Gamma$. Por Proposições 9.19 e 10.17 e **????**, $\Gamma$ é inconsistente. Isso contradiz a suposição de que $\Gamma$ é consistente. Logo, não pode ser o caso que $\varphi \notin \Gamma$, de modo que $\varphi \in \Gamma$.

2. Exercício.

3. Primeiro mostramos que, se $\varphi \vee \psi \in \Gamma$, então $\varphi \in \Gamma$ ou $\psi \in \Gamma$. Suponha $\varphi \vee \psi \in \Gamma$ mas $\varphi \notin \Gamma$ e $\psi \notin \Gamma$. Como $\Gamma$ é completo, $\neg\varphi \in \Gamma$ e $\neg\psi \in \Gamma$. Por Proposições 9.22 e 10.20 e **????**, item (1), $\Gamma$ é inconsistente, uma contradição. Logo, $\varphi \in \Gamma$ ou $\psi \in \Gamma$.

   Para a direção reversa, suponha que $\varphi \in \Gamma$ ou $\psi \in \Gamma$. Por Proposições 9.22 e 10.20 e **????**, item (2), $\Gamma \vdash \varphi \vee \psi$. Por (1), $\varphi \vee \psi \in \Gamma$, como requerido.

4. Exercício. □

## 13.4 Lema de Lindenbaum

Provamos agora um lema que mostra que qualquer conjunto consistente de sentenças está contido em algum conjunto de sentenças que não é apenas consistente, mas também completo. A prova funciona adicionando uma sentença de cada vez, garantindo a cada passo que o conjunto permanece consistente.

Fazemos isso de modo que, para todo $\varphi$, ou $\varphi$ ou $\neg\varphi$ seja adicionada em algum estágio. A união de todos os estágios dessa construção então contém ou $\varphi$ ou sua negação $\neg\varphi$ e é, portanto, completa. Ela também é consistente, já que nos asseguramos, a cada estágio, de não introduzir uma inconsistência.

**Lema 13.3 (Lema de Lindenbaum).** *Todo conjunto consistente $\Gamma$ em uma linguagem $\mathcal{L}$ pode ser estendido a um conjunto consistente completo $\Gamma^*$.*

*Prova.* Seja $\Gamma$ consistente. Sejam $\varphi_0$, $\varphi_1$, ... uma enumeração de todas as sentenças de $\mathcal{L}$. Defina $\Gamma_0 = \Gamma$, e

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{\varphi_n\} & \text{se } \Gamma_n \cup \{\varphi_n\} \text{ é consistente;} \\ \Gamma_n \cup \{\neg\varphi_n\} & \text{caso contrário.} \end{cases}$$

Seja $\Gamma^* = \bigcup_{n\geq 0} \Gamma_n$.

Cada $\Gamma_n$ é consistente: $\Gamma_0$ é consistente por definição. Se $\Gamma_{n+1} = \Gamma_n \cup \{\varphi_n\}$, isso é porque este último é consistente. Se não é, $\Gamma_{n+1} = \Gamma_n \cup \{\neg\varphi_n\}$. Temos que verificar que $\Gamma_n \cup \{\neg\varphi_n\}$ é consistente. Suponha que não seja. Então *ambos* $\Gamma_n \cup \{\varphi_n\}$ e $\Gamma_n \cup \{\neg\varphi_n\}$ são inconsistentes. Isso significa que $\Gamma_n$ seria inconsistente por **??????????** e Proposições 9.20 e 10.18, contrariando a hipótese de indução.

Para todo $n$ e todo $i < n$, $\Gamma_i \subseteq \Gamma_n$. Isso segue por uma simples indução sobre $n$. Para $n = 0$, não há $i < 0$, de modo que a afirmação vale automaticamente. Para o passo indutivo, suponha que ela seja verdadeira para $n$. Mostramos que, se $i < n+1$, então $\Gamma_i \subseteq \Gamma_{n+1}$. Temos $\Gamma_{n+1} = \Gamma_n \cup \{\varphi_n\}$ ou $= \Gamma_n \cup \{\neg\varphi_n\}$ por construção. Logo $\Gamma_n \subseteq \Gamma_{n+1}$. Se $i < n+1$, então $\Gamma_i \subseteq \Gamma_n$ por hipótese indutiva (se $i < n$) ou pelo fato trivial de que $\Gamma_n \subseteq \Gamma_n$ (se $i = n$). Obtemos que $\Gamma_i \subseteq \Gamma_{n+1}$ por transitividade de $\subseteq$.

Disso segue que $\Gamma^*$ é consistente. Eis o porquê: Seja $\Gamma' \subseteq \Gamma^*$ finito. Cada $\psi \in \Gamma'$ também está em $\Gamma_i$ para algum $i$. Seja $n$ o maior destes. Como $\Gamma_i \subseteq \Gamma_n$ se $i \leq n$, todo $\psi \in \Gamma'$ também está $\in \Gamma_n$, isto é, $\Gamma' \subseteq \Gamma_n$, e $\Gamma_n$ é consistente. Assim, todo subconjunto finito $\Gamma' \subseteq \Gamma^*$ é consistente. Por **??????????** e Proposições 9.16 e 10.14, $\Gamma^*$ é consistente.

Toda sentença de $\mathrm{Frm}(\mathcal{L})$ aparece na lista usada para definir $\Gamma^*$. Se $\varphi_n \notin \Gamma^*$, então isso é porque $\Gamma_n \cup \{\varphi_n\}$ era inconsistente. Mas então $\neg\varphi_n \in \Gamma^*$, de modo que $\Gamma^*$ é completo. □

## 13.5 Construção de um Modelo

Estamos agora prontos para definir a valoração que torna verdadeiras todas as $\varphi \in \Gamma$. Para fazer isso, primeiro aplicamos o Lema de Lindenbaum: obtemos um $\Gamma^* \supseteq \Gamma$ consistente completo. Deixamos as variáveis proposicionais em $\Gamma^*$ determinarem $\mathfrak{v}(\Gamma^*)$.

**Definição 13.4.** Suponha que $\Gamma^*$ seja um conjunto consistente completo de fórmulas. Então deixamos

$$\mathfrak{v}(\Gamma^*)(p) = \begin{cases} \mathbb{T} & \text{se } p \in \Gamma^* \\ \mathbb{F} & \text{se } p \notin \Gamma^* \end{cases}$$

**Lema 13.5 (Lema da Verdade).** *$\mathfrak{v}(\Gamma^*) \vDash \varphi$ se e somente se $\varphi \in \Gamma^*$.*

*Prova.* Provamos ambas as direções simultaneamente e por indução sobre $\varphi$.

1. $\varphi \equiv \bot$: $\mathfrak{v}(\Gamma^*) \nvDash \bot$ por definição de satisfação. Por outro lado, $\bot \notin \Gamma^*$ já que $\Gamma^*$ é consistente.

2. $\varphi \equiv p$: $\mathfrak{v}(\Gamma^*) \vDash p$ se e somente se $\mathfrak{v}(\Gamma^*)(p) = \mathbb{T}$ (pela definição de satisfação) se e somente se $p \in \Gamma^*$ (pela construção de $\mathfrak{v}(\Gamma^*)$).

3. $\varphi \equiv \neg\psi$: $\mathfrak{v}(\Gamma^*) \vDash \varphi$ se e somente se $\mathfrak{v}(\Gamma^*) \nvDash \psi$ (por definição de satisfação). Por hipótese de indução, $\mathfrak{v}(\Gamma^*) \nvDash \psi$ se e somente se $\psi \notin \Gamma^*$. Como $\Gamma^*$ é consistente e completo, $\psi \notin \Gamma^*$ se e somente se $\neg\psi \in \Gamma^*$.

4. $\varphi \equiv \psi \wedge \chi$: exercise.

5. $\varphi \equiv \psi \vee \chi$: $\mathfrak{v}(\Gamma^*) \vDash \varphi$ se e somente se $\mathfrak{v}(\Gamma^*) \vDash \psi$ ou $\mathfrak{v}(\Gamma^*) \vDash \chi$ (por definição de satisfação) se e somente se $\psi \in \Gamma^*$ ou $\chi \in \Gamma^*$ (por hipótese de indução). Este é o caso se e somente se $(\psi \vee \chi) \in \Gamma^*$ (por Proposição 13.2(3)).

6. $\varphi \equiv \psi \to \chi$: exercise.

## 13.6 O Teorema da Completude

Vamos combinar nossos resultados: chegamos ao teorema da completude.

**Teorema 13.6 (Teorema da Completude).** *Seja $\Gamma$ um conjunto de sentenças. Se $\Gamma$ é consistente, então é satisfatível.*

*Prova.* Suponha que $\Gamma$ seja consistente. Por Lema 13.3, existe um $\Gamma^* \supseteq \Gamma$ que é consistente e completo. Por Lema 13.5, $\mathfrak{v}(\Gamma^*) \vDash \varphi$ se e somente se $\varphi \in \Gamma^*$. Disso segue, em particular, que, para todo $\varphi \in \Gamma$, $\mathfrak{v}(\Gamma^*) \vDash \varphi$, de modo que $\Gamma$ é satisfatível. □

**Corolário 13.7 (Teorema da Completude, Segunda Versão).** *Para todo $\Gamma$ e sentenças $\varphi$: se $\Gamma \vDash \varphi$ então $\Gamma \vdash \varphi$.*

*Prova.* Note que os $\Gamma$ em Corolário 13.7 e Teorema 13.6 são universalmente quantificados. Para nos certificarmos de que não nos confundimos, reformulemos Teorema 13.6 usando uma variável diferente: para qualquer conjunto de sentenças $\Delta$, se $\Delta$ é consistente, então é satisfatível. Por contraposição, se $\Delta$ não é satisfatível, então $\Delta$ é inconsistente. Usaremos isso para provar o corolário.

Suponha que $\Gamma \vDash \varphi$. Então $\Gamma \cup \{\neg\varphi\}$ é insatisfatível por **??**. Tomando $\Gamma \cup \{\neg\varphi\}$ como nosso $\Delta$, a versão anterior de Teorema 13.6 nos dá que $\Gamma \cup \{\neg\varphi\}$ é inconsistente. Por **??????????** e Proposições 9.18 e 10.16, $\Gamma \vdash \varphi$. □

## 13.7 O Teorema da Compacidade

Uma consequência importante do teorema da completude é o teorema da compacidade. O teorema da compacidade afirma que, se cada subconjunto *finito* de um conjunto de sentenças é satisfatível, o conjunto inteiro é satisfatível — mesmo que o próprio conjunto seja infinito. Isso está longe de ser óbvio. Não há nada que pareça descartar, ao menos à primeira vista, a possibilidade de existirem conjuntos infinitos de sentenças que sejam contraditórios, mas em que a contradição só surge, por assim dizer, do número infinito. O teorema da compacidade diz que tal cenário pode ser descartado: não existem conjuntos infinitos insatisfatíveis de sentenças tais que cada subconjunto finito deles seja satisfatível. Como o teorema da completude, ele tem uma versão relacionada à consequência lógica: se um conjunto infinito de sentenças implica algo, então já um subconjunto finito o implica.

**Definição 13.8.** Um conjunto $\Gamma$ de fórmulas é *finitamente satisfatível* se e somente se todo $\Gamma_0 \subseteq \Gamma$ finito é satisfatível.

**Teorema 13.9 (Teorema da Compacidade).** *O seguinte vale para quaisquer sentenças $\Gamma$ e $\varphi$:*

1. *$\Gamma \vDash \varphi$ se e somente se existe um $\Gamma_0 \subseteq \Gamma$ finito tal que $\Gamma_0 \vDash \varphi$.*

2. *$\Gamma$ é satisfatível se e somente se é finitamente satisfatível.*

*Prova.* Provamos (2). Se $\Gamma$ é satisfatível, então existe a valoração $\mathfrak{v}$ tal que $\mathfrak{v} \vDash \varphi$ para todo $\varphi \in \Gamma$. É claro que essa $\mathfrak{v}$ também satisfaz todo subconjunto finito de $\Gamma$, de modo que $\Gamma$ é finitamente satisfatível.

Agora suponha que $\Gamma$ seja finitamente satisfatível. Então todo subconjunto finito $\Gamma_0 \subseteq \Gamma$ é satisfatível. Pela correção (**??????????** e Corolários 9.28 e 10.24), todo subconjunto finito é consistente. Então o próprio $\Gamma$ deve ser consistente por **??????????** e Proposições 9.16 e 10.14. Pela completude (Teorema 13.6), como $\Gamma$ é consistente, ele é satisfatível. □

## 13.8 Uma Prova Direta do Teorema da Compacidade

Podemos provar o Teorema da Compacidade diretamente, sem apelar ao Teorema da Completude, usando as mesmas ideias da prova do teorema da completude. Na prova do Teorema da Completude, começamos com um conjunto $\Gamma$ consistente de sentenças, expandimos-o para um conjunto $\Gamma^*$ de sentenças consistente e completo, e então mostramos que no valoração $\mathfrak{v}(\Gamma^*)$ construído a partir de $\Gamma^*$, todas as sentenças de $\Gamma$ são verdadeiras, de modo que $\Gamma$ é satisfatível.

Podemos usar o mesmo método para mostrar que um conjunto finitamente satisfatível de sentenças é satisfatível. Só temos que provar as versões correspondentes dos resultados que levam ao lema da verdade, substituindo "consistente" por "finitamente satisfatível".

**Proposição 13.10.** *Suponha que $\Gamma$ é completo e finitamente satisfatível. Então:*

1. *$(\varphi \wedge \psi) \in \Gamma$ se, e somente se, tanto $\varphi \in \Gamma$ quanto $\psi \in \Gamma$.*
2. *$(\varphi \vee \psi) \in \Gamma$ se, e somente se, $\varphi \in \Gamma$ ou $\psi \in \Gamma$.*
3. *$(\varphi \to \psi) \in \Gamma$ se, e somente se, $\varphi \notin \Gamma$ ou $\psi \in \Gamma$.*

**Lema 13.11.** *Todo conjunto finitamente satisfatível $\Gamma$ pode ser estendido a um conjunto completo e finitamente satisfatível $\Gamma^*$.*

**Teorema 13.12 (Compacidade).** *$\Gamma$ é satisfatível se, e somente se, é finitamente satisfatível.*

*Prova.* Se $\Gamma$ é satisfatível, então há a valoração $\mathfrak{v}$ tal que $\mathfrak{v} \vDash \varphi$ para todo $\varphi \in \Gamma$. É claro que esta $\mathfrak{v}$ também satisfaz todo subconjunto finito de $\Gamma$, de modo que $\Gamma$ é finitamente satisfatível.

Agora suponha que $\Gamma$ é finitamente satisfatível. Por Lema 13.11, $\Gamma$ pode ser estendido a um conjunto completo e finitamente satisfatível $\Gamma^*$. Construa o valoração $\mathfrak{v}(\Gamma^*)$ como em Definição 13.4. A prova do Lema da Verdade (Lema 13.5) funciona se substituirmos referências a Proposição 13.2. □

## Problemas

**Problema 13.1.** Complete a prova de Proposição 13.2.

**Problema 13.2.** Complete a prova de Lema 13.5.

**Problema 13.3.** Use Corolário 13.7 para provar Teorema 13.6, mostrando assim que as duas formulações do teorema da completude são equivalentes.

**Problema 13.4.** Para que um sistema de derivação seja completo, suas regras devem ser fortes o suficiente para provar que todo conjunto insatisfatível é inconsistente. Quais das regras de derivação foram necessárias para provar a completude? Alguma dessas regras não é usada em nenhum lugar da prova? Para responder a essas perguntas, faça uma lista ou diagrama que mostre quais das regras de derivação foram usadas em quais resultados que levam à prova de Teorema 13.6. Certifique-se de anotar quaisquer usos tácitos de regras nessas provas.

**Problema 13.5.** Prove (1) de Teorema 13.9.

**Problema 13.6.** Prove Proposição 13.10. Evite o uso de $\vdash$.

**Problema 13.7.** Prove Lema 13.11. (Dica: o passo crucial é mostrar que se $\Gamma_n$ é finitamente satisfatível, então ou $\Gamma_n \cup \{\varphi_n\}$ ou $\Gamma_n \cup \{\neg\varphi_n\}$ é finitamente satisfatível.)

**Problema 13.8.** Escreva a prova completa do Lema da Verdade (Lema 13.5) na versão necessária para a prova de Teorema 13.12.

# Parte III

# Lógica de Primeira Ordem

Esta parte cobre a metateoria da lógica de primeira ordem através completude. Atualmente não depende de um tratamento separado de lógica proposicional; tudo está provado. Os arquivos de origem serão exclua o material sobre quantificadores (e substitua "estrutura" com "valoração", $\mathfrak{M}$ com $\mathfrak{v}$, etc.) se a tag "FOL" é falsa. Na verdade, a maior parte do material da peça na lógica proposicional é simplesmente o material de primeira ordem com o Etiqueta "FOL" desativada.

Se a parte sobre lógica proposicional for incluída, isso resulta em uma muita repetição. Está planeado, no entanto, tornar possível deixe esta parte levar em conta o material sobre lógica proposicional (e excluir o material já abordado, bem como encurtar as provas com referências aos respectivos lugares no proposicional parte).

# Capítulo 14

# Introdução à Lógica de Primeira Ordem

## 14.1 Lógica de Primeira Ordem

Você provavelmente já conhece a lógica de primeira ordem da sua primeira introdução à lógica formal.[1] Pode conhecê-la como "lógica quantificacional" ou "lógica de predicados". A lógica de primeira ordem, antes de tudo, é uma linguagem formal. Isso significa que ela tem um certo vocabulário, e suas expressões são cadeias desse vocabulário. Mas nem toda cadeia é permitida. Há diferentes tipos de expressões permitidas: termos, fórmulas e sentenças. Estamos principalmente interessados em sentenças da lógica de primeira ordem: elas nos fornecem um análogo formal de sentenças do inglês, e sobre elas podemos fazer as perguntas que um lógico tipicamente se interessa. Por exemplo:

- $\psi$ segue logicamente de $\varphi$?
- $\varphi$ é logicamente verdadeira, logicamente falsa ou contingente?
- $\varphi$ e $\psi$ são equivalentes?

Essas perguntas são primariamente perguntas sobre o "significado" das sentenças da lógica de primeira ordem. Por exemplo, um filósofo analisaria a pergunta de se $\psi$ segue logicamente de $\varphi$ como perguntando: há um caso em que $\varphi$ é verdadeira mas $\psi$ é falsa ($\psi$ não segue de $\varphi$), ou todo caso que torna $\varphi$ verdadeira também torna $\psi$ verdadeira ($\psi$ segue de $\varphi$)? Mas ainda não nos foi dito o que é um "caso"—esse é o trabalho da *semântica*. A semântica da lógica de primeira ordem fornece um modelo matematicamente preciso da ideia intuitiva do filósofo de "caso", e também—e isso é importante—do que significa

[1] De fato, mais ou menos assumimos que sim! Se não conhece, pode revisar um livro-texto mais elementar, como *forall x* (Magnus et al., 2021).

uma sentença $\varphi$ ser *verdadeira em* um caso. Chamamos o modelo matematicamente preciso que desenvolveremos de a estrutura. A relação que torna "verdadeira em" precisa é chamada de relação de *satisfação*. Assim, o que definiremos é "$\varphi$ é satisfeita em $\mathfrak{M}$" (em símbolos: $\mathfrak{M} \vDash \varphi$) para sentenças $\varphi$ e estruturas $\mathfrak{M}$. Uma vez feito isso, também podemos dar definições precisas dos outros termos semânticos como "segue de" ou "é logicamente verdadeira". Essas definições tornarão possível decidir, novamente com precisão matemática, se, por exemplo, $\forall x\,(\varphi(x) \to \psi(x)), \exists x\,\varphi(x) \vDash \exists x\,\psi(x)$. A resposta será, é claro, "sim". Se você já foi treinado para simbolizar sentenças do inglês na lógica de primeira ordem, reconhecerá isto como, por exemplo, a simbolização de "Todas as formigas são insetos, há formigas, portanto há insetos." Isso é obviamente um argumento válido, e assim nosso modelo matemático de "segue de" para nossa linguagem formal deve dar a mesma resposta.

Outro tópico que você provavelmente lembra da sua primeira introdução à lógica formal é que há *derivações*. Se você fez um primeiro curso de lógica formal, seu professor o fez praticar a encontrar tais derivações, talvez até uma derivação que mostra que a consequência acima vale. Há muitas maneiras diferentes de dar derivações: você pode ter feito algo chamado "dedução natural" ou "árvores de verdade", mas há muitas outras. O propósito dos sistemas de derivação é fornecer ferramentas com as quais as perguntas dos lógicos acima podem ser respondidas: por exemplo, uma derivação de dedução natural em que $\forall x\,(\varphi(x) \to \psi(x))$ e $\exists x\,\varphi(x)$ são premissas e $\exists x\,\psi(x)$ é a conclusão (última linha) *verifica* que $\exists x\,\psi(x)$ segue logicamente de $\forall x\,(\varphi(x) \to \psi(x))$ e $\exists x\,\varphi(x)$.

Mas por quê? À primeira vista, os sistemas de derivação não têm nada a ver com semântica: dar uma derivação formal envolve apenas dispor símbolos de certas maneiras regidas por regras; eles não mencionam "casos" ou "verdadeira em" de forma alguma. A conexão entre sistemas de derivação e semântica tem de ser estabelecida por uma investigação metalógica. O que é necessário é uma prova matemática, por exemplo, de que uma derivação formal de $\exists x\,\psi(x)$ a partir das premissas $\forall x\,(\varphi(x) \to \psi(x))$ e $\exists x\,\varphi(x)$ é possível se, e somente se, $\exists x\,\psi(x)$ é consequência de $\forall x\,(\varphi(x) \to \psi(x))$ e $\exists x\,\varphi(x)$ em conjunto. Antes que isso possa ser feito, entretanto, muito trabalho minucioso tem de ser realizado para acertar as definições de sintaxe e semântica.

## 14.2 Sintaxe

Primeiro devemos tornar preciso quais cadeias de símbolos contam como sentenças da lógica de primeira ordem. Faremos isso mais adiante; por enquanto, procederemos por exemplos. Os blocos de construção básicos—o vocabulário—da lógica de primeira ordem dividem-se em duas partes. A primeira parte são os símbolos que usamos para dizer coisas específicas ou para destacar coisas es-

pecíficas. Destacamos coisas usando símbolos de constante, e dizemos coisas sobre o que destacamos usando símbolos de predicado. Por exemplo, poderíamos usar $a$ como a símbolo de constante para destacar uma única coisa, e então dizer algo sobre ela usando a sentença $P(a)$. Se você tem significados para "$a$" e "$P$" em mente, pode ler $P(a)$ como uma sentença do inglês (e provavelmente já fez isso quando aprendeu lógica formal pela primeira vez). Uma vez que se tem tais sentenças simples da lógica de primeira ordem, pode-se construir outras mais complexas usando a segunda parte do vocabulário: os símbolos lógicos (conectivos e quantificadores). Assim, por exemplo, podemos formar expressões como $(P(a) \wedge Q(b))$ ou $\exists x\, P(x)$.

Para fornecer as definições precisas de semântica e as regras dos nossos sistemas de derivação necessárias para o estudo meta-lógico rigoroso, temos primeiro que dar uma definição precisa do que conta como a sentença da lógica de primeira ordem. A ideia básica é fácil o suficiente de entender: há algumas sentenças simples que podemos formar apenas a partir de símbolos de predicado e símbolos de constante, como $P(a)$. E então a partir destas formamos outras mais complexas usando os conectivos e quantificadores. Mas quais são exatamente as regras pelas quais nos é permitido formar sentenças mais complexas? Elas devem ser especificadas; caso contrário, não definimos "sentença da lógica de primeira ordem" com precisão suficiente. Há algumas questões. A primeira é obter as cadeias certas para contarem como sentenças. A segunda é fazê-lo de tal forma que possamos dar provas matemáticas sobre *todas* as sentenças. Finalmente, teremos também que dar definições precisas de algumas operações rudimentares com sentenças, como "substituir todo $x$ em $\varphi$ por $b$." O problema é que os quantificadores e variáveis que temos na lógica de primeira ordem tornam não inteiramente óbvio como isso deve ser feito. Por exemplo, $\exists x\, P(a)$ deve contar como a sentença? E quanto a $\exists x\, \exists x\, P(x)$? Qual deveria ser o resultado de "substituir $x$ por $b$ em $(P(x) \wedge \exists x\, P(x))$"?

## 14.3 Fórmulas

Eis a abordagem que usaremos para especificar rigorosamente as sentenças da lógica de primeira ordem e para lidar com as questões decorrentes do uso de variáveis. Primeiro definimos um conjunto *diferente* de expressões: fórmulas. Uma vez feito isso, podemos considerar o papel que as variáveis desempenham nelas—e, com base em algumas outras ideias, nomeadamente as de variáveis "livres" e "ligadas", podemos definir o que é uma sentença (nomeadamente, uma fórmula sem variáveis livres). Fazemos isso não apenas porque torna a definição de "sentença" mais gerenciável, mas também porque será crucial para a maneira como definimos a noção semântica de satisfação.

Vamos definir "fórmula" para uma linguagem simples de primeira ordem, contendo apenas um único símbolo de predicado $P$ e um único símbolo de constante $a$, e apenas os símbolos lógicos $\neg$, $\wedge$ e $\exists$. Nossas definições comple-

tas serão muito mais gerais: permitiremos infinitos símbolos de predicado e símbolos de constante. De fato, também consideraremos símbolos de função que podem ser combinados com símbolos de constante e variáveis para formar "termos". Por enquanto, $a$ e as variáveis serão nossos únicos termos. Precisamos de infinitas variáveis. Oficialmente usaremos os símbolos $v_0$, $v_1$, ..., como variáveis.

**Definição 14.1.** O conjunto de *fórmulas* Frm é definido da seguinte forma:

1. $P(a)$ e $P(v_i)$ são fórmulas ($i \in \mathbb{N}$).
2. Se $\varphi$ é uma fórmula, então $\neg\varphi$ é uma fórmula.
3. Se $\varphi$ e $\psi$ são fórmulas, então $(\varphi \wedge \psi)$ é uma fórmula.
4. Se $\varphi$ é uma fórmula e $x$ é uma variável, então $\exists x\, \varphi$ é uma fórmula.
5. Nada mais é uma fórmula.

(1) nos diz que $P(a)$ e $P(v_i)$ são fórmulas, para qualquer $i \in \mathbb{N}$. Estas são as chamadas fórmulas *atômicas*. Elas nos dão algo com que começar. As outras cláusulas nos dão maneiras de formar novas fórmulas a partir daquelas que já formamos. Assim, por exemplo, por (2), obtemos que $\neg P(v_2)$ é uma fórmula, já que $P(v_2)$ já é uma fórmula por (1). Então, por (4), obtemos que $\exists v_2\, \neg P(v_2)$ é outra fórmula, e assim por diante. (5) nos diz que *somente* cadeias que podemos formar desta maneira contam como fórmulas. Em particular, $\exists v_0\, P(a)$ e $\exists v_0\, \exists v_0\, P(a)$ *contam* como fórmulas, e $(\neg P(a))$ não conta, por causa dos parênteses externos supérfluos.

Esta maneira de definir fórmulas é chamada de *definição indutiva*, e nos permite provar coisas sobre fórmulas usando uma versão de prova por indução chamada *indução estrutural*. Estas são discutidas de maneira geral em Seção 75.4 e Seção 75.5, que você deve revisar antes de mergulhar nas provas mais adiante. Basicamente, a ideia é que, se você quer dar uma prova de que algo é verdadeiro para todas as fórmulas, mostra primeiro que é verdadeiro para as fórmulas atômicas e então que *se* for verdadeiro para qualquer fórmula $\varphi$ (e $\psi$), *também* é verdadeiro para $\neg\varphi$, $(\varphi \wedge \psi)$ e $\exists x\, \varphi$. Por exemplo, isso prova que é verdadeiro para $\exists v_2\, \neg P(v_2)$: da primeira parte você sabe que é verdadeiro para a fórmula atômica $P(v_2)$. Então obtém que é verdadeiro para $\neg P(v_2)$ pela segunda parte, e novamente que é verdadeiro para $\exists v_2\, \neg P(v_2)$ em si. Como todas as fórmulas são geradas indutivamente a partir de fórmulas atômicas, isso funciona para qualquer uma delas.

## 14.4 Satisfação

Já podemos avançar para a semântica da lógica de primeira ordem assim que sabemos o que são fórmulas: aqui, a definição básica é a de a estrutura. Para

nossa linguagem simples, uma estrutura $\mathfrak{M}$ tem apenas três componentes: um conjunto não vazio $|\mathfrak{M}|$ chamado de *domínio*, o que $a$ designa em $\mathfrak{M}$, e do que $P$ é verdadeiro em $\mathfrak{M}$. O objeto designado por $a$ é denotado por $a^{\mathfrak{M}}$ e o conjunto de coisas das quais $P$ é verdadeiro por $P^{\mathfrak{M}}$. A estrutura $\mathfrak{M}$ consiste apenas nestas três coisas: $|\mathfrak{M}|$, $a^{\mathfrak{M}} \in |\mathfrak{M}|$ e $P^{\mathfrak{M}} \subseteq |\mathfrak{M}|$. O caso geral será mais complicado, pois haverá muitos símbolos de predicado e símbolos de constante, os símbolos de constante podem ter mais de um lugar, e haverá também símbolos de função.

Isso basta para dar uma definição de satisfação para fórmulas que não contêm variáveis. A ideia é dar uma definição indutiva que espelha a maneira como definimos fórmulas. Especificamos quando uma fórmula atômica é satisfeita em $\mathfrak{M}$, e então quando, por exemplo, $\neg\varphi$ é satisfeita em $\mathfrak{M}$ com base em se $\varphi$ é ou não satisfeita em $\mathfrak{M}$. Por exemplo, poderíamos definir:

1. $P(a)$ é satisfeita em $\mathfrak{M}$ se, e somente se, $a^{\mathfrak{M}} \in P^{\mathfrak{M}}$.

2. $\neg\varphi$ é satisfeita em $\mathfrak{M}$ se, e somente se, $\varphi$ não é satisfeita em $\mathfrak{M}$.

3. $(\varphi \wedge \psi)$ é satisfeita em $\mathfrak{M}$ se, e somente se, $\varphi$ é satisfeita em $\mathfrak{M}$ e $\psi$ também é satisfeita em $\mathfrak{M}$.

Digamos que $|\mathfrak{M}| = \{0,1,2\}$, $a^{\mathfrak{M}} = 1$ e $P^{\mathfrak{M}} = \{1,2\}$. Esta definição nos diria que $P(a)$ é satisfeita em $\mathfrak{M}$ (pois $a^{\mathfrak{M}} = 1 \in \{1,2\} = P^{\mathfrak{M}}$). Nos diria ainda que $\neg P(a)$ não é satisfeita em $\mathfrak{M}$, e que, por sua vez, $\neg\neg P(a)$ é, e que $(\neg P(a) \wedge P(a))$ não é satisfeita, e assim por diante.

A dificuldade surge quando queremos dar uma definição para os quantificadores: gostaríamos de dizer algo como: "$\exists v_0\, P(v_0)$ é satisfeita se, e somente se, $P(v_0)$ é satisfeita." Mas a estrutura $\mathfrak{M}$ não nos diz o que fazer com variáveis. O que realmente queremos dizer é que $P(v_0)$ é satisfeita *para algum valor de* $v_0$. Para tornar isso preciso, precisamos de uma maneira de atribuir membros de $|\mathfrak{M}|$ não apenas a $a$, mas também a $v_0$. Para isso, introduzimos *atribuições de variáveis*. Uma atribuição de variáveis é simplesmente uma função $s$ que mapeia variáveis para membros de $|\mathfrak{M}|$ (em nosso exemplo, para um entre 1, 2 ou 3). Como não sabemos de antemão quais variáveis podem aparecer em uma fórmula, não podemos limitar a quais variáveis $s$ atribui valores. A solução simples é exigir que $s$ atribua valores a *todas* as variáveis $v_0, v_1, \ldots$ Usaremos apenas aquelas de que precisarmos.

Em vez de definir a satisfação de fórmulas apenas em relação a uma estrutura, definiremos em relação a uma estrutura $\mathfrak{M}$ *e* uma atribuição de variáveis $s$, e escreveremos $\mathfrak{M}, s \vDash \varphi$ por brevidade. Nossa definição agora incluirá uma cláusula adicional para lidar com fórmulas atômicas contendo variáveis:

1. $\mathfrak{M}, s \vDash P(a)$ se, e somente se, $a^{\mathfrak{M}} \in P^{\mathfrak{M}}$.

2. $\mathfrak{M}, s \vDash P(v_i)$ se, e somente se, $s(v_i) \in P^{\mathfrak{M}}$.

3. $\mathfrak{M}, s \vDash \neg\varphi$ se, e somente se, não $\mathfrak{M}, s \vDash \varphi$.

4. $\mathfrak{M}, s \vDash (\varphi \wedge \psi)$ se, e somente se, $\mathfrak{M}, s \vDash \varphi$ e $\mathfrak{M}, s \vDash \psi$.

Ok, isso resolve um problema: agora podemos dizer quando $\mathfrak{M}$ satisfaz $P(v_0)$ para o valor $s(v_0)$. Para obter a definição correta para $\exists v_0\, P(v_0)$ temos que fazer mais uma coisa: queremos que $\mathfrak{M}, s \vDash \exists v_0\, P(v_0)$ se, e somente se, $\mathfrak{M}, s' \vDash P(v_0)$ para *alguma* maneira $s'$ de atribuir um valor a $v_0$. Mas o valor atribuído a $v_0$ não precisa necessariamente ser o valor que $s(v_0)$ escolhe. Introduziremos uma notação para isso: se $m \in |\mathfrak{M}|$, então deixamos $s[m/v_0]$ ser a atribuição que é igual a $s$ (para todas as variáveis diferentes de $v_0$), exceto que a $v_0$ atribui $m$. Agora nossa definição pode ser:

5. $\mathfrak{M}, s \vDash \exists v_i\, \varphi$ se, e somente se, $\mathfrak{M}, s[m/v_i] \vDash \varphi$ para algum $m \in |\mathfrak{M}|$.

Funciona? Digamos que $s(v_i) = 0$ para todo $i \in \mathbb{N}$. $\mathfrak{M}, s \vDash \exists v_0\, P(v_0)$ se, e somente se, há um $m \in |\mathfrak{M}|$ tal que $\mathfrak{M}, s[m/v_0] \vDash P(v_0)$. E há: podemos escolher $m = 1$ ou $m = 2$. Note que isso é verdadeiro mesmo que o valor $s(v_0)$ atribuído a $v_0$ por $s$—neste caso, 0—não faça o trabalho. Temos $\mathfrak{M}, s[1/v_0] \vDash P(v_0)$, mas não $\mathfrak{M}, s \vDash P(v_0)$.

Se isso parece confuso e trabalhoso: é. Mas a complexidade adicional é necessária para dar uma definição precisa e indutiva de satisfação para todas as fórmulas, e precisamos de algo assim para definir precisamente as noções semânticas. Há outras maneiras de fazer isso, mas todas são igualmente (in)elegantes.

## 14.5 Sentenças

Ok, agora temos uma (esboço de uma) definição de satisfação ("verdadeira em") para estruturas e fórmulas. Mas isso requer um ingrediente adicional—uma atribuição de variável—e o que queríamos era uma definição de sentenças. Como nos livramos das atribuições, e o que são sentenças?

Você provavelmente se lembra de uma discussão, em sua primeira introdução à lógica formal, sobre a relação entre variáveis e quantificadores. Um quantificador é sempre seguido por a variável e, então, na parte da sentença à qual esse quantificador se aplica (seu "escopo"), entendemos que a variável está "ligada" a esse quantificador. Em fórmulas, não se exigia que toda variável tivesse um quantificador correspondente, e as variáveis sem quantificadores correspondentes são "livres" ou "não ligadas". Tomaremos as sentenças como sendo todas aquelas fórmulas que não têm variáveis livres.

Novamente, a ideia intuitiva de quando uma ocorrência de a variável em a fórmula $\varphi$ está ligada, de qual quantificador a liga e de quando ela é livre não é difícil de captar. Você pode ter aprendido um método para testar isso, talvez envolvendo a contagem de parênteses. Temos que insistir em uma definição precisa—e, como definimos fórmulas por indução, podemos dar

uma definição das ocorrências livres e ligadas de a variável $x$ em a fórmula $\varphi$ também por indução. Por exemplo, ela poderia ter este aspecto para nossa linguagem simplificada:

1. Se $\varphi$ é atômica, todas as ocorrências de $x$ nela são livres (isto é, a ocorrência de $x$ em $P(x)$ é livre).
2. Se $\varphi$ é da forma $\neg\psi$, então uma ocorrência de $x$ em $\neg\psi$ é livre se, e somente se, a ocorrência correspondente de $x$ for livre em $\psi$ (isto é, as ocorrências livres de variáveis em $\psi$ são exatamente as ocorrências correspondentes em $\neg\psi$).
3. Se $\varphi$ é da forma $(\psi \wedge \chi)$, então uma ocorrência de $x$ em $(\psi \wedge \chi)$ é livre se, e somente se, a ocorrência correspondente de $x$ for livre em $\psi$ ou em $\chi$.
4. Se $\varphi$ é da forma $\exists x\, \psi$, então nenhuma ocorrência de $x$ em $\varphi$ é livre; se é da forma $\exists y\, \psi$, em que $y$ é uma variável diferente de $x$, então uma ocorrência de $x$ em $\exists y\, \psi$ é livre se, e somente se, a ocorrência correspondente de $x$ for livre em $\psi$.

Uma vez que tenhamos uma definição precisa de ocorrências livres e ligadas de variáveis, podemos simplesmente dizer: a sentença é qualquer fórmula sem ocorrências livres de variáveis.

## 14.6 Noções Semânticas

Mencionamos acima que, quando consideramos se $\mathfrak{M}, s \vDash \varphi$ vale, (por conveniência) deixamos $s$ atribuir valores a todas as variáveis, mas apenas os valores que atribui às variáveis em $\varphi$ são usados. De fato, são apenas os valores das variáveis *livres* em $\varphi$ que importam. É claro que, por sermos cuidadosos, vamos provar esse fato. Como as sentenças não têm variáveis livres, $s$ não importa de modo algum quando se trata de saber se são satisfeitas em a estrutura. Assim, quando $\varphi$ é a sentença, podemos definir $\mathfrak{M} \vDash \varphi$ como significando "$\mathfrak{M}, s \vDash \varphi$ para todo $s$," o que, aliás, é verdadeiro se, e somente se, $\mathfrak{M}, s \vDash \varphi$ para pelo menos um $s$. Precisamos introduzir atribuições de variáveis para obter uma definição funcional de satisfação para fórmulas, mas para sentenças, a satisfação é independente das atribuições de variáveis.

Uma vez que temos uma definição de "$\mathfrak{M} \vDash \varphi$," sabemos o que "caso" e "verdadeira em" significam no que diz respeito às sentenças da lógica de primeira ordem. Com base na definição de $\mathfrak{M} \vDash \varphi$ para sentenças, podemos então definir as noções semânticas básicas de validade, consequência e satisfatibilidade. Uma sentença é válida, $\vDash \varphi$, se toda estrutura a satisfaz. Ela é consequência de um conjunto de sentenças, $\Gamma \vDash \varphi$, se toda estrutura que satisfaz todas as sentenças em $\Gamma$ também satisfaz $\varphi$. E um conjunto de sentenças é satisfatível se alguma estrutura satisfaz todas as sentenças nele ao mesmo tempo.

Como as fórmulas são definidas indutivamente, e a satisfação é, por sua vez, definida por indução na estrutura das fórmulas, podemos usar indução para provar propriedades da nossa semântica e relacionar as noções semânticas definidas. Vamos reunir e provar algumas dessas propriedades, em parte porque são individualmente interessantes, mas principalmente porque muitas delas serão úteis quando formos investigar a relação entre semântica e sistemas de derivação. Para isso, também teremos que definir (precisamente, isto é, por indução) algumas noções sintáticas e operações que ainda não mencionamos.

## 14.7 Substituição

Discutiremos um exemplo para ilustrar como as coisas se articulam e como o desenvolvimento da sintaxe e da semântica estabelece as bases para nossas investigações mais avançadas posteriormente. Nossos sistemas de derivação deveriam permitir-nos derivar $P(a)$ de $\forall v_0\, P(v_0)$. Talvez até queiramos afirmar isso como uma regra de inferência. No entanto, para fazê-lo, devemos ser capazes de enunciá-lo nos termos mais gerais: não apenas para $P$, $a$ e $v_0$, mas para qualquer fórmula $\varphi$, e termo $t$, e variável $x$. (Lembre-se de que símbolos de constante são termos, mas vamos considerar também termos mais complicados construídos a partir de símbolos de constante e símbolos de função.) Então, queremos ser capazes de dizer algo como, "sempre que você tiver derivado $\forall x\, \varphi(x)$ você está justificado ao inferir $\varphi(t)$—o resultado da remoção de $\forall x$ e substituindo $x$ por $t$." Mas o que exatamente significa "substituir $x$ por $t$"? Qual é a relação entre $\varphi(x)$ e $\varphi(t)$? Isso sempre funciona?

Para tornar isso preciso, definimos a operação de *substituição*. A substituição é realmente complicada, porque não podemos simplesmente substituir todos os $x$ em $\varphi$ por $t$, e nem todos os $t$ podem ser substituídos por qualquer $x$. Lidaremos com isso novamente usando definições indutivas. Mas uma vez feito isso, especificando uma regra de inferência como "inferir $\varphi(t)$ de $\forall x\, \varphi(x)$" torna-se uma definição precisa. Além disso, seremos capazes de mostrar que esta é uma boa regra de inferência no sentido de que $\varphi(t)$ é consequência de $\forall x\, \varphi(x)$. Mas para provar isso, temos de provar novamente algo que à primeira vista pode levá-lo a perguntar "por que estamos fazendo isso?" Que $\varphi(t)$ seja consequência de $\forall x\, \varphi(x)$ depende do fato de que se $\mathfrak{M} \vDash \varphi(t)$ vale ou não depende apenas do valor do termo $t$, ou seja, se deixarmos $m$ ser qualquer membro de $|\mathfrak{M}|$ que for selecionado por $t$, então $\mathfrak{M}, s \vDash \varphi(t)$ se, e somente se, $\mathfrak{M}, s[m/x] \vDash \varphi(x)$. Isso vale mesmo quando $t$ contém variáveis, mas teremos que ter cuidado com a forma exata como declaramos o resultado.

## 14.8 Modelos e Teorias

Uma vez que definimos a sintaxe e a semântica da lógica de primeira ordem, podemos trabalhar investigando as propriedades de estruturas e as noções semânticas. Também podemos definir sistemas de derivação e investigá-los. Para um conjunto de sentenças, podemos perguntar: quais estruturas tornam todas as sentenças desse conjunto verdadeiras? Dado um conjunto de sentenças $\Gamma$, uma estrutura $\mathfrak{M}$ que as satisfaz é chamada de *modelo de* $\Gamma$. Podemos começar de $\Gamma$ e tentar encontrar seus modelos—como eles são? Quão grandes ou pequenos precisam ser? Mas também podemos começar com uma única estrutura ou coleção de estruturas e perguntar: quais sentenças são verdadeiras nelas? Há sentenças que *caracterizam* essas estruturas no sentido de que elas, e somente elas, são verdadeiras nelas? Esses tipos de questões são o domínio da *teoria dos modelos*. Elas também fundamentam o *método axiomático*: descrever uma coleção de estruturas por um conjunto de sentenças, os axiomas de uma teoria. Isso é possível pela observação de que exatamente aquelas sentenças que são consequência na lógica de primeira ordem dos axiomas são verdadeiras em todos os modelos dos axiomas.

Como exemplo muito simples, considere pré-ordens. Uma pré-ordem é uma relação $R$ sobre algum conjunto $A$ que é reflexiva e transitiva. Um conjunto $A$ com uma relação binária $R \subseteq A \times A$ sobre ele é exatamente o que precisaríamos para dar uma estrutura para uma linguagem de primeira ordem com um único símbolo de predicado de dois lugares $P$: definiríamos $|\mathfrak{M}| = A$ e $P^{\mathfrak{M}} = R$. Como $R$ é uma pré-ordem, é reflexiva e transitiva, e podemos encontrar um conjunto $\Gamma$ de sentenças da lógica de primeira ordem que diz isso:

$$\forall v_0 \, P(v_0, v_0)$$
$$\forall v_0 \, \forall v_1 \, \forall v_2 \, ((P(v_0, v_1) \land P(v_1, v_2)) \to P(v_0, v_2))$$

Estas sentenças são apenas as simbolizações de "para todo $x$, $Rxx$" ($R$ é reflexiva) e "sempre que $Rxy$ e $Ryz$, então também $Rxz$" ($R$ é transitiva). Vemos que uma estrutura $\mathfrak{M}$ é um modelo dessas duas sentenças $\Gamma$ se, e somente se, $R$ (isto é, $P^{\mathfrak{M}}$), é uma pré-ordem sobre $A$ (isto é, $|\mathfrak{M}|$). Em outras palavras, os modelos de $\Gamma$ são exatamente as pré-ordens. Qualquer propriedade de todas as pré-ordens que possa ser expressa na linguagem de primeira ordem apenas com $P$ como símbolo de predicado (como reflexividade e transitividade acima), é consequência das duas sentenças em $\Gamma$ e vice-versa. Assim, qualquer coisa que possamos provar sobre modelos de $\Gamma$ provamos sobre todas as pré-ordens.

Para qualquer teoria particular e classe de modelos (como $\Gamma$ e todas as pré-ordens), haverá questões interessantes sobre o que pode ser expresso na linguagem de primeira ordem correspondente, e o que não pode ser expresso. Há algumas propriedades de estruturas que são interessantes para todas as

linguagens e classes de modelos, a saber, aquelas que dizem respeito ao tamanho do domínio. Pode-se sempre expressar, por exemplo, que o domínio contém exatamente $n$ membros, para qualquer $n \in \mathbb{Z}^+$. Pode-se também expressar, usando um conjunto de infinitas sentenças, que o domínio é infinito. Mas não se pode expressar que o domínio é finito, ou que o domínio é não enumerável. Estes resultados sobre as limitações das linguagens de primeira ordem são consequências dos teoremas da compacidade e de Löwenheim–Skolem.

## 14.9 Correção e Completude

Também introduziremos sistemas de derivação para a lógica de primeira ordem. Há muitos sistemas de derivação que os lógicos desenvolveram, mas todos definem a mesma relação de derivabilidade entre sentenças. Dizemos que $\Gamma$ *deriva* $\varphi$, $\Gamma \vdash \varphi$, se há uma derivação de um certo tipo precisamente definido. As derivações são sempre disposições finitas de símbolos—talvez uma lista de sentenças, ou alguma estrutura mais complicada. O propósito dos sistemas de derivação é fornecer uma ferramenta para determinar se uma sentença é consequência de algum conjunto $\Gamma$. Para servir a esse propósito, deve ser verdade que $\Gamma \vDash \varphi$ se, e somente se, $\Gamma \vdash \varphi$.

Se $\Gamma \vdash \varphi$ mas não $\Gamma \vDash \varphi$, nosso sistema de derivação seria forte demais, provaria demais. A propriedade de que se $\Gamma \vdash \varphi$ então $\Gamma \vDash \varphi$ é chamada de *correção*, e é um requisito mínimo para qualquer bom sistema de derivação. Por outro lado, se $\Gamma \vDash \varphi$ mas não $\Gamma \vdash \varphi$, então nosso sistema de derivação é fraco demais, não prova o suficiente. A propriedade de que se $\Gamma \vDash \varphi$ então $\Gamma \vdash \varphi$ é chamada de *completude*. A correção é usualmente relativamente fácil de provar (por indução na estrutura das derivações, que são definidas indutivamente). A completude é mais difícil de provar.

Correção e completude têm várias consequências importantes. Se um conjunto de sentenças $\Gamma$ deriva uma contradição (como $\varphi \wedge \neg\varphi$), ele é chamado de *inconsistente*. $\Gamma$s inconsistentes não podem ter modelos; são insatisfatíveis. Da completude segue a contrapositiva: qualquer $\Gamma$ que não seja inconsistente—ou, como diremos, *consistente*—tem um modelo. De fato, isso é equivalente à completude, e é a forma de completude que de fato provaremos. É um resultado profundo e talvez surpreendente: apenas o fato de que você não pode provar $\varphi \wedge \neg\varphi$ a partir de $\Gamma$ garante que há uma estrutura que é como $\Gamma$ a descreve. Assim, a completude dá uma resposta à pergunta: quais conjuntos de sentenças têm modelos? Resposta: todos e somente os conjuntos consistentes têm.

Os teoremas de correção e completude têm duas consequências importantes: a compacidade e o teorema de Löwenheim–Skolem. Estes são resultados importantes na teoria de modelos e podem ser usados para estabelecer muitos resultados interessantes. Já mencionamos dois: a lógica de primeira ordem

não pode expressar que o domínio de uma estrutura é finito ou que é não enumerável.

Historicamente, tudo isso—como definir a sintaxe e a semântica da lógica de primeira ordem, como definir bons sistemas de derivação, como provar que são corretos e completos, ficar claro sobre o que pode e não pode ser expresso em linguagens de primeira ordem—levou muito tempo para ser descoberto e acertado. Agora sabemos como fazer isso, mas percorrer todos os detalhes ainda pode ser confuso e tedioso. Mas também é importante, porque os métodos desenvolvidos aqui para a linguagem formal da lógica de primeira ordem são aplicados em todo lugar em lógica, ciência da computação e linguística. Assim, trabalhar os detalhes compensa a longo prazo.

# Capítulo 15

# Sintaxe da Lógica de Primeira Ordem

## 15.1 Introdução

Para desenvolver a teoria e a metateoria da lógica de primeira ordem, devemos primeiro definir a sintaxe e a semântica de suas expressões. As expressões da lógica de primeira ordem são termos e fórmulas. Termos são formados a partir de variáveis, símbolos de constante e símbolos de função. Fórmulas, por sua vez, são formadas a partir de símbolos de predicado juntamente com termos (estes formam as menores fórmulas, as "atômicas"), e então, a partir de fórmulas atômicas, podemos formar outras mais complexas usando conectivos lógicos e quantificadores. Há muitas maneiras diferentes de estabelecer as regras de formação; damos apenas uma possível. Outros sistemas escolherão símbolos diferentes, selecionarão conjuntos diferentes de conectivos como primitivos, usarão parênteses de forma diferente (ou nem mesmo os usarão, como no caso da chamada notação polonesa). O que todas as abordagens têm em comum, no entanto, é que as regras de formação definem o conjunto de termos e fórmulas *indutivamente*. Se feito corretamente, cada expressão pode resultar essencialmente de uma única maneira de acordo com as regras de formação. A definição indutiva que resulta em expressões que são *de leitura única* significa que podemos dar significados a essas expressões usando o mesmo método—a definição indutiva.

## 15.2 Linguagens de Primeira Ordem

As expressões da lógica de primeira ordem são construídas a partir de um vocabulário básico contendo *variáveis*, *símbolos de constante*, *símbolos de predicado* e às vezes *símbolos de função*. A partir deles, juntamente com conectivos lógicos, quantificadores e símbolos de pontuação como parênteses e vírgulas, formam-se *termos* e *fórmulas*.

Informalmente, símbolos de predicado são nomes para propriedades e relações, símbolos de constante são nomes para objetos individuais, e símbolos de função são nomes para mapeamentos. Estes, exceto a predicado de identidade $=$, são os *símbolos não lógicos* e juntos constituem uma linguagem. Qualquer linguagem de primeira ordem $\mathcal{L}$ é determinada por seus símbolos não lógicos. No caso mais geral, $\mathcal{L}$ contém infinitos símbolos de cada tipo.

No caso geral, fazemos uso dos seguintes símbolos na lógica de primeira ordem:

1. Símbolos lógicos
   a) Conectivos lógicos: $\neg$ (negação), $\wedge$ (conjunção), $\vee$ (disjunção), $\rightarrow$ (condicional), $\forall$ (quantificador universal), $\exists$ (quantificador existencial).
   b) A constante proposicional para falsidade $\bot$.
   c) A predicado de identidade de dois lugares $=$.
   d) Um conjunto infinito enumerável de variáveis: $v_0$, $v_1$, $v_2$, ...
2. Símbolos não lógicos, que constituem a *linguagem padrão* da lógica de primeira ordem
   a) Um conjunto infinito enumerável de símbolos de predicado de $n$ lugares para cada $n > 0$: $A^n_0$, $A^n_1$, $A^n_2$, ...
   b) Um conjunto infinito enumerável de símbolos de constante: $c_0$, $c_1$, $c_2$, ....
   c) Um conjunto infinito enumerável de símbolos de função de $n$ lugares para cada $n > 0$: $f^n_0$, $f^n_1$, $f^n_2$, ...
3. Sinais de pontuação: (, ) e a vírgula.

A maioria de nossas definições e resultados será formulada para a linguagem padrão completa da lógica de primeira ordem. No entanto, dependendo da aplicação, também podemos restringir a linguagem a apenas alguns símbolos de predicado, símbolos de constante e símbolos de função.

**Exemplo 15.1.** A linguagem $\mathcal{L}_A$ da aritmética contém um único símbolo de predicado de dois lugares $<$, um único símbolo de constante $0$, um símbolo de função de um lugar $'$, e dois símbolos de função de dois lugares $+$ e $\times$.

**Exemplo 15.2.** A linguagem da teoria dos conjuntos $\mathcal{L}_Z$ contém apenas o único símbolo de predicado de dois lugares $\in$.

**Exemplo 15.3.** A linguagem das ordens $\mathcal{L}_\leq$ contém apenas o símbolo de predicado de dois lugares $\leq$.

Novamente, estas são convenções: oficialmente, estes são apenas apelidos, por exemplo, $<$, $\in$ e $\leq$ são apelidos para $A^2_0$, o para $c_0$, $'$ para $f^1_0$, $+$ para $f^2_0$, $\times$ para $f^2_1$.

Além dos conectivos primitivos e quantificadores introduzidos acima, também usamos os seguintes símbolos *definidos*: $\leftrightarrow$ (bicondicional), verdade $\top$

Um símbolo definido não faz parte oficialmente da linguagem, mas é introduzido como uma abreviação informal: ele nos permite abreviar fórmulas que, se usássemos apenas símbolos primitivos, ficariam bastante longas. Isso é obviamente uma vantagem. A maior vantagem, no entanto, é que as provas ficam mais curtas. Se um símbolo é primitivo, ele tem que ser tratado separadamente nas provas. Quanto mais símbolos primitivos, portanto, mais longas nossas provas.

Você pode estar familiarizado com terminologia e símbolos diferentes dos que usamos acima. Textos de lógica (e professores) comumente usam $\sim$, $\neg$, ou ! para "negação", $\wedge$, $\cdot$, ou & para "conjunção". Símbolos comumente usados para o "condicional" ou "implicação" são $\rightarrow$, $\Rightarrow$, e $\supset$. Símbolos para "bicondicional", "bi-implicação", ou "equivalência (material)" são $\leftrightarrow$, $\Leftrightarrow$, e $\equiv$. O símbolo $\bot$ é chamado de várias formas: "falsidade", "falsum", "absurdo", ou "bottom". O símbolo $\top$ é chamado de várias formas: "verdade", "verum", ou "top".

É convencional usar letras minúsculas (por exemplo, $a$, $b$, $c$) do início do alfabeto latino para símbolos de constante (às vezes chamados de nomes), e letras minúsculas do final (por exemplo, $x$, $y$, $z$) para variáveis. Quantificadores combinam-se com variáveis, por exemplo, $x$; variações notacionais incluem $\forall x$, $(\forall x)$, $(x)$, $\Pi x$, $\bigwedge_x$ para o quantificador universal e $\exists x$, $(\exists x)$, $(Ex)$, $\Sigma x$, $\bigvee_x$ para o quantificador existencial.

Poderíamos tratar todos os operadores proposicionais e ambos os quantificadores como símbolos primitivos da linguagem. Poderíamos, em vez disso, escolher um estoque menor de símbolos primitivos e tratar os outros operadores lógicos como definidos. Conjuntos "funcionalmente completos para a verdade" de operadores booleanos incluem $\{\neg, \vee\}$, $\{\neg, \wedge\}$, e $\{\neg, \rightarrow\}$—estes podem ser combinados com qualquer um dos quantificadores para uma linguagem de primeira ordem expressivamente completa.

Você pode estar familiarizado com dois outros operadores lógicos: a barra de Sheffer $|$ (em homenagem a Henry Sheffer), e a seta de Peirce $\downarrow$, também conhecida como adaga de Quine. Quando recebem suas leituras usuais de "nand" e "nor" (respectivamente), esses operadores são funcionalmente completos para a verdade por si sós.

## 15.3 Termos e Fórmulas

Uma vez dada uma linguagem de primeira ordem $\mathcal{L}$, podemos definir expressões construídas a partir do vocabulário básico de $\mathcal{L}$. Estas incluem, em

particular, *termos* e *fórmulas*.

**Definição 15.4 (Termos).** O conjunto de *termos* $\mathrm{Trm}(\mathcal{L})$ de $\mathcal{L}$ é definido indutivamente por:

1. Toda variável é um termo.
2. Todo símbolo de constante de $\mathcal{L}$ é um termo.
3. Se $f$ é um símbolo de função de $n$ lugares e $t_1, \ldots, t_n$ são termos, então $f(t_1, \ldots, t_n)$ é um termo.
4. Nada mais é um termo.

Um termo que não contém variáveis é um *termo fechado*.

Os símbolos de constante aparecem em nossa especificação da linguagem e dos termos como uma categoria separada de símbolos, mas eles poderiam, em vez disso, ter sido incluídos como símbolos de função de zero lugares. Poderíamos então dispensar a segunda cláusula da definição de termos. Bastaria entender $f(t_1, \ldots, t_n)$ como apenas $f$ sozinho se $n = 0$.

**Definição 15.5 (Fórmulas).** O conjunto de *fórmulas* $\mathrm{Frm}(\mathcal{L})$ da linguagem $\mathcal{L}$ é definido indutivamente como segue:

1. $\bot$ é uma fórmula atômica.
2. Se $R$ é um símbolo de predicado de $n$ lugares de $\mathcal{L}$ e $t_1, \ldots, t_n$ são termos de $\mathcal{L}$, então $R(t_1, \ldots, t_n)$ é uma fórmula atômica.
3. Se $t_1$ e $t_2$ são termos de $\mathcal{L}$, então $=(t_1, t_2)$ é uma fórmula atômica.
4. Se $\varphi$ é a fórmula, então $\neg\varphi$ é a fórmula.
5. Se $\varphi$ e $\psi$ são fórmulas, então $(\varphi \wedge \psi)$ é a fórmula.
6. Se $\varphi$ e $\psi$ são fórmulas, então $(\varphi \vee \psi)$ é a fórmula.
7. Se $\varphi$ e $\psi$ são fórmulas, então $(\varphi \to \psi)$ é a fórmula.
8. Se $\varphi$ é a fórmula e $x$ é a variável, então $\forall x\, \varphi$ é a fórmula.
9. Se $\varphi$ é a fórmula e $x$ é a variável, então $\exists x\, \varphi$ é a fórmula.
10. Nada mais é a fórmula.

As definições do conjunto de termos e do conjunto de fórmulas são *definições indutivas*. Essencialmente, construímos o conjunto de fórmulas em infinitos estágios. No estágio inicial, declaramos que todas as fórmulas atômicas

são fórmulas; isso corresponde aos primeiros casos da definição, isto é, os casos para $\bot$, $R(t_1, \ldots, t_n)$ e $=(t_1, t_2)$. "Fórmula atômica" significa, portanto, qualquer fórmula desta forma.

Os outros casos da definição dão regras para construir novas fórmulas a partir de fórmulas já construídas. No segundo estágio, podemos usá-los para construir fórmulas a partir de fórmulas atômicas. No terceiro estágio, construímos novas fórmulas a partir das fórmulas atômicas e daquelas obtidas no segundo estágio, e assim por diante. Uma fórmula é qualquer coisa que seja eventualmente construída em tal estágio, e nada mais.

Por convenção, escrevemos $=$ entre seus argumentos e omitimos os parênteses: $t_1 = t_2$ é uma abreviação para $=(t_1, t_2)$. Além disso, $\neg=(t_1, t_2)$ é abreviado como $t_1 \neq t_2$. Ao escrever uma fórmula $(\psi * \chi)$ construída a partir de $\psi$, $\chi$ usando um conectivo de dois lugares $*$, frequentemente omitiremos o par de parênteses mais externo e escreveremos simplesmente $\psi * \chi$.

Alguns textos de lógica exigem que a variável $x$ deva ocorrer em $\varphi$ para que $\exists x\, \varphi$ e $\forall x\, \varphi$ contem como fórmulas. Nada de ruim acontece se você não exigir isso, e isso torna as coisas mais fáceis.

**Definição 15.6.** As fórmulas construídas usando os operadores definidos devem ser entendidas como segue:

1. $\top$ abrevia $\neg\bot$.
2. $\varphi \leftrightarrow \psi$ abrevia $(\varphi \to \psi) \wedge (\psi \to \varphi)$.

Se trabalhamos em uma linguagem para uma aplicação específica, frequentemente escreveremos símbolos de predicado e símbolos de função de dois lugares entre os respectivos termos, por exemplo, $t_1 < t_2$ e $(t_1 + t_2)$ na linguagem da aritmética e $t_1 \in t_2$ na linguagem da teoria dos conjuntos. A função sucessora na linguagem da aritmética é até escrita convencionalmente *depois* de seu argumento: $t'$. Oficialmente, no entanto, estas são apenas abreviações convencionais para $A^2_0(t_1, t_2)$, $f^2_0(t_1, t_2)$, $A^2_0(t_1, t_2)$ e $f^1_0(t)$, respectivamente.

**Definição 15.7 (Identidade sintática).** O símbolo $\equiv$ expressa a identidade sintática entre cadeias de símbolos, isto é, $\varphi \equiv \psi$ sse $\varphi$ e $\psi$ são cadeias de símbolos do mesmo comprimento e que contêm o mesmo símbolo em cada posição.

O símbolo $\equiv$ pode ser ladeado por cadeias obtidas por concatenação, por exemplo, $\varphi \equiv (\psi \vee \chi)$ significa: a cadeia de símbolos $\varphi$ é a mesma cadeia que aquela obtida concatenando um parêntese de abertura, a cadeia $\psi$, o símbolo $\vee$, a cadeia $\chi$, e um parêntese de fechamento, nesta ordem. Se este é o caso, então sabemos que o primeiro símbolo de $\varphi$ é um parêntese de abertura, $\varphi$ contém $\psi$ como uma subcadeia (começando no segundo símbolo), essa subcadeia é seguida por $\vee$, etc.

Como termos e fórmulas são construídos a partir de elementos básicos via definições indutivas, podemos usar os seguintes princípios de indução para provar coisas sobre eles.

**Lema 15.8 (*Princípio de indução sobre termos*).** *Seja $\mathcal{L}$ uma linguagem de primeira ordem. Se uma propriedade P é tal que*

1. *ela vale para toda variável $v$,*
2. *ela vale para todo símbolo de constante $a$ de $\mathcal{L}$, e*
3. *ela vale para $f(t_1, \ldots, t_n)$ sempre que vale para $t_1, \ldots, t_n$ e $f$ é um símbolo de função de $n$ lugares de $\mathcal{L}$*

*(supondo que $t_1, \ldots, t_n$ são termos de $\mathcal{L}$), então P vale para todo termo em* $\mathrm{Trm}(\mathcal{L})$.

**Lema 15.9 (*Princípio de indução sobre fórmulas*).** *Seja $\mathcal{L}$ uma linguagem de primeira ordem. Se uma propriedade P vale para todas as fórmulas atômicas e é tal que*

1. *ela vale para $\neg\varphi$ sempre que vale para $\varphi$;*
2. *ela vale para $(\varphi \wedge \psi)$ sempre que vale para $\varphi$ e $\psi$;*
3. *ela vale para $(\varphi \vee \psi)$ sempre que vale para $\varphi$ e $\psi$;*
4. *ela vale para $(\varphi \to \psi)$ sempre que vale para $\varphi$ e $\psi$;*
5. *ela vale para $\exists x\, \varphi$ sempre que vale para $\varphi$;*
6. *ela vale para $\forall x\, \varphi$ sempre que vale para $\varphi$;*

*(supondo que $\varphi$ e $\psi$ são fórmulas de $\mathcal{L}$), então P vale para todas as fórmulas em* $\mathrm{Frm}(\mathcal{L})$.

## 15.4 Leitura Única

A maneira como definimos fórmulas garante que toda fórmula tem uma *leitura única*, isto é, há essencialmente apenas uma maneira de construí-la de acordo com nossas regras de formação para fórmulas e apenas uma maneira de "interpretá-la". Se não fosse assim, teríamos fórmulas ambíguas, isto é, fórmulas que têm mais de uma leitura ou interpretação—e isso é claramente algo que queremos evitar. Mas, mais importante, sem essa propriedade, a maioria das definições e provas que vamos dar não funcionaria.

Talvez a melhor maneira de deixar isso claro seja ver o que aconteceria se tivéssemos dado regras ruins para formar fórmulas que não garantissem a leitura única. Por exemplo, poderíamos ter esquecido os parênteses nas regras de formação para conectivos, por exemplo, poderíamos ter permitido isto:

> Se $\varphi$ e $\psi$ são fórmulas, então $\varphi \to \psi$ também é.

Partindo de uma fórmula atômica $\theta$, isso nos permitiria formar $\theta \to \theta$. A partir disso, juntamente com $\theta$, obteríamos $\theta \to \theta \to \theta$. Mas há duas maneiras de fazer isso:

1. Tomamos $\theta$ como $\varphi$ e $\theta \to \theta$ como $\psi$.
2. Tomamos $\varphi$ como $\theta \to \theta$ e $\psi$ é $\theta$.

Correspondentemente, há duas maneiras de "ler" a fórmula $\theta \to \theta \to \theta$. Ela é da forma $\psi \to \chi$ onde $\psi$ é $\theta$ e $\chi$ é $\theta \to \theta$, mas *ela é também* da forma $\psi \to \chi$ com $\psi$ sendo $\theta \to \theta$ e $\chi$ sendo $\theta$.

Se isso acontece, nossas definições nem sempre funcionarão. Por exemplo, quando definimos o operador principal de uma fórmula, dizemos: em uma fórmula da forma $\psi \to \chi$, o operador principal é a ocorrência indicada de $\to$. Mas se podemos casar a fórmula $\theta \to \theta \to \theta$ com $\psi \to \chi$ das duas maneiras diferentes mencionadas acima, então em um caso obtemos a primeira ocorrência de $\to$ como o operador principal, e no segundo caso a segunda ocorrência. Mas pretendemos que o operador principal seja uma *função* da fórmula, isto é, toda fórmula deve ter exatamente uma ocorrência de operador principal.

**Lema 15.10.** *O número de parênteses esquerdos e direitos em a fórmula $\varphi$ é igual.*

*Prova.* Provamos isso por indução sobre a maneira como $\varphi$ é construída. Isso requer duas coisas: (a) Temos primeiro que provar que todas as fórmulas atômicas têm a propriedade em questão (a base da indução). (b) Então temos que provar que, quando construímos novas fórmulas a partir de fórmulas dadas, as novas fórmulas têm a propriedade, desde que as antigas a tenham.

Seja $l(\varphi)$ o número de parênteses esquerdos, e $r(\varphi)$ o número de parênteses direitos em $\varphi$, e $l(t)$ e $r(t)$ similarmente o número de parênteses esquerdos e direitos em um termo $t$.

1. $\varphi \equiv \bot$: $\varphi$ tem 0 parênteses esquerdos e 0 parênteses direitos.
2. $\varphi \equiv R(t_1, \ldots, t_n)$: $l(\varphi) = 1 + l(t_1) + \cdots + l(t_n) = 1 + r(t_1) + \cdots + r(t_n) = r(\varphi)$. Aqui usamos o fato, deixado como exercício, de que $l(t) = r(t)$ para qualquer termo $t$.
3. $\varphi \equiv t_1 = t_2$: $l(\varphi) = l(t_1) + l(t_2) = r(t_1) + r(t_2) = r(\varphi)$.
4. $\varphi \equiv \neg\psi$: Por hipótese de indução, $l(\psi) = r(\psi)$. Assim $l(\varphi) = l(\psi) = r(\psi) = r(\varphi)$.
5. $\varphi \equiv (\psi * \chi)$: Por hipótese de indução, $l(\psi) = r(\psi)$ e $l(\chi) = r(\chi)$. Assim $l(\varphi) = 1 + l(\psi) + l(\chi) = 1 + r(\psi) + r(\chi) = r(\varphi)$.
6. $\varphi \equiv \forall x\, \psi$: Por hipótese de indução, $l(\psi) = r(\psi)$. Assim, $l(\varphi) = l(\psi) = r(\psi) = r(\varphi)$.

7. $\varphi \equiv \exists x\, \psi$: Analogamente. □

**Definição 15.11 (Prefixo próprio).** Uma cadeia de símbolos $\psi$ é um *prefixo próprio* de uma cadeia de símbolos $\varphi$ se a concatenação de $\psi$ e uma cadeia de símbolos não vazia resulta em $\varphi$.

**Lema 15.12.** *Se $\varphi$ é a fórmula, e $\psi$ é um prefixo próprio de $\varphi$, então $\psi$ não é a fórmula.*

*Prova.* Exercício. □

**Proposição 15.13.** *Se $\varphi$ é uma fórmula atômica, então ela satisfaz uma, e apenas uma, das seguintes condições.*

1. $\varphi \equiv \bot$.
2. $\varphi \equiv R(t_1, \ldots, t_n)$ *onde $R$ é um símbolo de predicado de $n$ lugares, $t_1, \ldots, t_n$ são termos, e cada um de $R, t_1, \ldots, t_n$ é determinado de forma única.*
3. $\varphi \equiv t_1 = t_2$ *onde $t_1$ e $t_2$ são termos determinados de forma única.*

*Prova.* Exercício. □

**Proposição 15.14 (Leitura Única).** *Toda fórmula satisfaz uma, e apenas uma, das seguintes condições.*

1. *$\varphi$ é atômica.*
2. *$\varphi$ é da forma $\neg\psi$.*
3. *$\varphi$ é da forma $(\psi \wedge \chi)$.*
4. *$\varphi$ é da forma $(\psi \vee \chi)$.*
5. *$\varphi$ é da forma $(\psi \to \chi)$.*
6. *$\varphi$ é da forma $\forall x\, \psi$.*
7. *$\varphi$ é da forma $\exists x\, \psi$.*

*Além disso, em cada caso $\psi$, ou $\psi$ e $\chi$, são determinados de forma única. Isso significa que, por exemplo, não há pares diferentes $\psi$, $\chi$ e $\psi'$, $\chi'$ tais que $\varphi$ seja ao mesmo tempo da forma $(\psi \to \chi)$ e $(\psi' \to \chi')$.*

*Prova.* As regras de formação exigem que, se a fórmula não é atômica, ela deve começar com um parêntese de abertura (, $\neg$, ou um quantificador. Por outro lado, toda fórmula que começa com um dos seguintes símbolos deve ser atômica: a símbolo de predicado, a símbolo de função, a símbolo de constante, $\bot$.

Então, na verdade só temos que mostrar que se $\varphi$ é da forma $(\psi * \chi)$ e também da forma $(\psi' *' \chi')$, então $\psi \equiv \psi'$, $\chi \equiv \chi'$, e $* = *'$.

Então suponha que tanto $\varphi \equiv (\psi * \chi)$ quanto $\varphi \equiv (\psi' *' \chi')$. Então ou $\psi \equiv \psi'$ ou não. Se for, claramente $* = *'$ e $\chi \equiv \chi'$, pois elas então são subcadeias de $\varphi$ que começam no mesmo lugar e têm o mesmo comprimento. O outro caso é $\psi \not\equiv \psi'$. Como $\psi$ e $\psi'$ são ambas subcadeias de $\varphi$ que começam no mesmo lugar, uma deve ser um prefixo próprio da outra. Mas isso é impossível por Lema 15.12. □

## 15.5 Operador principal de uma Fórmula

Frequentemente é útil falar sobre o último operador usado na construção de a fórmula $\varphi$. Esse operador é chamado de *operador principal* de $\varphi$. Intuitivamente, é o operador "mais externo" de $\varphi$. Por exemplo, o operador principal de $\neg\varphi$ é $\neg$, o operador principal de $(\varphi \vee \psi)$ é $\vee$, etc.

**Definição 15.15 (Operador principal).** O *operador principal* de a fórmula $\varphi$ é definido como segue:

1. $\varphi$ is atomic: $\varphi$ não tem operador principal.
2. $\varphi \equiv \neg\psi$: o operador principal de $\varphi$ é $\neg$.
3. $\varphi \equiv (\psi \wedge \chi)$: o operador principal de $\varphi$ é $\wedge$.
4. $\varphi \equiv (\psi \vee \chi)$: o operador principal de $\varphi$ é $\vee$.
5. $\varphi \equiv (\psi \to \chi)$: o operador principal de $\varphi$ é $\to$.
6. $\varphi \equiv \forall x\, \psi$: o operador principal de $\varphi$ é $\forall$.
7. $\varphi \equiv \exists x\, \psi$: o operador principal de $\varphi$ é $\exists$.

Em cada caso, pretendemos a *ocorrência* específica indicada do operador principal na fórmula. Por exemplo, como a fórmula $((\theta \to \alpha) \to (\alpha \to \theta))$ é da forma $(\psi \to \chi)$ onde $\psi$ é $(\theta \to \alpha)$ e $\chi$ é $(\alpha \to \theta)$, a segunda ocorrência de $\to$ é o operador principal.

Esta é uma definição *recursiva* de uma função que mapeia todas as fórmulas não atômicas para sua ocorrência de operador principal. Por causa da maneira como as fórmulas são definidas indutivamente, toda fórmula $\varphi$ satisfaz um dos casos em Definição 15.15. Isso garante que, para cada fórmula $\varphi$ não atômica, existe um operador principal. Como cada fórmula satisfaz apenas uma dessas condições, e como as fórmulas menores a partir das quais $\varphi$ é construída são determinadas de forma única em cada caso, a ocorrência de operador principal de $\varphi$ é única, e assim definimos uma função.

Chamamos as fórmulas pelos nomes em Tabela 15.1 dependendo de qual símbolo é seu operador principal. Lembre-se, no entanto, de que os operadores definidos não aparecem oficialmente em fórmulas. Eles são apenas abreviações, então oficialmente não podem ser o operador principal de uma fórmula. Em provas sobre todas as fórmulas, eles, portanto, não precisam ser tratados separadamente.

| Operador principal | Tipo de fórmula | Exemplo |
|---|---|---|
| nenhum | (fórmula) atômica | $\bot$, $R(t_1, \ldots, t_n)$, $t_1 = t_2$ |
| $\neg$ | negação | $\neg\varphi$ |
| $\wedge$ | conjunção | $(\varphi \wedge \psi)$ |
| $\vee$ | disjunção | $(\varphi \vee \psi)$ |
| $\rightarrow$ | condicional | $(\varphi \rightarrow \psi)$ |
| $\leftrightarrow$ | bicondicional | $(\varphi \leftrightarrow \psi)$ |
| $\forall$ | (fórmula) universal | $\forall x\, \varphi$ |
| $\exists$ | (fórmula) existencial | $\exists x\, \varphi$ |

Tabela 15.1: Operador principal e nomes de fórmulas

## 15.6 Subfórmulas

Frequentemente é útil falar sobre as fórmulas que "compõem" uma dada fórmula. Chamamos estas de suas *subfórmulas*. Qualquer fórmula conta como a subfórmula de si mesma; uma subfórmula de $\varphi$ diferente do próprio $\varphi$ é uma *subfórmula própria*.

**Definição 15.16 (Subfórmula imediata).** Se $\varphi$ é a fórmula, as *subfórmulas imediatas* de $\varphi$ são definidas indutivamente como segue:

1. Fórmulas atômicas não têm subfórmulas imediatas.
2. $\varphi \equiv \neg\psi$: A única subfórmula imediata de $\varphi$ é $\psi$.
3. $\varphi \equiv (\psi * \chi)$: As subfórmulas imediatas de $\varphi$ são $\psi$ e $\chi$ ($*$ é qualquer um dos conectivos de dois lugares).
4. $\varphi \equiv \forall x\, \psi$: A única subfórmula imediata de $\varphi$ é $\psi$.
5. $\varphi \equiv \exists x\, \psi$: A única subfórmula imediata de $\varphi$ é $\psi$.

**Definição 15.17 (Subfórmula própria).** Se $\varphi$ é a fórmula, as *subfórmulas próprias* de $\varphi$ são definidas recursivamente como segue:

1. Fórmulas atômicas não têm subfórmulas próprias.
2. $\varphi \equiv \neg\psi$: As subfórmulas próprias de $\varphi$ são $\psi$ juntamente com todas as subfórmulas próprias de $\psi$.

3. $\varphi \equiv (\psi * \chi)$: As subfórmulas próprias de $\varphi$ são $\psi$, $\chi$, juntamente com todas as subfórmulas próprias de $\psi$ e as de $\chi$.

4. $\varphi \equiv \forall x\, \psi$: As subfórmulas próprias de $\varphi$ são $\psi$ juntamente com todas as subfórmulas próprias de $\psi$.

5. $\varphi \equiv \exists x\, \psi$: As subfórmulas próprias de $\varphi$ são $\psi$ juntamente com todas as subfórmulas próprias de $\psi$.

**Definição 15.18 (Subfórmula).** As subfórmulas de $\varphi$ são o próprio $\varphi$ juntamente com todas as suas subfórmulas próprias.

Note a diferença sutil em como definimos subfórmulas imediatas e subfórmulas próprias. No primeiro caso, definimos diretamente as subfórmulas imediatas de uma fórmula $\varphi$ para cada forma possível de $\varphi$. É uma definição explícita por casos, e os casos espelham a definição indutiva do conjunto de fórmulas. No segundo caso, também espelhamos a maneira como o conjunto de todas as fórmulas é definido, mas em cada caso também incluímos as subfórmulas próprias das fórmulas menores $\psi$, $\chi$ além dessas próprias fórmulas. Isso torna a definição *recursiva*. Em geral, uma definição de uma função sobre um conjunto definido indutivamente (no nosso caso, fórmulas) é recursiva se os casos na definição da função fazem uso da própria função. Para ser bem definida, devemos garantir, no entanto, que só usamos os valores da função para argumentos que vêm "antes" daquele que estamos definindo—no nosso caso, ao definir "subfórmula própria" para $(\psi * \chi)$ usamos apenas as subfórmulas próprias das fórmulas "anteriores" $\psi$ e $\chi$.

**Proposição 15.19.** *Suponha que $\psi$ é uma subfórmula de $\varphi$ e $\chi$ é uma subfórmula de $\psi$. Então $\chi$ é uma subfórmula de $\varphi$. Em outras palavras, a relação de subfórmula é transitiva.*

**Proposição 15.20.** *Suponha que $\varphi$ é uma fórmula com $n$ conectivos e quantificadores. Então $\varphi$ tem no máximo $2n + 1$ subfórmulas.*

## 15.7 Sequências de Formação

Definir fórmulas via uma definição indutiva, e a técnica complementar de provar propriedades de fórmulas via indução, é uma abordagem elegante e eficiente. No entanto, também pode ser útil considerar uma abordagem mais ascendente, passo a passo, da construção de fórmulas, o que fazemos aqui usando a noção de uma *sequência de formação*. Para mostrar como termos e fórmulas podem ser introduzidos dessa maneira sem precisar referir-se a suas definições indutivas, primeiro introduzimos a noção de uma cadeia arbitrária de símbolos extraída de alguma linguagem $\mathcal{L}$.

**Definição 15.21 (Cadeias).** Suponha que $\mathcal{L}$ é uma linguagem de primeira ordem. Uma *$\mathcal{L}$-cadeia* é uma sequência finita de símbolos de $\mathcal{L}$. Quando a linguagem $\mathcal{L}$ está claramente fixada pelo contexto, frequentemente nos referiremos a uma $\mathcal{L}$-cadeia simplesmente como uma *cadeia*.

**Exemplo 15.22.** Para qualquer linguagem de primeira ordem $\mathcal{L}$, todas as $\mathcal{L}$-fórmulas são $\mathcal{L}$-cadeias, mas não reciprocamente. Por exemplo,

$$)(v_0 \to \exists$$

é uma $\mathcal{L}$-cadeia mas não uma $\mathcal{L}$-fórmula.

**Definição 15.23 (Sequências de formação para termos).** Uma sequência finita de $\mathcal{L}$-cadeias $\langle t_0, \ldots, t_n \rangle$ é uma *sequência de formação* para um termo $t$ se $t \equiv t_n$ e para todo $i \leq n$, ou $t_i$ é a variável ou a símbolo de constante, ou $\mathcal{L}$ contém um símbolo de função $f$ $k$-ário e existem $m_0, \ldots, m_k < i$ tais que $t_i \equiv f(t_{m_0}, \ldots, t_{m_k})$. Quando for necessário distinguir, nos referiremos às sequências de formação para termos como *sequências de formação de termos*.

**Exemplo 15.24.** A sequência

$$\langle c_0, v_0, f_0^2(c_0, v_0), f_0^1(f_0^2(c_0, v_0)) \rangle$$

é uma sequência de formação para o termo $f_0^1(f_0^2(c_0, v_0))$, assim como

$$\langle v_0, c_0, f_0^2(c_0, v_0), f_0^1(f_0^2(c_0, v_0)) \rangle.$$

**Definição 15.25 (Sequências de formação para fórmulas).** Uma sequência finita de $\mathcal{L}$-cadeias $\langle \varphi_0, \ldots, \varphi_n \rangle$ é uma *sequência de formação* para $\varphi$ se $\varphi \equiv \varphi_n$ e para todo $i \leq n$, ou $\varphi_i$ é uma fórmula atômica ou existem $j, k < i$ e a variável $x$ tais que uma das seguintes condições vale:

1. $\varphi_i \equiv \neg \varphi_j$.
2. $\varphi_i \equiv (\varphi_j \wedge \varphi_k)$.
3. $\varphi_i \equiv (\varphi_j \vee \varphi_k)$.
4. $\varphi_i \equiv (\varphi_j \to \varphi_k)$.
5. $\varphi_i \equiv \forall x \, \varphi_j$.
6. $\varphi_i \equiv \exists x \, \varphi_j$.

Quando for necessário distinguir, nos referiremos às sequências de formação para fórmulas como *sequências de formação de fórmulas*.

**Exemplo 15.26.**

$$\langle A^1_0(v_0), A^1_1(c_1), (A^1_1(c_1) \land A^1_0(v_0)), \exists v_0\, (A^1_1(c_1) \land A^1_0(v_0))\rangle$$

é uma sequência de formação de $\exists v_0\, (A^1_1(c_1) \land A^1_0(v_0))$, assim como

$$\langle A^1_0(v_0), A^1_1(c_1), (A^1_1(c_1) \land A^1_0(v_0)), A^1_1(c_1), \forall v_1\, A^1_0(v_0), \exists v_0\, (A^1_1(c_1) \land A^1_0(v_0))\rangle.$$

Como pode ser visto no segundo exemplo, sequências de formação podem conter "lixo": fórmulas que são redundantes ou não contribuem para a construção.

**Proposição 15.27.** *Toda fórmula $\varphi$ em $\mathrm{Frm}(\mathcal{L})$ tem uma sequência de formação.*

*Prova.* Suponha que $\varphi$ é atômica. Então a sequência $\langle\varphi\rangle$ é uma sequência de formação para $\varphi$. Agora suponha que $\psi$ e $\chi$ têm sequências de formação $\langle\psi_0, \ldots, \psi_n\rangle$ e $\langle\chi_0, \ldots, \chi_m\rangle$ respectivamente.

1. Se $\varphi \equiv \neg\psi$, então $\langle\psi_0, \ldots, \psi_n, \neg\psi_n\rangle$ é uma sequência de formação para $\varphi$.
2. Se $\varphi \equiv (\psi \land \chi)$, então $\langle\psi_0, \ldots, \psi_n, \chi_0, \ldots, \chi_m, (\psi_n \land \chi_m)\rangle$ é uma sequência de formação para $\varphi$.
3. Se $\varphi \equiv (\psi \lor \chi)$, então $\langle\psi_0, \ldots, \psi_n, \chi_0, \ldots, \chi_m, (\psi_n \lor \chi_m)\rangle$ é uma sequência de formação para $\varphi$.
4. Se $\varphi \equiv (\psi \to \chi)$, então $\langle\psi_0, \ldots, \psi_n, \chi_0, \ldots, \chi_m, (\psi_n \to \chi_m)\rangle$ é uma sequência de formação para $\varphi$.
5. Se $\varphi \equiv \forall x\, \psi$, então $\langle\psi_0, \ldots, \psi_n, \forall x\, \psi_n\rangle$ é uma sequência de formação para $\varphi$.
6. Se $\varphi \equiv \exists x\, \psi$, então $\langle\psi_0, \ldots, \psi_n, \exists x\, \psi_n\rangle$ é uma sequência de formação para $\varphi$.

Pelo princípio de indução sobre fórmulas, toda fórmula tem uma sequência de formação. □

Também podemos provar a recíproca. Isso é importante porque mostra que nossas duas maneiras de definir fórmulas são equivalentes: elas dão os mesmos resultados. Isso também significa que podemos provar teoremas sobre fórmulas usando indução ordinária sobre o comprimento das sequências de formação.

**Lema 15.28.** *Suponha que $\langle\varphi_0, \ldots, \varphi_n\rangle$ é uma sequência de formação para $\varphi_n$, e que $k \leq n$. Então $\langle\varphi_0, \ldots, \varphi_k\rangle$ é uma sequência de formação para $\varphi_k$.*

*Prova.* Exercício. □

**Teorema 15.29.** $\mathrm{Frm}(\mathcal{L})$ *é o conjunto de todas as* $\mathcal{L}$*-cadeias* $\varphi$ *tais que existe uma sequência de formação de fórmulas para* $\varphi$*.*

*Prova.* Seja $F$ o conjunto de todas as cadeias de símbolos na linguagem $\mathcal{L}$ que têm uma sequência de formação. Vimos em Proposição 15.27 que $\mathrm{Frm}(\mathcal{L}) \subseteq F$, então agora provamos a recíproca.

Suponha que $\varphi$ tem uma sequência de formação $\langle \varphi_0, \ldots, \varphi_n \rangle$. Provamos que $\varphi \in \mathrm{Frm}(\mathcal{L})$ por indução forte sobre $n$. Nossa hipótese de indução é que toda cadeia de símbolos com uma sequência de formação de comprimento $m < n$ está em $\mathrm{Frm}(\mathcal{L})$. Pela definição de uma sequência de formação, ou $\varphi \equiv \varphi_n$ é atômica ou devem existir $j, k < n$ tais que um dos seguintes casos vale:

1. $\varphi \equiv \neg\varphi_j$.
2. $\varphi \equiv (\varphi_j \wedge \varphi_k)$.
3. $\varphi \equiv (\varphi_j \vee \varphi_k)$.
4. $\varphi \equiv (\varphi_j \to \varphi_k)$.
5. $\varphi \equiv \forall x\, \varphi_j$.
6. $\varphi \equiv \exists x\, \varphi_j$.

Agora raciocinamos por casos. Se $\varphi$ é atômica então $\varphi_n \in \mathrm{Frm}(\mathcal{L}_0)$. Suponha, em vez disso, que $\varphi \equiv (\varphi_j \wedge \varphi_k)$. Por Lema 15.28, $\langle \varphi_0, \ldots, \varphi_j \rangle$ e $\langle \varphi_0, \ldots, \varphi_k \rangle$ são sequências de formação para $\varphi_j$ e $\varphi_k$, respectivamente. Como estas são subsequências iniciais próprias da sequência de formação para $\varphi$, ambas têm comprimento menor que $n$. Portanto, pela hipótese de indução, $\varphi_j$ e $\varphi_k$ estão em $\mathrm{Frm}(\mathcal{L}_0)$, e pela definição de a fórmula, $(\varphi_j \wedge \varphi_k)$ também está. Os outros casos seguem por raciocínio análogo. □

Sequências de formação para termos têm propriedades semelhantes às das fórmulas.

**Proposição 15.30.** $\mathrm{Trm}(\mathcal{L})$ *é o conjunto de todas as* $\mathcal{L}$*-cadeias* $t$ *tais que existe uma sequência de formação de termos para* $t$*.*

*Prova.* Exercício. □

Há dois tipos de "lixo" que podem aparecer em sequências de formação: elementos repetidos, e elementos que são irrelevantes para a construção da fórmula ou termo. Podemos eliminar ambos olhando para sequências de formação mínimas.

**Definição 15.31 (Sequências de formação mínimas).** Uma sequência de formação $\langle \varphi_0, \ldots, \varphi_n \rangle$ para uma fórmula $\varphi$ é uma *sequência de formação mínima* para $\varphi$ se, para toda outra sequência de formação $s$ para $\varphi$, o comprimento de $s$ é maior ou igual a $n+1$.

Similarmente, uma sequência de formação $\langle t_0, \ldots, t_n \rangle$ para um termo $t$ é uma *sequência de formação mínima* para $t$ se, para toda outra sequência de formação $s$ para $t$, o comprimento de $s$ é maior ou igual a $n+1$.

Note que uma fórmula ou termo pode ter mais de uma sequência de formação mínima, mas elas conterão exatamente as mesmas cadeias.

**Proposição 15.32.** *As seguintes condições são equivalentes:*

1. *$\psi$ é uma sub-fórmula de $\varphi$.*
2. *$\psi$ ocorre em toda sequência de formação de $\varphi$.*
3. *$\psi$ ocorre em uma sequência de formação mínima de $\varphi$.*

*Prova.* Exercício. □

**Observações históricas** Sequências de formação foram introduzidas por Raymond Smullyan em seu livro-texto *First-Order Logic* (Smullyan, 1968). Propriedades adicionais de sequências de formação foram estabelecidas por Zuckerman (1973).

## 15.8 Variáveis Livres e Sentenças

**Definição 15.33 (Ocorrências livres de a variável).** As ocorrências *livres* de a variável em a fórmula são definidas indutivamente como segue:

1. $\varphi$ is atomic: todas as ocorrências de variável em $\varphi$ são livres.
2. $\varphi \equiv \neg\psi$: as ocorrências livres de variável de $\varphi$ são exatamente as de $\psi$.
3. $\varphi \equiv (\psi * \chi)$: as ocorrências livres de variável de $\varphi$ são as em $\psi$ juntamente com as em $\chi$.
4. $\varphi \equiv \forall x\, \psi$: as ocorrências livres de variável em $\varphi$ são todas as em $\psi$ exceto as ocorrências de $x$.
5. $\varphi \equiv \exists x\, \psi$: as ocorrências livres de variável em $\varphi$ são todas as em $\psi$ exceto as ocorrências de $x$.

**Definição 15.34 (Variáveis Ligadas).** Uma ocorrência de a variável em uma fórmula $\varphi$ é *ligada* se não é livre.

**Definição 15.35 (Escopo).** Se $\forall x\, \psi$ é uma ocorrência de uma subfórmula em uma fórmula $\varphi$, então a ocorrência correspondente de $\psi$ em $\varphi$ é chamada de *escopo* da ocorrência correspondente de $\forall x$. Analogamente para $\exists x$.

Se $\psi$ é o escopo de uma ocorrência de quantificador $\forall x$ ou $\exists x$ em $\varphi$, então as ocorrências livres de $x$ em $\psi$ são ligadas em $\forall x\, \psi$ e $\exists x\, \psi$. Dizemos que essas ocorrências são *ligadas pela* ocorrência de quantificador mencionada.

**Exemplo 15.36.** Considere a seguinte fórmula:

$$\exists v_0\ \underbrace{A_0^2(v_0, v_1)}_{\psi}$$

$\psi$ representa o escopo de $\exists v_0$. O quantificador liga a ocorrência de $v_0$ em $\psi$, mas não liga a ocorrência de $v_1$. Então $v_1$ é uma variável livre neste caso.

Agora podemos ver como isso poderia funcionar em uma fórmula $\varphi$ mais complicada:

$$\forall v_0\ \underbrace{(A_0^1(v_0) \to A_0^2(v_0, v_1))}_{\psi} \to \exists v_1\ \underbrace{(A_1^2(v_0, v_1) \vee \forall v_0\ \overbrace{\neg A_1^1(v_0)}^{\theta})}_{\chi}$$

$\psi$ é o escopo do primeiro $\forall v_0$, $\chi$ é o escopo de $\exists v_1$, e $\theta$ é o escopo do segundo $\forall v_0$. O primeiro $\forall v_0$ liga as ocorrências de $v_0$ em $\psi$, $\exists v_1$ liga a ocorrência de $v_1$ em $\chi$, e o segundo $\forall v_0$ liga a ocorrência de $v_0$ em $\theta$. A primeira ocorrência de $v_1$ e a quarta ocorrência de $v_0$ são livres em $\varphi$. A última ocorrência de $v_0$ é livre em $\theta$, mas ligada em $\chi$ e $\varphi$.

**Definição 15.37 (Sentença).** A fórmula $\varphi$ é a *sentença* sse não contém ocorrências livres de variáveis.

## 15.9 Substituição

**Definição 15.38 (Substituição em um termo).** Definimos $s[t/x]$, o resultado de *substituir* $t$ por toda ocorrência de $x$ em $s$, recursivamente:

1. $s \equiv c$: $s[t/x]$ é simplesmente $s$.
2. $s \equiv y$: $s[t/x]$ é também simplesmente $s$, desde que $y$ seja uma variável e $y \not\equiv x$.
3. $s \equiv x$: $s[t/x]$ é $t$.
4. $s \equiv f(t_1, \ldots, t_n)$: $s[t/x]$ é $f(t_1[t/x], \ldots, t_n[t/x])$.

**Definição 15.39.** Um termo $t$ está *livre para* $x$ em $\varphi$ se nenhuma das ocorrências livres de $x$ em $\varphi$ ocorre no escopo de um quantificador que liga uma variável em $t$.

**Exemplo 15.40.**

1. $v_8$ está livre para $v_1$ em $\exists v_3 A_4^2(v_3, v_1)$
2. $f_1^2(v_1, v_2)$ *não* está livre para $v_0$ em $\forall v_2 A_4^2(v_0, v_2)$

**Definição 15.41 (Substituição em a fórmula).** Se $\varphi$ é a fórmula, $x$ é a variável, e $t$ é um termo livre para $x$ em $\varphi$, então $\varphi[t/x]$ é o resultado de substituir $t$ por todas as ocorrências livres de $x$ em $\varphi$.

1. $\varphi \equiv \bot$: $\varphi[t/x]$ é $\bot$.
2. $\varphi \equiv P(t_1, \ldots, t_n)$: $\varphi[t/x]$ é $P(t_1[t/x], \ldots, t_n[t/x])$.
3. $\varphi \equiv t_1 = t_2$: $\varphi[t/x]$ é $t_1[t/x] = t_2[t/x]$.
4. $\varphi \equiv \neg\psi$: $\varphi[t/x]$ é $\neg\psi[t/x]$.
5. $\varphi \equiv (\psi \wedge \chi)$: $\varphi[t/x]$ é $(\psi[t/x] \wedge \chi[t/x])$.
6. $\varphi \equiv (\psi \vee \chi)$: $\varphi[t/x]$ é $(\psi[t/x] \vee \chi[t/x])$.
7. $\varphi \equiv (\psi \to \chi)$: $\varphi[t/x]$ é $(\psi[t/x] \to \chi[t/x])$.
8. $\varphi \equiv \forall y\, \psi$: $\varphi[t/x]$ é $\forall y\, \psi[t/x]$, desde que $y$ seja uma variável diferente de $x$; caso contrário $\varphi[t/x]$ é simplesmente $\varphi$.
9. $\varphi \equiv \exists y\, \psi$: $\varphi[t/x]$ é $\exists y\, \psi[t/x]$, desde que $y$ seja uma variável diferente de $x$; caso contrário $\varphi[t/x]$ é simplesmente $\varphi$.

Note que a substituição pode ser vácua: Se $x$ não ocorre de modo algum em $\varphi$, então $\varphi[t/x]$ é simplesmente $\varphi$.

A restrição de que $t$ deve estar livre para $x$ em $\varphi$ é necessária para excluir casos como o seguinte. Se $\varphi \equiv \exists y\, x < y$ e $t \equiv y$, então $\varphi[t/x]$ seria $\exists y\, y < y$. Neste caso a variável livre $y$ é "capturada" pelo quantificador $\exists y$ ao substituir, e isso é indesejável. Por exemplo, gostaríamos que fosse o caso que, sempre que $\forall x\, \psi$ vale, $\psi[t/x]$ também vale. Mas considere $\forall x \exists y\, x < y$ (aqui $\psi$ é $\exists y\, x < y$). É uma sentença que é verdadeira a respeito, por exemplo, dos números naturais: para todo número $x$ há um número $y$ maior que ele. Se permitíssemos $y$ como uma possível substituição para $x$, terminaríamos com $\psi[y/x] \equiv \exists y\, y < y$, que é falsa. Prevenimos isso exigindo que nenhuma das variáveis livres em $t$ acabe sendo ligada por um quantificador em $\varphi$.

Frequentemente usamos a seguinte convenção para evitar notação incômoda: Se $\varphi$ é a fórmula que pode conter a variável $x$ livre, também escrevemos $\varphi(x)$ para indicar isso. Quando está claro qual $\varphi$ e $x$ temos em mente, e $t$ é um termo (suposto estar livre para $x$ em $\varphi(x)$), então escrevemos $\varphi(t)$ como abreviação de $\varphi[t/x]$. Assim, por exemplo, poderíamos dizer, "chamamos $\varphi(t)$ de uma instância de $\forall x\, \varphi(x)$." Com isso queremos dizer que se $\varphi$ é qualquer fórmula, $x$ a variável, e $t$ um termo que está livre para $x$ em $\varphi$, então $\varphi[t/x]$ é uma instância de $\forall x\, \varphi$.

## Problemas

**Problema 15.1.** Prove Lema 15.8.

**Problema 15.2.** Prove que, para qualquer termo $t$, $l(t) = r(t)$.

**Problema 15.3.** Prove Lema 15.12.

**Problema 15.4.** Prove Proposição 15.13 (Dica: Formule e prove uma versão de Lema 15.12 para termos.)

**Problema 15.5.** Prove Proposição 15.19.

**Problema 15.6.** Prove Proposição 15.20.

**Problema 15.7.** Prove Lema 15.28.

**Problema 15.8.** Prove Proposição 15.30. Dica: use uma estratégia semelhante à usada na prova de Teorema 15.29.

**Problema 15.9.** Prove Proposição 15.32.

**Problema 15.10.** Dê uma definição indutiva das ocorrências de variáveis ligadas nos moldes de Definição 15.33.

# Capítulo 16

# Semântica da Lógica de Primeira Ordem

## 16.1 Introdução

Dar o significado das expressões é o domínio da semântica. O conceito central em semântica é o de satisfação em a estrutura. A estrutura dá significado aos blocos de construção da linguagem: a domínio é um conjunto não vazio de objetos. Os quantificadores são interpretados como variando sobre esse domínio, aos símbolos de constante são atribuídos elementos no domínio, aos símbolos de função são atribuídas funções do domínio para si mesmo, e aos símbolos de predicado são atribuídas relações sobre o domínio. O domínio junto com as atribuições ao vocabulário básico constitui a estrutura. Variáveis podem aparecer em fórmulas, e para dar uma semântica, também temos que atribuir membros do domínio a elas—isto é uma atribuição de variáveis. A relação de satisfação, finalmente, reúne tudo isso. A fórmula pode ser satisfeita em a estrutura $\mathfrak{M}$ relativamente a uma atribuição de variáveis $s$, escrita como $\mathfrak{M}, s \vDash \varphi$. Essa relação também é definida por indução sobre a estrutura de $\varphi$, usando as tabelas de verdade para os conectivos lógicos para definir, por exemplo, a satisfação de $(\varphi \wedge \psi)$ em termos da satisfação (ou não) de $\varphi$ e $\psi$. Acontece então que a atribuição de variáveis é irrelevante se a fórmula $\varphi$ é a sentença, isto é, não tem variáveis livres, e assim podemos falar de sentenças sendo simplesmente satisfeitas (ou não) em estruturas.

Com base na relação de satisfação $\mathfrak{M} \vDash \varphi$ para sentenças podemos então definir as noções semânticas básicas de validade, consequência e satisfatibilidade. A sentença é válida, $\vDash \varphi$, se toda estrutura a satisfaz. Ela é consequência de um conjunto de sentenças, $\Gamma \vDash \varphi$, se toda estrutura que satisfaz todas as sentenças em $\Gamma$ também satisfaz $\varphi$. E um conjunto de sentenças é satisfatível se alguma estrutura satisfaz todas as sentenças nele ao mesmo tempo. Como fórmulas são definidas indutivamente, e a satisfação é por sua vez definida por indução sobre a estrutura das fórmulas, podemos usar indução para pro-

var propriedades de nossa semântica e para relacionar as noções semânticas definidas.

## 16.2 Estruturas para Linguagens de Primeira Ordem

As linguagens de primeira ordem são, por si mesmas, *não interpretadas:* os símbolos de constante, símbolos de função e símbolos de predicado não têm nenhum significado específico associado a eles. Os significados são dados especificando-se a *estrutura*. Ela especifica o *domínio*, isto é, os objetos que os símbolos de constante denotam, sobre os quais os símbolos de função operam e sobre os quais os quantificadores variam. Além disso, ela especifica quais símbolos de constante denotam quais objetos, como a símbolo de função mapeia objetos para objetos, e a quais objetos os símbolos de predicado se aplicam. Estruturas são a base para as noções *semânticas* em lógica, por exemplo, a noção de consequência, validade, satisfatibilidade. Elas são chamadas de várias formas na literatura: "estruturas", "interpretações" ou "modelos".

**Definição 16.1 (Estruturas).** A *estrutura* $\mathfrak{M}$, para uma linguagem $\mathcal{L}$ de lógica de primeira ordem consiste nos seguintes elementos:

1. *Domínio:* um conjunto não vazio, $|\mathfrak{M}|$
2. *Interpretação dos símbolos de constante:* para cada símbolo de constante $c$ de $\mathcal{L}$, um membro $c^{\mathfrak{M}} \in |\mathfrak{M}|$
3. *Interpretação dos símbolos de predicado:* para cada símbolo de predicado $R$ de $n$ lugares de $\mathcal{L}$ (distinto de $=$), uma relação de $n$ lugares $R^{\mathfrak{M}} \subseteq |\mathfrak{M}|^n$
4. *Interpretação dos símbolos de função:* para cada símbolo de função $f$ de $n$ lugares de $\mathcal{L}$, uma função de $n$ lugares $f^{\mathfrak{M}} \colon |\mathfrak{M}|^n \to |\mathfrak{M}|$

**Exemplo 16.2.** A estrutura $\mathfrak{M}$ para a linguagem da aritmética consiste em um conjunto, um elemento de $|\mathfrak{M}|$, $\mathsf{o}^{\mathfrak{M}}$, como interpretação do símbolo de constante $\mathsf{o}$, uma função de um lugar $\mathsf{'}^{\mathfrak{M}} \colon |\mathfrak{M}| \to |\mathfrak{M}|$, duas funções de dois lugares $+^{\mathfrak{M}}$ e $\times^{\mathfrak{M}}$, ambas $|\mathfrak{M}|^2 \to |\mathfrak{M}|$, e uma relação de dois lugares $<^{\mathfrak{M}} \subseteq |\mathfrak{M}|^2$.

Um exemplo óbvio de tal estrutura é o seguinte:

1. $|\mathfrak{N}| = \mathbb{N}$
2. $\mathsf{o}^{\mathfrak{N}} = 0$
3. $\mathsf{'}^{\mathfrak{N}}(n) = n + 1$ para todos $n \in \mathbb{N}$
4. $+^{\mathfrak{N}}(n, m) = n + m$ para todos $n, m \in \mathbb{N}$
5. $\times^{\mathfrak{N}}(n, m) = n \cdot m$ para todos $n, m \in \mathbb{N}$
6. $<^{\mathfrak{N}} = \{\langle n, m\rangle : n \in \mathbb{N}, m \in \mathbb{N}, n < m\}$

A estrutura $\mathfrak{N}$ para $\mathcal{L}_A$ assim definida é chamada de *modelo padrão da aritmética*, porque interpreta as constantes não lógicas de $\mathcal{L}_A$ exatamente como se esperaria.

No entanto, há muitas outras estruturas possíveis para $\mathcal{L}_A$. Por exemplo, poderíamos tomar como domínio o conjunto $\mathbb{Z}$ dos inteiros em vez de $\mathbb{N}$, e definir as interpretações de $0$, $'$, $+$, $\times$, $<$ adequadamente. Mas também podemos definir estruturas para $\mathcal{L}_A$ que não têm nada, nem mesmo remotamente, a ver com números.

**Exemplo 16.3.** Uma estrutura $\mathfrak{M}$ para a linguagem $\mathcal{L}_Z$ da teoria dos conjuntos requer apenas um conjunto e uma única relação de dois lugares. Então, tecnicamente, por exemplo, o conjunto das pessoas mais a relação "$x$ é mais velho que $y$" poderia ser usado como a estrutura para $\mathcal{L}_Z$, assim como $\mathbb{N}$ junto com $n \geq m$ para $n, m \in \mathbb{N}$.

Uma estrutura particularmente interessante para $\mathcal{L}_Z$ na qual os membros do domínio são de fato conjuntos, e a interpretação de $\in$ é de fato a relação "$x$ é um membro de $y$" é a estrutura $\mathfrak{HF}$ dos *conjuntos hereditariamente finitos*:

1. $|\mathfrak{HF}| = \emptyset \cup \wp(\emptyset) \cup \wp(\wp(\emptyset)) \cup \wp(\wp(\wp(\emptyset))) \cup \ldots$;
2. $\in^{\mathfrak{HF}} = \{\langle x, y\rangle : x, y \in |\mathfrak{HF}|, x \in y\}$.

As estipulações que fazemos sobre o que conta como a estrutura impactam nossa lógica. Por exemplo, a escolha de impedir domínios vazios garante, dada a explicação usual de satisfação (ou verdade) para sentenças quantificadas, que $\exists x\,(\varphi(x) \vee \neg\varphi(x))$ é válida—isto é, uma verdade lógica. E a estipulação de que todos os símbolos de constante devem referir-se a um objeto no domínio garante que a generalização existencial é um padrão de inferência correto: $\varphi(a)$, portanto $\exists x\,\varphi(x)$. Se permitíssemos que nomes se referissem a algo fora do domínio, ou que não se referissem, então estaríamos a caminho de uma *lógica livre*, na qual a generalização existencial requer uma premissa adicional: $\varphi(a)$ e $\exists x\, x = a$, portanto $\exists x\,\varphi(x)$.

## 16.3 Estruturas Cobertas para Linguagens de Primeira Ordem

Lembre-se de que um termo é *fechado* se não contém variáveis.

**Definição 16.4 (Valor de termos fechados).** Se $t$ é um termo fechado da linguagem $\mathcal{L}$ e $\mathfrak{M}$ é a estrutura para $\mathcal{L}$, o *valor* $\mathrm{Val}^{\mathfrak{M}}(t)$ é definido como segue:

1. Se $t$ é apenas o símbolo de constante $c$, então $\mathrm{Val}^{\mathfrak{M}}(c) = c^{\mathfrak{M}}$.
2. Se $t$ é da forma $f(t_1, \ldots, t_n)$, então

$$\mathrm{Val}^{\mathfrak{M}}(t) = f^{\mathfrak{M}}(\mathrm{Val}^{\mathfrak{M}}(t_1), \ldots, \mathrm{Val}^{\mathfrak{M}}(t_n)).$$

**Definição 16.5 (Estrutura Coberta).** A estrutura é *coberta* se todo elemento do domínio é o valor de algum termo fechado.

**Exemplo 16.6.** Seja $\mathcal{L}$ a linguagem com os símbolos de constante $zero$, $um$, $dois$, ..., o símbolo de predicado binário $<$, e os símbolos de função binários $+$ e $\times$. Então a estrutura $\mathfrak{M}$ para $\mathcal{L}$ é aquela com domínio $|\mathfrak{M}| = \{0, 1, 2, \ldots\}$ e atribuições $zero^{\mathfrak{M}} = 0$, $um^{\mathfrak{M}} = 1$, $dois^{\mathfrak{M}} = 2$, e assim por diante. Para o símbolo de relação binário $<$, o conjunto $<^{\mathfrak{M}}$ é o conjunto de todos os pares $\langle c_1, c_2\rangle \in |\mathfrak{M}|^2$ tais que $c_1$ é menor que $c_2$: por exemplo, $\langle 1, 3\rangle \in <^{\mathfrak{M}}$ mas $\langle 2, 2\rangle \notin <^{\mathfrak{M}}$. Para o símbolo de função binário $+$, defina $+^{\mathfrak{M}}$ da maneira usual—por exemplo, $+^{\mathfrak{M}}(2, 3)$ resulta em 5, e analogamente para o símbolo de função binário $\times$. Portanto, o valor de $quatro$ é apenas 4, e o valor de $\times(dois, +(tres, zero))$ (ou em notação infixa, $dois \times (tres + zero)$) é

$$\begin{aligned}
\mathrm{Val}^{\mathfrak{M}}(\times(dois, +(tres, zero))) &= \\
&= \times^{\mathfrak{M}}(\mathrm{Val}^{\mathfrak{M}}(dois), \mathrm{Val}^{\mathfrak{M}}(+(tres, zero))) \\
&= \times^{\mathfrak{M}}(\mathrm{Val}^{\mathfrak{M}}(dois), +^{\mathfrak{M}}(\mathrm{Val}^{\mathfrak{M}}(tres), \mathrm{Val}^{\mathfrak{M}}(zero))) \\
&= \times^{\mathfrak{M}}(dois^{\mathfrak{M}}, +^{\mathfrak{M}}(tres^{\mathfrak{M}}, zero^{\mathfrak{M}})) \\
&= \times^{\mathfrak{M}}(2, +^{\mathfrak{M}}(3, 0)) \\
&= \times^{\mathfrak{M}}(2, 3) \\
&= 6
\end{aligned}$$

## 16.4 Satisfação de a Fórmula em a Estrutura

A noção básica que relaciona expressões como termos e fórmulas, por um lado, e estruturas, por outro, são as de *valor* de um termo e *satisfação* de a fórmula. Informalmente, o valor de um termo é um membro de a estrutura—se o termo é apenas uma constante, seu valor é o objeto atribuído à constante pela estrutura, e se ele é construído usando símbolos de função, o valor é calculado a partir dos valores das constantes e das funções atribuídas às funções no termo. A fórmula é *satisfeita* em a estrutura se a interpretação dada aos predicados torna a fórmula verdadeira no domínio da estrutura. Essa noção de satisfação é especificada indutivamente: a especificação da estrutura afirma diretamente quando fórmulas atômicas são satisfeitas, e definimos quando uma fórmula complexa é satisfeita dependendo do conectivo principal ou quantificador e de se as subfórmulas imediatas são ou não satisfeitas.

O caso dos quantificadores aqui é um pouco delicado, pois a subfórmula imediata de uma fórmula quantificada tem uma variável livre, e estruturas não especificam os valores das variáveis. Para lidar com essa dificuldade, também introduzimos *atribuições de variáveis* e definimos a satisfação não em relação a a estrutura sozinha, mas em relação a a estrutura mais uma atribuição de variáveis.

**Definição 16.7 (Atribuição de Variáveis).** Uma *atribuição de variáveis* $s$ para a estrutura $\mathfrak{M}$ é uma função que mapeia cada variável para um membro de $|\mathfrak{M}|$, isto é, $s\colon \mathrm{Var} \to |\mathfrak{M}|$.

A estrutura atribui a valor a cada símbolo de constante, e uma atribuição de variáveis a cada variável. Mas queremos usar termos construídos a partir deles para também nomear membros do domínio. Para isso, definimos o valor dos termos indutivamente. Para símbolos de constante e variáveis, o valor é exatamente como a estrutura ou a atribuição de variáveis o especifica; para termos mais complexos, ele é calculado recursivamente usando as funções que a estrutura atribui aos símbolos de função.

**Definição 16.8 (Valor de Termos).** Se $t$ é um termo da linguagem $\mathcal{L}$, $\mathfrak{M}$ é a estrutura para $\mathcal{L}$, e $s$ é uma atribuição de variáveis para $\mathfrak{M}$, o *valor* $\mathrm{Val}_s^{\mathfrak{M}}(t)$ é definido como segue:

1. $t \equiv c$: $\mathrm{Val}_s^{\mathfrak{M}}(t) = c^{\mathfrak{M}}$.
2. $t \equiv x$: $\mathrm{Val}_s^{\mathfrak{M}}(t) = s(x)$.
3. $t \equiv f(t_1, \ldots, t_n)$:

$$\mathrm{Val}_s^{\mathfrak{M}}(t) = f^{\mathfrak{M}}(\mathrm{Val}_s^{\mathfrak{M}}(t_1), \ldots, \mathrm{Val}_s^{\mathfrak{M}}(t_n)).$$

**Definição 16.9 ($x$-Variante).** Se $s$ é uma atribuição de variáveis para a estrutura $\mathfrak{M}$, então qualquer atribuição de variáveis $s'$ para $\mathfrak{M}$ que difere de $s$ no máximo no que atribui a $x$ é chamada de *$x$-variante* de $s$. Se $s'$ é uma $x$-variante de $s$ escrevemos $s' \sim_x s$.

Note que uma $x$-variante de uma atribuição $s$ não *precisa* atribuir algo diferente a $x$. De fato, toda atribuição conta como uma $x$-variante de si mesma.

**Definição 16.10.** Se $s$ é uma atribuição de variáveis para a estrutura $\mathfrak{M}$ e $m \in |\mathfrak{M}|$, então a atribuição $s[m/x]$ é a atribuição de variáveis definida por

$$s[m/x](y) = \begin{cases} m & \text{se } y \equiv x \\ s(y) & \text{caso contrário.} \end{cases}$$

Em outras palavras, $s[m/x]$ é a $x$-variante particular de $s$ que atribui o membro $m$ do domínio a $x$, e atribui as mesmas coisas às variáveis diferentes de $x$ que $s$ atribui.

**Definição 16.11 (Satisfação).** A satisfação de a fórmula $\varphi$ em a estrutura $\mathfrak{M}$ relativamente a uma atribuição de variáveis $s$, em símbolos: $\mathfrak{M}, s \vDash \varphi$, é definida recursivamente como segue. (Escrevemos $\mathfrak{M}, s \nvDash \varphi$ para significar "não $\mathfrak{M}, s \vDash \varphi$".)

1. $\varphi \equiv \bot$: $\mathfrak{M}, s \nvDash \varphi$.
2. $\varphi \equiv R(t_1, \ldots, t_n)$: $\mathfrak{M}, s \vDash \varphi$ sse $\langle \mathrm{Val}_s^{\mathfrak{M}}(t_1), \ldots, \mathrm{Val}_s^{\mathfrak{M}}(t_n)\rangle \in R^{\mathfrak{M}}$.
3. $\varphi \equiv t_1 = t_2$: $\mathfrak{M}, s \vDash \varphi$ sse $\mathrm{Val}_s^{\mathfrak{M}}(t_1) = \mathrm{Val}_s^{\mathfrak{M}}(t_2)$.
4. $\varphi \equiv \neg\psi$: $\mathfrak{M}, s \vDash \varphi$ sse $\mathfrak{M}, s \nvDash \psi$.
5. $\varphi \equiv (\psi \wedge \chi)$: $\mathfrak{M}, s \vDash \varphi$ sse $\mathfrak{M}, s \vDash \psi$ e $\mathfrak{M}, s \vDash \chi$.
6. $\varphi \equiv (\psi \vee \chi)$: $\mathfrak{M}, s \vDash \varphi$ sse $\mathfrak{M}, s \vDash \psi$ ou $\mathfrak{M}, s \vDash \chi$ (ou ambos).
7. $\varphi \equiv (\psi \to \chi)$: $\mathfrak{M}, s \vDash \varphi$ sse $\mathfrak{M}, s \nvDash \psi$ ou $\mathfrak{M}, s \vDash \chi$ (ou ambos).
8. $\varphi \equiv \forall x\, \psi$: $\mathfrak{M}, s \vDash \varphi$ sse para todo membro $m \in |\mathfrak{M}|$, $\mathfrak{M}, s[m/x] \vDash \psi$.
9. $\varphi \equiv \exists x\, \psi$: $\mathfrak{M}, s \vDash \varphi$ sse para pelo menos um membro $m \in |\mathfrak{M}|$, $\mathfrak{M}, s[m/x] \vDash \psi$.

As atribuições de variáveis são importantes nas últimas duas cláusulas. Não podemos definir a satisfação de $\forall x\, \psi(x)$ por "para todo $m \in |\mathfrak{M}|$, $\mathfrak{M} \vDash \psi(m)$". Não podemos definir a satisfação de $\exists x\, \psi(x)$ por "para pelo menos um $m \in |\mathfrak{M}|$, $\mathfrak{M} \vDash \psi(m)$". A razão é que, se $m \in |\mathfrak{M}|$, ele não é um símbolo da linguagem, e portanto $\psi(m)$ não é a fórmula (isto é, $\psi[m/x]$ é indefinido). Também não podemos supor que temos símbolos de constante ou termos disponíveis que nomeiem cada membro de $\mathfrak{M}$, já que não há nada na definição de estruturas que o exija. Na linguagem padrão, o conjunto de símbolos de constante é infinito enumerável, então se $|\mathfrak{M}|$ não é enumerável não há sequer símbolos de constante suficientes para nomear cada objeto.

Resolvemos esse problema introduzindo atribuições de variáveis, que nos permitem ligar variáveis diretamente a membros do domínio. Então, em vez de dizer que, por exemplo, $\exists x\, \psi(x)$ é satisfeita em $\mathfrak{M}$ sse para pelo menos um $m \in |\mathfrak{M}|$, dizemos que ela é satisfeita em $\mathfrak{M}$ *relativamente a* $s$ sse $\psi(x)$ é satisfeita relativamente a $s[m/x]$ para pelo menos um $m \in |\mathfrak{M}|$.

**Exemplo 16.12.** Seja $\mathcal{L} = \{a, b, f, R\}$ onde $a$ e $b$ são símbolos de constante, $f$ é um símbolo de função de dois lugares, e $R$ é um símbolo de predicado de dois lugares. Considere a estrutura $\mathfrak{M}$ definida por:

1. $|\mathfrak{M}| = \{1, 2, 3, 4\}$
2. $a^{\mathfrak{M}} = 1$
3. $b^{\mathfrak{M}} = 2$
4. $f^{\mathfrak{M}}(x, y) = x + y$ se $x + y \leq 3$ e $= 3$ caso contrário.
5. $R^{\mathfrak{M}} = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 3\rangle, \langle 2, 4\rangle\}$

A função $s(x) = 1$ que atribui $1 \in |\mathfrak{M}|$ a cada variável é uma atribuição de variáveis para $\mathfrak{M}$.

Então

$$\mathrm{Val}_s^{\mathfrak{M}}(f(a,b)) = f^{\mathfrak{M}}(\mathrm{Val}_s^{\mathfrak{M}}(a), \mathrm{Val}_s^{\mathfrak{M}}(b)).$$

Como $a$ e $b$ são símbolos de constante, $\mathrm{Val}_s^{\mathfrak{M}}(a) = a^{\mathfrak{M}} = 1$ e $\mathrm{Val}_s^{\mathfrak{M}}(b) = b^{\mathfrak{M}} = 2$. Então

$$\mathrm{Val}_s^{\mathfrak{M}}(f(a,b)) = f^{\mathfrak{M}}(1,2) = 1 + 2 = 3.$$

Para calcular o valor de $f(f(a,b),a)$ temos que considerar

$$\mathrm{Val}_s^{\mathfrak{M}}(f(f(a,b),a)) = f^{\mathfrak{M}}(\mathrm{Val}_s^{\mathfrak{M}}(f(a,b)), \mathrm{Val}_s^{\mathfrak{M}}(a)) = f^{\mathfrak{M}}(3,1) = 3,$$

já que $3 + 1 > 3$. Como $s(x) = 1$ e $\mathrm{Val}_s^{\mathfrak{M}}(x) = s(x)$, também temos

$$\mathrm{Val}_s^{\mathfrak{M}}(f(f(a,b),x)) = f^{\mathfrak{M}}(\mathrm{Val}_s^{\mathfrak{M}}(f(a,b)), \mathrm{Val}_s^{\mathfrak{M}}(x)) = f^{\mathfrak{M}}(3,1) = 3,$$

Uma fórmula atômica $R(t_1, t_2)$ é satisfeita se a tupla de valores de seus argumentos, isto é, $\langle \mathrm{Val}_s^{\mathfrak{M}}(t_1), \mathrm{Val}_s^{\mathfrak{M}}(t_2)\rangle$, é um membro de $R^{\mathfrak{M}}$. Assim, por exemplo, temos $\mathfrak{M}, s \vDash R(b, f(a,b))$ já que $\langle \mathrm{Val}^{\mathfrak{M}}(b), \mathrm{Val}^{\mathfrak{M}}(f(a,b))\rangle = \langle 2,3\rangle \in R^{\mathfrak{M}}$, mas $\mathfrak{M}, s \nvDash R(x, f(a,b))$ já que $\langle 1,3\rangle \notin R^{\mathfrak{M}}[s]$.

Para determinar se uma fórmula não atômica $\varphi$ é satisfeita, aplicam-se as cláusulas da definição indutiva que se aplicam ao conectivo principal. Por exemplo, o conectivo principal em $R(a,a) \to (R(b,x) \vee R(x,b))$ é o $\to$, e

$$\begin{aligned}&\mathfrak{M}, s \vDash R(a,a) \to (R(b,x) \vee R(x,b)) \text{ sse}\\ &\quad \mathfrak{M}, s \nvDash R(a,a) \text{ ou } \mathfrak{M}, s \vDash R(b,x) \vee R(x,b)\end{aligned}$$

Como $\mathfrak{M}, s \vDash R(a,a)$ (porque $\langle 1,1\rangle \in R^{\mathfrak{M}}$) ainda não podemos determinar a resposta e devemos primeiro descobrir se $\mathfrak{M}, s \vDash R(b,x) \vee R(x,b)$:

$$\begin{aligned}&\mathfrak{M}, s \vDash R(b,x) \vee R(x,b) \text{ sse}\\ &\quad \mathfrak{M}, s \vDash R(b,x) \text{ ou } \mathfrak{M}, s \vDash R(x,b)\end{aligned}$$

E este é o caso, já que $\mathfrak{M}, s \vDash R(x,b)$ (porque $\langle 1,2\rangle \in R^{\mathfrak{M}}$).

Lembre-se de que uma $x$-variante de $s$ é uma atribuição de variáveis que difere de $s$ no máximo no que atribui a $x$. Para cada membro de $|\mathfrak{M}|$, há uma $x$-variante de $s$:

$$\begin{aligned}s_1 &= s[1/x], & s_2 &= s[2/x],\\ s_3 &= s[3/x], & s_4 &= s[4/x].\end{aligned}$$

Assim, por exemplo, $s_2(x) = 2$ e $s_2(y) = s(y) = 1$ para todas as variáveis $y$ diferentes de $x$. Estas são todas as $x$-variantes de $s$ para a estrutura $\mathfrak{M}$, já que $|\mathfrak{M}| = \{1, 2, 3, 4\}$. Note, em particular, que $s_1 = s$ ($s$ é sempre uma $x$-variante de si mesma).

Para determinar se uma fórmula quantificada existencialmente $\exists x\, \varphi(x)$ é satisfeita, temos que determinar se $\mathfrak{M}, s[m/x] \vDash \varphi(x)$ para pelo menos um $m \in |\mathfrak{M}|$. Assim,

$$\mathfrak{M}, s \vDash \exists x\, (R(b, x) \vee R(x, b)),$$

já que $\mathfrak{M}, s[1/x] \vDash R(b, x) \vee R(x, b)$ ($s[3/x]$ também serviria). Mas,

$$\mathfrak{M}, s \nvDash \exists x\, (R(b, x) \wedge R(x, b))$$

já que, qualquer que seja o $m \in |\mathfrak{M}|$ que escolhamos, $\mathfrak{M}, s[m/x] \nvDash R(b, x) \wedge R(x, b)$.

Para determinar se uma fórmula quantificada universalmente $\forall x\, \varphi(x)$ é satisfeita, temos que determinar se $\mathfrak{M}, s[m/x] \vDash \varphi(x)$ para todo $m \in |\mathfrak{M}|$. Assim,

$$\mathfrak{M}, s \vDash \forall x\, (R(x, a) \to R(a, x)),$$

já que $\mathfrak{M}, s[m/x] \vDash R(x, a) \to R(a, x)$ para todo $m \in |\mathfrak{M}|$. Para $m = 1$, temos $\mathfrak{M}, s[1/x] \vDash R(a, x)$ então o consequente é verdadeiro; para $m = 2$, 3, e 4, temos $\mathfrak{M}, s[m/x] \nvDash R(x, a)$, então o antecedente é falso. Mas,

$$\mathfrak{M}, s \nvDash \forall x\, (R(a, x) \to R(x, a))$$

já que $\mathfrak{M}, s[2/x] \nvDash R(a, x) \to R(x, a)$ (porque $\mathfrak{M}, s[2/x] \vDash R(a, x)$ e $\mathfrak{M}, s[2/x] \nvDash R(x, a)$).

Para um caso mais complicado, considere

$$\forall x\, (R(a, x) \to \exists y\, R(x, y)).$$

Como $\mathfrak{M}, s[3/x] \nvDash R(a, x)$ e $\mathfrak{M}, s[4/x] \nvDash R(a, x)$, os casos interessantes em que temos que nos preocupar com o consequente do condicional são apenas $m = 1$ e $= 2$. $\mathfrak{M}, s[1/x] \vDash \exists y\, R(x, y)$ vale? Vale se há pelo menos um $n \in |\mathfrak{M}|$ tal que $\mathfrak{M}, s[1/x][n/y] \vDash R(x, y)$. De fato, se tomarmos $n = 1$, temos $s[1/x][n/y] = s[1/y] = s$. Como $s(x) = 1$, $s(y) = 1$, e $\langle 1, 1\rangle \in R^{\mathfrak{M}}$, a resposta é sim.

Para determinar se $\mathfrak{M}, s[2/x] \vDash \exists y\, R(x, y)$, temos que olhar para as atribuições de variáveis $s[2/x][n/y]$. Aqui, para $n = 1$, essa atribuição é $s_2 = s[2/x]$, que não satisfaz $R(x, y)$ ($s_2(x) = 2$, $s_2(y) = 1$, e $\langle 2, 1\rangle \notin R^{\mathfrak{M}}$). No entanto, considere $s[2/x][3/y] = s_2[3/y]$. $\mathfrak{M}, s_2[3/y] \vDash R(x, y)$ já que $\langle 2, 3\rangle \in R^{\mathfrak{M}}$, e assim $\mathfrak{M}, s_2 \vDash \exists y\, R(x, y)$.

Assim, para todo $n \in |\mathfrak{M}|$, ou $\mathfrak{M}, s[m/x] \nvDash R(a, x)$ (se $m = 3$, 4) ou $\mathfrak{M}, s[m/x] \vDash \exists y\, R(x, y)$ (se $m = 1, 2$), e assim

$$\mathfrak{M}, s \vDash \forall x\, (R(a, x) \to \exists y\, R(x, y)).$$

Por outro lado,

$$\mathfrak{M}, s \nvDash \exists x\, (R(a,x) \wedge \forall y\, R(x,y)).$$

Temos $\mathfrak{M}, s[m/x] \vDash R(a,x)$ apenas para $m = 1$ e $m = 2$. Mas para ambos esses valores de $m$, há por sua vez um $n \in |\mathfrak{M}|$, a saber $n = 4$, tal que $\mathfrak{M}, s[m/x][n/y] \nvDash R(x,y)$ e assim $\mathfrak{M}, s[m/x] \nvDash \forall y\, R(x,y)$ para $m = 1$ e $m = 2$. Em suma, não há $m \in |\mathfrak{M}|$ tal que $\mathfrak{M}, s[m/x] \vDash R(a,x) \wedge \forall y\, R(x,y)$.

## 16.5 Atribuições de Variáveis

Uma atribuição de variáveis $s$ fornece um valor para *toda* variável—e há infinitas delas. Isso, é claro, não é necessário. Exigimos que as atribuições de variáveis atribuam valores a todas as variáveis simplesmente porque isso torna as coisas muito mais fáceis. O valor de um termo $t$, e se a fórmula $\varphi$ é satisfeita em a estrutura com respeito a $s$, dependem apenas das atribuições que $s$ faz às variáveis em $t$ e às variáveis livres de $\varphi$. Esse é o conteúdo das próximas duas proposições. Para tornar precisa a ideia de "depende de", mostramos que quaisquer duas atribuições de variáveis que concordam em todas as variáveis em $t$ dão o mesmo valor, e que $\varphi$ é satisfeita relativamente a uma sse é satisfeita relativamente à outra se duas atribuições de variáveis concordam em todas as variáveis livres de $\varphi$.

**Proposição 16.13.** *Se as variáveis em um termo $t$ estão entre $x_1, \ldots, x_n$, e $s_1(x_i) = s_2(x_i)$ para $i = 1, \ldots, n$, então* $\mathrm{Val}^{\mathfrak{M}}_{s_1}(t) = \mathrm{Val}^{\mathfrak{M}}_{s_2}(t)$.

*Prova.* Por indução sobre a complexidade de $t$. Para o caso base, $t$ pode ser a símbolo de constante ou uma das variáveis $x_1, \ldots, x_n$. Se $t = c$, então $\mathrm{Val}^{\mathfrak{M}}_{s_1}(t) = c^{\mathfrak{M}} = \mathrm{Val}^{\mathfrak{M}}_{s_2}(t)$. Se $t = x_i$, $s_1(x_i) = s_2(x_i)$ pela hipótese da proposição, e assim $\mathrm{Val}^{\mathfrak{M}}_{s_1}(t) = s_1(x_i) = s_2(x_i) = \mathrm{Val}^{\mathfrak{M}}_{s_2}(t)$.

Para o passo indutivo, suponha que $t = f(t_1, \ldots, t_k)$ e que a afirmação vale para $t_1, \ldots, t_k$. Então

$$\begin{aligned}\mathrm{Val}^{\mathfrak{M}}_{s_1}(t) &= \mathrm{Val}^{\mathfrak{M}}_{s_1}(f(t_1, \ldots, t_k)) \\ &= f^{\mathfrak{M}}(\mathrm{Val}^{\mathfrak{M}}_{s_1}(t_1), \ldots, \mathrm{Val}^{\mathfrak{M}}_{s_1}(t_k)).\end{aligned}$$

Para $j = 1, \ldots, k$, as variáveis de $t_j$ estão entre $x_1, \ldots, x_n$. Pela hipótese de indução, $\mathrm{Val}^{\mathfrak{M}}_{s_1}(t_j) = \mathrm{Val}^{\mathfrak{M}}_{s_2}(t_j)$. Assim,

$$\begin{aligned}\mathrm{Val}^{\mathfrak{M}}_{s_1}(t) &= \mathrm{Val}^{\mathfrak{M}}_{s_1}(f(t_1, \ldots, t_k)) \\ &= f^{\mathfrak{M}}(\mathrm{Val}^{\mathfrak{M}}_{s_1}(t_1), \ldots, \mathrm{Val}^{\mathfrak{M}}_{s_1}(t_k)) \\ &= f^{\mathfrak{M}}(\mathrm{Val}^{\mathfrak{M}}_{s_2}(t_1), \ldots, \mathrm{Val}^{\mathfrak{M}}_{s_2}(t_k)) \\ &= \mathrm{Val}^{\mathfrak{M}}_{s_2}(f(t_1, \ldots, t_k)) = \mathrm{Val}^{\mathfrak{M}}_{s_2}(t).\end{aligned}$$

□

**Proposição 16.14.** *Se as variáveis livres em $\varphi$ estão entre $x_1, \ldots, x_n$, e $s_1(x_i) = s_2(x_i)$ para $i = 1, \ldots, n$, então $\mathfrak{M}, s_1 \vDash \varphi$ sse $\mathfrak{M}, s_2 \vDash \varphi$.*

*Prova.* Usamos indução sobre a complexidade de $\varphi$. Para o caso base, onde $\varphi$ é atômica, $\varphi$ pode ser: $\bot$, $R(t_1, \ldots, t_k)$ para um predicado $R$ de $k$ lugares e termos $t_1, \ldots, t_k$, ou $t_1 = t_2$ para termos $t_1$ e $t_2$. Nos dois últimos casos, demonstramos apenas a direção direta do bicondicional, já que a prova da recíproca é simétrica.

1. $\varphi \equiv \bot$: tanto $\mathfrak{M}, s_1 \nvDash \varphi$ quanto $\mathfrak{M}, s_2 \nvDash \varphi$.

2. $\varphi \equiv R(t_1, \ldots, t_k)$: seja $\mathfrak{M}, s_1 \vDash \varphi$. Então

   $$\langle \mathrm{Val}^{\mathfrak{M}}_{s_1}(t_1), \ldots, \mathrm{Val}^{\mathfrak{M}}_{s_1}(t_k) \rangle \in R^{\mathfrak{M}}.$$

   Para $i = 1, \ldots, k$, $\mathrm{Val}^{\mathfrak{M}}_{s_1}(t_i) = \mathrm{Val}^{\mathfrak{M}}_{s_2}(t_i)$ por Proposição 16.13. Então também temos $\langle \mathrm{Val}^{\mathfrak{M}}_{s_2}(t_i), \ldots, \mathrm{Val}^{\mathfrak{M}}_{s_2}(t_k) \rangle \in R^{\mathfrak{M}}$, e portanto $\mathfrak{M}, s_2 \vDash \varphi$.

3. $\varphi \equiv t_1 = t_2$: suponha $\mathfrak{M}, s_1 \vDash \varphi$. Então $\mathrm{Val}^{\mathfrak{M}}_{s_1}(t_1) = \mathrm{Val}^{\mathfrak{M}}_{s_1}(t_2)$. Assim,

   $$\begin{aligned} \mathrm{Val}^{\mathfrak{M}}_{s_2}(t_1) &= \mathrm{Val}^{\mathfrak{M}}_{s_1}(t_1) && \text{(por Proposição 16.13)} \\ &= \mathrm{Val}^{\mathfrak{M}}_{s_1}(t_2) && \text{(já que } \mathfrak{M}, s_1 \vDash t_1 = t_2\text{)} \\ &= \mathrm{Val}^{\mathfrak{M}}_{s_2}(t_2) && \text{(por Proposição 16.13),} \end{aligned}$$

   então $\mathfrak{M}, s_2 \vDash t_1 = t_2$.

Agora suponha $\mathfrak{M}, s_1 \vDash \psi$ sse $\mathfrak{M}, s_2 \vDash \psi$ para todas as fórmulas $\psi$ menos complexas que $\varphi$. O passo de indução procede por casos determinados pelo operador principal de $\varphi$. Em cada caso, demonstramos apenas a direção direta do bicondicional; a prova da direção reversa é simétrica. Em todos os casos exceto os dos quantificadores, aplicamos a hipótese de indução às subfórmulas $\psi$ de $\varphi$. As variáveis livres de $\psi$ estão entre as de $\varphi$. Assim, se $s_1$ e $s_2$ concordam nas variáveis livres de $\varphi$, elas também concordam nas de $\psi$, e a hipótese de indução se aplica a $\psi$.

1. $\varphi \equiv \neg\psi$: se $\mathfrak{M}, s_1 \vDash \varphi$, então $\mathfrak{M}, s_1 \nvDash \psi$, então pela hipótese de indução, $\mathfrak{M}, s_2 \nvDash \psi$, portanto $\mathfrak{M}, s_2 \vDash \varphi$.

2. $\varphi \equiv \psi \wedge \chi$: exercise.

3. $\varphi \equiv \psi \vee \chi$: se $\mathfrak{M}, s_1 \vDash \varphi$, então $\mathfrak{M}, s_1 \vDash \psi$ ou $\mathfrak{M}, s_1 \vDash \chi$. Pela hipótese de indução, $\mathfrak{M}, s_2 \vDash \psi$ ou $\mathfrak{M}, s_2 \vDash \chi$, então $\mathfrak{M}, s_2 \vDash \varphi$.

4. $\varphi \equiv \psi \to \chi$: exercise.

5. $\varphi \equiv \exists x\, \psi$: se $\mathfrak{M}, s_1 \vDash \varphi$, há um $m \in |\mathfrak{M}|$ tal que $\mathfrak{M}, s_1[m/x] \vDash \psi$. Sejam $s_1' = s_1[m/x]$ e $s_2' = s_2[m/x]$. As variáveis livres de $\psi$ estão entre $x_1$, ..., $x_n$, e $x$. $s_1'(x_i) = s_2'(x_i)$, já que $s_1'$ e $s_2'$ são $x$-variantes de $s_1$ e $s_2$, respectivamente, e por hipótese $s_1(x_i) = s_2(x_i)$. $s_1'(x) = s_2'(x) = m$ pela forma como definimos $s_1'$ e $s_2'$. Então a hipótese de indução se aplica a $\psi$ e $s_1'$, $s_2'$, então $\mathfrak{M}, s_2' \vDash \psi$. Portanto, já que $s_2' = s_2[m/x]$, há um $m \in |\mathfrak{M}|$ tal que $\mathfrak{M}, s_2[m/x] \vDash \psi$, e assim $\mathfrak{M}, s_2 \vDash \varphi$.

6. $\varphi \equiv \forall x\, \psi$: exercise.

Por indução, obtemos que $\mathfrak{M}, s_1 \vDash \varphi$ sse $\mathfrak{M}, s_2 \vDash \varphi$ sempre que as variáveis livres em $\varphi$ estão entre $x_1, \ldots, x_n$ e $s_1(x_i) = s_2(x_i)$ para $i = 1, \ldots, n$. □

Sentenças não têm variáveis livres, então quaisquer duas atribuições de variáveis atribuem as mesmas coisas a todas as (zero) variáveis livres de qualquer sentença. A proposição que acabamos de provar significa, então, que se a sentença é satisfeita ou não em uma estrutura relativamente a uma atribuição de variáveis é completamente independente da atribuição. Registraremos esse fato. Ele justifica a definição de satisfação de a sentença em a estrutura (sem mencionar uma atribuição de variáveis) que segue.

**Corolário 16.15.** *Se $\varphi$ é a sentença e $s$ uma atribuição de variáveis, então $\mathfrak{M}, s \vDash \varphi$ sse $\mathfrak{M}, s' \vDash \varphi$ para toda atribuição de variáveis $s'$.*

*Prova.* Seja $s'$ uma atribuição de variáveis qualquer. Como $\varphi$ é a sentença, ela não tem variáveis livres, e assim toda atribuição de variáveis $s'$ trivialmente atribui as mesmas coisas a todas as variáveis livres de $\varphi$ que faz $s$. Então a condição de Proposição 16.14 é satisfeita, e temos $\mathfrak{M}, s \vDash \varphi$ sse $\mathfrak{M}, s' \vDash \varphi$. □

**Definição 16.16.** Se $\varphi$ é a sentença, dizemos que a estrutura $\mathfrak{M}$ *satisfaz* $\varphi$, $\mathfrak{M} \vDash \varphi$, sse $\mathfrak{M}, s \vDash \varphi$ para todas as atribuições de variáveis $s$.

Se $\mathfrak{M} \vDash \varphi$, também dizemos simplesmente que $\varphi$ *é verdadeira em* $\mathfrak{M}$. A noção de satisfação se estende naturalmente de sentenças individuais para conjuntos de sentenças.

**Definição 16.17.** Se $\Gamma$ é um conjunto de sentenças $\Gamma$, dizemos que a estrutura $\mathfrak{M}$ *satisfaz* $\Gamma$, $\mathfrak{M} \vDash \Gamma$, sse $\mathfrak{M} \vDash \varphi$ para todo $\varphi \in \Gamma$.

**Proposição 16.18.** *Seja $\mathfrak{M}$ a estrutura, $\varphi$ a sentença, e $s$ uma atribuição de variáveis. $\mathfrak{M} \vDash \varphi$ sse $\mathfrak{M}, s \vDash \varphi$.*

*Prova.* Exercício. □

**Proposição 16.19.** *Suponha que $\varphi(x)$ contém apenas $x$ livre, e $\mathfrak{M}$ é a estrutura. Então:*

1. $\mathfrak{M} \vDash \exists x\, \varphi(x)$ *sse* $\mathfrak{M}, s \vDash \varphi(x)$ *para pelo menos uma atribuição de variáveis* $s$.

2. $\mathfrak{M} \vDash \forall x\, \varphi(x)$ *sse* $\mathfrak{M}, s \vDash \varphi(x)$ *para todas as atribuições de variáveis* $s$.

*Prova.* Exercício. □

## 16.6 Extensionalidade

A extensionalidade, às vezes chamada de relevância, pode ser expressa informalmente da seguinte forma: os únicos fatores que influenciam a satisfação de fórmula $\varphi$ em a estrutura $\mathfrak{M}$ em relação a uma atribuição de variáveis $s$ são o tamanho do domínio e as atribuições feitas por $\mathfrak{M}$ e $s$ aos elementos da linguagem que de fato aparecem em $\varphi$.

Uma consequência imediata da extensionalidade é que, quando duas estruturas $\mathfrak{M}$ e $\mathfrak{M}'$ concordam em todos os elementos da linguagem que aparecem em uma sentença $\varphi$ e têm o mesmo domínio, $\mathfrak{M}$ e $\mathfrak{M}'$ também devem concordar quanto a se $\varphi$ em si é verdadeira ou não.

**Proposição 16.20 (Extensionalidade).** *Seja* $\varphi$ *a fórmula, e* $\mathfrak{M}_1$ *e* $\mathfrak{M}_2$ *estruturas com* $|\mathfrak{M}_1| = |\mathfrak{M}_2|$, *e* $s$ *uma atribuição de variáveis sobre* $|\mathfrak{M}_1| = |\mathfrak{M}_2|$. *Se* $c^{\mathfrak{M}_1} = c^{\mathfrak{M}_2}$, $R^{\mathfrak{M}_1} = R^{\mathfrak{M}_2}$, *e* $f^{\mathfrak{M}_1} = f^{\mathfrak{M}_2}$ *para todo símbolo de constante* $c$, *símbolo de relação* $R$, *e símbolo de função* $f$ *que ocorre em* $\varphi$, *então* $\mathfrak{M}_1, s \vDash \varphi$ *sse* $\mathfrak{M}_2, s \vDash \varphi$.

*Prova.* Primeiro prove (por indução sobre $t$) que, para todo termo, $\mathrm{Val}_s^{\mathfrak{M}_1}(t) = \mathrm{Val}_s^{\mathfrak{M}_2}(t)$. Então prove a proposição por indução sobre $\varphi$, fazendo uso da afirmação que acabamos de provar para a base da indução (onde $\varphi$ é atômica).□

**Corolário 16.21 (Extensionalidade para Sentenças).** *Seja* $\varphi$ *a sentença e* $\mathfrak{M}_1, \mathfrak{M}_2$ *como em Proposição 16.20. Então* $\mathfrak{M}_1 \vDash \varphi$ *sse* $\mathfrak{M}_2 \vDash \varphi$.

*Prova.* Segue de Proposição 16.20 por Corolário 16.15. □

Além disso, o valor de um termo, e se a estrutura satisfaz ou não a fórmula, dependem apenas dos valores de seus subtermos.

**Proposição 16.22.** *Seja* $\mathfrak{M}$ *a estrutura,* $t$ *e* $t'$ *termos, e* $s$ *uma atribuição de variáveis. Então* $\mathrm{Val}_s^{\mathfrak{M}}(t[t'/x]) = \mathrm{Val}^{\mathfrak{M}}_{s[\mathrm{Val}_s^{\mathfrak{M}}(t')/x]}(t)$.

*Prova.* Por indução sobre $t$.

1. Se $t$ é uma constante, digamos, $t \equiv c$, então $t[t'/x] = c$, e $\mathrm{Val}_s^{\mathfrak{M}}(c) = c^{\mathfrak{M}} = \mathrm{Val}^{\mathfrak{M}}_{s[\mathrm{Val}_s^{\mathfrak{M}}(t')/x]}(c)$.

2. Se $t$ é uma variável diferente de $x$, digamos, $t \equiv y$, então $t[t'/x] = y$, e $\mathrm{Val}_s^{\mathfrak{M}}(y) = \mathrm{Val}^{\mathfrak{M}}_{s[\mathrm{Val}_s^{\mathfrak{M}}(t')/x]}(y)$ já que $s \sim_x s[\mathrm{Val}_s^{\mathfrak{M}}(t')/x]$.

3. Se $t \equiv x$, então $t[t'/x] = t'$. Mas $\mathrm{Val}^{\mathfrak{M}}_{s[\mathrm{Val}^{\mathfrak{M}}_s(t')/x]}(x) = \mathrm{Val}^{\mathfrak{M}}_s(t')$ pela definição de $s[\mathrm{Val}^{\mathfrak{M}}_s(t')/x]$.

4. Se $t \equiv f(t_1, \ldots, t_n)$ então temos:

$$\begin{aligned}
&\mathrm{Val}^{\mathfrak{M}}_s(t[t'/x]) = \\
&\quad = \mathrm{Val}^{\mathfrak{M}}_s(f(t_1[t'/x], \ldots, t_n[t'/x])) \\
&\qquad \text{pela definição de } t[t'/x] \\
&\quad = f^{\mathfrak{M}}(\mathrm{Val}^{\mathfrak{M}}_s(t_1[t'/x]), \ldots, \mathrm{Val}^{\mathfrak{M}}_s(t_n[t'/x])) \\
&\qquad \text{pela definição de } \mathrm{Val}^{\mathfrak{M}}_s(f(\ldots)) \\
&\quad = f^{\mathfrak{M}}(\mathrm{Val}^{\mathfrak{M}}_{s[\mathrm{Val}^{\mathfrak{M}}_s(t')/x]}(t_1), \ldots, \mathrm{Val}^{\mathfrak{M}}_{s[\mathrm{Val}^{\mathfrak{M}}_s(t')/x]}(t_n)) \\
&\qquad \text{pela hipótese de indução} \\
&\quad = \mathrm{Val}^{\mathfrak{M}}_{s[\mathrm{Val}^{\mathfrak{M}}_s(t')/x]}(t) \text{ pela definição de } \mathrm{Val}^{\mathfrak{M}}_{s[\mathrm{Val}^{\mathfrak{M}}_s(t')/x]}(f(\ldots))
\end{aligned}$$ □

**Proposição 16.23.** *Seja $\mathfrak{M}$ a estrutura, $\varphi$ a fórmula, $t'$ um termo, e $s$ uma atribuição de variáveis. Então $\mathfrak{M}, s \vDash \varphi[t'/x]$ sse $\mathfrak{M}, s[\mathrm{Val}^{\mathfrak{M}}_s(t')/x] \vDash \varphi$.*

*Prova.* Exercício. □

O ponto de Proposições 16.22 e 16.23 é o seguinte. Suponha que temos um termo $t$ ou a fórmula $\varphi$ e algum termo $t'$, e queremos saber o valor de $t[t'/x]$ ou se $\varphi[t'/x]$ é ou não satisfeita em a estrutura $\mathfrak{M}$ em relação a uma atribuição de variáveis $s$. Então podemos ou realizar a substituição primeiro e depois considerar o valor ou a satisfação em relação a $\mathfrak{M}$ e $s$, ou podemos primeiro determinar o valor $m = \mathrm{Val}^{\mathfrak{M}}_s(t')$ de $t'$ em $\mathfrak{M}$ em relação a $s$, mudar a atribuição de variáveis para $s[m/x]$ e então considerar o valor de $t$ em $\mathfrak{M}$ e $s[m/x]$, ou se $\mathfrak{M}, s[m/x] \vDash \varphi$. Proposições 16.22 e 16.23 garantem que a resposta será a mesma, independentemente de como o façamos.

## 16.7 Noções Semânticas

Dada a definição de estruturas para linguagens de primeira ordem, podemos definir algumas propriedades semânticas básicas de sentenças e relações entre elas. A mais simples destas é a noção de *validade* de uma sentença. Uma sentença é válida se é satisfeita em toda estrutura. Sentenças válidas são aquelas que são satisfeitas independentemente de como os símbolos não lógicos nela são interpretados. Sentenças válidas são, portanto, também chamadas de *verdades lógicas*—elas são verdadeiras, isto é, satisfeitas, em qualquer estrutura e, portanto, sua verdade depende apenas dos símbolos lógicos que nelas ocorrem e de sua estrutura sintática, mas não dos símbolos não lógicos ou de sua interpretação.

**Definição 16.24 (Validade).** Uma sentença $\varphi$ é *válida*, $\vDash \varphi$, sse $\mathfrak{M} \vDash \varphi$ para toda estrutura $\mathfrak{M}$.

**Definição 16.25 (Consequência).** Uma sentença $\varphi$ é *consequência* de um conjunto de sentenças $\Gamma$, $\Gamma \vDash \varphi$, sse para toda estrutura $\mathfrak{M}$ com $\mathfrak{M} \vDash \Gamma$, $\mathfrak{M} \vDash \varphi$.

**Definição 16.26 (Satisfatibilidade).** Um conjunto de sentenças $\Gamma$ é *satisfatível* se $\mathfrak{M} \vDash \Gamma$ para alguma estrutura $\mathfrak{M}$. Se $\Gamma$ não é satisfatível ele é chamado de *insatisfatível*.

**Proposição 16.27.** *Uma sentença $\varphi$ é válida sse $\Gamma \vDash \varphi$ para todo conjunto de sentenças $\Gamma$.*

*Prova.* Para a direção direta, seja $\varphi$ válida, e seja $\Gamma$ um conjunto de sentenças. Seja $\mathfrak{M}$ a estrutura tal que $\mathfrak{M} \vDash \Gamma$. Como $\varphi$ é válida, $\mathfrak{M} \vDash \varphi$, portanto $\Gamma \vDash \varphi$.

Para a contrapositiva da direção reversa, seja $\varphi$ inválida, então há a estrutura $\mathfrak{M}$ com $\mathfrak{M} \nvDash \varphi$. Quando $\Gamma = \{\top\}$, como $\top$ é válida, $\mathfrak{M} \vDash \Gamma$. Portanto, há a estrutura $\mathfrak{M}$ tal que $\mathfrak{M} \vDash \Gamma$ mas $\mathfrak{M} \nvDash \varphi$, portanto $\varphi$ não é consequência de $\Gamma$. □

**Proposição 16.28.** *$\Gamma \vDash \varphi$ sse $\Gamma \cup \{\neg\varphi\}$ é insatisfatível.*

*Prova.* Para a direção direta, suponha $\Gamma \vDash \varphi$ e suponha, ao contrário, que há a estrutura $\mathfrak{M}$ tal que $\mathfrak{M} \vDash \Gamma \cup \{\neg\varphi\}$. Como $\mathfrak{M} \vDash \Gamma$ e $\Gamma \vDash \varphi$, $\mathfrak{M} \vDash \varphi$. Além disso, como $\mathfrak{M} \vDash \Gamma \cup \{\neg\varphi\}$, $\mathfrak{M} \vDash \neg\varphi$, então temos tanto $\mathfrak{M} \vDash \varphi$ quanto $\mathfrak{M} \nvDash \varphi$, uma contradição. Portanto, não pode haver tal estrutura $\mathfrak{M}$, então $\Gamma \cup \{\neg\varphi\}$ é insatisfatível.

Para a direção reversa, suponha que $\Gamma \cup \{\neg\varphi\}$ é insatisfatível. Então, para toda estrutura $\mathfrak{M}$, ou $\mathfrak{M} \nvDash \Gamma$ ou $\mathfrak{M} \vDash \varphi$. Portanto, para toda estrutura $\mathfrak{M}$ com $\mathfrak{M} \vDash \Gamma$, $\mathfrak{M} \vDash \varphi$, então $\Gamma \vDash \varphi$. □

**Proposição 16.29.** *Se $\Gamma \subseteq \Gamma'$ e $\Gamma \vDash \varphi$, então $\Gamma' \vDash \varphi$.*

*Prova.* Suponha que $\Gamma \subseteq \Gamma'$ e $\Gamma \vDash \varphi$. Seja $\mathfrak{M}$ uma estrutura tal que $\mathfrak{M} \vDash \Gamma'$; então $\mathfrak{M} \vDash \Gamma$, e como $\Gamma \vDash \varphi$, obtemos que $\mathfrak{M} \vDash \varphi$. Portanto, sempre que $\mathfrak{M} \vDash \Gamma'$, $\mathfrak{M} \vDash \varphi$, então $\Gamma' \vDash \varphi$. □

**Teorema 16.30 (Teorema da Dedução Semântica).** *$\Gamma \cup \{\varphi\} \vDash \psi$ sse $\Gamma \vDash \varphi \to \psi$.*

*Prova.* Para a direção direta, seja $\Gamma \cup \{\varphi\} \vDash \psi$ e seja $\mathfrak{M}$ a estrutura tal que $\mathfrak{M} \vDash \Gamma$. Se $\mathfrak{M} \vDash \varphi$, então $\mathfrak{M} \vDash \Gamma \cup \{\varphi\}$, então, como $\psi$ é consequência de $\Gamma \cup \{\varphi\}$, obtemos $\mathfrak{M} \vDash \psi$. Portanto, $\mathfrak{M} \vDash \varphi \to \psi$, então $\Gamma \vDash \varphi \to \psi$.

Para a direção reversa, seja $\Gamma \vDash \varphi \to \psi$ e $\mathfrak{M}$ a estrutura tal que $\mathfrak{M} \vDash \Gamma \cup \{\varphi\}$. Então $\mathfrak{M} \vDash \Gamma$, então $\mathfrak{M} \vDash \varphi \to \psi$, e como $\mathfrak{M} \vDash \varphi$, $\mathfrak{M} \vDash \psi$. Portanto, sempre que $\mathfrak{M} \vDash \Gamma \cup \{\varphi\}$, $\mathfrak{M} \vDash \psi$, então $\Gamma \cup \{\varphi\} \vDash \psi$. □

**Proposição 16.31.** *Seja $\mathfrak{M}$ a estrutura, e $\varphi(x)$ a fórmula com uma variável livre $x$, e $t$ um termo fechado. Então:*

1. $\varphi(t) \vDash \exists x\, \varphi(x)$
2. $\forall x\, \varphi(x) \vDash \varphi(t)$

*Prova.* 1. Suponha $\mathfrak{M} \vDash \varphi(t)$. Seja $s$ uma atribuição de variáveis com $s(x) = \mathrm{Val}^{\mathfrak{M}}(t)$. Então $\mathfrak{M}, s \vDash \varphi(t)$ já que $\varphi(t)$ é a sentença. Por Proposição 16.23, $\mathfrak{M}, s \vDash \varphi(x)$. Por Proposição 16.19, $\mathfrak{M} \vDash \exists x\, \varphi(x)$.

2. Exercício. □

## Problemas

**Problema 16.1.** $\mathfrak{N}$, o modelo padrão da aritmética, é coberto? Explique.

**Problema 16.2.** Seja $\mathcal{L} = \{c, f, A\}$ com um símbolo de constante, um símbolo de função de um lugar e um símbolo de predicado de dois lugares, e seja a estrutura $\mathfrak{M}$ dada por

1. $|\mathfrak{M}| = \{1, 2, 3\}$
2. $c^{\mathfrak{M}} = 3$
3. $f^{\mathfrak{M}}(1) = 2, f^{\mathfrak{M}}(2) = 3, f^{\mathfrak{M}}(3) = 2$
4. $A^{\mathfrak{M}} = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\}$

(a) Seja $s(v) = 1$ para todas as variáveis $v$. Descubra se

$$\mathfrak{M}, s \vDash \exists x\, (A(f(z), c) \to \forall y\, (A(y, x) \vee A(f(y), x)))$$

Explique por que sim ou por que não.

(b) Dê uma estrutura e uma atribuição de variáveis diferentes nas quais a fórmula não seja satisfeita.

**Problema 16.3.** Complete a prova de Proposição 16.14.

**Problema 16.4.** Prove Proposição 16.18

**Problema 16.5.** Prove Proposição 16.19.

**Problema 16.6.** Suponha que $\mathcal{L}$ é uma linguagem sem símbolos de função. Dada uma estrutura $\mathfrak{M}$, $c$ a símbolo de constante e $a \in |\mathfrak{M}|$, defina $\mathfrak{M}[a/c]$ como a estrutura que é exatamente como $\mathfrak{M}$, exceto que $c^{\mathfrak{M}[a/c]} = a$. Defina $\mathfrak{M} \mid\!\vDash \varphi$ para sentenças $\varphi$ por:

1. $\varphi \equiv \bot$: não $\mathfrak{M} \mid\!\models \varphi$.
2. $\varphi \equiv R(d_1, \ldots, d_n)$: $\mathfrak{M} \mid\!\models \varphi$ sse $\langle d_1^{\mathfrak{M}}, \ldots, d_n^{\mathfrak{M}} \rangle \in R^{\mathfrak{M}}$.
3. $\varphi \equiv d_1 = d_2$: $\mathfrak{M} \mid\!\models \varphi$ sse $d_1^{\mathfrak{M}} = d_2^{\mathfrak{M}}$.
4. $\varphi \equiv \neg\psi$: $\mathfrak{M} \mid\!\models \varphi$ sse não $\mathfrak{M} \mid\!\models \psi$.
5. $\varphi \equiv (\psi \wedge \chi)$: $\mathfrak{M} \mid\!\models \varphi$ sse $\mathfrak{M} \mid\!\models \psi$ e $\mathfrak{M} \mid\!\models \chi$.
6. $\varphi \equiv (\psi \vee \chi)$: $\mathfrak{M} \mid\!\models \varphi$ sse $\mathfrak{M} \mid\!\models \psi$ ou $\mathfrak{M} \mid\!\models \chi$ (ou ambos).
7. $\varphi \equiv (\psi \to \chi)$: $\mathfrak{M} \mid\!\models \varphi$ sse não $\mathfrak{M} \mid\!\models \psi$ ou $\mathfrak{M} \mid\!\models \chi$ (ou ambos).
8. $\varphi \equiv \forall x\, \psi$: $\mathfrak{M} \mid\!\models \varphi$ sse para todo $a \in |\mathfrak{M}|$, $\mathfrak{M}[a/c] \mid\!\models \psi[c/x]$, se $c$ não ocorre em $\psi$.
9. $\varphi \equiv \exists x\, \psi$: $\mathfrak{M} \mid\!\models \varphi$ sse há um $a \in |\mathfrak{M}|$ tal que $\mathfrak{M}[a/c] \mid\!\models \psi[c/x]$, se $c$ não ocorre em $\psi$.

Sejam $x_1, \ldots, x_n$ todas as variáveis livres em $\varphi$, $c_1, \ldots, c_n$ símbolos de constante não presentes em $\varphi$, $a_1, \ldots, a_n \in |\mathfrak{M}|$, e $s(x_i) = a_i$.

Mostre que $\mathfrak{M}, s \vDash \varphi$ sse $\mathfrak{M}[a_1/c_1, \ldots, a_n/c_n] \mid\!\models \varphi[c_1/x_1] \ldots [c_n/x_n]$.

(Este problema mostra que é possível dar uma semântica para a lógica de primeira ordem que dispensa atribuições de variáveis.)

**Problema 16.7.** Suponha que $f$ é um símbolo de função não presente em $\varphi(x, y)$. Mostre que há a estrutura $\mathfrak{M}$ tal que $\mathfrak{M} \vDash \forall x\, \exists y\, \varphi(x, y)$ sse há uma $\mathfrak{M}'$ tal que $\mathfrak{M}' \vDash \forall x\, \varphi(x, f(x))$.

(Este problema é um caso especial do que é conhecido como Teorema de Skolem; $\forall x\, \varphi(x, f(x))$ é chamado de *forma normal de Skolem* de $\forall x\, \exists y\, \varphi(x, y)$.)

**Problema 16.8.** Faça a prova de Proposição 16.20 em detalhe.

**Problema 16.9.** Prove Proposição 16.23

**Problema 16.10.**

1. Mostre que $\Gamma \vDash \bot$ sse $\Gamma$ é insatisfatível.
2. Mostre que $\Gamma \cup \{\varphi\} \vDash \bot$ sse $\Gamma \vDash \neg\varphi$.
3. Suponha que $c$ não ocorre em $\varphi$ nem em $\Gamma$. Mostre que $\Gamma \vDash \forall x\, \varphi$ sse $\Gamma \vDash \varphi[c/x]$.

**Problema 16.11.** Complete a prova de Proposição 16.31.

# Capítulo 17

# Teorias e Seus Modelos

## 17.1 Introdução

O desenvolvimento do método axiomático é uma conquista significativa na história da ciência, e é de especial importância na história da matemática. Um desenvolvimento axiomático de um campo envolve o esclarecimento de muitas questões: Do que trata o campo? Quais são os conceitos mais fundamentais? Como eles se relacionam? Todos os conceitos do campo podem ser definidos em termos desses conceitos fundamentais? Que leis esses conceitos obedecem, e devem obedecer?

O método axiomático e a lógica foram feitos um para o outro. A lógica formal fornece as ferramentas para formular teorias axiomáticas, para provar teoremas a partir dos axiomas da teoria de uma maneira precisamente especificada, para estudar as propriedades de todos os sistemas que satisfazem os axiomas de uma maneira sistemática.

**Definição 17.1.** Um conjunto de sentenças $\Gamma$ é *fechado* sse, sempre que $\Gamma \models \varphi$ então $\varphi \in \Gamma$. O *fecho* de um conjunto de sentenças $\Gamma$ é $\{\varphi : \Gamma \models \varphi\}$.

Dizemos que $\Gamma$ é *axiomatizado por* um conjunto de sentenças $\Delta$ se $\Gamma$ é o fecho de $\Delta$.

Podemos pensar em uma teoria axiomática como o conjunto de sentenças que é axiomatizado por seu conjunto de axiomas $\Delta$. Em outras palavras, quando temos uma linguagem de primeira ordem que contém símbolos não lógicos para os primitivos da ciência desenvolvida axiomaticamente que desejamos estudar, juntamente com um conjunto de sentenças que expressam as leis fundamentais da ciência, podemos pensar na teoria como representada por todas as sentenças nessa linguagem que são consequência dos axiomas. Isso varia de exemplos simples com apenas um único primitivo e axiomas simples, como a teoria das ordens parciais, até teorias complexas como a mecânica newtoniana.

Os fatos lógicos importantes que tornam essa abordagem formal do método axiomático tão importante são os seguintes. Suponha que $\Gamma$ é um sistema de axiomas para uma teoria, isto é, um conjunto de sentenças.

1. Podemos afirmar precisamente quando um sistema de axiomas captura uma classe pretendida de estruturas. Isto é, se estamos interessados em uma certa classe de estruturas, capturaremos com sucesso essa classe por um sistema de axiomas $\Gamma$ sse as estruturas são exatamente aquelas $\mathfrak{M}$ tais que $\mathfrak{M} \vDash \Gamma$.

2. Podemos falhar nesse aspecto porque há $\mathfrak{M}$ tais que $\mathfrak{M} \vDash \Gamma$, mas $\mathfrak{M}$ não é uma das estruturas que pretendemos. Isso pode nos levar a adicionar axiomas que não são verdadeiros em $\mathfrak{M}$.

3. Se somos bem-sucedidos pelo menos no aspecto de que $\Gamma$ é verdadeiro em todas as estruturas pretendidas, então uma sentença $\varphi$ é verdadeira em todas as estruturas pretendidas sempre que $\Gamma \vDash \varphi$. Assim, podemos usar ferramentas lógicas (como métodos de derivação) para mostrar que sentenças são verdadeiras em todas as estruturas pretendidas simplesmente mostrando que elas são consequência dos axiomas.

4. Às vezes não temos estruturas pretendidas em mente, mas em vez disso partimos dos próprios axiomas: começamos com alguns primitivos que queremos que satisfaçam certas leis que codificamos em um sistema de axiomas. Uma coisa que gostaríamos de verificar imediatamente é que os axiomas não se contradizem: se o fizerem, não pode haver conceitos que obedeçam a essas leis, e teremos tentado estabelecer uma teoria incoerente. Podemos verificar que isso não acontece encontrando um modelo de $\Gamma$. E se há modelos da nossa teoria, podemos usar métodos lógicos para investigá-los, e também podemos usar métodos lógicos para construir modelos.

5. A independência dos axiomas é, igualmente, uma questão importante. Pode acontecer que um dos axiomas seja, na verdade, uma consequência dos outros, e seja, portanto, redundante. Podemos provar que um axioma $\varphi$ em $\Gamma$ é redundante provando $\Gamma \setminus \{\varphi\} \vDash \varphi$. Também podemos provar que um axioma não é redundante mostrando que $(\Gamma \setminus \{\varphi\}) \cup \{\neg\varphi\}$ é satisfatível. Por exemplo, foi assim que se mostrou que o postulado das paralelas é independente dos outros axiomas da geometria.

6. Outra questão importante é a da definibilidade de conceitos em uma teoria: A escolha da linguagem determina em que consistem os modelos de uma teoria. Mas nem todo aspecto de uma teoria deve ser representado separadamente em seus modelos. Por exemplo, toda ordenação $\leq$ determina uma ordenação estrita correspondente $<$—dada uma, nós podemos definir a outra. Então não é necessário que um modelo de uma

teoria que envolve tal ordem deva conter *também* a ordenação estrita correspondente. Quando é o caso, em geral, de que uma relação pode ser definida em termos de outras? Quando é impossível definir uma relação em termos de outras (e, portanto, deve-se adicioná-la aos primitivos da linguagem)?

## 17.2 Expressando Propriedades de Estruturas

Frequentemente é útil e importante expressar condições sobre funções e relações, ou, mais geralmente, que as funções e relações em uma estrutura satisfaçam essas condições. Por exemplo, nós gostaríamos de ter maneiras de distinguir aquelas estruturas para uma linguagem que "capturam" o que queremos que os símbolos de predicado "signifiquem" daquelas que não capturam. É claro que somos completamente livres para especificar quais estruturas "pretendemos", por exemplo, podemos especificar que a interpretação do símbolo de predicado $\leq$ deve ser uma ordenação, ou que estamos interessados apenas em interpretações de $\mathcal{L}$ nas quais o domínio consiste em conjuntos e $\in$ é interpretado pela relação "é um membro de". Mas podemos fazer isso com sentenças da linguagem? Em outras palavras, quais condições sobre a estrutura $\mathfrak{M}$ podemos expressar por a sentença (ou talvez um conjunto de sentenças) na linguagem de $\mathfrak{M}$? Há algumas condições que não conseguiremos expressar. Por exemplo, não há sentença de $\mathcal{L}_A$ que seja verdadeira em uma estrutura $\mathfrak{M}$ somente se $|\mathfrak{M}| = \mathbb{N}$. Não podemos expressar "o domínio contém apenas números naturais". Mas há "propriedades estruturais" de estruturas que talvez possamos expressar. Quais propriedades de estruturas podemos expressar por sentenças? Ou, dito de outra forma, quais coleções de estruturas podemos descrever como aquelas que tornam a sentença (ou conjunto de sentenças) verdadeira?

**Definição 17.2 (Modelo de um conjunto).** Seja $\Gamma$ um conjunto de sentenças em uma linguagem $\mathcal{L}$. Nós dizemos que a estrutura $\mathfrak{M}$ *é um modelo de* $\Gamma$ se $\mathfrak{M} \vDash \varphi$ para todo $\varphi \in \Gamma$.

**Exemplo 17.3.** A sentença $\forall x\, x \leq x$ é verdadeira em $\mathfrak{M}$ sse $\leq^{\mathfrak{M}}$ é uma relação reflexiva. A sentença $\forall x \forall y\, ((x \leq y \wedge y \leq x) \to x = y)$ é verdadeira em $\mathfrak{M}$ sse $\leq^{\mathfrak{M}}$ é antissimétrica. A sentença $\forall x \forall y \forall z\, ((x \leq y \wedge y \leq z) \to x \leq z)$ é verdadeira em $\mathfrak{M}$ sse $\leq^{\mathfrak{M}}$ é transitiva. Assim, os modelos de

$$\begin{aligned} \{ \quad & \forall x\, x \leq x, \\ & \forall x \forall y\, ((x \leq y \wedge y \leq x) \to x = y), \\ & \forall x \forall y \forall z\, ((x \leq y \wedge y \leq z) \to x \leq z) \quad \} \end{aligned}$$

são exatamente aquelas estruturas nas quais $\leq^{\mathfrak{M}}$ é reflexiva, antissimétrica e transitiva, isto é, uma ordem parcial. Portanto, podemos tomá-las como axiomas para a *teoria de primeira ordem das ordens parciais*.

## 17.3 Exemplos de Teorias de Primeira Ordem

**Exemplo 17.4.** A teoria das ordens lineares estritas na linguagem $\mathcal{L}_<$ é axiomatizada pelo conjunto

$$\begin{aligned}\{\quad & \forall x \neg x < x, \\ & \forall x \forall y \, ((x < y \vee y < x) \vee x = y), \\ & \forall x \forall y \forall z \, ((x < y \wedge y < z) \to x < z) \quad \}\end{aligned}$$

Ela captura completamente as estruturas pretendidas: toda ordem linear estrita é um modelo deste sistema de axiomas e, vice-versa, se $R$ é uma ordem linear sobre um conjunto $X$, então a estrutura $\mathfrak{M}$ com $|\mathfrak{M}| = X$ e $<^{\mathfrak{M}} = R$ é um modelo desta teoria.

**Exemplo 17.5.** A teoria dos grupos na linguagem $\mathtt{1}$ (símbolo de constante), $\cdot$ (símbolo de função de dois lugares) é axiomatizada por

$$\begin{aligned}&\forall x \, (x \cdot \mathtt{1}) = x \\ &\forall x \forall y \forall z \, (x \cdot (y \cdot z)) = ((x \cdot y) \cdot z) \\ &\forall x \exists y \, (x \cdot y) = \mathtt{1}\end{aligned}$$

**Exemplo 17.6.** A teoria da aritmética de Peano é axiomatizada pelas seguintes sentenças na linguagem da aritmética $\mathcal{L}_A$.

$$\begin{aligned}&\forall x \forall y \, (x' = y' \to x = y) \\ &\forall x \, \mathtt{0} \neq x' \\ &\forall x \, (x + \mathtt{0}) = x \\ &\forall x \forall y \, (x + y') = (x + y)' \\ &\forall x \, (x \times \mathtt{0}) = \mathtt{0} \\ &\forall x \forall y \, (x \times y') = ((x \times y) + x) \\ &\forall x \forall y \, (x < y \leftrightarrow \exists z \, (z' + x) = y)\end{aligned}$$

mais todas as sentenças da forma

$$(\varphi(\mathtt{0}) \wedge \forall x \, (\varphi(x) \to \varphi(x'))) \to \forall x \, \varphi(x)$$

Como há infinitas sentenças desta última forma, este sistema de axiomas é infinito. Esta última forma é chamada de *esquema de indução*. (Na verdade, o esquema de indução é um pouco mais complicado do que deixamos transparecer aqui.)

O último axioma é uma *definição explícita* de $<$.

**Exemplo 17.7.** A teoria dos conjuntos puros desempenha um papel importante nos fundamentos (e na filosofia) da matemática. Um conjunto é puro se

todos os seus membros são também conjuntos puros. O conjunto vazio conta, portanto, como puro, mas um conjunto que tem como um membro algo que não é um conjunto não seria puro. Então os conjuntos puros são aqueles que são formados apenas a partir do conjunto vazio e sem "urelementos", isto é, objetos que não são, eles próprios, conjuntos.

O seguinte poderia ser considerado um sistema de axiomas para uma teoria dos conjuntos puros:

$$\begin{aligned}
&\exists x \neg \exists y\, y \in x \\
&\forall x \forall y \, (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y) \\
&\forall x \forall y \exists z \forall u \, (u \in z \leftrightarrow (u = x \vee u = y)) \\
&\forall x \exists y \forall z \, (z \in y \leftrightarrow \exists u \, (z \in u \wedge u \in x))
\end{aligned}$$

mais todas as sentenças da forma

$$\exists x \forall y \, (y \in x \leftrightarrow \varphi(y))$$

O primeiro axioma diz que há um conjunto sem membros (isto é, $\emptyset$ existe); o segundo diz que conjuntos são extensionais; o terceiro que, para quaisquer conjuntos $X$ e $Y$, o conjunto $\{X, Y\}$ existe; o quarto que, para qualquer conjunto $X$, o conjunto $\cup X$ existe, onde $\cup X$ é a união de todos os elementos de $X$.

As sentenças mencionadas por último são chamadas coletivamente de *esquema de compreensão ingênuo*. Ele essencialmente diz que, para todo $\varphi(x)$, o conjunto $\{x : \varphi(x)\}$ existe—então, à primeira vista, um axioma verdadeiro, útil e talvez até necessário. É chamado de "ingênuo" porque, como se vê, ele torna esta teoria insatisfatível: se você toma $\varphi(y)$ como $\neg y \in y$, obtém a sentença

$$\exists x \forall y \, (y \in x \leftrightarrow \neg y \in y)$$

e esta sentença não é satisfeita em nenhuma estrutura.

**Exemplo 17.8.** Na área da *mereologia*, a relação de *parte* é uma relação fundamental. Assim como as teorias de conjuntos, há teorias de parte que axiomatizam várias concepções (às vezes conflitantes) dessa relação.

A linguagem da mereologia contém um único símbolo de predicado de dois lugares $P$, e $P(x, y)$ "significa" que $x$ é uma parte de $y$. Quando temos essa interpretação em mente, a estrutura para essa linguagem é chamada de *estrutura de parte*. É claro que nem toda estrutura para um único predicado de dois lugares realmente merecerá esse nome. Para ter uma chance de capturar "parte", $P^{\mathfrak{M}}$ deve satisfazer algumas condições, que podemos estabelecer como axiomas para uma teoria de parte. Por exemplo, a parte é uma ordem parcial sobre objetos: todo objeto é uma parte (ainda que uma parte *imprópria*) de si mesmo; dois objetos diferentes não podem ser partes um do outro; uma

parte de uma parte de um objeto é, ela própria, parte daquele objeto. Note que, nesse sentido, "é uma parte de" se assemelha a "é um subconjunto de", mas não se assemelha a "é um elemento de", que não é nem reflexiva nem transitiva.

$$\forall x\, P(x,x)$$
$$\forall x\, \forall y\, ((P(x,y) \wedge P(y,x)) \rightarrow x = y)$$
$$\forall x\, \forall y\, \forall z\, ((P(x,y) \wedge P(y,z)) \rightarrow P(x,z))$$

Além disso, quaisquer dois objetos têm uma soma mereológica (um objeto que tem esses dois objetos como partes, e é minimal nesse aspecto).

$$\forall x\, \forall y\, \exists z\, \forall u\, (P(z,u) \leftrightarrow (P(x,u) \wedge P(y,u)))$$

Estes são apenas alguns dos princípios básicos de parte considerados pelos metafísicos. Princípios adicionais, no entanto, rapidamente se tornam difíceis de formular ou escrever sem primeiro introduzir algumas relações definidas. Por exemplo, a maioria dos metafísicos interessados em mereologia também considera o seguinte como um princípio válido: sempre que um objeto $x$ tem uma parte própria $y$, ele também tem uma parte $z$ que não tem partes em comum com $y$, e tal que a fusão de $y$ e $z$ é $x$.

## 17.4 Expressando Relações em a Estrutura

Um uso principal que se pode dar às fórmulas é expressar propriedades e relações em a estrutura $\mathfrak{M}$ em termos dos primitivos da linguagem $\mathcal{L}$ de $\mathfrak{M}$. Com isso queremos dizer o seguinte: o domínio de $\mathfrak{M}$ é um conjunto de objetos. Os símbolos de constante, símbolos de função e símbolos de predicado são interpretados em $\mathfrak{M}$ por alguns objetos em $|\mathfrak{M}|$, funções sobre $|\mathfrak{M}|$, e relações sobre $|\mathfrak{M}|$. Por exemplo, se $A^2_0$ está em $\mathcal{L}$, então $\mathfrak{M}$ atribui a ele uma relação $R = A^{2\mathfrak{M}}_0$. Então a fórmula $A^2_0(v_1, v_2)$ *expressa* exatamente essa relação, no seguinte sentido: se uma atribuição de variáveis $s$ mapeia $v_1$ para $a \in |\mathfrak{M}|$ e $v_2$ para $b \in |\mathfrak{M}|$, então

$$Rab \quad \text{sse} \quad \mathfrak{M}, s \vDash A^2_0(v_1, v_2).$$

Note que temos que envolver atribuições de variáveis aqui: não podemos simplesmente dizer "$Rab$ sse $\mathfrak{M} \vDash A^2_0(a,b)$" porque $a$ e $b$ não são símbolos da nossa linguagem: eles são membros de $|\mathfrak{M}|$.

Como não temos apenas fórmulas atômicas, mas podemos combiná-las usando os conectivos lógicos e os quantificadores, fórmulas mais complexas podem definir outras relações que não estão diretamente embutidas em $\mathfrak{M}$. Estamos interessados em como fazer isso e, especificamente, quais relações podemos definir em a estrutura.

**Definição 17.9.** Seja $\varphi(v_1, \ldots, v_n)$ a fórmula de $\mathcal{L}$ na qual apenas $v_1, \ldots, v_n$ ocorrem livres, e seja $\mathfrak{M}$ a estrutura para $\mathcal{L}$. $\varphi(v_1, \ldots, v_n)$ *expressa a relação* $R \subseteq |\mathfrak{M}|^n$ sse

$$Ra_1 \ldots a_n \quad \text{sse} \quad \mathfrak{M}, s \vDash \varphi(v_1, \ldots, v_n)$$

para qualquer atribuição de variáveis $s$ com $s(v_i) = a_i$ $(i = 1, \ldots, n)$.

**Exemplo 17.10.** No modelo padrão da aritmética $\mathfrak{N}$, a fórmula $v_1 < v_2 \vee v_1 = v_2$ expressa a relação $\leq$ sobre $\mathbb{N}$. A fórmula $v_2 = v_1'$ expressa a relação sucessora, isto é, a relação $R \subseteq \mathbb{N}^2$ onde $Rnm$ vale se $m$ é o sucessor de $n$. A fórmula $v_1 = v_2'$ expressa a relação predecessora. As fórmulas $\exists v_3 \, (v_3 \neq 0 \wedge v_2 = (v_1 + v_3))$ e $\exists v_3 \, (v_1 + v_3{}') = v_2$ ambas expressam a relação $<$. Isso significa que o símbolo de predicado $<$ é, na verdade, supérfluo na linguagem da aritmética; ele pode ser definido.

Essa ideia não é interessante apenas em estruturas específicas, mas geralmente sempre que usamos uma linguagem para descrever um modelo ou modelos pretendidos, isto é, quando consideramos teorias. Essas teorias frequentemente contêm apenas alguns símbolos de predicado como símbolos básicos, mas no domínio que elas são usadas para descrever muitas outras relações frequentemente desempenham um papel importante. Se essas outras relações podem ser sistematicamente expressas pelas relações que interpretam os símbolos de predicado básicos da linguagem, nós dizemos que podemos *defini-las* na linguagem.

## 17.5 A Teoria dos Conjuntos

Quase toda a matemática pode ser desenvolvida na teoria dos conjuntos. Desenvolver a matemática nessa teoria envolve uma série de coisas. Primeiro, requer um conjunto de axiomas para a relação $\in$. Vários sistemas de axiomas diferentes foram desenvolvidos, às vezes com propriedades conflitantes de $\in$. O sistema de axiomas conhecido como **ZFC**, a teoria dos conjuntos de Zermelo–Fraenkel com o axioma da escolha, destaca-se: é de longe o mais amplamente usado e estudado, porque acontece que seus axiomas bastam para provar quase todas as coisas que os matemáticos esperam ser capazes de provar. Mas antes que isso possa ser estabelecido, é primeiro necessário deixar claro como podemos sequer *expressar* todas as coisas que os matemáticos gostariam de expressar. Para começar, a linguagem não contém símbolos de constante nem símbolos de função, então parece, à primeira vista, pouco claro que possamos falar sobre conjuntos particulares (como $\emptyset$ ou $\mathbb{N}$), falar sobre operações sobre conjuntos (como $X \cup Y$ e $\wp(X)$), muito menos outras construções que envolvem coisas diferentes de conjuntos, como relações e funções.

Para começar, "é um elemento de" não é a única relação na qual estamos interessados: "é um subconjunto de" parece quase tão importante. Mas nós

podemos *definir* "é um subconjunto de" em termos de "é um elemento de". Para fazer isso, temos que encontrar a fórmula $\varphi(x, y)$ na linguagem da teoria dos conjuntos que é satisfeita por um par de conjuntos $\langle X, Y\rangle$ sse $X \subseteq Y$. Mas $X$ é um subconjunto de $Y$ exatamente quando todos os membros de $X$ são também membros de $Y$. Então podemos definir $\subseteq$ pela fórmula

$$\forall z\,(z \in x \to z \in y)$$

Agora, sempre que quisermos usar a relação $\subseteq$ em uma fórmula, nós poderíamos, em vez disso, usar aquela fórmula (com $x$ e $y$ adequadamente substituídos, e a variável ligada $z$ renomeada se necessário). Por exemplo, a extensionalidade dos conjuntos significa que se quaisquer conjuntos $x$ e $y$ estão contidos um no outro, então $x$ e $y$ devem ser o mesmo conjunto. Isso pode ser expresso por $\forall x\,\forall y\,((x \subseteq y \wedge y \subseteq x) \to x = y)$, ou, se substituirmos $\subseteq$ pela definição acima, por

$$\forall x\,\forall y\,((\forall z\,(z \in x \to z \in y) \wedge \forall z\,(z \in y \to z \in x)) \to x = y).$$

Este é, de fato, um dos axiomas de **ZFC**, o "axioma da extensionalidade".

Não há símbolo de constante para $\emptyset$, mas podemos expressar "$x$ é vazio" por $\neg\exists y\, y \in x$. Então "$\emptyset$ existe" torna-se a sentença $\exists x\,\neg\exists y\, y \in x$. Este é outro axioma de **ZFC**. (Note que o axioma da extensionalidade implica que há apenas um conjunto vazio.) Sempre que quisermos falar sobre $\emptyset$ na linguagem da teoria dos conjuntos, nós escreveríamos isso como "há um conjunto que é vazio e ..." Como exemplo, para expressar o fato de que $\emptyset$ é um subconjunto de todo conjunto, poderíamos escrever

$$\exists x\,(\neg\exists y\, y \in x \wedge \forall z\, x \subseteq z)$$

onde, é claro, $x \subseteq z$ teria, por sua vez, que ser substituído por sua definição.

Para falar sobre operações sobre conjuntos, como $X \cup Y$ e $\wp(X)$, nós temos que usar um truque semelhante. Não há símbolos de função na linguagem da teoria dos conjuntos, mas podemos expressar as relações funcionais $X \cup Y = Z$ e $\wp(X) = Y$ por

$$\forall u\,((u \in x \vee u \in y) \leftrightarrow u \in z)$$
$$\forall u\,(u \subseteq x \leftrightarrow u \in y)$$

já que os membros de $X \cup Y$ são exatamente os conjuntos que são ou membros de $X$ ou membros de $Y$, e os membros de $\wp(X)$ são exatamente os subconjuntos de $X$. No entanto, isso não nos permite usar $x \cup y$ ou $\wp(x)$ como se fossem termos: só podemos usar as fórmulas inteiras que definem as relações $X \cup Y = Z$ e $\wp(X) = Y$. De fato, não sabemos que essas relações são alguma vez satisfeitas, isto é, não sabemos que uniões e conjuntos potência sempre existem. Por exemplo, a sentença $\forall x\,\exists y\,\wp(x) = y$ é outro axioma de **ZFC** (o axioma do conjunto potência).

E quanto a falar de pares ordenados ou funções? Aqui temos que explicar como podemos pensar em pares ordenados e funções como tipos especiais de conjuntos. Uma maneira de definir o par ordenado $\langle x, y\rangle$ é como o conjunto $\{\{x\}, \{x, y\}\}$. Mas, como antes, não podemos introduzir a símbolo de função que nomeie esse conjunto; só podemos definir a relação $\langle x, y\rangle = z$, isto é, $\{\{x\}, \{x, y\}\} = z$:

$$\forall u\,(u \in z \leftrightarrow (\forall v\,(v \in u \leftrightarrow v = x) \vee \forall v\,(v \in u \leftrightarrow (v = x \vee v = y))))$$

Isso diz que os membros $u$ de $z$ são exatamente aqueles conjuntos que ou têm $x$ como seu único membro ou têm $x$ e $y$ como seus únicos membros (em outras palavras, aqueles conjuntos que são ou idênticos a $\{x\}$ ou idênticos a $\{x, y\}$). Uma vez que temos isso, podemos dizer outras coisas, por exemplo, que $X \times Y = Z$:

$$\forall z\,(z \in Z \leftrightarrow \exists x\,\exists y\,(x \in X \wedge y \in Y \wedge \langle x, y\rangle = z))$$

Uma função $f\colon X \to Y$ pode ser pensada como a relação $f(x) = y$, isto é, como o conjunto de pares $\{\langle x, y\rangle : f(x) = y\}$. Nós podemos então dizer que um conjunto $f$ é uma função de $X$ em $Y$ se (a) é uma relação $\subseteq X \times Y$, (b) é total, isto é, para todo $x \in X$ há algum $y \in Y$ tal que $\langle x, y\rangle \in f$ e (c) é funcional, isto é, sempre que $\langle x, y\rangle, \langle x, y'\rangle \in f$, $y = y'$ (porque os valores de funções devem ser únicos). Então "$f$ é uma função de $X$ em $Y$" pode ser escrito como:

$$\begin{aligned}&\forall u\,(u \in f \to \exists x\,\exists y\,(x \in X \wedge y \in Y \wedge \langle x, y\rangle = u)) \wedge\\ &\forall x\,(x \in X \to (\exists y\,(y \in Y \wedge \text{mapeia}(f, x, y)) \wedge\\ &\qquad\qquad (\forall y\,\forall y'\,((\text{mapeia}(f, x, y) \wedge \text{mapeia}(f, x, y')) \to y = y')))\end{aligned}$$

onde $\text{mapeia}(f, x, y)$ abrevia $\exists v\,(v \in f \wedge \langle x, y\rangle = v)$ (esta fórmula expressa "$f(x) = y$").

Agora também não é difícil expressar que $f\colon X \to Y$ é injetiva, por exemplo:

$$\begin{aligned}f\colon X \to Y \wedge \forall x\,\forall x'\,((x \in X \wedge x' \in X \wedge\\ \exists y\,(\text{mapeia}(f, x, y) \wedge \text{mapeia}(f, x', y))) \to x = x')\end{aligned}$$

Uma função $f\colon X \to Y$ é injetiva sse, sempre que $f$ mapeia $x, x' \in X$ para um único $y$, $x = x'$. Se abreviarmos esta fórmula como $\text{inj}(f, X, Y)$, já estamos em posição de afirmar na linguagem da teoria dos conjuntos algo tão não trivial quanto o teorema de Cantor: não há função injetiva de $\wp(X)$ em $X$:

$$\forall X\,\forall Y\,(\wp(X) = Y \to \neg\exists f\,\text{inj}(f, Y, X))$$

Poderíamos pensar que a teoria dos conjuntos requer outro axioma que garanta a existência de um conjunto para toda propriedade definidora. Se

$\varphi(x)$ é uma fórmula da teoria dos conjuntos com a variável $x$ livre, podemos considerar a sentença

$$\exists y \, \forall x \, (x \in y \leftrightarrow \varphi(x)).$$

Esta sentença afirma que há um conjunto $y$ cujos membros são todos e somente aqueles $x$ que satisfazem $\varphi(x)$. Este esquema é chamado de "princípio da compreensão". Parece muito útil; infelizmente é inconsistente. Tome $\varphi(x) \equiv \neg x \in x$, então o princípio da compreensão afirma

$$\exists y \, \forall x \, (x \in y \leftrightarrow x \notin x),$$

isto é, afirma a existência de um conjunto de todos os conjuntos que não são membros de si mesmos. Nenhum tal conjunto pode existir—este é o Paradoxo de Russell. **ZFC**, de fato, contém uma versão restrita—e consistente—deste princípio, o princípio da separação:

$$\forall z \, \exists y \, \forall x \, (x \in y \leftrightarrow (x \in z \wedge \varphi(x)).$$

## 17.6 Expressando o Tamanho de Estruturas

Há algumas propriedades de estruturas que podemos expressar mesmo sem usar os símbolos não lógicos de uma linguagem. Por exemplo, há sentenças que são verdadeiras em a estrutura se, e somente se, o domínio da estrutura tem pelo menos, no máximo ou exatamente um certo número $n$ de membros.

**Proposição 17.11.** *A sentença*

$$\begin{aligned}\varphi_{\geq n} \equiv \exists x_1 \, \exists x_2 \, \ldots \exists x_n \\ (x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_1 \neq x_4 \wedge \cdots \wedge x_1 \neq x_n \wedge \\ x_2 \neq x_3 \wedge x_2 \neq x_4 \wedge \cdots \wedge x_2 \neq x_n \wedge \\ \vdots \\ x_{n-1} \neq x_n)\end{aligned}$$

*é verdadeira em a estrutura $\mathfrak{M}$ se, e somente se, $|\mathfrak{M}|$ contém pelo menos n membros. Consequentemente, $\mathfrak{M} \vDash \neg\varphi_{\geq n+1}$ se, e somente se, $|\mathfrak{M}|$ contém no máximo n membros.*

**Proposição 17.12.** *A sentença*

$$\begin{aligned}\varphi_{=n} \equiv \exists x_1\, \exists x_2\, \ldots \exists x_n \\ (x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_1 \neq x_4 \wedge \cdots \wedge x_1 \neq x_n \wedge \\ x_2 \neq x_3 \wedge x_2 \neq x_4 \wedge \cdots \wedge x_2 \neq x_n \wedge \\ \vdots \\ x_{n-1} \neq x_n \wedge \\ \forall y\, (y = x_1 \vee \cdots \vee y = x_n))\end{aligned}$$

*é verdadeira em a estrutura $\mathfrak{M}$ se, e somente se, $|\mathfrak{M}|$ contém exatamente n membros.*

**Proposição 17.13.** *Uma estrutura é infinita se, e somente se, é um modelo de*

$$\{\varphi_{\geq 1}, \varphi_{\geq 2}, \varphi_{\geq 3}, \ldots\}.$$

Não há uma única sentença puramente lógica que seja verdadeira em $\mathfrak{M}$ se, e somente se, $|\mathfrak{M}|$ é infinito. No entanto, pode-se dar sentenças com símbolos de predicado não lógicos que só têm modelos infinitos (embora nem toda estrutura infinita seja modelo delas). A propriedade de ser uma estrutura finita e a propriedade de ser uma estrutura não enumerável nem sequer podem ser expressas com um conjunto infinito de sentenças. Estes fatos seguem dos teoremas da compacidade e de Löwenheim–Skolem.

## Problemas

**Problema 17.1.** Encontre fórmulas em $\mathcal{L}_A$ que definam as seguintes relações:

1. $n$ está entre $i$ e $j$;
2. $n$ divide $m$ exatamente (isto é, $m$ é um múltiplo de $n$);
3. $n$ é um número primo (isto é, nenhum número além de 1 e $n$ divide $n$ exatamente).

**Problema 17.2.** Suponha que a fórmula $\varphi(v_1, v_2)$ expressa a relação $R \subseteq |\mathfrak{M}|^2$ em a estrutura $\mathfrak{M}$. Encontre fórmulas que expressem as seguintes relações:

1. a inversa $R^{-1}$ de $R$;
2. o produto relativo $R \mid R$;

Você consegue encontrar uma maneira de expressar $R^+$, o fecho transitivo de $R$?

**Problema 17.3.** Seja $\mathcal{L}$ a linguagem contendo apenas um símbolo de predicado de 2 lugares $<$ (sem outros símbolos de constante, símbolos de função ou símbolos de predicado— exceto, é claro, $=$). Seja $\mathfrak{N}$ a estrutura tal que $|\mathfrak{N}| = \mathbb{N}$, e $<^{\mathfrak{N}} = \{\langle n, m\rangle : n < m\}$. Prove o seguinte:

1. $\{0\}$ é definível em $\mathfrak{N}$;
2. $\{1\}$ é definível em $\mathfrak{N}$;
3. $\{2\}$ é definível em $\mathfrak{N}$;
4. para cada $n \in \mathbb{N}$, o conjunto $\{n\}$ é definível em $\mathfrak{N}$;
5. todo subconjunto finito de $|\mathfrak{N}|$ é definível em $\mathfrak{N}$;
6. todo subconjunto cofinito de $|\mathfrak{N}|$ é definível em $\mathfrak{N}$ (onde $X \subseteq \mathbb{N}$ é cofinito sse $\mathbb{N} \setminus X$ é finito).

**Problema 17.4.** Mostre que o princípio da compreensão é inconsistente dando a derivação que mostre

$$\exists y\, \forall x\, (x \in y \leftrightarrow x \notin x) \vdash \bot.$$

Pode ajudar mostrar primeiro $(A \to \neg A) \wedge (\neg A \to A) \vdash \bot$.

# Capítulo 18

# Sistemas de Derivação

Este capítulo reúne material geral sobre sistemas de derivação. Um livro-texto que usa um sistema específico pode inserir a seção de introdução mais a seção de panorama relevante no início do capítulo que introduz esse sistema.

## 18.1 Introdução

As lógicas comumente têm tanto uma semântica quanto um sistema de derivação. A semântica trata de conceitos como verdade, satisfatibilidade, validade e consequência. O propósito dos sistemas de derivação é fornecer um método puramente sintático de estabelecer consequência e validade. Eles são puramente sintáticos no sentido de que uma derivação em tal sistema é um objeto sintático finito, geralmente uma sequência (ou outra disposição finita) de sentenças ou fórmulas. Bons sistemas de derivação têm a propriedade de que qualquer sequência ou disposição dada de sentenças ou fórmulas pode ser verificada mecanicamente como "correta".

Os sistemas de derivação mais simples (e historicamente os primeiros) para a lógica de primeira ordem foram *axiomáticos*. Uma sequência de fórmulas conta como uma derivação em tal sistema se cada fórmula individual nela é ou está entre um conjunto fixo de "axiomas" ou segue de fórmulas anteriores na sequência por uma entre um número fixo de "regras de inferência"—e pode ser verificado mecanicamente se uma fórmula é um axioma e se segue corretamente de outras fórmulas por uma das regras de inferência. Sistemas de derivação axiomáticos são fáceis de descrever—e também fáceis de tratar meta-teoricamente—mas as derivações neles são difíceis de ler e entender, e também difíceis de produzir.

Outros sistemas de derivação foram desenvolvidos com o objetivo de facilitar a construção de derivações ou facilitar a compreensão de derivações

uma vez completas. Exemplos são a dedução natural, árvores de verdade, também conhecidas como provas por tableaux, e o cálculo de sequentes. Alguns sistemas de derivação são projetados especialmente com a mecanização em mente; por exemplo, o método da resolução é fácil de implementar em software (mas suas derivações são essencialmente impossíveis de entender). A maioria desses outros sistemas de derivação representa derivações como árvores de fórmulas em vez de sequências. Isso facilita ver quais partes de uma derivação dependem de quais outras partes.

Assim, para uma dada lógica, como a lógica de primeira ordem, os diferentes sistemas de derivação darão diferentes explicações do que significa uma sentença ser um *teorema* e o que significa uma sentença ser derivável a partir de outras. Seja como for feito isso (via derivações axiomáticas, deduções naturais, derivações de sequentes, árvores de verdade, refutações por resolução), queremos que essas relações correspondam às noções semânticas de validade e consequência. Escrevamos $\vdash \varphi$ para "$\varphi$ é um teorema" e "$\Gamma \vdash \varphi$" para "$\varphi$ é derivável de $\Gamma$." Seja como for $\vdash$ definido, queremos que corresponda a $\vDash$, isto é:

1. $\vdash \varphi$ se, e somente se, $\vDash \varphi$
2. $\Gamma \vdash \varphi$ se, e somente se, $\Gamma \vDash \varphi$

A direção "somente se" acima é chamada de *correção*. Um sistema de derivação é correto se a derivabilidade garante consequência (ou validade). Todo sistema de derivação decente tem que ser correto; sistemas de derivação incorretos não são úteis de modo algum. Afinal, o propósito inteiro de uma derivação é fornecer uma garantia sintática de validade ou consequência. Provaremos a correção para os sistemas de derivação que apresentamos.

A direção conversa "se" também é importante: é chamada de *completude*. Um sistema de derivação completo é forte o suficiente para mostrar que $\varphi$ é um teorema sempre que $\varphi$ é válida, e que $\Gamma \vdash \varphi$ sempre que $\Gamma \vDash \varphi$. A completude é mais difícil de estabelecer, e algumas lógicas não têm sistemas de derivação completos. A lógica de primeira ordem tem. Kurt Gödel foi o primeiro a provar a completude para um sistema de derivação da lógica de primeira ordem em sua dissertação de 1929.

Outro conceito ligado aos sistemas de derivação é o de *consistência*. Um conjunto de sentenças é chamado inconsistente se qualquer coisa pode ser derivada dele, e consistente caso contrário. A inconsistência é a contrapartida sintática da insatisfatibilidade: como conjuntos insatisfatíveis, conjuntos inconsistentes de sentenças não fazem boas teorias; são defeituosos de maneira fundamental. Conjuntos consistentes de sentenças podem não ser verdadeiros ou úteis, mas pelo menos passam esse limiar mínimo de utilidade lógica. Para diferentes sistemas de derivação, a definição específica de consistência de conjuntos de sentenças pode diferir, mas como $\vdash$, queremos que a consistência coincida com sua contrapartida semântica, a satisfatibilidade. Queremos que

seja sempre o caso que $\Gamma$ é consistente se, e somente se, é satisfatível. Aqui, a direção "somente se" corresponde à completude (consistência garante satisfatibilidade), e a direção "se" corresponde à correção (satisfatibilidade garante consistência). De fato, para a lógica clássica de primeira ordem, as duas versões de correção e completude são equivalentes.

## 18.2 O Cálculo de Sequentes

Enquanto muitos sistemas de derivação operam com disposições de sentenças, o cálculo de sequentes opera com *sequentes*. Um sequente é uma expressão da forma

$$\varphi_1, \ldots, \varphi_m \Rightarrow \psi_1, \ldots, \psi_m,$$

isto é, um par de sequências de sentenças, separadas pelo símbolo de sequente $\Rightarrow$. Qualquer uma das sequências pode ser vazia. Uma derivação no cálculo de sequentes é uma árvore de sequentes, em que os sequentes mais altos são de uma forma especial (são chamados de "sequentes iniciais" ou "axiomas") e todo outro sequente segue dos sequentes imediatamente acima dele por uma das regras de inferência. As regras de inferência ou manipulam as sentenças nos sequentes (adicionando, removendo ou rearranjando-as à esquerda ou à direita), ou introduzem uma fórmula complexa na conclusão da regra. Por exemplo, a regra $\wedge$L permite a inferência de $\varphi, \Gamma \Rightarrow \Delta$ para $\varphi \wedge \psi, \Gamma \Rightarrow \Delta$, e a $\rightarrow$R permite a inferência de $\varphi, \Gamma \Rightarrow \Delta, \psi$ para $\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi$, para quaisquer $\Gamma$, $\Delta$, $\varphi$ e $\psi$. (Em particular, $\Gamma$ e $\Delta$ podem ser vazios.)

A relação $\vdash$ baseada no cálculo de sequentes é definida da seguinte forma: $\Gamma \vdash \varphi$ se, e somente se, há alguma sequência $\Gamma_0$ tal que toda $\varphi$ em $\Gamma_0$ está em $\Gamma$ e há uma derivação com o sequente $\Gamma_0 \Rightarrow \varphi$ em sua raiz. $\varphi$ é um teorema no cálculo de sequentes se o sequente $\Rightarrow \varphi$ tem uma derivação. Por exemplo, aqui está uma derivação que mostra que $\vdash (\varphi \wedge \psi) \rightarrow \varphi$:

$$\dfrac{\dfrac{\varphi \Rightarrow \varphi}{\varphi \wedge \psi \Rightarrow \varphi}\,\wedge\text{L}}{\Rightarrow (\varphi \wedge \psi) \rightarrow \varphi}\,\rightarrow\text{R}$$

Um conjunto $\Gamma$ é inconsistente no cálculo de sequentes se há uma derivação de $\Gamma_0 \Rightarrow$ (em que toda $\varphi \in \Gamma_0$ está em $\Gamma$ e o lado direito do sequente é vazio). Usando a regra WR, qualquer sentença pode ser derivada a partir de um conjunto inconsistente.

O cálculo de sequentes foi inventado na década de 1930 por Gerhard Gentzen. Por causa de seu desenho sistemático e simétrico, é um formalismo muito útil para desenvolver uma teoria de derivações. É relativamente fácil encontrar derivações no cálculo de sequentes, mas essas derivações são frequentemente difíceis de ler e sua conexão com provas às vezes não é fácil de ver. Provou ser uma abordagem muito elegante a sistemas de derivação, no entanto, e muitas lógicas têm sistemas de cálculo de sequentes.

## 18.3 Dedução Natural

A dedução natural é um sistema de derivação destinado a espelhar o raciocínio real (especialmente o tipo de raciocínio regimentado empregado por matemáticos). O raciocínio real procede por vários padrões "naturais". Por exemplo, a prova por casos nos permite estabelecer uma conclusão com base em uma premissa disjuntiva, estabelecendo que a conclusão segue de qualquer um dos disjuntos. A prova indireta nos permite estabelecer uma conclusão mostrando que sua negação leva a uma contradição. A prova condicional estabelece uma afirmação condicional "se ... então ..." mostrando que o consequente segue do antecedente. A dedução natural é uma formalização de algumas dessas inferências naturais. Cada um dos conectivos lógicos e quantificadores vem com duas regras, uma de introdução e uma de eliminação, e cada uma corresponde a um desses padrões de inferência natural. Por exemplo, $\rightarrow$Intro corresponde à prova condicional, e $\vee$Elim à prova por casos. Uma regra particularmente simples é $\wedge$Elim, que permite a inferência de $\varphi \wedge \psi$ para $\varphi$ (ou $\psi$).

Uma característica que distingue a dedução natural de outros sistemas de derivação é o uso de hipóteses. Uma derivação em dedução natural é uma árvore de fórmulas. Uma única fórmula fica na raiz da árvore de fórmulas, e as "folhas" da árvore são fórmulas das quais a conclusão é derivada. Na dedução natural, algumas fórmulas folha desempenham um papel dentro da derivação, mas são "consumidas" quando a derivação atinge a conclusão. Isso corresponde à prática, no raciocínio real, de introduzir hipóteses que só permanecem em vigor por um curto período. Por exemplo, em uma prova por casos, assumimos a verdade de cada um dos disjuntos; na prova condicional, assumimos a verdade do antecedente; na prova indireta, assumimos a verdade da negação da conclusão. Essa maneira de introduzir hipóteses hipotéticas e depois descartá-las a serviço de estabelecer um passo intermediário é uma marca da dedução natural. As fórmulas nas folhas de uma derivação em dedução natural são chamadas de hipóteses, e algumas das regras de inferência podem descarregá-las. Por exemplo, se temos uma derivação de $\psi$ a partir de algumas hipóteses que incluem $\varphi$, então a regra $\rightarrow$Intro nos permite inferir $\varphi \rightarrow \psi$ e descartar qualquer hipótese da forma $\varphi$. (Para acompanhar quais hipóteses são descartadas em quais inferências, rotulamos a inferência e as hipóteses que ela descarta com um número.) As hipóteses que permanecem não descarregadas no final da derivação são, juntas, suficientes para a verdade da conclusão, de modo que uma derivação estabelece que suas hipóteses não descarregadas implicam sua conclusão.

A relação $\Gamma \vdash \varphi$ baseada na dedução natural vale se, e somente se, há uma derivação em que $\varphi$ é a última sentença na árvore, e toda folha que está não descarregada está em $\Gamma$. $\varphi$ é um teorema na dedução natural se, e somente se, há uma derivação em que $\varphi$ é a última sentença e todas as hipóteses são descarregadas. Por exemplo, aqui está uma derivação que mostra que $\vdash (\varphi \wedge$

$\psi) \to \varphi$:

$$\dfrac{\dfrac{[\varphi \wedge \psi]^1}{\varphi}\,\wedge\text{Elim}}{(\varphi \wedge \psi) \to \varphi}\,{}^{1}\,\to\text{Intro}$$

O rótulo 1 indica que a hipótese $\varphi \wedge \psi$ é descarregada na inferência $\to$Intro.

Um conjunto $\Gamma$ é inconsistente se, e somente se, $\Gamma \vdash \bot$ na dedução natural. A regra $\bot_I$ faz com que, a partir de um conjunto inconsistente, qualquer sentença possa ser derivada.

Sistemas de dedução natural foram desenvolvidos por Gerhard Gentzen e Stanisław Jaśkowski na década de 1930, e depois por Dag Prawitz e Frederic Fitch. Porque suas inferências espelham métodos naturais de prova, é favorecida por filósofos. As versões desenvolvidas por Fitch são frequentemente usadas em livros introdutórios de lógica. Na filosofia da lógica, as regras da dedução natural às vezes foram tomadas como dando os significados dos operadores lógicos ("semântica da Teoria da Prova").

## 18.4 Tableaux

Enquanto muitos sistemas de derivação operam com disposições de sentenças, os tableaux operam com fórmulas assinadas. A fórmula assinada é um par consistindo em um sinal de valor de verdade ($\mathbb{T}$ ou $\mathbb{F}$) e a sentença

$$\mathbb{T}\varphi \text{ ou } \mathbb{F}\varphi.$$

A tableau consiste em fórmulas assinadas dispostas em uma árvore ramificada para baixo. Começa com várias *hipóteses* e continua com fórmulas assinadas que resultam de uma das fórmulas assinadas acima dela pela aplicação de uma das regras de inferência. Cada regra nos permite adicionar uma ou mais fórmulas assinadas ao final de um ramo, ou duas fórmulas assinadas lado a lado—neste caso um ramo se divide em dois, com as duas fórmulas assinadas adicionadas formando os finais dos dois ramos.

Uma regra aplicada a uma fórmula assinada complexa resulta na adição de fórmulas assinadas que são sub-fórmulas imediatas. Elas vêm em pares, uma regra para cada um dos dois sinais. Por exemplo, a regra $\wedge\mathbb{T}$ se aplica a $\mathbb{T}\varphi \wedge \psi$, e permite a adição tanto das duas fórmulas assinadas $\mathbb{T}\varphi$ quanto de $\mathbb{T}\psi$ ao final de qualquer ramo que contém $\mathbb{T}\varphi \wedge \psi$, e a regra $\varphi \wedge \psi\mathbb{F}$ permite que um ramo seja dividido adicionando $\mathbb{F}\varphi$ e $\mathbb{F}\psi$ lado a lado. A tableau é fechado se cada um de seus ramos contém um par correspondente de fórmulas assinadas $\mathbb{T}\varphi$ e $\mathbb{F}\varphi$.

A relação $\vdash$ baseada em tableaux é definida da seguinte forma: $\Gamma \vdash \varphi$ se, e somente se, há algum conjunto finito $\Gamma_0 = \{\psi_1, \ldots, \psi_n\} \subseteq \Gamma$ tal que há um tableau fechado para as hipóteses

$$\{\mathbb{F}\varphi, \mathbb{T}\psi_1, \ldots, \mathbb{T}\psi_n\}$$

Por exemplo, aqui está um tableau fechado que mostra que $\vdash (\varphi \wedge \psi) \to \varphi$:

| | | |
|---|---|---|
| 1. | $\mathbb{F}\,(\varphi \wedge \psi) \to \varphi$ | Assumption |
| 2. | $\mathbb{T}\,\varphi \wedge \psi$ | $\to\mathbb{F}\,1$ |
| 3. | $\mathbb{F}\,\varphi$ | $\to\mathbb{F}\,1$ |
| 4. | $\mathbb{T}\,\varphi$ | $\to\mathbb{T}\,2$ |
| 5. | $\mathbb{T}\,\psi$ | $\to\mathbb{T}\,2$ |
| | $\otimes$ | |

Um conjunto $\Gamma$ é inconsistente no cálculo de tableau se há um tableau fechado para hipóteses

$$\{\mathbb{T}\,\psi_1, \ldots, \mathbb{T}\,\psi_n\}$$

para algum $\psi_i \in \Gamma$.

Os Tableaux foram inventados na década de 1950 independentemente por Evert Beth e Jaakko Hintikka, e simplificados e popularizados por Raymond Smullyan. São muito fáceis de usar, pois construir um tableau é um procedimento muito sistemático. Por causa da natureza sistemática dos tableaux, eles também se prestam à implementação por computador. No entanto, um tableau é frequentemente difícil de ler e sua conexão com provas às vezes não é fácil de ver. A abordagem também é bastante geral, e muitas lógicas diferentes têm sistemas de tableau. Os Tableaux também nos ajudam a encontrar estruturas que satisfazem sentenças (ou conjuntos de sentenças) dadas: se o conjunto é satisfatível, ele não terá um tableau fechado, isto é, qualquer tableau terá um ramo aberto. A estrutura satisfatória pode ser "lida" de um ramo aberto, desde que toda regra que seja possível aplicar tenha sido aplicada naquele ramo. Há também uma conexão muito estreita com o cálculo de sequentes: essencialmente, um tableau fechado é uma derivação condensada no cálculo de sequentes, escrita de cabeça para baixo.

## 18.5 Dedução Axiomática

As derivações axiomáticas são os sistemas de derivação lógicos mais antigos e mais simples. Suas derivações são simplesmente sequências de sentenças. Uma sequência de sentenças conta como uma derivação correta se toda sentença $\varphi$ nela satisfaz uma das seguintes condições:

1. $\varphi$ é um axioma, ou
2. $\varphi$ é um membro de um dado conjunto $\Gamma$ de sentenças, ou
3. $\varphi$ é justificada por uma regra de inferência.

Para ser um axioma, $\varphi$ tem que ter a forma de um entre vários esquemas fixos de sentença. Há muitos conjuntos de esquemas de axiomas que fornecem

um sistema de derivação satisfatório (correto e completo) para a lógica de primeira ordem. Alguns são organizados de acordo com os conectivos que governam, por exemplo, os esquemas

$$\varphi \to (\psi \to \varphi) \qquad \psi \to (\psi \vee \chi) \qquad (\psi \wedge \chi) \to \psi$$

são axiomas comuns que governam $\to$, $\vee$ e $\wedge$. Alguns sistemas de axiomas visam um número mínimo de axiomas. Dependendo dos conectivos tomados como primitivos, é até possível encontrar sistemas de axiomas que consistem em um único axioma.

Uma regra de inferência é uma afirmação condicional que dá uma condição suficiente para que uma sentença em uma derivação seja justificada. O modus ponens é uma regra muito comum desse tipo: diz que se $\varphi$ e $\varphi \to \psi$ já estão justificados, então $\psi$ está justificado. Isso significa que uma linha em uma derivação que contém a sentença $\psi$ está justificada, desde que tanto $\varphi$ quanto $\varphi \to \psi$ (para alguma sentença $\varphi$) apareçam na derivação antes de $\psi$.

A relação $\vdash$ baseada em derivações axiomáticas é definida da seguinte forma: $\Gamma \vdash \varphi$ se, e somente se, há uma derivação com a sentença $\varphi$ como sua última fórmula (e $\Gamma$ é tomado como o conjunto de sentenças nessa derivação que são justificadas por (2) acima). $\varphi$ é um teorema se $\varphi$ tem uma derivação em que $\Gamma$ é vazio, isto é, toda sentença na derivação é justificada por (1) ou (3). Por exemplo, aqui está uma derivação que mostra que $\vdash \varphi \to (\psi \to (\psi \vee \varphi))$:

1. $\psi \to (\psi \vee \varphi)$
2. $(\psi \to (\psi \vee \varphi)) \to (\varphi \to (\psi \to (\psi \vee \varphi)))$
3. $\varphi \to (\psi \to (\psi \vee \varphi))$

A sentença na linha 1 tem a forma do axioma $\varphi \to (\varphi \vee \psi)$ (com os papéis de $\varphi$ e $\psi$ invertidos). A sentença na linha 2 tem a forma do axioma $\varphi \to (\psi \to \varphi)$. Assim, ambas as linhas estão justificadas. A linha 3 é justificada por modus ponens: se a abreviarmos como $\theta$, então a linha 2 tem a forma $\chi \to \theta$, onde $\chi$ é $\psi \to (\psi \vee \varphi)$, isto é, a linha 1.

Um conjunto $\Gamma$ é inconsistente se $\Gamma \vdash \bot$. Um sistema de axiomas completo também provará que $\bot \to \varphi$ para qualquer $\varphi$, e assim, se $\Gamma$ é inconsistente, então $\Gamma \vdash \varphi$ para qualquer $\varphi$.

Sistemas de derivações axiomáticas para lógica foram dados pela primeira vez por Gottlob Frege em sua *Begriffsschrift* de 1879, que por essa razão é frequentemente considerada a primeira obra da lógica moderna. Foram aperfeiçoados em *Principia Mathematica* de Alfred North Whitehead e Bertrand Russell e por David Hilbert e seus alunos na década de 1920. São assim frequentemente chamados de "sistemas de Frege" ou "sistemas de Hilbert". São muito versáteis no sentido de que é frequentemente fácil encontrar um sistema axiomático para uma lógica. Porque as derivações têm uma estrutura muito simples e apenas uma ou duas regras de inferência, também é relativamente fácil provar coisas *sobre* eles. No entanto, são muito difíceis de usar na prática, isto é, é difícil encontrar e escrever provas.

# Capítulo 19

# O Cálculo de Sequentes

Este capítulo apresenta o cálculo de sequentes padrão LK de Gentzen para a lógica clássica de primeira ordem. Ele poderia ter mais exemplos e exercícios. Para incluir ou excluir material relevante ao cálculo de sequentes como sistema de prova, use a tag "prfLK".

## 19.1 Regras e Derivações

Para o que segue, sejam $\Gamma, \Delta, \Pi, \Lambda$ representando sequências finitas de sentenças.

**Definição 19.1 (Sequente).** Um *sequente* é uma expressão da forma

$$\Gamma \Rightarrow \Delta$$

em que $\Gamma$ e $\Delta$ são sequências finitas (possivelmente vazias) de sentenças da linguagem $\mathcal{L}$. $\Gamma$ é chamado de *antecedente*, enquanto $\Delta$ é o *sucedente*.

A ideia intuitiva por trás de um sequente é: se todas as sentenças no antecedente valem, então ao menos uma das sentenças no sucedente vale. Isto é, se $\Gamma = \langle \varphi_1, \ldots, \varphi_m \rangle$ e $\Delta = \langle \psi_1, \ldots, \psi_n \rangle$, então $\Gamma \Rightarrow \Delta$ vale se, e somente se,

$$(\varphi_1 \wedge \cdots \wedge \varphi_m) \rightarrow (\psi_1 \vee \cdots \vee \psi_n)$$

vale. Há dois casos especiais: quando $\Gamma$ é vazio e quando $\Delta$ é vazio. Quando $\Gamma$ é vazio, isto é, $m = 0$, $\Rightarrow \Delta$ vale se, e somente se, $\psi_1 \vee \cdots \vee \psi_n$ vale. Quando $\Delta$ é vazio, isto é, $n = 0$, $\Gamma \Rightarrow$ vale se, e somente se, $\neg(\varphi_1 \wedge \cdots \wedge \varphi_m)$ vale. Dizemos que um sequente é válido se, e somente se, a sentença correspondente é válida.

Se $\Gamma$ é uma sequência de sentenças, escrevemos $\Gamma, \varphi$ para o resultado de acrescentar $\varphi$ à extremidade direita de $\Gamma$ (e $\varphi, \Gamma$ para o resultado de acrescentar $\varphi$ à extremidade esquerda de $\Gamma$). Se $\Delta$ também é uma sequência de sentenças, então $\Gamma, \Delta$ é a concatenação das duas sequências.

**Definição 19.2 (Sequente Inicial).** Um *sequente inicial* é um sequente de uma das seguintes formas:

1. $\varphi \Rightarrow \varphi$
2. $\bot \Rightarrow$

para qualquer sentença $\varphi$ na linguagem.

Derivações no cálculo de sequentes são certas árvores de sequentes, em que os sequentes no topo são sequentes iniciais e, se um sequente está abaixo de um ou dois outros sequentes, ele deve seguir corretamente por uma regra de inferência. As regras para **LK** dividem-se em dois tipos principais: regras *lógicas* e regras *estruturais*. As regras lógicas recebem o nome do operador principal da sentença que contém $\varphi$ e/ou $\psi$ no sequente inferior. Cada uma vem em duas versões, uma para inferir um sequente com a sentença que contém o operador lógico à esquerda, e uma com a sentença à direita.

## 19.2 Regras Proposicionais

**Regras para $\neg$**

$$\frac{\Gamma \Rightarrow \Delta, \varphi}{\neg\varphi, \Gamma \Rightarrow \Delta}\,\neg\mathrm{L} \qquad \frac{\varphi, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\varphi}\,\neg\mathrm{R}$$

**Regras para $\wedge$**

$$\frac{\varphi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}\,\wedge\mathrm{L} \qquad \frac{\psi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}\,\wedge\mathrm{L} \qquad \frac{\Gamma \Rightarrow \Delta, \varphi \qquad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}\,\wedge\mathrm{R}$$

**Regras para $\vee$**

$$\frac{\varphi, \Gamma \Rightarrow \Delta \qquad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta}\,\vee\mathrm{L} \qquad \frac{\Gamma \Rightarrow \Delta, \varphi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}\,\vee\mathrm{R} \qquad \frac{\Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}\,\vee\mathrm{R}$$

**Regras para $\rightarrow$**

$$\frac{\Gamma \Rightarrow \Delta, \varphi \qquad \psi, \Pi \Rightarrow \Lambda}{\varphi \rightarrow \psi, \Gamma, \Pi \Rightarrow \Delta, \Lambda} \rightarrow\text{L} \qquad\qquad \frac{\varphi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi} \rightarrow\text{R}$$

## 19.3 Regras de Quantificadores

**Regras para $\forall$**

$$\frac{\varphi(t), \Gamma \Rightarrow \Delta}{\forall x\, \varphi(x), \Gamma \Rightarrow \Delta} \forall\text{L} \qquad\qquad \frac{\Gamma \Rightarrow \Delta, \varphi(a)}{\Gamma \Rightarrow \Delta, \forall x\, \varphi(x)} \forall\text{R}$$

Em $\forall$L, $t$ é um termo fechado (isto é, um termo sem variáveis). Em $\forall$R, $a$ é a símbolo de constante que não pode ocorrer em lugar algum do sequente inferior da regra $\forall$R. Chamamos $a$ de *variável própria* da inferência $\forall$R.[1]

**Regras para $\exists$**

$$\frac{\varphi(a), \Gamma \Rightarrow \Delta}{\exists x\, \varphi(x), \Gamma \Rightarrow \Delta} \exists\text{L} \qquad\qquad \frac{\Gamma \Rightarrow \Delta, \varphi(t)}{\Gamma \Rightarrow \Delta, \exists x\, \varphi(x)} \exists\text{R}$$

Novamente, $t$ é um termo fechado, e $a$ é a símbolo de constante que não ocorre no sequente inferior da regra $\exists$L. Chamamos $a$ de *variável própria* da inferência $\exists$L.

A condição de que uma variável própria não ocorra no sequente inferior da inferência $\forall$R ou $\exists$L é chamada de *condição de variável própria*.

Lembre-se da convenção de que, quando $\varphi$ é a fórmula com a variável $x$ livre, indicamos isso escrevendo $\varphi(x)$. No mesmo contexto, $\varphi(t)$ é então uma abreviação de $\varphi[t/x]$. Assim, poderíamos também escrever a regra $\exists$R como:

$$\frac{\Gamma \Rightarrow \Delta, \varphi[t/x]}{\Gamma \Rightarrow \Delta, \exists x\, \varphi} \exists\text{R}$$

Note que $t$ pode já ocorrer em $\varphi$, por exemplo, $\varphi$ poderia ser $P(t, x)$. Assim, inferir $\Gamma \Rightarrow \Delta, \exists x\, P(t, x)$ de $\Gamma \Rightarrow \Delta, P(t, t)$ é uma aplicação correta de $\exists$R—pode-se "substituir" uma ou mais, e não necessariamente todas, as ocorrências de $t$

[1] Usamos o termo "variável própria" embora $a$ na regra acima seja a símbolo de constante. Isso tem razões históricas.

na premissa pela variável $x$ ligada. Contudo, as condições de variável própria em $\forall$R e $\exists$L exigem que a símbolo de constante $a$ não ocorra em $\varphi$. Portanto, não se pode inferir corretamente $\Gamma \Rightarrow \Delta, \forall x\, P(a,x)$ de $\Gamma \Rightarrow \Delta, P(a,a)$ usando $\forall$R.

Em $\exists$R e $\forall$L não há restrições sobre o termo $t$. Por outro lado, nas regras $\exists$L e $\forall$R, a condição de variável própria exige que a símbolo de constante $a$ não ocorra em lugar algum fora de $\varphi(a)$ no sequente superior. Isso é necessário para garantir que o sistema seja correto, isto é, que só deriva sequentes que sejam válidos. Sem essa condição, o seguinte seria permitido:

$$\dfrac{\dfrac{\varphi(a) \Rightarrow \varphi(a)}{\exists x\, \varphi(x) \Rightarrow \varphi(a)}\,{}^*\exists\text{L}}{\exists x\, \varphi(x) \Rightarrow \forall x\, \varphi(x)}\,\forall\text{R} \qquad \dfrac{\dfrac{\varphi(a) \Rightarrow \varphi(a)}{\varphi(a) \Rightarrow \forall x\, \varphi(x)}\,{}^*\forall\text{R}}{\exists x\, \varphi(x) \Rightarrow \forall x\, \varphi(x)}\,\exists\text{L}$$

Contudo, $\exists x\, \varphi(x) \Rightarrow \forall x\, \varphi(x)$ não é válido.

## 19.4 Regras Estruturais

Precisamos também de algumas regras que nos permitam reorganizar sentenças nos lados esquerdo e direito de um sequente. Como as regras lógicas exigem que as sentenças na premissa sobre as quais a regra atua estejam ou na extremidade esquerda ou na extremidade direita, precisamos de uma regra de "troca" que nos permita mover sentenças para a posição correta. Às vezes também é importante poder combinar duas sentenças idênticas em uma só, e acrescentar a sentença em qualquer um dos lados.

### Enfraquecimento

$$\dfrac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\,\text{WL} \qquad\qquad \dfrac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi}\,\text{WR}$$

### Contração

$$\dfrac{\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\,\text{CL} \qquad\qquad \dfrac{\Gamma \Rightarrow \Delta, \varphi, \varphi}{\Gamma \Rightarrow \Delta, \varphi}\,\text{CR}$$

### Troca

$$\frac{\Gamma, \varphi, \psi, \Pi \Rightarrow \Delta}{\Gamma, \psi, \varphi, \Pi \Rightarrow \Delta}\,\text{XL} \qquad \frac{\Gamma \Rightarrow \Delta, \varphi, \psi, \Lambda}{\Gamma \Rightarrow \Delta, \psi, \varphi, \Lambda}\,\text{XR}$$

Uma série de inferências de enfraquecimento, contração e troca será frequentemente indicada por linhas de inferência duplas.

A regra a seguir, chamada de "corte", não é estritamente necessária, mas torna muito mais fácil reutilizar e combinar derivações.

$$\frac{\Gamma \Rightarrow \Delta, \varphi \qquad \varphi, \Pi \Rightarrow \Lambda}{\Gamma, \Pi \Rightarrow \Delta, \Lambda}\,\text{Cut}$$

## 19.5 Derivações

Já dissemos como é um sequente inicial e demos as regras de inferência. Derivações no cálculo de sequentes são geradas indutivamente a partir disso: cada derivação ou é um sequente inicial por si só, ou consiste em uma ou duas derivações seguidas de uma inferência.

**Definição 19.3 (LK-derivação).** Uma **LK**-*derivação* de um sequente $S$ é uma árvore finita de sequentes que satisfaz as seguintes condições:

1. Os sequentes no topo da árvore são sequentes iniciais.
2. O sequente na base da árvore é $S$.
3. Todo sequente na árvore exceto $S$ é uma premissa de uma aplicação correta de uma regra de inferência cuja conclusão está diretamente abaixo daquele sequente na árvore.

Dizemos então que $S$ é o *sequente final* da derivação e que $S$ é *derivável em* **LK** (ou **LK**-derivável).

**Exemplo 19.4.** Todo sequente inicial, por exemplo, $\chi \Rightarrow \chi$, é a derivação. Podemos obter uma nova derivação a partir disso aplicando, digamos, a regra WL,

$$\frac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\,\text{WL}$$

A regra, contudo, deve ser geral: podemos substituir o $\varphi$ na regra por qualquer sentença, por exemplo, também por $\theta$. Se a premissa corresponde ao nosso sequente inicial $\chi \Rightarrow \chi$, isso significa que tanto $\Gamma$ quanto $\Delta$ são apenas $\chi$, e a conclusão seria então $\theta, \chi \Rightarrow \chi$. Assim, o seguinte é a derivação:

$$\frac{\chi \Rightarrow \chi}{\theta, \chi \Rightarrow \chi}\,\mathrm{WL}$$

Podemos agora aplicar outra regra, digamos XL, que nos permite trocar duas sentenças à esquerda. Assim, o seguinte também é uma derivação correta:

$$\dfrac{\dfrac{\chi \Rightarrow \chi}{\theta, \chi \Rightarrow \chi}\,\mathrm{WL}}{\chi, \theta \Rightarrow \chi}\,\mathrm{XL}$$

Nesta aplicação da regra, que foi dada como

$$\frac{\Gamma, \varphi, \psi, \Pi \Rightarrow \Delta}{\Gamma, \psi, \varphi, \Pi \Rightarrow \Delta,}\,\mathrm{XL}$$

tanto $\Gamma$ quanto $\Pi$ eram vazios, $\Delta$ é $\chi$, e os papéis de $\varphi$ e $\psi$ são desempenhados por $\theta$ e $\chi$, respectivamente. De modo muito semelhante, vemos também que

$$\frac{\theta \Rightarrow \theta}{\chi, \theta \Rightarrow \theta}\,\mathrm{WL}$$

é a derivação. Agora podemos pegar essas duas derivações e combiná-las usando $\wedge$R. Aquela regra era

$$\frac{\Gamma \Rightarrow \Delta, \varphi \qquad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}\,\wedge\mathrm{R}$$

No nosso caso, as premissas devem corresponder aos últimos sequentes das derivações que terminam nas premissas. Isso significa que $\Gamma$ é $\chi, \theta$, $\Delta$ é vazio, $\varphi$ é $\chi$ e $\psi$ é $\theta$. Assim, a conclusão, se a inferência for correta, é $\chi, \theta \Rightarrow \chi \wedge \theta$.

$$\dfrac{\dfrac{\dfrac{\chi \Rightarrow \chi}{\theta, \chi \Rightarrow \chi}\,\mathrm{WL}}{\chi, \theta \Rightarrow \chi}\,\mathrm{XL} \qquad \dfrac{\theta \Rightarrow \theta}{\chi, \theta \Rightarrow \theta}\,\mathrm{WL}}{\chi, \theta \Rightarrow \chi \wedge \theta}\,\wedge\mathrm{R}$$

É claro que também podemos inverter as premissas; então $\varphi$ seria $\theta$ e $\psi$ seria $\chi$.

$$\dfrac{\dfrac{\theta \Rightarrow \theta}{\chi, \theta \Rightarrow \theta}\,\mathrm{WL} \qquad \dfrac{\dfrac{\chi \Rightarrow \chi}{\theta, \chi \Rightarrow \chi}\,\mathrm{WL}}{\chi, \theta \Rightarrow \chi}\,\mathrm{XL}}{\chi, \theta \Rightarrow \theta \wedge \chi}\,\wedge\mathrm{R}$$

## 19.6 Exemplos de Derivações

**Exemplo 19.5.** Dê uma **LK**-derivação para o sequente $\varphi \wedge \psi \Rightarrow \varphi$.

Começamos escrevendo o sequente final desejado na base da derivação.

$$\frac{}{\varphi \wedge \psi \;\Rightarrow\; \varphi}$$

Em seguida, precisamos descobrir que tipo de inferência poderia ter um sequente inferior dessa forma. Poderia ser uma regra estrutural, mas é uma boa ideia começar procurando uma regra lógica. O único conectivo lógico que ocorre no sequente inferior é $\wedge$, então procuramos uma regra de $\wedge$ e, como o símbolo $\wedge$ ocorre no antecedente, estamos diante da regra $\wedge$L.

$$\frac{}{\varphi \wedge \psi \;\Rightarrow\; \varphi}\,\wedge\mathrm{L}$$

Há duas opções para o que poderia ter sido o sequente superior da inferência $\wedge$L: poderíamos ter um sequente superior $\varphi \Rightarrow \varphi$ ou $\psi \Rightarrow \varphi$. Claramente, $\varphi \Rightarrow \varphi$ é um sequente inicial (o que é bom), enquanto $\psi \Rightarrow \varphi$ não é derivável em geral. Preenchemos o sequente superior:

$$\frac{\varphi \;\Rightarrow\; \varphi}{\varphi \wedge \psi \;\Rightarrow\; \varphi}\,\wedge\mathrm{L}$$

Agora temos uma **LK**-derivação correta do sequente $\varphi \wedge \psi \Rightarrow \varphi$.

**Exemplo 19.6.** Dê uma **LK**-derivação para o sequente $\neg\varphi \vee \psi \Rightarrow \varphi \to \psi$.

Comece escrevendo o sequente final desejado na base da derivação.

$$\frac{}{\neg\varphi \vee \psi \;\Rightarrow\; \varphi \to \psi}$$

Para encontrar uma regra lógica que pudesse nos dar esse sequente final, olhamos para os conectivos lógicos no sequente final: $\neg$, $\vee$ e $\to$. No momento, só nos importam $\vee$ e $\to$, porque são operadores principais de sentenças no sequente final, enquanto $\neg$ está dentro do escopo de outro conectivo, de modo que cuidaremos dele depois. Nossas opções de regras lógicas para a inferência final são, portanto, a regra $\vee$L e a regra $\to$R. Poderíamos escolher qualquer uma das regras, na verdade, mas vamos escolher a regra $\to$R (quando não fosse por outro motivo, porque ela nos permite adiar a divisão em dois ramos). De acordo com a forma das inferências $\to$R que podem produzir o sequente inferior, isto deve ser assim:

$$\frac{\dfrac{}{\varphi, \neg\varphi \vee \psi \;\Rightarrow\; \psi}}{\neg\varphi \vee \psi \;\Rightarrow\; \varphi \to \psi}\,\to\mathrm{R}$$

Se movermos $\neg\varphi \vee \psi$ para a parte externa do antecedente, podemos aplicar a regra $\vee$L. De acordo com o esquema, isto deve se dividir em dois sequentes superiores como segue:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\varphi, \varphi \Rightarrow \psi} \quad \dfrac{}{\psi, \varphi \Rightarrow \psi}}{\neg\varphi \vee \psi, \varphi \Rightarrow \psi}\vee\mathrm{L}}{\varphi, \neg\varphi \vee \psi \Rightarrow \psi}\mathrm{XR}}{\neg\varphi \vee \psi \Rightarrow \varphi \to \psi}\to\mathrm{R}$$

Lembre-se de que estamos tentando subir até sequentes iniciais; parece que estamos bem perto! O ramo direito está a apenas um enfraquecimento e uma troca de um sequente inicial, e então estará pronto:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\varphi, \varphi \Rightarrow \psi} \quad \dfrac{\dfrac{\dfrac{}{\psi \Rightarrow \psi}\mathrm{WL}}{\varphi, \psi \Rightarrow \psi}\mathrm{XL}}{\psi, \varphi \Rightarrow \psi}}{\neg\varphi \vee \psi, \varphi \Rightarrow \psi}\vee\mathrm{L}}{\varphi, \neg\varphi \vee \psi \Rightarrow \psi}\mathrm{XR}}{\neg\varphi \vee \psi \Rightarrow \varphi \to \psi}\to\mathrm{R}$$

Agora, olhando para o ramo esquerdo, o único conectivo lógico em qualquer sentença é o símbolo $\neg$ nas sentenças do antecedente, então estamos diante de uma instância da regra $\neg$L.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \Rightarrow \psi, \varphi}}{\neg\varphi, \varphi \Rightarrow \psi}\neg\mathrm{L} \quad \dfrac{\dfrac{\dfrac{}{\psi \Rightarrow \psi}\mathrm{WL}}{\varphi, \psi \Rightarrow \psi}\mathrm{XL}}{\psi, \varphi \Rightarrow \psi}}{\neg\varphi \vee \psi, \varphi \Rightarrow \psi}\vee\mathrm{L}}{\varphi, \neg\varphi \vee \psi \Rightarrow \psi}\mathrm{XR}}{\neg\varphi \vee \psi \Rightarrow \varphi \to \psi}\to\mathrm{R}$$

De modo semelhante a como finalizamos o ramo direito, estamos a apenas um enfraquecimento e uma troca de finalizar também este ramo esquerdo.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \Rightarrow \varphi}\mathrm{WR}}{\varphi \Rightarrow \varphi, \psi}\mathrm{XR}}{\varphi \Rightarrow \psi, \varphi}\neg\mathrm{L} \quad \dfrac{\dfrac{\dfrac{}{\psi \Rightarrow \psi}\mathrm{WL}}{\varphi, \psi \Rightarrow \psi}\mathrm{XL}}{\psi, \varphi \Rightarrow \psi}}{\neg\varphi, \varphi \Rightarrow \psi}\vee\mathrm{L}}{\neg\varphi \vee \psi, \varphi \Rightarrow \psi}\mathrm{XR}}{\varphi, \neg\varphi \vee \psi \Rightarrow \psi}\mathrm{XR}}{\neg\varphi \vee \psi \Rightarrow \varphi \to \psi}\to\mathrm{R}$$

**Exemplo 19.7.** Dê uma **LK**-derivação do sequente $\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)$

Usando as técnicas acima, começamos escrevendo o sequente final desejado na base.

$$\dfrac{}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}$$

Os conectivos principais disponíveis das sentenças no sequente final são o símbolo $\vee$ e o símbolo $\neg$. Funcionaria aplicar aqui ou a regra $\vee$L ou a regra $\neg$R, mas começamos com a regra $\neg$R porque ela evita, por ora, a divisão em dois ramos:

$$\dfrac{\dfrac{}{\varphi \wedge \psi, \neg\varphi \vee \neg\psi \Rightarrow}}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}\,\neg\text{R}$$

Agora temos a escolha de olhar para a regra $\wedge$L ou a regra $\vee$L. Vejamos o que acontece quando aplicamos a regra $\wedge$L: temos a escolha de começar com o sequente $\varphi, \neg\varphi \vee \psi \Rightarrow$ ou com o sequente $\psi, \neg\varphi \vee \psi \Rightarrow$ . Como a derivação é simétrica em relação a $\varphi$ e $\psi$, vamos com o primeiro:

$$\dfrac{\dfrac{\dfrac{}{\varphi, \neg\varphi \vee \neg\psi \Rightarrow}}{\varphi \wedge \psi, \neg\varphi \vee \neg\psi \Rightarrow}\,\wedge\text{L}}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}\,\neg\text{R}$$

Continuando a preencher a derivação, vemos que esbarramos em um problema:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \Rightarrow \varphi}}{\neg\varphi, \varphi \Rightarrow}\,\neg\text{L} \quad \dfrac{\dfrac{}{\varphi \Rightarrow \psi}\,?}{\neg\psi, \varphi \Rightarrow}\,\neg\text{L}}{\neg\varphi \vee \neg\psi, \varphi \Rightarrow}\,\vee\text{L}}{\varphi, \neg\varphi \vee \neg\psi \Rightarrow}\,\text{XL}}{\varphi \wedge \psi, \neg\varphi \vee \neg\psi \Rightarrow}\,\wedge\text{L}}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}\,\neg\text{R}$$

O topo do ramo direito não pode ser reduzido mais, e ele não pode ser levado, por meio de inferências estruturais, a um sequente inicial, então este não é o caminho certo a tomar. Assim, claramente, foi um erro aplicar a regra $\wedge$L acima. Voltando ao que tínhamos antes e executando a regra $\vee$L em vez disso, obtemos

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\varphi, \varphi \wedge \psi \Rightarrow} \quad \dfrac{}{\neg\psi, \varphi \wedge \psi \Rightarrow}}{\neg\varphi \vee \neg\psi, \varphi \wedge \psi \Rightarrow}\,\vee\text{L}}{\varphi \wedge \psi, \neg\varphi \vee \neg\psi \Rightarrow}\,\text{XL}}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}\,\neg\text{R}$$

Completando cada ramo como fizemos antes, obtemos

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \Rightarrow \varphi}}{\varphi \wedge \psi \Rightarrow \varphi}\,\wedge\text{L}}{\neg\varphi, \varphi \wedge \psi \Rightarrow}\,\neg\text{L} \quad \dfrac{\dfrac{\dfrac{}{\psi \Rightarrow \psi}}{\varphi \wedge \psi \Rightarrow \psi}\,\wedge\text{L}}{\neg\psi, \varphi \wedge \psi \Rightarrow}\,\neg\text{L}}{\neg\varphi \vee \neg\psi, \varphi \wedge \psi \Rightarrow}\,\vee\text{L}}{\varphi \wedge \psi, \neg\varphi \vee \neg\psi \Rightarrow}\,\text{XL}}{\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)}\,\neg\text{R}$$

(Poderíamos ter executado as regras de $\wedge$ mais abaixo do que as regras de $\neg$ nesses passos e ainda assim obtido uma derivação correta).

**Exemplo 19.8.** Até agora não usamos a regra de contração, mas às vezes ela é necessária. Eis um exemplo em que isso acontece. Suponha que queiramos provar $\Rightarrow \varphi \vee \neg\varphi$. Aplicar $\vee$R de trás para frente nos daria uma destas duas derivações:

$$\dfrac{\dfrac{}{\Rightarrow \varphi}}{\Rightarrow \varphi \vee \neg\varphi}\vee\mathrm{R} \qquad \dfrac{\dfrac{\dfrac{}{\varphi \Rightarrow}}{\Rightarrow \neg\varphi}\neg\mathrm{R}}{\Rightarrow \varphi \vee \neg\varphi}\vee\mathrm{R}$$

Nenhuma destas, é claro, termina em um sequente inicial. O truque é perceber que a regra de contração nos permite combinar duas cópias de a sentença em uma só—e quando estamos buscando uma prova, isto é, indo de baixo para cima, podemos manter uma cópia de $\varphi \vee \neg\varphi$ na premissa, por exemplo,

$$\dfrac{\dfrac{\dfrac{}{\Rightarrow \varphi \vee \neg\varphi, \varphi}}{\Rightarrow \varphi \vee \neg\varphi, \varphi \vee \neg\varphi}\vee\mathrm{R}}{\Rightarrow \varphi \vee \neg\varphi}\mathrm{CR}$$

Agora podemos aplicar $\vee$R uma segunda vez, e também obter $\neg\varphi$, o que leva a uma derivação completa.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \Rightarrow \varphi}}{\Rightarrow \varphi, \neg\varphi}\neg\mathrm{R}}{\Rightarrow \varphi, \varphi \vee \neg\varphi}\vee\mathrm{R}}{\Rightarrow \varphi \vee \neg\varphi, \varphi}\mathrm{XR}}{\Rightarrow \varphi \vee \neg\varphi, \varphi \vee \neg\varphi}\vee\mathrm{R}}{\Rightarrow \varphi \vee \neg\varphi}\mathrm{CR}$$

## 19.7 Derivações com Quantificadores

**Exemplo 19.9.** Dê uma **LK**-derivação do sequente $\exists x\, \neg\varphi(x) \Rightarrow \neg\forall x\, \varphi(x)$.

Ao lidar com quantificadores, temos de cuidar para não violar a condição de variável própria, e às vezes isso exige que brinquemos com a ordem de execução de certas inferências. Em geral, ajuda tentar cuidar primeiro das regras sujeitas à condição de variável própria (elas ficarão mais abaixo na prova finalizada). Além disso, é uma boa ideia tentar olhar adiante e adivinhar como o sequente inicial poderia ser. No nosso caso, ele terá de ser algo como $\varphi(a) \Rightarrow \varphi(a)$. Isso significa que, ao "reverter" as regras de quantificador, teremos de escolher o mesmo termo—que chamaremos de $a$—tanto para a regra $\forall$ quanto para a regra $\exists$. Se escolhêssemos termos diferentes para cada regra, acabaríamos com algo como $\varphi(a) \Rightarrow \varphi(b)$, que, é claro, não é derivável.

Começando como de costume, escrevemos

$$\frac{}{\exists x\, \neg\varphi(x) \;\Rightarrow\; \neg\forall x\, \varphi(x)}$$

Poderíamos executar a regra $\exists$L ou a regra $\neg$R. Como a regra $\exists$L está sujeita à condição de variável própria, é uma boa ideia cuidar dela mais cedo do que mais tarde, então faremos essa primeiro.

$$\frac{\dfrac{}{\neg\varphi(a) \;\Rightarrow\; \neg\forall x\, \varphi(x)}}{\exists x\, \neg\varphi(x) \;\Rightarrow\; \neg\forall x\, \varphi(x)}\,\exists\text{L}$$

Aplicando as regras $\neg$L e $\neg$R de trás para frente, obtemos

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x\, \varphi(x) \;\Rightarrow\; \varphi(a)}}{\neg\varphi(a), \forall x\, \varphi(x) \;\Rightarrow}\,\neg\text{L}}{\forall x\, \varphi(x), \neg\varphi(a) \;\Rightarrow}\,\text{XL}}{\neg\varphi(a) \;\Rightarrow\; \neg\forall x\varphi(x)}\,\neg\text{R}}{\exists x\neg\varphi(x) \;\Rightarrow\; \neg\forall x\varphi(x)}\,\exists\text{L}$$

Neste ponto, nossa única opção é executar a regra $\forall$L. Como essa regra não está sujeita à restrição de variável própria, estamos livres. Lembre-se, queremos tentar obter um sequente inicial (da forma $\varphi(a) \Rightarrow \varphi(a)$), então devemos escolher $a$ como nosso argumento para $\varphi$ ao aplicarmos a regra.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi(a) \;\Rightarrow\; \varphi(a)}}{\forall x\, \varphi(x) \;\Rightarrow\; \varphi(a)}\,\forall\text{L}}{\neg\varphi(a), \forall x\, \varphi(x) \;\Rightarrow}\,\neg\text{L}}{\forall x\, \varphi(x), \neg\varphi(a) \;\Rightarrow}\,\text{XL}}{\neg\varphi(a) \;\Rightarrow\; \neg\forall x\, \varphi(x)}\,\neg\text{R}}{\exists x\, \neg\varphi(x) \;\Rightarrow\; \neg\forall x\, \varphi(x)}\,\exists\text{L}$$

É importante, especialmente ao lidar com quantificadores, verificar com cuidado neste ponto que a condição de variável própria não foi violada. Como a única regra que aplicamos sujeita à condição de variável própria foi $\exists$L, e a variável própria $a$ não ocorre em seu sequente inferior (o sequente final), esta é uma derivação correta.

Esta seção reúne as definições da relação de demonstrabilidade e de consistência para a dedução natural.

## 19.8 Noções da Teoria da Prova

Assim como definimos uma série de noções semânticas importantes (validade, consequência, satisfatibilidade), definimos agora as *noções da teoria da*

*prova* correspondentes. Elas não são definidas por apelo à satisfação de sentenças em estruturas, mas por apelo à derivabilidade ou à não derivabilidade de certos sequentes. Foi uma descoberta importante que essas noções coincidem. Que elas coincidem é o conteúdo dos teoremas da *correção* e da *completude*.

**Definição 19.10 (Teoremas).** A sentença $\varphi$ é um *teorema* se há a derivação em **LK** do sequente $\Rightarrow \varphi$. Escrevemos $\vdash \varphi$ se $\varphi$ é um teorema e $\nvdash \varphi$ se não é.

**Definição 19.11 (Derivabilidade).** A sentença $\varphi$ é *derivável de* um conjunto de sentenças $\Gamma$, $\Gamma \vdash \varphi$, se, e somente se, há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ e uma sequência $\Gamma_0'$ das sentenças em $\Gamma_0$ tal que **LK** deriva $\Gamma_0' \Rightarrow \varphi$. Se $\varphi$ não é derivável de $\Gamma$, escrevemos $\Gamma \nvdash \varphi$.

Por causa das regras de contração, enfraquecimento e troca, a ordem e o número de sentenças em $\Gamma_0'$ não importam: se um sequente $\Gamma_0' \Rightarrow \varphi$ é derivável, então também o é $\Gamma_0'' \Rightarrow \varphi$ para qualquer $\Gamma_0''$ que contenha as mesmas sentenças que $\Gamma_0'$. Por exemplo, se $\Gamma_0 = \{\psi, \chi\}$, então tanto $\Gamma_0' = \langle \psi, \psi, \chi \rangle$ quanto $\Gamma_0'' = \langle \chi, \chi, \psi \rangle$ são sequências que contêm apenas as sentenças em $\Gamma_0$. Se um sequente contendo uma delas é derivável, o outro também é, por exemplo:

$$\dfrac{\dfrac{\dfrac{\vdots}{\psi, \psi, \chi \Rightarrow \varphi}}{\psi, \chi \Rightarrow \varphi}\,\mathrm{CL}}{\chi, \psi \Rightarrow \varphi}\,\mathrm{XL}}{\chi, \chi, \psi \Rightarrow \varphi}\,\mathrm{WL}$$

De agora em diante, diremos que, se $\Gamma_0$ é um conjunto finito de sentenças, então $\Gamma_0 \Rightarrow \varphi$ é qualquer sequente em que o antecedente é uma sequência de sentenças em $\Gamma_0$, e incluiremos tacitamente contrações, trocas e enfraquecimentos se necessário.

**Definição 19.12 (Consistência).** Um conjunto de sentenças $\Gamma$ é *inconsistente* se, e somente se, há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ tal que **LK** deriva $\Gamma_0 \Rightarrow$ . Se $\Gamma$ não é inconsistente, isto é, se para todo $\Gamma_0 \subseteq \Gamma$ finito, **LK** não deriva $\Gamma_0 \Rightarrow$ , dizemos que é *consistente*.

**Proposição 19.13 (Reflexividade).** *Se $\varphi \in \Gamma$, então $\Gamma \vdash \varphi$.*

*Prova.* O sequente inicial $\varphi \Rightarrow \varphi$ é derivável, e $\{\varphi\} \subseteq \Gamma$. □

**Proposição 19.14 (Monotonicidade).** *Se $\Gamma \subseteq \Delta$ e $\Gamma \vdash \varphi$, então $\Delta \vdash \varphi$.*

*Prova.* Suponha $\Gamma \vdash \varphi$, isto é, há um $\Gamma_0 \subseteq \Gamma$ finito tal que $\Gamma_0 \Rightarrow \varphi$ é derivável. Como $\Gamma \subseteq \Delta$, então $\Gamma_0$ também é um subconjunto finito de $\Delta$. A derivação de $\Gamma_0 \Rightarrow \varphi$ mostra, assim, também que $\Delta \vdash \varphi$. □

**Proposição 19.15 (Transitividade).** *Se $\Gamma \vdash \varphi$ e $\{\varphi\} \cup \Delta \vdash \psi$, então $\Gamma \cup \Delta \vdash \psi$.*

*Prova.* Se $\Gamma \vdash \varphi$, há um $\Gamma_0 \subseteq \Gamma$ finito e a derivação $\pi_0$ de $\Gamma_0 \Rightarrow \varphi$. Se $\{\varphi\} \cup \Delta \vdash \psi$, então, para algum subconjunto finito $\Delta_0 \subseteq \Delta$, há a derivação $\pi_1$ de $\varphi, \Delta_0 \Rightarrow \psi$. Considere a seguinte derivação:

$$\dfrac{\begin{array}{cc}\vdots\,\pi_0 & \vdots\,\pi_1\\ \Gamma_0 \Rightarrow \varphi & \varphi, \Delta_0 \Rightarrow \psi\end{array}}{\Gamma_0, \Delta_0 \Rightarrow \psi}\ \text{Cut}$$

Como $\Gamma_0 \cup \Delta_0 \subseteq \Gamma \cup \Delta$, isso mostra $\Gamma \cup \Delta \vdash \psi$. □

Note que isso significa, em particular, que se $\Gamma \vdash \varphi$ e $\varphi \vdash \psi$, então $\Gamma \vdash \psi$. Segue-se também que se $\varphi_1, \ldots, \varphi_n \vdash \psi$ e $\Gamma \vdash \varphi_i$ para cada $i$, então $\Gamma \vdash \psi$.

**Proposição 19.16.** *$\Gamma$ é inconsistente se, e somente se, $\Gamma \vdash \varphi$ para toda sentença $\varphi$.*

*Prova.* Exercício. □

**Proposição 19.17 (Compacidade).**
1. *Se $\Gamma \vdash \varphi$, então há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ tal que $\Gamma_0 \vdash \varphi$.*
2. *Se todo subconjunto finito de $\Gamma$ é consistente, então $\Gamma$ é consistente.*

*Prova.*
1. Se $\Gamma \vdash \varphi$, então há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ tal que o sequente $\Gamma_0 \Rightarrow \varphi$ tem a derivação. Consequentemente, $\Gamma_0 \vdash \varphi$.
2. Se $\Gamma$ é inconsistente, há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ tal que **LK** deriva $\Gamma_0 \Rightarrow$ . Mas então $\Gamma_0$ é um subconjunto finito de $\Gamma$ que é inconsistente. □

## 19.9 Derivabilidade e Consistência

Estabeleceremos agora uma série de propriedades da relação de derivabilidade. Elas são interessantes por si mesmas, mas cada uma terá um papel na prova do teorema da completude.

**Proposição 19.18.** *Se $\Gamma \vdash \varphi$ e $\Gamma \cup \{\varphi\}$ é inconsistente, então $\Gamma$ é inconsistente.*

*Prova.* Há $\Gamma_0$ e $\Gamma_1 \subseteq \Gamma$ finitos tais que **LK** deriva $\Gamma_0 \Rightarrow \varphi$ e $\varphi, \Gamma_1 \Rightarrow$ . Seja $\pi_0$ a **LK**-derivação de $\Gamma_0 \Rightarrow \varphi$ e $\pi_1$ a **LK**-derivação de $\Gamma_1, \varphi \Rightarrow$ . Podemos então derivar

$$\dfrac{\begin{array}{cc}\vdots\,\pi_0 & \vdots\,\pi_1\\ \Gamma_0 \Rightarrow \varphi & \varphi, \Gamma_1 \Rightarrow\end{array}}{\Gamma_0, \Gamma_1 \Rightarrow}\ \text{Cut}$$

Como $\Gamma_0 \subseteq \Gamma$ e $\Gamma_1 \subseteq \Gamma$, $\Gamma_0 \cup \Gamma_1 \subseteq \Gamma$; portanto, $\Gamma$ é inconsistente. □

**Proposição 19.19.** *$\Gamma \vdash \varphi$ se, e somente se, $\Gamma \cup \{\neg\varphi\}$ é inconsistente.*

*Prova.* Primeiro, suponha $\Gamma \vdash \varphi$, isto é, há a derivação $\pi_0$ de $\Gamma \Rightarrow \varphi$. Acrescentando uma regra ¬L, obtemos a derivação de $\neg\varphi, \Gamma \Rightarrow$ , isto é, $\Gamma \cup \{\neg\varphi\}$ é inconsistente.

Se $\Gamma \cup \{\neg\varphi\}$ é inconsistente, há a derivação $\pi_1$ de $\neg\varphi, \Gamma \Rightarrow$ . O seguinte é a derivação de $\Gamma \Rightarrow \varphi$:

$$\dfrac{\dfrac{\varphi \Rightarrow \varphi}{\Rightarrow \varphi, \neg\varphi}\ \neg\text{R} \qquad \begin{array}{c}\\ \vdots\,\pi_1\\ \neg\varphi, \Gamma \Rightarrow\end{array}}{\Gamma \Rightarrow \varphi}\ \text{Cut}$$

□

**Proposição 19.20.** *Se $\Gamma \vdash \varphi$ e $\neg\varphi \in \Gamma$, então $\Gamma$ é inconsistente.*

*Prova.* Suponha $\Gamma \vdash \varphi$ e $\neg\varphi \in \Gamma$. Então há a derivação $\pi$ de um sequente $\Gamma_0 \Rightarrow \varphi$. O sequente $\neg\varphi, \Gamma_0 \Rightarrow$ também é derivável:

$$\dfrac{\begin{array}{cc}\vdots\,\pi & \dfrac{\dfrac{\varphi \Rightarrow \varphi}{\neg\varphi, \varphi \Rightarrow}\ \neg\text{L}}{\varphi, \neg\varphi \Rightarrow}\ \text{XL}\\ \Gamma_0 \Rightarrow \varphi & \end{array}}{\Gamma_0, \neg\varphi \Rightarrow}\ \text{Cut}$$

Como $\neg\varphi \in \Gamma$ e $\Gamma_0 \subseteq \Gamma$, isso mostra que $\Gamma$ é inconsistente. □

**Proposição 19.21.** *Se $\Gamma \cup \{\varphi\}$ e $\Gamma \cup \{\neg\varphi\}$ são ambos inconsistentes, então $\Gamma$ é inconsistente.*

*Prova.* Há conjuntos finitos $\Gamma_0 \subseteq \Gamma$ e $\Gamma_1 \subseteq \Gamma$ e **LK**-derivações $\pi_0$ e $\pi_1$ de $\varphi, \Gamma_0 \Rightarrow$ e $\neg\varphi, \Gamma_1 \Rightarrow$ , respectivamente. Podemos então derivar

$$\dfrac{\dfrac{\begin{array}{c}\vdots\,\pi_0\\ \varphi, \Gamma_0 \Rightarrow\end{array}}{\Gamma_0 \Rightarrow \neg\varphi}\ \neg\text{R} \qquad \begin{array}{c}\\ \vdots\,\pi_1\\ \neg\varphi, \Gamma_1 \Rightarrow\end{array}}{\Gamma_0, \Gamma_1 \Rightarrow}\ \text{Cut}$$

Como $\Gamma_0 \subseteq \Gamma$ e $\Gamma_1 \subseteq \Gamma$, $\Gamma_0 \cup \Gamma_1 \subseteq \Gamma$. Portanto, $\Gamma$ é inconsistente. □

## 19.10 Derivabilidade e os Conectivos Proposicionais

Estabelecemos que a relação de derivabilidade $\vdash$ do cálculo de sequentes é forte o suficiente para estabelecer alguns fatos básicos envolvendo os conectivos proposicionais, tais como $\varphi \wedge \psi \vdash \varphi$ e $\varphi, \varphi \to \psi \vdash \psi$ (modus ponens). Esses fatos são necessários para a prova do teorema da completude.

**Proposição 19.22.** *1. Tanto $\varphi \wedge \psi \vdash \varphi$ quanto $\varphi \wedge \psi \vdash \psi$.*

*2. $\varphi, \psi \vdash \varphi \wedge \psi$.*

*Prova.* 1. Ambos os sequentes $\varphi \wedge \psi \Rightarrow \varphi$ e $\varphi \wedge \psi \Rightarrow \psi$ são deriváveis:

$$\dfrac{\varphi \Rightarrow \varphi}{\varphi \wedge \psi \Rightarrow \varphi}\,\wedge\mathrm{L} \qquad \dfrac{\psi \Rightarrow \psi}{\varphi \wedge \psi \Rightarrow \psi}\,\wedge\mathrm{L}$$

2. Eis a derivação do sequente $\varphi, \psi \Rightarrow \varphi \wedge \psi$:

$$\dfrac{\varphi \Rightarrow \varphi \qquad \psi \Rightarrow \psi}{\varphi, \psi \Rightarrow \varphi \wedge \psi}\,\wedge\mathrm{R}$$

□

**Proposição 19.23.** *1. $\varphi \vee \psi, \neg\varphi, \neg\psi$ é inconsistente.*

*2. Tanto $\varphi \vdash \varphi \vee \psi$ quanto $\psi \vdash \varphi \vee \psi$.*

*Prova.* 1. Damos a derivação do sequente $\varphi \vee \psi, \neg\varphi, \neg\psi \Rightarrow$:

$$\dfrac{\dfrac{\dfrac{\varphi \Rightarrow \varphi}{\neg\varphi, \varphi \Rightarrow}\,\neg\mathrm{L}}{\varphi, \neg\varphi, \neg\psi \Rightarrow} \qquad \dfrac{\dfrac{\psi \Rightarrow \psi}{\neg\psi, \psi \Rightarrow}\,\neg\mathrm{L}}{\psi, \neg\varphi, \neg\psi \Rightarrow}}{\varphi \vee \psi, \neg\varphi, \neg\psi \Rightarrow}\,\vee\mathrm{L}$$

(Lembre-se de que linhas de inferência duplas indicam várias inferências de enfraquecimento, contração e troca.)

2. Ambos os sequentes $\varphi \Rightarrow \varphi \vee \psi$ e $\psi \Rightarrow \varphi \vee \psi$ têm derivações:

$$\dfrac{\varphi \Rightarrow \varphi}{\varphi \Rightarrow \varphi \vee \psi}\,\vee\mathrm{R} \qquad \dfrac{\psi \Rightarrow \psi}{\psi \Rightarrow \varphi \vee \psi}\,\vee\mathrm{R}$$

□

**Proposição 19.24.** *1. $\varphi, \varphi \to \psi \vdash \psi$.*

*2. Tanto $\neg\varphi \vdash \varphi \to \psi$ quanto $\psi \vdash \varphi \to \psi$.*

*Prova.* 1. O sequente $\varphi \to \psi, \varphi \Rightarrow \psi$ é derivável:

$$\dfrac{\varphi \Rightarrow \varphi \qquad \psi \Rightarrow \psi}{\varphi \to \psi, \varphi \Rightarrow \psi} \to\text{L}$$

2. Ambos os sequentes $\neg\varphi \Rightarrow \varphi \to \psi$ e $\psi \Rightarrow \varphi \to \psi$ são deriváveis:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\varphi \Rightarrow \varphi}{\neg\varphi, \varphi \Rightarrow}\neg\text{L}}{\varphi, \neg\varphi \Rightarrow}\text{XL}}{\varphi, \neg\varphi \Rightarrow \psi}\text{WR}}{\neg\varphi \Rightarrow \varphi \to \psi}\to\text{R} \qquad \dfrac{\dfrac{\dfrac{\psi \Rightarrow \psi}{\varphi, \psi \Rightarrow \psi}\text{WL}}{\psi \Rightarrow \varphi \to \psi}\to\text{R}}$$

□

## 19.11 Derivabilidade e os Quantificadores

O teorema da completude também exige que as regras do cálculo de sequentes produzam os fatos sobre $\vdash$ estabelecidos nesta seção.

**Teorema 19.25.** *Se $c$ é uma constante que não ocorre em $\Gamma$ ou $\varphi(x)$ e $\Gamma \vdash \varphi(c)$, então $\Gamma \vdash \forall x\, \varphi(x)$.*

*Prova.* Seja $\pi_0$ uma **LK**-derivação de $\Gamma_0 \Rightarrow \varphi(c)$ para algum $\Gamma_0 \subseteq \Gamma$ finito. Acrescentando uma inferência $\forall$R, obtemos a derivação de $\Gamma_0 \Rightarrow \forall x\, \varphi(x)$, já que $c$ não ocorre em $\Gamma$ ou $\varphi(x)$ e, assim, a condição de variável própria é satisfeita. □

**Proposição 19.26.** *1. $\varphi(t) \vdash \exists x\, \varphi(x)$.*

*2. $\forall x\, \varphi(x) \vdash \varphi(t)$.*

*Prova.* 1. O sequente $\varphi(t) \Rightarrow \exists x\, \varphi(x)$ é derivável:

$$\dfrac{\varphi(t) \Rightarrow \varphi(t)}{\varphi(t) \Rightarrow \exists x\, \varphi(x)} \exists\text{R}$$

2. O sequente $\forall x\, \varphi(x) \Rightarrow \varphi(t)$ é derivável:

$$\dfrac{\varphi(t) \Rightarrow \varphi(t)}{\forall x\, \varphi(x) \Rightarrow \varphi(t)} \forall\text{L}$$

□

## 19.12 Correção

Um sistema de derivação, tal como o cálculo de sequentes, é *correto* se não pode derivar coisas que de fato não valem. A correção é, assim, uma espécie de propriedade de segurança garantida para sistemas de derivação. Dependendo de qual propriedade da teoria da prova está em questão, gostaríamos de saber, por exemplo, que

1. todo $\varphi$ derivável é válido;
2. se a sentença é derivável de algumas outras, ela também é consequência delas;
3. se um conjunto de sentenças é inconsistente, ele é insatisfatível.

Essas são propriedades importantes de um sistema de derivação. Se alguma delas não vale, o sistema de derivação é deficiente—ele deriva demais. Consequentemente, estabelecer a correção de um sistema de derivação é da máxima importância.

Como todas essas propriedades da teoria da prova são definidas via derivabilidade no cálculo de sequentes de certos sequentes, provar (1)–(3) acima requer provar algo sobre as propriedades semânticas dos sequentes deriváveis. Primeiro definiremos o que significa um sequente ser *válido*, e então mostraremos que todo sequente derivável é válido. (1)–(3) seguem-se então como corolários desse resultado.

**Definição 19.27.** A estrutura $\mathfrak{M}$ *satisfaz* um sequente $\Gamma \Rightarrow \Delta$ se, e somente se, ou $\mathfrak{M} \nvDash \varphi$ para algum $\varphi \in \Gamma$ ou $\mathfrak{M} \vDash \varphi$ para algum $\varphi \in \Delta$.

Um sequente é *válido* se, e somente se, toda estrutura $\mathfrak{M}$ o satisfaz.

**Teorema 19.28 (Correção).** *Se* **LK** *deriva* $\Theta \Rightarrow \Xi$, *então* $\Theta \Rightarrow \Xi$ *é válido.*

*Prova.* Seja $\pi$ a derivação de $\Theta \Rightarrow \Xi$. Procedemos por indução sobre o número de inferências $n$ em $\pi$.

Se o número de inferências é 0, então $\pi$ consiste apenas em um sequente inicial. Todo sequente inicial $\varphi \Rightarrow \varphi$ é obviamente válido, pois para toda $\mathfrak{M}$, ou $\mathfrak{M} \nvDash \varphi$ ou $\mathfrak{M} \vDash \varphi$.

Se o número de inferências é maior que 0, distinguimos casos de acordo com o tipo da inferência mais inferior. Pela hipótese de indução, podemos supor que as premissas dessa inferência são válidas, já que o número de inferências na derivação de qualquer premissa é menor que $n$.

Primeiro, consideramos as inferências possíveis com apenas uma premissa.

1. A última inferência é um enfraquecimento. Então $\Theta \Rightarrow \Xi$ é $\varphi, \Gamma \Rightarrow \Delta$ (se a última inferência é WL) ou $\Gamma \Rightarrow \Delta, \varphi$ (se é WR), e a derivação termina em uma de

$$\frac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta\end{array}}{\varphi, \Gamma \Rightarrow \Delta}\,\mathrm{WL} \qquad \frac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta\end{array}}{\Gamma \Rightarrow \Delta, \varphi}\,\mathrm{WR}$$

Pela hipótese de indução, $\Gamma \Rightarrow \Delta$ é válido, isto é, para toda estrutura $\mathfrak{M}$, ou há algum $\chi \in \Gamma$ tal que $\mathfrak{M} \nvDash \chi$ ou há algum $\chi \in \Delta$ tal que $\mathfrak{M} \vDash \chi$.

Se $\mathfrak{M} \nvDash \chi$ para algum $\chi \in \Gamma$, então $\chi \in \Theta$ também, já que $\Theta = \varphi, \Gamma$, e assim $\mathfrak{M} \nvDash \chi$ para algum $\chi \in \Theta$. Analogamente, se $\mathfrak{M} \vDash \chi$ para algum $\chi \in \Delta$, como $\chi \in \Xi$, $\mathfrak{M} \vDash \chi$ para algum $\chi \in \Xi$. Consequentemente, $\Theta \Rightarrow \Xi$ é válido.

2. A última inferência é ¬L: Então a premissa da última inferência é $\Gamma \Rightarrow \Delta, \varphi$ e a conclusão é $\neg\varphi, \Gamma \Rightarrow \Delta$, isto é, a derivação termina em

$$\frac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta, \varphi\end{array}}{\neg\varphi, \Gamma \Rightarrow \Delta}\,\neg\mathrm{L}$$

e $\Theta = \neg\varphi, \Gamma$ enquanto $\Xi = \Delta$.

A hipótese de indução nos diz que $\Gamma \Rightarrow \Delta, \varphi$ é válido, isto é, para toda $\mathfrak{M}$, ou (a) para algum $\chi \in \Gamma$, $\mathfrak{M} \nvDash \chi$, ou (b) para algum $\chi \in \Delta$, $\mathfrak{M} \vDash \chi$, ou (c) $\mathfrak{M} \vDash \varphi$. Queremos mostrar que $\Theta \Rightarrow \Xi$ também é válido. Seja $\mathfrak{M}$ a estrutura. Se (a) vale, então há $\chi \in \Gamma$ tal que $\mathfrak{M} \nvDash \chi$, mas $\chi \in \Theta$ também. Se (b) vale, há $\chi \in \Delta$ tal que $\mathfrak{M} \vDash \chi$, mas $\chi \in \Xi$ também. Por fim, se $\mathfrak{M} \vDash \varphi$, então $\mathfrak{M} \nvDash \neg\varphi$. Como $\neg\varphi \in \Theta$, há $\chi \in \Theta$ tal que $\mathfrak{M} \nvDash \chi$. Consequentemente, $\Theta \Rightarrow \Xi$ é válido.

3. A última inferência é ¬R: Exercício.

4. A última inferência é ∧L: Há duas variantes: $\varphi \wedge \psi$ pode ser inferido à esquerda a partir de $\varphi$ ou de $\psi$ no lado esquerdo da premissa. No primeiro caso, $\pi$ termina em

$$\frac{\begin{array}{c}\vdots\\ \varphi, \Gamma \Rightarrow \Delta\end{array}}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}\,\wedge\mathrm{L}$$

e $\Theta = \varphi \wedge \psi, \Gamma$ enquanto $\Xi = \Delta$. Considere a estrutura $\mathfrak{M}$. Como, pela hipótese de indução, $\varphi, \Gamma \Rightarrow \Delta$ é válido, (a) $\mathfrak{M} \nvDash \varphi$, (b) $\mathfrak{M} \nvDash \chi$ para algum $\chi \in \Gamma$, ou (c) $\mathfrak{M} \vDash \chi$ para algum $\chi \in \Delta$. No caso (a), $\mathfrak{M} \nvDash \varphi \wedge \psi$, então

há $\chi \in \Theta$ (a saber, $\varphi \wedge \psi$) tal que $\mathfrak{M} \nvDash \chi$. No caso (b), há $\chi \in \Gamma$ tal que $\mathfrak{M} \nvDash \chi$, e $\chi \in \Theta$ também. No caso (c), há $\chi \in \Delta$ tal que $\mathfrak{M} \vDash \chi$, e $\chi \in \Xi$ também, já que $\Xi = \Delta$. Assim, em cada caso, $\mathfrak{M}$ satisfaz $\varphi \wedge \psi, \Gamma \Rightarrow \Delta$. Como $\mathfrak{M}$ era arbitrário, $\Gamma \Rightarrow \Delta$ é válido. O caso em que $\varphi \wedge \psi$ é inferido a partir de $\psi$ é tratado da mesma forma, mudando $\varphi$ para $\psi$.

5. A última inferência é $\vee$R: Há duas variantes: $\varphi \vee \psi$ pode ser inferido à direita a partir de $\varphi$ ou de $\psi$ no lado direito da premissa. No primeiro caso, $\pi$ termina em

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta, \varphi\end{array}}{\Gamma \Rightarrow \Delta, \varphi \vee \psi} \vee\text{R}$$

   Agora $\Theta = \Gamma$ e $\Xi = \Delta, \varphi \vee \psi$. Considere a estrutura $\mathfrak{M}$. Como $\Gamma \Rightarrow \Delta, \varphi$ é válido, (a) $\mathfrak{M} \vDash \varphi$, (b) $\mathfrak{M} \nvDash \chi$ para algum $\chi \in \Gamma$, ou (c) $\mathfrak{M} \vDash \chi$ para algum $\chi \in \Delta$. No caso (a), $\mathfrak{M} \vDash \varphi \vee \psi$. No caso (b), há $\chi \in \Gamma$ tal que $\mathfrak{M} \nvDash \chi$. No caso (c), há $\chi \in \Delta$ tal que $\mathfrak{M} \vDash \chi$. Assim, em cada caso, $\mathfrak{M}$ satisfaz $\Gamma \Rightarrow \Delta, \varphi \vee \psi$, isto é, $\Theta \Rightarrow \Xi$. Como $\mathfrak{M}$ era arbitrário, $\Theta \Rightarrow \Xi$ é válido. O caso em que $\varphi \vee \psi$ é inferido a partir de $\psi$ é tratado da mesma forma, mudando $\varphi$ para $\psi$.

6. A última inferência é $\rightarrow$R: Então $\pi$ termina em

$$\dfrac{\begin{array}{c}\vdots\\ \varphi, \Gamma \Rightarrow \Delta, \psi\end{array}}{\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi} \rightarrow\text{R}$$

   Novamente, a hipótese de indução diz que a premissa é válida; queremos mostrar que a conclusão também é válida. Seja $\mathfrak{M}$ arbitrário. Como $\varphi, \Gamma \Rightarrow \Delta, \psi$ é válido, ao menos um dos seguintes casos ocorre: (a) $\mathfrak{M} \nvDash \varphi$, (b) $\mathfrak{M} \vDash \psi$, (c) $\mathfrak{M} \nvDash \chi$ para algum $\chi \in \Gamma$, ou (d) $\mathfrak{M} \vDash \chi$ para algum $\chi \in \Delta$. Nos casos (a) e (b), $\mathfrak{M} \vDash \varphi \rightarrow \psi$ e assim há um $\chi \in \Delta, \varphi \rightarrow \psi$ tal que $\mathfrak{M} \vDash \chi$. No caso (c), para algum $\chi \in \Gamma$, $\mathfrak{M} \nvDash \chi$. No caso (d), para algum $\chi \in \Delta$, $\mathfrak{M} \vDash \chi$. Em cada caso, $\mathfrak{M}$ satisfaz $\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi$. Como $\mathfrak{M}$ era arbitrário, $\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi$ é válido.

7. A última inferência é $\forall$L: Então há a fórmula $\varphi(x)$ e um termo fechado $t$ tais que $\pi$ termina em

$$\dfrac{\begin{array}{c}\vdots\\ \varphi(t), \Gamma \Rightarrow \Delta\end{array}}{\forall x\, \varphi(x), \Gamma \Rightarrow \Delta}\,\forall\mathrm{L}$$

Queremos mostrar que a conclusão $\forall x\, \varphi(x), \Gamma \Rightarrow \Delta$ é válida. Considere a estrutura $\mathfrak{M}$. Como a premissa $\varphi(t), \Gamma \Rightarrow \Delta$ é válida, (a) $\mathfrak{M} \nvDash \varphi(t)$, (b) $\mathfrak{M} \nvDash \chi$ para algum $\chi \in \Gamma$, ou (c) $\mathfrak{M} \vDash \chi$ para algum $\chi \in \Delta$. No caso (a), por Proposição 16.31, se $\mathfrak{M} \vDash \forall x\, \varphi(x)$, então $\mathfrak{M} \vDash \varphi(t)$. Como $\mathfrak{M} \nvDash \varphi(t)$, $\mathfrak{M} \nvDash \forall x\, \varphi(x)$ . Nos casos (b) e (c), $\mathfrak{M}$ também satisfaz $\forall x\, \varphi(x), \Gamma \Rightarrow \Delta$. Como $\mathfrak{M}$ era arbitrário, $\forall x\, \varphi(x), \Gamma \Rightarrow \Delta$ é válido.

8. A última inferência é $\exists$R: Exercício.

9. A última inferência é $\forall$R: Então há a fórmula $\varphi(x)$ e a símbolo de constante $a$ tais que $\pi$ termina em

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta, \varphi(a)\end{array}}{\Gamma \Rightarrow \Delta, \forall x\, \varphi(x)}\,\forall\mathrm{R}$$

em que a condição de variável própria é satisfeita, isto é, $a$ não ocorre em $\varphi(x)$, $\Gamma$ ou $\Delta$. Pela hipótese de indução, a premissa da última inferência é válida. Temos de mostrar que a conclusão também é válida, isto é, que para qualquer estrutura $\mathfrak{M}$, (a) $\mathfrak{M} \vDash \forall x\, \varphi(x)$, (b) $\mathfrak{M} \nvDash \chi$ para algum $\chi \in \Gamma$, ou (c) $\mathfrak{M} \vDash \chi$ para algum $\chi \in \Delta$.

Suponha que $\mathfrak{M}$ seja a estrutura arbitrária. Se (b) ou (c) vale, terminamos, então suponha que nenhuma vale: para todo $\chi \in \Gamma$, $\mathfrak{M} \vDash \chi$, e para todo $\chi \in \Delta$, $\mathfrak{M} \nvDash \chi$. Temos de mostrar que (a) vale, isto é, $\mathfrak{M} \vDash \forall x\, \varphi(x)$. Por Proposição 16.19, basta mostrar que $\mathfrak{M}, s \vDash \varphi(x)$ para toda atribuição de variáveis $s$. Então seja $s$ uma atribuição de variáveis arbitrária. Considere a estrutura $\mathfrak{M}'$ que é exatamente como $\mathfrak{M}$ exceto que $a^{\mathfrak{M}'} = s(x)$. Por Corolário 16.21, para qualquer $\chi \in \Gamma$, $\mathfrak{M}' \vDash \chi$ já que $a$ não ocorre em $\Gamma$, e para qualquer $\chi \in \Delta$, $\mathfrak{M}' \nvDash \chi$. Mas a premissa é válida, então $\mathfrak{M}' \vDash \varphi(a)$. Por Proposição 16.18, $\mathfrak{M}', s \vDash \varphi(a)$, já que $\varphi(a)$ é uma sentença. Agora $s \sim_x s$ com $s(x) = \mathrm{Val}_s^{\mathfrak{M}'}(a)$, já que definimos $\mathfrak{M}'$ exatamente desse modo. Assim Proposição 16.23 se aplica, e obtemos $\mathfrak{M}', s \vDash \varphi(x)$. Como $a$ não ocorre em $\varphi(x)$, por Proposição 16.20, $\mathfrak{M}, s \vDash \varphi(x)$. Como $s$ era arbitrário, completamos a prova de que $\mathfrak{M}, s \vDash \varphi(x)$ para toda atribuição de variáveis.

10. A última inferência é $\exists$L: Exercício.

Agora consideremos as inferências possíveis com duas premissas.

1. A última inferência é um corte: então $\pi$ termina em

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ \Gamma \Rightarrow \Delta, \varphi & \varphi, \Pi \Rightarrow \Lambda\end{array}}{\Gamma, \Pi \Rightarrow \Delta, \Lambda}\ \text{Cut}$$

   Seja $\mathfrak{M}$ a estrutura. Pela hipótese de indução, as premissas são válidas, então $\mathfrak{M}$ satisfaz ambas as premissas. Distinguimos dois casos: (a) $\mathfrak{M} \nvDash \varphi$ e (b) $\mathfrak{M} \vDash \varphi$. No caso (a), para que $\mathfrak{M}$ satisfaça a premissa esquerda, ela deve satisfazer $\Gamma \Rightarrow \Delta$. Mas então também satisfaz a conclusão. No caso (b), para que $\mathfrak{M}$ satisfaça a premissa direita, ela deve satisfazer $\Pi \setminus \Lambda$. Novamente, $\mathfrak{M}$ satisfaz a conclusão.

2. A última inferência é $\wedge$R. Então $\pi$ termina em

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ \Gamma \Rightarrow \Delta, \varphi & \Gamma \Rightarrow \Delta, \psi\end{array}}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}\ \wedge\text{R}$$

   Considere a estrutura $\mathfrak{M}$. Se $\mathfrak{M}$ satisfaz $\Gamma \Rightarrow \Delta$, terminamos. Então suponha que não. Como $\Gamma \Rightarrow \Delta, \varphi$ é válido pela hipótese de indução, $\mathfrak{M} \vDash \varphi$. Analogamente, como $\Gamma \Rightarrow \Delta, \psi$ é válido, $\mathfrak{M} \vDash \psi$. Mas então $\mathfrak{M} \vDash \varphi \wedge \psi$.

3. A última inferência é $\vee$L: Exercício.

4. A última inferência é $\rightarrow$L. Então $\pi$ termina em

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ \Gamma \Rightarrow \Delta, \varphi & \psi, \Pi \Rightarrow \Lambda\end{array}}{\varphi \rightarrow \psi, \Gamma, \Pi \Rightarrow \Delta, \Lambda}\ \rightarrow\text{L}$$

   Novamente, considere a estrutura $\mathfrak{M}$ e suponha que $\mathfrak{M}$ não satisfaça $\Gamma, \Pi \Rightarrow \Delta, \Lambda$. Temos de mostrar que $\mathfrak{M} \nvDash \varphi \rightarrow \psi$. Se $\mathfrak{M}$ não satisfaz $\Gamma, \Pi \Rightarrow \Delta, \Lambda$, não satisfaz nem $\Gamma \Rightarrow \Delta$ nem $\Pi \Rightarrow \Lambda$. Como $\Gamma \Rightarrow \Delta, \varphi$ é válido, temos $\mathfrak{M} \vDash \varphi$. Como $\psi, \Pi \Rightarrow \Lambda$ é válido, temos $\mathfrak{M} \nvDash \psi$. Mas então $\mathfrak{M} \nvDash \varphi \rightarrow \psi$, que é o que queríamos mostrar. □

**Corolário 19.29.** *Se $\vdash \varphi$, então $\varphi$ é válido.*

**Corolário 19.30.** *Se $\Gamma \vdash \varphi$, então $\Gamma \vDash \varphi$.*

*Prova.* Se $\Gamma \vdash \varphi$, então, para algum subconjunto finito $\Gamma_0 \subseteq \Gamma$, há a derivação de $\Gamma_0 \Rightarrow \varphi$. Por Teorema 19.28, toda estrutura $\mathfrak{M}$ ou torna algum $\psi \in \Gamma_0$ falso ou torna $\varphi$ verdadeiro. Logo, se $\mathfrak{M} \vDash \Gamma$, então também $\mathfrak{M} \vDash \varphi$. □

**Corolário 19.31.** *Se $\Gamma$ é satisfatível, então é consistente.*

*Prova.* Provamos a contrapositiva. Suponha que $\Gamma$ não seja consistente. Então há um $\Gamma_0 \subseteq \Gamma$ finito e a derivação de $\Gamma_0 \Rightarrow \quad$. Por Teorema 19.28, $\Gamma_0 \Rightarrow \quad$ é válido. Em outras palavras, para toda estrutura $\mathfrak{M}$, há $\chi \in \Gamma_0$ tal que $\mathfrak{M} \nvDash \chi$, e como $\Gamma_0 \subseteq \Gamma$, esse $\chi$ também está em $\Gamma$. Assim, nenhuma $\mathfrak{M}$ satisfaz $\Gamma$, e $\Gamma$ não é satisfatível. □

## 19.13 Derivações com Predicado de identidade

Derivações com predicado de identidade requerem sequentes iniciais e regras de inferência adicionais.

**Definição 19.32 (Sequentes iniciais para $=$).** Se $t$ é um termo fechado, então $\Rightarrow t = t$ é um sequente inicial.

As regras para $=$ são ($t_1$ e $t_2$ são termos fechados):

$$\frac{t_1 = t_2, \Gamma \Rightarrow \Delta, \varphi(t_1)}{t_1 = t_2, \Gamma \Rightarrow \Delta, \varphi(t_2)} = \qquad \frac{t_1 = t_2, \Gamma \Rightarrow \Delta, \varphi(t_2)}{t_1 = t_2, \Gamma \Rightarrow \Delta, \varphi(t_1)} =$$

**Exemplo 19.33.** Se $s$ e $t$ são termos fechados, então $s = t, \varphi(s) \vdash \varphi(t)$:

$$\dfrac{\dfrac{\varphi(s) \Rightarrow \varphi(s)}{s = t, \varphi(s) \Rightarrow \varphi(s)}\,\mathrm{WL}}{s = t, \varphi(s) \Rightarrow \varphi(t)}\,=$$

Isso pode ser familiar como o princípio da substitutibilidade de idênticos, ou Lei de Leibniz.

**LK** prova que $=$ é simétrica e transitiva:

$$\dfrac{\dfrac{\Rightarrow t_1 = t_1}{t_1 = t_2 \Rightarrow t_1 = t_1}\,\mathrm{WL}}{t_1 = t_2 \Rightarrow t_2 = t_1}\,= \qquad \dfrac{\dfrac{\dfrac{t_1 = t_2 \Rightarrow t_1 = t_2}{t_2 = t_3, t_1 = t_2 \Rightarrow t_1 = t_2}\,\mathrm{WL}}{t_2 = t_3, t_1 = t_2 \Rightarrow t_1 = t_3}\,=}{t_1 = t_2, t_2 = t_3 \Rightarrow t_1 = t_3}\,\mathrm{XL}$$

Na derivação à esquerda, a fórmula $x = t_1$ é o nosso $\varphi(x)$. À direita, tomamos $\varphi(x)$ como $t_1 = x$.

## 19.14 Correção com Predicado de identidade

**Proposição 19.34. LK** *com sequentes iniciais e regras para a identidade é correto.*

*Prova.* Sequentes iniciais da forma $\Rightarrow t = t$ são válidos, pois para toda estrutura $\mathfrak{M}$, $\mathfrak{M} \vDash t = t$. (Note que supomos que o termo $t$ seja fechado, isto é, que não contenha variáveis, de modo que atribuições de variáveis são irrelevantes).

Suponha que a última inferência em a derivação seja $=$. Então a premissa é $t_1 = t_2, \Gamma \Rightarrow \Delta, \varphi(t_1)$ e a conclusão é $t_1 = t_2, \Gamma \Rightarrow \Delta, \varphi(t_2)$. Considere a estrutura $\mathfrak{M}$. Precisamos mostrar que a conclusão é válida, isto é, se $\mathfrak{M} \vDash t_1 = t_2$ e $\mathfrak{M} \vDash \Gamma$, então ou $\mathfrak{M} \vDash \chi$ para algum $\chi \in \Delta$ ou $\mathfrak{M} \vDash \varphi(t_2)$.

Pela hipótese de indução, a premissa é válida. Isso significa que, se $\mathfrak{M} \vDash t_1 = t_2$ e $\mathfrak{M} \vDash \Gamma$, então ou (a) para algum $\chi \in \Delta$, $\mathfrak{M} \vDash \chi$, ou (b) $\mathfrak{M} \vDash \varphi(t_1)$. No caso (a), terminamos. Considere o caso (b). Seja $s$ uma atribuição de variáveis com $s(x) = \mathrm{Val}^{\mathfrak{M}}(t_1)$. Por Proposição 16.18, $\mathfrak{M}, s \vDash \varphi(t_1)$. Como $s \sim_x s$, por Proposição 16.23, $\mathfrak{M}, s \vDash \varphi(x)$. Como $\mathfrak{M} \vDash t_1 = t_2$, temos $\mathrm{Val}^{\mathfrak{M}}(t_1) = \mathrm{Val}^{\mathfrak{M}}(t_2)$, e portanto $s(x) = \mathrm{Val}^{\mathfrak{M}}(t_2)$. Aplicando Proposição 16.23 novamente, temos também $\mathfrak{M}, s \vDash \varphi(t_2)$. Por Proposição 16.18, $\mathfrak{M} \vDash \varphi(t_2)$. □

## Problemas

**Problema 19.1.** Dê derivações dos seguintes sequentes:

1. $\varphi \wedge (\psi \wedge \chi) \Rightarrow (\varphi \wedge \psi) \wedge \chi$.
2. $\varphi \vee (\psi \vee \chi) \Rightarrow (\varphi \vee \psi) \vee \chi$.
3. $\varphi \to (\psi \to \chi) \Rightarrow \psi \to (\varphi \to \chi)$.
4. $\varphi \Rightarrow \neg\neg\varphi$.

**Problema 19.2.** Dê derivações dos seguintes sequentes:

1. $(\varphi \vee \psi) \to \chi \Rightarrow \varphi \to \chi$.
2. $(\varphi \to \chi) \wedge (\psi \to \chi) \Rightarrow (\varphi \vee \psi) \to \chi$.
3. $\Rightarrow \neg(\varphi \wedge \neg\varphi)$.
4. $\psi \to \varphi \Rightarrow \neg\varphi \to \neg\psi$.
5. $\Rightarrow (\varphi \to \neg\varphi) \to \neg\varphi$.
6. $\Rightarrow \neg(\varphi \to \psi) \to \neg\psi$.
7. $\varphi \to \chi \Rightarrow \neg(\varphi \wedge \neg\chi)$.
8. $\varphi \wedge \neg\chi \Rightarrow \neg(\varphi \to \chi)$.

9. $\varphi \vee \psi, \neg\psi \Rightarrow \varphi$.
10. $\neg\varphi \vee \neg\psi \Rightarrow \neg(\varphi \wedge \psi)$.
11. $\Rightarrow (\neg\varphi \wedge \neg\psi) \to \neg(\varphi \vee \psi)$.
12. $\Rightarrow \neg(\varphi \vee \psi) \to (\neg\varphi \wedge \neg\psi)$.

**Problema 19.3.** Dê derivações dos seguintes sequentes:

1. $\neg(\varphi \to \psi) \Rightarrow \varphi$.
2. $\neg(\varphi \wedge \psi) \Rightarrow \neg\varphi \vee \neg\psi$.
3. $\varphi \to \psi \Rightarrow \neg\varphi \vee \psi$.
4. $\Rightarrow \neg\neg\varphi \to \varphi$.
5. $\varphi \to \psi, \neg\varphi \to \psi \Rightarrow \psi$.
6. $(\varphi \wedge \psi) \to \chi \Rightarrow (\varphi \to \chi) \vee (\psi \to \chi)$.
7. $(\varphi \to \psi) \to \varphi \Rightarrow \varphi$.
8. $\Rightarrow (\varphi \to \psi) \vee (\psi \to \chi)$.

(Todos esses requerem a regra CR.)

**Problema 19.4.** Dê derivações dos seguintes sequentes:

1. $\Rightarrow (\forall x\, \varphi(x) \wedge \forall y\, \psi(y)) \to \forall z\, (\varphi(z) \wedge \psi(z))$.
2. $\Rightarrow (\exists x\, \varphi(x) \vee \exists y\, \psi(y)) \to \exists z\, (\varphi(z) \vee \psi(z))$.
3. $\forall x\, (\varphi(x) \to \psi) \Rightarrow \exists y\, \varphi(y) \to \psi$.
4. $\forall x\, \neg\varphi(x) \Rightarrow \neg\exists x\, \varphi(x)$.
5. $\Rightarrow \neg\exists x\, \varphi(x) \to \forall x\, \neg\varphi(x)$.
6. $\Rightarrow \neg\exists x\, \forall y\, ((\varphi(x,y) \to \neg\varphi(y,y)) \wedge (\neg\varphi(y,y) \to \varphi(x,y)))$.

**Problema 19.5.** Dê derivações dos seguintes sequentes:

1. $\Rightarrow \neg\forall x\, \varphi(x) \to \exists x\, \neg\varphi(x)$.
2. $(\forall x\, \varphi(x) \to \psi) \Rightarrow \exists y\, (\varphi(y) \to \psi)$.
3. $\Rightarrow \exists x\, (\varphi(x) \to \forall y\, \varphi(y))$.

(Todos esses requerem a regra CR.)

**Problema 19.6.** Prove Proposição 19.16

**Problema 19.7.** Prove que $\Gamma \vdash \neg\varphi$ se, e somente se, $\Gamma \cup \{\varphi\}$ é inconsistente.

**Problema 19.8.** Complete a prova de Teorema 19.28.

**Problema 19.9.** Dê derivações dos seguintes sequentes:

1. $\Rightarrow \forall x\, \forall y\, ((x = y \wedge \varphi(x)) \rightarrow \varphi(y))$
2. $\exists x\, \varphi(x) \wedge \forall y\, \forall z\, ((\varphi(y) \wedge \varphi(z)) \rightarrow y = z) \Rightarrow \exists x\, (\varphi(x) \wedge \forall y\, (\varphi(y) \rightarrow y = x))$

# Capítulo 20

# Dedução Natural

Este capítulo apresenta um sistema de dedução natural no estilo de Gentzen/Prawitz.

Para incluir ou excluir material relevante à dedução natural como sistema de prova, use a tag "prfND".

## 20.1 Regras e Derivações

Sistemas de dedução natural pretendem ser um paralelo próximo do raciocínio informal usado em provas matemáticas (daí serem, de certo modo, "naturais"). Provas em dedução natural começam com hipóteses. Em seguida, aplicam-se regras de inferência. As hipóteses são "descarregadas" pelas regras de inferência $\neg$Intro, $\rightarrow$Intro, $\vee$Elim e $\exists$Elim, e o rótulo da hipótese descarregada é colocado ao lado da inferência para maior clareza.

**Definição 20.1 (Hipótese).** Uma *hipótese* é qualquer sentença na posição mais alta de qualquer ramo.

Derivações em dedução natural são certas árvores de sentenças, em que as sentenças no topo são hipóteses e, se a sentença está abaixo de um, dois ou três outros sequentes, ela deve seguir corretamente por uma regra de inferência. As sentenças no topo da inferência são chamadas de *premissas* e a sentença abaixo, de *conclusão* da inferência. As regras vêm em pares, uma regra de introdução e uma de eliminação para cada operador lógico. Elas introduzem a operador lógico na conclusão ou removem a operador lógico de uma premissa da regra. Algumas das regras permitem que uma hipótese de certo tipo seja *descarregada*. Para indicar qual hipótese é descarregada por qual inferência, também atribuímos rótulos tanto à hipótese quanto à inferência. Isso é indicado escrevendo-se a hipótese como "$[\varphi]^n$."

É costume considerar regras para todos os operadores lógicos $\wedge$, $\vee$, $\rightarrow$, $\neg$ e $\bot$, mesmo que alguns deles sejam definidos.

## 20.2 Regras Proposicionais

**Regras para $\wedge$**

$$\frac{\varphi \qquad \psi}{\varphi \wedge \psi}\ \wedge\text{Intro}$$

$$\frac{\varphi \wedge \psi}{\varphi}\ \wedge\text{Elim} \qquad \frac{\varphi \wedge \psi}{\psi}\ \wedge\text{Elim}$$

**Regras para $\vee$**

$$\frac{\varphi}{\varphi \vee \psi}\ \vee\text{Intro} \qquad \frac{\psi}{\varphi \vee \psi}\ \vee\text{Intro}$$

$$\overset{n}{\dfrac{\varphi \vee \psi \qquad \begin{array}{c}[\varphi]^n \\ \vdots \\ \chi\end{array} \qquad \begin{array}{c}[\psi]^n \\ \vdots \\ \chi\end{array}}{\chi}}\ \vee\text{Elim}$$

**Regras para $\rightarrow$**

$$\overset{n}{\dfrac{\begin{array}{c}[\varphi]^n \\ \vdots \\ \psi\end{array}}{\varphi \rightarrow \psi}}\ \rightarrow\text{Intro}$$

$$\frac{\varphi \rightarrow \psi \qquad \varphi}{\psi}\ \rightarrow\text{Elim}$$

**Regras para $\neg$**

$$\overset{n}{\dfrac{\begin{array}{c}[\varphi]^n \\ \vdots \\ \bot\end{array}}{\neg\varphi}}\ \neg\text{Intro}$$

$$\frac{\neg\varphi \qquad \varphi}{\bot}\ \neg\text{Elim}$$

### Regras para $\bot$

$$\frac{\bot}{\varphi}\,\bot_I \qquad\qquad \begin{array}{c}[\neg\varphi]^n\\ \vdots\\ \bot\end{array}\;{}^{n}\,\bot_C\;\varphi$$

Note que $\neg$Intro e $\bot_C$ são muito semelhantes: a diferença é que $\neg$Intro deriva uma sentença negada $\neg\varphi$, mas $\bot_C$, uma sentença positiva $\varphi$.

Sempre que uma regra indica que alguma hipótese pode ser descarregada, nós tomamos isso como uma permissão, mas não uma exigência. Por exemplo, na regra $\rightarrow$Intro, podemos descarregar qualquer número de hipóteses da forma $\varphi$ na derivação da premissa $\psi$, inclusive zero.

## 20.3 Regras de Quantificadores

### Regras para $\forall$

$$\frac{\varphi(a)}{\forall x\,\varphi(x)}\,\forall\text{Intro} \qquad\qquad \frac{\forall x\,\varphi(x)}{\varphi(t)}\,\forall\text{Elim}$$

Nas regras para $\forall$, $t$ é um termo fechado (um termo que não contém nenhuma variável), e $a$ é a símbolo de constante que não ocorre na conclusão $\forall x\,\varphi(x)$, nem em qualquer hipótese que esteja não descarregada na derivação que termina com a premissa $\varphi(a)$. Chamamos $a$ de *variável própria* da inferência $\forall$Intro.[1]

### Regras para $\exists$

$$\frac{\varphi(t)}{\exists x\,\varphi(x)}\,\exists\text{Intro} \qquad\qquad {}^{n}\,\frac{\exists x\,\varphi(x) \qquad \begin{array}{c}[\varphi(a)]^n\\ \vdots\\ \chi\end{array}}{\chi}\,\exists\text{Elim}$$

[1] Usamos o termo "variável própria" embora $a$ na regra acima seja uma constante. Isso tem razões históricas.

Novamente, $t$ é um termo fechado, e $a$ é a símbolo de constante que não ocorre na premissa $\exists x\, \varphi(x)$, na conclusão $\chi$, nem em qualquer hipótese que esteja não descarregada nas derivações que terminam com as duas premissas (além das hipóteses $\varphi(a)$). Chamamos $a$ de *variável própria* da inferência $\exists$Elim.

A condição de que uma variável própria não ocorra nem nas premissas nem em qualquer hipótese que esteja não descarregada nas derivações que levam às premissas para a inferência $\forall$Intro ou $\exists$Elim é chamada de *condição de variável própria*.

Lembre-se da convenção de que, quando $\varphi$ é a fórmula com a variável $x$ livre, indicamos isso escrevendo $\varphi(x)$. No mesmo contexto, $\varphi(t)$ é então uma abreviação de $\varphi[t/x]$. Assim, poderíamos também escrever a regra $\exists$Intro como:

$$\frac{\varphi[t/x]}{\exists x\, \varphi}\ \exists\text{Intro}$$

Note que $t$ pode já ocorrer em $\varphi$, por exemplo, $\varphi$ poderia ser $P(t, x)$. Assim, inferir $\exists x\, P(t, x)$ de $P(t, t)$ é uma aplicação correta de $\exists$Intro—pode-se "substituir" uma ou mais, e não necessariamente todas, as ocorrências de $t$ na premissa pela variável $x$ ligada. Contudo, as condições de variável própria em $\forall$Intro e $\exists$Elim exigem que a símbolo de constante $a$ não ocorra em $\varphi$. Portanto, não se pode inferir corretamente $\forall x\, P(a, x)$ de $P(a, a)$ usando $\forall$Intro.

Em $\exists$Intro e $\forall$Elim não há restrições, e o termo $t$ pode ser qualquer coisa, de modo que não temos de nos preocupar com nenhuma condição. Por outro lado, nas regras $\exists$Elim e $\forall$Intro, a condição de variável própria exige que a símbolo de constante $a$ não ocorra em lugar algum na conclusão nem em uma hipótese não descarregada. A condição é necessária para garantir que o sistema seja correto, isto é, que só deriva sentenças de hipóteses não descarregadas das quais elas se seguem. Sem essa condição, o seguinte seria permitido:

$$\dfrac{\exists x\, \varphi(x) \qquad \dfrac{[\varphi(a)]^1}{\forall x\, \varphi(x)}\ {*}\forall\text{Intro}}{\forall x\, \varphi(x)}\ \exists\text{Elim}$$

Contudo, $\exists x\, \varphi(x) \nvDash \forall x\, \varphi(x)$.

Como as regras de eliminação para quantificadores só permitem substituir variáveis por termos fechados, segue-se que qualquer fórmula que possa ser derivada de um conjunto de sentenças é ela própria a sentença.

## 20.4 Derivações

Já dissemos o que é uma hipótese e demos as regras de inferência. Derivações em dedução natural são geradas indutivamente a partir disso: cada derivação ou é uma hipótese por si só, ou consiste em uma, duas ou três derivações seguidas de uma inferência correta.

**Definição 20.2 (Derivação).** A *derivação* de a sentença $\varphi$ a partir de hipóteses $\Gamma$ é uma árvore finita de sentenças que satisfaz as seguintes condições:

1. As sentenças no topo da árvore ou estão em $\Gamma$ ou são descarregadas por uma inferência na árvore.

2. A sentença na base da árvore é $\varphi$.

3. Toda sentença na árvore exceto a sentença $\varphi$ na base é uma premissa de uma aplicação correta de uma regra de inferência cuja conclusão está diretamente abaixo daquela sentença na árvore.

Dizemos então que $\varphi$ é a *conclusão* da derivação e $\Gamma$, suas hipóteses não descarregadas.

Se existe a derivação de $\varphi$ a partir de $\Gamma$, dizemos que $\varphi$ é *derivável* a partir de $\Gamma$, ou, em símbolos: $\Gamma \vdash \varphi$. Se há a derivação de $\varphi$ em que toda hipótese é descarregada, escrevemos $\vdash \varphi$.

**Exemplo 20.3.** Toda hipótese por si só é a derivação. Assim, por exemplo, $\varphi$ por si só é a derivação, e $\psi$ por si só também. Podemos obter uma nova derivação a partir delas aplicando, digamos, a regra $\wedge$Intro,

$$\dfrac{\varphi \qquad \psi}{\varphi \wedge \psi}\,\wedge\text{Intro}$$

Essas regras devem ser gerais: podemos substituir o $\varphi$ e $\psi$ nela por quaisquer sentenças, por exemplo, por $\chi$ e $\theta$. Então a conclusão seria $\chi \wedge \theta$, e assim

$$\dfrac{\chi \qquad \theta}{\chi \wedge \theta}\,\wedge\text{Intro}$$

é uma derivação correta. É claro que também podemos trocar as hipóteses, de modo que $\theta$ desempenhe o papel de $\varphi$ e $\chi$ o de $\psi$. Assim,

$$\dfrac{\theta \qquad \chi}{\theta \wedge \chi}\,\wedge\text{Intro}$$

também é uma derivação correta.

Podemos agora aplicar outra regra, digamos, $\rightarrow$Intro, que nos permite concluir um condicional e nos permite descarregar qualquer hipótese que seja idêntica ao antecedente desse condicional. Assim, ambas as seguintes seriam derivações corretas:

$$1\,\dfrac{\dfrac{[\chi]^1 \qquad \theta}{\chi \wedge \theta}\,\wedge\text{Intro}}{\chi \rightarrow (\chi \wedge \theta)}\,\rightarrow\text{Intro} \qquad 1\,\dfrac{\dfrac{\chi \qquad [\theta]^1}{\chi \wedge \theta}\,\wedge\text{Intro}}{\theta \rightarrow (\chi \wedge \theta)}\,\rightarrow\text{Intro}$$

Elas mostram, respectivamente, que $\theta \vdash \chi \to (\chi \wedge \theta)$ e $\chi \vdash \theta \to (\chi \wedge \theta)$.

Lembre-se de que descarregar hipóteses é uma permissão, não uma exigência: não temos de descarregar as hipóteses. Em particular, podemos aplicar uma regra mesmo que as hipóteses não estejam presentes na derivação. Por exemplo, o seguinte é válido, embora não haja hipótese $\varphi$ a ser descarregada:

$$\dfrac{\psi}{\varphi \to \psi}\,{}^{1}\,{\to}\text{Intro}$$

## 20.5 Exemplos de Derivações

**Exemplo 20.4.** Vamos dar a derivação da sentença $(\varphi \wedge \psi) \to \varphi$.

Começamos escrevendo a conclusão desejada na parte inferior da derivação.

$$\dfrac{}{(\varphi \wedge \psi) \to \varphi}$$

Em seguida, precisamos descobrir que tipo de inferência poderia resultar em a sentença desta forma. O operador principal da conclusão é $\to$, então tentaremos chegar à conclusão usando a regra $\to$Intro. O melhor é anotar as suposições envolvidas e rotular as regras de inferência conforme avançamos, para que seja fácil ver se todas as suposições foram descarregadas ao final da prova.

$$\dfrac{\begin{array}{c}[\varphi \wedge \psi]^{1} \\ \vdots \\ \varphi\end{array}}{(\varphi \wedge \psi) \to \varphi}\,{}^{1}\,{\to}\text{Intro}$$

Agora precisamos preencher os passos da suposição $\varphi \wedge \psi$ até $\varphi$. Como só temos um conectivo com o qual lidar, $\wedge$, devemos usar a regra $\wedge$ elim. Isso nos dá a seguinte prova:

$$\dfrac{\dfrac{[\varphi \wedge \psi]^{1}}{\varphi}\,{\wedge}\text{Elim}}{(\varphi \wedge \psi) \to \varphi}\,{}^{1}\,{\to}\text{Intro}$$

Agora temos uma derivação correta de $(\varphi \wedge \psi) \to \varphi$.

**Exemplo 20.5.** Agora vamos dar a derivação de $(\neg\varphi \vee \psi) \to (\varphi \to \psi)$.

Começamos escrevendo a conclusão desejada na parte inferior da derivação.

$$\dfrac{}{(\neg\varphi \vee \psi) \to (\varphi \to \psi)}$$

Para encontrar uma regra lógica que possa nos dar esta conclusão, observamos os conectivos lógicos na conclusão: $\neg$, $\vee$ e $\rightarrow$. Por enquanto, só nos interessa a primeira ocorrência de $\rightarrow$, porque é o operador principal da sentença na conclusão, enquanto $\neg$, $\vee$ e a segunda ocorrência de $\rightarrow$ estão dentro do escopo de outro conectivo, então cuidaremos deles depois. Começamos, portanto, com a regra $\rightarrow$Intro. Uma aplicação correta deve ser assim:

$$\dfrac{\begin{array}{c}[\neg\varphi \vee \psi]^1 \\ \vdots \\ \varphi \rightarrow \psi\end{array}}{(\neg\varphi \vee \psi) \rightarrow (\varphi \rightarrow \psi)}\ {\scriptstyle 1}\ \rightarrow\text{Intro}$$

Isso nos deixa com duas possibilidades para continuar. Podemos continuar trabalhando de baixo para cima e procurar outra aplicação da regra $\rightarrow$Intro, ou podemos trabalhar de cima para baixo e aplicar a regra $\vee$Elim. Vamos adotar a segunda opção. Usaremos a suposição $\neg\varphi \vee \psi$ como a premissa mais à esquerda de $\vee$Elim. Para uma aplicação válida de $\vee$Elim, as outras duas premissas devem ser idênticas à conclusão $\varphi \rightarrow \psi$, mas cada uma pode ser derivada, por sua vez, de outra suposição, a saber, um dos dois disjuntos de $\neg\varphi \vee \psi$. Nossa derivação ficará, então, assim:

$$\dfrac{\dfrac{\begin{array}{ccc}[\neg\varphi \vee \psi]^1 & \begin{array}{c}[\neg\varphi]^2 \\ \vdots \\ \varphi \rightarrow \psi\end{array} & \begin{array}{c}[\psi]^2 \\ \vdots \\ \varphi \rightarrow \psi\end{array}\end{array}}{\varphi \rightarrow \psi}\ {\scriptstyle 2}\ \vee\text{Elim}}{(\neg\varphi \vee \psi) \rightarrow (\varphi \rightarrow \psi)}\ {\scriptstyle 1}\ \rightarrow\text{Intro}$$

Em cada um dos dois ramos à direita, queremos derivar $\varphi \rightarrow \psi$, o que é melhor feito usando $\rightarrow$Intro.

$$\dfrac{\dfrac{\begin{array}{ccc}[\neg\varphi \vee \psi]^1 & \dfrac{\begin{array}{c}[\neg\varphi]^2, [\varphi]^3 \\ \vdots \\ \psi\end{array}}{\varphi \rightarrow \psi}\ {\scriptstyle 3}\ \rightarrow\text{Intro} & \dfrac{\begin{array}{c}[\psi]^2, [\varphi]^4 \\ \vdots \\ \psi\end{array}}{\varphi \rightarrow \psi}\ {\scriptstyle 4}\ \rightarrow\text{Intro}\end{array}}{\varphi \rightarrow \psi}\ {\scriptstyle 2}\ \vee\text{Elim}}{(\neg\varphi \vee \psi) \rightarrow (\varphi \rightarrow \psi)}\ {\scriptstyle 1}\ \rightarrow\text{Intro}$$

Nas duas partes que faltam na derivação, precisamos de derivações de $\psi$ a partir de $\neg\varphi$ e $\varphi$ no meio, e a partir de $\varphi$ e $\psi$ à esquerda. Comecemos pelo primeiro caso. $\neg\varphi$ e $\varphi$ são as duas premissas de $\neg$Elim:

$$\dfrac{[\neg\varphi]^2 \qquad [\varphi]^3}{\dfrac{\bot}{\vdots\;\psi}}\,\neg\text{Elim}$$

Usando $\bot_I$, podemos obter $\psi$ como conclusão e completar o ramo.

$$\dfrac{\dfrac{[\neg\varphi\vee\psi]^1 \qquad \dfrac{\dfrac{\dfrac{[\neg\varphi]^2 \qquad [\varphi]^3}{\bot}\,\bot\text{Intro}}{\psi}\,\bot_I}{\varphi\to\psi}\,3{\to}\text{Intro} \qquad \dfrac{[\psi]^2,[\varphi]^4}{\vdots\;\psi}}{\varphi\to\psi}\,2{\vee}\text{Elim}}{(\neg\varphi\vee\psi)\to(\varphi\to\psi)}\,1{\to}\text{Intro}$$

Vejamos agora o ramo mais à direita. Aqui é importante perceber que a definição de derivação *permite que hipóteses sejam descarregadas* mas *não exige* que o sejam. Em outras palavras, se pudermos derivar $\psi$ a partir de uma das suposições $\varphi$ e $\psi$ sem usar a outra, tudo bem. E para derivar $\psi$ a partir de $\psi$ é trivial: $\psi$ por si só é tal a derivação, e nenhuma inferência é necessária. Portanto, podemos simplesmente eliminar a suposição $\varphi$.

$$\dfrac{\dfrac{[\neg\varphi\vee\psi]^1 \qquad \dfrac{\dfrac{\dfrac{[\neg\varphi]^2 \qquad [\varphi]^3}{\bot}\,\neg\text{Elim}}{\psi}\,\bot_I}{\varphi\to\psi}\,3{\to}\text{Intro} \qquad \dfrac{[\psi]^2}{\varphi\to\psi}\,{\to}\text{Intro}}{\varphi\to\psi}\,2{\vee}\text{Elim}}{(\neg\varphi\vee\psi)\to(\varphi\to\psi)}\,1{\to}\text{Intro}$$

Observe que, na derivação concluída, a inferência $\to$Intro mais à direita na verdade não descarrega nenhuma hipótese.

**Exemplo 20.6.** Até agora não precisamos da regra $\bot_C$. Ela é especial porque nos permite descarregar uma hipótese que não é uma sub-fórmula da conclusão da regra. Está intimamente relacionada à regra $\bot_I$. Na verdade, a regra $\bot_I$ é um caso especial da regra $\bot_C$—existe uma lógica chamada "lógica intuicionista" na qual apenas $\bot_I$ é permitida. A regra $\bot_C$ é um último recurso quando nada mais funciona. Por exemplo, suponha que queiramos derivar $\varphi\vee\neg\varphi$. Nossa estratégia usual seria tentar derivar $\varphi\vee\neg\varphi$ usando $\vee$Intro. Mas isso exigiria derivar $\varphi$ ou $\neg\varphi$ a partir de nenhuma suposição, e isso não pode ser feito. $\bot_C$ ao resgate!

$$\dfrac{\dfrac{\begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1\\ \vdots\\ \bot\end{array}}{\varphi \vee \neg\varphi}\,{\scriptstyle 1}\,\bot_C}{}$$

Agora procuramos a derivação de $\bot$ a partir de $\neg(\varphi \vee \neg\varphi)$. Como $\bot$ é a conclusão de ¬Elim, podemos tentar isso:

$$\dfrac{\dfrac{\begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1\\ \vdots\\ \neg\varphi\end{array} \qquad \begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1\\ \vdots\\ \varphi\end{array}}{\bot}\,\neg\text{Elim}}{\dfrac{\bot}{\varphi \vee \neg\varphi}\,{\scriptstyle 1}\,\bot_C}$$

Nossa estratégia para encontrar a derivação de $\neg\varphi$ exige uma aplicação de ¬Intro:

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1, [\varphi]^2\\ \vdots\\ \bot\end{array}}{\neg\varphi}\,{\scriptstyle 2}\,\neg\text{Intro} \qquad \begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1\\ \vdots\\ \varphi\end{array}}{\bot}\,\neg\text{Elim}}{\dfrac{\bot}{\varphi \vee \neg\varphi}\,{\scriptstyle 1}\,\bot_C}$$

Aqui, podemos obter $\bot$ facilmente aplicando ¬Elim à suposição $\neg(\varphi \vee \neg\varphi)$ e a $\varphi \vee \neg\varphi$, que segue da nossa nova suposição $\varphi$ por ∨Intro:

$$\dfrac{\dfrac{\dfrac{\dfrac{[\neg(\varphi \vee \neg\varphi)]^1 \qquad \dfrac{[\varphi]^2}{\varphi \vee \neg\varphi}\,\vee\text{Intro}}{\bot}\,\neg\text{Elim}}{\neg\varphi}\,{\scriptstyle 2}\,\neg\text{Intro} \qquad \begin{array}{c}[\neg(\varphi \vee \neg\varphi)]^1\\ \vdots\\ \varphi\end{array}}{\bot}\,\neg\text{Elim}}{\dfrac{\bot}{\varphi \vee \neg\varphi}\,{\scriptstyle 1}\,\bot_C}$$

No lado direito usamos a mesma estratégia, exceto que obtemos $\varphi$ por $\bot_C$:

$$\dfrac{\dfrac{\dfrac{\dfrac{[\neg(\varphi \vee \neg\varphi)]^1 \qquad \dfrac{[\varphi]^2}{\varphi \vee \neg\varphi}\,\vee\text{Intro}}{\bot}\,\neg\text{Elim}}{\neg\varphi}\,{\scriptstyle 2}\,\neg\text{Intro} \qquad \dfrac{\dfrac{[\neg(\varphi \vee \neg\varphi)]^1 \qquad \dfrac{[\neg\varphi]^3}{\varphi \vee \neg\varphi}\,\vee\text{Intro}}{\bot}\,\neg\text{Elim}}{\varphi}\,{\scriptstyle 3}\,\bot_C}{\bot}\,\neg\text{Elim}}{\dfrac{\bot}{\varphi \vee \neg\varphi}\,{\scriptstyle 1}\,\bot_C}$$

## 20.6 Derivações com Quantificadores

**Exemplo 20.7.** Ao lidar com quantificadores, temos de cuidar para não violar a condição de variável própria, e às vezes isso exige que brinquemos com a ordem de execução de certas inferências. Em geral, ajuda tentar cuidar primeiro das regras sujeitas à condição de variável própria (elas ficarão mais abaixo na prova finalizada).

Vamos ver como daríamos a derivação de fórmula $\exists x\, \neg\varphi(x) \to \neg\forall x\, \varphi(x)$. Começando como de costume, escrevemos

$$\frac{}{\exists x\, \neg\varphi(x) \to \neg\forall x\, \varphi(x)}$$

Começamos escrevendo o que seria necessário para justificar esse último passo usando a regra $\to$Intro.

$$\dfrac{\begin{array}{c}[\exists x\, \neg\varphi(x)]^1 \\ \vdots \\ \neg\forall x\, \varphi(x)\end{array}}{\exists x\, \neg\varphi(x) \to \neg\forall x\, \varphi(x)}\ {\scriptstyle 1}\ \to\text{Intro}$$

Como não há uma regra óbvia para aplicar a $\neg\forall x\, \varphi(x)$, prosseguiremos montando a derivação de modo que possamos usar a regra $\exists$Elim. Aqui devemos prestar atenção à condição de variável própria e escolher uma constante que não apareça em $\exists x\, \varphi(x)$ nem em quaisquer suposições das quais ela dependa. (Como, no entanto, nenhum símbolo de constante aparece, qualquer escolha servirá.)

$$\dfrac{\dfrac{\begin{array}{cc}[\exists x\, \neg\varphi(x)]^1 & \neg\forall x\, \varphi(x)\end{array}}{\neg\forall x\, \varphi(x)}\ {\scriptstyle 2}\ \exists\text{Elim}}{\exists x\, \neg\varphi(x) \to \neg\forall x\, \varphi(x)}\ {\scriptstyle 1}\ \to\text{Intro}$$

$$\begin{array}{c}[\neg\varphi(a)]^2 \\ \vdots \end{array}$$

Para derivar $\neg\forall x\, \varphi(x)$, tentaremos usar a regra $\neg$Intro: isso exige que derivemos uma contradição, possivelmente usando $\forall x\, \varphi(x)$ como suposição adicional. É claro que essa contradição pode envolver a suposição $\neg\varphi(a)$, que será descarregada pela inferência $\exists$Elim. Podemos montá-la da seguinte forma:

$$\dfrac{\dfrac{[\exists x\, \neg\varphi(x)]^1 \qquad \dfrac{\dfrac{[\neg\varphi(a)]^2,\, [\forall x\, \varphi(x)]^3}{\vdots}}{\bot}\, 3}{\neg\forall x\, \varphi(x)}\, \neg\text{Intro}}{\exists x\, \neg\varphi(x)}\, 2\ \exists\text{Elim}}{\exists x\, \neg\varphi(x) \to \neg\forall x\, \varphi(x)}\, 1\ \to\text{Intro}$$

Parece que estamos perto de obter uma contradição. A regra mais fácil de aplicar é a ∀Elim, que não possui condição de variável própria. Como podemos usar qualquer termo que queiramos para substituir o $x$ universalmente quantificado, faz mais sentido continuar usando $a$ para chegarmos a uma contradição.

$$\dfrac{\dfrac{[\exists x\, \neg\varphi(x)]^1 \qquad \dfrac{\dfrac{[\neg\varphi(a)]^2 \qquad \dfrac{[\forall x\, \varphi(x)]^3}{\varphi(a)}\, \forall\text{Elim}}{\bot}\, \neg\text{Elim}}{\neg\forall x\, \varphi(x)}\, 3\ \neg\text{Intro}}{\exists x\, \neg\varphi(x)}\, 2\ \exists\text{Elim}}{\exists x\, \neg\varphi(x) \to \neg\forall x\, \varphi(x)}\, 1\ \to\text{Intro}$$

É importante, especialmente ao lidar com quantificadores, verificar com cuidado neste ponto que a condição de variável própria não foi violada. Como a única regra que aplicamos sujeita à condição de variável própria foi ∃Elim, e a variável própria $a$ não ocorre em nenhuma suposição da qual dependa, esta é uma derivação correta.

**Exemplo 20.8.** Às vezes podemos derivar a fórmula a partir de outras fórmulas. Nesses casos, podemos ter suposições não descarregadas. É importante acompanhar nossas suposições, bem como o objetivo final.

Vamos ver como daríamos a derivação de fórmula $\exists x\, \chi(x, b)$ a partir das suposições $\exists x\, (\varphi(x) \wedge \psi(x))$ e $\forall x\, (\psi(x) \to \chi(x, b))$. Começando como de costume, escrevemos a conclusão na parte inferior.

$$\dfrac{}{\exists x\, \chi(x, b)}$$

Temos duas premissas com as quais trabalhar. Para usar a primeira, isto é, tentar encontrar a derivação de $\exists x\, \chi(x, b)$ a partir de $\exists x\, (\varphi(x) \wedge \psi(x))$, usaríamos a regra ∃Elim. Como ela possui condição de variável própria, aplicaremos essa regra primeiro. Obtemos o seguinte:

$$\dfrac{\exists x\,(\varphi(x) \wedge \psi(x)) \qquad \begin{array}{c}[\varphi(a) \wedge \psi(a)]^1 \\ \vdots \\ \exists x\,\chi(x,b)\end{array}}{\exists x\,\chi(x,b)}\,{}^{1}\exists\text{Elim}$$

As duas suposições com as quais estamos trabalhando compartilham $\psi$. Pode ser útil neste ponto aplicar $\wedge$Elim para separar $\psi(a)$.

$$\dfrac{\exists x\,(\varphi(x) \wedge \psi(x)) \qquad \begin{array}{c}\dfrac{[\varphi(a) \wedge \psi(a)]^1}{\psi(a)}\,\wedge\text{Elim} \\ \vdots \\ \exists x\,\chi(x,b)\end{array}}{\exists x\,\chi(x,b)}\,{}^{1}\exists\text{Elim}$$

A segunda suposição com a qual temos de trabalhar é $\forall x\,(\psi(x) \to \chi(x,b))$. Como não há condição de variável própria, podemos instanciar $x$ com o símbolo de constante $a$ usando $\forall$Elim para obter $\psi(a) \to \chi(a,b)$. Agora temos tanto $\psi(a) \to \chi(a,b)$ quanto $\psi(a)$. Nosso próximo passo deve ser uma aplicação direta da regra $\to$Elim.

$$\dfrac{\exists x\,(\varphi(x) \wedge \psi(x)) \qquad \begin{array}{c}\dfrac{\dfrac{\forall x\,(\psi(x) \to \chi(x,b))}{\psi(a) \to \chi(a,b)}\,\forall\text{Elim} \qquad \dfrac{[\varphi(a) \wedge \psi(a)]^1}{\psi(a)}\,\wedge\text{Elim}}{\chi(a,b)}\,\to\text{Elim} \\ \vdots \\ \exists x\,\chi(x,b)\end{array}}{\exists x\,\chi(x,b)}\,{}^{1}\exists\text{Elim}$$

Estamos quase lá! Uma aplicação de $\exists$Intro e atingimos nosso objetivo.

$$\dfrac{\exists x\,(\varphi(x) \wedge \psi(x)) \qquad \begin{array}{c}\dfrac{\dfrac{\forall x\,(\psi(x) \to \chi(x,b))}{\psi(a) \to \chi(a,b)}\,\forall\text{Elim} \qquad \dfrac{[\varphi(a) \wedge \psi(a)]^1}{\psi(a)}\,\wedge\text{Elim}}{\chi(a,b)}\,\to\text{Elim} \\ \dfrac{\chi(a,b)}{\exists x\,\chi(x,b)}\,\exists\text{Intro}\end{array}}{\exists x\,\chi(x,b)}\,{}^{1}\exists\text{Elim}$$

Como garantimos em cada etapa que as condições de variável própria não foram violadas, podemos estar confiantes de que esta é uma derivação correta.

**Exemplo 20.9.** Dê a derivação de fórmula $\neg\forall x\,\varphi(x)$ a partir das suposições $\forall x\,\varphi(x) \to \exists y\,\psi(y)$ e $\neg\exists y\,\psi(y)$. Começando como de costume, escrevemos a fórmula alvo na parte inferior.

$$\frac{}{\neg\forall x\, \varphi(x)}$$

A última linha da derivação é uma negação, então vamos tentar usar ¬Intro. Isso exigirá que descubramos como derivar uma contradição.

$$\dfrac{\begin{array}{c}[\forall x\, \varphi(x)]^1 \\ \vdots \\ \bot\end{array}}{\neg\forall x\, \varphi(x)}\, 1\ \neg\text{Intro}$$

Até aqui, tudo bem. Podemos usar ∀Elim, mas não é óbvio se isso nos ajudará a alcançar nosso objetivo. Em vez disso, vamos usar uma de nossas suposições. $\forall x\, \varphi(x) \to \exists y\, \psi(y)$ junto com $\forall x\, \varphi(x)$ nos permitirá usar a regra →Elim.

$$\dfrac{\begin{array}{c}\dfrac{\forall x\, \varphi(x) \to \exists y\, \psi(y) \qquad [\forall x\, \varphi(x)]^1}{\exists y\, \psi(y)}\ \to\text{Elim} \\ \vdots \\ \bot\end{array}}{\neg\forall x\, \varphi(x)}\, 1\ \neg\text{Intro}$$

Agora temos uma suposição final com a qual trabalhar, e parece que isso nos ajudará a chegar a uma contradição usando ¬Elim.

$$\dfrac{\begin{array}{cc}\neg\exists y\, \psi(y) & \dfrac{\forall x\, \varphi(x) \to \exists y\, \psi(y) \qquad [\forall x\, \varphi(x)]^1}{\exists y\, \psi(y)}\ \to\text{Elim} \\ & \bot\end{array}}{\neg\forall x\, \varphi(x)}\, 1\ \neg\text{Intro}\ \neg\text{Elim}$$

## 20.7 Noções da Teoria da Prova

Esta seção reúne as definições da relação de demonstrabilidade e de consistência para a dedução natural.

Assim como definimos várias noções semânticas importantes (validade, consequência, satisfatibilidade), agora definimos noções *da Teoria da Prova* correspondentes. Elas não são definidas por apelo à satisfação de sentenças em estruturas, mas por apelo à derivabilidade ou não derivabilidade de certas sentenças a partir de outras. Foi uma descoberta importante que essas noções coincidem. Que coincidem é o conteúdo dos teoremas de *correção* e *completude*.

**Definição 20.10 (Teoremas).** Uma sentença $\varphi$ é um *teorema* se há uma derivação de $\varphi$ em dedução natural na qual todas as hipóteses são descarregadas. Escrevemos $\vdash \varphi$ se $\varphi$ é um teorema e $\nvdash \varphi$ se não o é.

**Definição 20.11 (Derivabilidade).** A sentença $\varphi$ é *derivável de* um conjunto de sentenças $\Gamma$, $\Gamma \vdash \varphi$, se há uma derivação com conclusão $\varphi$ e na qual toda hipótese é ou descarregada ou está em $\Gamma$. Se $\varphi$ não é derivável de $\Gamma$, escrevemos $\Gamma \nvdash \varphi$.

**Definição 20.12 (Consistência).** Um conjunto de sentenças $\Gamma$ é *inconsistente* se, e somente se, $\Gamma \vdash \bot$. Se $\Gamma$ não é inconsistente, isto é, se $\Gamma \nvdash \bot$, dizemos que é *consistente*.

**Proposição 20.13 (Reflexividade).** *Se $\varphi \in \Gamma$, então $\Gamma \vdash \varphi$.*

*Prova.* A hipótese $\varphi$ por si só é uma derivação de $\varphi$ em que toda hipótese não descarregada (isto é, $\varphi$) está em $\Gamma$. □

**Proposição 20.14 (Monotonicidade).** *Se $\Gamma \subseteq \Delta$ e $\Gamma \vdash \varphi$, então $\Delta \vdash \varphi$.*

*Prova.* Qualquer derivação de $\varphi$ a partir de $\Gamma$ é também uma derivação de $\varphi$ a partir de $\Delta$. □

**Proposição 20.15 (Transitividade).** *Se $\Gamma \vdash \varphi$ e $\{\varphi\} \cup \Delta \vdash \psi$, então $\Gamma \cup \Delta \vdash \psi$.*

*Prova.* Se $\Gamma \vdash \varphi$, há uma derivação $\delta_0$ de $\varphi$ com todas as hipóteses não descarregadas em $\Gamma$. Se $\{\varphi\} \cup \Delta \vdash \psi$, então há uma derivação $\delta_1$ de $\psi$ com todas as hipóteses não descarregadas em $\{\varphi\} \cup \Delta$. Considere agora:

$$\dfrac{\dfrac{\begin{array}{c}\Delta, [\varphi]^1 \\ \vdots\,\delta_1 \\ \psi\end{array}}{1\ \varphi \to \psi}\ {\to}\text{Intro} \qquad \begin{array}{c}\Gamma \\ \vdots\,\delta_0 \\ \varphi\end{array}}{\psi}\ {\to}\text{Elim}$$

As hipóteses não descarregadas estão agora todas entre $\Gamma \cup \Delta$, de modo que isto mostra $\Gamma \cup \Delta \vdash \psi$. □

Quando $\Gamma = \{\varphi_1, \varphi_2, \ldots, \varphi_k\}$ é um conjunto finito, podemos usar a notação simplificada $\varphi_1, \varphi_2, \ldots, \varphi_k \vdash \psi$ para $\Gamma \vdash \psi$; em particular, $\varphi \vdash \psi$ significa que $\{\varphi\} \vdash \psi$.

Note que se $\Gamma \vdash \varphi$ e $\varphi \vdash \psi$, então $\Gamma \vdash \psi$. Segue também que se $\varphi_1, \ldots, \varphi_n \vdash \psi$ e $\Gamma \vdash \varphi_i$ para cada $i$, então $\Gamma \vdash \psi$.

**Proposição 20.16.** *As seguintes afirmações são equivalentes.*

1. *$\Gamma$ é inconsistente.*
2. *$\Gamma \vdash \varphi$ para toda sentença $\varphi$.*
3. *$\Gamma \vdash \varphi$ e $\Gamma \vdash \neg\varphi$ para alguma sentença $\varphi$.*

*Prova.* Exercício. □

**Proposição 20.17 (Compacidade).** *1. Se $\Gamma \vdash \varphi$, então há um subconjunto finito $\Gamma_0 \subseteq \Gamma$ tal que $\Gamma_0 \vdash \varphi$.*

*2. Se todo subconjunto finito de $\Gamma$ é consistente, então $\Gamma$ é consistente.*

*Prova.* 1. Se $\Gamma \vdash \varphi$, então há uma derivação $\delta$ de $\varphi$ a partir de $\Gamma$. Seja $\Gamma_0$ o conjunto de hipóteses não descarregadas de $\delta$. Como toda derivação é finita, $\Gamma_0$ só pode conter finitamente muitas sentenças. Assim, $\delta$ é uma derivação de $\varphi$ a partir de um $\Gamma_0$ finito $\subseteq \Gamma$.

2. Isto é a contrapositiva de (1) no caso especial $\varphi \equiv \bot$. □

## 20.8 Derivabilidade e Consistência

Estabeleceremos agora várias propriedades da relação de derivabilidade. Elas são independentemente interessantes, mas cada uma desempenhará um papel na prova do teorema da completude.

**Proposição 20.18.** *Se $\Gamma \vdash \varphi$ e $\Gamma \cup \{\varphi\}$ é inconsistente, então $\Gamma$ é inconsistente.*

*Prova.* Seja a derivação de $\varphi$ a partir de $\Gamma$ igual a $\delta_1$ e a derivação de $\bot$ a partir de $\Gamma \cup \{\varphi\}$ igual a $\delta_2$. Podemos então derivar:

$$\dfrac{\dfrac{\begin{array}{c}\Gamma, [\varphi]^1 \\ \vdots\,\delta_2 \\ \bot\end{array}}{\neg\varphi}\,{}^1\neg\text{Intro} \qquad \begin{array}{c}\Gamma \\ \vdots\,\delta_1 \\ \varphi\end{array}}{\bot}\,\neg\text{Elim}$$

Na nova derivação, a hipótese $\varphi$ é descarregada, de modo que é uma derivação a partir de $\Gamma$. □

**Proposição 20.19.** *$\Gamma \vdash \varphi$ se, e somente se, $\Gamma \cup \{\neg\varphi\}$ é inconsistente.*

*Prova.* Primeiro suponha que $\Gamma \vdash \varphi$, isto é, há uma derivação $\delta_0$ de $\varphi$ a partir de hipóteses não descarregadas $\Gamma$. Obtemos uma derivação de $\bot$ a partir de $\Gamma \cup \{\neg\varphi\}$ da seguinte forma:

$$\dfrac{\neg\varphi \qquad \begin{array}{c}\Gamma\\ \vdots\\ \delta_0\\ \vdots\\ \varphi\end{array}}{\bot}\ \neg\text{Elim}$$

Agora suponha que $\Gamma \cup \{\neg\varphi\}$ é inconsistente, e seja $\delta_1$ a derivação correspondente de $\bot$ a partir de hipóteses não descarregadas em $\Gamma \cup \{\neg\varphi\}$. Obtemos uma derivação de $\varphi$ apenas a partir de $\Gamma$ usando $\bot_C$:

$$\begin{array}{c}\Gamma, [\neg\varphi]^1\\ \vdots\\ \delta_1\\ \vdots\\ \bot\end{array}\ \dfrac{}{\varphi}\ {\scriptstyle 1}\ \bot_C$$

□

**Proposição 20.20.** *Se $\Gamma \vdash \varphi$ e $\neg\varphi \in \Gamma$, então $\Gamma$ é inconsistente.*

*Prova.* Suponha que $\Gamma \vdash \varphi$ e $\neg\varphi \in \Gamma$. Então há uma derivação $\delta$ de $\varphi$ a partir de $\Gamma$. Considere esta aplicação simples da regra ¬Elim:

$$\dfrac{\neg\varphi \qquad \begin{array}{c}\Gamma\\ \vdots\\ \delta\\ \vdots\\ \varphi\end{array}}{\bot}\ \neg\text{Elim}$$

Como $\neg\varphi \in \Gamma$, todas as hipóteses não descarregadas estão em $\Gamma$; isto mostra que $\Gamma \vdash \bot$. □

**Proposição 20.21.** *Se $\Gamma \cup \{\varphi\}$ e $\Gamma \cup \{\neg\varphi\}$ são ambos inconsistentes, então $\Gamma$ é inconsistente.*

*Prova.* Há derivações $\delta_1$ e $\delta_2$ de $\bot$ a partir de $\Gamma \cup \{\varphi\}$ e de $\bot$ a partir de $\Gamma \cup \{\neg\varphi\}$, respectivamente. Podemos então derivar

$$\dfrac{\dfrac{\begin{array}{c}\Gamma, [\neg\varphi]^2\\ \vdots\\ \delta_2\\ \vdots\\ \bot\end{array}}{\neg\neg\varphi}\ {\scriptstyle 2}\ \neg\text{Intro} \qquad \dfrac{\begin{array}{c}\Gamma, [\varphi]^1\\ \vdots\\ \delta_1\\ \vdots\\ \bot\end{array}}{\neg\varphi}\ {\scriptstyle 1}\ \neg\text{Intro}}{\bot}\ \neg\text{Elim}$$

Como as hipóteses $\varphi$ e $\neg\varphi$ são descarregadas, isto é uma derivação de $\bot$ apenas a partir de $\Gamma$. Logo $\Gamma$ é inconsistente. □

## 20.9 Derivabilidade e os Conectivos Proposicionais

Estabelecemos que a relação de derivabilidade $\vdash$ da dedução natural é forte o suficiente para estabelecer alguns fatos básicos envolvendo os conectivos proposicionais, tais como $\varphi \wedge \psi \vdash \varphi$ e $\varphi, \varphi \to \psi \vdash \psi$ (modus ponens). Esses fatos são necessários para a prova do teorema da completude.

**Proposição 20.22.** *1. Tanto $\varphi \wedge \psi \vdash \varphi$ quanto $\varphi \wedge \psi \vdash \psi$.*

*2. $\varphi, \psi \vdash \varphi \wedge \psi$.*

*Prova.* 1. Podemos derivar ambos:

$$\frac{\varphi \wedge \psi}{\varphi}\,\wedge\text{Elim} \qquad \frac{\varphi \wedge \psi}{\psi}\,\wedge\text{Elim}$$

2. Podemos derivar:

$$\frac{\varphi \qquad \psi}{\varphi \wedge \psi}\,\wedge\text{Intro}$$

□

**Proposição 20.23.** *1. $\varphi \vee \psi, \neg\varphi, \neg\psi$ é inconsistente.*

*2. Tanto $\varphi \vdash \varphi \vee \psi$ quanto $\psi \vdash \varphi \vee \psi$.*

*Prova.* 1. Considere a seguinte derivação:

$$\dfrac{\varphi \vee \psi \qquad \dfrac{\neg\varphi \qquad [\varphi]^1}{\bot}\,\neg\text{Elim} \qquad \dfrac{\neg\psi \qquad [\psi]^1}{\bot}\,\neg\text{Elim}}{\bot}\,{}^{1}\vee\text{Elim}$$

Esta é a derivação de $\bot$ a partir das hipóteses não descarregadas $\varphi \vee \psi$, $\neg\varphi$ e $\neg\psi$.

2. Podemos derivar ambos:

$$\frac{\varphi}{\varphi \vee \psi}\,\vee\text{Intro} \qquad \frac{\psi}{\varphi \vee \psi}\,\vee\text{Intro}$$

□

**Proposição 20.24.** *1. $\varphi, \varphi \to \psi \vdash \psi$.*

*2. Tanto $\neg\varphi \vdash \varphi \to \psi$ quanto $\psi \vdash \varphi \to \psi$.*

*Prova.* 1. Podemos derivar:

$$\frac{\varphi \to \psi \qquad \varphi}{\psi}\,\to\text{Elim}$$

2. Isso é mostrado pelas duas derivações seguintes:

$$\dfrac{\dfrac{\dfrac{\neg\varphi \qquad [\varphi]^1}{\bot}\,\neg\text{Elim}}{\psi}\,\bot_I}{\varphi \to \psi}\,{}^{1}\!\to\text{Intro} \qquad\qquad \dfrac{\psi}{\varphi \to \psi}\,\to\text{Intro}$$

Note que $\to$Intro pode, mas não precisa, descarregar a hipótese $\varphi$. □

## 20.10 Derivabilidade e os Quantificadores

O teorema da completude também requer que as regras de dedução natural produzam os fatos sobre $\vdash$ estabelecidos nesta seção.

**Teorema 20.25.** *Se $c$ é uma constante que não ocorre em $\Gamma$ ou $\varphi(x)$ e $\Gamma \vdash \varphi(c)$, então $\Gamma \vdash \forall x\, \varphi(x)$.*

*Prova.* Seja $\delta$ uma derivação de $\varphi(c)$ a partir de $\Gamma$. Adicionando uma inferência $\forall$Intro, obtemos uma derivação de $\forall x\, \varphi(x)$. Como $c$ não ocorre em $\Gamma$ ou $\varphi(x)$, a condição de variável própria é satisfeita. □

**Proposição 20.26.** *1. $\varphi(t) \vdash \exists x\, \varphi(x)$.*

*2. $\forall x\, \varphi(x) \vdash \varphi(t)$.*

*Prova.* 1. A seguinte é uma derivação de $\exists x\, \varphi(x)$ a partir de $\varphi(t)$:

$$\dfrac{\varphi(t)}{\exists x\, \varphi(x)}\,\exists\text{Intro}$$

2. A seguinte é uma derivação de $\varphi(t)$ a partir de $\forall x\, \varphi(x)$:

$$\dfrac{\forall x\, \varphi(x)}{\varphi(t)}\,\forall\text{Elim}$$

□

## 20.11 Correção

Um sistema de derivação, como a dedução natural, é *correto* se não pode derivar coisas que de fato não seguem. A correção é assim uma espécie de propriedade de segurança garantida para sistemas de derivação. Dependendo de qual propriedade da Teoria da Prova está em questão, gostaríamos de saber, por exemplo, que

1. toda sentença derivável é válida;
2. se uma sentença é derivável a partir de outras, ela também é uma consequência delas;
3. se um conjunto de sentenças é inconsistente, ele é insatisfatível.

Estas são propriedades importantes de um sistema de derivação. Se alguma delas não vale, o sistema de derivação é deficiente—ele deriva demais. Consequentemente, estabelecer a correção de um sistema de derivação é da maior importância.

**Teorema 20.27 (Correção).** *Se $\varphi$ é derivável a partir das hipóteses não descarregadas $\Gamma$, então $\Gamma \vDash \varphi$.*

*Prova.* Seja $\delta$ uma derivação de $\varphi$. Procedemos por indução no número de inferências em $\delta$.

Para a base da indução, mostramos a afirmação quando o número de inferências é 0. Neste caso, $\delta$ consiste apenas de uma única sentença $\varphi$, isto é, uma hipótese. Essa hipótese é não descarregada, pois hipóteses só podem ser descarregadas por inferências, e não há inferências. Assim, qualquer estrutura $\mathfrak{M}$ que satisfaz todas as hipóteses não descarregadas da prova também satisfaz $\varphi$.

Agora o passo indutivo. Suponha que $\delta$ contém $n$ inferências. A(s) premissa(s) da inferência mais baixa são derivadas usando sub-derivações, cada uma das quais contém menos de $n$ inferências. Assumimos a hipótese de indução: as premissas da inferência mais baixa seguem das hipóteses não descarregadas das sub-derivações que terminam nessas premissas. Temos que mostrar que a conclusão $\varphi$ segue das hipóteses não descarregadas de toda a prova.

Distinguimos casos de acordo com o tipo da inferência mais baixa. Primeiro, consideramos as possíveis inferências com apenas uma premissa.

1. Suponha que a última inferência é ¬Intro: a derivação tem a forma

$$\dfrac{\begin{array}{c}\Gamma, [\varphi]^n \\ \vdots \\ \delta_1 \\ \vdots \\ \bot\end{array}}{\neg\varphi}\ {}^{n}\neg\text{Intro}$$

   Pela hipótese de indução, $\bot$ segue das hipóteses não descarregadas $\Gamma \cup \{\varphi\}$ de $\delta_1$. Considere a estrutura $\mathfrak{M}$. Precisamos mostrar que, se $\mathfrak{M} \vDash \Gamma$, então $\mathfrak{M} \vDash \neg\varphi$. Suponha por redução ao absurdo que $\mathfrak{M} \vDash \Gamma$, mas $\mathfrak{M} \nvDash \neg\varphi$, isto é, $\mathfrak{M} \vDash \varphi$. Isto significaria que $\mathfrak{M} \vDash \Gamma \cup \{\varphi\}$. Isto é contrário à nossa hipótese de indução. Logo, $\mathfrak{M} \vDash \neg\varphi$.

2. A última inferência é ∧Elim: há duas variantes: $\varphi$ ou $\psi$ pode ser inferido da premissa $\varphi \wedge \psi$. Considere o primeiro caso. A derivação $\delta$ tem este aspecto:

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots\,\delta_1\,\vdots \\ \varphi \wedge \psi\end{array}}{\varphi}\ \wedge\text{Elim}$$

   Pela hipótese de indução, $\varphi \wedge \psi$ segue das hipóteses não descarregadas $\Gamma$ de $\delta_1$. Considere a estrutura $\mathfrak{M}$. Precisamos mostrar que, se $\mathfrak{M} \vDash \Gamma$, então $\mathfrak{M} \vDash \varphi$. Suponha $\mathfrak{M} \vDash \Gamma$. Pela nossa hipótese de indução ($\Gamma \vDash \varphi \wedge \psi$), sabemos que $\mathfrak{M} \vDash \varphi \wedge \psi$. Por definição, $\mathfrak{M} \vDash \varphi \wedge \psi$ se, e somente se, $\mathfrak{M} \vDash \varphi$ e $\mathfrak{M} \vDash \psi$. (O caso em que $\psi$ é inferido de $\varphi \wedge \psi$ é tratado de forma similar.)

3. A última inferência é ∨Intro: há duas variantes: $\varphi \vee \psi$ pode ser inferido da premissa $\varphi$ ou da premissa $\psi$. Considere o primeiro caso. A derivação tem a forma

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots\,\delta_1\,\vdots \\ \varphi\end{array}}{\varphi \vee \psi}\ \vee\text{Intro}$$

   Pela hipótese de indução, $\varphi$ segue das hipóteses não descarregadas $\Gamma$ de $\delta_1$. Considere a estrutura $\mathfrak{M}$. Precisamos mostrar que, se $\mathfrak{M} \vDash \Gamma$, então $\mathfrak{M} \vDash \varphi \vee \psi$. Suponha $\mathfrak{M} \vDash \Gamma$; então $\mathfrak{M} \vDash \varphi$, pois $\Gamma \vDash \varphi$ (a hipótese de indução). Logo também deve ser o caso que $\mathfrak{M} \vDash \varphi \vee \psi$. (O caso em que $\varphi \vee \psi$ é inferido de $\psi$ é tratado de forma similar.)

4. A última inferência é →Intro: $\varphi \to \psi$ é inferido de uma subprova com hipótese $\varphi$ e conclusão $\psi$, isto é,

$$\dfrac{\begin{array}{c}\Gamma, [\varphi]^n \\ \vdots\,\delta_1\,\vdots \\ \psi\end{array}}{\varphi \to \psi}\ {}^{n}\ \to\text{Intro}$$

   Pela hipótese de indução, $\psi$ segue das hipóteses não descarregadas de $\delta_1$, isto é, $\Gamma \cup \{\varphi\} \vDash \psi$. Considere a estrutura $\mathfrak{M}$. As hipóteses não descarregadas de $\delta$ são apenas $\Gamma$, pois $\varphi$ é descartada na última inferência.

Precisamos mostrar que $\Gamma \vDash \varphi \to \psi$. Por redução ao absurdo, suponha que para alguma estrutura $\mathfrak{M}$, $\mathfrak{M} \vDash \Gamma$ mas $\mathfrak{M} \nvDash \varphi \to \psi$. Assim, $\mathfrak{M} \vDash \varphi$ e $\mathfrak{M} \nvDash \psi$. Mas por hipótese, $\psi$ é uma consequência de $\Gamma \cup \{\varphi\}$, isto é, $\mathfrak{M} \vDash \psi$, o que é uma contradição. Logo, $\Gamma \vDash \varphi \to \psi$.

5. A última inferência é $\bot_I$: aqui, $\delta$ termina em

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots\,\delta_1 \\ \vdots \\ \bot\end{array}}{\varphi}\,\bot_I$$

Pela hipótese de indução, $\Gamma \vDash \bot$. Temos que mostrar que $\Gamma \vDash \varphi$. Suponha o contrário; então para algum $\mathfrak{M}$ temos $\mathfrak{M} \vDash \Gamma$ e $\mathfrak{M} \nvDash \varphi$. Mas sempre temos $\mathfrak{M} \nvDash \bot$, de modo que isto significaria que $\Gamma \nvDash \bot$, contrariando a hipótese de indução.

6. A última inferência é $\bot_C$: Exercício.

7. A última inferência é ∀Intro: então $\delta$ tem a forma

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots\,\delta_1 \\ \vdots \\ \varphi(a)\end{array}}{\forall x\, \varphi(x)}\,\forall\text{Intro}$$

A premissa $\varphi(a)$ é consequência das hipóteses não descarregadas $\Gamma$ pela hipótese de indução. Considere alguma estrutura $\mathfrak{M}$ tal que $\mathfrak{M} \vDash \Gamma$. Precisamos mostrar que $\mathfrak{M} \vDash \forall x\, \varphi(x)$. Como $\forall x\, \varphi(x)$ é a sentença, isto significa que temos que mostrar que para toda atribuição de variáveis $s$, $\mathfrak{M}, s \vDash \varphi(x)$ (Proposição 16.19). Como $\Gamma$ consiste inteiramente em sentenças, $\mathfrak{M}, s \vDash \psi$ para todo $\psi \in \Gamma$ por Definição 16.11. Seja $\mathfrak{M}'$ como $\mathfrak{M}$, exceto que $a^{\mathfrak{M}'} = s(x)$. Como $a$ não ocorre em $\Gamma$, $\mathfrak{M}' \vDash \Gamma$ por Corolário 16.21. Como $\Gamma \vDash \varphi(a)$, $\mathfrak{M}' \vDash \varphi(a)$. Como $\varphi(a)$ é a sentença, $\mathfrak{M}', s \vDash \varphi(a)$ por Proposição 16.18. $\mathfrak{M}', s \vDash \varphi(x)$ se, e somente se, $\mathfrak{M}' \vDash \varphi(a)$ por Proposição 16.23 (lembre que $\varphi(a)$ é apenas $\varphi(x)[a/x]$). Assim, $\mathfrak{M}', s \vDash \varphi(x)$. Como $a$ não ocorre em $\varphi(x)$, por Proposição 16.20, $\mathfrak{M}, s \vDash \varphi(x)$. Mas $s$ foi uma atribuição de variáveis arbitrária, de modo que $\mathfrak{M} \vDash \forall x\, \varphi(x)$.

8. A última inferência é ∃Intro: Exercício.

9. A última inferência é ∀Elim: Exercício.

Agora consideremos as possíveis inferências com várias premissas: $\vee$Elim, $\wedge$Intro, $\rightarrow$Elim, e $\exists$Elim.

1. A última inferência é $\wedge$Intro. $\varphi \wedge \psi$ é inferido das premissas $\varphi$ e $\psi$ e $\delta$ tem a forma

$$\dfrac{\begin{array}{cc}\Gamma_1 & \Gamma_2 \\ \vdots & \vdots \\ \vdots\,\delta_1 & \vdots\,\delta_2 \\ \vdots & \vdots \\ \varphi & \psi\end{array}}{\varphi \wedge \psi}\ \wedge\text{Intro}$$

   Pela hipótese de indução, $\varphi$ segue das hipóteses não descarregadas $\Gamma_1$ de $\delta_1$ e $\psi$ segue das hipóteses não descarregadas $\Gamma_2$ de $\delta_2$. As hipóteses não descarregadas de $\delta$ são $\Gamma_1 \cup \Gamma_2$, de modo que temos que mostrar que $\Gamma_1 \cup \Gamma_2 \vDash \varphi \wedge \psi$. Considere a estrutura $\mathfrak{M}$ com $\mathfrak{M} \vDash \Gamma_1 \cup \Gamma_2$. Como $\mathfrak{M} \vDash \Gamma_1$, deve ser o caso que $\mathfrak{M} \vDash \varphi$, pois $\Gamma_1 \vDash \varphi$, e como $\mathfrak{M} \vDash \Gamma_2$, $\mathfrak{M} \vDash \psi$, pois $\Gamma_2 \vDash \psi$. Juntas, $\mathfrak{M} \vDash \varphi \wedge \psi$.

2. A última inferência é $\vee$Elim: Exercício.

3. A última inferência é $\rightarrow$Elim. $\psi$ é inferido das premissas $\varphi \rightarrow \psi$ e $\varphi$. A derivação $\delta$ tem este aspecto:

$$\dfrac{\begin{array}{cc}\Gamma_1 & \Gamma_2 \\ \vdots & \vdots \\ \vdots\,\delta_1 & \vdots\,\delta_2 \\ \vdots & \vdots \\ \varphi \rightarrow \psi & \varphi\end{array}}{\psi}\ \rightarrow\text{Elim}$$

   Pela hipótese de indução, $\varphi \rightarrow \psi$ segue das hipóteses não descarregadas $\Gamma_1$ de $\delta_1$ e $\varphi$ segue das hipóteses não descarregadas $\Gamma_2$ de $\delta_2$. Considere a estrutura $\mathfrak{M}$. Precisamos mostrar que, se $\mathfrak{M} \vDash \Gamma_1 \cup \Gamma_2$, então $\mathfrak{M} \vDash \psi$. Suponha $\mathfrak{M} \vDash \Gamma_1 \cup \Gamma_2$. Como $\Gamma_1 \vDash \varphi \rightarrow \psi$, $\mathfrak{M} \vDash \varphi \rightarrow \psi$. Como $\Gamma_2 \vDash \varphi$, temos $\mathfrak{M} \vDash \varphi$. Isto significa que $\mathfrak{M} \vDash \psi$ (pois se $\mathfrak{M} \nvDash \psi$, como $\mathfrak{M} \vDash \varphi$, teríamos $\mathfrak{M} \nvDash \varphi \rightarrow \psi$, contradizendo $\mathfrak{M} \vDash \varphi \rightarrow \psi$).

4. A última inferência é $\neg$Elim: Exercício.

5. A última inferência é $\exists$Elim: Exercício. □

**Corolário 20.28.** *Se $\vdash \varphi$, então $\varphi$ é válida.*

**Corolário 20.29.** *Se $\Gamma$ é satisfatível, então é consistente.*

*Prova.* Provamos a contrapositiva. Suponha que $\Gamma$ não é consistente. Então $\Gamma \vdash \bot$, isto é, há uma derivação de $\bot$ a partir de hipóteses não descarregadas em $\Gamma$. Por Teorema 20.27, qualquer estrutura $\mathfrak{M}$ que satisfaz $\Gamma$ deve satisfazer $\bot$. Como $\mathfrak{M} \nvDash \bot$ para toda estrutura $\mathfrak{M}$, nenhuma $\mathfrak{M}$ pode satisfazer $\Gamma$, isto é, $\Gamma$ não é satisfatível. □

## 20.12 Derivações com Predicado de identidade

As Derivações com predicado de identidade requerem regras de inferência adicionais.

$$\frac{}{t = t}\ =\text{Intro} \qquad \frac{t_1 = t_2 \qquad \varphi(t_1)}{\varphi(t_2)}\ =\text{Elim} \qquad \frac{t_1 = t_2 \qquad \varphi(t_2)}{\varphi(t_1)}\ =\text{Elim}$$

Nas regras acima, $t$, $t_1$ e $t_2$ são termos fechados. A regra =Intro nos permite derivar qualquer afirmação de identidade da forma $t = t$ diretamente, sem hipóteses.

**Exemplo 20.30.** Se $s$ e $t$ são termos fechados, então $\varphi(s), s = t \vdash \varphi(t)$:

$$\frac{s = t \qquad \varphi(s)}{\varphi(t)}\ =\text{Elim}$$

Isto pode ser familiar como o "princípio da substituibilidade dos identicos", ou Lei de Leibniz.

**Exemplo 20.31.** Derivamos a sentença

$$\forall x\, \forall y\, ((\varphi(x) \wedge \varphi(y)) \to x = y)$$

a partir da sentença

$$\exists x\, \forall y\, (\varphi(y) \to y = x)$$

Desenvolvemos a derivação de trás para frente:

$$\dfrac{\dfrac{\dfrac{\exists x\, \forall y\, (\varphi(y) \to y = x) \quad [\varphi(a) \wedge \varphi(b)]^1}{\vdots}}{\dfrac{a = b}{((\varphi(a) \wedge \varphi(b)) \to a = b)}\ {}^1\to\text{Intro}}\ \forall\text{Intro}}{\forall y\, ((\varphi(a) \wedge \varphi(y)) \to a = y)}\ \forall\text{Intro}$$
$$\forall x\, \forall y\, ((\varphi(x) \wedge \varphi(y)) \to x = y)$$

Agora teremos que usar a hipótese principal: como é uma fórmula existencial, usamos ∃Elim para derivar a conclusão intermediária $a = b$.

$$\dfrac{\exists x\, \forall y\, (\varphi(y) \to y = x) \qquad \begin{array}{c}[\forall y\, (\varphi(y) \to y = c)]^2 \\ [\varphi(a) \wedge \varphi(b)]^1 \\ \vdots \\ a = b\end{array}}{\dfrac{\dfrac{\dfrac{a = b}{((\varphi(a) \wedge \varphi(b)) \to a = b)}\,{\scriptstyle 1}\,\to\text{Intro}}{\forall y\, ((\varphi(a) \wedge \varphi(y)) \to a = y)}\,\forall\text{Intro}}{\forall x\, \forall y\, ((\varphi(x) \wedge \varphi(y)) \to x = y)}\,\forall\text{Intro}}\,{\scriptstyle 2}\,\exists\text{Elim}$$

A sub-derivação no canto superior direito é completada usando suas hipóteses para mostrar que $a = c$ e $b = c$. Isso requer duas derivações separadas. A derivação para $a = c$ é a seguinte:

$$\dfrac{\dfrac{[\forall y\, (\varphi(y) \to y = c)]^2}{\varphi(a) \to a = c}\,\forall\text{Elim} \qquad \dfrac{[\varphi(a) \wedge \varphi(b)]^1}{\varphi(a)}\,\wedge\text{Elim}}{a = c}\,\to\text{Elim}$$

De $a = c$ e $b = c$ derivamos $a = b$ por $=$Elim.

## 20.13 Correção com Predicado de identidade

**Proposição 20.32.** *A dedução natural com regras para $=$ é correta.*

*Prova.* Qualquer fórmula da forma $t = t$ é válida, pois para toda estrutura $\mathfrak{M}$, $\mathfrak{M} \vDash t = t$. (Note que assumimos que o termo $t$ é fechado, isto é, não contém variáveis, de modo que as atribuições de variáveis são irrelevantes).

Suponha que a última inferência em uma derivação é $=$Elim, isto é, a derivação tem a seguinte forma:

$$\dfrac{\begin{array}{c}\Gamma_1 \\ \vdots\,\delta_1 \\ t_1 = t_2\end{array} \qquad \begin{array}{c}\Gamma_2 \\ \vdots\,\delta_2 \\ \varphi(t_1)\end{array}}{\varphi(t_2)}\,=\text{Elim}$$

As premissas $t_1 = t_2$ e $\varphi(t_1)$ são derivadas a partir de hipóteses não descarregadas $\Gamma_1$ e $\Gamma_2$, respectivamente. Queremos mostrar que $\varphi(t_2)$ segue de $\Gamma_1 \cup \Gamma_2$. Considere uma estrutura $\mathfrak{M}$ com $\mathfrak{M} \vDash \Gamma_1 \cup \Gamma_2$. Pela hipótese de indução, $\mathfrak{M} \vDash \varphi(t_1)$ e $\mathfrak{M} \vDash t_1 = t_2$. Portanto, $\mathrm{Val}^{\mathfrak{M}}(t_1) = \mathrm{Val}^{\mathfrak{M}}(t_2)$. Seja $s$ qualquer atribuição de variáveis e $m = \mathrm{Val}^{\mathfrak{M}}(t_1) = \mathrm{Val}^{\mathfrak{M}}(t_2)$. Por Proposição 16.23,

$\mathfrak{M}, s \vDash \varphi(t_1)$ se, e somente se, $\mathfrak{M}, s[m/x] \vDash \varphi(x)$ se, e somente se, $\mathfrak{M}, s \vDash \varphi(t_2)$. Como $\mathfrak{M} \vDash \varphi(t_1)$, temos $\mathfrak{M} \vDash \varphi(t_2)$. □

## Problemas

**Problema 20.1.** Dê derivações que mostrem o seguinte:

1. $\varphi \wedge (\psi \wedge \chi) \vdash (\varphi \wedge \psi) \wedge \chi$.
2. $\varphi \vee (\psi \vee \chi) \vdash (\varphi \vee \psi) \vee \chi$.
3. $\varphi \to (\psi \to \chi) \vdash \psi \to (\varphi \to \chi)$.
4. $\varphi \vdash \neg\neg\varphi$.

**Problema 20.2.** Dê derivações que mostrem o seguinte:

1. $(\varphi \vee \psi) \to \chi \vdash \varphi \to \chi$.
2. $(\varphi \to \chi) \wedge (\psi \to \chi) \vdash (\varphi \vee \psi) \to \chi$.
3. $\vdash \neg(\varphi \wedge \neg\varphi)$.
4. $\psi \to \varphi \vdash \neg\varphi \to \neg\psi$.
5. $\vdash (\varphi \to \neg\varphi) \to \neg\varphi$.
6. $\vdash \neg(\varphi \to \psi) \to \neg\psi$.
7. $\varphi \to \chi \vdash \neg(\varphi \wedge \neg\chi)$.
8. $\varphi \wedge \neg\chi \vdash \neg(\varphi \to \chi)$.
9. $\varphi \vee \psi, \neg\psi \vdash \varphi$.
10. $\neg\varphi \vee \neg\psi \vdash \neg(\varphi \wedge \psi)$.
11. $\vdash (\neg\varphi \wedge \neg\psi) \to \neg(\varphi \vee \psi)$.
12. $\vdash \neg(\varphi \vee \psi) \to (\neg\varphi \wedge \neg\psi)$.

**Problema 20.3.** Dê derivações que mostrem o seguinte:

1. $\neg(\varphi \to \psi) \vdash \varphi$.
2. $\neg(\varphi \wedge \psi) \vdash \neg\varphi \vee \neg\psi$.
3. $\varphi \to \psi \vdash \neg\varphi \vee \psi$.
4. $\vdash \neg\neg\varphi \to \varphi$.
5. $\varphi \to \psi, \neg\varphi \to \psi \vdash \psi$.

6. $(\varphi \wedge \psi) \to \chi \vdash (\varphi \to \chi) \vee (\psi \to \chi)$.
7. $(\varphi \to \psi) \to \varphi \vdash \varphi$.
8. $\vdash (\varphi \to \psi) \vee (\psi \to \chi)$.

(Todos exigem a regra $\bot_C$ .)

**Problema 20.4.** Dê derivações que mostrem o seguinte:

1. $\vdash (\forall x\, \varphi(x) \wedge \forall y\, \psi(y)) \to \forall z\, (\varphi(z) \wedge \psi(z))$.
2. $\vdash (\exists x\, \varphi(x) \vee \exists y\, \psi(y)) \to \exists z\, (\varphi(z) \vee \psi(z))$.
3. $\forall x\, (\varphi(x) \to \psi) \vdash \exists y\, \varphi(y) \to \psi$.
4. $\forall x\, \neg\varphi(x) \vdash \neg\exists x\, \varphi(x)$.
5. $\vdash \neg\exists x\, \varphi(x) \to \forall x\, \neg\varphi(x)$.
6. $\vdash \neg\exists x\, \forall y\, ((\varphi(x,y) \to \neg\varphi(y,y)) \wedge (\neg\varphi(y,y) \to \varphi(x,y)))$.

**Problema 20.5.** Dê derivações que mostrem o seguinte:

1. $\vdash \neg\forall x\, \varphi(x) \to \exists x\, \neg\varphi(x)$.
2. $(\forall x\, \varphi(x) \to \psi) \vdash \exists y\, (\varphi(y) \to \psi)$.
3. $\vdash \exists x\, (\varphi(x) \to \forall y\, \varphi(y))$.

(Todas exigem a regra $\bot_C$ .)

**Problema 20.6.** Prove Proposição 20.16

**Problema 20.7.** Prove que $\Gamma \vdash \neg\varphi$ se, e somente se, $\Gamma \cup \{\varphi\}$ é inconsistente.

**Problema 20.8.** Complete a prova de Teorema 20.27.

**Problema 20.9.** Prove que $=$ é simétrica e transitiva, isto é, dê derivações de $\forall x\, \forall y\, (x = y \to y = x)$ e $\forall x\, \forall y\, \forall z((x = y \wedge y = z) \to x = z)$

**Problema 20.10.** Dê derivações das seguintes fórmulas:

1. $\forall x\, \forall y\, ((x = y \wedge \varphi(x)) \to \varphi(y))$
2. $\exists x\, \varphi(x) \wedge \forall y\, \forall z\, ((\varphi(y) \wedge \varphi(z)) \to y = z) \to \exists x\, (\varphi(x) \wedge \forall y\, (\varphi(y) \to y = x))$

# Capítulo 21

# Tableaux

This chapter presents a signed analytic tableaux system.
To include or exclude material relevant to natural deduction as a proof system, use the “prfTab” tag.

# Capítulo 22

# Axiomatic Derivações

No effort has been made yet to ensure that the material in this chapter respects various tags indicating which connectives and quantifiers are primitive or defined: all are assumed to be primitive, except $\leftrightarrow$ which is assumed to be defined. If the FOL tag is true, we produce a version with quantifiers, otherwise without.

# Capítulo 23

# O Teorema da Completude

## 23.1 Introdução

O teorema da completude é um dos resultados mais fundamentais sobre lógica. Ele vem em duas formulações, cuja equivalência iremos provar. Em sua primeira formulação, ele diz algo fundamental sobre a relação entre consequência semântica e nosso sistema de derivação: se a sentença $\varphi$ segue de algumas sentenças $\Gamma$, então também existe a derivação que estabelece $\Gamma \vdash \varphi$. Assim, o sistema de derivação é tão forte quanto pode possivelmente ser sem provar coisas que de fato não se seguem.

Em sua segunda formulação, ele pode ser enunciado como um resultado de existência de modelo: todo conjunto consistente de sentenças é satisfatível. A consistência é uma noção da teoria da prova: ela diz que nosso sistema de derivação é incapaz de produzir certas derivações. Mas quem garante que, só porque não há derivações de um certo tipo a partir de $\Gamma$, está garantido que existe a estrutura $\mathfrak{M}$? Antes de o teorema da completude ser provado pela primeira vez — na verdade, antes de termos os sistemas de derivação que temos hoje — o grande matemático alemão David Hilbert defendia a visão de que a consistência das teorias matemáticas garante a existência dos objetos de que elas tratam. Ele colocou isso da seguinte forma em uma carta a Gottlob Frege:

> Se os axiomas dados arbitrariamente não se contradizem uns aos outros com todas as suas consequências, então eles são verdadeiros e as coisas definidas pelos axiomas existem. Este é para mim o critério de verdade e existência.

Frege discordou veementemente. A segunda formulação do teorema da completude mostra que Hilbert estava certo pelo menos no sentido de que, se os axiomas são consistentes, então existe *alguma* estrutura que os torna todos verdadeiros.

Estas não são as únicas razões pelas quais o teorema da completude — ou melhor, sua prova — é importante. Ele tem uma série de consequências importantes, algumas das quais discutiremos separadamente. Por exemplo, como toda derivação que mostra $\Gamma \vdash \varphi$ é finita e, portanto, só pode usar uma quantidade finita das sentenças em $\Gamma$, segue do teorema da completude que, se $\varphi$ é uma consequência de $\Gamma$, então já é uma consequência de um subconjunto finito de $\Gamma$. Isso é chamado de *compacidade*. Equivalentemente, se todo subconjunto finito de $\Gamma$ é consistente, então o próprio $\Gamma$ deve ser consistente.

Embora o teorema da compacidade decorra do teorema da completude pelo desvio através de derivações, também é possível usar a *prova do* teorema da completude para estabelecê-lo diretamente. Pois o que a prova faz é tomar um conjunto de sentenças com uma certa propriedade — a consistência — e construir a estrutura a partir desse conjunto que possui certas propriedades (neste caso, que ela satisfaz o conjunto). Quase exatamente a mesma construção pode ser usada para estabelecer a compacidade diretamente, partindo de conjuntos "finitamente satisfatíveis" de sentenças em vez de conjuntos consistentes. A construção também produz outras consequências, por exemplo, que todo conjunto satisfatível de sentenças tem um modelo finito ou infinitos enumeráveis. (Esse resultado é chamado de teorema de Löwenheim–Skolem.) Em geral, a construção de estruturas a partir de conjuntos de sentenças é usada com frequência em lógica, e às vezes até em filosofia.

## 23.2 Esboço da Prova

A prova do teorema da completude é um pouco complexa e, em uma primeira leitura, é fácil se perder. Então, vamos esboçar a prova. O primeiro passo é uma mudança de perspectiva, que nos permite enxergar um caminho para uma prova. Quando a completude é pensada como "sempre que $\Gamma \vDash \varphi$ então $\Gamma \vdash \varphi$", pode ser difícil até mesmo ter uma ideia: pois, para mostrar que $\Gamma \vdash \varphi$, temos que encontrar a derivação, e não parece que a hipótese de que $\Gamma \vDash \varphi$ nos ajude nisso de alguma forma. Para alguns sistemas de prova, é possível construir diretamente a derivação, mas adotaremos uma abordagem um pouco diferente. A mudança de perspectiva necessária é esta: a completude também pode ser formulada como: "se $\Gamma$ é consistente, então é satisfatível". Talvez possamos usar a informação em $\Gamma$ juntamente com a hipótese de que ela é consistente para construir a estrutura que satisfaça toda sentença em $\Gamma$. Afinal, sabemos que tipo de estrutura estamos procurando: uma que seja como $\Gamma$ a descreve!

Se $\Gamma$ contém apenas sentenças atômicas, é fácil construir um modelo para ele. Suponha que as sentenças atômicas sejam todas da forma $P(a_1, \ldots, a_n)$ onde os $a_i$ são símbolos de constante. Tudo o que temos a fazer é apresentar a domínio $|\mathfrak{M}|$ e uma atribuição para $P$ de modo que $\mathfrak{M} \vDash P(a_1, \ldots, a_n)$. Mas isso não é muito difícil: faça $|\mathfrak{M}| = \mathbb{N}$, $c_i^{\mathfrak{M}} = i$ e, para cada $P(a_1, \ldots, a_n) \in \Gamma$,

coloque a tupla $\langle k_1, \ldots, k_n \rangle$ em $P^{\mathfrak{M}}$, onde $k_i$ é o índice do símbolo de constante $a_i$ (isto é, $a_i \equiv c_{k_i}$).

Agora suponha que $\Gamma$ contenha alguma fórmula $\neg\psi$, com $\psi$ atômica. Poderíamos temer que a construção de $\mathfrak{M}$ interfira na possibilidade de tornar $\neg\psi$ verdadeira. Mas é aqui que entra a consistência de $\Gamma$: se $\neg\psi \in \Gamma$, então $\psi \notin \Gamma$, caso contrário $\Gamma$ seria inconsistente. E se $\psi \notin \Gamma$, então, de acordo com nossa construção de $\mathfrak{M}$, $\mathfrak{M} \not\models \psi$, logo $\mathfrak{M} \models \neg\psi$. Até aqui, tudo bem.

E se $\Gamma$ contiver fórmulas complexas, não atômicas? Digamos que ele contenha $\varphi \wedge \psi$. Para tornar isso verdadeiro, devemos proceder como se tanto $\varphi$ quanto $\psi$ estivessem em $\Gamma$. E se $\varphi \vee \psi \in \Gamma$, então teremos que tornar pelo menos um deles verdadeiro, isto é, proceder como se um deles estivesse em $\Gamma$.

Isso sugere a seguinte ideia: adicionamos fórmulas adicionais a $\Gamma$ de modo a (a) manter o conjunto resultante consistente e (b) garantir que, para toda sentença $\varphi$ atômica possível, ou $\varphi$ está no conjunto resultante, ou $\neg\varphi$ está, e (c) tais que, sempre que $\varphi \wedge \psi$ está no conjunto, então tanto $\varphi$ quanto $\psi$ também estão; se $\varphi \vee \psi$ está no conjunto, pelo menos um dentre $\varphi$ ou $\psi$ também está, etc. Continuamos fazendo isso (potencialmente para sempre). Chame o conjunto de todas as fórmulas assim adicionadas de $\Gamma^*$. Então a nossa construção acima nos forneceria a estrutura $\mathfrak{M}$ para a qual poderíamos provar, por indução, que ela satisfaz todas as sentenças em $\Gamma^*$ e, portanto, também todas as sentenças em $\Gamma$, já que $\Gamma \subseteq \Gamma^*$. Acontece que garantir (a) e (b) é suficiente. Um conjunto de sentenças para o qual (b) vale é chamado de *completo*. Assim, nossa tarefa será estender o conjunto consistente $\Gamma$ a um conjunto consistente e completo $\Gamma^*$.

Há um problema neste plano: se $\exists x\, \varphi(x) \in \Gamma$, esperaríamos poder escolher algum símbolo de constante $c$ e adicionar $\varphi(c)$ neste processo. Mas como sabemos que sempre podemos fazer isso? Talvez tenhamos apenas alguns símbolos de constante em nossa linguagem, e, para cada um deles, tenhamos $\neg\varphi(c) \in \Gamma$. Também não podemos adicionar $\varphi(c)$, já que isso tornaria o conjunto inconsistente, e não saberíamos se $\mathfrak{M}$ tem que tornar $\varphi(c)$ ou $\neg\varphi(c)$ verdadeira. Além disso, pode acontecer de $\Gamma$ conter apenas sentenças em uma linguagem que não tem símbolo de constante algum (por exemplo, a linguagem da teoria dos conjuntos).

A solução para este problema é simplesmente adicionar infinitas constantes no começo, além de sentenças que as conectam com os quantificadores da maneira correta. (Claro, temos que verificar que isso não pode introduzir uma inconsistência.)

Nossa construção original funciona bem se tivermos apenas símbolos de constante nas sentenças atômicas. Mas a linguagem também pode conter símbolos de função. Nesse caso, pode ser complicado encontrar as funções certas em $\mathbb{N}$ para atribuir a esses símbolos de função de modo a fazer tudo funcionar. Então, aqui vai outro truque: em vez de usar $i$ para interpretar $c_i$, basta tomar o próprio conjunto de símbolos de constante como o domínio.

Então $\mathfrak{M}$ pode atribuir cada símbolo de constante a si mesmo: $c_i^{\mathfrak{M}} = c_i$. Mas por que não ir até o fim: seja $|\mathfrak{M}|$ o conjunto de todos os *termos* da linguagem! Se fizermos isso, há uma atribuição óbvia de funções (que tomam termos como argumentos e têm termos como valores) aos símbolos de função: atribuímos ao símbolo de função $f_i^n$ a função que, dados $n$ termos $t_1, \ldots, t_n$ como entrada, produz o termo $f_i^n(t_1, \ldots, t_n)$ como valor.

A última peça do quebra-cabeça é o que fazer com $=$. O símbolo de predicado $=$ tem uma interpretação fixa: $\mathfrak{M} \vDash t = t'$ se e somente se $\mathrm{Val}^{\mathfrak{M}}(t) = \mathrm{Val}^{\mathfrak{M}}(t')$. Agora, se ajustarmos as coisas de modo que o valor de um termo $t$ seja o próprio $t$, então esta estrutura não tornará verdadeira *nenhuma* sentença da forma $t = t'$ a menos que $t$ e $t'$ sejam um único e mesmo termo. E, claro, isso é um problema, já que basicamente toda teoria interessante em uma linguagem com símbolos de função terá como teoremas sentenças $t = t'$ onde $t$ e $t'$ não são o mesmo termo (por exemplo, em teorias da aritmética: $(\mathsf{o} + \mathsf{o}) = \mathsf{o}$). Para resolver este problema, mudamos o domínio de $\mathfrak{M}$: em vez de usar termos como os objetos em $|\mathfrak{M}|$, usamos conjuntos de termos, e cada conjunto é tal que contém todos aqueles termos que as sentenças em $\Gamma$ exigem que sejam iguais. Assim, por exemplo, se $\Gamma$ é uma teoria da aritmética, um desses conjuntos conterá: $\mathsf{o}$, $(\mathsf{o} + \mathsf{o})$, $(\mathsf{o} \times \mathsf{o})$, etc. Este será o conjunto que atribuímos a $\mathsf{o}$, e acontecerá que este conjunto também é o valor de todos os termos nele, por exemplo, também de $(\mathsf{o} + \mathsf{o})$. Portanto, a sentença $(\mathsf{o} + \mathsf{o}) = \mathsf{o}$ será verdadeira nesta estrutura revisada.

Então, aqui está o que faremos. Primeiro investigamos as propriedades dos conjuntos consistentes completos; em particular, provamos que um conjunto consistente completo contém $\varphi \wedge \psi$ se e somente se contém tanto $\varphi$ quanto $\psi$, contém $\varphi \vee \psi$ se e somente se contém pelo menos um deles, etc. (Proposição 23.2). Em seguida, definimos e investigamos conjuntos "saturados" de sentenças. Um conjunto saturado é aquele que contém condicionais que ligam cada sentença quantificada às suas instâncias (Definição 23.5). Mostramos que qualquer conjunto consistente $\Gamma$ sempre pode ser estendido a um conjunto saturado $\Gamma'$ (Lema 23.6). Se um conjunto é consistente, saturado e completo, ele também tem a propriedade de conter $\exists x\, \varphi(x)$ se e somente se contém $\varphi(t)$ para algum termo fechado $t$ e $\forall x\, \varphi(x)$ se e somente se contém $\varphi(t)$ para todo termo fechado $t$ (Proposição 23.7). Em seguida, tomaremos o conjunto consistente saturado $\Gamma'$ e mostraremos que ele pode ser estendido a um conjunto saturado, consistente e completo $\Gamma^*$ (Lema 23.8). Este conjunto $\Gamma^*$ é o que usaremos para definir nosso modelo de termos $\mathfrak{M}(\Gamma^*)$. O modelo de termos tem o conjunto de termos fechados como seu domínio, e a interpretação de seus símbolos de predicado é dada pelas sentenças atômicas em $\Gamma^*$ (Definição 23.9). Usaremos as propriedades dos conjuntos consistentes completos e saturados para mostrar que, de fato, $\mathfrak{M}(\Gamma^*) \vDash \varphi$ se e somente se $\varphi \in \Gamma^*$ (Lema 23.12) e, portanto, em particular, $\mathfrak{M}(\Gamma^*) \vDash \Gamma$. Por fim, consideraremos como definir um modelo de termos se $\Gamma$ contém $=$ também

(Definição 23.16) e mostraremos que ele satisfaz $\Gamma^*$ (Lema 23.19).

## 23.3 Conjuntos Consistentes Completos de Sentenças

**Definição 23.1 (Conjunto completo).** Um conjunto $\Gamma$ de sentenças é *completo* se e somente se, para qualquer sentença $\varphi$, ou $\varphi \in \Gamma$ ou $\neg\varphi \in \Gamma$.

Conjuntos completos de sentenças não deixam questões sem resposta. Para qualquer sentença $\varphi$, $\Gamma$ "diz" se $\varphi$ é verdadeira ou falsa. A importância dos conjuntos completos estende-se para além da prova do teorema da completude. Uma teoria que é completa e axiomatizável, por exemplo, é sempre decidível.

Conjuntos consistentes completos são importantes na prova de completude já que podemos garantir que todo conjunto consistente de sentenças $\Gamma$ está contido em um conjunto consistente completo $\Gamma^*$. Um conjunto consistente completo contém, para cada sentença $\varphi$, ou $\varphi$ ou sua negação $\neg\varphi$, mas não ambas. Isso é verdade em particular para sentenças atômicas, de modo que, a partir de um conjunto consistente completo em uma linguagem adequadamente expandida por símbolos de constante, podemos construir a estrutura onde a interpretação dos símbolos de predicado é definida de acordo com quais sentenças atômicas estão em $\Gamma^*$. Pode-se então mostrar que esta estrutura torna verdadeiras todas as sentenças em $\Gamma^*$ (e, portanto, também todas aquelas em $\Gamma$). A prova deste último fato requer que $\neg\varphi \in \Gamma^*$ se e somente se $\varphi \notin \Gamma^*$, $(\varphi \vee \psi) \in \Gamma^*$ se e somente se $\varphi \in \Gamma^*$ ou $\psi \in \Gamma^*$, etc.

No que se segue, usaremos com frequência, de modo tácito, as propriedades de reflexividade, monotonicidade e transitividade de $\vdash$ (ver Seções 19.8 e 20.7 e **????**).

**Proposição 23.2.** *Suponha que $\Gamma$ seja completo e consistente. Então:*

1. *Se $\Gamma \vdash \varphi$, então $\varphi \in \Gamma$.*
2. *$\varphi \wedge \psi \in \Gamma$ se e somente se $\varphi \in \Gamma$ e $\psi \in \Gamma$.*
3. *$\varphi \vee \psi \in \Gamma$ se e somente se $\varphi \in \Gamma$ ou $\psi \in \Gamma$.*
4. *$\varphi \to \psi \in \Gamma$ se e somente se $\varphi \notin \Gamma$ ou $\psi \in \Gamma$.*

*Prova.* Suponhamos, para tudo o que se segue, que $\Gamma$ seja completo e consistente.

1. Se $\Gamma \vdash \varphi$, então $\varphi \in \Gamma$.

   Suponha que $\Gamma \vdash \varphi$. Suponha, ao contrário, que $\varphi \notin \Gamma$. Como $\Gamma$ é completo, $\neg\varphi \in \Gamma$. Por Proposições 19.20 e 20.20 e **????**, $\Gamma$ é inconsistente. Isso contradiz a suposição de que $\Gamma$ é consistente. Logo, não pode ser o caso que $\varphi \notin \Gamma$, de modo que $\varphi \in \Gamma$.

2. Exercício.

3. Primeiro mostramos que, se $\varphi \vee \psi \in \Gamma$, então $\varphi \in \Gamma$ ou $\psi \in \Gamma$. Suponha $\varphi \vee \psi \in \Gamma$ mas $\varphi \notin \Gamma$ e $\psi \notin \Gamma$. Como $\Gamma$ é completo, $\neg\varphi \in \Gamma$ e $\neg\psi \in \Gamma$. Por Proposições 19.23 e 20.23 e **????**, item (1), $\Gamma$ é inconsistente, uma contradição. Logo, $\varphi \in \Gamma$ ou $\psi \in \Gamma$.

   Para a direção reversa, suponha que $\varphi \in \Gamma$ ou $\psi \in \Gamma$. Por Proposições 19.23 e 20.23 e **????**, item (2), $\Gamma \vdash \varphi \vee \psi$. Por (1), $\varphi \vee \psi \in \Gamma$, como requerido.

4. Exercício. □

## 23.4 Expansão de Henkin

Parte do desafio em provar o teorema da completude é que o modelo que construímos a partir de um conjunto consistente completo $\Gamma$ deve tornar verdadeiras todas as fórmulas quantificadas em $\Gamma$. Para garantir isso, usamos um truque devido a Leon Henkin. Em essência, o truque consiste em expandir a linguagem por infinitos símbolos de constante e adicionar, para cada fórmula com uma variável livre $\varphi(x)$, uma fórmula da forma $\exists x\, \varphi(x) \to \varphi(c)$, onde $c$ é um dos novos símbolos de constante. Quando construímos a estrutura que satisfaz $\Gamma$, isso garantirá que cada sentença existencial verdadeira tenha uma testemunha entre as novas constantes.

**Proposição 23.3.** *Se $\Gamma$ é consistente em $\mathcal{L}$ e $\mathcal{L}'$ é obtida de $\mathcal{L}$ adicionando-se a infinito enumerável conjunto de novos símbolos de constante $d_0, d_1, \ldots$, então $\Gamma$ é consistente em $\mathcal{L}'$.*

**Definição 23.4 (Conjunto saturado).** Um conjunto $\Gamma$ de fórmulas de uma linguagem $\mathcal{L}$ é *saturado* se e somente se, para cada fórmula $\varphi(x) \in \mathrm{Frm}(\mathcal{L})$ com uma variável livre $x$, existe a símbolo de constante $c \in \mathcal{L}$ tal que $\exists x\, \varphi(x) \to \varphi(c) \in \Gamma$.

A definição a seguir será usada na prova do próximo teorema.

**Definição 23.5.** Seja $\mathcal{L}'$ como em Proposição 23.3. Fixe uma enumeração $\varphi_0(x_0)$, $\varphi_1(x_1), \ldots$ de todas as fórmulas $\varphi_i(x_i)$ de $\mathcal{L}'$ nas quais uma variável $(x_i)$ ocorre livre. Definimos as sentenças $\theta_n$ por indução sobre $n$.

Seja $c_0$ o primeiro símbolo de constante dentre os $d_i$ que adicionamos a $\mathcal{L}$ que não ocorre em $\varphi_0(x_0)$. Supondo que $\theta_0, \ldots, \theta_{n-1}$ já tenham sido definidas, seja $c_n$ o primeiro dentre os novos símbolos de constante $d_i$ que não ocorre nem em $\theta_0, \ldots, \theta_{n-1}$ nem em $\varphi_n(x_n)$.

Agora seja $\theta_n$ a fórmula $\exists x_n\, \varphi_n(x_n) \to \varphi_n(c_n)$.

**Lema 23.6.** *Todo conjunto consistente $\Gamma$ pode ser estendido a um conjunto saturado consistente $\Gamma'$.*

*Prova.* Dado um conjunto consistente de sentenças $\Gamma$ em uma linguagem $\mathcal{L}$, expanda a linguagem adicionando a infinito enumerável conjunto de novos símbolos de constante para formar $\mathcal{L}'$. Por Proposição 23.3, $\Gamma$ ainda é consistente na linguagem mais rica. Além disso, seja $\theta_i$ como em Definição 23.5. Seja

$$\Gamma_0 = \Gamma$$
$$\Gamma_{n+1} = \Gamma_n \cup \{\theta_n\}$$

isto é, $\Gamma_{n+1} = \Gamma \cup \{\theta_0, \ldots, \theta_n\}$, e seja $\Gamma' = \bigcup_n \Gamma_n$. $\Gamma'$ é claramente saturado.

Se $\Gamma'$ fosse inconsistente, então, para algum $n$, $\Gamma_n$ seria inconsistente (Exercício: explique por quê). Portanto, para mostrar que $\Gamma'$ é consistente, basta mostrar, por indução sobre $n$, que cada conjunto $\Gamma_n$ é consistente.

A base da indução é simplesmente a afirmação de que $\Gamma_0 = \Gamma$ é consistente, que é a hipótese do teorema. Para o passo de indução, suponha que $\Gamma_n$ seja consistente mas $\Gamma_{n+1} = \Gamma_n \cup \{\theta_n\}$ seja inconsistente. Lembre que $\theta_n$ é $\exists x_n\, \varphi_n(x_n) \to \varphi_n(c_n)$, onde $\varphi_n(x_n)$ é a fórmula de $\mathcal{L}'$ com apenas a variável $x_n$ livre. Pela maneira como escolhemos os $c_n$ (ver Definição 23.5), $c_n$ não ocorre em $\varphi_n(x_n)$ nem em $\Gamma_n$.

Se $\Gamma_n \cup \{\theta_n\}$ é inconsistente, então $\Gamma_n \vdash \neg\theta_n$ e, portanto, ambos os seguintes valem:

$$\Gamma_n \vdash \exists x_n\, \varphi_n(x_n) \qquad \Gamma_n \vdash \neg\varphi_n(c_n)$$

Como $c_n$ não ocorre em $\Gamma_n$ ou em $\varphi_n(x_n)$, **??????????** e Teoremas 19.25 e 20.25 se aplica. De $\Gamma_n \vdash \neg\varphi_n(c_n)$, obtemos $\Gamma_n \vdash \forall x_n\, \neg\varphi_n(x_n)$. Assim, temos que ambos $\Gamma_n \vdash \exists x_n\, \varphi_n(x_n)$ e $\Gamma_n \vdash \forall x_n\, \neg\varphi_n(x_n)$, de modo que o próprio $\Gamma_n$ é inconsistente. (Note que $\forall x_n\, \neg\varphi_n(x_n) \vdash \neg\exists x_n\, \varphi_n(x_n)$.) Contradição: supunha-se que $\Gamma_n$ fosse consistente. Logo, $\Gamma_n \cup \{\theta_n\}$ é consistente. □

Mostraremos agora que conjuntos *completos*, consistentes que são saturados têm a propriedade de que contêm uma sentença universalmente quantificada se e somente se contêm todas as suas instâncias e contêm uma sentença existencialmente quantificada se e somente se contêm pelo menos uma instância. Usaremos isso para mostrar que a estrutura que geraremos a partir de um conjunto completo, consistente, saturado torna todas as suas sentenças quantificadas verdadeiras.

**Proposição 23.7.** *Suponha que $\Gamma$ seja completo, consistente e saturado.*

1. *$\exists x\, \varphi(x) \in \Gamma$ se e somente se $\varphi(t) \in \Gamma$ para pelo menos um termo fechado $t$.*
2. *$\forall x\, \varphi(x) \in \Gamma$ se e somente se $\varphi(t) \in \Gamma$ para todo termo fechado $t$.*

*Prova.* 1. Suponha primeiro que $\exists x\, \varphi(x) \in \Gamma$. Como $\Gamma$ é saturado, $(\exists x\, \varphi(x) \to \varphi(c)) \in \Gamma$ para algum símbolo de constante $c$. Por **??????????** e Proposições 19.24 e 20.24, item (1), e Proposição 23.2(1), $\varphi(c) \in \Gamma$.

Para a outra direção, a saturação não é necessária: Suponha $\varphi(t) \in \Gamma$. Então $\Gamma \vdash \exists x\, \varphi(x)$ por **??????????** e Proposições 19.26 e 20.26, item (1). Por Proposição 23.2(1), $\exists x\, \varphi(x) \in \Gamma$.

2. Exercício. □

## 23.5 Lema de Lindenbaum

Provamos agora um lema que mostra que qualquer conjunto consistente de sentenças está contido em algum conjunto de sentenças que não é apenas consistente, mas também completo. A prova funciona adicionando uma sentença de cada vez, garantindo a cada passo que o conjunto permanece consistente. Fazemos isso de modo que, para todo $\varphi$, ou $\varphi$ ou $\neg\varphi$ seja adicionada em algum estágio. A união de todos os estágios dessa construção então contém ou $\varphi$ ou sua negação $\neg\varphi$ e é, portanto, completa. Ela também é consistente, já que nos asseguramos, a cada estágio, de não introduzir uma inconsistência.

**Lema 23.8 (Lema de Lindenbaum).** *Todo conjunto consistente $\Gamma$ em uma linguagem $\mathcal{L}$ pode ser estendido a um conjunto consistente completo $\Gamma^*$.*

*Prova.* Seja $\Gamma$ consistente. Sejam $\varphi_0$, $\varphi_1$, ... uma enumeração de todas as sentenças de $\mathcal{L}$. Defina $\Gamma_0 = \Gamma$, e

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{\varphi_n\} & \text{se } \Gamma_n \cup \{\varphi_n\} \text{ é consistente;} \\ \Gamma_n \cup \{\neg\varphi_n\} & \text{caso contrário.} \end{cases}$$

Seja $\Gamma^* = \bigcup_{n\geq 0} \Gamma_n$.

Cada $\Gamma_n$ é consistente: $\Gamma_0$ é consistente por definição. Se $\Gamma_{n+1} = \Gamma_n \cup \{\varphi_n\}$, isso é porque este último é consistente. Se não é, $\Gamma_{n+1} = \Gamma_n \cup \{\neg\varphi_n\}$. Temos que verificar que $\Gamma_n \cup \{\neg\varphi_n\}$ é consistente. Suponha que não seja. Então *ambos* $\Gamma_n \cup \{\varphi_n\}$ e $\Gamma_n \cup \{\neg\varphi_n\}$ são inconsistentes. Isso significa que $\Gamma_n$ seria inconsistente por **??????????** e Proposições 19.21 e 20.21, contrariando a hipótese de indução.

Para todo $n$ e todo $i < n$, $\Gamma_i \subseteq \Gamma_n$. Isso segue por uma simples indução sobre $n$. Para $n = 0$, não há $i < 0$, de modo que a afirmação vale automaticamente. Para o passo indutivo, suponha que ela seja verdadeira para $n$. Mostramos que, se $i < n+1$, então $\Gamma_i \subseteq \Gamma_{n+1}$. Temos $\Gamma_{n+1} = \Gamma_n \cup \{\varphi_n\}$ ou $= \Gamma_n \cup \{\neg\varphi_n\}$ por construção. Logo $\Gamma_n \subseteq \Gamma_{n+1}$. Se $i < n+1$, então $\Gamma_i \subseteq \Gamma_n$ por hipótese indutiva (se $i < n$) ou pelo fato trivial de que $\Gamma_n \subseteq \Gamma_n$ (se $i = n$). Obtemos que $\Gamma_i \subseteq \Gamma_{n+1}$ por transitividade de $\subseteq$.

Disso segue que $\Gamma^*$ é consistente. Eis o porquê: Seja $\Gamma' \subseteq \Gamma^*$ finito. Cada $\psi \in \Gamma'$ também está em $\Gamma_i$ para algum $i$. Seja $n$ o maior destes. Como $\Gamma_i \subseteq \Gamma_n$ se $i \leq n$, todo $\psi \in \Gamma'$ também está $\in \Gamma_n$, isto é, $\Gamma' \subseteq \Gamma_n$, e $\Gamma_n$ é consistente. Assim, todo subconjunto finito $\Gamma' \subseteq \Gamma^*$ é consistente. Por **??????????** e Proposições 19.17 e 20.17, $\Gamma^*$ é consistente.

Toda sentença de $\mathrm{Frm}(\mathcal{L})$ aparece na lista usada para definir $\Gamma^*$. Se $\varphi_n \notin \Gamma^*$, então isso é porque $\Gamma_n \cup \{\varphi_n\}$ era inconsistente. Mas então $\neg\varphi_n \in \Gamma^*$, de modo que $\Gamma^*$ é completo. □

## 23.6 Construção de um Modelo

Por ora, não nos preocupamos com $=$, isto é, queremos apenas mostrar que um conjunto consistente $\Gamma$ de sentenças que não contém $=$ é satisfatível. Primeiro estendemos $\Gamma$ a um conjunto consistente, completo e saturado $\Gamma^*$. Nesse caso, a definição de um modelo $\mathfrak{M}(\Gamma^*)$ é simples: Tomamos o conjunto de termos fechados de $\mathcal{L}'$ como o domínio. Atribuímos cada símbolo de constante a si mesmo e nos asseguramos de que, mais geralmente, para todo termo fechado $t$, $\mathrm{Val}^{\mathfrak{M}(\Gamma^*)}(t) = t$. Aos símbolos de predicado são atribuídas extensões de tal forma que uma sentença atômica é verdadeira em $\mathfrak{M}(\Gamma^*)$ se e somente se está em $\Gamma^*$. Isso obviamente tornará verdadeiras em $\mathfrak{M}(\Gamma^*)$ todas as sentenças atômicas em $\Gamma^*$. As demais são verdadeiras desde que o $\Gamma^*$ com que começamos seja consistente, completo e saturado.

**Definição 23.9 (Modelo de termos).** Seja $\Gamma^*$ um conjunto consistente, completo e saturado de sentenças em uma linguagem $\mathcal{L}$. O *modelo de termos* $\mathfrak{M}(\Gamma^*)$ de $\Gamma^*$ é a estrutura definida como segue:

1. O domínio $|\mathfrak{M}(\Gamma^*)|$ é o conjunto de todos os termos fechados de $\mathcal{L}$.

2. A interpretação de a símbolo de constante $c$ é o próprio $c$: $c^{\mathfrak{M}(\Gamma^*)} = c$.

3. Ao símbolo de função $f$ é atribuída a função que, dados como argumentos os termos fechados $t_1, \ldots, t_n$, tem como valor o termo fechado $f(t_1, \ldots, t_n)$:
$$f^{\mathfrak{M}(\Gamma^*)}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$$

4. Se $R$ é um símbolo de predicado de $n$ lugares, então
$$\langle t_1, \ldots, t_n \rangle \in R^{\mathfrak{M}(\Gamma^*)} \text{ se e somente se } R(t_1, \ldots, t_n) \in \Gamma^*.$$

Verificaremos agora que de fato temos $\mathrm{Val}^{\mathfrak{M}(\Gamma^*)}(t) = t$.

**Lema 23.10.** *Seja $\mathfrak{M}(\Gamma^*)$ o modelo de termos de Definição 23.9; então $\mathrm{Val}^{\mathfrak{M}(\Gamma^*)}(t) = t$.*

*Prova.* A prova é por indução sobre $t$, onde o caso base, quando $t$ é a símbolo de constante, segue diretamente da definição do modelo de termos. Para o

passo de indução, assuma que $t_1, \ldots, t_n$ são termos fechados tais que $\mathrm{Val}^{\mathfrak{M}(\Gamma^*)}(t_i) = t_i$ e que $f$ é a símbolo de função $n$-ária. Então

$$\begin{aligned}\mathrm{Val}^{\mathfrak{M}(\Gamma^*)}(f(t_1, \ldots, t_n)) &= f^{\mathfrak{M}(\Gamma^*)}(\mathrm{Val}^{\mathfrak{M}(\Gamma^*)}(t_1), \ldots, \mathrm{Val}^{\mathfrak{M}(\Gamma^*)}(t_n)) \\ &= f^{\mathfrak{M}(\Gamma^*)}(t_1, \ldots, t_n) \\ &= f(t_1, \ldots, t_n),\end{aligned}$$

e, assim, por indução, isto vale para todo termo fechado $t$. □

A estrutura $\mathfrak{M}$ pode tornar verdadeira uma sentença $\exists x\, \varphi(x)$ existencialmente quantificada sem que haja uma instância $\varphi(t)$ que ela torne verdadeira. A estrutura $\mathfrak{M}$ pode tornar verdadeiras todas as instâncias $\varphi(t)$ de uma sentença $\forall x\, \varphi(x)$ universalmente quantificada sem tornar $\forall x\, \varphi(x)$ verdadeira. Isso ocorre porque, em geral, nem todo membro de $|\mathfrak{M}|$ é o valor de um termo fechado ($\mathfrak{M}$ pode não ser coberta). Esta é a razão pela qual a relação de satisfação é definida por meio de atribuições de variáveis. Entretanto, para o nosso modelo de termos $\mathfrak{M}(\Gamma^*)$ isso não seria necessário — porque ela é coberta. Este é o conteúdo do próximo resultado.

**Proposição 23.11.** *Seja $\mathfrak{M}(\Gamma^*)$ o modelo de termos de Definição 23.9.*

1. *$\mathfrak{M}(\Gamma^*) \vDash \exists x\, \varphi(x)$ se e somente se $\mathfrak{M}(\Gamma^*) \vDash \varphi(t)$ para pelo menos um termo fechado $t$.*
2. *$\mathfrak{M}(\Gamma^*) \vDash \forall x\, \varphi(x)$ se e somente se $\mathfrak{M}(\Gamma^*) \vDash \varphi(t)$ para todo termo fechado $t$.*

*Prova.* 1. Por Proposição 16.19, $\mathfrak{M}(\Gamma^*) \vDash \exists x\, \varphi(x)$ se e somente se, para pelo menos uma atribuição de variáveis $s$, $\mathfrak{M}(\Gamma^*), s \vDash \varphi(x)$. Como $|\mathfrak{M}(\Gamma^*)|$ consiste nos termos fechados de $\mathcal{L}$, este é o caso se e somente se há pelo menos um termo fechado $t$ tal que $s(x) = t$ e $\mathfrak{M}(\Gamma^*), s \vDash \varphi(x)$. Por Proposição 16.23, $\mathfrak{M}(\Gamma^*), s \vDash \varphi(x)$ se e somente se $\mathfrak{M}(\Gamma^*), s \vDash \varphi(t)$, onde $s(x) = t$. Por Proposição 16.18, $\mathfrak{M}(\Gamma^*), s \vDash \varphi(t)$ se e somente se $\mathfrak{M}(\Gamma^*) \vDash \varphi(t)$, já que $\varphi(t)$ é uma sentença.

2. Exercício. □

**Lema 23.12 (Lema da Verdade).** *Suponha que $\varphi$ não contenha $=$. Então $\mathfrak{M}(\Gamma^*) \vDash \varphi$ se e somente se $\varphi \in \Gamma^*$.*

*Prova.* Provamos ambas as direções simultaneamente e por indução sobre $\varphi$.

1. $\varphi \equiv \bot$: $\mathfrak{M}(\Gamma^*) \nvDash \bot$ por definição de satisfação. Por outro lado, $\bot \notin \Gamma^*$ já que $\Gamma^*$ é consistente.
2. $\varphi \equiv R(t_1, \ldots, t_n)$: $\mathfrak{M}(\Gamma^*) \vDash R(t_1, \ldots, t_n)$ se e somente se $\langle t_1, \ldots, t_n \rangle \in R^{\mathfrak{M}(\Gamma^*)}$ (pela definição de satisfação) se e somente se $R(t_1, \ldots, t_n) \in \Gamma^*$ (pela construção de $\mathfrak{M}(\Gamma^*)$).

3. $\varphi \equiv \neg\psi$: $\mathfrak{M}(\Gamma^*) \vDash \varphi$ se e somente se $\mathfrak{M}(\Gamma^*) \nvDash \psi$ (por definição de satisfação). Por hipótese de indução, $\mathfrak{M}(\Gamma^*) \nvDash \psi$ se e somente se $\psi \notin \Gamma^*$. Como $\Gamma^*$ é consistente e completo, $\psi \notin \Gamma^*$ se e somente se $\neg\psi \in \Gamma^*$.

4. $\varphi \equiv \psi \wedge \chi$: exercise.

5. $\varphi \equiv \psi \vee \chi$: $\mathfrak{M}(\Gamma^*) \vDash \varphi$ se e somente se $\mathfrak{M}(\Gamma^*) \vDash \psi$ ou $\mathfrak{M}(\Gamma^*) \vDash \chi$ (por definição de satisfação) se e somente se $\psi \in \Gamma^*$ ou $\chi \in \Gamma^*$ (por hipótese de indução). Este é o caso se e somente se $(\psi \vee \chi) \in \Gamma^*$ (por Proposição 23.2(3)).

6. $\varphi \equiv \psi \to \chi$: exercise.

7. $\varphi \equiv \forall x\, \psi(x)$: exercise.

8. $\varphi \equiv \exists x\, \psi(x)$: $\mathfrak{M}(\Gamma^*) \vDash \varphi$ se e somente se $\mathfrak{M}(\Gamma^*) \vDash \psi(t)$ para pelo menos um termo $t$ (Proposição 23.11). Por hipótese de indução, este é o caso se e somente se $\psi(t) \in \Gamma^*$ para pelo menos um termo $t$. Por Proposição 23.7, isto, por sua vez, é o caso se e somente se $\exists x\, \psi(x) \in \Gamma^*$. □

## 23.7 Identidade

A construção do modelo de termos dada na seção anterior é suficiente para estabelecer a completude da lógica de primeira ordem para conjuntos $\Gamma$ que não contêm $=$. O modelo de termos satisfaz todo $\varphi \in \Gamma^*$ que não contém $=$ (e, portanto, todo $\varphi \in \Gamma$). Ele não funciona, no entanto, se $=$ está presente. A razão é que $\Gamma^*$ pode então conter a sentença $t = t'$, mas no modelo de termos o valor de qualquer termo é esse próprio termo. Logo, se $t$ e $t'$ são termos diferentes, seus valores no modelo de termos — isto é, $t$ e $t'$, respectivamente — são diferentes, e assim $t = t'$ é falsa. Podemos corrigir isso, no entanto, usando uma construção conhecida como "fatoração".

**Definição 23.13.** Seja $\Gamma^*$ um conjunto consistente e completo de sentenças em $\mathcal{L}$. Definimos a relação $\approx$ sobre o conjunto de termos fechados de $\mathcal{L}$ por

$$t \approx t' \quad \text{se e somente se} \quad t = t' \in \Gamma^*$$

**Proposição 23.14.** *A relação $\approx$ tem as seguintes propriedades:*

1. *$\approx$ é reflexiva.*

2. *$\approx$ é simétrica.*

3. *$\approx$ é transitiva.*

4. *Se $t \approx t'$, $f$ é a símbolo de função, e $t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n$ são termos fechados, então*

$$f(t_1, \ldots, t_{i-1}, t, t_{i+1}, \ldots, t_n) \approx f(t_1, \ldots, t_{i-1}, t', t_{i+1}, \ldots, t_n).$$

5. *Se $t \approx t'$, $R$ é a símbolo de predicado, e $t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n$ são termos fechados, então*

$$R(t_1, \ldots, t_{i-1}, t, t_{i+1}, \ldots, t_n) \in \Gamma^* \text{ se e somente se } R(t_1, \ldots, t_{i-1}, t', t_{i+1}, \ldots, t_n) \in \Gamma^*.$$

*Prova.* Como $\Gamma^*$ é consistente e completo, $t = t' \in \Gamma^*$ se e somente se $\Gamma^* \vdash t = t'$. Assim, basta mostrar o seguinte:

1. $\Gamma^* \vdash t = t$ para todos os termos fechados $t$.
2. Se $\Gamma^* \vdash t = t'$ então $\Gamma^* \vdash t' = t$.
3. Se $\Gamma^* \vdash t = t'$ e $\Gamma^* \vdash t' = t''$, então $\Gamma^* \vdash t = t''$.
4. Se $\Gamma^* \vdash t = t'$, então

$$\Gamma^* \vdash f(t_1, \ldots, t_{i-1}, t, t_{i+1}, , \ldots, t_n) = f(t_1, \ldots, t_{i-1}, t', t_{i+1}, \ldots, t_n)$$

   para todo símbolo de função $f$ de $n$ lugares e termos fechados $t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n$.

5. Se $\Gamma^* \vdash t = t'$ e $\Gamma^* \vdash R(t_1, \ldots, t_{i-1}, t, t_{i+1}, \ldots, t_n)$, então $\Gamma^* \vdash R(t_1, \ldots, t_{i-1}, t', t_{i+1}, \ldots, t_n)$ para todo símbolo de predicado $R$ de $n$ lugares e termos fechados $t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n$. □

**Definição 23.15.** Suponha que $\Gamma^*$ seja um conjunto consistente e completo em uma linguagem $\mathcal{L}$, $t$ seja um termo fechado e $\approx$ como na definição anterior. Então:

$$[t]_\approx = \{t' : t' \in \mathrm{Trm}(\mathcal{L}), t \approx t'\}$$

e $\mathrm{Trm}(\mathcal{L})/_\approx = \{[t]_\approx : t \in \mathrm{Trm}(\mathcal{L})\}$.

**Definição 23.16.** Seja $\mathfrak{M} = \mathfrak{M}(\Gamma^*)$ o modelo de termos para $\Gamma^*$ de Definição 23.9. Então $\mathfrak{M}/_\approx$ é a seguinte estrutura:

1. $|\mathfrak{M}/_\approx| = \mathrm{Trm}(\mathcal{L})/_\approx$.
2. $c^{\mathfrak{M}/_\approx} = [c]_\approx$
3. $f^{\mathfrak{M}/_\approx}([t_1]_\approx, \ldots, [t_n]_\approx) = [f(t_1, \ldots, t_n)]_\approx$

4. $\langle [t_1]_\approx, \ldots, [t_n]_\approx \rangle \in R^{\mathfrak{M}/\approx}$ se e somente se $\mathfrak{M} \vDash R(t_1, \ldots, t_n)$, isto é, se e somente se $R(t_1, \ldots, t_n) \in \Gamma^*$.

Note que definimos $f^{\mathfrak{M}/\approx}$ e $R^{\mathfrak{M}/\approx}$ para elementos de $\mathrm{Trm}(\mathcal{L})/\approx$ referindo-nos a eles como $[t]_\approx$, isto é, por meio de *representantes* $t \in [t]_\approx$. Temos que nos assegurar de que essas definições não dependam da escolha desses representantes, isto é, de que, para algumas outras escolhas $t'$ que determinam as mesmas classes de equivalência ($[t]_\approx = [t']_\approx$), as definições produzam o mesmo resultado. Por exemplo, se $R$ é um símbolo de predicado de um lugar, a última cláusula da definição diz que $[t]_\approx \in R^{\mathfrak{M}/\approx}$ se e somente se $\mathfrak{M} \vDash R(t)$. Se, para algum outro termo $t'$ com $t \approx t'$, $\mathfrak{M} \nvDash R(t)$, então a definição exigiria $[t']_\approx \notin R^{\mathfrak{M}/\approx}$. Se $t \approx t'$, então $[t]_\approx = [t']_\approx$, mas não podemos ter ao mesmo tempo $[t]_\approx \in R^{\mathfrak{M}/\approx}$ e $[t]_\approx \notin R^{\mathfrak{M}/\approx}$. Entretanto, Proposição 23.14 garante que isso não pode acontecer.

**Proposição 23.17.** *$\mathfrak{M}/\approx$ está bem definida, isto é, se $t_1, \ldots, t_n, t'_1, \ldots, t'_n$ são termos fechados, e $t_i \approx t'_i$, então*

1. $[f(t_1, \ldots, t_n)]_\approx = [f(t'_1, \ldots, t'_n)]_\approx$, *isto é,*

$$f(t_1, \ldots, t_n) \approx f(t'_1, \ldots, t'_n)$$

   *e*

2. $\mathfrak{M} \vDash R(t_1, \ldots, t_n)$ *se e somente se* $\mathfrak{M} \vDash R(t'_1, \ldots, t'_n)$, *isto é,*

$$R(t_1, \ldots, t_n) \in \Gamma^* \text{ se e somente se } R(t'_1, \ldots, t'_n) \in \Gamma^*.$$

*Prova.* Segue de Proposição 23.14 por indução sobre $n$. □

Como no caso do modelo de termos, antes de provar o lema da verdade precisamos do seguinte lema.

**Lema 23.18.** *Seja $\mathfrak{M} = \mathfrak{M}(\Gamma^*)$; então* $\mathrm{Val}^{\mathfrak{M}/\approx}(t) = [t]_\approx$.

*Prova.* A prova é similar à de Lema 23.10. □

**Lema 23.19.** *$\mathfrak{M}/\approx \vDash \varphi$ se e somente se $\varphi \in \Gamma^*$ para todas as sentenças $\varphi$.*

*Prova.* Por indução sobre $\varphi$, exatamente como na prova de Lema 23.12. O único caso que precisa de atenção adicional é quando $\varphi \equiv t = t'$.

$$\begin{aligned} \mathfrak{M}/\approx \vDash t = t' &\text{ se e somente se } [t]_\approx = [t']_\approx \text{ (por definição de } \mathfrak{M}/\approx) \\ &\text{se e somente se } t \approx t' \text{ (por definição de } [t]_\approx) \\ &\text{se e somente se } t = t' \in \Gamma^* \text{ (por definição de } \approx). \end{aligned}$$

□

Note que, embora $\mathfrak{M}(\Gamma^*)$ seja sempre enumerável e infinita, $\mathfrak{M}/_{\approx}$ pode ser finita, já que pode ocorrer que haja apenas finitas classes $[t]_{\approx}$. Isso é de se esperar, já que $\Gamma$ pode conter sentenças que exigem que qualquer estrutura na qual elas sejam verdadeiras seja finita. Por exemplo, $\forall x \forall y\, x = y$ é a sentença consistente, mas é satisfeita apenas em estruturas com a domínio que contém exatamente um membro.

## 23.8 O Teorema da Completude

Vamos combinar nossos resultados: chegamos ao teorema da completude.

**Teorema 23.20 (Teorema da Completude).** *Seja $\Gamma$ um conjunto de sentenças. Se $\Gamma$ é consistente, então é satisfatível.*

*Prova.* Suponha que $\Gamma$ seja consistente. Por Lema 23.6, existe um conjunto saturado consistente $\Gamma' \supseteq \Gamma$. Por Lema 23.8, existe um $\Gamma^* \supseteq \Gamma'$ que é consistente e completo. Como $\Gamma' \subseteq \Gamma^*$, para cada fórmula $\varphi(x)$, $\Gamma^*$ contém a sentença da forma $\exists x\, \varphi(x) \to \varphi(c)$ e, assim, $\Gamma^*$ é saturado. Se $\Gamma$ não contém $=$, então, por Lema 23.12, $\mathfrak{M}(\Gamma^*) \vDash \varphi$ se e somente se $\varphi \in \Gamma^*$. Disso segue, em particular, que, para todo $\varphi \in \Gamma$, $\mathfrak{M}(\Gamma^*) \vDash \varphi$, de modo que $\Gamma$ é satisfatível. Se $\Gamma$ de fato contém $=$, então, por Lema 23.19, para todas as sentenças $\varphi$, $\mathfrak{M}/_{\approx} \vDash \varphi$ se e somente se $\varphi \in \Gamma^*$. Em particular, $\mathfrak{M}/_{\approx} \vDash \varphi$ para todo $\varphi \in \Gamma$, de modo que $\Gamma$ é satisfatível. □

**Corolário 23.21 (Teorema da Completude, Segunda Versão).** *Para todo $\Gamma$ e sentenças $\varphi$: se $\Gamma \vDash \varphi$ então $\Gamma \vdash \varphi$.*

*Prova.* Note que os $\Gamma$ em Corolário 23.21 e Teorema 23.20 são universalmente quantificados. Para nos certificarmos de que não nos confundimos, reformulemos Teorema 23.20 usando uma variável diferente: para qualquer conjunto de sentenças $\Delta$, se $\Delta$ é consistente, então é satisfatível. Por contraposição, se $\Delta$ não é satisfatível, então $\Delta$ é inconsistente. Usaremos isso para provar o corolário.

Suponha que $\Gamma \vDash \varphi$. Então $\Gamma \cup \{\neg\varphi\}$ é insatisfatível por Proposição 16.28. Tomando $\Gamma \cup \{\neg\varphi\}$ como nosso $\Delta$, a versão anterior de Teorema 23.20 nos dá que $\Gamma \cup \{\neg\varphi\}$ é inconsistente. Por **??????????** e Proposições 19.19 e 20.19, $\Gamma \vdash \varphi$. □

## 23.9 O Teorema da Compacidade

Uma consequência importante do teorema da completude é o teorema da compacidade. O teorema da compacidade afirma que, se cada subconjunto *finito* de um conjunto de sentenças é satisfatível, o conjunto inteiro é satisfatível — mesmo que o próprio conjunto seja infinito. Isso está longe de ser

óbvio. Não há nada que pareça descartar, ao menos à primeira vista, a possibilidade de existirem conjuntos infinitos de sentenças que sejam contraditórios, mas em que a contradição só surge, por assim dizer, do número infinito. O teorema da compacidade diz que tal cenário pode ser descartado: não existem conjuntos infinitos insatisfatíveis de sentenças tais que cada subconjunto finito deles seja satisfatível. Como o teorema da completude, ele tem uma versão relacionada à consequência lógica: se um conjunto infinito de sentenças implica algo, então já um subconjunto finito o implica.

**Definição 23.22.** Um conjunto $\Gamma$ de fórmulas é *finitamente satisfatível* se e somente se todo $\Gamma_0 \subseteq \Gamma$ finito é satisfatível.

**Teorema 23.23 (Teorema da Compacidade).** *O seguinte vale para quaisquer sentenças $\Gamma$ e $\varphi$:*

1. *$\Gamma \vDash \varphi$ se e somente se existe um $\Gamma_0 \subseteq \Gamma$ finito tal que $\Gamma_0 \vDash \varphi$.*
2. *$\Gamma$ é satisfatível se e somente se é finitamente satisfatível.*

*Prova.* Provamos (2). Se $\Gamma$ é satisfatível, então existe a estrutura $\mathfrak{M}$ tal que $\mathfrak{M} \vDash \varphi$ para todo $\varphi \in \Gamma$. É claro que essa $\mathfrak{M}$ também satisfaz todo subconjunto finito de $\Gamma$, de modo que $\Gamma$ é finitamente satisfatível.

Agora suponha que $\Gamma$ seja finitamente satisfatível. Então todo subconjunto finito $\Gamma_0 \subseteq \Gamma$ é satisfatível. Pela correção (**??????????** e Corolários 19.31 e 20.29), todo subconjunto finito é consistente. Então o próprio $\Gamma$ deve ser consistente por **??????????** e Proposições 19.17 e 20.17. Pela completude (Teorema 23.20), como $\Gamma$ é consistente, ele é satisfatível. □

**Exemplo 23.24.** Em todo modelo $\mathfrak{M}$ de uma teoria $\Gamma$, cada termo $t$ obviamente designa um membro de $|\mathfrak{M}|$. Podemos garantir que também seja verdade que todo membro de $|\mathfrak{M}|$ seja designado por algum termo? Em outras palavras, existem teorias $\Gamma$ cujos modelos são todos cobertos? O teorema da compacidade mostra que esse não é o caso se $\Gamma$ tem modelos infinitos. Eis como ver isso: Seja $\mathfrak{M}$ um modelo infinito de $\Gamma$, e seja $c$ a símbolo de constante que não está na linguagem de $\Gamma$. Seja $\Delta$ o conjunto de todas as sentenças $c \neq t$ para $t$ um termo na linguagem $\mathcal{L}$ de $\Gamma$, isto é,

$$\Delta = \{c \neq t : t \in \mathrm{Trm}(\mathcal{L})\}.$$

Um subconjunto finito de $\Gamma \cup \Delta$ pode ser escrito como $\Gamma' \cup \Delta'$, com $\Gamma' \subseteq \Gamma$ e $\Delta' \subseteq \Delta$. Como $\Delta'$ é finito, ele pode conter apenas finitos termos. Seja $a \in |\mathfrak{M}|$ um membro de $|\mathfrak{M}|$ que não é designado por nenhum deles, e seja $\mathfrak{M}'$ a estrutura que é exatamente como $\mathfrak{M}$, mas com $c^{\mathfrak{M}'} = a$ também. Como $a \neq \mathrm{Val}^{\mathfrak{M}}(t)$ para todo $t$ que ocorre em $\Delta'$, $\mathfrak{M}' \vDash \Delta'$. Como $\mathfrak{M} \vDash \Gamma$, $\Gamma' \subseteq \Gamma$, e $c$ não ocorre em $\Gamma$, também $\mathfrak{M}' \vDash \Gamma'$. Juntando, $\mathfrak{M}' \vDash \Gamma' \cup \Delta'$ para todo subconjunto finito $\Gamma' \cup \Delta'$ de $\Gamma \cup \Delta$. Assim, todo subconjunto finito de $\Gamma \cup \Delta$

é satisfatível. Por compacidade, o próprio $\Gamma \cup \Delta$ é satisfatível. Logo, existem modelos $\mathfrak{M} \vDash \Gamma \cup \Delta$. Todo tal $\mathfrak{M}$ é um modelo de $\Gamma$, mas não é coberto, já que $\mathrm{Val}^{\mathfrak{M}}(c) \neq \mathrm{Val}^{\mathfrak{M}}(t)$ para todos os termos $t$ de $\mathcal{L}$.

**Exemplo 23.25.** Considere a linguagem $\mathcal{L}$ contendo o símbolo de predicado $<$, símbolos de constante $\mathtt{0}$, $\mathtt{1}$, e símbolos de função $+$, $\times$, e $-$. Seja $\Gamma$ o conjunto de todas as sentenças nesta linguagem verdadeiras na estrutura $\mathfrak{Q}$ com domínio $\mathbb{Q}$ e as interpretações óbvias. $\Gamma$ é o conjunto de todas as sentenças de $\mathcal{L}$ verdadeiras a respeito dos números racionais. É claro que, em $\mathbb{Q}$ (e mesmo em $\mathbb{R}$), não há números $r$ que sejam maiores que 0 mas menores que $1/k$ para todo $k \in \mathbb{Z}^+$. Tal número, se existisse, seria um *infinitesimal:* não nulo, mas infinitamente pequeno. O teorema da compacidade pode ser usado para mostrar que há modelos de $\Gamma$ nos quais infinitesimais existem. Não temos a símbolo de função para a divisão em nossa linguagem (a divisão por zero é indefinida, e símbolos de função têm de ser interpretadas por funções totais). Contudo, ainda podemos expressar que $r < 1/k$, já que isso ocorre se e somente se $r \cdot k < 1$. Agora seja $c$ a símbolo de constante nova e seja $\Delta$

$$\{\mathtt{0} < c\} \cup \{c \times \overline{k} < \mathtt{1} : k \in \mathbb{Z}^+\}$$

(onde $\overline{k} = (\mathtt{1} + (\mathtt{1} + \cdots + (\mathtt{1} + \mathtt{1}) \ldots))$ com $k$ $\mathtt{1}$'s). Para qualquer subconjunto finito $\Delta_0$ de $\Delta$ existe um $K$ tal que todas as sentenças $c \times \overline{k} < \mathtt{1}$ em $\Delta_0$ têm $k < K$. Se expandirmos $\mathfrak{Q}$ para $\mathfrak{Q}'$ com $c^{\mathfrak{Q}'} = 1/K$ temos que $\mathfrak{Q}' \vDash \Gamma_0 \cup \Delta_0$ para qualquer $\Gamma_0 \subseteq \Gamma$ finito, e assim $\Gamma \cup \Delta$ é finitamente satisfatível (Exercício: prove isso em detalhe). Por compacidade, $\Gamma \cup \Delta$ é satisfatível. Qualquer modelo $\mathfrak{S}$ de $\Gamma \cup \Delta$ contém um infinitesimal, a saber $c^{\mathfrak{S}}$.

**Exemplo 23.26.** Sabemos que a lógica de primeira ordem com predicado de identidade pode expressar que o tamanho do domínio deve ter algum tamanho mínimo: A sentença $\varphi_{\geq n}$ (que diz "existem pelo menos $n$ objetos distintos") é verdadeira apenas em estruturas onde $|\mathfrak{M}|$ tem pelo menos $n$ objetos. Assim, se tomarmos

$$\Delta = \{\varphi_{\geq n} : n \geq 1\}$$

então qualquer modelo de $\Delta$ deve ser infinito. Desse modo, podemos garantir que uma teoria só tenha modelos infinitos adicionando $\Delta$ a ela: os modelos de $\Gamma \cup \Delta$ são todos os modelos infinitos de $\Gamma$, e apenas eles.

Portanto, a lógica de primeira ordem pode expressar a infinitude. O teorema da compacidade mostra que ela não pode expressar a finitude, no entanto. Pois suponha que algum conjunto de sentenças $\Lambda$ fosse satisfeito em todas as estruturas finitas, e apenas nelas. Então $\Delta \cup \Lambda$ é finitamente satisfatível. Por quê? Suponha que $\Delta' \cup \Lambda' \subseteq \Delta \cup \Lambda$ seja finito, com $\Delta' \subseteq \Delta$ e $\Lambda' \subseteq \Lambda$. Seja $n$ o maior número tal que $\varphi_{\geq n} \in \Delta'$. $\Lambda$, sendo satisfeito em todas as estruturas finitas, tem um modelo $\mathfrak{M}$ com um número finito de membros, mas $\geq n$ deles. Mas então $\mathfrak{M} \vDash \Delta' \cup \Lambda'$. Por compacidade, $\Delta \cup \Lambda$ tem um

modelo infinito, contradizendo a suposição de que $\Lambda$ é satisfeito apenas em estruturas finitas.

## 23.10 Uma Prova Direta do Teorema da Compacidade

Podemos provar o Teorema da Compacidade diretamente, sem apelar ao Teorema da Completude, usando as mesmas ideias da prova do teorema da completude. Na prova do Teorema da Completude, começamos com um conjunto $\Gamma$ consistente de sentenças, expandimos-o para um conjunto $\Gamma^*$ de sentenças consistente, saturado, e completo, e então mostramos que no modelo de termos $\mathfrak{M}(\Gamma^*)$ construído a partir de $\Gamma^*$, todas as sentenças de $\Gamma$ são verdadeiras, de modo que $\Gamma$ é satisfatível.

Podemos usar o mesmo método para mostrar que um conjunto finitamente satisfatível de sentenças é satisfatível. Só temos que provar as versões correspondentes dos resultados que levam ao lema da verdade, substituindo "consistente" por "finitamente satisfatível".

**Proposição 23.27.** *Suponha que $\Gamma$ é completo e finitamente satisfatível. Então:*

1. *$(\varphi \wedge \psi) \in \Gamma$ se, e somente se, tanto $\varphi \in \Gamma$ quanto $\psi \in \Gamma$.*
2. *$(\varphi \vee \psi) \in \Gamma$ se, e somente se, $\varphi \in \Gamma$ ou $\psi \in \Gamma$.*
3. *$(\varphi \to \psi) \in \Gamma$ se, e somente se, $\varphi \notin \Gamma$ ou $\psi \in \Gamma$.*

**Lema 23.28.** *Todo conjunto finitamente satisfatível $\Gamma$ pode ser estendido a um conjunto saturado finitamente satisfatível $\Gamma'$.*

**Proposição 23.29.** *Suponha que $\Gamma$ é completo, finitamente satisfatível e saturado.*

1. *$\exists x\, \varphi(x) \in \Gamma$ se, e somente se, $\varphi(t) \in \Gamma$ para pelo menos um termo fechado $t$.*
2. *$\forall x\, \varphi(x) \in \Gamma$ se, e somente se, $\varphi(t) \in \Gamma$ para todos os termos fechados $t$.*

**Lema 23.30.** *Todo conjunto finitamente satisfatível $\Gamma$ pode ser estendido a um conjunto completo e finitamente satisfatível $\Gamma^*$.*

**Teorema 23.31 (Compacidade).** *$\Gamma$ é satisfatível se, e somente se, é finitamente satisfatível.*

*Prova.* Se $\Gamma$ é satisfatível, então há a estrutura $\mathfrak{M}$ tal que $\mathfrak{M} \vDash \varphi$ para todo $\varphi \in \Gamma$. É claro que esta $\mathfrak{M}$ também satisfaz todo subconjunto finito de $\Gamma$, de modo que $\Gamma$ é finitamente satisfatível.

Agora suponha que $\Gamma$ é finitamente satisfatível. Por Lema 23.28, há um conjunto finitamente satisfatível e saturado $\Gamma' \supseteq \Gamma$. Por Lema 23.30, $\Gamma'$ pode ser estendido a um conjunto completo e finitamente satisfatível $\Gamma^*$, e $\Gamma^*$ ainda é saturado. Construa o modelo de termos $\mathfrak{M}(\Gamma^*)$ como em Definição 23.9.

Note que Proposição 23.11 não dependeu do fato de que $\Gamma^*$ é consistente (ou completo ou saturado, aliás), mas apenas do fato de que $\mathfrak{M}(\Gamma^*)$ é coberta. A prova do Lema da Verdade (Lema 23.12) funciona se substituirmos referências a Proposição 23.2 e Proposição 23.7 por referências a Proposição 23.27 e Proposição 23.29□

## 23.11 O Teorema de Löwenheim–Skolem

O Teorema de Löwenheim–Skolem diz que se uma teoria tem um modelo infinito, então ela também tem um modelo que é no máximo infinito enumerável. Uma consequência imediata desse fato é que a lógica de primeira ordem não pode expressar que o tamanho de a estrutura é não enumerável: qualquer sentença ou conjunto de sentenças satisfeito em todas as estruturas não enumeráveis também é satisfeito em alguma estrutura enumerável.

**Teorema 23.32.** *Se $\Gamma$ é consistente, então ela tem um modelo enumerável, isto é, é satisfatível em a estrutura cujo domínio é finito ou infinito enumerável.*

*Prova.* Se $\Gamma$ é consistente, a estrutura $\mathfrak{M}$ fornecida pela prova do teorema da completude tem um domínio $|\mathfrak{M}|$ que não é maior do que o conjunto dos termos da linguagem $\mathcal{L}$. Assim $\mathfrak{M}$ é no máximo infinito enumerável. □

**Teorema 23.33.** *Se $\Gamma$ é um conjunto consistente de sentenças na linguagem da lógica de primeira ordem sem identidade, então ela tem um modelo infinito enumerável, isto é, é satisfatível em a estrutura cujo domínio é infinito e enumerável.*

*Prova.* Se $\Gamma$ é consistente e não contém sentenças em que a identidade aparece, então a estrutura $\mathfrak{M}$ fornecida pela prova do teorema da completude tem um domínio $|\mathfrak{M}|$ idêntico ao conjunto dos termos da linguagem $\mathcal{L}'$. Assim $\mathfrak{M}$ é infinito enumerável, pois $\mathrm{Trm}(\mathcal{L}')$ o é. □

**Exemplo 23.34 (Paradoxo de Skolem).** A teoria dos conjuntos de Zermelo–Fraenkel **ZFC** é um arcabouço muito poderoso no qual praticamente todas as afirmações matemáticas podem ser expressas, incluindo fatos sobre os tamanhos de conjuntos. Assim, por exemplo, **ZFC** pode provar que o conjunto $\mathbb{R}$ dos números reais é não enumerável, pode provar o Teorema de Cantor de que o conjunto potência de qualquer conjunto é maior do que o próprio conjunto, etc. Se **ZFC** é consistente, seus modelos são todos infinitos e, além disso, todos contêm membros sobre os quais a teoria diz que são não enumeráveis, como o elemento que torna verdadeiro o teorema de **ZFC** de que o conjunto potência dos números naturais existe. Pelo Teorema de Löwenheim–Skolem, **ZFC** também tem modelos enumeráveis—modelos que contêm conjuntos "não enumeráveis", mas que eles mesmos são enumeráveis.

## Problemas

**Problema 23.1.** Complete a prova de Proposição 23.2.

**Problema 23.2.** Complete a prova de Proposição 23.11.

**Problema 23.3.** Complete a prova de Lema 23.12.

**Problema 23.4.** Complete a prova de Proposição 23.14.

**Problema 23.5.** Complete a prova de Lema 23.18.

**Problema 23.6.** Use Corolário 23.21 para provar Teorema 23.20, mostrando assim que as duas formulações do teorema da completude são equivalentes.

**Problema 23.7.** Para que um sistema de derivação seja completo, suas regras devem ser fortes o suficiente para provar que todo conjunto insatisfatível é inconsistente. Quais das regras de derivação foram necessárias para provar a completude? Alguma dessas regras não é usada em nenhum lugar da prova? Para responder a essas perguntas, faça uma lista ou diagrama que mostre quais das regras de derivação foram usadas em quais resultados que levam à prova de Teorema 23.20. Certifique-se de anotar quaisquer usos tácitos de regras nessas provas.

**Problema 23.8.** Prove (1) de Teorema 23.23.

**Problema 23.9.** No modelo padrão da aritmética $\mathfrak{N}$, não há membro $k \in |\mathfrak{N}|$ que satisfaça toda fórmula $\overline{n} < x$ (onde $\overline{n}$ é $0^{\prime\cdots\prime}$ com $n$ $\prime$'s). Use o teorema da compacidade para mostrar que o conjunto de sentenças na linguagem da aritmética que são verdadeiras no modelo padrão da aritmética $\mathfrak{N}$ também são verdadeiras em a estrutura $\mathfrak{N}'$ que contém um membro que *de fato* satisfaz toda fórmula $\overline{n} < x$.

**Problema 23.10.** Prove Proposição 23.27. Evite o uso de $\vdash$.

**Problema 23.11.** Prove Lema 23.28. (Dica: o passo crucial é mostrar que se $\Gamma_n$ é finitamente satisfatível, então $\Gamma_n \cup \{\theta_n\}$ também o é, sem qualquer apelo a derivações ou consistência.)

**Problema 23.12.** Prove Proposição 23.29.

**Problema 23.13.** Prove Lema 23.30. (Dica: o passo crucial é mostrar que se $\Gamma_n$ é finitamente satisfatível, então ou $\Gamma_n \cup \{\varphi_n\}$ ou $\Gamma_n \cup \{\neg\varphi_n\}$ é finitamente satisfatível.)

**Problema 23.14.** Escreva a prova completa do Lema da Verdade (Lema 23.12) na versão necessária para a prova de Teorema 23.31.

# Capítulo 24

# Além da lógica de primeira ordem

Este capítulo, adaptado das notas de lógica de Jeremy Avigad, fornece o mais breve vislumbre de quais outros sistemas lógicos existem. Pretende ser um capítulo que sugere tópicos adicionais para estudo em um curso que não os cobre. Cada um dos tópicos mencionados aqui irá — espero — eventualmente receber seu próprio tratamento em nível de parte no Projeto Open Logic.

## 24.1 Visão Geral

A lógica de primeira ordem não é o único sistema de lógica de interesse: há muitas extensões e variações da lógica de primeira ordem. Uma lógica normalmente consiste na especificação formal de uma linguagem, geralmente, mas nem sempre, em um sistema dedutivo e, geralmente, mas nem sempre, em uma semântica pretendida. Mas o uso técnico do termo levanta uma pergunta óbvia: o que as lógicas que não são lógicas de primeira ordem têm a ver com a palavra "lógica", usada no sentido intuitivo ou filosófico? Todos os sistemas descritos abaixo são projetados para modelar o raciocínio de uma forma ou de outra; podemos dizer o que os torna lógicos?

Não há respostas fáceis. A palavra "lógica" é usada de diferentes maneiras e em diferentes contextos, e a noção, como a de "verdade", tem sido analisada a partir de numerosos posicionamentos filosóficos. Por exemplo, pode-se considerar que o objetivo do raciocínio lógico é a determinação de quais afirmações são necessariamente verdadeiras, verdadeiras a priori, verdadeiras independentemente da interpretação dos termos não lógicos, verdadeiras em virtude de sua forma, ou verdadeiras por convenção linguística; e cada uma dessas concepções requer bastante esclarecimento. Mesmo que se restrinja a atenção ao tipo de lógica usada na matemática, há pouco acordo quanto ao seu alcance. Por exemplo, no *Principia Mathematica*, Russell e Whi-

tehead tentaram desenvolver a matemática com base na lógica, na tradição *logicista* iniciada por Frege. Seu sistema de lógica era uma forma de lógica de tipo superior semelhante à descrita abaixo. No final, foram forçados a introduzir axiomas que, pela maioria dos padrões, não parecem puramente lógicos (notavelmente, o axioma do infinito e o axioma da redutibilidade), mas pode-se, ainda assim, sustentar que algumas formas de raciocínio de ordem superior devem ser aceitas como lógicas. Em contraste, Quine, cuja ontologia não admite "proposições" como objetos legítimos de discurso, argumenta que a lógica de segunda ordem e a de ordem superior são realmente manifestações da teoria dos conjuntos em pele de cordeiro; em outras palavras, sistemas que envolvem quantificação sobre predicados não são puramente lógicos.

Por enquanto, é melhor deixar tais questões filosóficas para um dia chuvoso e simplesmente pensar nos sistemas abaixo como idealizações formais de vários tipos de raciocínio, lógico ou não.

## 24.2 Lógica de Múltiplas Ordenações

Na lógica de primeira ordem, variáveis e quantificadores variam sobre um único domínio. Mas é frequentemente útil ter vários domínios (disjuntos): por exemplo, pode-se querer ter a domínio de números, a domínio de objetos geométricos, a domínio de funções de números para números, a domínio de grupos abelianos, e assim por diante.

A lógica de múltiplas ordenações fornece esse tipo de arcabouço. Começa-se com uma lista de "ordenações"—a "ordenação" de um objeto indica o "domínio" que ele deveria habitar. Tem-se então variáveis e quantificadores para cada ordenação e (geralmente) uma predicado de identidade para cada ordenação. Funções e relações também são "tipadas" pelas ordenações dos objetos que podem receber como argumentos. Caso contrário, mantêm-se as regras usuais da lógica de primeira ordem, com versões das regras de quantificadores repetidas para cada ordenação.

Por exemplo, para estudar relações internacionais, poderíamos escolher uma linguagem com dois tipos de objetos, cidadãos franceses e cidadãos alemães. Poderíamos ter uma relação unária, "bebe vinho", para objetos da primeira ordenação; outra relação unária, "come wurst", para objetos da segunda ordenação; e uma relação binária, "forma um casal multinacional", que recebe dois argumentos, onde o primeiro argumento é da primeira ordenação e o segundo argumento é da segunda ordenação. Se usarmos variáveis $a$, $b$, $c$ para variar sobre cidadãos franceses e $x$, $y$, $z$ para variar sobre cidadãos alemães, então

$$\forall a \, \forall x [(CasadoCom(a, x) \rightarrow (BebeVinho(a) \vee \neg ComeWurst(x))]]$$

afirma que, se algum francês for casado com um alemão, ou o francês bebe vinho ou o alemão não come wurst.

A lógica de múltiplas ordenações pode ser embutida na lógica de primeira ordem de maneira natural, reunindo todos os objetos dos domínios de múltiplas ordenações em um único domínio de primeira ordem, usando símbolos de predicado unários para acompanhar as ordenações e relativizando quantificadores. Por exemplo, a linguagem de primeira ordem correspondente ao exemplo acima teria símbolos de predicado unários "$Alemao$" e "$Frances$", além das outras relações descritas, com os requisitos de ordenação eliminados. Um quantificador ordenado $\forall x\, \varphi$, onde $x$ é a variável da ordenação alemã, traduz-se para

$$\forall x\, (Alemao(x) \to \varphi).$$

Precisamos adicionar axiomas que garantam que as ordenações sejam separadas—por exemplo, $\forall x\, \neg(Alemao(x) \wedge Frances(x))$—, bem como axiomas que garantam que "bebe vinho" só vale de objetos que satisfazem o símbolo de predicado $Frances(x)$, etc. Com essas convenções e axiomas, não é difícil mostrar que sentenças de múltiplas ordenações traduzem-se em sentenças de primeira ordem, e derivações de múltiplas ordenações traduzem-se em derivações de primeira ordem. Além disso, estruturas de múltiplas ordenações "traduzem-se" em estruturas de primeira ordem correspondentes e vice-versa, de modo que também temos um teorema de completude para a lógica de múltiplas ordenações.

## 24.3 Lógica de Segunda Ordem

A linguagem da lógica de segunda ordem permite quantificar não apenas sobre a domínio de indivíduos, mas também sobre relações nesse domínio. Dada uma linguagem de primeira ordem $\mathcal{L}$, para cada $k$ adiciona-se variáveis $R$ que variam sobre relações $k$-árias, e permite-se quantificação sobre essas variáveis. Se $R$ é a variável para uma relação $k$-ária, e $t_1, \ldots, t_k$ são termos ordinários (de primeira ordem), $R(t_1, \ldots, t_k)$ é uma fórmula atômica. Caso contrário, o conjunto de fórmulas é definido exatamente como no caso da lógica de primeira ordem, com cláusulas adicionais para quantificação de segunda ordem. Note que temos apenas a predicado de identidade para termos de primeira ordem: se $R$ e $S$ são variáveis de relação de mesma aridade $k$, podemos definir $R = S$ como uma abreviação de

$$\forall x_1 \ldots \forall x_k\, (R(x_1, \ldots, x_k) \leftrightarrow S(x_1, \ldots, x_k)).$$

As regras para a lógica de segunda ordem simplesmente estendem as regras de quantificadores às novas variáveis de segunda ordem. Aqui, porém, é preciso ter um pouco de cuidado para explicar como essas variáveis interagem com os símbolos de predicado de $\mathcal{L}$, e com fórmulas de $\mathcal{L}$ de modo mais geral. No mínimo, variáveis de relação contam como termos, de modo que temos inferências da forma

$$\varphi(R) \vdash \exists R\, \varphi(R)$$

Mas se $\mathcal{L}$ é a linguagem da aritmética com um símbolo de relação constante $<$, também esperaríamos que a seguinte inferência fosse válida:

$$x < y \vdash \exists R\, R(x, y)$$

ou, para uma dada fórmula $\varphi$,

$$\varphi(x_1, \ldots, x_k) \vdash \exists R\, R(x_1, \ldots, x_k)$$

Mais geralmente, podemos querer permitir inferências da forma

$$\varphi[\lambda \vec{x}.\, \psi(\vec{x})\,/\,R] \vdash \exists R\, \varphi$$

onde $\varphi[\lambda \vec{x}.\, \psi(\vec{x})\,/\,R]$ denota o resultado de substituir cada fórmula atômica da forma $Rt_1, \ldots, t_k$ em $\varphi$ por $\psi(t_1, \ldots, t_k)$. Esta última regra é equivalente a ter um *esquema de compreensão*, isto é, um axioma da forma

$$\exists R\, \forall x_1, \ldots, x_k\, (\varphi(x_1, \ldots, x_k) \leftrightarrow R(x_1, \ldots, x_k)),$$

um para cada fórmula $\varphi$ na linguagem de segunda ordem, em que $R$ não é uma variável livre. (Exercício: mostre que se $R$ for permitida em $\varphi$, esse esquema é inconsistente!)

Quando lógicos se referem aos "axiomas da lógica de segunda ordem", geralmente querem dizer a extensão mínima da lógica de primeira ordem pelas regras de quantificadores de segunda ordem juntamente com o esquema de compreensão. Mas é frequentemente interessante estudar subsistemas mais fracos desses axiomas e regras. Por exemplo, note que em toda a sua generalidade o esquema de axiomas de compreensão é *impredicativo*: ele permite afirmar a existência de uma relação $R(x_1, \ldots, x_k)$ que é "definida" por a fórmula com quantificadores de segunda ordem; e esses quantificadores variam sobre o conjunto de todas essas relações—um conjunto que inclui $R$ em si! Por volta da virada do século XX, uma reação comum ao paradoxo de Russell foi atribuir a culpa a tais definições e evitá-las ao desenvolver os fundamentos da matemática. Se se proíbe o uso de quantificadores de segunda ordem na fórmula $\varphi$, tem-se uma forma *predicativa* de compreensão, que é um pouco mais fraca.

Do ponto de vista semântico, pode-se pensar em uma estrutura de segunda ordem como consistindo em uma estrutura de primeira ordem para a linguagem, juntamente com um conjunto de relações no domínio sobre o qual variem os quantificadores de segunda ordem (mais precisamente, para cada $k$ há um conjunto de relações de aridade $k$). É claro que, se a compreensão estiver incluída no sistema de derivação, então temos o requisito adicional de que há relações suficientes na "parte de segunda ordem" para satisfazer os axiomas de compreensão—caso contrário, o sistema de derivação não é correto! Uma maneira fácil de garantir que há relações suficientes é tomar a parte de segunda ordem como consistindo de *todas* as relações sobre a parte de

primeira ordem. Uma tal estrutura é chamada *plena*, e, de certo modo, é realmente a "estrutura pretendida" para a linguagem. Se restringirmos a atenção a estruturas plenas, temos o que se conhece como a semântica de segunda ordem *plena*. Nesse caso, especificar uma estrutura reduz-se a especificar a parte de primeira ordem, pois o conteúdo da parte de segunda ordem segue disso implicitamente.

Para resumir, há certa ambiguidade ao falar de lógica de segunda ordem. Em termos do sistema de derivação, pode-se ter em mente

1. Um sistema de derivação de segunda ordem "mínimo", juntamente com alguns axiomas de compreensão.

2. O sistema de derivação de segunda ordem "padrão", com compreensão plena.

Em termos da semântica, pode interessar

1. A semântica "fraca", em que a estrutura consiste em uma parte de primeira ordem, juntamente com uma parte de segunda ordem grande o suficiente para satisfazer os axiomas de compreensão.

2. A semântica de segunda ordem "padrão", em que se consideram apenas estruturas plenas.

Quando lógicos não especificam o sistema de derivação ou a semântica que têm em mente, geralmente se referem ao segundo item de cada lista. A vantagem de usar essa semântica é que, como veremos, ela nos dá descrições categóricas de muitas estruturas matemáticas naturais; ao mesmo tempo, o sistema de derivação é bastante forte, e correto para essa semântica. A desvantagem é que o sistema de derivação *não* é completo para a semântica; de fato, *nenhum* sistema de derivação efetivamente dado é completo para a semântica plena de segunda ordem. Por outro lado, veremos que o sistema de derivação *é* completo para a semântica enfraquecida; isso implica que, se uma sentença não for demonstrável, então há *alguma* estrutura, não necessariamente a plena, na qual ela é falsa.

A linguagem da lógica de segunda ordem é bastante rica. Pode-se identificar relações unárias com subconjuntos do domínio, e assim, em particular, pode-se quantificar sobre esses conjuntos; por exemplo, pode-se expressar indução para os números naturais com um único axioma

$$\forall R\,((R(\mathsf{0}) \land \forall x\,(R(x) \to R(x'))) \to \forall x\,R(x)).$$

Se se toma a linguagem da aritmética com os símbolos $\mathsf{0}, \prime, +, \times$ e $<$, pode-se adicionar os seguintes axiomas para descrever seu comportamento:

1. $\forall x\,\neg x' = \mathsf{0}$

2. $\forall x \, \forall y \, (s(x) = s(y) \to x = y)$
3. $\forall x \, (x + 0) = x$
4. $\forall x \, \forall y \, (x + y') = (x + y)'$
5. $\forall x \, (x \times 0) = 0$
6. $\forall x \, \forall y \, (x \times y') = ((x \times y) + x)$
7. $\forall x \, \forall y \, (x < y \leftrightarrow \exists z \, y = (x + z'))$

Não é difícil mostrar que esses axiomas, juntamente com o axioma de indução acima, fornecem uma descrição categórica da estrutura $\mathfrak{N}$, o modelo padrão da aritmética, desde que estejamos usando a semântica plena de segunda ordem. Dada qualquer estrutura $\mathfrak{M}$ na qual esses axiomas são verdadeiros, defina uma função $f$ de $\mathbb{N}$ para o domínio de $\mathfrak{M}$ usando recursão ordinária em $\mathbb{N}$, de modo que $f(0) = 0^{\mathfrak{M}}$ e $f(x + 1) = {}'^{\mathfrak{M}}(f(x))$. Usando indução ordinária em $\mathbb{N}$ e o fato de que os axiomas (1) e (2) valem em $\mathfrak{M}$, vemos que $f$ é injetiva. Para ver que $f$ é sobrejetiva, seja $P$ o conjunto de elementos de $|\mathfrak{M}|$ que estão no alcance de $f$. Como $\mathfrak{M}$ é plena, $P$ está no domínio de segunda ordem. Pela construção de $f$, sabemos que $0^{\mathfrak{M}}$ está em $P$, e que $P$ é fechado sob ${}'^{\mathfrak{M}}$. O fato de que o axioma de indução vale em $\mathfrak{M}$ (em particular, para $P$) garante que $P$ é igual a todo o domínio de primeira ordem de $\mathfrak{M}$. Isso mostra que $f$ é uma bijeção. Mostrar que $f$ é um homomorfismo não é mais difícil, usando indução ordinária em $\mathbb{N}$ repetidamente.

Em termos teórico-conjuntistas, uma função é apenas um tipo especial de relação; por exemplo, uma função unária $f$ pode ser identificada com uma relação binária $R$ que satisfaz $\forall x \, \exists! y \, R(x, y)$. Como resultado, pode-se também quantificar sobre funções. Usando a semântica plena, pode-se então definir a classe de estruturas infinitas como a classe de estruturas $\mathfrak{M}$ para as quais há uma função injetiva do domínio de $\mathfrak{M}$ para um subconjunto próprio de si mesma:

$$\exists f \, (\forall x \, \forall y \, (f(x) = f(y) \to x = y) \wedge \exists y \, \forall x \, f(x) \neq y).$$

A negação dessa sentença define então a classe de estruturas finitas.

Além disso, pode-se definir a classe de ordens bem-fundadas, adicionando o seguinte à definição de uma ordenação linear:

$$\forall P \, (\exists x \, P(x) \to \exists x \, (P(x) \wedge \forall y \, (y < x \to \neg P(y)))).$$

Isso afirma que todo conjunto não vazio tem um elemento mínimo, módulo a identificação de "conjunto" com "relação unária". Como outro exemplo, pode-se expressar a noção de conexidade para grafos, dizendo que não há separação não trivial dos vértices em partes desconectadas:

$$\neg \exists A \, (\exists x \, A(x) \wedge \exists y \, \neg A(y) \wedge \forall w \, \forall z \, ((A(w) \wedge \neg A(z)) \to \neg R(w, z))).$$

Como mais um exemplo, pode-se tentar, como exercício, definir a classe de estruturas finitas cujo domínio tem tamanho par. De modo ainda mais impressionante, pode-se fornecer uma descrição categórica dos números reais como um corpo ordenado completo que contém os racionais.

Em suma, a lógica de segunda ordem é muito mais expressiva do que a lógica de primeira ordem. Essa é a boa notícia; agora a má. Já mencionamos que não há sistema de derivação efetivo que seja completo para a semântica plena de segunda ordem. Para o bem ou para o mal, muitas das propriedades da lógica de primeira ordem estão ausentes, incluindo compacidade e os teoremas de Löwenheim–Skolem.

Por outro lado, se se está disposto a abrir mão da semântica plena de segunda ordem em favor da mais fraca, então o sistema de derivação mínimo de segunda ordem é completo para essa semântica. Em outras palavras, se lemos $\vdash$ como "demonstra no sistema mínimo" e $\models$ como "implica logicamente na semântica fraca", podemos mostrar que sempre que $\Gamma \models \varphi$, então $\Gamma \vdash \varphi$. Se se quer incluir axiomas específicos de compreensão no sistema de derivação, é preciso restringir a semântica a estruturas de segunda ordem que satisfaçam esses axiomas: por exemplo, se $\Delta$ consiste em um conjunto de axiomas de compreensão (possivelmente todos eles), temos que, se $\Gamma \cup \Delta \models \varphi$, então $\Gamma \cup \Delta \vdash \varphi$. Em particular, se $\varphi$ não for demonstrável usando os axiomas de compreensão que estamos considerando, então há um modelo de $\neg\varphi$ no qual esses axiomas de compreensão ainda assim valem.

A maneira mais fácil de ver que o teorema de completude vale para a semântica fraca é pensar na lógica de segunda ordem como uma lógica de múltiplas ordenações, da seguinte forma. Uma ordenação é interpretada como o domínio ordinário de "primeira ordem", e então, para cada $k$, temos a domínio de "relações de aridade $k$." Tomamos a linguagem com símbolos de relação incorporados "$verd_k(R, x_1, \ldots, x_k)$", destinados a afirmar que $R$ vale de $x_1$, $\ldots$, $x_k$, onde $R$ é uma variável da ordenação "relação $k$-ária" e $x_1$, $\ldots$, $x_k$ são objetos da ordenação de primeira ordem.

Com essa identificação, a semântica fraca de segunda ordem é essencialmente a semântica usual da lógica de múltiplas ordenações; e já observamos que a lógica de múltiplas ordenações pode ser embutida na lógica de primeira ordem. Módulo as traduções de ida e volta, então, a concepção mais fraca de lógica de segunda ordem é realmente uma forma disfarçada de lógica de primeira ordem, em que o domínio contém tanto "objetos" quanto "relações" governados pelos axiomas apropriados.

## 24.4 Lógica de Ordem Superior

Passar da lógica de primeira ordem para a de segunda ordem nos permitiu falar sobre conjuntos de objetos no domínio de primeira ordem, dentro da linguagem formal. Por que parar aí? Por exemplo, a lógica de terceira ordem

deveria nos permitir lidar com conjuntos de conjuntos de objetos, ou talvez até conjuntos que contenham tanto objetos quanto conjuntos de objetos. E a lógica de quarta ordem nos permitirá falar sobre conjuntos de objetos desse tipo. Como se pode imaginar, pode-se iterar essa ideia arbitrariamente.

Na prática, a lógica de ordem superior é frequentemente formulada em termos de funções em vez de relações. (Módulo as identificações naturais, essa diferença é inessencial.) Dadas algumas "ordenações" básicas $A$, $B$, $C$, ... (que agora chamaremos de "tipos"), podemos criar novos estipulando

> Se $\sigma$ e $\tau$ são tipos finitos, então $\sigma \to \tau$ também o é.

Pense nos tipos como "rótulos" sintáticos que classificam os objetos que queremos em nosso domínio; $\sigma \to \tau$ descreve aqueles objetos que são funções que levam objetos de tipo $\sigma$ a objetos de tipo $\tau$. Por exemplo, podemos querer ter um tipo $\Omega$ de valores de verdade, "verdadeiro" e "falso", e um tipo $\mathbb{N}$ de números naturais. Nesse caso, pode-se pensar em objetos de tipo $\mathbb{N} \to \Omega$ como relações unárias, ou subconjuntos de $\mathbb{N}$; objetos de tipo $\mathbb{N} \to \mathbb{N}$ são funções de números naturais para números naturais; e objetos de tipo $(\mathbb{N} \to \mathbb{N}) \to \mathbb{N}$ são "funcionais", isto é, funções de tipo superior que levam funções a números.

Como no caso da lógica de segunda ordem, pode-se pensar na lógica de ordem superior como uma espécie de lógica de múltiplas ordenações, em que há uma ordenação para cada tipo de objeto que queremos considerar. Mas é usualmente mais claro simplesmente definir a sintaxe da lógica de tipos superiores a partir dos fundamentos. Por exemplo, podemos definir um conjunto de tipos finitos indutivamente, da seguinte forma:

1. $\mathbb{N}$ é um tipo finito.
2. Se $\sigma$ e $\tau$ são tipos finitos, então $\sigma \to \tau$ também o é.
3. Se $\sigma$ e $\tau$ são tipos finitos, então $\sigma \times \tau$ também o é.

Intuitivamente, $\mathbb{N}$ denota o tipo dos números naturais, $\sigma \to \tau$ denota o tipo de funções de $\sigma$ para $\tau$, e $\sigma \times \tau$ denota o tipo de pares de objetos, um de $\sigma$ e outro de $\tau$. Podemos então definir um conjunto de termos indutivamente, da seguinte forma:

1. Para cada tipo $\sigma$, há um estoque de variáveis $x$, $y$, $z$, ... de tipo $\sigma$
2. $0$ é um termo de tipo $\mathbb{N}$
3. $S$ (sucessor) é um termo de tipo $\mathbb{N} \to \mathbb{N}$
4. Se $s$ é um termo de tipo $\sigma$, e $t$ é um termo de tipo $\mathbb{N} \to (\sigma \to \sigma)$, então $R_{st}$ é um termo de tipo $\mathbb{N} \to \sigma$

5. Se $s$ é um termo de tipo $\tau \to \sigma$ e $t$ é um termo de tipo $\tau$, então $s(t)$ é um termo de tipo $\sigma$
6. Se $s$ é um termo de tipo $\sigma$ e $x$ é uma variável de tipo $\tau$, então $\lambda x.\, s$ é um termo de tipo $\tau \to \sigma$.
7. Se $s$ é um termo de tipo $\sigma$ e $t$ é um termo de tipo $\tau$, então $\langle s, t \rangle$ é um termo de tipo $\sigma \times \tau$.
8. Se $s$ é um termo de tipo $\sigma \times \tau$, então $p_1(s)$ é um termo de tipo $\sigma$ e $p_2(s)$ é um termo de tipo $\tau$.

Intuitivamente, $R_{st}$ denota a função definida recursivamente por

$$R_{st}(0) = s$$
$$R_{st}(x+1) = t(x, R_{st}(x)),$$

$\langle s, t \rangle$ denota o par cuja primeira componente é $s$ e cuja segunda componente é $t$, e $p_1(s)$ e $p_2(s)$ denotam o primeiro e o segundo elementos ("projeções") de $s$. Finalmente, $\lambda x.\, s$ denota a função $f$ definida por

$$f(x) = s$$

para qualquer $x$ de tipo $\sigma$; assim o item (6) nos dá uma forma de compreensão, permitindo-nos definir funções usando termos. As fórmulas são construídas a partir de afirmações de predicado de identidade $s = t$ entre termos do mesmo tipo, dos conectivos proposicionais usuais e da quantificação de ordem superior. Pode-se então tomar os axiomas do sistema como as equações básicas que governam os termos definidos acima, juntamente com as regras usuais da lógica com quantificadores e predicado de identidade.

Se se aumenta o sistema de tipos finitos com um tipo $\Omega$ de valores de verdade, é preciso incluir axiomas que governem seu uso também. De fato, se se for astuto, pode-se eliminar fórmulas complexas inteiramente, substituindo-as por termos de tipo $\Omega$! O sistema de prova pode então ser modificado de acordo. O resultado é essencialmente a *teoria simples dos tipos* apresentada por Alonzo Church na década de 1930.

Como no caso da lógica de segunda ordem, há diferentes versões de semântica de tipos superiores que se pode querer usar. Na versão completa, variáveis de tipo $\sigma \to \tau$ variam sobre o conjunto de *todas* as funções dos objetos de tipo $\sigma$ para objetos de tipo $\tau$. Como se pode imaginar, essa semântica é forte demais para admitir um sistema de derivação completo e efetivo. Mas pode-se considerar uma semântica mais fraca, em que a estrutura consiste em conjuntos de elementos $T_\tau$ para cada tipo $\tau$, juntamente com operações apropriadas para aplicação, projeção, etc. Se os detalhes forem desenvolvidos corretamente, pode-se obter teoremas de completude para os tipos de sistemas de derivação descritos acima.

A lógica de ordem superior é atraente porque fornece um arcabouço no qual podemos embutir boa parte da matemática de maneira natural: a partir de $\mathbb{N}$, pode-se definir números reais, funções contínuas e assim por diante. É também particularmente atraente no contexto da lógica intuicionista, pois os tipos têm interpretações "construtivas" claras. De fato, pode-se desenvolver versões construtivas da semântica de tipos superiores (baseadas na lógica intuicionista, em vez da clássica) que esclarecem bastante essas interpretações construtivas e são, em muitos aspectos, mais interessantes do que as contrapartes clássicas.

## 24.5 Lógica Intuicionista

Em contraste com a lógica de segunda ordem e de ordem superior, a lógica intuicionista de primeira ordem representa uma restrição da versão clássica, destinada a modelar um tipo de raciocínio mais "construtivo". Os exemplos a seguir podem ilustrar algumas das motivações subjacentes.

Suponha que alguém se aproximasse de você um dia e anunciasse que havia determinado um número natural $x$, com a propriedade de que se $x$ é primo, a hipótese de Riemann é verdadeira, e se $x$ é composto, a hipótese de Riemann é falsa. Ótimas notícias! Se a hipótese de Riemann é verdadeira ou não é uma das grandes questões em aberto da matemática, e aqui parecem ter reduzido o problema a um cálculo, isto é, à determinação de se um número específico é primo ou não.

Qual é o valor mágico de $x$? Eles o descrevem assim: $x$ é o número natural que é igual a 7 se a hipótese de Riemann é verdadeira, e 9 caso contrário.

Com raiva, você exige seu dinheiro de volta. De um ponto de vista clássico, a descrição acima de fato determina um valor único de $x$; mas o que você realmente quer é um valor de $x$ que seja dado *explicitamente*.

Para tomar outro exemplo, talvez menos artificial, considere a seguinte questão. Sabemos que é possível elevar um número irracional a uma potência racional e obter um resultado racional. Por exemplo, $\sqrt{2}^2 = 2$. O que é menos claro é se é possível elevar um número irracional a uma potência *irracional* e obter um resultado racional. O seguinte teorema responde afirmativamente:

**Teorema 24.1.** *Existem números irracionais $a$ e $b$ tais que $a^b$ é racional.*

*Prova.* Considere $\sqrt{2}^{\sqrt{2}}$. Se isto é racional, terminamos: podemos tomar $a = b = \sqrt{2}$. Caso contrário, é irracional. Então temos

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2,$$

que é certamente racional. Assim, neste caso, tome $a$ como $\sqrt{2}^{\sqrt{2}}$, e $b$ como $\sqrt{2}$.□

Isso constitui uma prova válida? A maioria dos matemáticos sente que sim. Mas, novamente, há algo um pouco insatisfatório aqui: provamos a existência de um par de números reais com uma certa propriedade, sem poder dizer *qual* par de números é. É possível provar o mesmo resultado, mas de tal forma que o par $a$, $b$ *é* dado na prova: tome $a = \sqrt{3}$ e $b = \log_3 4$. Então

$$a^b = \sqrt{3}^{\log_3 4} = 3^{1/2 \cdot \log_3 4} = (3^{\log_3 4})^{1/2} = 4^{1/2} = 2,$$

pois $3^{\log_3 x} = x$.

A lógica intuicionista foi concebida para modelar um tipo de raciocínio no qual movimentos como o da primeira prova são proibidos. Provar a existência de um $x$ que satisfaz $\varphi(x)$ significa que se deve fornecer um $x$ específico e uma prova de que ele satisfaz $\varphi$, como na segunda prova. Provar que $\varphi$ ou $\psi$ vale requer que se possa provar um ou outro.

Formalmente falando, a lógica intuicionista de primeira ordem é o que se obtém se se restringe um sistema de derivação para a lógica de primeira ordem de certa maneira. Similarmente, há versões intuicionistas da lógica de segunda ou de ordem superior. Do ponto de vista matemático, estes são apenas sistemas dedutivos formais, mas, como já observado, são destinados a modelar um tipo de raciocínio matemático. Pode-se tomar isso como o tipo de raciocínio justificado por uma certa visão filosófica da matemática (como o intuicionismo de Brouwer); pode-se tomá-lo como um tipo de raciocínio matemático mais "concreto" e satisfatório (na linha do construtivismo de Bishop); e pode-se discutir se a descrição formal captura ou não a motivação informal. Mas quaisquer que sejam as posições filosóficas que possamos ter, podemos estudar a lógica intuicionista como uma lógica formalmente apresentada; e por quaisquer razões, muitos lógicos matemáticos acham interessante fazê-lo.

Há uma interpretação construtiva informal dos conectivos intuicionistas, usualmente conhecida como interpretação BHK (em homenagem a Brouwer, Heyting e Kolmogorov). Ela funciona assim: uma prova de $\varphi \wedge \psi$ consiste em uma prova de $\varphi$ emparelhada com uma prova de $B$; uma prova de $\varphi \vee \psi$ consiste em uma prova de $\varphi$, ou uma prova de $\psi$, onde temos informação explícita sobre qual é o caso; uma prova de $\varphi \to \psi$ consiste em um procedimento que transforma uma prova de $\varphi$ em uma prova de $\psi$; uma prova de $\forall x\, \varphi(x)$ consiste em um procedimento que retorna uma prova de $\varphi(x)$ para qualquer valor de $x$; e uma prova de $\exists x\, \varphi(x)$ consiste em um valor de $x$, juntamente com uma prova de que esse valor satisfaz $\varphi$. Pode-se descrever a interpretação em termos computacionais conhecidos como o "isomorfismo de Curry–Howard" ou o "paradigma fórmulas-como-tipos": pense em a fórmula como especificando um certo tipo de dado, e provas como objetos computacionais desses tipos de dados que nos permitem ver que a fórmula correspondente é verdadeira.

A lógica intuicionista é frequentemente pensada como a lógica clássica "menos" a lei do terceiro excluído. O seguinte teorema torna isso mais preciso.

**Teorema 24.2.** *Intuicionisticamente, os seguintes esquemas de axiomas são equivalentes:*

1. $(\neg\varphi \to \bot) \to \varphi$.
2. $\varphi \vee \neg\varphi$
3. $\neg\neg\varphi \to \varphi$

Obter instâncias de um esquema a partir de qualquer um dos outros é um bom exercício em lógica intuicionista.

Os primeiros sistemas dedutivos para a lógica proposicional intuicionista, apresentados como formalizações do intuicionismo de Brouwer, são devidos, independentemente, a Kolmogorov, Glivenko e Heyting. A primeira formalização da lógica intuicionista de primeira ordem (e partes da matemática intuicionista) é devida a Heyting. Embora vários esquemas válidos clássicamente não sejam válidos intuicionisticamente, muitos o são.

A *tradução de dupla negação* descreve uma relação importante entre a lógica clássica e a intuicionista. Ela é definida indutivamente da seguinte forma (pense em $\varphi^N$ como a tradução "intuicionista" da fórmula clássica $\varphi$):

$$\begin{aligned}
\varphi^N &\equiv \neg\neg\varphi \quad \text{para fórmulas atômicas } \varphi \\
(\varphi \wedge \psi)^N &\equiv (\varphi^N \wedge \psi^N) \\
(\varphi \vee \psi)^N &\equiv \neg\neg(\varphi^N \vee \psi^N) \\
(\varphi \to \psi)^N &\equiv (\varphi^N \to \psi^N) \\
(\forall x\, \varphi)^N &\equiv \forall x\, \varphi^N \\
(\exists x\, \varphi)^N &\equiv \neg\neg\exists x\, \varphi^N
\end{aligned}$$

Kolmogorov e Glivenko tiveram versões dessa tradução para a lógica proposicional; para a lógica de predicados, é devida a Gödel e Gentzen, independentemente. Temos

**Teorema 24.3.** 1. *$\varphi \leftrightarrow \varphi^N$ é demonstrável classicamente*

2. *Se $\varphi$ é demonstrável classicamente, então $\varphi^N$ é demonstrável intuicionisticamente.*

Podemos agora imaginar o seguinte diálogo. Matemático clássico: "Provei $\varphi$!" Matemático intuicionista: "Sua prova não é válida. O que você realmente provou é $\varphi^N$." Matemático clássico: "Tudo bem para mim!" Quanto ao matemático clássico, o intuicionista está apenas sendo minucioso, pois os dois são equivalentes. Mas o intuicionista insiste que há uma diferença.

Note que a tradução acima diz respeito apenas à lógica pura; ela não aborda a questão de quais são os axiomas *não lógicos* adequados para a matemática clássica e intuicionista, ou qual é a relação entre eles. Mas a seguinte extensão ligeira do teorema acima fornece alguma informação útil:

**Teorema 24.4.** *Se $\Gamma$ prova $\varphi$ classicamente, então $\Gamma^N$ prova $\varphi^N$ intuicionisticamente.*

Em outras palavras, se $\varphi$ é demonstrável a partir de algumas hipóteses classicamente, então $\varphi^N$ é demonstrável a partir de suas traduções de dupla negação.

Para mostrar que uma sentença ou fórmula proposicional é intuicionisticamente válida, basta fornecer uma prova. Mas como se pode mostrar que ela não é válida? Para esse propósito, precisamos de uma semântica que seja correta e, de preferência, completa. Uma semântica devida a Kripke se encaixa bem.

Podemos jogar o mesmo jogo que fizemos para a lógica clássica: definir a semântica e provar correção e completude. Vale a pena, no entanto, notar a seguinte distinção. No caso da lógica clássica, a semântica era a "óbvia", num sentido implícito no significado dos conectivos. Embora se possa fornecer alguma motivação intuitiva para a semântica de Kripke, esta não oferece o mesmo sentimento de inevitabilidade. Além disso, a noção de estrutura clássica é uma noção matemática natural, de modo que podemos ou tomar a noção de estrutura como uma ferramenta para estudar a lógica clássica de primeira ordem, ou tomar a lógica clássica de primeira ordem como uma ferramenta para estudar estruturas matemáticas. Em contraste, as estruturas de Kripke só podem ser vistas como um construto lógico; elas não parecem ter interesse matemático independente.

Uma estrutura de Kripke $\mathfrak{M} = \langle W, R, V \rangle$ para uma linguagem proposicional consiste em um conjunto $W$, uma ordem parcial $R$ em $W$ com um menor membro, e uma atribuição "monótona" de variáveis proposicionais aos membros de $W$. A intuição é que os membros de $W$ representam "mundos", ou "estados de conhecimento"; um elemento $v \geq u$ representa um "possível estado futuro" de $u$; e as variáveis proposicionais atribuídas a $u$ são as proposições que se sabe serem verdadeiras no estado $u$. A relação de forçamento $\mathfrak{M}, w \Vdash \varphi$ estende essa relação a fórmulas arbitrárias na linguagem; leia $\mathfrak{M}, w \Vdash \varphi$ como "$\varphi$ é verdadeira no estado $w$." A relação é definida indutivamente, da seguinte forma:

1. $\mathfrak{M}, w \Vdash p_i$ se, e somente se, $p_i$ é uma das variáveis proposicionais atribuídas a $w$.

2. $\mathfrak{M}, w \nVdash \bot$.

3. $\mathfrak{M}, w \Vdash (\varphi \wedge \psi)$ se, e somente se, $\mathfrak{M}, w \Vdash \varphi$ e $\mathfrak{M}, w \Vdash \psi$.

4. $\mathfrak{M}, w \Vdash (\varphi \vee \psi)$ se, e somente se, $\mathfrak{M}, w \Vdash \varphi$ ou $\mathfrak{M}, w \Vdash \psi$.

5. $\mathfrak{M}, w \Vdash (\varphi \to \psi)$ se, e somente se, sempre que $w' \geq w$ e $\mathfrak{M}, w' \Vdash \varphi$, então $\mathfrak{M}, w' \Vdash \psi$.

É um bom exercício tentar mostrar que $\neg(p \wedge q) \to (\neg p \vee \neg q)$ não é intuicionisticamente válida, preparando uma estrutura de Kripke que forneça um contraexemplo.

## 24.6 Lógicas Modais

Considere o seguinte exemplo de uma sentença condicional:

> Se Jeremy está sozinho naquela sala, então ele está bêbado, nu e dançando nas cadeiras.

Este é um exemplo de uma asserção condicional que pode ser materialmente verdadeira, mas ainda assim enganosa, pois parece sugerir que há um vínculo mais forte entre o antecedente e a conclusão do que simplesmente o fato de que ou o antecedente é falso ou a conclusão é verdadeira. Ou seja, a formulação sugere que a afirmação não é apenas verdadeira neste mundo particular (onde pode ser trivialmente verdadeira, porque Jeremy não está sozinho na sala), mas que, além disso, a conclusão *teria sido* verdadeira *se* o antecedente tivesse sido verdadeiro. Em outras palavras, pode-se tomar a asserção como significando que a afirmação é verdadeira não apenas neste mundo, mas em qualquer mundo "possível"; ou que ela é *necessariamente* verdadeira, em oposição a ser apenas verdadeira neste mundo particular.

A lógica modal foi concebida para dar sentido a esse tipo de necessidade. Obtém-se a lógica proposicional modal a partir da lógica proposicional ordinária adicionando um operador caixa; isto é, se $\varphi$ é a fórmula, então $\Box\varphi$ também o é. Intuitivamente, $\Box\varphi$ afirma que $\varphi$ é *necessariamente* verdadeira, ou verdadeira em qualquer mundo possível. $\Diamond\varphi$ é usualmente tomada como abreviação de $\neg\Box\neg\varphi$, e pode ser lida como afirmando que $\varphi$ é *possivelmente* verdadeira. É claro que a modalidade também pode ser adicionada à lógica de predicados.

Estruturas de Kripke podem ser usadas para fornecer uma semântica para a lógica modal; de fato, Kripke projetou essa semântica tendo a lógica modal em mente. Em vez de restringir a ordens parciais, de modo mais geral tem-se um conjunto de "mundos possíveis", $P$, e uma relação binária de "acessibilidade" $R(x, y)$ entre mundos. Intuitivamente, $R(p, q)$ afirma que o mundo $q$ é compatível com $p$; isto é, se estamos "em" o mundo $p$, temos que considerar a possibilidade de que o mundo pudesse ter sido como $q$.

A lógica modal é às vezes chamada de lógica "intensional", em oposição a uma "extensional". A semântica pretendida para uma lógica extensional,

como a lógica clássica, refere-se apenas a um único mundo, o "atual"; enquanto a semântica para uma lógica "intensional" depende de uma ontologia mais elaborada. Além de estruturar a necessidade, pode-se usar a modalidade para estruturar outras construções linguísticas, reinterpretando $\Box$ e $\Diamond$ de acordo com a aplicação. Por exemplo:

1. Na lógica de demonstrabilidade, $\Box\varphi$ é lida como "$\varphi$ é demonstrável" e $\Diamond\varphi$ é lida como "$\varphi$ é consistente".

2. Na lógica epistêmica, pode-se ler $\Box\varphi$ como "eu sei $\varphi$" ou "eu acredito em $\varphi$".

3. Na lógica temporal, pode-se ler $\Box\varphi$ como "$\varphi$ é sempre verdadeira" e $\Diamond\varphi$ como "$\varphi$ é às vezes verdadeira".

Gostaríamos de aumentar a lógica com regras e axiomas que lidem com modalidade. Por exemplo, o sistema **S4** consiste nos axiomas e regras ordinários da lógica proposicional, juntamente com os seguintes axiomas:

$$\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$$
$$\Box\varphi \to \varphi$$
$$\Box\varphi \to \Box\Box\varphi$$

assim como uma regra, "de $\varphi$ conclua $\Box\varphi$." **S5** adiciona o seguinte axioma:

$$\Diamond\varphi \to \Box\Diamond\varphi$$

Variações desses axiomas podem ser adequadas para diferentes aplicações; por exemplo, S5 é usualmente tomado para caracterizar a noção de necessidade lógica. E o aspecto agradável é que se pode usualmente encontrar uma semântica para a qual o sistema de derivação é correto e completo, restringindo a relação de acessibilidade nas estruturas de Kripke de maneiras naturais. Por exemplo, **S4** corresponde à classe de estruturas de Kripke em que a relação de acessibilidade é reflexiva e transitiva. **S5** corresponde à classe de estruturas de Kripke em que a relação de acessibilidade é *universal*, isto é, todo mundo é acessível a partir de qualquer outro; assim $\Box\varphi$ vale se, e somente se, $\varphi$ vale em todo mundo.

## 24.7 Outras Lógicas

Como você já deve ter percebido, não é difícil projetar uma nova lógica. Você também pode criar a sua própria sintaxe, montar um sistema dedutivo e elaborar uma semântica para acompanhá-la. Talvez você tenha que ser um pouco esperto se quiser que o sistema de derivação seja completo para a semântica, e pode exigir algum esforço convencer o mundo em geral de que a sua lógica

é realmente interessante. Mas, em troca, você pode desfrutar de horas de diversão sadia, explorando as propriedades matemáticas e computacionais da sua lógica.

As últimas décadas testemunharam uma verdadeira explosão de lógicas formais. A lógica difusa é projetada para modelar o raciocínio sobre propriedades vagas. A lógica probabilística é projetada para modelar o raciocínio sobre a incerteza. As lógicas *default* (de exceções) e as lógicas não monotônicas são projetadas para modelar formas revogáveis de raciocínio, isto é, inferências "razoáveis" que podem mais tarde ser derrubadas diante de novas informações. Há lógicas epistêmicas, projetadas para modelar o raciocínio sobre o conhecimento; lógicas causais, projetadas para modelar o raciocínio sobre relações causais; e até mesmo lógicas "deônticas", que são projetadas para modelar o raciocínio sobre obrigações morais e éticas. Dependendo de a principal motivação para a introdução desses sistemas ser filosófica, matemática ou computacional, você pode encontrar estudos sobre essas criaturas sob a rubrica de lógica matemática, lógica filosófica, inteligência artificial, ciência cognitiva ou outro lugar.

A lista não tem fim, e as possibilidades parecem infinitas. Talvez nunca alcancemos o sonho de Leibniz de reduzir toda a razão humana a cálculo — mas isso não pode nos impedir de tentar.

# Parte IV

# Model Theory

Material on model theory is incomplete and experimental. It is currently simply an adaptation of Aldo Antonelli's notes on model theory, less those topics covered in the part on first-order logic (theories, completeness, compactness). It requires much more introduction, motivation, and explanation, as well as exercises, to be useful for a textbook. Andy Arana is at planning to work on this part specifically (issue #65).

## Capítulo 25

# Basics of Model Theory

## Capítulo 26

# Models of Arithmetic

## Capítulo 27

# The Interpolation Theorem

## Capítulo 28

# Lindström's Theorem

# Parte V

# Computability

This part is based on Jeremy Avigad's notes on computability theory. Only the chapter on recursive functions contains exercises yet, and everything could stand to be expanded with motivation, examples, details, and exercises.

# Capítulo 29

# Recursive Functions

These are Jeremy Avigad's notes on recursive functions, revised and expanded by Richard Zach. This chapter does contain some exercises, and can be included independently to provide the basis for a discussion of arithmetization of syntax.

# Capítulo 30

# Computability Theory

Material in this chapter should be reviewed and expanded. In particular, there are no exercises yet.

# Parte VI

# Máquinas de Turing

# Capítulo 31

# Computações de Máquinas de Turing

## 31.1 Introdução

O que significa dizer que uma função, digamos, de $\mathbb{N}$ para $\mathbb{N}$ é *computável*? Entre as primeiras respostas, e a mais conhecida, está a de que uma função é computável se puder ser computada por uma máquina de Turing. Essa noção foi apresentada por Alan Turing em 1936. As máquinas de Turing são um exemplo de *modelo de computação*—uma maneira matematicamente precisa de definir a ideia de um "procedimento computacional." O que exatamente isso significa é debatido, mas há amplo consenso de que as máquinas de Turing são uma forma de especificar procedimentos computacionais. Embora o termo "máquina de Turing" evoque a imagem de uma máquina física com partes móveis, estritamente falando uma máquina de Turing é um construto puramente matemático e, como tal, idealiza a ideia de um procedimento computacional. Por exemplo, não impomos restrição alguma aos requisitos de tempo ou memória de uma máquina de Turing: máquinas de Turing podem computar algo mesmo que a computação exija mais espaço de armazenamento ou mais passos do que há átomos no universo.

Talvez seja melhor pensar em uma máquina de Turing como um programa para um tipo especial de mecanismo imaginário. Esse mecanismo consiste em uma *fita* e uma *cabeça de leitura-escrita*. Na nossa versão das máquinas de Turing, a fita é infinita em uma direção (à direita) e é dividida em *quadrados*, cada um dos quais pode conter um símbolo de um *alfabeto* finito. Esses alfabetos podem conter qualquer número de símbolos diferentes, mas nos contentaremos em geral com três: $\triangleright$, 0 e 1. Quando o mecanismo é iniciado, a fita está vazia (ou seja, cada quadrado contém o símbolo 0), exceto o quadrado mais à esquerda, que contém $\triangleright$, e um número finito de quadrados que contêm a *entrada*. A qualquer momento, o mecanismo está em um de um número finito de *estados*. No início, a cabeça examina o quadrado mais à esquerda e

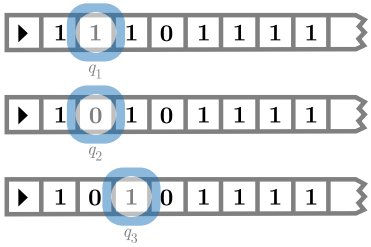



Figura 31.1: Uma máquina de Turing executando seu programa.

em um *estado inicial* especificado. A cada passo da execução do mecanismo, o conteúdo do quadrado atualmente examinado, junto com o estado em que o mecanismo se encontra e o programa da máquina de Turing, determinam o que acontece em seguida. O programa da máquina de Turing é dado por uma função parcial que recebe como entrada um estado $q$ e um símbolo $\sigma$ e produz uma tripla $\langle q', \sigma', D\rangle$. Sempre que o mecanismo está no estado $q$ e lê o símbolo $\sigma$, substitui o símbolo no quadrado atual por $\sigma'$, a cabeça move-se à esquerda, à direita ou permanece no lugar conforme $D$ seja $L$, $R$ ou $N$, e o mecanismo passa ao estado $q'$.

Por exemplo, considere a situação em Figura 31.1. A parte visível da fita da máquina de Turing contém o símbolo de fim de fita $\triangleright$ no quadrado mais à esquerda, seguido de três 1's, um 0 e mais quatro 1's. A cabeça está lendo o terceiro quadrado da esquerda, que contém um 1, e está no estado $q_1$—dizemos que "a máquina está lendo um 1 no estado $q_1$." Se o programa da máquina de Turing retornar, para a entrada $\langle q_1, 1\rangle$, a tripla $\langle q_2, 0, N\rangle$, a máquina substituiria o 1 no terceiro quadrado por um 0, deixaria a cabeça de leitura/escrita onde está e passaria ao estado $q_2$. Se então o programa retornar $\langle q_3, 0, R\rangle$ para a entrada $\langle q_2, 0\rangle$, a máquina sobrescreveria o 0 com outro 0 (efetivamente, deixando inalterado o conteúdo da fita sob a cabeça de leitura/escrita), moveria um quadrado à direita e entraria no estado $q_3$. E assim por diante.

Dizemos que a máquina *para* quando encontra algum estado, $q_n$, e símbolo, $\sigma$, tais que não há instrução para $\langle q_n, \sigma\rangle$, ou seja, a função de transição para a entrada $\langle q_n, \sigma\rangle$ é indefinida. Em outras palavras, a máquina não tem instrução a executar e, nesse ponto, cessa a operação. A parada às vezes é representada por um estado de parada específico $h$. Isso será demonstrado com mais detalhes adiante.

A beleza do artigo de Turing, "On computable numbers," está em que ele apresenta não só uma definição formal, mas também um argumento de que a definição captura a noção intuitiva de computabilidade. Pela definição, deve ficar claro que toda função computável por uma máquina de Turing é computável no sentido intuitivo. Turing oferece três tipos de argumento de que o inverso é verdadeiro, ou seja, que toda função que naturalmente conside-

raríamos computável é computável por tal máquina. São eles (nas palavras de Turing):

1. Um apelo direto à intuição.

2. Uma prova da equivalência de duas definições (caso a nova definição tenha maior apelo intuitivo).

3. Dar exemplos de grandes classes de números que são computáveis.

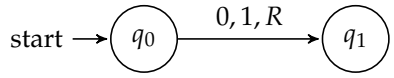
Nosso objetivo é tentar definir a noção de computabilidade "em princípio," ou seja, sem levar em conta limitações práticas de tempo e espaço. Claro, com a definição mais ampla de computabilidade em vigor, pode-se então considerar computação com recursos limitados; isso forma o cerne do assunto conhecido como "complexidade computacional."

**Observações históricas** Alan Turing inventou as máquinas de Turing em 1936. Embora seu interesse na época fosse a decidibilidade da lógica de primeira ordem, o artigo tem sido descrito como um trabalho definitivo sobre os fundamentos do projeto de computadores. No artigo, Turing concentra-se em números reais computáveis, ou seja, números reais cujas expansões decimais são computáveis; mas observa que não é difícil adaptar suas noções a funções computáveis sobre os números naturais, e assim por diante. Note que isso foi cinco anos inteiros antes de o primeiro computador de propósito geral em funcionamento ser construído em 1941 (pelo alemão Konrad Zuse na sala de estar dos pais), sete anos antes de Turing e seus colegas em Bletchley Park construírem o Colossus que quebrava códigos (1943), nove anos antes do ENIAC americano (1945), doze anos antes do primeiro computador britânico de propósito geral—a Manchester Small-Scale Experimental Machine—ser construída em Manchester (1948), e treze anos antes dos americanos testarem o BINAC (1949). A Manchester SSEM tem a distinção de ser o primeiro computador com programa armazenado—as máquinas anteriores tinham de ser recabeada manualmente para cada nova tarefa.

## 31.2 Representando Máquinas de Turing

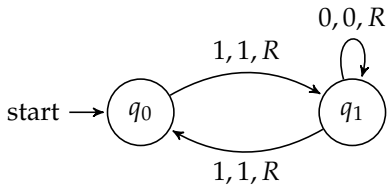
As máquinas de Turing podem ser representadas visualmente por *diagramas de estado*. Os diagramas são compostos por células de estado conectadas por setas. Sem surpresa, cada célula de estado representa um estado da máquina. Cada seta representa uma instrução que pode ser executada a partir desse estado, com as especificações da instrução escritas acima ou abaixo da seta apropriada. Considere a seguinte máquina, que tem apenas dois estados internos,

$q_0$ e $q_1$, e uma instrução:




Lembre-se de que a máquina de Turing tem uma cabeça de leitura/escrita e uma fita com a entrada escrita nela. A instrução pode ser lida como *se lendo um* 0 *no estado* $q_0$*, escreva um* 1*, mova-se à direita, e vá para o estado* $q_1$. Isto é equivalente à função de transição que mapeia $\langle q_0, 0\rangle$ em $\langle q_1, 1, R\rangle$.

**Exemplo 31.1.** *Máquina Par*: A seguinte máquina de Turing para se, e somente se, houver um número par de 1 na fita (sob a suposição de que todos os 1 vêm antes do primeiro 0 na fita).




O diagrama de estado corresponde à seguinte função de transição:

$$\delta(q_0, 1) = \langle q_1, 1, R\rangle,$$
$$\delta(q_1, 1) = \langle q_0, 1, R\rangle,$$
$$\delta(q_1, 0) = \langle q_1, 0, R\rangle$$

A máquina acima para apenas quando a entrada é um número par de traços. Caso contrário, a máquina (teoricamente) continua a operar indefinidamente. Para qualquer máquina e entrada, é possível rastrear as *configurações* da máquina a fim de determinar a saída. Daremos uma definição formal de configurações mais adiante. Por enquanto, podemos pensar intuitivamente nas configurações como uma série de diagramas que mostram o estado da máquina em qualquer instante durante a operação. As configurações mostram o conteúdo da fita, o estado da máquina e a posição da cabeça de leitura/escrita.

Vamos rastrear as configurações da máquina par se ela for iniciada com uma entrada de quatro 1. Nesse caso, esperamos que a máquina pare. Em seguida, executaremos a máquina com uma entrada de três 1, na qual a máquina rodará para sempre.

A máquina inicia no estado $q_0$, examinando o 1 mais à esquerda. Podemos representar o estado inicial da máquina da seguinte forma:

$$\triangleright 1_0 1110\ldots$$

A configuração acima é direta. Como se pode ver, a máquina inicia no estado um, examinando o 1 mais à esquerda. Isso é representado por um subscrito do nome do estado no primeiro 1. A instrução aplicável neste ponto é $\delta(q_0, 1) = \langle q_1, 1, R\rangle$, e assim a máquina move-se à direita na fita e muda para o estado $q_1$.

$$\triangleright 1 1_1 1 1 0 \ldots$$

Como a máquina está agora no estado $q_1$ examinando um 1, temos que "seguir" a instrução $\delta(q_1, 1) = \langle q_0, 1, R\rangle$. Isso resulta na configuração

$$\triangleright 1 1 1_0 1 0 \ldots$$

À medida que a máquina continua, as regras são aplicadas novamente na mesma ordem, resultando nas duas configurações a seguir:

$$\triangleright 1 1 1 1_1 0 \ldots$$

$$\triangleright 1 1 1 1 0_0 \ldots$$

A máquina está agora no estado $q_0$ examinando um 0. Com base no diagrama de transição, podemos ver facilmente que não há nenhuma instrução a ser executada, e portanto a máquina parou. Isso significa que a entrada foi aceita.

Suponha que, em seguida, iniciemos a máquina com uma entrada de três 1. As primeiras configurações são semelhantes, pois as mesmas instruções são executadas, com apenas uma pequena diferença na entrada da fita:

$$\triangleright 1_0 1 1 0 \ldots$$

$$\triangleright 1 1_1 1 0 \ldots$$

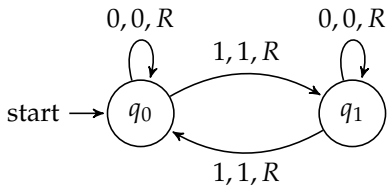
$$\triangleright 1 1 1_0 0 \ldots$$

$$\triangleright 1 1 1 0_1 \ldots$$

A máquina já percorreu todos os 1 e está lendo um 0 no estado $q_1$. Como mostrado no diagrama, há uma instrução da forma $\delta(q_1, 0) = \langle q_1, 0, R\rangle$. Como a fita está preenchida com 0 indefinidamente para a direita, a máquina continuará a executar esta instrução *para sempre*, permanecendo no estado $q_1$ e movendo-se cada vez mais à direita. A máquina nunca para, e não aceita a entrada.

É importante observar que nem todas as máquinas param. Se parar significa que a máquina fica sem instruções a executar, então podemos criar uma máquina que nunca para, simplesmente garantindo que haja uma seta de saída para cada símbolo em cada estado. A máquina par pode ser modificada para rodar indefinidamente adicionando uma instrução para examinar um 0 em $q_0$.

**Exemplo 31.2.**




As tabelas de máquina são outra forma de representar máquinas de Turing. As tabelas de máquina têm o alfabeto da fita exibido no eixo $x$, e o conjunto de estados da máquina ao longo do eixo $y$. Dentro da tabela, na interseção de cada estado e símbolo, está escrito o resto da instrução—o novo estado, o novo símbolo e a direção do movimento. As tabelas de máquina facilitam determinar em que estado, e para qual símbolo, a máquina para. Sempre que há uma lacuna na tabela, há um ponto possível para a máquina parar. Ao contrário dos diagramas de estado e dos conjuntos de instruções, em que os pontos nos quais a máquina para nem sempre são imediatamente óbvios, quaisquer pontos de parada são rapidamente identificados ao encontrar as lacunas na tabela de máquina.

**Exemplo 31.3.** A tabela de máquina da máquina par é:

| | 0 | 1 | ▷ |
|---|---|---|---|
| $q_0$ | | $1, q_1, R$ | |
| $q_1$ | $0, q_1, R$ | $1, q_0, R$ | |

Como podemos ver, a máquina para ao examinar um 0 no estado $q_0$.

Até aqui consideramos apenas máquinas que leem e aceitam entradas. No entanto, as máquinas de Turing têm a capacidade de tanto ler quanto escrever. Um exemplo de tal máquina (embora haja muitos, muitos exemplos) é um *duplicador*. Um duplicador, quando iniciado com um bloco de $n$ 1 na fita, produz como saída um bloco de $2n$ 1.

**Exemplo 31.4.** Antes de construir uma máquina duplicadora, é importante elaborar uma *estratégia* para resolver o problema. Como a máquina (tal como a formulamos) não consegue lembrar quantos 1 já leu, precisamos encontrar uma maneira de rastrear todos os 1 na fita. Uma dessas maneiras é separar a saída da entrada com um 0. A máquina pode então apagar o primeiro 1 da entrada, percorrer o resto da entrada, deixar um 0, e escrever dois novos 1. A máquina então voltará e encontrará o segundo 1 na entrada, e duplicará esse também. Para cada 1 de entrada, ela escreverá dois 1 de saída. Ao apagar a entrada conforme a máquina avança, podemos garantir que nenhum 1 seja perdido ou duplicado duas vezes. Quando toda a entrada é apagada, restarão $2n$ 1 na fita. O diagrama de estado da máquina de Turing resultante está representado na Figura 31.2.

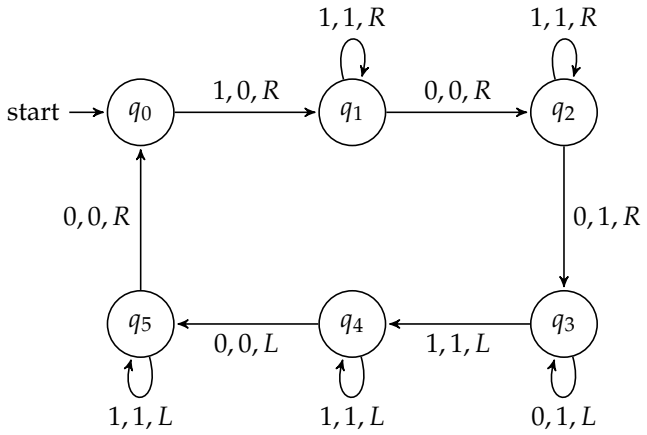



Figura 31.2: Uma máquina duplicadora

## 31.3 Máquinas de Turing

A definição formal do que constitui uma máquina de Turing parece abstrata, mas é na verdade simples: apenas reúne em uma estrutura matemática toda a informação necessária para especificar o funcionamento de uma máquina de Turing. Isso inclui (1) em quais estados a máquina pode estar, (2) quais símbolos são permitidos na fita, (3) em qual estado a máquina deve começar e (4) qual é o conjunto de instruções da máquina.

**Definição 31.5 (Máquina de Turing).** Uma *máquina de Turing* $M$ é uma tupla $\langle Q, \Sigma, q_0, \delta \rangle$ consistindo de

1. um conjunto finito de *estados* $Q$,
2. um *alfabeto* finito $\Sigma$ que inclui $\triangleright$ e $0$,
3. um *estado inicial* $q_0 \in Q$,
4. um *conjunto de instruções* finito $\delta \colon Q \times \Sigma \nrightarrow Q \times \Sigma \times \{L, R, N\}$.

A função parcial $\delta$ também é chamada de *função de transição* de $M$.

Supomos que a fita é infinita em apenas uma direção. Por essa razão é útil designar um símbolo especial $\triangleright$ como marcador da extremidade esquerda da fita. Isso facilita que programas de máquinas de Turing saibam quando estão "em perigo" de sair da fita. Poderíamos supor que esse símbolo nunca é sobrescrito, ou seja, que $\delta(q, \triangleright) = \langle q', \triangleright, x \rangle$ se $\delta(q, \triangleright)$ estiver definido. Alguns

livros-texto fazem isso; nós não. Basta ter cuidado ao construir sua máquina de Turing para que ela nunca sobrescreva $\triangleright$. Além disso, há casos em que permitir tal sobrescrita oferece alguma flexibilidade conveniente.

**Exemplo 31.6.** *Máquina dos pares:* A máquina dos pares é formalmente a quádrupla $\langle Q, \Sigma, q_0, \delta\rangle$ onde

$$\begin{aligned} Q &= \{q_0, q_1\} \\ \Sigma &= \{\triangleright, 0, 1\}, \\ \delta(q_0, 1) &= \langle q_1, 1, R\rangle, \\ \delta(q_1, 1) &= \langle q_0, 1, R\rangle, \\ \delta(q_1, 0) &= \langle q_1, 0, R\rangle. \end{aligned}$$

## 31.4 Configurações e Computações

Lembre-se de acompanhar as configurações da máquina dos pares anteriormente. O mecanismo imaginário formado pela fita, pela cabeça de leitura-escrita e pelo programa da máquina de Turing é, na verdade, apenas uma maneira intuitiva de visualizar o que é uma computação de máquina de Turing. Formalmente, podemos definir a computação de uma máquina de Turing sobre uma dada entrada como uma sequência de *configurações*—e uma configuração, por sua vez, é uma sequência de símbolos (correspondendo ao conteúdo da fita em um dado ponto da computação), um número que indica a posição da cabeça de leitura-escrita e um estado. Com isso, podemos definir o que a máquina de Turing $M$ computa sobre uma dada entrada.

**Definição 31.7 (Configuração).** Uma *configuração* da máquina de Turing $M = \langle Q, \Sigma, q_0, \delta\rangle$ é uma tripla $\langle C, m, q\rangle$ onde

1. $C \in \Sigma^*$ é uma sequência finita de símbolos de $\Sigma$,
2. $m \in \mathbb{N}$ é um número $< \text{len}(C)$, e
3. $q \in Q$

Intuitivamente, a sequência $C$ é o conteúdo da fita (símbolos de todos os quadrados desde o quadrado mais à esquerda até o último não vazio ou previamente visitado), $m$ é o número do quadrado que a cabeça de leitura-escrita está examinando (começando com 0 como o número do quadrado mais à esquerda), e $q$ é o estado atual da máquina.

A possível entrada para uma máquina de Turing é uma sequência de símbolos, geralmente uma sequência que codifica um número de alguma forma. A configuração inicial da máquina de Turing é aquela configuração em que iniciamos a máquina de Turing para trabalhar sobre essa entrada: a fita contém

o marcador de fim de fita imediatamente seguido da entrada escrita nos quadrados à direita, a cabeça de leitura-escrita está examinando o quadrado mais à esquerda da entrada (ou seja, o quadrado à direita do marcador de fim esquerdo), e o mecanismo está no estado inicial designado $q_0$.

**Definição 31.8 (Configuração inicial).** A *configuração inicial* de $M$ para a entrada $I \in \Sigma^*$ é

$$\langle \triangleright \frown I, 1, q_0 \rangle.$$

O símbolo $\frown$ denota *concatenação*—a cadeia de entrada começa imediatamente após o marcador de fim esquerdo.

**Definição 31.9.** Dizemos que uma configuração $\langle C, m, q \rangle$ *produz a configuração* $\langle C', m', q' \rangle$ *em um passo* (de acordo com $M$), sse

1. o $m$-ésimo símbolo de $C$ é $\sigma$,
2. o conjunto de instruções de $M$ especifica $\delta(q, \sigma) = \langle q', \sigma', D \rangle$,
3. o $m$-ésimo símbolo de $C'$ é $\sigma'$, e
4. a) $D = L$ e $m' = m - 1$ se $m > 0$, caso contrário $m' = 0$, ou
   b) $D = R$ e $m' = m + 1$, ou
   c) $D = N$ e $m' = m$,
5. se $m' = \text{len}(C)$, então $\text{len}(C') = \text{len}(C) + 1$ e o $m'$-ésimo símbolo de $C'$ é 0. Caso contrário $\text{len}(C') = \text{len}(C)$.
6. para todo $i$ tal que $i < \text{len}(C)$ e $i \neq m$, $C'(i) = C(i)$,

**Definição 31.10.** Uma *execução de $M$ sobre a entrada $I$* é uma sequência $C_i$ de configurações de $M$, onde $C_0$ é a configuração inicial de $M$ para a entrada $I$, e cada $C_i$ produz $C_{i+1}$ em um passo.

Dizemos que *$M$ para sobre a entrada $I$ após $k$ passos* se $C_k = \langle C, m, q \rangle$, o $m$-ésimo símbolo de $C$ é $\sigma$, e $\delta(q, \sigma)$ é indefinido. Nesse caso, a *saída* de $M$ para a entrada $I$ é $O$, onde $O$ é uma cadeia de símbolos que não termina em 0 tal que $C = \triangleright \frown O \frown 0^j$ para algum $j \in \mathbb{N}$. ($0^j$ é uma sequência de $j$ 0's.)

De acordo com esta definição, a saída $O$ de $M$ sempre termina em um símbolo diferente de 0, ou, se no instante $k$ toda a fita estiver preenchida com 0 (exceto o $\triangleright$ mais à esquerda), $O$ é a cadeia vazia.

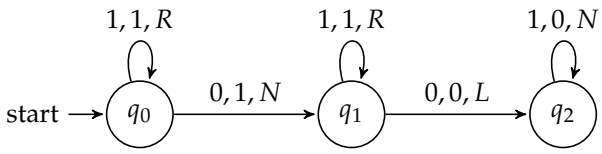



Figura 31.3: Uma máquina que computa $f(x, y) = x + y$

## 31.5 Representação Unária de Números

As máquinas de Turing trabalham sobre sequências de símbolos escritos em sua fita. Dependendo do alfabeto que uma máquina de Turing usa, essas sequências de símbolos podem representar diversas entradas e saídas. De particular interesse, é claro, estão as máquinas de Turing que computam funções *aritméticas*, isto é, funções de números naturais. Uma maneira simples de representar inteiros positivos é codificá-los como sequências de um único símbolo 1. Se $n \in \mathbb{N}$, seja $1^n$ a sequência vazia se $n = 0$, e caso contrário a sequência composta de exatamente $n$ 1.

**Definição 31.11 (Computação).** Uma máquina de Turing $M$ *computa* a função $f : \mathbb{N}^k \to \mathbb{N}$ sse $M$ para com a entrada

$$1^{n_1}01^{n_2}0 \dots 01^{n_k}$$

produzindo a saída $1^{f(n_1,\dots,n_k)}$.

**Exemplo 31.12.** *Adição:* Vamos construir uma máquina que computa a função $f(n, m) = n + m$. Isso requer uma máquina que comece com dois blocos de 1 de comprimento $n$ e $m$ na fita, e pare com um único bloco composto de $n + m$ 1. Os dois blocos de entrada de 1 estão separados por um 0, então um método seria escrever um traço no quadrado que contém o 0, e apagar o último 1.

Em Exemplo 31.4, demos um exemplo de uma máquina de Turing que recebe como entrada uma sequência de 1 e para com uma sequência de duas vezes mais 1 na fita—a máquina duplicadora. No entanto, como a saída contém 0 à esquerda do bloco duplicado de 1, ela não computa de fato a função $f(x) = 2x$, como você poderia ter suposto. Descreveremos duas maneiras de corrigir isso.

**Exemplo 31.13.** A máquina em Figura 31.4 computa a função $f(x) = 2x$. Em vez de apagar a entrada e escrever dois 1 na extremidade direita para cada 1 da entrada, como faz a máquina de Exemplo 31.4, esta máquina adiciona um único 1 à direita para cada 1 da entrada. Ela precisa rastrear onde a entrada

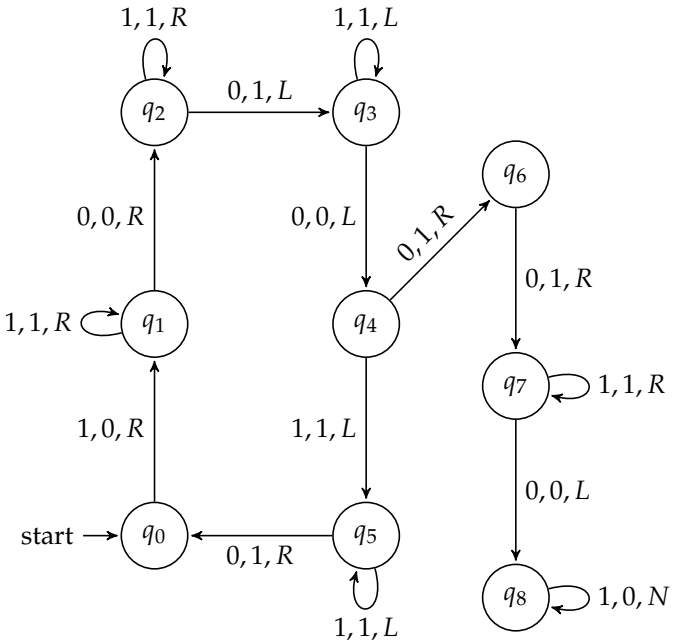



Figura 31.4: Uma máquina que computa $f(x) = 2x$

termina, então deixa um 0 entre a entrada e os traços adicionados, que ela preenche com um 1 bem ao final. E temos que "lembrar" onde estamos na entrada, então substituímos temporariamente um 1 do bloco de entrada por um 0.

**Exemplo 31.14.** Uma segunda possibilidade para computar $f(x) = 2x$ é manter a máquina duplicadora original, mas adicionar estados e instruções ao final que movam o bloco duplicado de traços para a extremidade esquerda da fita. A máquina em Figura 31.5 faz exatamente esta última parte: iniciada em uma fita composta de um bloco de 0 seguido de um bloco de 1 (e com a cabeça posicionada em qualquer lugar do bloco de 0), ela apaga os 1 um a um e os escreve no início da fita. Para conseguir saber quando ela termina, primeiro marca o fim do bloco de 1 com um símbolo $\triangleright$, que é apagado ao final. Começamos a numerar os estados em $q_6$, de modo que possam ser adicionados à máquina duplicadora. Tudo de que você precisará é uma instrução adicional $\delta(q_0, 0) = \langle q_6, 0, N\rangle$, isto é, uma seta de $q_0$ para $q_6$ rotulada $0, 0, N$. (Há um problema sutil: a máquina resultante não funciona para a entrada $x = 0$. Deixaremos isso como exercício.)

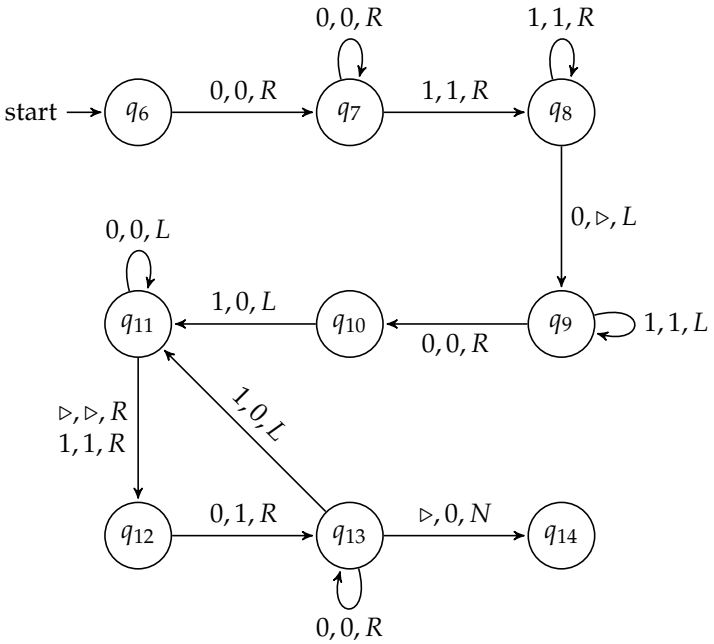



Figura 31.5: Movendo um bloco de 1 para a esquerda

**Definição 31.15.** Uma máquina de Turing $M$ computa a função parcial $f\colon \mathbb{N}^k \nrightarrow \mathbb{N}$ sse,

1. $M$ para com a entrada $1^{n_1} \frown 0 \frown \ldots \frown 0 \frown 1^{n_k}$ produzindo a saída $1^m$ se $f(n_1, \ldots, n_k) = m$.

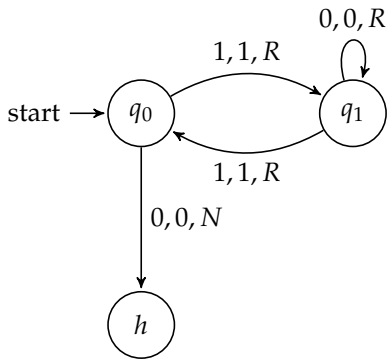
2. $M$ não para de modo algum, ou para com uma saída que não é um único bloco de 1 se $f(n_1, \ldots, n_k)$ é indefinida.

## 31.6 Estados de Parada

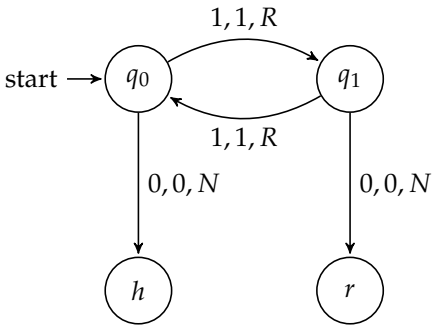
Embora tenhamos definido nossas máquinas para parar apenas quando não há instrução a executar, representações comuns de máquinas de Turing têm um *estado de parada* dedicado $h$, de modo que $h \in Q$.

A ideia por trás de um estado de parada é simples: quando a máquina terminou a operação (está pronta para aceitar a entrada, ou terminou de escrever a saída), ela entra em um estado $h$ onde para. Algumas máquinas têm dois estados de parada, um que aceita a entrada e outro que rejeita a entrada.

**Exemplo 31.16.** *Estados de parada*. Para elucidar esse conceito, comecemos com uma alteração da máquina dos pares. Em vez de fazer a máquina parar no estado $q_0$ se a entrada for par, podemos adicionar uma instrução para enviar a máquina a um estado de parada.




Vamos expandir ainda mais o exemplo. Quando a máquina determina que a entrada é ímpar, ela nunca para. Podemos alterar a máquina para incluir um estado de *rejeição* substituindo a instrução em laço por uma instrução para ir a um estado de rejeição $r$.




Adicionar um estado de parada dedicado pode ser vantajoso em casos como este, em que deixa explícito quando a máquina aceita/rejeita certas entradas. No entanto, é importante notar que nenhum poder computacional é ganho ao adicionar um estado de parada dedicado. Da mesma forma, uma noção menos formal de parada tem suas próprias vantagens. A definição de parada usada até agora neste capítulo torna a prova do *Problema da Parada* intuitiva e fácil de demonstrar. Por essa razão, continuamos com nossa definição original.

## 31.7 Máquinas Disciplinadas

Na Seção 31.6, consideramos máquinas de Turing que têm um único estado

de parada designado $h$—tais máquinas são garantidas de parar, se pararem de fato, no estado $h$. Dessa forma, máquinas com um único estado de parada são mais "disciplinadas" do que permitimos que máquinas de Turing sejam em geral. Há outras restrições que podemos impor ao comportamento das máquinas de Turing. Por exemplo, também não proibimos máquinas de Turing de apagar o marcador de fim de fita no quadrado 0, ou de tentar mover-se à esquerda a partir do quadrado 0. (Nossa definição afirma que a cabeça simplesmente permanece no quadrado 0 nesse caso; outras definições fazem a máquina parar.) Da mesma forma, às vezes é desejável poder supor que uma máquina de Turing, se parar de fato, para no quadrado 1.

**Definição 31.17.** Uma máquina de Turing $M$ é *disciplinada* sse

1. ela tem um único estado de parada designado $h$,
2. ela para, se parar de fato, enquanto examina o quadrado 1,
3. ela nunca apaga o símbolo $\triangleright$ no quadrado 0, e
4. ela nunca tenta mover-se à esquerda a partir do quadrado 0.

Já discutimos que qualquer máquina de Turing pode ser transformada em uma com o mesmo comportamento, mas com um estado de parada designado. Isso é feito simplesmente adicionando um novo estado $h$, e adicionando uma instrução $\delta(q, \sigma) = \langle h, \sigma, N\rangle$ para qualquer par $\langle q, \sigma\rangle$ onde o $\delta$ original é indefinido. É verdade, embora tedioso de provar, que qualquer máquina de Turing $M$ pode ser transformada em uma máquina de Turing disciplinada $M'$ que para nas mesmas entradas e produz a mesma saída. Por exemplo, se a máquina de Turing para e não está no quadrado 1, podemos adicionar algumas instruções para fazer a cabeça mover-se à esquerda até encontrar o marcador de fim de fita, depois mover um quadrado à direita, e então parar. Deixamos a você pensar sobre como as outras condições podem ser tratadas.

**Exemplo 31.18.** Em Figura 31.6, transformamos a máquina de adição de Exemplo 31.12 em uma máquina disciplinada.

**Proposição 31.19.** *Para toda máquina de Turing $M$, há uma máquina de Turing disciplinada $M'$ que para com saída $O$ se $M$ para com saída $O$, e não para se $M$ não para. Em particular, qualquer função $f : \mathbb{N}^n \to \mathbb{N}$ computável por uma máquina de Turing também é computável por uma máquina de Turing disciplinada.*

## 31.8 Combinando Máquinas de Turing

Os exemplos de máquinas de Turing que vimos até agora foram bastante simples por natureza. Mas, de fato, qualquer problema que possa ser resolvido

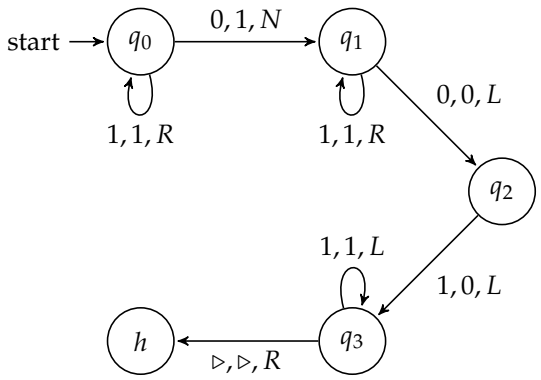



Figura 31.6: Uma máquina de adição disciplinada

com qualquer linguagem de programação moderna também pode ser resolvido com máquinas de Turing. Para construir máquinas de Turing mais complexas, é importante nos convencer de que podemos combiná-las, de modo a construir máquinas que resolvam problemas mais complexos quebrando o procedimento em partes mais simples. Se conseguirmos encontrar uma maneira natural de quebrar um problema complexo em partes constituintes, podemos atacar o problema em vários estágios, criando várias máquinas de Turing simples e combinando-as em uma única máquina capaz de resolver o problema. Esse ponto é especialmente importante ao atacar o Problema da Parada na próxima seção.

Como combinamos as máquinas de Turing $M = \langle Q, \Sigma, q_0, \delta \rangle$ e $M' = \langle Q', \Sigma', q_0', \delta' \rangle$? Usamos agora a configuração da fita após $M$ ter parado como a configuração de entrada de uma execução da máquina $M'$. Para obter uma única máquina de Turing $M \frown M'$ que faz isso, faça o seguinte:

1. Renumere (ou rerrotule) todos os estados $Q'$ de $M'$ de modo que $M$ e $M'$ não tenham estados em comum ($Q \cap Q' = \emptyset$).

2. Os estados de $M \frown M'$ são $Q \cup Q'$.

3. O alfabeto da fita é $\Sigma \cup \Sigma'$.

4. O estado inicial é $q_0$.

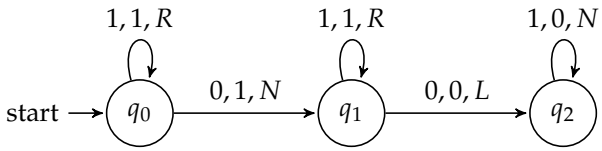
5. A função de transição é a função $\delta''$ dada por:

$$\delta''(q,\sigma) = \begin{cases} \delta(q,\sigma) & \text{se } q \in Q \\ \delta'(q,\sigma) & \text{se } q \in Q' \\ \langle q'_0, \sigma, N\rangle & \text{se } q \in Q \text{ e } \delta(q,\sigma) \text{ é indefinida} \end{cases}$$

A máquina resultante usa as instruções de $M$ quando está em um estado $q \in Q$, e as instruções de $M'$ quando está em um estado $q \in Q'$. Quando está em um estado $q \in Q$ e examina um símbolo $\sigma$ para o qual $M$ não tem transição (isto é, $M$ teria parado), ela entra no estado inicial de $M'$ (e deixa o conteúdo da fita e a posição da cabeça como estão).

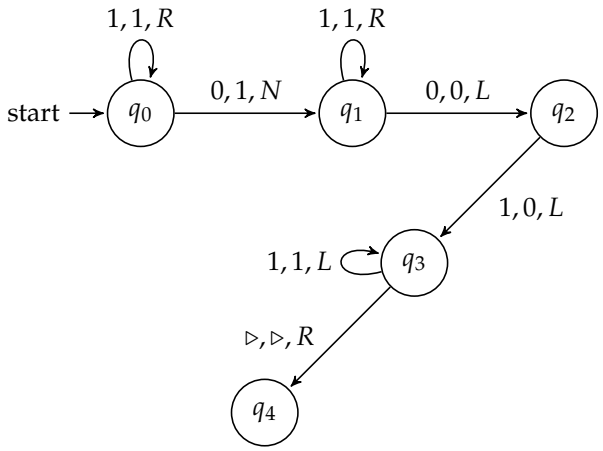
Note que, a menos que a máquina $M$ seja disciplinada, não sabemos onde está a cabeça da fita quando $M$ para, então a configuração de parada de $M$ não precisa ter a cabeça examinando o quadrado 1. Ao combinar máquinas, é importante ter isso em mente.

**Exemplo 31.20.** *Combinando Máquinas:* Projetaremos uma máquina que, quando iniciada com uma entrada composta de dois blocos de 1 de comprimento $n$ e $m$, para com um único bloco de $2(m+n)$ 1 na fita. Para construir essa máquina, podemos combinar duas máquinas que já conhecemos: a máquina de adição e a duplicadora. Começamos desenhando um diagrama de estado para a máquina de adição.




Em vez de parar no estado $q_2$, queremos continuar a operação a fim de duplicar a saída. Lembre-se de que a máquina duplicadora apaga o primeiro traço da entrada e escreve dois traços em uma saída separada. Vamos adicionar uma instrução para garantir que a cabeça da fita esteja lendo o primeiro traço

da saída da máquina de adição.




Agora é fácil duplicar a entrada—tudo o que temos a fazer é conectar a máquina duplicadora ao estado $q_4$. Isso requer renomear os estados da máquina duplicadora de modo que comecem em $q_4$ em vez de $q_0$—dessa forma não acabamos com dois estados iniciais. O diagrama final deve ter a aparência da Figura 31.7.

**Proposição 31.21.** *Se $M$ e $M'$ são disciplinadas e computam as funções $f\colon \mathbb{N}^k \to \mathbb{N}$ e $f'\colon \mathbb{N} \to \mathbb{N}$, respectivamente, então $M \frown M'$ é disciplinada e computa $f' \circ f$.*

*Prova.* Como $M$ é disciplinada, quando para com saída $f(n_1, \ldots, n_k) = m$, a cabeça está examinando o quadrado 1. Se agora entrarmos no estado inicial de $M'$, a máquina parará com saída $f'(m)$, novamente examinando o quadrado 1. As demais condições de Definição 31.17 também são satisfeitas. □

## 31.9 Variantes de Máquinas de Turing

Na verdade, há muitas maneiras possíveis de definir máquinas de Turing, das quais a nossa é apenas uma. De certas formas, nossa definição é mais liberal do que outras. Permitimos alfabetos finitos arbitrários; uma definição mais restrita poderia permitir apenas dois símbolos de fita, 1 e 0. Permitimos que a máquina escreva um símbolo na fita e se mova ao mesmo tempo; outras definições permitem escrever ou mover. Permitimos a possibilidade de escrever sem mover a cabeça da fita; outras definições omitem a "instrução" $N$. Em outros aspectos, nossa definição é mais restritiva. Assumimos que a fita é infinita em apenas uma direção; outras definições permitem que a fita seja infinita tanto para a esquerda quanto para a direita. Na verdade, pode-se até mesmo permitir qualquer número de fitas separadas, ou até mesmo uma grade infinita de quadrados. Representamos o conjunto de instruções da máquina de

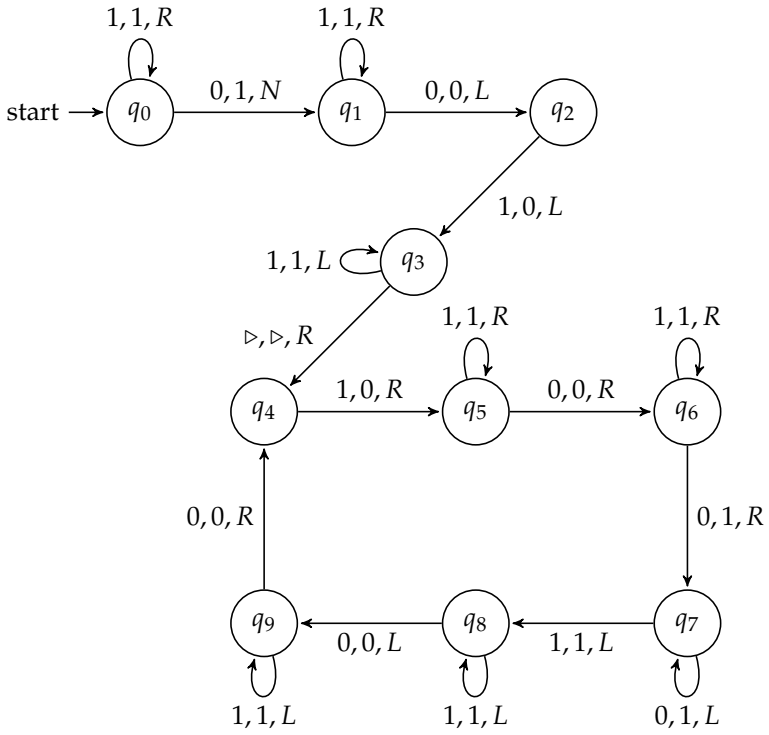



Figura 31.7: Combinando as máquinas de adição e duplicadora

Turing por uma função de transição; outras definições usam uma relação de transição em que a máquina tem mais de uma instrução possível em qualquer situação dada.

Essa última flexibilização da definição é particularmente interessante. Em nossa definição, quando a máquina está no estado $q$ lendo o símbolo $\sigma$, $\delta(q, \sigma)$ determina qual é o novo símbolo, o novo estado e a nova posição da cabeça da fita. Mas se permitirmos que o conjunto de instruções seja uma relação entre pares estado-símbolo atuais $\langle q, \sigma \rangle$ e novas triplas estado-símbolo-direção $\langle q', \sigma', D \rangle$, a ação da máquina de Turing pode não ser exclusivamente determinada — a relação de instrução pode conter tanto $\langle q, \sigma, q', \sigma', D \rangle$ quanto $\langle q, \sigma, q'', \sigma'', D' \rangle$. Nesse caso, temos uma máquina de Turing *não determinística*. Estas desempenham um papel importante na teoria da complexidade computacional.

Há também diferentes convenções para quando uma máquina de Turing para: dizemos que ela para quando a função de transição é indefinida; ou-

tras definições exigem que a máquina esteja em um estado de parada especial designado. Explicamos na Seção 31.6 por que exigir um estado de parada designado não é uma restrição que impacta o que as máquinas de Turing podem calcular. Como as fitas de nossas máquinas de Turing são infinitas em apenas uma direção, há casos em que uma máquina de Turing não consegue executar adequadamente uma instrução: se ela lê o quadrado mais à esquerda e deveria se mover para a esquerda. De acordo com a nossa definição, ela simplesmente permanece no lugar em vez de "cair", mas poderíamos tê-la definido de modo que ela pare quando isso acontecer. Essa definição também é equivalente: poderíamos simular o comportamento de uma máquina de Turing que para quando tenta se mover para a esquerda do quadrado 0 excluindo cada transição $\delta(q, \triangleright) = \langle q', \sigma, L\rangle$—então, em vez de tentar mover para a esquerda em $\triangleright$, a máquina para.[1]

Há também diferentes maneiras de representar números (e, portanto, a função de entrada-saída calculada por uma máquina de Turing): usamos representação unária, mas você também pode usar representação binária. Isso requer dois símbolos além de 0 e $\triangleright$.

Agora, aqui está um fato interessante: nenhuma dessas variações importa para quais funções são Turing-computáveis. *Se uma função é Turing-computável segundo uma definição, ela é Turing-computável segundo todas elas.*

Não entraremos nos detalhes de como verificar isso. Eis apenas um exemplo: não ganhamos nenhum poder computacional adicional ao permitir uma fita que é infinita em ambas as direções, ou múltiplas fitas. A razão é, aproximadamente, que uma máquina de Turing com uma única fita infinita unidirecional pode simular múltiplas fitas ou fitas infinitas bidirecionais. Por exemplo, usando estados e instruções adicionais, podemos "traduzir" um programa para uma máquina com múltiplas fitas ou fita infinita bidirecional em um programa para uma máquina com uma única fita infinita unidirecional. A máquina traduzida pode usar os quadrados pares para os quadrados da fita 1 (ou os quadrados "positivos" de uma fita infinita bidirecional) e os quadrados ímpares para os quadrados da fita 2 (ou os quadrados "negativos").

## 31.10 A Tese de Church–Turing

As máquinas de Turing devem ser um substituto preciso do conceito de procedimento efetivo. Turing pensava que quem compreendesse tanto o conceito de procedimento efetivo quanto o de máquina de Turing teria a intuição de que tudo o que pudesse ser feito por meio de um procedimento efetivo poderia ser feito por uma máquina de Turing. Essa afirmação é sustentada pelo

[1] Isso não funciona *muito bem*, pois nada nos impede de escrever e ler $\triangleright$ em quadrados que não sejam o quadrado 0 (veja Exemplo 31.14). Podemos contornar isso adicionando um segundo símbolo $\triangleright'$ para usar em seu lugar para tal propósito.

fato de que todas as outras propostas precisas de substituto do conceito de procedimento efetivo se mostram extensionalmente equivalentes ao conceito de máquina de Turing —ou seja, podem computar exatamente o mesmo conjunto de funções. Essa afirmação chama-se *tese de Church–Turing*.

**Definição 31.22 (Tese de Church–Turing).** A *tese de Church–Turing* afirma que tudo o que é computável por meio de um procedimento efetivo é computável por máquina de Turing.

A tese de Church–Turing é invocada de duas maneiras. O primeiro tipo de uso é uma desculpa para a preguiça. Suponha que temos uma descrição de um procedimento efetivo para computar algo, digamos, em "pseudocódigo." Então podemos invocar a tese de Church–Turing para justificar a afirmação de que a mesma função é computada por alguma máquina de Turing, mesmo que não a tenhamos de fato construído.

O outro uso da tese de Church–Turing é mais filosoficamente interessante. Pode-se mostrar que existem funções que não podem ser computadas por máquinas de Turing. Disso, usando a tese de Church–Turing, conclui-se que não podem ser computadas efetivamente, usando qualquer procedimento que seja. Pois se houvesse tal procedimento, pela tese de Church–Turing seguiria que haveria uma máquina de Turing para ele. Assim, se podemos provar que não há máquina de Turing que o compute, também não pode haver um procedimento efetivo. Em particular, a tese de Church–Turing é invocada para afirmar que o chamado problema da parada não só não pode ser resolvido por máquinas de Turing, como não pode ser resolvido efetivamente de modo algum.

## Problemas

**Problema 31.1.** Escolha uma entrada arbitrária e rastreie as configurações da máquina duplicadora em Exemplo 31.4.

**Problema 31.2.** Projete uma máquina de Turing com alfabeto $\{\triangleright, 0, A, B\}$ que aceite, isto é, pare, qualquer cadeia de $A$ e $B$ na qual o número de $A$ seja igual ao número de $B$ *e* todos os $A$ precedam todos os $B$, e que rejeite, isto é, não pare, qualquer cadeia em que o número de $A$ não seja igual ao número de $B$, ou os $A$ não precedam todos os $B$. (Por exemplo, a máquina deve aceitar $AABB$, e $AAABBB$, mas rejeitar tanto $AAB$ quanto $AABBAABB$.)

**Problema 31.3.** Projete uma máquina de Turing com alfabeto $\{\triangleright, 0, A, B\}$ que receba como entrada qualquer cadeia $\alpha$ de $A$ e $B$ e a duplique para produzir uma saída da forma $\alpha\alpha$. (Por exemplo, a entrada $ABBA$ deve resultar na saída $ABBAABBA$).

**Problema 31.4.** *Alfabética?:* Projete uma máquina de Turing com alfabeto $\{\triangleright, 0, A, B\}$ que, ao receber como entrada uma sequência finita de $A$ e $B$, verifique se todos os $A$ aparecem à esquerda de todos os $B$ ou não. A máquina deve deixar a cadeia de entrada na fita, e ou parar, se a cadeia for "alfabética", ou rodar para sempre, se a cadeia não for.

**Problema 31.5.** *Ordenador alfabético:* Projete uma máquina de Turing com alfabeto $\{\triangleright, 0, A, B\}$ que receba como entrada uma sequência finita de $A$ e $B$ e os reorganize de modo que todos os $A$ fiquem à esquerda de todos os $B$. (Por exemplo, a sequência $BABAA$ deve tornar-se a sequência $AAABB$, e a sequência $ABBABB$ deve tornar-se a sequência $AABBBB$).

**Problema 31.6.** Dê uma definição para quando uma máquina de Turing $M$ computa a função $f\colon \mathbb{N}^k \to \mathbb{N}^m$.

**Problema 31.7.** Rastreie as configurações da máquina de Exemplo 31.12 para a entrada $\langle 3, 2\rangle$. O que acontece se a máquina computa $0 + 0$?

**Problema 31.8.** Em Exemplo 31.14 descrevemos uma máquina composta de uma combinação da máquina duplicadora de Figura 31.4 e da máquina movedora de Figura 31.5. O que acontece se você inicia essa máquina combinada com a entrada $x = 0$, isto é, em uma fita vazia? Como você corrigiria a máquina de modo que, nesse caso, ela parasse com saída $2x = 0$? (Você deve conseguir fazer isso adicionando um estado e uma transição.)

**Problema 31.9.** *Subtração:* Projete uma máquina de Turing que, ao receber uma entrada de duas cadeias não vazias de traços de comprimento $n$ e $m$, em que $n > m$, compute a função $f(n, m) = n - m$.

**Problema 31.10.** *Igualdade:* Projete uma máquina de Turing para computar a seguinte função:

$$\text{igualdade}(n, m) = \begin{cases} 1 & \text{se } n = m \\ 0 & \text{se } n \neq m \end{cases}$$

em que $n$ e $m \in \mathbb{Z}^+$.

**Problema 31.11.** Projete uma máquina de Turing para computar a função $\min(x, y)$, em que $x$ e $y$ são inteiros positivos representados na fita por cadeias de 1 separadas por um 0. Você pode usar símbolos adicionais no alfabeto da máquina.

A função min seleciona o menor valor entre seus argumentos, de modo que $\min(3, 5) = 3$, $\min(20, 16) = 16$, e $\min(4, 4) = 4$, e assim por diante.

**Problema 31.12.** Dê uma máquina disciplinada que computa $f(x) = x + 1$.

**Problema 31.13.** Encontre uma máquina disciplinada que, quando iniciada com entrada $1^n$ produz saída $1^n \frown 0 \frown 1^n$.

**Problema 31.14.** Dê uma máquina de Turing disciplinada que computa $f(x) = x + 2$ tomando a máquina $M$ de PROBLEMA 31.12 e construindo $M \frown M$.

# Capítulo 32

# Indecidibilidade

## 32.1 Introdução

Pode parecer óbvio que nem toda função, nem mesmo toda função aritmética, pode ser computável. Há simplesmente um número grande demais delas, cujo comportamento é complicado demais. Funções definidas a partir do decaimento de partículas radioativas, por exemplo, ou de outro comportamento caótico ou aleatório. Suponha que comecemos a contar intervalos de 1 segundo a partir de um dado instante e definamos a função $f(n)$ como o número de partículas no universo que decaem no $n$-ésimo intervalo de 1 segundo após aquele momento inicial. Esta parece ser uma candidata a função que jamais poderemos ter esperança de computar.

Mas uma coisa é não conseguir imaginar como se computaria tais funções, e outra bem diferente é de fato provar que elas são incomputáveis. Na verdade, mesmo funções que parecem irremediavelmente complicadas podem, em um sentido abstrato, ser computáveis. Por exemplo, suponha que o universo seja finito no tempo—algum dia, num futuro muito distante, o universo se contrairá em um único ponto, como preveem algumas teorias cosmológicas. Então há apenas um número finito (mas incrivelmente grande) de segundos a partir daquele momento inicial para os quais $f(n)$ está definida. E qualquer função que esteja definida para apenas finitas entradas é computável: poderíamos listar as saídas em uma grande tabela, ou codificá-la em um diagrama de transição de estados de máquina de Turing muito grande.

Frequentemente estamos interessados em casos especiais de funções cujos valores fornecem as respostas a perguntas de sim/não. Por exemplo, a pergunta "$n$ é um número primo?" está associada à função

$$\text{primo}(n) = \begin{cases} 1 & \text{se } n \text{ é primo} \\ 0 & \text{caso contrário.} \end{cases}$$

Dizemos que uma pergunta de sim/não pode ser *efetivamente decidida* se a função associada de valores $1/0$ é efetivamente computável.

Para provar matematicamente que há funções que não podem ser efetivamente computadas, ou problemas que não podem ser efetivamente decididos, é essencial fixar um modelo específico de computação e mostrar que há funções que ele não pode computar ou problemas que ele não pode decidir. Podemos mostrar, por exemplo, que nem toda função pode ser computada por máquinas de Turing, e nem todo problema pode ser decidido por máquinas de Turing. Podemos então apelar para a tese de Church-Turing para concluir que não apenas as máquinas de Turing não são poderosas o suficiente para computar toda função, como também nenhum procedimento efetivo o é.

A chave para provar tais resultados negativos é o fato de que podemos atribuir números às próprias máquinas de Turing. A maneira mais fácil de fazer isso é enumerá-las, talvez fixando um modo específico de escrever máquinas de Turing e seus programas e, em seguida, listando-os de maneira sistemática. Uma vez que vejamos que isso pode ser feito, então a existência de funções Turing-incomputáveis decorre de simples considerações de cardinalidade: o conjunto de funções de $\mathbb{N}$ a $\mathbb{N}$ (na verdade, mesmo apenas de $\mathbb{N}$ a $\{0,1\}$) é não enumerável, mas como podemos enumerar todas as máquinas de Turing, o conjunto de funções Turing-computáveis é apenas infinito enumerável.

Também podemos definir funções e problemas *específicos* que podemos provar ser incomputáveis e indecidíveis, respectivamente. Um desses problemas é o assim chamado *Problema da Parada.* Máquinas de Turing podem ser finitamente descritas listando-se suas instruções. Tal descrição de uma máquina de Turing, isto é, um programa de máquina de Turing, pode é claro ser usada como entrada para outra máquina de Turing. Assim, podemos considerar máquinas de Turing que decidem perguntas sobre outras máquinas de Turing. Uma pergunta particularmente interessante é esta: "A máquina de Turing dada eventualmente para quando iniciada na entrada $n$?" Seria bom se houvesse uma máquina de Turing que pudesse decidir essa pergunta: pense nela como uma máquina de Turing de controle de qualidade que garante que as máquinas de Turing não fiquem presas em laços infinitos e coisas do tipo. O fato interessante, que Turing provou, é que não pode haver tal máquina de Turing. Não pode haver uma única máquina de Turing que, quando iniciada em uma entrada que consiste em uma descrição de uma máquina de Turing $M$ e algum número $n$, sempre pare com saída 1 ou 0 conforme a máquina $M$ teria parado ou não quando iniciada na entrada $n$.

Uma vez que tenhamos exemplos de problemas indecidíveis específicos, podemos usá-los para mostrar que outros problemas também são indecidíveis. Por exemplo, um célebre problema indecidível é a pergunta "A fórmula $\varphi$ de primeira ordem é válida?". Não há máquina de Turing que, dada como entrada uma fórmula $\varphi$ de primeira ordem, tenha garantia de parar com saída 1 ou 0 conforme $\varphi$ seja válida ou não. Historicamente, a questão de encontrar um procedimento para resolver efetivamente esse problema foi chamada simplesmente de "o" problema da decisão; e assim dizemos que o problema da

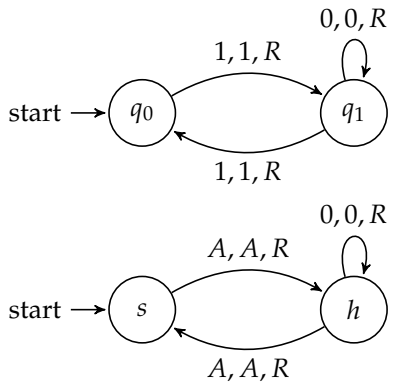



Figura 32.1: Variantes da máquina *Par*

decisão é insolúvel. Turing e Church provaram esse resultado independentemente mais ou menos na mesma época, de modo que ele também é chamado de Teorema de Church-Turing.

## 32.2 Enumerando Máquinas de Turing

Podemos mostrar que o conjunto de todas as máquinas de Turing é enumerável. Isso decorre do fato de que cada máquina de Turing pode ser finitamente descrita. O conjunto de estados e o vocabulário da fita são conjuntos finitos. A função de transição é uma função parcial de $Q \times \Sigma$ a $Q \times \Sigma \times \{L, R, N\}$ e, portanto, também pode ser especificada listando-se seus valores para os finitos pares de argumentos para os quais está definida.

Isso é verdade até certo ponto, mas há uma diferença sutil. A definição de máquinas de Turing não fez restrição alguma sobre quais membros o conjunto de estados e o alfabeto da fita podem ter. Assim, por exemplo, para todo número real, há tecnicamente uma máquina de Turing que usa esse número como um estado. Contudo, o *comportamento* da máquina de Turing é independente de quais objetos servem como estados e vocabulário. Considere as duas máquinas de Turing na Figura 32.1. Esses dois diagramas correspondem a duas máquinas, $M$ com o alfabeto de fita $\Sigma = \{\triangleright, 0, 1\}$ e conjunto de estados $\{q_0, q_1\}$, e $M'$ com alfabeto $\Sigma' = \{\triangleright, 0, A\}$ e estados $\{s, h\}$. Mas, quanto ao resto, suas instruções são as mesmas: $M$ para em uma sequência de $n$ 1 se, e somente se, $n$ é par, e $M'$ para em uma sequência de $n$ $A$ se, e somente se, $n$ é par. Tudo o que fizemos foi renomear 1 para $A$, $q_0$ para $s$ e $q_1$ para $h$. Esse exemplo se generaliza: podemos considerar máquinas de Turing como sendo a mesma desde que uma resulte da outra por tal renomeação de símbolos e estados. Na verdade, podemos simplesmente pensar nos símbolos e estados

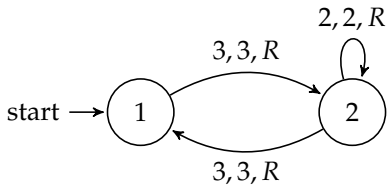



Figura 32.2: Uma máquina *Par* padrão

de uma máquina de Turing como inteiros positivos: em vez de $\sigma_0$ pense 1, em vez de $\sigma_1$ pense 2, etc.; $\triangleright$ é 1, 0 é 2, etc. Dessa forma, a máquina *Par* torna-se a máquina representada na Figura 32.2. Poderíamos chamar de máquina *padrão* uma máquina de Turing cujos estados e símbolos são inteiros positivos, e considerar apenas máquinas padrão de agora em diante.[1]

Queríamos mostrar que o conjunto de máquinas de Turing é enumerável e, tendo em mente as considerações acima, basta mostrar que o conjunto de máquinas de Turing padrão é enumerável. Suponha que nos seja dada uma máquina de Turing padrão $M = \langle Q, \Sigma, q_0, \delta \rangle$. Como poderíamos descrevê-la usando uma cadeia finita de inteiros positivos? Primeiro listaremos o número de estados, os próprios estados, o número de símbolos, os próprios símbolos e o estado inicial. (Lembre-se, todos esses são inteiros positivos, já que $M$ é uma máquina padrão.) E quanto a $\delta$? O conjunto de argumentos possíveis, isto é, pares $\langle q, \sigma \rangle$, é finito, já que $Q$ e $\Sigma$ são finitos. Assim, a informação em $\delta$ é simplesmente a lista finita de todas as 5-uplas $\langle q, \sigma, q', \sigma', d \rangle$ em que $\delta(q, \sigma) = \langle q', \sigma', D \rangle$, e $d$ é um número que codifica a direção $D$ (digamos, 1 para $L$, 2 para $R$ e 3 para $N$).

Dessa forma, toda máquina de Turing padrão pode ser descrita por uma lista finita de inteiros positivos, isto é, como uma sequência $s_M \in (\mathbb{Z}^+)^*$. Por exemplo, a máquina *Par* padrão é codificada pela sequência

$$2, \underbrace{1,2}_{Q}, 3, \overbrace{1,2,3}^{\Sigma}, 1, \underbrace{1,3,2,3,2}_{\delta(1,3)=\langle 2,3,R\rangle}, \overbrace{2,2,2,2,2}^{\delta(2,2)=\langle 2,2,R\rangle}, \underbrace{2,3,1,3,2}_{\delta(2,3)=\langle 1,3,R\rangle}.$$

**Teorema 32.1.** *Há funções de* $\mathbb{N}$ *a* $\mathbb{N}$ *que não são Turing-computáveis.*

*Prova.* Sabemos que o conjunto de sequências finitas de inteiros positivos $(\mathbb{Z}^+)^*$ é enumerável (PROBLEMA 4.7). Isso nos dá que o conjunto de descrições de máquinas de Turing padrão, como um subconjunto de $(\mathbb{Z}^+)^*$, é ele próprio

[1] A terminologia "máquina padrão" não é padrão.

enumerável. Toda função Turing-computável de $\mathbb{N}$ a $\mathbb{N}$ é computada por alguma (na verdade, muitas) máquina de Turing. Renomeando seus estados e símbolos para inteiros positivos (em particular, $\triangleright$ como 1, 0 como 2 e 1 como 3), podemos ver que toda função Turing-computável é computada por uma máquina de Turing padrão. Isso significa que o conjunto de todas as funções Turing-computáveis de $\mathbb{N}$ a $\mathbb{N}$ é também enumerável.

Por outro lado, o conjunto de todas as funções de $\mathbb{N}$ a $\mathbb{N}$ não é enumerável (PROBLEMA 4.35). Se todas as funções fossem computáveis por alguma máquina de Turing, poderíamos enumerar o conjunto de todas as funções listando todas as descrições de máquinas de Turing que as computam. Logo, há algumas funções que não são Turing-computáveis. □

## 32.3 Máquinas de Turing Universais

Na Seção 32.2 discutimos como toda máquina de Turing pode ser descrita por uma sequência finita de inteiros. Essa sequência codifica os estados, o alfabeto, o estado inicial e as instruções da máquina de Turing. Também observamos que o conjunto de todas essas descrições é enumerável. Como o conjunto de tais descrições é infinito enumerável, isso significa que há uma função sobrejetiva de $\mathbb{N}$ nessas descrições. Uma tal função sobrejetiva pode ser obtida, por exemplo, usando o método zigue-zague de Cantor. Ele nos dá uma maneira de enumerar todas as (descrições de) máquinas de Turing. Se fixarmos uma tal enumeração, passa a fazer sentido falar da primeira, da segunda, ..., $e$-ésima máquina de Turing. Esses números são chamados de *índices*.

**Definição 32.2.** Se $M$ é a $e$-ésima máquina de Turing (em nossa enumeração fixada), dizemos que $e$ é um *índice* de $M$. Escrevemos $M_e$ para a $e$-ésima máquina de Turing.

Uma máquina pode ter mais de um índice; por exemplo, duas descrições de $M$ podem diferir na ordem em que listamos suas instruções, e essas diferentes descrições terão índices diferentes.

É importante notar que é possível dar a enumeração das descrições de máquinas de Turing de tal modo que possamos computar efetivamente a descrição de $M$ a partir de seu índice, e computar efetivamente um índice de uma máquina $M$ a partir de sua descrição. Pela tese de Church-Turing, é então possível encontrar uma máquina de Turing que recupera a descrição da máquina de Turing com índice $e$ e escreve a descrição correspondente em sua fita como saída. A descrição seria uma sequência de blocos de 1 (representando os inteiros positivos na sequência que descreve $M_e$).

Diante disso, torna-se natural perguntar: que funções de índices de máquinas de Turing são elas próprias computáveis por máquinas de Turing? Que propriedades de índices de máquinas de Turing podem ser decididas por máquinas de Turing? Um exemplo: a função que leva um índice $e$ ao número de estados

que a máquina de Turing com índice $e$ possui é computável por uma máquina de Turing. Eis o que tal máquina de Turing faria: iniciada em uma fita contendo um único bloco de $e$ 1, ela primeiro decodificaria $e$ em sua descrição. A descrição passa a ser representada por uma sequência de blocos de 1 na fita. Como o primeiro membro nessa sequência é o número de estados, tudo o que resta a fazer agora é apagar tudo, exceto o primeiro bloco de 1, e então parar.

Um resultado notável é o seguinte:

**Teorema 32.3.** *Há uma* máquina de Turing universal $U$ *que, quando iniciada na entrada* $\langle e, n \rangle$*,*

1. *para se, e somente se,* $M_e$ *para na entrada* $n$*, e*
2. *se* $M_e$ *para com saída* $m$*, então* $U$ *também para.*

*Assim,* $U$ *computa a função* $f : \mathbb{N} \times \mathbb{N} \nrightarrow \mathbb{N}$ *dada por* $f(e, n) = m$ *se* $M_e$ *iniciada na entrada* $n$ *para com saída* $m$*, e indefinida caso contrário.*

*Prova.* Produzir de fato $U$ é basicamente impossível, já que se trata de uma máquina extremamente complicada. Mas podemos descrever em linhas gerais como ela funciona, e então invocar a tese de Church-Turing. Quando ela começa, a fita de $U$ contém um bloco de $e$ 1 seguido de um bloco de $n$ 1. Ela primeiro "decodifica" o índice $e$ à direita da entrada $n$. Isso produz uma lista de números (isto é, blocos de 1 separados por 0) que descreve as instruções da máquina $M_e$. Em seguida, $U$ escreve o número do estado inicial de $M_e$ e o número 1 na fita, à direita da descrição de $M_e$. (Novamente, esses são representados em unário, como blocos de 1.) Depois, ela copia a entrada (bloco de $n$ 1) para a direita—mas substitui cada 1 por um bloco de três 1 (lembre-se, o número do símbolo 1 é 3, sendo 1 o número de $\triangleright$ e 2 o número de 0). Na extremidade esquerda dessa sequência de blocos (separados por símbolos 0 na fita de $U$), ela escreve um único 1, o código de $\triangleright$.

$U$ agora tem em sua fita: o índice $e$, o número $n$, o número de código do estado inicial (o "estado atual"), o número da posição inicial do cabeçote 1 (a "posição atual do cabeçote") e o conteúdo inicial da "fita" (uma sequência de blocos de 1 representando os números de código dos símbolos de $M_e$—os "símbolos"—separados por 0).

Ela agora simula o que $M_e$ faria se iniciada na entrada $n$, fazendo o seguinte:

1. Encontrar o número $k$ da "posição atual do cabeçote" (no início, esse é 1),
2. Mover-se para o $k$-ésimo bloco na "fita" para ver qual é o "símbolo" ali,
3. Encontrar a instrução que corresponde ao "estado" e ao "símbolo" atuais,

4. Voltar para o $k$-ésimo bloco na "fita" e substituir o "símbolo" ali pelo número de código do símbolo que $M_e$ escreveria,
5. Mover o cabeçote para onde ela registra o "estado" atual e substituir o número ali pelo número do novo estado,
6. Mover-se para o lugar onde ela registra a "posição na fita" e apagar um 1 ou adicionar um 1 (se a instrução mandar mover para a esquerda ou para a direita, respectivamente).
7. Repetir.[2]

Se $M_e$ iniciada na entrada $n$ nunca para, então $U$ também nunca para, de modo que sua saída é indefinida.

Se no passo (3) acontecer de a descrição de $M_e$ não conter nenhuma instrução para o par "estado"/"símbolo" atual, então $M_e$ pararia. Se isso acontecer, $U$ apaga a parte de sua fita à esquerda da "fita". Para cada bloco de três 1 (representando um 1 na fita de $M_e$), ela escreve um 1 na extremidade esquerda de sua própria fita, e apaga sucessivamente a "fita". Quando isso está concluído, a fita de $U$ contém um único bloco de 1 de comprimento $m$.

Se $U$ encontrar algo diferente de um bloco de três 1 na "fita", ela para imediatamente. Como a fita de $U$ nesse caso não contém um único bloco de 1, sua saída não é um número natural, isto é, $f(e,n)$ é indefinida nesse caso. □

## 32.4 O Problema da Parada

Suponha que tenhamos fixado alguma enumeração das descrições de máquinas de Turing. Cada máquina de Turing recebe assim um *índice*: seu lugar na enumeração $M_1, M_2, M_3, \ldots$ das descrições de máquinas de Turing.

Sabemos que devem existir funções não-Turing-computáveis: o conjunto de descrições de máquinas de Turing—e, portanto, o conjunto de máquinas de Turing—é enumerável, mas o conjunto de todas as funções de $\mathbb{N}$ a $\mathbb{N}$ não é. Mas também podemos encontrar exemplos específicos de funções não computáveis. Uma dessas funções é a função de parada.

**Definição 32.4 (Função de parada).** A *função de parada* $h$ é definida como

$$h(e,n) = \begin{cases} 0 & \text{se a máquina } M_e \text{ não para na entrada } n \\ 1 & \text{se a máquina } M_e \text{ para na entrada } n \end{cases}$$

**Definição 32.5 (Problema da parada).** O *Problema da Parada* é o problema de determinar (para quaisquer $e$, $n$) se a máquina de Turing $M_e$ para com uma entrada de $n$ traços.

[2] Estamos passando por cima de algumas dificuldades sutis aqui. Por exemplo, $U$ pode precisar de algum espaço extra quando incrementa o contador onde mantém o registro da "posição atual do cabeçote"—nesse caso, terá de mover toda a "fita" para a direita.

Mostramos que $h$ não é Turing-computável mostrando que uma função relacionada, $s$, não é Turing-computável. Esta prova baseia-se no fato de que tudo o que pode ser computado por uma máquina de Turing pode ser computado por uma máquina de Turing disciplinada (Seção 31.7), e no fato de que duas máquinas de Turing podem ser conectadas para criar uma única máquina (Seção 31.8).

**Definição 32.6.** A função $s$ é definida como

$$s(e) = \begin{cases} 0 & \text{se a máquina } M_e \text{ não para na entrada } e \\ 1 & \text{se a máquina } M_e \text{ para na entrada } e \end{cases}$$

**Lema 32.7.** *A função $s$ não é Turing-computável.*

*Prova.* Suponha, por contradição, que a função $s$ seja Turing-computável. Então haveria uma máquina de Turing $S$ que computa $s$. Podemos supor, sem perda de generalidade, que quando $S$ para, ela o faz examinando o primeiro quadrado (isto é, que ela é disciplinada). Esta máquina pode ser "conectada" a outra máquina $J$, que para se for iniciada na entrada 0 (isto é, se ela lê 0 no estado inicial enquanto examina o quadrado à direita do símbolo de fim de fita), e caso contrário vagueia para a direita, sem nunca parar. $S \frown J$, a máquina criada conectando-se $S$ a $J$, é uma máquina de Turing, logo é $M_e$ para algum $e$ (isto é, aparece em algum lugar da enumeração). Inicie $M_e$ em uma entrada de $e$ 1. Há duas possibilidades: ou $M_e$ para ou não para.

1. Suponha que $M_e$ pare para uma entrada de $e$ 1. Então $s(e) = 1$. Assim, $S$, quando iniciada em $e$, para com um único 1 como saída na fita. Então $J$ começa com um 1 na fita. Nesse caso, $J$ não para. Mas $M_e$ é a máquina $S \frown J$, de modo que ela deveria fazer exatamente o que $S$ seguida de $J$ faria (isto é, neste caso, vaguear para a direita e nunca parar). Logo, $M_e$ não pode parar para uma entrada de $e$ 1.

2. Agora suponha que $M_e$ não pare para uma entrada de $e$ 1. Então $s(e) = 0$, e $S$, quando iniciada na entrada $e$, para com uma fita em branco. $J$, quando iniciada em uma fita em branco, para imediatamente. Novamente, $M_e$ faz o que $S$ seguida de $J$ faria, de modo que $M_e$ deve parar para uma entrada de $e$ 1.

Em cada caso chegamos a uma contradição com nossa suposição. Isso mostra que não pode haver uma máquina de Turing $S$: $s$ não é Turing-computável. □

**Teorema 32.8 (Insolubilidade do Problema da Parada).** *O problema da parada é insolúvel, isto é, a função $h$ não é Turing-computável.*

*Prova.* Suponha que $h$ fosse Turing-computável, digamos, por uma máquina de Turing $H$. Poderíamos usar $H$ para construir uma máquina de Turing que

computa $s$: primeiro, fazer uma cópia da entrada (separada por um símbolo 0). Depois, voltar ao início e executar $H$. Claramente podemos fazer uma máquina que realiza a primeira tarefa (veja PROBLEMA 31.13), e se $H$ existisse, poderíamos "conectá-la" a tal máquina copiadora para obter uma nova máquina que determinaria se $M_e$ para na entrada $e$, isto é, computa $s$. Mas já mostramos que não pode existir tal máquina. Portanto, $h$ também não é Turing-computável. □

## 32.5 O Problema da Decisão

Dizemos que a lógica de primeira ordem é *decidível* se, e somente se, há um método efetivo para determinar se uma dada sentença é válida ou não. Acontece que não existe tal método: o problema de decidir a validade de sentenças de primeira ordem é insolúvel.

A fim de estabelecer esse importante resultado negativo, provamos que o problema da decisão não pode ser resolvido por uma máquina de Turing. Isto é, mostramos que não existe máquina de Turing que, sempre que iniciada em uma fita que contém uma sentença de primeira ordem, eventualmente para e produz 1 ou 0 conforme a sentença seja válida ou não. Pela tese de Church-Turing, toda função que é computável é Turing-computável. Logo, se essa "função de validade" fosse de algum modo efetivamente computável, ela seria Turing-computável. Se ela não é Turing-computável, então também não pode ser efetivamente computável.

Nossa estratégia para provar que o problema da decisão é insolúvel é reduzir o problema da parada a ele. Isso significa o seguinte: provamos que a função $h(e, w)$ que para com saída 1 se a máquina de Turing descrita por $e$ para na entrada $w$ e produz 0 caso contrário não é Turing-computável. Mostraremos que se houvesse uma máquina de Turing que decide a validade de sentenças de primeira ordem, então haveria também uma máquina de Turing que computa $h$. Como $h$ não pode ser computada por uma máquina de Turing, também não pode haver uma máquina de Turing que decide a validade.

O primeiro passo nessa estratégia é mostrar que, para toda entrada $w$ e máquina de Turing $M$, podemos descrever efetivamente a sentença $\tau(M, w)$ representando o conjunto de instruções de $M$ e a entrada $w$, e a sentença $\alpha(M, w)$ exprimindo "$M$ eventualmente para", tal que:

$$\vDash \tau(M, w) \to \alpha(M, w) \text{ se, e somente se, } M \text{ para na entrada } w.$$

A maior parte de nossa prova consistirá em descrever essas sentenças $\tau(M, w)$ e $\alpha(M, w)$ e em verificar que $\tau(M, w) \to \alpha(M, w)$ é válida se, e somente se, $M$ para na entrada $w$.

## 32.6 Representando Máquinas de Turing

A fim de representar máquinas de Turing e seu comportamento por meio de a sentença da lógica de primeira ordem, temos de definir uma linguagem adequada. A linguagem consiste em duas partes: símbolos de predicado para descrever configurações da máquina, e expressões para numerar os passos de execução ("momentos") e as posições na fita.

Introduzimos dois tipos de símbolos de predicado, ambos de 2 lugares: para cada estado $q$, a símbolo de predicado $Q_q$, e para cada símbolo de fita $\sigma$, a símbolo de predicado $S_\sigma$. Os primeiros permitem-nos descrever o estado de $M$ e a posição de seu cabeçote de fita; os segundos permitem-nos descrever o conteúdo da fita.

A fim de exprimir as posições do cabeçote de fita e o número de passos executados, precisamos de uma maneira de exprimir números. Isso é feito usando a símbolo de constante $\mathsf{o}$ e uma função de 1 lugar $\prime$, a função sucessor. Por convenção, ela é escrita *depois* de seu argumento (e omitimos os parênteses).

Para cada número $n$ há um termo canônico $\overline{n}$, o *numeral* de $n$, que o representa em $\mathcal{L}_M$. $\overline{0}$ é $\mathsf{o}$, $\overline{1}$ é $\mathsf{o}'$, $\overline{2}$ é $\mathsf{o}''$, e assim por diante. Mais formalmente:

$$\begin{aligned}\overline{0} &= \mathsf{o}\\ \overline{n+1} &= \overline{n}'\end{aligned}$$

O termo $\overline{0}$, isto é, $\mathsf{o}$, nomeia a posição mais à esquerda na fita, bem como o instante anterior ao primeiro passo de execução (a configuração inicial). O termo $\overline{1}$, isto é, $\mathsf{o}'$, nomeia o quadrado à direita do quadrado mais à esquerda, e o instante posterior ao primeiro passo de execução, e assim por diante.

Também introduzimos a símbolo de predicado $<$ para exprimir tanto a ordenação das posições na fita (quando significa "à esquerda de") quanto a dos passos de execução (caso em que significa "antes").

Uma vez que tenhamos a linguagem montada, listamos os "axiomas" de $\tau(M, w)$, isto é, as sentenças que, tomadas em conjunto, descrevem o comportamento de $M$ quando executada na entrada $w$. Haverá sentenças que estabelecem condições sobre $\mathsf{o}$, $\prime$ e $<$, sentenças que descrevem a configuração de entrada, e sentenças que descrevem qual é a configuração de $M$ após executar uma instrução particular.

**Definição 32.9.** Dada uma máquina de Turing $M = \langle Q, \Sigma, q_0, \delta\rangle$, a linguagem $\mathcal{L}_M$ consiste em:

1. Um símbolo de predicado de dois lugares $Q_q(x, y)$ para todo estado $q \in Q$. Intuitivamente, $Q_q(\overline{m}, \overline{n})$ exprime "após $n$ passos, $M$ está no estado $q$ examinando o $m$-ésimo quadrado."

2. Um símbolo de predicado de dois lugares $S_\sigma(x, y)$ para todo símbolo $\sigma \in \Sigma$. Intuitivamente, $S_\sigma(\overline{m}, \overline{n})$ exprime "após $n$ passos, o $m$-ésimo quadrado contém o símbolo $\sigma$."

3. Um símbolo de constante $\mathsf{0}$

4. Um símbolo de função de um lugar $'$

5. Um símbolo de predicado de dois lugares $<$

As sentenças que descrevem a operação da máquina de Turing $M$ na entrada $w = \sigma_{i_1} \dots \sigma_{i_k}$ são as seguintes:

1. Axiomas que descrevem números e $<$:

   a) A sentença que diz que todo número é menor que seu sucessor:

   $$\forall x\, x < x'$$

   b) A sentença que garante que $<$ é transitivo:

   $$\forall x \forall y \forall z\, ((x < y \wedge y < z) \to x < z)$$

2. Axiomas que descrevem a configuração de entrada:

   a) Após 0 passos—antes de a máquina começar—$M$ está no estado inicial $q_0$, examinando o quadrado 1:

   $$Q_{q_0}(\overline{1}, \overline{0})$$

   b) Os primeiros $k + 1$ quadrados contêm os símbolos $\triangleright, \sigma_{i_1}, \dots, \sigma_{i_k}$:

   $$S_\triangleright(\overline{0}, \overline{0}) \wedge S_{\sigma_{i_1}}(\overline{1}, \overline{0}) \wedge \dots \wedge S_{\sigma_{i_k}}(\overline{k}, \overline{0})$$

   c) Caso contrário, a fita está vazia:

   $$\forall x\, (\overline{k} < x \to S_0(x, \overline{0}))$$

3. Axiomas que descrevem a transição de uma configuração para a seguinte:

   Para o que segue, seja $\varphi(x, y)$ a conjunção de todas as sentenças da forma

   $$\forall z\, (((z < x \vee x < z) \wedge S_\sigma(z, y)) \to S_\sigma(z, y'))$$

   em que $\sigma \in \Sigma$. Usamos $\varphi(\overline{m}, \overline{n})$ para exprimir "exceto no quadrado $m$, a fita após $n + 1$ passos é a mesma que após $n$ passos."

a) Para toda instrução $\delta(q_i, \sigma) = \langle q_j, \sigma', R\rangle$, a sentença:

$$\begin{aligned}\forall x\, \forall y\, ((Q_{q_i}(x,y) \wedge S_\sigma(x,y)) \rightarrow \\ (Q_{q_j}(x',y') \wedge S_{\sigma'}(x,y') \wedge \varphi(x,y)))\end{aligned}$$

Isto diz que se, após $y$ passos, a máquina está no estado $q_i$ examinando o quadrado $x$ que contém o símbolo $\sigma$, então após $y+1$ passos ela está examinando o quadrado $x+1$, está no estado $q_j$, o quadrado $x$ agora contém $\sigma'$, e todo quadrado distinto de $x$ contém o mesmo símbolo que continha após $y$ passos.

b) Para toda instrução $\delta(q_i, \sigma) = \langle q_j, \sigma', L\rangle$, a sentença:

$$\begin{aligned}&\forall x\, \forall y\, ((Q_{q_i}(x',y) \wedge S_\sigma(x',y)) \rightarrow \\ &\quad (Q_{q_j}(x,y') \wedge S_{\sigma'}(x',y') \wedge \varphi(x,y))) \wedge \\ &\forall y\, ((Q_{q_i}(\overline{0},y) \wedge S_\sigma(\overline{0},y)) \rightarrow \\ &\quad (Q_{q_j}(\overline{0},y') \wedge S_{\sigma'}(\overline{0},y') \wedge \varphi(\overline{0},y)))\end{aligned}$$

Reserve um momento para pensar em como isso funciona: agora não começamos com "se examinando o quadrado $x$ ...", mas: "se examinando o quadrado $x+1$ ...". Um movimento para a esquerda significa que no próximo passo a máquina está examinando o quadrado $x$. Mas o quadrado em que se escreve é $x+1$. Fazemos assim porque não temos subtração nem uma função predecessor.

Note que os números da forma $x+1$ são 1, 2, ..., isto é, isso não cobre o caso em que a máquina está examinando o quadrado 0 e deveria mover-se para a esquerda (o que, é claro, não pode fazer—ela simplesmente permanece onde está). Esse caso especial é coberto pela segunda conjunção: ela diz que se, após $y$ passos, a máquina está examinando o quadrado 0 no estado $q_i$ e o quadrado 0 contém o símbolo $\sigma$, então após $y+1$ passos ela ainda está examinando o quadrado 0, está agora no estado $q_j$, o símbolo no quadrado 0 é $\sigma'$, e os quadrados distintos do quadrado 0 contêm os mesmos símbolos que continham após $y$ passos.

c) Para toda instrução $\delta(q_i, \sigma) = \langle q_j, \sigma', N\rangle$, a sentença:

$$\begin{aligned}\forall x\, \forall y\, ((Q_{q_i}(x,y) \wedge S_\sigma(x,y)) \rightarrow \\ (Q_{q_j}(x,y') \wedge S_{\sigma'}(x,y') \wedge \varphi(x,y)))\end{aligned}$$

Seja $\tau(M, w)$ a conjunção de todas as sentenças acima para a máquina de Turing $M$ e a entrada $w$.

A fim de exprimir que $M$ eventualmente para, temos de encontrar uma sentença que diga "após algum número de passos, a função de transição será

indefinida." Seja $X$ o conjunto de todos os pares $\langle q, \sigma \rangle$ tais que $\delta(q, \sigma)$ é indefinida. Seja então $\alpha(M, w)$ a sentença

$$\exists x \, \exists y \, ( \bigvee_{\langle q,\sigma \rangle \in X} (Q_q(x, y) \wedge S_\sigma(x, y)))$$

Se usarmos uma máquina de Turing com um estado de parada designado $h$, é ainda mais fácil: então a sentença $\alpha(M, w)$

$$\exists x \, \exists y \, Q_h(x, y)$$

exprime que a máquina eventualmente para.

**Proposição 32.10.** *Se $m < k$, então $\tau(M, w) \vDash \overline{m} < \overline{k}$*

*Prova.* Exercício. □

## 32.7 Verificando a Representação

A fim de verificar que nossa representação funciona, temos de provar duas coisas. Primeiro, temos de mostrar que se $M$ para na entrada $w$, então $\tau(M, w) \rightarrow \alpha(M, w)$ é válida. Em seguida, temos de mostrar a recíproca, isto é, que se $\tau(M, w) \rightarrow \alpha(M, w)$ é válida, então $M$ de fato eventualmente para quando executada na entrada $w$.

A estratégia para prová-las é bem diferente. Para o primeiro resultado, temos de mostrar que a sentença da lógica de primeira ordem (a saber, $\tau(M, w) \rightarrow \alpha(M, w)$) é válida. A maneira mais fácil de fazer isso é dar a derivação. Nossa prova, porém, deve funcionar para todos os $M$ e $w$, de modo que não há realmente uma única sentença para a qual tenhamos de dar a derivação, mas infinitas. Assim, o melhor que podemos fazer é provar por indução que, sejam quais forem $M$ e $w$, e por mais passos que $M$ leve para parar na entrada $w$, haverá a derivação de $\tau(M, w) \rightarrow \alpha(M, w)$.

Naturalmente, nossa indução procederá sobre o número de passos que $M$ leva antes de atingir uma configuração de parada. Em nossa prova indutiva, estabeleceremos que para cada passo $n$ da execução de $M$ na entrada $w$, $\tau(M, w) \vDash \chi(M, w, n)$, em que $\chi(M, w, n)$ descreve corretamente a configuração de $M$ executada em $w$ após $n$ passos. Ora, se $M$ para na entrada $w$ após, digamos, $n$ passos, $\chi(M, w, n)$ descreverá uma configuração de parada. Mostraremos também que $\chi(M, w, n) \vDash \alpha(M, w)$ sempre que $\chi(M, w, n)$ descreve uma configuração de parada. Assim, se $M$ para na entrada $w$, então para algum $n$, $M$ estará em uma configuração de parada após $n$ passos. Logo, $\tau(M, w) \vDash \chi(M, w, n)$ em que $\chi(M, w, n)$ descreve uma configuração de parada, e como nesse caso $\chi(M, w, n) \vDash \alpha(M, w)$, obtemos que $T(M, w) \vDash \alpha(M, w)$, isto é, que $\vDash \tau(M, w) \rightarrow \alpha(M, w)$.

A estratégia para a recíproca é bem diferente. Aqui supomos que $\vDash \tau(M, w) \rightarrow \alpha(M, w)$ e temos de provar que $M$ para na entrada $w$. Da hipótese obtemos

que $\tau(M,w) \vDash \alpha(M,w)$, isto é, $\alpha(M,w)$ é verdadeira em toda estrutura em que $\tau(M,w)$ é verdadeira. Assim, descreveremos a estrutura $\mathfrak{M}$ em que $\tau(M,w)$ é verdadeira: seu domínio será $\mathbb{N}$, e a interpretação de todos os $Q_q$ e $S_\sigma$ será dada pelas configurações de $M$ durante uma execução na entrada $w$. Assim, por exemplo, $\mathfrak{M} \vDash Q_q(\overline{m},\overline{n})$ se, e somente se, $T$, quando executada na entrada $w$ por $n$ passos, está no estado $q$ e examinando o quadrado $m$. Ora, como $\tau(M,w) \vDash \alpha(M,w)$ por hipótese, e como $\mathfrak{M} \vDash \tau(M,w)$ por construção, $\mathfrak{M} \vDash \alpha(M,w)$. Mas $\mathfrak{M} \vDash \alpha(M,w)$ se, e somente se, há algum $n \in |\mathfrak{M}| = \mathbb{N}$ tal que $M$, executada na entrada $w$, está em uma configuração de parada após $n$ passos.

**Definição 32.11.** Seja $\chi(M,w,n)$ a sentença

$$Q_q(\overline{m},\overline{n}) \wedge S_{\sigma_0}(\overline{0},\overline{n}) \wedge \cdots \wedge S_{\sigma_k}(\overline{k},\overline{n}) \wedge \forall x\,(\overline{k} < x \to S_0(x,\overline{n}))$$

em que $q$ é o estado de $M$ no instante $n$, $M$ está examinando o quadrado $m$ no instante $n$, o quadrado $i$ contém o símbolo $\sigma_i$ no instante $n$ para $0 \leq i \leq k$, e $k$ é o quadrado não-vazio mais à direita da fita no instante 0, ou o quadrado mais à direita que o cabeçote de fita visitou após $n$ passos, o que for maior.

**Lema 32.12.** *Se $M$ executada na entrada $w$ está em uma configuração de parada após $n$ passos, então $\chi(M,w,n) \vDash \alpha(M,w)$.*

*Prova.* Suponha que $M$ pare para a entrada $w$ após $n$ passos. Há algum estado $q$, quadrado $m$ e símbolo $\sigma$ tais que:

1. Após $n$ passos, $M$ está no estado $q$ examinando o quadrado $m$ no qual aparece $\sigma$.

2. A função de transição $\delta(q,\sigma)$ é indefinida.

$\chi(M,w,n)$ é a descrição dessa configuração e incluirá as cláusulas $Q_q(\overline{m},\overline{n})$ e $S_\sigma(\overline{m},\overline{n})$. Essas cláusulas juntas implicam $\alpha(M,w)$:

$$\exists x\,\exists y\,(\bigvee_{\langle q,\sigma\rangle \in X} (Q_q(x,y) \wedge S_\sigma(x,y)))$$

já que $Q_{q'}(\overline{m},\overline{n}) \wedge S_{\sigma'}(\overline{m},\overline{n}) \vDash \bigvee_{\langle q,\sigma\rangle \in X}(Q_q(\overline{m},\overline{n}) \wedge S_\sigma(\overline{m},\overline{n}))$, pois $\langle q',\sigma'\rangle \in X$. □

Assim, se $M$ para na entrada $w$, então há algum $n$ tal que $\chi(M,w,n) \vDash \alpha(M,w)$. Mostraremos agora que para qualquer instante $n$, $\tau(M,w) \vDash \chi(M,w,n)$.

**Lema 32.13.** *Para cada $n$, se $M$ não parou após $n$ passos, $\tau(M,w) \vDash \chi(M,w,n)$.*

*Prova.* Base da indução: Se $n = 0$, então as fórmulas componentes de $\chi(M, w, 0)$ são também fórmulas componentes de $\tau(M, w)$, logo implicadas por ela.

Hipótese de indução: Se $M$ não parou antes do $n$-ésimo passo, então $\tau(M, w) \vDash \chi(M, w, n)$. Temos de mostrar que (a menos que $\chi(M, w, n)$ descreva uma configuração de parada), $\tau(M, w) \vDash \chi(M, w, n + 1)$.

Suponha $n > 0$ e que, após $n$ passos, $M$ iniciada em $w$ esteja no estado $q$ examinando o quadrado $m$. Como $M$ não para após $n$ passos, deve haver no programa de $M$ uma instrução de uma das três formas seguintes:

1. $\delta(q, \sigma) = \langle q', \sigma', R\rangle$
2. $\delta(q, \sigma) = \langle q', \sigma', L\rangle$
3. $\delta(q, \sigma) = \langle q', \sigma', N\rangle$

Consideraremos cada um desses três casos por sua vez.

1. Suponha que haja uma instrução da forma (1). Por Definição 32.9(3a), isso significa que

$$\begin{aligned}&\forall x\, \forall y\, ((Q_q(x, y) \wedge S_\sigma(x, y)) \rightarrow \\ &\qquad (Q_{q'}(x', y') \wedge S_{\sigma'}(x, y') \wedge \varphi(x, y)))\end{aligned}$$

   é uma fórmula componente de $\tau(M, w)$. Isso implica a seguinte sentença (instanciação universal, $\overline{m}$ por $x$ e $\overline{n}$ por $y$):

$$\begin{aligned}&(Q_q(\overline{m}, \overline{n}) \wedge S_\sigma(\overline{m}, \overline{n})) \rightarrow \\ &\qquad (Q_{q'}(\overline{m}', \overline{n}') \wedge S_{\sigma'}(\overline{m}, \overline{n}') \wedge \varphi(\overline{m}, \overline{n})).\end{aligned}$$

   Por hipótese de indução, $\tau(M, w) \vDash \chi(M, w, n)$, isto é,

$$\begin{aligned}&Q_q(\overline{m}, \overline{n}) \wedge S_{\sigma_0}(\overline{0}, \overline{n}) \wedge \cdots \wedge S_{\sigma_k}(\overline{k}, \overline{n}) \wedge \\ &\qquad \forall x\, (\overline{k} < x \rightarrow S_0(x, \overline{n}))\end{aligned}$$

   Como após $n$ passos o quadrado de fita $m$ contém $\sigma$, a fórmula componente correspondente é $S_\sigma(\overline{m}, \overline{n})$, de modo que isso implica:

$$Q_q(\overline{m}, \overline{n}) \wedge S_\sigma(\overline{m}, \overline{n})$$

   Obtemos agora

$$\begin{aligned}&Q_{q'}(\overline{m}', \overline{n}') \wedge S_{\sigma'}(\overline{m}, \overline{n}') \wedge \\ &\qquad S_{\sigma_0}(\overline{0}, \overline{n}') \wedge \cdots \wedge S_{\sigma_k}(\overline{k}, \overline{n}') \wedge \\ &\qquad \forall x\, (\overline{k} < x \rightarrow S_0(x, \overline{n}'))\end{aligned}$$

como segue: A primeira linha vem diretamente do consequente do condicional precedente, por modus ponens. Cada fórmula componente na linha do meio—que exclui $S_{\sigma_m}(\overline{m}, \overline{n}')$—decorre da fórmula componente correspondente em $\chi(M, w, n)$ junto com $\varphi(\overline{m}, \overline{n})$.

Se $m < k$, $\tau(M, w) \vdash \overline{m} < \overline{k}$ (Proposição 32.10) e, por transitividade de $<$, temos $\forall x\,(\overline{k} < x \to \overline{m} < x)$. Se $m = k$, então $\forall x\,(\overline{k} < x \to \overline{m} < x)$ apenas por lógica. A última linha decorre então da fórmula componente correspondente em $\chi(M, w, n)$, de $\forall x\,(\overline{k} < x \to \overline{m} < x)$ e de $\varphi(\overline{m}, \overline{n})$. Se $m < k$, isto já é $\chi(M, w, n+1)$.

Agora suponha $m = k$. Nesse caso, após $n+1$ passos, o cabeçote de fita também visitou o quadrado $k+1$, que agora é o quadrado mais à direita visitado. Assim, $\chi(M, w, n+1)$ tem uma nova fórmula componente, $S_0(\overline{k}', \overline{n}')$, e a última fórmula componente é $\forall x\,(\overline{k}' < x \to S_0(x, \overline{n}'))$. Temos de verificar que essas duas sentenças também são implicadas.

Já temos $\forall x\,(\overline{k} < x \to S_0(x, \overline{n}'))$. Em particular, isso nos dá $\overline{k} < \overline{k}' \to S_0(\overline{k}', \overline{n}')$. Do axioma $\forall x\, x < x'$ obtemos $\overline{k} < \overline{k}'$. Por modus ponens, segue-se $S_0(\overline{k}', \overline{n}')$.

Além disso, como $\tau(M, w) \vdash \overline{k} < \overline{k}'$, o axioma da transitividade de $<$ nos dá $\forall x\,(\overline{k}' < x \to S_0(x, \overline{n}'))$. (Deixamos a verificação disso como exercício.)

2. Suponha que haja uma instrução da forma (2). Então, por Definição 32.9(3b),

$$\begin{aligned}
&\forall x\,\forall y\,((Q_q(x', y) \wedge S_\sigma(x', y)) \to \\
&\qquad (Q_{q'}(x, y') \wedge S_{\sigma'}(x', y') \wedge \varphi(x, y))) \wedge \\
&\forall y\,((Q_{q_i}(\overline{0}, y) \wedge S_\sigma(\overline{0}, y)) \to \\
&\qquad (Q_{q_j}(\overline{0}, y') \wedge S_{\sigma'}(\overline{0}, y') \wedge \varphi(\overline{0}, y)))
\end{aligned}$$

é uma fórmula componente de $\tau(M, w)$. Se $m > 0$, então seja $l = m - 1$ (isto é, $m = l + 1$). A primeira fórmula componente da sentença acima implica o seguinte:

$$\begin{aligned}
&(Q_q(\overline{l}', \overline{n}) \wedge S_\sigma(\overline{l}', \overline{n})) \to \\
&\qquad (Q_{q'}(\overline{l}, \overline{n}') \wedge S_{\sigma'}(\overline{l}', \overline{n}') \wedge \varphi(\overline{l}, \overline{n}))
\end{aligned}$$

Caso contrário, seja $l = m = 0$ e considere a seguinte sentença implicada pela segunda fórmula componente:

$$\begin{aligned}
&((Q_{q_i}(\overline{0}, \overline{n}) \wedge S_\sigma(\overline{0}, \overline{n})) \to \\
&\qquad (Q_{q_j}(\overline{0}, \overline{n}') \wedge S_{\sigma'}(\overline{0}, \overline{n}') \wedge \varphi(\overline{0}, \overline{n})))
\end{aligned}$$

Qualquer das sentenças implica

$$\begin{aligned} &Q_{q'}(\overline{l}, \overline{n}') \wedge S_{\sigma'}(\overline{m}, \overline{n}') \wedge \\ &\quad S_{\sigma_0}(\overline{0}, \overline{n}') \wedge \cdots \wedge S_{\sigma_k}(\overline{k}, \overline{n}') \wedge \\ &\quad \forall x\, (\overline{k} < x \to S_0(x, \overline{n}')) \end{aligned}$$

como antes. (Note que no primeiro caso, $\overline{l}' \equiv \overline{l+1} \equiv \overline{m}$ e no segundo caso $\overline{l} \equiv \overline{0}$.) Mas isto é justamente $\chi(M, w, n+1)$.

3. O caso (3) é deixado como exercício.

Mostramos que para qualquer $n$, $\tau(M, w) \vDash \chi(M, w, n)$. □

**Lema 32.14.** *Se $M$ para na entrada $w$, então $\tau(M, w) \to \alpha(M, w)$ é válida.*

*Prova.* Por Lema 32.13, sabemos que, para qualquer instante $n$, a descrição $\chi(M, w, n)$ da configuração de $M$ no instante $n$ é implicada por $\tau(M, w)$. Suponha que $M$ pare após $k$ passos. Nesse ponto, ela estará examinando o quadrado $m$, para algum $m \in \mathbb{N}$. Então $\chi(M, w, k)$ descreve uma configuração de parada de $M$, isto é, contém como fórmulas componentes tanto $Q_q(\overline{m}, \overline{k})$ quanto $S_\sigma(\overline{m}, \overline{k})$ com $\delta(q, \sigma)$ indefinida. Assim, por Lema 32.12, $\chi(M, w, k) \vDash \alpha(M, w)$. Mas como $\tau(M, w) \vDash \chi(M, w, k)$, temos $\tau(M, w) \vDash \alpha(M, w)$ e portanto $\tau(M, w) \to \alpha(M, w)$ é válida. □

Para completar a verificação de nossa afirmação, temos também de estabelecer a direção reversa: se $\tau(M, w) \to \alpha(M, w)$ é válida, então $M$ de fato para quando iniciada na entrada $w$.

**Lema 32.15.** *Se $\vDash \tau(M, w) \to \alpha(M, w)$, então $M$ para na entrada $w$.*

*Prova.* Considere a $\mathcal{L}_M$-estrutura $\mathfrak{M}$ com domínio $\mathbb{N}$ que interpreta $\mathrm{o}$ como $0$, $\prime$ como a função sucessor e $<$ como a relação menor-que, e os predicados $Q_q$ e $S_\sigma$ como segue:

$$Q_q^{\mathfrak{M}} = \{\langle m, n\rangle : \begin{array}{l}\text{iniciada em } w, \text{ após } n \text{ passos,} \\ M \text{ está no estado } q \text{ examinando o quadrado } m\end{array}\}$$

$$S_\sigma^{\mathfrak{M}} = \{\langle m, n\rangle : \begin{array}{l}\text{iniciada em } w, \text{ após } n \text{ passos,} \\ \text{o quadrado } m \text{ de } M \text{ contém o símbolo } \sigma\end{array}\}$$

Em outras palavras, construímos a estrutura $\mathfrak{M}$ de modo que ela descreva o que $M$ iniciada na entrada $w$ de fato faz, passo a passo. Claramente, $\mathfrak{M} \vDash \tau(M, w)$. Se $\vDash \tau(M, w) \to \alpha(M, w)$, então também $\mathfrak{M} \vDash \alpha(M, w)$, isto é,

$$\mathfrak{M} \vDash \exists x\, \exists y\, (\bigvee_{\langle q, \sigma\rangle \in X} (Q_q(x, y) \wedge S_\sigma(x, y))).$$

Como $|\mathfrak{M}| = \mathbb{N}$, deve haver $m, n \in \mathbb{N}$ tais que $\mathfrak{M} \vDash Q_q(\overline{m}, \overline{n}) \wedge S_\sigma(\overline{m}, \overline{n})$ para algum $q$ e $\sigma$ tais que $\delta(q, \sigma)$ é indefinida. Pela definição de $\mathfrak{M}$, isso significa que $M$ iniciada na entrada $w$ após $n$ passos está no estado $q$ e lendo o símbolo $\sigma$, e a função de transição é indefinida, isto é, $M$ parou. □

## 32.8 O Problema da Decisão é Insolúvel

**Teorema 32.16.** *O problema da decisão é insolúvel: Não há máquina de Turing $D$ tal que, quando iniciada em uma fita que contém como entrada a sentença $\psi$ da lógica de primeira ordem, $D$ eventualmente para e produz 1 se, e somente se, $\psi$ é válida, e 0 caso contrário.*

*Prova.* Suponha que o problema da decisão fosse solúvel, isto é, suponha que houvesse uma máquina de Turing $D$. Então poderíamos resolver o problema da parada como segue. Construímos uma máquina de Turing $E$ que, dado como entrada o número $e$ da máquina de Turing $M_e$ e a entrada $w$, computa a sentença correspondente $\tau(M_e, w) \to \alpha(M_e, w)$ e para, examinando o quadrado mais à esquerda na fita. A máquina $E \frown D$ então, dada a entrada $e$ e $w$, primeiro computaria $\tau(M_e, w) \to \alpha(M_e, w)$ e depois executaria a máquina do problema da decisão $D$ nessa entrada. $D$ para com saída 1 se, e somente se, $\tau(M_e, w) \to \alpha(M_e, w)$ é válida, e produz 0 caso contrário. Por Lema 32.15 e Lema 32.14, $\tau(M_e, w) \to \alpha(M_e, w)$ é válida se, e somente se, $M_e$ para na entrada $w$. Assim, $E \frown D$, dada a entrada $e$ e $w$, para com saída 1 se, e somente se, $M_e$ para na entrada $w$, e para com saída 0 caso contrário. Em outras palavras, $E \frown D$ resolveria o problema da parada. Mas sabemos, por Teorema 32.8, que não pode existir tal máquina de Turing. □

**Corolário 32.17.** *É indecidível se uma sentença arbitrária da lógica de primeira ordem é satisfatível.*

*Prova.* Suponha que a satisfatibilidade fosse decidível por uma máquina de Turing $S$. Então poderíamos resolver o problema da decisão como segue: Dada como entrada a sentença $B$, mova $\psi$ um quadrado para a direita. Volte ao quadrado 1 e escreva o símbolo $\neg$.

Agora execute a máquina de Turing $S$. Ela eventualmente para com saída 1 (se $\neg\psi$ é satisfatível) ou 0 (se $\neg\psi$ é insatisfatível) na fita. Se há um 1 no quadrado 1, apague-o; se o quadrado 1 está vazio, escreva um 1 e então pare.

Essa máquina de Turing sempre para, e sua saída é 1 se, e somente se, $\neg\psi$ é insatisfatível, e 0 caso contrário. Como $\psi$ é válida se, e somente se, $\neg\psi$ é insatisfatível, a máquina produz 1 se, e somente se, $\psi$ é válida, e 0 caso contrário, isto é, ela resolveria o problema da decisão. □

Portanto, não há máquina de Turing que sempre dê uma resposta "sim" ou "não" correta à pergunta "$\psi$ é uma sentença válida da lógica de primeira

ordem?" No entanto, *há* uma máquina de Turing que sempre dá uma resposta "sim" correta—mas que simplesmente não para se a resposta é "não". Isso decorre do teorema da correção e completude da lógica de primeira ordem, e do fato de que derivações podem ser efetivamente enumeradas.

**Teorema 32.18.** *A validade de sentenças de primeira ordem é semidecidível: Há uma máquina de Turing $E$ que, quando iniciada em uma fita que contém como entrada a sentença $\psi$ da lógica de primeira ordem, $E$ eventualmente para e produz 1 se, e somente se, $\psi$ é válida, mas não para caso contrário.*

*Prova.* Todas as derivações possíveis da lógica de primeira ordem podem ser geradas, uma após a outra, por um algoritmo efetivo. A máquina $E$ faz isso e, quando encontra a derivação que mostra que $\vdash \psi$, ela para com saída 1. Pelo teorema da correção, se $E$ para com saída 1, é porque $\vDash \psi$. Pelo teorema da completude, se $\vDash \psi$, há a derivação que mostra que $\vdash \psi$. Como $E$ gera sistematicamente todas as derivações possíveis, ela eventualmente encontrará uma que mostra $\vdash \psi$, de modo que eventualmente parará com saída 1. □

## 32.9 Teorema de Trakhtenbrot

Na Seção 32.6 definimos as sentenças $\tau(M, w)$ e $\alpha(M, w)$ para uma máquina de Turing $M$ e uma cadeia de entrada $w$. Em seguida, mostramos em Lema 32.14 e Lema 32.15 que $\tau(M, w) \to \alpha(M, w)$ é válida se, e somente se, $M$, iniciada na entrada $w$, eventualmente para. Como o Problema da Parada é indecidível, isso implica que a validade e a satisfatibilidade de sentenças da lógica de primeira ordem são indecidíveis (Teorema 32.16 e Corolário 32.17).

Mas a validade e a satisfatibilidade de sentenças são definidas para estruturas arbitrárias, finitas ou infinitas. Você poderia suspeitar que é mais fácil decidir se a sentença é satisfatível em uma estrutura finita (ou válida em todas as estruturas finitas). Podemos adaptar a prova da insolubilidade do problema da decisão de modo que ela mostre que não é esse o caso.

Primeiro, se você voltar à prova de Lema 32.15, verá que o que fizemos ali foi produzir um modelo $\mathfrak{M}$ de $\tau(M, w)$ que descreve exatamente o que a máquina $M$ faz quando iniciada na entrada $w$. O domínio daquele modelo era $\mathbb{N}$, isto é, infinito. Mas se $M$ de fato para na entrada $w$, podemos construir um modelo finito $\mathfrak{M}'$ da mesma maneira. Suponha que $M$ iniciada na entrada $w$ pare após $k$ passos. Tome como domínio $|\mathfrak{M}'|$ o conjunto $\{0, \ldots, n\}$, em que $n$ é o maior entre $k$ e o comprimento de $w$, e seja

$$\prime^{\mathfrak{M}'}(x) = \begin{cases} x+1 & \text{se } x < n \\ n & \text{caso contrário,} \end{cases}$$

e $\langle x, y\rangle \in <^{\mathfrak{M}'}$ se, e somente se, $x < y$ ou $x = y = n$. Quanto ao resto, $\mathfrak{M}'$ é definida tal como $\mathfrak{M}$. Pela definição de $\mathfrak{M}'$, tal como na prova de Lema 32.15,

$\mathfrak{M}' \vDash \tau(M, w)$. E como supusemos que $M$ para na entrada $w$, $\mathfrak{M}' \vDash \alpha(M, w)$. Assim, $\mathfrak{M}'$ é um modelo finito de $\tau(M, w) \wedge \alpha(M, w)$ (note que substituímos $\rightarrow$ por $\wedge$).

Estamos a meio caminho de uma prova: mostramos que se $M$ para na entrada $w$, então $\tau(M, w) \wedge \alpha(M, w)$ tem um modelo finito. Infelizmente, a recíproca disso não vale, isto é, há máquinas de Turing que não param em alguma entrada $w$, mas $\tau(M, w) \wedge \alpha(M, w)$ ainda assim tem um modelo finito. Por exemplo, considere a máquina $M$ com o único estado $q_0$ e a instrução $\delta(q_0, 0) = \langle q_0, 0, N\rangle$. Iniciada na entrada vazia $w = \Lambda$, essa máquina nunca para: está em um laço infinito, mas não altera a fita nem move o cabeçote. Todas as configurações são as mesmas (mesmo estado, mesma posição do cabeçote, mesmo conteúdo da fita). Podemos definir uma estrutura finita $\mathfrak{M}''$ que satisfaz $\tau(M, \Lambda) \wedge \alpha(M, \Lambda)$ (exercício). Podemos, no entanto, modificar $\tau(M, w)$ de modo adequado para que tais estruturas sejam descartadas.

Considere as sentenças que descrevem a operação da máquina de Turing $M$ na entrada $w = \sigma_{i_1} \ldots \sigma_{i_k}$:

1. Axiomas que descrevem números e $<$ (tal como na definição de $\tau(M, w)$ na Seção 32.6).

2. Axiomas que descrevem a configuração de entrada: tal como na definição de $\tau(M, w)$.

3. Axiomas que descrevem a transição de uma configuração para a seguinte:

   Para o que segue, seja $\varphi(x, y)$ como antes, e seja

   $$\psi(y) \equiv \forall x\, (x < y \rightarrow x \neq y).$$

   a) Para toda instrução $\delta(q_i, \sigma) = \langle q_j, \sigma', R\rangle$, a sentença:

   $$\begin{aligned}&\forall x\, \forall y\, ((Q_{q_i}(x, y) \wedge S_\sigma(x, y)) \rightarrow \\ &\qquad (Q_{q_j}(x', y') \wedge S_{\sigma'}(x, y') \wedge \varphi(x, y) \wedge \psi(y')))\end{aligned}$$

   b) Para toda instrução $\delta(q_i, \sigma) = \langle q_j, \sigma', L\rangle$, a sentença

   $$\begin{aligned}&\forall x\, \forall y\, ((Q_{q_i}(x', y) \wedge S_\sigma(x', y)) \rightarrow \\ &\qquad (Q_{q_j}(x, y') \wedge S_{\sigma'}(x', y') \wedge \varphi(x, y))) \wedge \\ &\forall y\, ((Q_{q_i}(\overline{0}, y) \wedge S_\sigma(\overline{0}, y)) \rightarrow \\ &\qquad (Q_{q_j}(\overline{0}, y') \wedge S_{\sigma'}(\overline{0}, y') \wedge \varphi(\overline{0}, y) \wedge \psi(y')))\end{aligned}$$

   c) Para toda instrução $\delta(q_i, \sigma) = \langle q_j, \sigma', N\rangle$, a sentença:

   $$\begin{aligned}&\forall x\, \forall y\, ((Q_{q_i}(x, y) \wedge S_\sigma(x, y)) \rightarrow \\ &\qquad (Q_{q_j}(x, y') \wedge S_{\sigma'}(x, y') \wedge \varphi(x, y) \wedge \psi(y')))\end{aligned}$$

Como você pode ver, as sentenças que descrevem as transições de $M$ são as mesmas que a sentença correspondente em $\tau(M, w)$, exceto que adicionamos $\psi(y')$ ao final. $\psi(y')$ garante que o número $y'$ da "próxima" configuração é diferente de todos os números anteriores $\mathsf{o}, \mathsf{o}', \ldots$.

Seja $\tau'(M, w)$ a conjunção de todas as sentenças acima para a máquina de Turing $M$ e a entrada $w$.

**Lema 32.19.** *Se $M$ iniciada na entrada $w$ para, então $\tau'(M, w) \wedge \alpha(M, w)$ tem um modelo finito.*

*Prova.* Seja $\mathfrak{M}'$ como na prova de Lema 32.15, exceto que

$$\begin{aligned} |\mathfrak{M}'| &= \{0, \ldots, n\}, \\ '^{\mathfrak{M}'}(x) &= \begin{cases} x+1 & \text{se } x < n \\ n & \text{caso contrário,} \end{cases} \\ \langle x, y\rangle \in <^{\mathfrak{M}'} &\text{ sse } x < y \text{ ou } x = y = n, \end{aligned}$$

em que $n = \max(k, \mathrm{len}(w))$ e $k$ é o menor número tal que $M$ iniciada na entrada $w$ parou após $k$ passos. Deixamos como exercício a verificação de que $\mathfrak{M}' \vDash \tau'(M, w) \wedge E(M, w)$. □

**Lema 32.20.** *Se $\tau'(M, w) \wedge \alpha(M, w)$ tem um modelo finito, então $M$ iniciada na entrada $w$ para.*

*Prova.* Mostramos a contrapositiva. Suponha que $M$ iniciada em $w$ não pare. Se $\tau'(M, w) \wedge \alpha(M, w)$ não tem modelo algum, terminamos. Então suponha que $\mathfrak{M}$ seja um modelo de $\tau(M, w) \wedge \alpha(M, w)$. Temos de mostrar que ele não pode ser finito.

Podemos provar, tal como em Lema 32.13, que se $M$, iniciada na entrada $w$, não parou após $n$ passos, então $\tau'(M, w) \vDash \chi(M, w, n) \wedge \psi(\overline{n})$. Como $M$ iniciada na entrada $w$ não para, $\tau'(M, w) \vDash \chi(M, w, n) \wedge \psi(\overline{n})$ para todo $n \in \mathbb{N}$. Note que, por Proposição 32.10, $\tau'(M, w) \vDash \overline{k} < \overline{n}$ para todo $k < n$. Além disso, $\psi(\overline{n}) \vDash \overline{k} < \overline{n} \to \overline{k} \neq \overline{n}$. Assim, $\mathfrak{M} \vDash \overline{k} \neq \overline{n}$ para todo $k < n$, isto é, os infinitos termos $\overline{k}$ devem ter todos valores diferentes em $\mathfrak{M}$. Mas isso requer que $|\mathfrak{M}|$ seja infinito, de modo que $\mathfrak{M}$ não pode ser um modelo finito de $\tau'(M, w) \wedge \alpha(M, w)$. □

**Teorema 32.21 (Teorema de Trakhtenbrot).** *É indecidível se uma sentença arbitrária da lógica de primeira ordem tem um modelo finito (isto é, é finitamente satisfatível).*

*Prova.* Suponha que houvesse uma máquina de Turing $F$ que decide o problema da satisfatibilidade finita. Então, dada qualquer máquina de Turing $M$ e entrada $w$, poderíamos computar a sentença $\tau'(M, w) \wedge \alpha(M, w)$ e usar $F$ para decidir se ela tem um modelo finito. Por Lemas 32.19 e 32.20, ela tem se,

e somente se, $M$ iniciada na entrada $w$ para. Assim, poderíamos usar $F$ para resolver o problema da parada, que sabemos ser insolúvel. □

**Corolário 32.22.** *Não pode haver um sistema de derivação que seja correto e completo para a validade* finita*, isto é, um sistema de derivação que tenha $\vdash \psi$ se, e somente se, $\mathfrak{M} \vDash \psi$ para toda estrutura finita $\mathfrak{M}$.*

*Prova.* Exercício. □

## Problemas

**Problema 32.1.** Você consegue pensar em uma maneira de descrever máquinas de Turing que não exija que os estados e os símbolos do alfabeto sejam listados explicitamente? Você pode definir sua própria noção de máquina "padrão", mas diga algo sobre por que toda máquina de Turing pode ser computada por uma máquina "padrão" no seu novo sentido.

**Problema 32.2.** O problema da Parada com Três (3-Parada) é o problema de dar um procedimento de decisão para determinar se uma máquina de Turing escolhida arbitrariamente para ou não para uma entrada de três 1 em uma fita que, fora isso, está em branco. Prove que o problema 3-Parada é insolúvel.

**Problema 32.3.** Mostre que se o problema da parada é solúvel para pares de máquina de Turing e entrada $M_e$ e $n$ em que $e \neq n$, então ele também é solúvel para os casos em que $e = n$.

**Problema 32.4.** Provamos que o problema da parada é insolúvel se a entrada é um número $e$, que identifica uma máquina de Turing $M_e$ por meio de uma enumeração de todas as máquinas de Turing. E se permitirmos a descrição de máquinas de Turing de Seção 32.2 diretamente como entrada? Pode haver uma máquina de Turing que decide o problema da parada, mas que recebe como entrada descrições de máquinas de Turing em vez de índices? Explique por que sim ou por que não.

**Problema 32.5.** Mostre que a função *parcial* $s'$ definida como

$$s'(e) = \begin{cases} 1 & \text{se a máquina } M_e \text{ para na entrada } e \\ \text{indefinida} & \text{se a máquina } M_e \text{ não para na entrada } e \end{cases}$$

*é* Turing-computável.

**Problema 32.6.** Prove Proposição 32.10. (Dica: use indução em $k - m$).

**Problema 32.7.** Complete o caso (3) da prova de Lema 32.13.

**Problema 32.8.** Dê a derivação de $S_{\sigma_i}(\overline{i}, \overline{n}')$ a partir de $S_{\sigma_i}(\overline{i}, \overline{n})$ e $\varphi(m, n)$ (supondo $i \neq m$, isto é, $i < m$ ou $m < i$).

**Problema 32.9.** Dê a derivação de $\forall x\,(\overline{k}' < x \to S_0(x, \overline{n}'))$ a partir de $\forall x\,(\overline{k} < x \to S_0(x, \overline{n}'))$, $\forall x\, x < x'$ e $\forall x\,\forall y\,\forall z\,((x < y \wedge y < z) \to x < z)$.)

**Problema 32.10.** Seja $M$ uma máquina de Turing com o único estado $q_0$ e a única instrução $\delta(q_0, 0) = \langle q, 0, N\rangle$. Seja $|\mathfrak{M}''| = \{0, 1, 2\}$, $\prime^{\mathfrak{M}''}(0) = \prime^{\mathfrak{M}'}(1) = 1$ e $\prime^{\mathfrak{M}''}(2) = 2$, e $<^{\mathfrak{M}''} = \{\langle 0, 1\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle\}$. Defina $Q_{q_0}^{\mathfrak{M}''}$, $S_0^{\mathfrak{M}''}$ e $S_\triangleright^{\mathfrak{M}''}$ de modo que $\tau(M, \Lambda)$ e $\alpha(M, \Lambda)$ se tornem verdadeiras e explique por que o são. Dica: Observe que $\delta(q_0, \triangleright)$ é indefinida. Garanta que

$$Q_{q_0}(\overline{1}, \overline{n}) \wedge S_\triangleright(\overline{0}, \overline{n}) \wedge \forall x\,(\overline{0} < x \to S_0(x, \overline{n})) \quad \text{para todo } n \in \mathbb{N}$$
$$\exists y\,(Q_{q_0}(\overline{0}, y) \wedge S_\triangleright(\overline{0}, y))$$

são ambas verdadeiras em $\mathfrak{M}''$.

**Problema 32.11.** Complete a prova de Lema 32.19 provando que $\mathfrak{M}' \vDash \tau(M, w) \wedge E(M, w)$.

**Problema 32.12.** Complete a prova de Lema 32.20 provando que se $M$, iniciada na entrada $w$, não parou após $n$ passos, então $\tau'(M, w) \vDash \psi(\overline{n})$.

**Problema 32.13.** Prove Corolário 32.22. Observe que $\psi$ é satisfeita em toda estrutura finita se, e somente se, $\neg\psi$ não é finitamente satisfatível. Explique por que a satisfatibilidade finita é semidecidível no sentido de Teorema 32.18. Use isso para argumentar que se houvesse um sistema de derivação para a validade finita, então a satisfatibilidade finita seria decidível.

# Parte VII

# Incompleteness

Material in this part covers the incompleteness theorems. It depends on material in the parts on first-order logic (esp., the proof system), the material on recursive functions (in the computability part). It is based on Jeremy Avigad's notes with revisions by Richard Zach.

## Capítulo 33

# Introduction to Incompleteness

# Capítulo 34

# Arithmetization of Syntax

Note that arithmetization for signed tableaux is not yet available.

# Capítulo 35

# Representability in Q

This chapter depends on material in the chapter on computability theory, but can be left out if that hasn't been covered. It's currently a basic conversion of Jeremy Avigad's notes, has not been revised, and is missing exercises.

## Capítulo 36

# Theories and Computability

## Capítulo 37

# Incompleteness and Provability

# Parte VIII

# Second-order Logic

This is the beginnings of a part on second-order logic.

# Capítulo 38

# Syntax and Semantics

Basic syntax and semantics for SOL covered so far. As a chapter it's too short. Substitution for second-order variables has to be covered to be able to talk about derivação systems for SOL, and there's some subtle issues there.

## Capítulo 39

# Metatheory of Second-order Logic

# Capítulo 40

# Second-order Logic and Set Theory

This section deals with coding powersets and the continuum in second-order logic. The results are stated but proofs have yet to be filled in. There are no problems yet—and the definitions and results themselves may have problems. Use with caution and report anything that's false or unclear.

# Parte IX

# The Lambda Calculus

This part deals with the lambda calculus. The introduction chapter is based on Jeremy Avigad's notes; part of it is now redundant and covered in later chapters. The chapters on syntax, Church–Rosser property, and lambda definability were produced by Zesen Qian during his Mitacs summer internship. They still have to be reviewed and revised.

# Capítulo 41

# Introduction

This chapter consists of Jeremy's original concise notes on the lambda calculus. The sections need to be combined, and the material on lambda definability merged with the material in the separate, more detailed chapter on lambda definability.

## Capítulo 42

# Syntax

## Capítulo 43

# The Church–Rosser Property

# Capítulo 44

# Lambda Definability

This chapter is experimental. It needs more explanation, and the material should be structured better into definitions and propositions with proofs, and more examples.

# Parte X

# Many-valued Logic

This part contains draft material on propositional many-valued logics.

## Capítulo 45

# Syntax and Semantics

## Capítulo 46

# Three-valued Logics

## Capítulo 47

# Infinite-valued Logics

## Capítulo 48

# Sequent Calculus

# Parte XI

# Normal Modal Logics

This part covers the metatheory of normal modal logics. It currently consists of Aldo Antonelli's notes on classical correspondence theory for basic modal logic.

## Capítulo 49

# Syntax and Semantics

## Capítulo 50

# Frame Definability

## Capítulo 51

# Axiomatic Derivações

## Capítulo 52

# Completeness and Canonical Models

## Capítulo 53

# Filtrations and Decidability

# Capítulo 54

# Modal Tableaux

Draft chapter on prefixed tableaux for modal logic. Needs more examples, completeness proofs, and discussion of how one can find countermodels from unsuccessful searches for closed tableaux.

# Capítulo 55

# Modal Sequent Calculus

Draft chapter on sequent calculi for modal logic. Needs more examples, soundness and completeness proofs.

# Parte XII

# Applied Modal Logic

This part contains experimental draft material on some applications of modal logic, such as temporal and epistemic logics.

# Capítulo 56

# Temporal Logics

This chapter covers temporal logics.

# Capítulo 57

# Epistemic Logics

This chapter covers the metatheory of epistemic logics. It is structured in a similar way to Aldo Antonelli's notes on classical basic modal logic, but has been rewritten by Audrey Yap in order to add material on bisimulation and dynamic epistemic logics.

# Parte XIII

# Intuitionistic Logic

## Capítulo 58

# Introduction

# Capítulo 59

# Semantics

This chapter collects definitions for semantics for intuitionistic logic. So far only Kripke and topological semantics are covered. There are no examples yet, either of how models make formulas true or of proofs that formulas are valid.

# Capítulo 60

# Soundness and Completeness

This chapter collects soundness and completeness results for propositional intuitionistic logic. It needs an introduction. The completeness proof makes use of facts about provability that should be stated and proved explicitly somewhere.

# Capítulo 61

# Intuitionistic Tableaux

Draft chapter on prefixed tableaux for intuitionistic logic. Needs more examples, completeness proofs, and discussion of how one can find countermodels from unsuccessful searches for closed tableaux.

# Capítulo 62

# Propositions as Types

This is a *very experimental* draft of a chapter on the Curry–Howard correspondence. It needs more explanation and motivation, and there are probably errors and omissions. The proof of normalization should be reviewed and expanded. There are no examples for the product type. Permutation and simplification conversions are not covered. It will make a lot more sense once there is also material on the (typed) lambda calculus which is basically presupposed here. Use with extreme caution.

# Parte XIV

# Counterfactuals

## Capítulo 63

# Introduction

## Capítulo 64

# Minimal Change Semantics

# Parte XV

# Set Theory

# Capítulo 65

# A Concepção Iterativa

## 65.1 Extensionalidade

O primeiro ponto a notar é que os conjuntos são individuados pelos seus membros. Mais precisamente:

**Extensionalidade (Extensionalidade).** Se os conjuntos $A$ e $B$ têm os mesmos membros, então $A$ e $B$ são o mesmo conjunto.

$$\forall A \, \forall B \, (\forall x \, (x \in A \leftrightarrow x \in B) \rightarrow A = B)$$

Assumimos isto ao longo de Parte I. Mas vale a pena repetir. O axioma de extensionalidade exprime a ideia fundamental de que um conjunto é determinado pelos seus membros. (Assim, os conjuntos podem contrastar-se com os *conceitos*, nos quais precisamente os mesmos objetos podem cair sob muitos conceitos diferentes.)

Por que aceitar este princípio? Ora, é plausível dizer que qualquer recusa da extensionalidade é uma decisão de abandonar tudo o que possa ser chamado *teoria dos conjuntos*. A teoria dos conjuntos não é mais nem menos do que a teoria de coleções extensionais.

O verdadeiro desafio na Parte XV, contudo, é estabelecer princípios que nos digam *que conjuntos existem*. E acaba por se verificar que a única resposta verdadeiramente "óbvia" a esta questão é provadamente errada.

## 65.2 Paradoxo de Russell (de novo)

Na Parte I, trabalhamos com uma teoria ingênua dos conjuntos. Mas, segundo uma concepção *muito* ingênua, os conjuntos são apenas as extensões dos predicados. Este pensamento ingênuo imporia o seguinte princípio:

*Compreensão ingênua.* $\{x : \varphi(x)\}$ existe para qualquer fórmula $\varphi$.

Por tentador que seja este princípio, é provadamente inconsistente. Vimo-lo na Seção 1.6, mas o resultado é tão importante, e tão direto, que vale a pena repetir. Ipsis verbis.

**Teorema 65.1 (Paradoxo de Russell).** *Não existe conjunto* $R = \{x : x \notin x\}$

*Prova.* Se $R = \{x : x \notin x\}$ existisse, então $R \in R$ sse $R \notin R$, o que é uma contradição. □

Russell descobriu este resultado em junho de 1901. (Não colocou, porém, o paradoxo exatamente na forma em que o acabamos de apresentar, pois estava a considerar a teoria dos conjuntos de Frege, tal como delineada em *Grundgesetze*. Voltaremos a isto na Seção 65.6.) Russell escreveu a Frege a 16 de junho de 1902, explicando a inconsistência no sistema de Frege. Para a correspondência, e um pouco de contexto, ver Heijenoort (1967, pp. 124–8).

Vale a pena enfatizar que esta prova de duas linhas é um resultado de *lógica pura*. De fato, usamos implicitamente um axioma (não lógico?) de extensionalidade na nossa notação $\{x : x \notin x\}$; pois $\{x : \varphi(x)\}$ deve ser *o único* (pela extensionalidade) conjunto dos $\varphi$s, se algum existir. Mas podemos evitar até o vestígio da extensionalidade, bastando enunciar o resultado assim: *não existe conjunto cujos membros sejam exatamente os conjuntos que não são membros de si próprios*. E isto pouco tem a ver com conjuntos. Como o próprio Russell observou, raciocínio rigorosamente análogo leva-nos a concluir: *nenhum homem barbeia exatamente os homens que não se barbeiam a si próprios*. Ou: *nenhum pug cheira exatamente os pugs que não se cheiram a si próprios*. E assim por diante. Esquematicamente, a forma do resultado é apenas:

$$\neg\exists x\forall z(Rzx \leftrightarrow \neg Rzz).$$

E isto não passa de um teorema (esquema) da lógica de primeira ordem. Consequentemente, não podemos evitar o paradoxo de Russell apenas mexendo na nossa teoria dos conjuntos; ele surge antes sequer de *chegarmos* à teoria dos conjuntos. Se formos usar lógica (clássica) de primeira ordem, temos simplesmente de *aceitar* que não existe conjunto $R = \{x : x \notin x\}$.

A consequência é esta. Se quisermos aceitar a compreensão ingênua enquanto *evitamos* a inconsistência, não basta mexer na *teoria dos conjuntos*. Teríamos, em vez disso, de reformular a nossa *lógica*.

É claro que já foram apresentadas teorias dos conjuntos com lógicas não clássicas. Mas são—no mínimo—não standard. A abordagem usual ao paradoxo de Russell é tratá-lo como uma prova direta de não existência e depois tentar aprender a viver com ela. É essa a abordagem que seguiremos.

## 65.3 Predicativo e Impredicativo

O conjunto de Russell, $R$, foi definido via $\{x : x \notin x\}$. Dito com mais detalhe, $R$ seria o conjunto que contém todos e apenas aqueles conjuntos que não são membros de si próprios. Assim, ao definir $R$, quantificamos sobre o domínio que conteria $R$ (se este existisse).

Isto é uma definição *impredicativa*. Mais em geral, podemos dizer que uma definição é impredicativa sse quantifica sobre um domínio que contém o objeto que está a ser definido.

Na sequência dos paradoxos, Whitehead, Russell, Poincaré e Weyl rejeitaram tais definições impredicativas como "viciosamente circulares":

> Uma análise dos paradoxos a evitar mostra que todos eles resultam de uma espécie de círculo vicioso. Os círculos viciosos em questão surgem ao supor que uma coleção de objetos pode conter membros que só podem ser definidos por meio da coleção como um todo[. . . . ¶]
>
> O princípio que nos permite evitar totalidades ilegítimas pode enunciar-se do seguinte modo: "Tudo o que envolve *todos* os membros de uma coleção não pode ser um dos membros da coleção"; ou, inversamente: "Se, supondo que uma certa coleção tivesse um todo, ela teria membros só definíveis em termos desse todo, então a dita coleção não tem todo." Chamaremos a isto o "princípio do círculo vicioso", porque nos permite evitar os círculos viciosos envolvidos na suposição de totalidades ilegítimas. (Whitehead and Russell, 1910, p. 37)

Se os acompanharmos na rejeição das definições impredicativas motivada pelo *princípio do círculo vicioso*, então podemos tentar substituir o desastroso esquema de compreensão ingênua (de Seção 65.2) por algo deste gênero:

> *Compreensão predicativa.* Para toda a fórmula $\varphi$ que quantifica apenas sobre conjuntos: existe o conjunto′ $\{x : \varphi(x)\}$.

Enquanto os conjuntos′ não forem conjuntos, não se seguirá contradição.

Infelizmente, a compreensão predicativa não é muito *abrangente*. Afinal, introduz-nos novas entidades, conjuntos′. Logo teremos de considerar fórmulas que quantificam sobre conjuntos′. Se estas derem sempre um conjunto′, então o paradoxo de Russell surgirá de novo, bastando considerar o conjunto′ de todos os conjuntos′ que não são membros de si próprios. Assim, a seguir o mesmo fio de ideias, temos de dizer que uma fórmula que quantifica sobre conjuntos′ produz um conjunto″ correspondente. E então precisaremos de conjuntos‴, conjuntos⁗, etc. Para evitar uma enxurrada de primos, será

mais fácil pensar nestes como conjuntos$_0$, conjuntos$_1$, conjuntos$_2$, conjuntos$_3$, conjuntos$_4$,.... E isto dar-nos-ia entrada na teoria (simples) dos tipos.

Há algumas objeções óbvias a tal teoria (embora não seja óbvio que sejam objeções *esmagadoras*). Em resumo: a teoria resultante é pouco manejável; é prolixa ao postular diferentes tipos de objetos; e não está claro, no fim, que as definições impredicativas sejam sequer *assim tão más*.

Para ilustrar o último ponto, consideremos esta observação de Ramsey:

> podemos referir-nos a um homem como o mais alto de um grupo, identificando-o por meio de uma totalidade da qual ele próprio é membro sem que haja círculo vicioso. (Ramsey, 1925)

O ponto de Ramsey é que "o homem mais alto do grupo" *é* uma definição impredicativa; mas é obviamente perfeitamente legítima.

Alguém poderá responder que, neste caso, poderíamos identificar a pessoa mais alta por meios *predicativos*. Por exemplo, talvez pudéssemos simplesmente apontar para o homem em questão. A objeção às definições impredicativas, então, teria claramente de se limitar a entidades que *só* possam ser identificadas impredicativamente. Mas mesmo assim, seria preciso ouvir mais, sobre por que tal "impredicatividade essencial" seria tão grave.[1]

Admitidamente, as definições impredicativas são péssimas notícias, se quisermos que as definições nos forneçam algo como uma receita para *criar* um objeto. Pois, dada uma definição impredicativa, estar-se-ia genuinamente preso a um círculo vicioso: para criar o objeto especificado impredicativamente, seria preciso *primeiro* criar todos os objetos (incluindo o objeto especificado impredicativamente), uma vez que este é especificado em termos de todos os objetos; logo seria preciso criar o objeto especificado impredicativamente antes de o ter criado. Mas, de novo, isto só é uma objeção séria a conjuntos especificados de modo "essencialmente impredicativo", se pensarmos nos conjuntos como coisas que *criamos*. E nós (provavelmente) não os criamos.

Assim—para o bem ou para o mal—a abordagem que se tornou comum não envolve tomar uma posição rígida sobre (im)predicatividade. Envolve antes o que hoje se considera a abordagem cumulativa-iterativa. No fim, isto permitir-nos-á estratificar os conjuntos em "estágios"—um *pouco* como a abordagem predicativa estratifica entidades em conjuntos$_0$, conjuntos$_1$, conjuntos$_2$, ...—mas não postularemos diferença de natureza entre eles.

## 65.4 A Abordagem Cumulativa-Iterativa

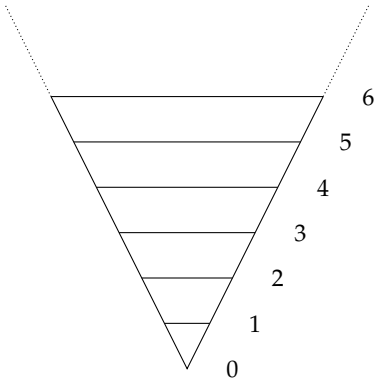
Eis um enunciado um pouco mais completo de como estratificaremos os conjuntos em estágios:

[1] Para mais, ver Linnebo (2010).

> Os conjuntos formam-se em *estágios*. Para cada estágio $S$, há certos estágios que são *anteriores* a $S$. No estágio $S$, cada coleção constituída por conjuntos formados em estágios anteriores a $S$ é formada num conjunto. Não há conjuntos além dos que são formados nos estágios. (Shoenfield, 1977, p. 323)

Isto é um esboço da *concepção cumulativa-iterativa do conjunto*. Servirá de base à teoria formal dos conjuntos que apresentamos em Parte XV.

Exploremos isto com um pouco mais de detalhe. Como Shoenfield descreve o processo, em cada estágio formamos novos conjuntos a partir dos conjuntos que tínhamos disponíveis nos estágios anteriores. Assim, na imagem de Shoenfield, no estágio inicial, estágio 0, não há estágios *anteriores*, e portanto *a fortiori* não há conjuntos disponíveis a partir de estágios anteriores.[2] Logo formamos apenas um conjunto: o conjunto sem membros $\emptyset$. No estágio 1, está exatamente um conjunto disponível a partir de estágios anteriores, logo apenas um conjunto novo é $\{\emptyset\}$. No estágio 2, dois conjuntos estão disponíveis a partir de estágios anteriores, e formamos dois conjuntos novos $\{\{\emptyset\}\}$ e $\{\emptyset, \{\emptyset\}\}$. No estágio 3, quatro conjuntos estão disponíveis a partir de estágios anteriores, logo formamos doze conjuntos novos.... Assim, a imagem cumulativa-iterativa dos conjuntos ficará algo assim (com números a indicar estágios):




Então: por que deveríamos aceitar esta narrativa?

Uma razão é que é uma narrativa agradável e tratável. Dado o fim da narrativa mais óbvia, isto é, a compreensão ingênua, precisamos de algo de substância.

Mas a narrativa não é *apenas* agradável. Temos boa razão para acreditar que qualquer teoria dos conjuntos baseada nesta narrativa será *consistente*. Eis a razão.

[2] Por que deveríamos supor que *existe* um primeiro estágio? Ver a nota de rodapé a *Estágios-são-ordenados* em Seção 66.1.

Dada a concepção cumulativa-iterativa do conjunto, formamos conjuntos em estágios; e os seus membros têm de ser objetos que já estavam disponíveis. Assim, para qualquer estágio $S$, podemos formar o conjunto

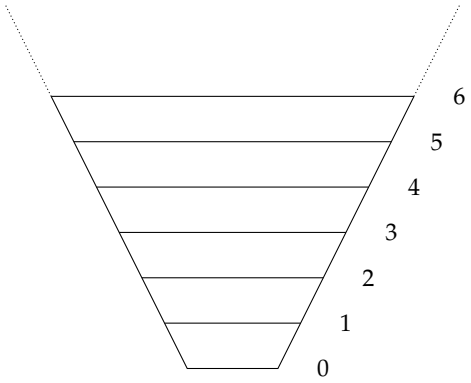
$$R_S = \{x : x \notin x \text{ e } x \text{ já estava disponível antes de } S\}$$

O raciocínio envolvido na prova do paradoxo de Russell estabelece agora que o próprio $R_S$ não está disponível antes do estágio $S$. E isso não é uma contradição. Além disso, se aceitarmos a concepção cumulativa-iterativa do conjunto, nem sequer deveríamos ter *esperado* poder formar o próprio conjunto de Russell. Pois esse seria o conjunto de todos os conjuntos que não são membros de si próprios que "alguma vez estarão disponíveis". Em resumo: o fato de, provadamente, não podermos formar o conjunto de Russell não é *surpreendente*, dada a narrativa cumulativa-iterativa; é antes *previsível*.

## 65.5 Urelementos ou Não?

Nos próximos capítulos, tentaremos extrair axiomas da concepção cumulativa-iterativa do conjunto. Mas, antes de avançar mais, precisamos de dizer algo mais sobre os *urelementos*.

A imagem de Seção 65.4 só nos permitia formar novos conjuntos a partir de *conjuntos* antigos. Contudo, podemos querer admitir que certos *não-conjuntos*—vacas, porcos, grãos de areia, ou o que seja—possam ser membros de conjuntos. Nesse caso, começaríamos com certos elementos básicos, *urelementos*, e diríamos que em cada estágio $S$ formaríamos "todos os possíveis" conjuntos constituídos por urelementos ou conjuntos formados em estágios anteriores a $S$ (em qualquer combinação). A imagem resultante parecer-se-ia mais com isto:




Temos pois uma decisão a tomar: *devemos admitir urelementos?*

Do ponto de vista filosófico, faz sentido incluir urelementos na nossa teorização. A principal razão é tornar a teoria dos conjuntos *aplicável*. Para ilustrar, recordemos de Capítulo 4 que dizemos que dois conjuntos $A$ e $B$ têm o mesmo

tamanho, isto é, $A \approx B$, sse existe uma bijeção entre eles. Agora, se as vacas no campo e os porcos no chiqueiro constituem ambos conjuntos, podemos oferecer um tratamento conjunto-teórico da afirmação "há tantas vacas como porcos". Mas se proibirmos urelementos, de modo que as vacas e os porcos *não* constituem conjuntos, esse tratamento conjunto-teórico deixará de estar disponível. De fato, não teremos capacidade direta de aplicar a teoria dos conjuntos a mais nada além dos próprios conjuntos. (Para mais razões para incluir urelementos, ver Potter 2004, pp. vi, 24, 50–1.)

Matematicamente, contudo, é bastante raro admitir urelementos. Em parte, porque é *ligeiramente* mais fácil formular a teoria dos conjuntos sem urelementos. Mas, ocasionalmente, encontram-se justificações mais interessantes para excluir urelementos da teoria dos conjuntos:

> De acordo com a convicção de que a teoria dos conjuntos é o fundamento da matemática, devemos ser capazes de captar toda a matemática apenas falando de conjuntos, pelo que as nossas variáveis não devem quantificar sobre objetos como vacas e porcos. (Kunen, 1980, p. 8)

Assim: um foco na aplicabilidade sugeriria *incluir* urelementos; um foco num objetivo fundacional redutivo (reduzir a matemática à teoria pura dos conjuntos) poderia sugerir *excluí-los*. Uma ligeira preguiça também aponta no sentido de excluir urelementos.

Seguiremos o caminho mais preguiçoso. Em parte, há também uma justificação pedagógica. O nosso objetivo é introduzir os elementos da teoria dos conjuntos de que precisa para começar na filosofia da teoria dos conjuntos. E a maior parte dessa literatura filosófica discute teorias dos conjuntos formuladas *sem* urelementos. Logo este livro será, talvez, mais útil se se mantiver bastante próximo dessa literatura.

## 65.6 Apêndice: Lei Básica V de Frege

Na Seção 65.2, explicamos que Russell formulou o paradoxo como um problema para o sistema que Frege delineou nos seus *Grundgesetze*. O sistema de Frege não incluía uma formulação direta da compreensão ingênua. Logo, neste apêndice, explicaremos muito sumariamente o que o sistema de Frege *incluía*, como se relaciona com a compreensão ingênua e como se relaciona com o paradoxo de Russell.

O sistema de Frege é de *segunda ordem* e foi concebido para formular a noção de *extensão de um conceito*.[3] Usando notação inspirada em Frege, escreveremos $\epsilon x\, F(x)$ para *a extensão do conceito* $F$. Este é um dispositivo que toma

[3] Estritamente falando, Frege tenta formalizar uma noção mais geral: o "valor de curso" de uma função. As extensões de conceitos são um caso especial da noção mais geral. Ver Heck (2012, pp. 8–9) para pormenores.

um *predicado*, "$F$", e transforma-o num *termo* (de primeira ordem), "$\epsilon x\, F(x)$". Com este dispositivo, Frege propôs a seguinte *definição* de pertença:

$$a \in b =_{\text{df}} \exists G(b = \epsilon x\, G(x) \wedge Ga)$$

grosso modo: $a \in b$ sse $a$ cai sob um conceito cuja extensão é $b$. (Note que o quantificador "$\exists G$" é de segunda ordem.) Frege também sustentava o seguinte princípio, conhecido como *Lei básica V*:

$$\epsilon x\, F(x) = \epsilon x\, G(x) \leftrightarrow \forall x(Fx \leftrightarrow Gx)$$

grosso modo: conceitos têm extensões idênticas sse são coextensivos. (De novo, tanto "$F$" como "$G$" estão em posição de predicado.) Um princípio simples liga agora a pertença à satisfação de propriedades:

**Lema 65.2 (em *Grundgesetze*).** $\forall F \forall a(a \in \epsilon x\, F(x) \leftrightarrow Fa)$

*Prova.* Fixe $F$ e $a$. Ora $a \in \epsilon x\, F(x)$ sse $\exists G(\epsilon x\, F(x) = \epsilon x\, G(x) \wedge Ga)$ (pela definição de pertença) sse $\exists G(\forall x(Fx \leftrightarrow Gx) \wedge Ga)$ (pela lei básica V) sse $Fa$ (por lógica elementar de segunda ordem). □

E disto resulta quase de imediato a compreensão ingênua:

**Lema 65.3 (em *Grundgesetze*.).** $\forall F \exists s \forall a(a \in s \leftrightarrow Fa)$

*Prova.* Fixe $F$; agora Lema 65.2 dá $\forall a(a \in \epsilon x\, F(x) \leftrightarrow Fa)$; logo $\exists s \forall a(a \in s \leftrightarrow Fa)$ por generalização existencial. O resultado segue-se, pois $F$ era arbitrário.□

O paradoxo de Russell segue tomando $F$ dado por $\forall x(Fx \leftrightarrow x \notin x)$.

# Capítulo 66

# Passos rumo a Z

## 66.1 A história com mais pormenor

Na Seção 65.4, citamos a descrição de Shoenfield do processo de formação de conjuntos. Queremos agora escrever mais alguns princípios, para tornar esta história um pouco mais precisa. Eis-os:

> *Estágios-são-chave*. Cada conjunto forma-se por algum estágio.
>
> *Estágios-são-ordenados*. Os estágios estão ordenados: alguns vêm *antes* de outros.[1]
>
> *Estágios-acumulam*. Para qualquer estágio $S$, e para quaisquer conjuntos que se formaram *antes* do estágio $S$: forma-se, no estágio $S$, um conjunto cujos membros são exatamente esses conjuntos. Mais nada se forma no estágio $S$.

Estes são princípios informais, mas poderemos usá-los para justificar vários dos axiomas da teoria de conjuntos de Zermelo.

(Convém uma palavra de cautela. Embora vamos apresentar alguns axiomas completamente standard, com nomes completamente standard, os princípios em itálico que acabamos de apresentar não têm nomes particulares na literatura. São apenas alcunhas que esperamos serem úteis.)

## 66.2 Separação

Começamos com um princípio que substitui a compreensão ingênua:

[1] Assumiremos de fato—tacitamente—que os estágios estão *bem ordenados*. O que isto significa explica-se no Capítulo 67. É um pressuposto substancial. De fato, usando uma técnica muito engenhosa devida a Scott (1974), este pressuposto pode ser *evitado* e depois *deduzido*. (Isto também explicará por que devemos pensar que existe um estágio inicial.) Não podemos aprofundar isso aqui; para mais, veja Button (2021).

**Esquema de Separação (Esquema de Separação).** Para cada fórmula $\varphi(x)$, isto é um axioma: para qualquer $A$, o conjunto $\{x \in A : \varphi(x)\}$ existe.

Note que isto não é um único axioma. É um *esquema* de axiomas. Há *infinitamente muitos* axiomas de Separação; um para cada fórmula $\varphi(x)$. O esquema pode igualmente ser (e normalmente é) escrito do seguinte modo:

> Para qualquer fórmula $\varphi(x)$ que não contenha "$S$", isto é um axioma:
>
> $$\forall A \exists S \forall x (x \in S \leftrightarrow (\varphi(x) \wedge x \in A)).$$

Em conformidade com a convenção assinalada no início da Parte XV, as fórmulas $\varphi$ nos axiomas de Separação podem ter parâmetros.[2]

A Separação justifica-se de imediato pela concepção cumulativa iterativa de conjuntos que vamos expondo. Para ver por que, seja $A$ um conjunto. Então $A$ forma-se por algum estágio $S$ (por *Estágios-são-chave*). Uma vez que $A$ se formou no estágio $S$, todos os membros de $A$ formaram-se antes do estágio $S$ (por *Estágios-acumulam*). Consideremos em particular todos os conjuntos que são membros de $A$ e que também satisfazem $\varphi$; claramente todos estes conjuntos também se formaram antes do estágio $S$. Logo formam-se num conjunto $\{x \in A : \varphi(x)\}$ também no estágio $S$ (por *Estágios-acumulam*).

Ao contrário da compreensão ingênua, isto evita o paradoxo de Russell. Pois não podemos simplesmente afirmar a existência do conjunto $\{x : x \notin x\}$. Pelo contrário, *dado* algum conjunto $A$, podemos afirmar a existência do conjunto $R_A = \{x \in A : x \notin x\}$. Mas isto só prova que $R_A \notin R_A$ e $R_A \notin A$, o que não é preocupante.

Contudo, a Separação tem uma consequência imediata e marcante:

**Teorema 66.1.** *Não existe conjunto* universal, *isto é,* $\{x : x = x\}$ *não existe.*

*Prova.* Por redução ao absurdo, suponhamos que $V$ é um conjunto universal. Então, por Separação, $R = \{x \in V : x \notin x\} = \{x : x \notin x\}$ existe, o que contradiz o paradoxo de Russell. □

A ausência de um conjunto universal—de fato, a abertura da hierarquia de conjuntos—é uma das ideias mais fundamentais por detrás da concepção cumulativa iterativa. Por isso vale a pena ver que, intuitivamente, poderíamos chegar lá por outro caminho. Um conjunto universal teria de ser um membro de si próprio. Mas, na nossa concepção cumulativa iterativa, cada conjunto aparece (pela primeira vez) na hierarquia no primeiro estágio imediatamente

[2] Para uma explicação do que isto significa, veja a discussão imediatamente a seguir a Corolário 6.7.

a seguir a todos os seus membros. Isto implica que *nenhum* conjunto pertence a si próprio. Pois qualquer conjunto que pertencesse a si próprio teria de ocorrer pela primeira vez imediatamente depois do estágio em que ocorreu pela primeira vez, o que é absurdo. (Veremos na Definição 68.15 como tornar esta explicação mais rigorosa, usando a noção de "posto" de um conjunto. Contudo, precisaremos de mais alguns axiomas para o fazer.)

Eis mais algumas consequências da Separação e da Extensionalidade.

**Proposição 66.2.** *Se existe algum conjunto, então $\emptyset$ existe.*

*Prova.* Se $A$ é um conjunto, $\emptyset = \{x \in A : x \neq x\}$ existe por Separação. □

**Proposição 66.3.** *$A \setminus B$ existe quaisquer que sejam os conjuntos $A$ e $B$*

*Prova.* $A \setminus B = \{x \in A : x \notin B\}$ existe por Separação. □

Também se verifica que existem (quase) interseções arbitrárias:

**Proposição 66.4.** *Se $A \neq \emptyset$, então $\bigcap A = \{x : (\forall y \in A)x \in y\}$ existe.*

*Prova.* Seja $A \neq \emptyset$, logo existe algum $c \in A$. Então $\bigcap A = \{x : (\forall y \in A)x \in y\} = \{x \in c : (\forall y \in A)x \in y\}$, que existe por Separação. □

Note, porém, a condição de que $A \neq \emptyset$; pois $\bigcap \emptyset$ seria o conjunto universal, vacuamente, o que contradiz Teorema 66.1.

## 66.3 União

Proposição 66.4 deu-nos interseções. Mas, se quisermos que existam uniões arbitrárias, precisamos de enunciar outro axioma:

**União (União).** Para qualquer conjunto $A$, o conjunto $\bigcup A = \{x : (\exists b \in A)x \in b\}$ existe.

$$\forall A \exists U \forall x (x \in U \leftrightarrow (\exists b \in A)x \in b)$$

Este axioma também se justifica pela concepção cumulativa iterativa. Seja $A$ um conjunto, logo $A$ forma-se por algum estágio $S$ (por *Estágios-são-chave*). Cada membro de $A$ formou-se *antes* de $S$ (por *Estágios-acumulam*); logo, raciocinando de modo análogo, cada membro de cada membro de $A$ formou-se antes de $S$. Assim, todos *esses* conjuntos estão disponíveis antes de $S$, para serem reunidos num conjunto em $S$. E esse conjunto é precisamente $\bigcup A$.

## 66.4 Pares

O próximo axioma a considerar é o seguinte:

**Pares (Pares).** Quaisquer que sejam os conjuntos $a, b$, o conjunto $\{a, b\}$ existe.

$$\forall a \forall b \exists P \forall x (x \in P \leftrightarrow (x = a \vee x = b))$$

Eis como justificar este axioma à luz da concepção iterativa. Suponhamos que $a$ está disponível no estágio $S$, e $b$ no estágio $T$. Seja $M$ o que quer que seja dos estágios $S$ e $T$ que ocorre mais tarde. Então, uma vez que $a$ e $b$ estão ambos disponíveis no estágio $M$, o conjunto $\{a, b\}$ é uma coleção possível disponível em qualquer estágio depois de $M$ (o que quer que seja o posterior).

Mas espera! Porquê assumir que *existem* estágios depois de $M$? Se não existir nenhum, a nossa justificação falha. Por isso, para justificar Pares, teremos de acrescentar outro princípio à história que contamos na Seção 66.1, nomeadamente:

> *Estágios-prosseguem*. Não há último estágio.

Este princípio está justificado? Nada na história de Shoenfield afirmava *explicitamente* que não há último estágio. Ainda assim, mesmo que seja (estritamente falando) um acréscimo à nossa história, encaixa bem na ideia básica de que os conjuntos se formam em estágios. Aceitá-lo-emos simplesmente no que se segue. E, assim, aceitaremos também o Axioma dos Pares.

Armados com este novo axioma, podemos provar a existência de muitos mais conjuntos. Por exemplo:

**Proposição 66.5.** *Quaisquer que sejam os conjuntos $a$ e $b$, existem os seguintes conjuntos:*

1. $\{a\}$
2. $a \cup b$
3. $\langle a, b \rangle$

*Prova.* (1). Por Pares, $\{a, a\}$ existe, o que é $\{a\}$ por Extensionalidade.

(2). Por Pares, $\{a, b\}$ existe. Ora, $a \cup b = \bigcup \{a, b\}$ existe por União.

(3). Por (1), $\{a\}$ existe. Por Pares, $\{a, b\}$ existe. Ora, $\{\{a\}, \{a, b\}\} = \langle a, b \rangle$ existe, de novo por Pares. □

## 66.5 Conjuntos potência

Prosseguiremos com outro axioma:

**Conjuntos potência (Conjuntos potência).** Para qualquer conjunto $A$, existe o conjunto $\wp(A) = \{x : x \subseteq A\}$.

$$\forall A \exists P \forall x (x \in P \leftrightarrow (\forall z \in x) z \in A)$$

A nossa justificação é bastante direta. Suponhamos que $A$ se forma no estágio $S$. Então todos os membros de $A$ estavam disponíveis antes de $S$ (por *Estágios-acumulam*). Logo, raciocinando como na justificação da Separação, cada subconjunto de $A$ forma-se até ao estágio $S$. Estão todos disponíveis, para serem reunidos num único conjunto, em qualquer estágio depois de $S$. E sabemos que existe algum tal estágio, pois $S$ não é o último estágio (por *Estágios-prosseguem*). Logo $\wp(A)$ existe.

Eis uma boa consequência dos conjuntos potência:

**Proposição 66.6.** *Dados quaisquer conjuntos $A, B$, o seu produto cartesiano $A \times B$ existe.*

*Prova.* O conjunto $\wp(\wp(A \cup B))$ existe por Conjuntos potência e Proposição 66.5. Logo, por Separação, existe este conjunto:

$$C = \{z \in \wp(\wp(A \cup B)) : (\exists x \in A)(\exists y \in B) z = \langle x, y \rangle\}.$$

Agora, para quaisquer $x \in A$ e $y \in B$, o conjunto $\langle x, y \rangle$ existe por Proposição 66.5. Além disso, uma vez que $x, y \in A \cup B$, temos $\{x\}, \{x, y\} \in \wp(A \cup B)$, e $\langle x, y \rangle \in \wp(\wp(A \cup B))$. Logo $A \times B = C$. □

Nesta prova, o axioma dos conjuntos potência interage com a Separação. E isso não surpreende. Sem Separação, o princípio dos conjuntos potência não seria muito *poderoso*. Afinal, a Separação nos diz que subconjuntos de um conjunto existem e, por conseguinte, determina quão "gordo" é cada conjunto potência.

## 66.6 Infinito

Já temos axiomas suficientes para garantir que há infinitamente muitos conjuntos (se é que existe algum). De fato, suponhamos que algum conjunto existe; então $\emptyset$ existe (por Proposição 66.2). Agora, para qualquer conjunto $x$, o conjunto $x \cup \{x\}$ existe por Proposição 66.5. Logo, aplicando isto algumas vezes, obtemos conjuntos como se segue:

0. $\emptyset$
1. $\{\emptyset\}$
2. $\{\emptyset, \{\emptyset\}\}$
3. $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

4. $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$

e podemos verificar que cada um destes conjuntos é distinto.

Começamos a numeração em 0, por várias razões. Mas uma delas é esta. Não é difícil verificar que o conjunto que rotulamos "$n$" tem exatamente $n$ membros e que (intuitivamente) se forma no $n$-ésimo estágio.

Contudo. Isto nos dá *infinitamente muitos* conjuntos, mas não garante que exista um conjunto *infinito*, isto é, um conjunto com infinitamente muitos membros. E isto importa deveras: a menos que encontremos um conjunto infinito de Dedekind, não podemos construir uma álgebra de Dedekind. Mas queremos uma álgebra de Dedekind, para a podermos tratar como o conjunto dos números naturais. (Compare-se com Seção 6.4.)

Importa que os axiomas que estabelecemos até aqui *não* garantem a existência de nenhum conjunto infinito. Por isso temos de enunciar um novo axioma:

**Infinito (Infinito).** Existe um conjunto, $I$, tal que $\emptyset \in I$ e $x \cup \{x\} \in I$ sempre que $x \in I$.

$$\begin{aligned}&\exists I((\exists o \in I)\forall x\ x \notin o \wedge \\ &\quad (\forall x \in I)(\exists s \in I)\forall z(z \in s \leftrightarrow (z \in x \vee z = x)))\end{aligned}$$

É fácil ver que o conjunto $I$ que nos é dado pelo Axioma do Infinito é infinito de Dedekind. O seu elemento distinguido é $\emptyset$, e a injeção em $I$ é dada por $s(x) = x \cup \{x\}$. Agora, Teorema 6.5 mostrou como extrair uma álgebra de Dedekind de um conjunto infinito de Dedekind; e trataremos isso como o nosso conjunto de números naturais. Mais precisamente:

**Definição 66.7.** Seja $I$ qualquer conjunto que nos seja dado pelo Axioma do Infinito. Seja $s$ a função $s(x) = x \cup \{x\}$. Seja $\omega = \mathrm{clo}_s(\emptyset)$. Chamamos *números naturais* aos membros de $\omega$, e dizemos que $n$ é o resultado de $n$ aplicações de $s$ a $\emptyset$.

Pode agora voltar atrás e verificar que o conjunto rotulado "$n$", há uns parágrafos, será tratado *como* o número $n$.

Discutiremos o significado desta estipulação na Seção 66.8. Por ora, permite-nos provar um resultado intuitivo:

**Proposição 66.8.** *Nenhum número natural é infinito de Dedekind.*

*Prova.* A prova é por indução, isto é, Teorema 6.6. Claramente $0 = \emptyset$ não é infinito de Dedekind. Para o passo indutivo, estabeleceremos a contrapositiva: se (absurdamente) $s(n)$ for infinito de Dedekind, então $n$ é infinito de Dedekind.

Suponhamos, pois, que $s(n)$ é infinito de Dedekind, isto é, que existe alguma injeção $f$ com $\mathrm{Im}(f) \subsetneq \mathrm{dom}(f) = s(n) = n \cup \{n\}$. Há dois casos a considerar.

*Caso 1:* $n \notin \mathrm{Im}(f)$. Então $\mathrm{Im}(f) \subseteq n$, e $f(n) \in n$. Seja $g = f\restriction_n$; agora $\mathrm{Im}(g) = \mathrm{Im}(f) \setminus \{f(n)\} \subsetneq n = \mathrm{dom}(g)$. Logo $n$ é infinito de Dedekind.

*Caso 2:* $n \in \mathrm{Im}(f)$. Fixemos $m \in \mathrm{dom}(f) \setminus \mathrm{Im}(f)$, e definamos uma função $h$ com domínio $s(n) = n \cup \{n\}$:

$$h(x) = \begin{cases} f(x) & \text{se } f(x) \neq n \\ m & \text{se } f(x) = n \end{cases}$$

Assim $h$ e $f$ coincidem em toda a parte, exceto que $h(f^{-1}(n)) = m \neq n = f(f^{-1}(n))$. Uma vez que $f$ é uma injeção, $n \notin \mathrm{Im}(h)$; e $\mathrm{Im}(h) \subsetneq \mathrm{dom}(h) = s(n)$. Logo $n$ é infinito de Dedekind, pelo argumento do Caso 1. □

A questão que permanece é como poderíamos *justificar* o Axioma do Infinito. A resposta curta é que precisaremos de acrescentar outro princípio à história que vamos contando. Esse princípio é o seguinte:

> *Estágios-atingem-o-infinito*. Há um estágio infinito. Isto é, há um estágio que (a) não é o primeiro estágio, e que (b) tem alguns estágios antes de si, mas que (c) não tem predecessor imediato.

O Axioma do Infinito segue-se diretamente deste princípio. Sabemos que o número natural $n$ se forma no estágio $n$. Logo o conjunto $\omega$ forma-se no primeiro estágio infinito. E o próprio $\omega$ testemunha o Axioma do Infinito.

Isto, porém, apenas nos leva de volta à questão de como justificar *Estágios-atingem-o-infinito*. Tal como *Estágios-prosseguem*, não fazia parte explícita da história que contamos sobre a hierarquia cumulativa iterativa. Mas mais do que isso: nada na própria ideia de uma hierarquia iterativa, em que os conjuntos se formam estágio a estágio, nos obriga a pensar que o processo envolve um estágio *infinito*. Parece perfeitamente coerente pensar que os estágios estão ordenados como os números naturais.

Isto, contudo, levanta um problema óbvio. Na Seção 6.4, consideramos a "prova" de Dedekind de que existe um conjunto infinito de Dedekind (de pensamentos). Isto poderá não lhe ter parecido muito satisfatório. Mas se *Estágios-atingem-o-infinito* não nos é "imposto" pela concepção iterativa de conjunto (nem pelas "leis do pensamento"), continuamos sem uma justificação intrínseca para a afirmação de que existe um conjunto infinito de Dedekind.

Há muito mais a dizer aqui, naturalmente. Mas esperamos que esteja agora num ponto em que possa começar a refletir sobre o que poderá *custar* justificar um axioma (ou um princípio). No que se segue tomaremos simplesmente *Estágios-atingem-o-infinito* como concedido.

## 66.7 $\mathbf{Z}^-$: um marco

Voltaremos a *Estágios-atingem-o-infinito* na parte seguinte. Contudo, com o Axioma do Infinito, atingimos um marco importante. Temos agora todos os axiomas necessários para a teoria $\mathbf{Z}^-$. Em detalhe:

**Definição 66.9.** A teoria $\mathbf{Z}^-$ tem estes axiomas: Extensionalidade, União, Pares, Conjuntos potência, Infinito, e todas as instâncias do esquema de Separação.

O nome abrevia *Zermelo* (*menos* algo que abordaremos mais tarde). Zermelo merece a honra, pois formulou essencialmente esta teoria no seu trabalho de 1908a.[3]

Esta teoria é bastante poderosa para permitir-nos fazer uma quantidade enorme de matemática. Em particular, *deverá* voltar atrás na Parte I e convencer-se de que tudo o que fizemos, ingenuamente, pode ser feito de modo mais formal dentro de $\mathbf{Z}^-$. (Depois de o fazer durante algum tempo, poderá querer avançar e ler a Seção 66.9.) Por isso, daqui em diante, e sem mais comentários, assumiremos estar a trabalhar em $\mathbf{Z}^-$ (pelo menos).

## 66.8 A escolher os números naturais

Na Definição 66.7, definimos explicitamente a expressão "números naturais". Como deve entender esta estipulação? Não é uma afirmação metafísica, mas apenas uma decisão de *tratar* certos conjuntos como os números naturais. Já abordamos razões para pensar assim na Seção 2.2, na Seção 5.5 e na Seção 6.4. Mas podemos tornar essas razões ainda mais nítidas.

O nosso Axioma do Infinito segue von Neumann (1925). Mas eis outro axioma, que poderíamos ter adotado em alternativa:

> *Axioma do Infinito de Zermelo 1908a.* Existe um conjunto $A$ tal que $\varnothing \in A$ e $(\forall x \in A)\{x\} \in A$.

Se tivéssemos usado o axioma de Zermelo em vez do nosso Axioma do Infinito (inspirado em von Neumann), ter-nos-iam sido dado igualmente um conjunto infinito de Dedekind e, portanto, uma álgebra de Dedekind. Na abordagem de Zermelo, o elemento distinguido da nossa álgebra seria de novo $\varnothing$ (o nosso sucedâneo de 0), mas a injeção seria dada pela aplicação $x \mapsto \{x\}$, em vez de $x \mapsto x \cup \{x\}$. A consequência mais simples é que Zermelo trata 2 como $\{\{\varnothing\}\}$, ao passo que nós (com von Neumann) tratamos 2 como $\{\varnothing, \{\varnothing\}\}$.

Porquê escolher um axioma do Infinito em vez do outro? A razão prática principal é que a abordagem de von Neumann "escala" bastante bem para números transfinitos. Exploraremos isto a partir do Capítulo 67 em diante. Porém, na simples perspectiva de *fazer aritmética*, ambas as abordagens serviriam igualmente bem. Por isso, se alguém lhe disser que os números naturais *são* conjuntos, a pergunta óbvia é: *Que conjuntos são eles?*

[3] Para comentários interessantes sobre a história e os pormenores técnicos, veja Potter (2004, Apêndice A).

Esta pergunta precisa foi tornada célebre por Benacerraf (1965). Mas vale a pena sublinhar que é apenas o exemplo mais famoso de um fenómeno que já encontramos muitas vezes. O ponto essencial é este. A teoria dos conjuntos nos dá uma maneira de *simular* vários tipos de entidades "intuitivas": os reais, os racionais, os inteiros e os naturais, sim; mas também pares ordenados, funções e relações. Contudo, a teoria dos conjuntos nunca nos fornece uma escolha *única* de simulação. Há *sempre* alternativas que—de modo direto—nos teriam servido tão bem.

## 66.9 Apêndice: Fechamento, compreensão e interseção

Na Seção 66.7, sugerimos que voltasse atrás no trabalho ingênuo da Parte I e verificasse que este pode ser realizado em $\mathbf{Z}^-$. Se seguiu esse conselho, *um* ponto poderá tê-lo feito tropeçar: o uso da *interseção* no tratamento por Dedekind dos *fechamentos*.

Recordemos, de Definição 6.2, que

$$\mathrm{clo}_f(o) = \bigcap\{X : o \in X \text{ e } X \text{ é } f\text{-fechado}\}.$$

A forma geral disto é uma definição da forma:

$$C = \bigcap\{X : \varphi(X)\}.$$

Mas isto deve fazer soar o alarme: uma vez que a compreensão ingênua falha, não há garantia de que $\{X : \varphi(X)\}$ exista. Parece, então, perigosamente, que tais definições são *truques*.

Felizmente, não são truques; ou melhor, se *o forem* tal como estão, então podemos empenhar-nos honestamente para as tornar legítimas. Esse trabalho honesto foi antecipado na Proposição 66.4, quando explicamos por que $\bigcap A$ existe para qualquer $A \neq \emptyset$. Mas vamos explicitá-lo.

Dada a Extensionalidade, se tentarmos definir $C$ como $\bigcap\{X : \varphi(X)\}$, tudo o que realmente pedimos é um objeto $C$ que satisfaça o seguinte:

$$\forall x(x \in C \leftrightarrow \forall X(\varphi(X) \to x \in X)) \tag{*}$$

Suponhamos, agora, que existe *algum* conjunto, $S$, tal que $\varphi(S)$. Então, para satisfazer Eq. (*), podemos simplesmente definir $C$ por *Separação*, do seguinte modo:

$$C = \{x \in S : \forall X(\varphi(X) \to x \in X)\}.$$

Deixamos como exercício verificar que esta definição produz Eq. (*), como desejado. E esta estratégia geral permitir-nos-á contornar qualquer uso aparente da compreensão ingênua na definição de interseções. No caso particular que nos levou a esta linha de raciocínio, nomeadamente o de $\mathrm{clo}_f(o)$, eis como isso funcionaria. Começamos a prova de Lema 6.3 ao notar que $o \in \mathrm{Im}(f) \cup \{o\}$ e que $\mathrm{Im}(f) \cup \{o\}$ é $f$-fechado. Assim, podemos definir o que queremos assim:

$$\mathrm{clo}_f(o) = \{x \in \mathrm{Im}(f) \cup \{o\} : (\forall X \ni o)(X \text{ é } f\text{-fechado} \to x \in X)\}.$$

## Problemas

**Problema 66.1.** Mostre que, quaisquer que sejam os conjuntos $a, b, c$, o conjunto $\{a, b, c\}$ existe.

**Problema 66.2.** Mostre que, quaisquer que sejam os conjuntos $a_1, \ldots, a_n$, o conjunto $\{a_1, \ldots, a_n\}$ existe.

**Problema 66.3.** Mostre que, quaisquer que sejam os conjuntos $A, B$: (i) existe o conjunto de todas as relações com domínio $A$ e contradomínio $B$; e (ii) existe o conjunto de todas as funções de $A$ para $B$.

**Problema 66.4.** Seja $A$ um conjunto, e seja $\sim$ uma relação de equivalência em $A$. Prove que existe o conjunto das classes de equivalência sob $\sim$ em $A$, isto é, $A/_\sim$.

# Capítulo 67

# Ordinais

## 67.1 Introdução

No Capítulo 66, postulamos que existe um estágio infinito da hierarquia, na forma de *Estágios-atingem-o-infinito* (ver também o nosso axioma do Infinito). Contudo, dado *Estágios-prosseguem*, não podemos parar no estágio infinito; temos de continuar. Assim: no estágio seguinte ao primeiro estágio infinito, formamos todas as coleções possíveis de conjuntos que estavam disponíveis no primeiro estágio infinito; e repetimos; e repetimos; e repetimos; ...

Implicitamente, o que aqui aconteceu foi começarmos a invocar uma noção "intuitiva" de número, segundo a qual podem existir números *depois* de todos os números naturais. Em particular, a noção em causa é a de *ordinal transfinito*. O objetivo deste capítulo é tornar esta ideia mais rigorosa. Exploraremos a noção geral de ordinal e depois definiremos explicitamente certos conjuntos para serem os nossos ordinais.

## 67.2 A Ideia Geral de um Ordinal

Considere os números naturais, na sua ordem habitual:

$$0 < 1 < 2 < 3 < 4 < 5 < \cdots$$

Chamamos a isto, na gíria, uma $\omega$-sucessão. E, de fato, esta ordenação geral espelha-se na nossa construção inicial dos estágios da hierarquia de conjuntos. Mas suponha agora que movemos 0 para o fim desta sucessão, de modo que fica depois de todos os outros números:

$$1 < 2 < 3 < 4 < 5 < \cdots < 0$$

Temos aqui as mesmas entidades, mas ordenadas de modo fundamentalmente diferente: a nossa primeira ordenação não tinha último elemento; a nova tem.

De fato, a nova ordenação consiste numa $\omega$-sucessão de entidades $(1, 2, 3, 4, 5, \ldots)$, seguida de outra entidade. Será uma sucessão do tipo $\omega + 1$.

Podemos gerar ainda mais tipos de ordenação, usando apenas estas entidades. Por exemplo, considere todos os números pares (na sua ordem natural) seguidos de todos os ímpares (na sua ordem natural):

$$0 \ < \ 2 \ < \ 4 \ < \ \cdots \ < \ 1 \ < \ 3 \ < \ \cdots$$

Isto é uma $\omega$-sucessão seguida de outra $\omega$-sucessão; uma sucessão do tipo $\omega + \omega$.

Pois bem, podemos continuar. Mas o que gostaríamos é de ter uma forma geral de entender esta linguagem sobre *ordenações*.

## 67.3 Boas Ordenações

A noção fundamental é a seguinte:

**Definição 67.1.** A relação $<$ *bem ordena* $A$ sse cumpre estas duas condições:

1. $<$ é conexa, isto é, para todos $a, b \in A$, ou $a < b$ ou $a = b$ ou $b < a$;
2. todo o subconjunto não vazio de $A$ tem um membro $<$-minimal, isto é, se $\emptyset \neq X \subseteq A$ então $(\exists m \in X)(\forall z \in X) z \not< m$

É fácil ver que os três exemplos que acabamos de considerar eram de fato relações de boa ordenação.

Eis algumas observações elementares mas extremamente importantes sobre boa ordenação.

**Proposição 67.2.** *Se $<$ bem ordena $A$, então todo o subconjunto não vazio de $A$ tem um único membro $<$-mínimo, e $<$ é irreflexiva, assimétrica e transitiva.*

*Prova.* Se $X$ é um subconjunto não vazio de $A$, tem um membro $<$-minimal $m$, isto é, $(\forall z \in X) z \not< m$. Como $<$ é conexa, $(\forall z \in X) m \leq z$. Logo $m$ é o membro $<$-mínimo de $X$.

Para a irreflexividade, fixe $a \in A$; o membro $<$-mínimo de $\{a\}$ é $a$, logo $a \not< a$. Para a transitividade, se $a < b < c$, então como $\{a, b, c\}$ tem um membro $<$-mínimo, $a < c$. A assimetria segue da irreflexividade e da transitividade □

**Proposição 67.3.** *Se $<$ bem ordena $A$, então para qualquer fórmula $\varphi(x)$:*

$$\textit{se } (\forall a \in A)((\forall b < a)\varphi(b) \to \varphi(a)), \textit{ então } (\forall a \in A)\varphi(a).$$

*Prova.* Provaremos a contrapositiva. Suponha $\neg(\forall a \in A)\varphi(a)$, isto é, que $X = \{x \in A : \neg\varphi(x)\} \neq \emptyset$. Então $X$ tem um membro $<$-minimal, $a$. Logo $(\forall b < a)\varphi(b)$ mas $\neg\varphi(a)$. □

Esta última propriedade deve recordar-lhe o princípio de indução forte nos naturais, isto é: se $(\forall n \in \omega)((\forall m < n)\varphi(m) \to \varphi(n))$, então $(\forall n \in \omega)\varphi(n)$. E esta propriedade torna a boa ordenação numa noção muito *robusta*.[1]

## 67.4 Isomorfismos de Ordem

Para explicar *quão* robusta é a boa ordenação, começaremos por introduzir um método para comparar boas ordenações.

**Definição 67.4.** Uma *boa ordenação* é um par $\langle A, < \rangle$, tal que $<$ bem ordena $A$. As boas ordenações $\langle A, < \rangle$ e $\langle B, \lessdot \rangle$ são *isomorfas por ordem* sse existe uma bijeção $f\colon A \to B$ tal que: $x < y$ sse $f(x) \lessdot f(y)$. Neste caso, escrevemos $\langle A, < \rangle \cong \langle B, \lessdot \rangle$, e dizemos que $f$ é um *isomorfismo de ordem*.

Daqui em diante, por brevidade, falaremos em "isomorfismos" em vez de "isomorfismos de ordem". Intuitivamente, os isomorfismos são bijeções que preservam estrutura. Eis alguns fatos simples sobre isomorfismos.

**Lema 67.5.** *Composições de isomorfismos são isomorfismos, isto é: se $f\colon A \to B$ e $g\colon B \to C$ são isomorfismos, então $(g \circ f)\colon A \to C$ é um isomorfismo.*

*Prova.* Fica como exercício. □

**Corolário 67.6.** *$X \cong Y$ é uma relação de equivalência.*

**Proposição 67.7.** *Se $\langle A, < \rangle$ e $\langle B, \lessdot \rangle$ são boas ordenações isomorfas, então o isomorfismo entre elas é único.*

*Prova.* Sejam $f$ e $g$ isomorfismos $A \to B$. Provaremos o resultado por indução, isto é, usando Proposição 67.3. Fixe $a \in A$, e suponha (para indução) que $(\forall b < a)f(b) = g(b)$. Fixe $x \in B$.

Se $x \lessdot f(a)$, então $f^{-1}(x) < a$, logo $g(f^{-1}(x)) \lessdot g(a)$, invocando o fato de $f$ e $g$ serem isomorfismos. Mas como $f^{-1}(x) < a$, pela suposição $x = f(f^{-1}(x)) = g(f^{-1}(x))$. Logo $x \lessdot g(a)$. Analogamente, se $x \lessdot g(a)$ então $x \lessdot f(a)$.

Generalizando, $(\forall x \in B)(x \lessdot f(a) \leftrightarrow x \lessdot g(a))$. Segue que $f(a) = g(a)$ por Proposição 2.27. Logo $(\forall a \in A)f(a) = g(a)$ por Proposição 67.3. □

Isto dá alguma ideia de que as boas ordenações são robustas. Mas para continuar a explicar isto, convém introduzir mais notação.

**Definição 67.8.** Quando $\langle A, < \rangle$ é uma boa ordenação com $a \in A$, seja $A_a = \{x \in A : x < a\}$. Dizemos que $A_a$ é um *segmento inicial* próprio de $A$ (e permitimos que o próprio $A$ seja um segmento inicial impróprio de $A$). Seja $<_a$ a restrição de $<$ ao segmento inicial, isto é, $<{\restriction}_{A_a^2}$.

[1] Lembrete: todas as fórmulas podem ter parâmetros (salvo indicação em contrário).

Com esta notação, podemos enunciar e provar que nenhuma boa ordenação é isomorfa a nenhum dos seus segmentos iniciais próprios.

**Lema 67.9.** *Se $\langle A, <\rangle$ é uma boa ordenação com $a \in A$, então $\langle A, <\rangle \ncong \langle A_a, <_a\rangle$*

*Prova.* Por redução ao absurdo, suponha $f\colon A \to A_a$ um isomorfismo. Como $f$ é uma bijeção e $A_a \subsetneq A$, usando Proposição 67.2 seja $b \in A$ o membro $<$-mínimo de $A$ tal que $b \neq f(b)$. Mostraremos que $(\forall x \in A)(x < b \leftrightarrow x < f(b))$, donde seguirá, por Proposição 2.27, que $b = f(b)$, completando a redução ao absurdo.

Suponha $x < b$. Logo $x = f(x)$, pela escolha de $b$. E $f(x) < f(b)$, por $f$ ser um isomorfismo. Logo $x < f(b)$.

Suponha $x < f(b)$. Logo $f^{-1}(x) < b$, por $f$ ser um isomorfismo, e portanto $f^{-1}(x) = x$ pela escolha de $b$. Logo $x < b$. □

O nosso resultado seguinte mostra, grosso modo, que um "segmento inicial" de um isomorfismo é um isomorfismo:

**Lema 67.10.** *Sejam $\langle A, <\rangle$ e $\langle B, \lessdot\rangle$ boas ordenações. Se $f\colon A \to B$ é um isomorfismo e $a \in A$, então $f{\restriction_{A_a}} : A_a \to B_{f(a)}$ é um isomorfismo.*

*Prova.* Como $f$ é um isomorfismo:

$$\begin{aligned} f[A_a] &= f[\{x \in A : x < a\}] \\ &= f[\{f^{-1}(y) \in A : f^{-1}(y) < a\}] \\ &= \{y \in B : y \lessdot f(a)\} \\ &= B_{f(a)} \end{aligned}$$

E $f{\restriction_{A_a}}$ preserva a ordem porque $f$ preserva. □

Os nossos dois resultados seguintes estabelecem que as boas ordenações são sempre comparáveis:

**Lema 67.11.** *Sejam $\langle A, <\rangle$ e $\langle B, \lessdot\rangle$ boas ordenações. Se $\langle A_{a_1}, <_{a_1}\rangle \cong \langle B_{b_1}, \lessdot_{b_1}\rangle$ e $\langle A_{a_2}, <_{a_2}\rangle \cong \langle B_{b_2}, \lessdot_{b_2}\rangle$, então $a_1 < a_2$ sse $b_1 \lessdot b_2$*

*Prova.* Provaremos da *esquerda para a direita*; a outra direção é análoga. Suponha ambos $\langle A_{a_1}, <_{a_1}\rangle \cong \langle B_{b_1}, \lessdot_{b_1}\rangle$ e $\langle A_{a_2}, <_{a_2}\rangle \cong \langle B_{b_2}, \lessdot_{b_2}\rangle$, com $f\colon A_{a_2} \to B_{b_2}$ o nosso isomorfismo. Seja $a_1 < a_2$; então $\langle A_{a_1}, <_{a_1}\rangle \cong \langle B_{f(a_1)}, \lessdot_{f(a_1)}\rangle$ por Lema 67.10. Logo $\langle B_{b_1}, \lessdot_{b_1}\rangle \cong \langle B_{f(a_1)}, \lessdot_{f(a_1)}\rangle$, e portanto $b_1 = f(a_1)$ por Lema 67.9. Ora, $b_1 \lessdot b_2$ pois o domínio de $f$ é $B_{b_2}$. □

**Teorema 67.12.** *Dadas quaisquer duas boas ordenações, uma é isomorfa a um segmento inicial (não necessariamente próprio) da outra.*

*Prova.* Sejam $\langle A, <\rangle$ e $\langle B, \lessdot\rangle$ boas ordenações. Usando a Separação, seja

$$f = \{\langle a, b\rangle \in A \times B : \langle A_a, <_a\rangle \cong \langle B_b, \lessdot_b\rangle\}.$$

Por Lema 67.11, $a_1 < a_2$ sse $b_1 \lessdot b_2$ para todos $\langle a_1, b_1\rangle, \langle a_2, b_2\rangle \in f$. Logo $f\colon \mathrm{dom}(f) \to \mathrm{Im}(f)$ é um isomorfismo.

Se $a_2 \in \mathrm{dom}(f)$ e $a_1 < a_2$, então $a_1 \in \mathrm{dom}(f)$ por Lema 67.10; logo $\mathrm{dom}(f)$ é um segmento inicial de $A$. Analogamente, $\mathrm{Im}(f)$ é um segmento inicial de $B$. Por redução ao absurdo, suponha que ambos são segmentos iniciais *próprios*. Então seja $a$ o membro $<$-mínimo de $A \setminus \mathrm{dom}(f)$, de modo que $\mathrm{dom}(f) = A_a$, e seja $b$ o membro $\lessdot$-mínimo de $B \setminus \mathrm{Im}(f)$, de modo que $\mathrm{Im}(f) = B_b$. Logo $f\colon A_a \to B_b$ é um isomorfismo, e portanto $\langle a, b\rangle \in f$, contradição. □

## 67.5 Construção de Von Neumann dos Ordinais

Teorema 67.12 sugere uma ideia. Poderíamos introduzir certos objetos, chamados *tipos de ordem*, para servirem de representantes das boas ordenações. Escrevendo $\mathrm{ord}(A, <)$ para o tipo de ordem da boa ordenação $\langle A, <\rangle$, gostaríamos de garantir os dois princípios seguintes:

$$\mathrm{ord}(A, <) = \mathrm{ord}(B, \lessdot) \text{ sse } \langle A, <\rangle \cong \langle B, \lessdot\rangle$$
$$\mathrm{ord}(A, <) < \mathrm{ord}(B, \lessdot) \text{ sse } \langle A, <\rangle \cong \langle B_b, \lessdot_b\rangle \text{ para algum } b \in B$$

Além disso, poderíamos esperar introduzir tipos de ordem *como certos conjuntos*, tal como podemos introduzir os números naturais como certos conjuntos.

A forma mais comum de o fazer—e a abordagem que seguiremos—é definir estes tipos de ordem via certos conjuntos bem ordenados *canónicos*. Estes conjuntos canónicos foram introduzidos pela primeira vez por von Neumann:

**Definição 67.13.** O conjunto $A$ é *transitivo* sse $(\forall x \in A)x \subseteq A$. Então $A$ é um *ordinal* sse $A$ é transitivo e bem ordenado por $\in$.

Daqui em diante, usaremos letras gregas para ordinais. Segue-se imediatamente da definição que, se $\alpha$ é um ordinal, então $\langle \alpha, \in_\alpha\rangle$ é uma boa ordenação, onde $\in_\alpha = \{\langle x, y\rangle \in \alpha^2 : x \in y\}$. Assim, abusando um pouco da notação, podemos dizer que o próprio $\alpha$ *é* uma boa ordenação.

Eis os primeiros ordinais:

$$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots$$

Repare que estes são precisamente os primeiros ordinais que encontramos no nosso Axioma do Infinito, isto é, na definição de von Neumann de $\omega$ (ver Seção 66.6). Isto não é coincidência. A definição de von Neumann dos ordinais trata os números naturais como ordinais, mas permite também ordinais transfinitos.

Como sempre, podemos agora perguntar: *são* estes os ordinais? Ou von Neumann deu-nos apenas alguns conjuntos que podemos *tratar* como os ordinais? O tipo de discussões que se podem ter sobre esta questão é semelhante às que tivemos na Seção 2.2, Seção 5.5, Seção 6.4, e Seção 66.8, pelo que não insistiremos no ponto. Em vez disso, daqui em diante usaremos "os ordinais" para falar dos "ordinais de von Neumann".

## 67.6 Propriedades Básicas dos Ordinais

Observamos que os primeiros ordinais são os números naturais. A razão principal para desenvolver uma teoria dos ordinais é alargar o princípio de indução que vale nos números naturais. Iremos construir isso através duma sucessão de resultados elementares.

**Lema 67.14.** *Todo o membro de um ordinal é um ordinal.*

*Prova.* Seja $\alpha$ um ordinal com $b \in \alpha$. Como $\alpha$ é transitivo, $b \subseteq \alpha$. Logo $\in$ bem ordena $b$ pois $\in$ bem ordena $\alpha$.

Para ver que $b$ é transitivo, suponha $x \in c \in b$. Logo $c \in \alpha$ pois $b \subseteq \alpha$. Outra vez, como $\alpha$ é transitivo, $c \subseteq \alpha$, de modo que $x \in \alpha$. Logo $x, c, b \in \alpha$. Mas $\in$ bem ordena $\alpha$, logo $\in$ é uma relação transitiva em $\alpha$ por Proposição 67.2. Logo, como $x \in c \in b$, temos $x \in b$. Generalizando, $c \subseteq b$ □

**Corolário 67.15.** $\alpha = \{\beta \in \alpha : \beta \text{ é um ordinal}\}$, *para qualquer ordinal* $\alpha$

*Prova.* Imediato a partir de Lema 67.14. □

A ideia grosseira dos dois resultados principais seguintes, Teorema 67.16 e Teorema 67.17, é que os ordinais eles próprios são bem ordenados por pertença:

**Teorema 67.16 (Indução Transfinita).** *Para qualquer fórmula* $\varphi(x)$*:*

$$\text{se } \exists\alpha\varphi(\alpha), \text{ então } \exists\alpha(\varphi(\alpha) \wedge (\forall\beta \in \alpha)\neg\varphi(\beta))$$

*onde os quantificadores exibidos ficam implicitamente restritos a ordinais.*

*Prova.* Suponha $\varphi(\alpha)$, para algum ordinal $\alpha$. Se $(\forall\beta \in \alpha)\neg\varphi(\beta)$, terminamos. Caso contrário, como $\alpha$ é um ordinal, tem um membro $\in$-mínimo que verifica $\varphi$, e este é um ordinal por Lema 67.14. □

Repare que podemos exprimir igualmente Teorema 67.16 como o esquema:

$$\text{se } \forall\alpha((\forall\beta \in \alpha)\varphi(\beta) \to \varphi(\alpha)), \text{ então } \forall\alpha\varphi(\alpha)$$

tomando simplesmente $\neg\varphi(\alpha)$ no Teorema 67.16, e depois fazendo manipulações lógicas elementares.

**Teorema 67.17 (Tricotomia).** *$\alpha \in \beta \vee \alpha = \beta \vee \beta \in \alpha$, para quaisquer ordinais $\alpha$ e $\beta$.*

*Prova.* A prova é por dupla indução, isto é, usando Teorema 67.16 duas vezes. Diga-se que $x$ é *comparável* com $y$ sse $x \in y \vee x = y \vee y \in x$.

Para a indução, suponha que todo o ordinal em $\alpha$ é comparável com *todo* o ordinal. Para uma segunda indução, suponha que $\alpha$ é comparável com todo o ordinal em $\beta$. Mostraremos que $\alpha$ é comparável com $\beta$. Por indução em $\beta$, seguirá que $\alpha$ é comparável com todo o ordinal; e por indução em $\alpha$, *todo* o ordinal é comparável com *todo* o ordinal, como pretendido. Basta supor que $\alpha \notin \beta$ e $\beta \notin \alpha$, e mostrar que $\alpha = \beta$.

Para mostrar que $\alpha \subseteq \beta$, fixe $\gamma \in \alpha$; este é um ordinal por Lema 67.14. Logo, pela primeira hipótese de indução, $\gamma$ é comparável com $\beta$. Mas se $\gamma = \beta$ ou $\beta \in \gamma$ então $\beta \in \alpha$ (invocando a transitividade de $\alpha$ se necessário), contra a suposição; logo $\gamma \in \beta$. Generalizando, $\alpha \subseteq \beta$.

Raciocínio exatamente análogo, usando a segunda hipótese de indução, mostra que $\beta \subseteq \alpha$. Logo $\alpha = \beta$. □

Assim, por vezes escreveremos $\alpha < \beta$ em vez de $\alpha \in \beta$, já que $\in$ se comporta como relação de ordem. Não há razões profundas para além da familiaridade, e porque é mais fácil escrever $\alpha \leq \beta$ do que $\alpha \in \beta \vee \alpha = \beta$.[2]

Eis duas consequências rápidas dos últimos resultados, a primeira das quais põe a nova notação em prática:

**Corolário 67.18.** *Se $\exists\alpha\varphi(\alpha)$, então $\exists\alpha(\varphi(\alpha) \wedge \forall\beta(\varphi(\beta) \to \alpha \leq \beta))$. Além disso, para quaisquer ordinais $\alpha, \beta, \gamma$, tanto $\alpha \notin \alpha$ como $\alpha \in \beta \in \gamma \to \alpha \in \gamma$.*

*Prova.* Tal como Proposição 67.2. □

**Corolário 67.19.** *$A$ é um ordinal sse $A$ é um conjunto transitivo de ordinais.*

*Prova. Da esquerda para a direita.* Por Lema 67.14. *Da direita para a esquerda.* Se $A$ é um conjunto transitivo de ordinais, então $\in$ bem ordena $A$ por Teorema 67.16 e Teorema 67.17. □

Agora, descrevemos Teorema 67.16 e Teorema 67.17 como dizendo que $\in$ bem ordena os ordinais. Contudo, temos de ser *muito cautelosos* com este tipo de afirmação, graças ao resultado seguinte:

**Teorema 67.20 (Paradoxo de Burali-Forti).** *Não existe conjunto de todos os ordinais*

[2] Poderíamos escrever $\alpha \subseteq \beta$; mas isso seria totalmente não convencional.

*Prova.* Por redução ao absurdo, suponha $O$ o conjunto de todos os ordinais. Se $\alpha \in \beta \in O$, então $\alpha$ é um ordinal, por Lema 67.14, logo $\alpha \in O$. Logo $O$ é transitivo, e portanto $O$ é um ordinal por Corolário 67.19. Daí $O \in O$, contradizendo Corolário 67.18. □

Este resultado deve o nome a Burali-Forti. Mas foi Cantor em 1899—numa carta a Dedekind—quem viu pela primeira vez com clareza a *contradição* em supor que existe um conjunto de todos os ordinais. Como van Heijenoort explica:

> O próprio Burali-Forti considerou a contradição como estabelecendo, por *reductio ad absurdum*, o resultado de que a ordenação natural dos ordinais é apenas uma ordenação parcial. (Heijenoort, 1967, p. 105)

Deixando de lado o erro de Burali-Forti, podemos resumir o precedente como segue. Os ordinais são conjuntos que individualmente são bem ordenados por pertença, e coletivamente são bem ordenados por pertença (sem coletivamente constituírem um conjunto).

Para concluir, eis mais propriedades básicas dos ordinais que seguem de Teorema 67.16 e Teorema 67.17.

**Proposição 67.21.** *Toda a sucessão estritamente descendente de ordinais é finita.*

*Prova.* Toda a sucessão infinita estritamente descendente de ordinais $\alpha_0 > \alpha_1 > \alpha_2 > \ldots$ não tem membro $<$-mínimo, contradizendo Teorema 67.16. □

**Proposição 67.22.** $\alpha \subseteq \beta \vee \beta \subseteq \alpha$, *para quaisquer ordinais* $\alpha, \beta$.

*Prova.* Se $\alpha \in \beta$, então $\alpha \subseteq \beta$ pois $\beta$ é transitivo. Analogamente, se $\beta \in \alpha$, então $\beta \subseteq \alpha$. E se $\alpha = \beta$, então $\alpha \subseteq \beta$ e $\beta \subseteq \alpha$. Logo, por Teorema 67.17 terminamos. □

**Proposição 67.23.** $\alpha = \beta$ *sse* $\alpha \cong \beta$, *para quaisquer ordinais* $\alpha, \beta$.

*Prova.* Os ordinais são boas ordenações; logo isto é imediato da Tricotomia (Teorema 67.17) e de Lema 67.9. □

## 67.7 Substituição

Na Seção 67.5, motivamos a introdução dos ordinais ao sugerir que os poderíamos tratar como tipos de ordem, isto é, como representantes canónicos de boas ordenações. Para que isso funcione, seria preciso provar que *toda a boa ordenação é isomorfa a algum ordinal*. Isso permitiria definir $\mathrm{ord}(A, <)$ como o ordinal $\alpha$ tal que $\langle A, < \rangle \cong \alpha$.

Infelizmente, *não* podemos provar o resultado desejado apenas com os axiomas introduzidos até aqui. (Veremos por que em Seção 69.2, mas por agora basta: não podemos.) Precisamos de uma ideia nova, e eis-a:

**Esquema de Substituição (Esquema de Substituição).** Para qualquer fórmula $\varphi(x, y)$, o seguinte é um axioma:

> para qualquer $A$, se $(\forall x \in A)\exists!y\, \varphi(x, y)$, então $\{y : (\exists x \in A)\varphi(x, y)\}$ existe.

Como na Separação, isto é um esquema: produz infinitamente muitos axiomas, um para cada uma das infinitas $\varphi$ distintas. E pode igualmente ser (e normalmente é) escrito assim:

Para qualquer fórmula $\varphi(x, y)$ que não contenha "$B$", o seguinte é um axioma:

$$\forall A[(\forall x \in A)\exists!y\, \varphi(x, y) \to \exists B \forall y(y \in B \leftrightarrow (\exists x \in A)\varphi(x, y))]$$

À primeira vista, contudo, esta é uma fórmula bastante intrincada. A consequência imediata seguinte da Substituição dá provavelmente uma expressão *mais clara* à ideia intuitiva com que trabalhamos:[3]

**Corolário 67.24.** *Para qualquer termo $\tau(x)$, e qualquer conjunto $A$, este conjunto existe:*

$$\{\tau(x) : x \in A\} = \{y : (\exists x \in A)y = \tau(x)\}.$$

*Prova.* Como $\tau$ é um *termo*, $\forall x \exists!y\, \tau(x) = y$. *A fortiori*, $(\forall x \in A)\exists!y\, \tau(x) = y$. Logo $\{y : (\exists x \in A)\tau(x) = y\}$ existe pela Substituição. □

Isto sugere que "Substituição" é um bom nome para o axioma: dado um conjunto $A$, pode formar um novo conjunto, $\{\tau(x) : x \in A\}$, substituindo cada membro de $A$ pela sua imagem sob $\tau$. De fato, seguindo a notação para a imagem de um conjunto sob uma função, poderíamos escrever $\tau[A]$ para $\{\tau(x) : x \in A\}$.

O essencial, porém, é que $\tau$ é um *termo*. Não tem de ser (um nome de) uma *função*, no sentido de Seção 3.3, isto é, um certo conjunto de pares ordenados. Afinal, se $f$ é uma função (nesse sentido), então o conjunto $f[A] = \{f(x) : x \in A\}$ é apenas um subconjunto particular de $\mathrm{Im}(f)$, e isso já está garantido a existir apenas com os axiomas de $\mathbf{Z}^-$.[4] A Substituição, em contraste, é um acréscimo *poderoso* aos nossos axiomas, como veremos no Capítulo 69.

[3] Um termo é uma expressão que designa exatamente um objeto (em qualquer instanciação das suas variáveis livres). Por exemplo, "$\emptyset$" é um termo que designa o conjunto vazio; "$\{x\}$" é um termo que designa o singular de $x$ (seja qual for $x$); "$x \cup y$" é um termo que designa a união de $x$ e de $y$ (sejam quais forem).

[4] Baste considerar $\{y \in \bigcup\bigcup f : (\exists x \in A)y = f(x)\}$.

## 67.8 $\mathbf{ZF}^-$: um marco

A questão de como justificar o Esquema de Substituição (se é que o justificamos) não é linear. Como tal, a reservamos para o Capítulo 69. No entanto, com a adição da Substituição, atingimos outro marco importante. Dispomos agora de todos os axiomas necessários para a teoria $\mathbf{ZF}^-$. Em detalhe:

**Definição 67.25.** A teoria $\mathbf{ZF}^-$ tem estes axiomas: Extensionalidade, União, Pares, Conjuntos das Partes, Infinito, e todas as instâncias dos esquemas de Separação e Substituição. Por outras palavras, $\mathbf{ZF}^-$ acrescenta a Substituição a $\mathbf{Z}^-$.

Isto designa a teoria de conjuntos de *Zermelo–Fraenkel* (*menos* algo que veremos mais adiante). Fraenkel recebe a honra, uma vez que lhe é atribuída a formulação da Substituição em 1922, embora a primeira formulação precisa seja devida a Skolem (1922).

## 67.9 Ordinais como Tipos de Ordem

Armados com a Substituição, e portanto trabalhando agora em $\mathbf{ZF}^-$, podemos finalmente provar o resultado a que vimos aspirando:

**Teorema 67.26.** *Toda a boa ordenação é isomorfa a um único ordinal.*

*Prova.* Seja $\langle A, < \rangle$ uma boa ordenação. Por Proposição 67.23, é isomorfa no máximo a um ordinal. Logo, por redução ao absurdo, suponha que $\langle A, < \rangle$ não é isomorfa a *nenhum* ordinal. Começaremos por "tornar $\langle A, < \rangle$ o mais pequena possível". Em detalhe: se algum segmento inicial próprio $\langle A_a, <_a \rangle$ não for isomorfo a nenhum ordinal, existe um $a \in A$ mínimo com essa propriedade; então seja $B = A_a$ e $\lessdot = <_a$. Caso contrário, seja $B = A$ e $\lessdot = <$.

Por definição, todo o segmento inicial próprio de $B$ é isomorfo a algum ordinal, que é único como acima. Logo, pela Substituição, o conjunto seguinte existe, e é uma função:

$$f = \{\langle \beta, b \rangle : b \in B \text{ e } \beta \cong \langle B_b, \lessdot_b \rangle\}$$

Para completar a redução ao absurdo, mostraremos que $f$ é um isomorfismo $\alpha \to B$, para algum ordinal $\alpha$.

É óbvio que $\operatorname{Im}(f) = B$. E por Lema 67.11, $f$ preserva a ordenação, isto é, $\gamma \in \beta$ sse $f(\gamma) \lessdot f(\beta)$. Para mostrar que $\operatorname{dom}(f)$ é um ordinal, por Corolário 67.19 basta mostrar que $\operatorname{dom}(f)$ é transitivo. Fixe então $\beta \in \operatorname{dom}(f)$, isto é, $\beta \cong \langle B_b, \lessdot_b \rangle$ para algum $b$. Se $\gamma \in \beta$, então $\gamma \in \operatorname{dom}(f)$ por Lema 67.10; generalizando, $\beta \subseteq \operatorname{dom}(f)$. □

Este resultado autoriza a definição seguinte, que queríamos apresentar desde Seção 67.5:

**Definição 67.27.** Se $\langle A, <\rangle$ é uma boa ordenação, então o seu tipo de ordem, $\operatorname{ord}(A, <)$, é o único ordinal $\alpha$ tal que $\langle A, <\rangle \cong \alpha$.

Além disso, esta definição autoriza dois princípios convenientes:

**Corolário 67.28.** *Sendo $\langle A, <\rangle$ e $\langle B, \lessdot\rangle$ boas ordenações:*

$$\operatorname{ord}(A, <) = \operatorname{ord}(B, \lessdot) \text{ sse } \langle A, <\rangle \cong \langle B, \lessdot\rangle$$
$$\operatorname{ord}(A, <) \in \operatorname{ord}(B, \lessdot) \text{ sse } \langle A, <\rangle \cong \langle B_b, \lessdot_b\rangle \text{ para algum } b \in B$$

*Prova.* A identidade vale por Proposição 67.23. Para provar a segunda afirmação, seja $\operatorname{ord}(A, <) = \alpha$ e $\operatorname{ord}(B, \lessdot) = \beta$, e seja $f : \beta \to \langle B, \lessdot\rangle$ o nosso isomorfismo. Então:

$$\begin{aligned}\alpha \in \beta \text{ sse } f\restriction_\alpha : \alpha \to B_{f(\alpha)} &\text{ é um isomorfismo}\\ &\text{sse } \langle A, <\rangle \cong \langle B_{f(\alpha)}, \lessdot_{f(\alpha)}\rangle\\ &\text{sse } \langle A, <\rangle \cong \langle B_b, \lessdot_b\rangle \text{ para algum } b \in B\end{aligned}$$

por Proposição 67.7, Lema 67.10, e Corolário 67.15. □

## 67.10 Ordinais Sucessores e Limites

Nos próximos capítulos, usaremos muito os ordinais. Por isso convém introduzir algumas noções simples.

**Definição 67.29.** Para qualquer ordinal $\alpha$, o seu *sucessor* é $\alpha^+ = \alpha \cup \{\alpha\}$. Dizemos que $\alpha$ é um ordinal *sucessor* se $\beta^+ = \alpha$ para algum ordinal $\beta$. Dizemos que $\alpha$ é um ordinal *limite* sse $\alpha$ não é nem vazio nem um ordinal sucessor.

O resultado seguinte mostra que esta é a noção certa de *sucessor*:

**Proposição 67.30.** *Para qualquer ordinal $\alpha$:*

1. *$\alpha \in \alpha^+$;*
2. *$\alpha^+$ é um ordinal;*
3. *não existe ordinal $\beta$ tal que $\alpha \in \beta \in \alpha^+$.*

*Prova.* Trivialmente, $\alpha \in \alpha \cup \{\alpha\} = \alpha^+$. Igualmente, $\alpha^+$ é um conjunto transitivo de ordinais, e portanto um ordinal por Corolário 67.19. E é impossível que $\alpha \in \beta \in \alpha^+$, pois então ou $\beta \in \alpha$ ou $\beta = \alpha$, contradizendo Corolário 67.18. □

Isto autoriza também uma variante de prova por indução transfinita:

**Teorema 67.31 (Indução Transfinita Simples).** *Seja $\varphi(x)$ uma fórmula tal que:*

1. $\varphi(\emptyset)$; *e*
2. *para qualquer ordinal* $\alpha$, *se* $\varphi(\alpha)$ *então* $\varphi(\alpha^+)$; *e*
3. *se* $\alpha$ *é um ordinal limite e* $(\forall \beta \in \alpha)\varphi(\beta)$, *então* $\varphi(\alpha)$.

*Então* $\forall \alpha \varphi(\alpha)$.

*Prova.* Provamos a contrapositiva. Logo, suponha que existe algum ordinal para o qual vale $\neg\varphi$; seja $\gamma$ o menor tal ordinal. Então ou $\gamma = \emptyset$, ou $\gamma = \alpha^+$ para algum $\alpha$ tal que $\varphi(\alpha)$; ou $\gamma$ é um ordinal limite e $(\forall \beta \in \gamma)\varphi(\beta)$. □

Um último bocado de notação será útil mais adiante:

**Definição 67.32.** Se $X$ é um conjunto de ordinais, então $\operatorname{lsub}(X) = \bigcup_{\alpha \in X} \alpha^+$.

Aqui, "lsub" abrevia "least strict upper bound" (majorante superior estrito mínimo).[5] O resultado seguinte explica isto:

**Proposição 67.33.** *Se* $X$ *é um conjunto de ordinais,* $\operatorname{lsub}(X)$ *é o menor ordinal estritamente maior do que todo o ordinal em* $X$.

*Prova.* Seja $Y = \{\alpha^+ : \alpha \in X\}$, de modo que $\operatorname{lsub}(X) = \bigcup Y$. Como os ordinais são transitivos e todo o membro de um ordinal é um ordinal, $\operatorname{lsub}(X)$ é um conjunto transitivo de ordinais, e portanto um ordinal por Corolário 67.19.

Se $\alpha \in X$, então $\alpha^+ \in Y$, logo $\alpha^+ \subseteq \bigcup Y = \operatorname{lsub}(X)$, e portanto $\alpha \in \operatorname{lsub}(X)$. Logo $\operatorname{lsub}(X)$ é estritamente maior do que todo o ordinal em $X$.

Inversamente, se $\alpha \in \operatorname{lsub}(X)$, então $\alpha \in \beta^+ \in Y$ para algum $\beta \in X$, de modo que $\alpha \leq \beta \in X$. Logo $\operatorname{lsub}(X)$ é o majorante superior estrito *mínimo* de $X$. □

## Problemas

**Problema 67.1.** Seção 67.2 apresentou três ordenações exemplo sobre os números naturais. Verifique que cada uma é uma boa ordenação.

**Problema 67.2.** Prove Lema 67.5.

**Problema 67.3.** Complete o raciocínio "exatamente análogo" na prova de Teorema 67.17.

**Problema 67.4.** Prove que, se cada membro de $X$ é um ordinal, então $\bigcup X$ é um ordinal.

[5] Alguns livros usam "$\sup(X)$" para isto. Mas outros usam "$\sup(X)$" para o majorante superior *não estrito* mínimo, isto é, simplesmente $\bigcup X$. Se $X$ tem um maior elemento, $\alpha$, estas noções divergem: o majorante superior estrito mínimo é $\alpha^+$, enquanto o majorante superior não estrito mínimo é apenas $\alpha$.

# Capítulo 68

# Estágios e postos

## 68.1 Definindo os estágios como os $V_\alpha$

No Capítulo 67, definimos boas ordenações e os ordinais (de von Neumann). Neste capítulo, usaremos isto para caracterizar a própria hierarquia de conjuntos. Para tal, recordemos que na Seção 67.10 definimos a noção de ordinal sucessor e ordinal limite. Usamos estas ideias na definição seguinte:

**Definição 68.1.**

$$\begin{aligned} V_\emptyset &= \emptyset \\ V_{\alpha^+} &= \wp(V_\alpha) && \text{para qualquer ordinal } \alpha \\ V_\alpha &= \bigcup_{\gamma<\alpha} V_\gamma && \text{quando } \alpha \text{ é um ordinal limite} \end{aligned}$$

Será uma definição por *recursão transfinita* nos ordinais. A este respeito, convém comparar com definições recursivas de funções nos números naturais.[1] Como ao tratar dos números naturais, define-se um caso base e casos sucessor; mas ao tratar de ordinais, também precisamos de descrever o comportamento nos casos *limite*.

Esta definição dos $V_\alpha$ será um marco importante. Motivamos informalmente a nossa hierarquia de conjuntos como formando conjuntos por *estágios*. Os $V_\alpha$ são, em efeito, precisamente esses estágios. Importa, contudo, que se trata de uma caracterização *interna* dos estágios. Em vez de sugerir um possível *modelo* da teoria, teremos definido os estágios *dentro* da nossa teoria dos conjuntos.

[1] Cf. as definições de adição, multiplicação e exponenciação em Seção 6.2.

## 68.2 Teorema(s) de recursão transfinita

O primeiro passo é, contudo, confirmar que Definição 68.1 é uma definição bem sucedida. De modo mais geral, precisamos de provar que qualquer tentativa de definir por recursão transfinita (transfinita) terá êxito. Esse é o objetivo deste texto.

*Aviso: este material é delicado*. A lição geral, no entanto, é bem simples: a indução transfinita mais o Esquema de Substituição garantem a legitimidade de (várias versões da) recursão transfinita.[2]

**Definição 68.2.** Seja $\tau(x)$ um termo; seja $f$ uma função; seja $\alpha$ um ordinal. Dizemos que $f$ é uma *aproximação de ordem* $\alpha$ para $\tau$ sse $\mathrm{dom}(f) = \alpha$ e $(\forall \beta \in \alpha) f(\beta) = \tau(f{\restriction_\beta})$.

**Lema 68.3 (Recursão limitada).** *Para qualquer termo $\tau(x)$ e qualquer ordinal $\alpha$, existe uma única aproximação de ordem $\alpha$ para $\tau$.*

*Prova.* Mostraremos que, para qualquer $\gamma \leq \alpha$, existe uma única aproximação de ordem $\gamma$.

Começamos por estabelecer a unicidade. Sejam $g$ e $h$ (respetivamente) aproximações de ordem $\gamma$ e $\delta$. Uma indução transfinita nos seus argumentos mostra que $g(\beta) = h(\beta)$ para qualquer $\beta \in \mathrm{dom}(g) \cap \mathrm{dom}(h) = \gamma \cap \delta = \min(\gamma, \delta)$. Logo as aproximações são únicas (se existem) e coincidem em todos os valores.

Para estabelecer a existência, usamos agora uma indução transfinita simples (Teorema 67.31) nos ordinais $\delta \leq \alpha$.

A função vazia é trivialmente uma aproximação de ordem $\emptyset$.

Se $g$ é uma aproximação de ordem $\gamma$, então $g \cup \{\langle \gamma, \tau(g)\rangle\}$ é uma aproximação de ordem $\gamma^+$.

Se $\gamma$ é um ordinal limite e $g_\delta$ é uma aproximação de ordem $\delta$ para todo o $\delta < \gamma$, seja $g = \bigcup_{\delta\in\gamma} g_\delta$. Isto é uma função, pois as várias $g_\delta$ coincidem em todos os valores. E se $\delta \in \gamma$ então $g(\delta) = g_{\delta^+}(\delta) = \tau(g_{\delta^+}{\restriction_\delta}) = \tau(g{\restriction_\delta})$.

Isto completa a prova por indução transfinita. □

Se nos permitirmos definir um *termo* em vez de uma função, podemos retirar a cota $\alpha$ do resultado anterior. No enunciado e na prova do resultado seguinte, quando $\sigma$ é um termo, definimos $\sigma{\restriction_\alpha} = \{\langle \beta, \sigma(\beta)\rangle : \beta \in \alpha\}$.

**Teorema 68.4 (Recursão geral).** *Para qualquer termo $\tau(x)$, podemos definir explicitamente um termo $\sigma(x)$ tal que $\sigma(\alpha) = \tau(\sigma{\restriction_\alpha})$ para qualquer ordinal $\alpha$.*

[2] Lembrete: todas as fórmulas e termos podem ter parâmetros (salvo indicação em contrário).

*Prova.* Para cada $\alpha$, por Lema 68.3 existe uma única aproximação de ordem $\alpha$, $f_\alpha$, para $\tau$. Definimos $\sigma(\alpha)$ como $f_{\alpha^+}(\alpha)$. Ora:

$$\begin{aligned}\sigma(\alpha) &= f_{\alpha^+}(\alpha)\\ &= \tau(f_{\alpha^+}{\restriction_\alpha})\\ &= \tau(\{\langle\beta, f_{\alpha^+}(\beta)\rangle : \beta \in \alpha\})\\ &= \tau(\{\langle\beta, f_{\beta^+}(\beta)\rangle : \beta \in \alpha\})\\ &= \tau(\sigma{\restriction_\alpha})\end{aligned}$$

notando que $f_{\beta^+}(\beta) = f_{\alpha^+}(\beta)$ para todo o $\beta < \alpha$, como no Lema 68.3. □

Notemos que Teorema 68.4 é um *esquema*. Crucialmente, não podemos esperar que $\sigma$ defina uma função, isto é, um certo tipo de *conjunto*, pois então $\mathrm{dom}(\sigma)$ seria o conjunto de todos os ordinais, contradizendo o paradoxo de Burali-Forti (Teorema 67.20).

Ainda falta mostrar, contudo, que Teorema 68.4 justifica a nossa definição dos $V_\alpha$. Isto pode não ser óbvio de imediato; mas tornar-se-á claro com uma última versão simples da recursão transfinita.

**Teorema 68.5 (Recursão simples).** *Para quaisquer termos $\tau(x)$ e $\theta(x)$ e qualquer conjunto $A$, podemos definir explicitamente um termo $\sigma(x)$ tal que:*

$$\begin{aligned}\sigma(\varnothing) &= A &&\\ \sigma(\alpha^+) &= \tau(\sigma(\alpha)) && \text{para qualquer ordinal } \alpha\\ \sigma(\alpha) &= \theta(\mathrm{Im}(\sigma{\restriction_\alpha})) && \text{quando } \alpha \text{ é um ordinal limite}\end{aligned}$$

*Prova.* Começamos por definir um termo, $\xi(x)$, do seguinte modo:

$$\xi(x) = \begin{cases} A & \text{se } x \text{ não é uma função cujo}\\ & \quad\text{domínio é um ordinal; caso contrário:}\\ \tau(x(\alpha)) & \text{se } \mathrm{dom}(x) = \alpha^+\\ \theta(\mathrm{Im}(x)) & \text{se } \mathrm{dom}(x) \text{ é um ordinal limite}\end{cases}$$

Por Teorema 68.4, existe um termo $\sigma(x)$ tal que $\sigma(\alpha) = \xi(\sigma{\restriction_\alpha})$ para todo o ordinal $\alpha$; além disso, $\sigma{\restriction_\alpha}$ é uma função com domínio $\alpha$. Mostramos que $\sigma$ tem as propriedades pretendidas, por indução transfinita simples (Teorema 67.31).

Primeiro, $\sigma(\varnothing) = \xi(\varnothing) = A$.

Segundo, $\sigma(\alpha^+) = \xi(\sigma{\restriction_{\alpha^+}}) = \tau(\sigma{\restriction_{\alpha^+}}(\alpha)) = \tau(\sigma(\alpha))$.

Por fim, $\sigma(\alpha) = \xi(\sigma{\restriction_\alpha}) = \theta(\mathrm{Im}(\sigma{\restriction_\alpha}))$, quando $\alpha$ é limite. □

Ora, para justificar Definição 68.1, basta tomar $A = \varnothing$, $\tau(x) = \wp(x)$ e $\theta(x) = \bigcup x$. Por fim, isto justifica a definição dos $V_\alpha$!

## 68.3 Propriedades básicas dos estágios

Para evidenciar a importância fundacional da definição dos $V_\alpha$, apresentaremos alguns resultados básicos sobre eles. Começamos com uma definição:[3]

**Definição 68.6.** O conjunto $A$ é *potente* sse $\forall x((\exists y \in A)x \subseteq y \to x \in A)$.

**Lema 68.7.** *Para cada ordinal $\alpha$:*

1. *Cada $V_\alpha$ é transitivo.*
2. *Cada $V_\alpha$ é potente.*
3. *Se $\gamma \in \alpha$, então $V_\gamma \in V_\alpha$ (e portanto também $V_\gamma \subseteq V_\alpha$, por (1))*

*Prova.* Provamos isto por indução transfinita (simultânea). Para a indução, supomos que (1)–(3) valem para cada ordinal $\beta < \alpha$.

O caso $\alpha = \emptyset$ é trivial.

Suponhamos $\alpha = \beta^+$. Para mostrar (3), se $\gamma \in \alpha$ então $V_\gamma \subseteq V_\beta$ por hipótese, logo $V_\gamma \in \wp(V_\beta) = V_\alpha$. Para mostrar (2), suponhamos $A \subseteq B \in V_\alpha$, isto é, $A \subseteq B \subseteq V_\beta$; então $A \subseteq V_\beta$, logo $A \in V_\alpha$. Para mostrar (1), notemos que se $x \in A \in V_\alpha$ temos $A \subseteq V_\beta$, logo $x \in V_\beta$, logo $x \subseteq V_\beta$ pois $V_\beta$ é transitivo por hipótese, e assim $x \in V_\alpha$.

Suponhamos que $\alpha$ é um ordinal limite. Para mostrar (3), se $\gamma \in \alpha$ então $\gamma \in \gamma^+ \in \alpha$, de modo que $V_\gamma \in V_{\gamma^+}$ por hipótese, logo $V_\gamma \in \bigcup_{\beta\in\alpha} V_\beta = V_\alpha$. Para mostrar (1) e (2), basta observar que uma união de conjuntos transitivos (respetivamente, potentes) é transitiva (respetivamente, potente). □

**Lema 68.8.** *Para cada ordinal $\alpha$, $V_\alpha \notin V_\alpha$.*

*Prova.* Por indução transfinita. Evidentemente $V_\emptyset \notin V_\emptyset$.

Se $V_{\alpha^+} \in V_{\alpha^+} = \wp(V_\alpha)$, então $V_{\alpha^+} \subseteq V_\alpha$; e como $V_\alpha \in V_{\alpha^+}$ por Lema 68.7, temos $V_\alpha \in V_\alpha$. Reciprocamente: se $V_\alpha \notin V_\alpha$ então $V_{\alpha^+} \notin V_{\alpha^+}$

Se $\alpha$ é limite e $V_\alpha \in V_\alpha = \bigcup_{\beta\in\alpha} V_\beta$, então $V_\alpha \in V_\beta$ para algum $\beta \in \alpha$; mas então também $V_\beta \in V_\alpha$, logo $V_\beta \in V_\beta$ por Lema 68.7 (duas vezes). Reciprocamente, se $V_\beta \notin V_\beta$ para todo o $\beta \in \alpha$, então $V_\alpha \notin V_\alpha$. □

**Corolário 68.9.** *Para quaisquer ordinais $\alpha, \beta$: $\alpha \in \beta$ sse $V_\alpha \in V_\beta$*

*Prova.* Lema 68.7 dá um sentido. Reciprocamente, suponhamos $V_\alpha \in V_\beta$. Então $\alpha \neq \beta$ por Lema 68.8; e $\beta \notin \alpha$, pois caso contrário teríamos $V_\beta \in V_\alpha$ e logo $V_\beta \in V_\beta$ por Lema 68.7 (duas vezes), contradizendo Lema 68.8. Logo $\alpha \in \beta$ por tricotomia. □

[3] Não há terminologia padrão para «potente»; este é o nome usado por Button (2021).

Tudo isto permite pensar em cada $V_\alpha$ como o $\alpha$-ésimo estágio da hierarquia. Eis a razão.

Certamente os nossos $V_\alpha$ podem ser vistos como formados num processo *iterativo*, pois o uso de ordinais acompanha a noção de iteração. Além disso, se um estágio é formado antes do outro, isto é, $V_\beta \in V_\alpha$, isto é, $\beta \in \alpha$, então o nosso processo de formação é *cumulativo*, pois $V_\beta \subseteq V_\alpha$. Finalmente, estamos de fato a formar *todas* as coleções possíveis de conjuntos que estavam disponíveis em qualquer estágio anterior, pois qualquer estágio sucessor $V_{\alpha^+}$ é o conjunto potência do seu predecessor $V_\alpha$.

Em resumo: com $\mathbf{ZF}^-$, estamos *quase* a terminar de articular a nossa visão da hierarquia cumulativa e iterativa de conjuntos. (Embora, naturalmente, ainda precisemos de justificar o Esquema de Substituição.)

## 68.4 Fundação

Estamos apenas *quase* concluídos—e não *totalmente* concluídos—porque nada em $\mathbf{ZF}^-$ garante que *todo* o conjunto está em algum $V_\alpha$, isto é, que todo o conjunto é formado em algum estágio.

Há, contudo, um sentido (matemático) bastante direto em que não *importa* se existem conjuntos fora da hierarquia. (Se os houver, podemos simplesmente ignorá-los.) Mas motivamos o nosso *conceito* de conjunto com a ideia de que todo o conjunto é formado em algum estágio (ver *Estágios-são-chave* na Seção 66.1). Logo queremos excluir a possibilidade de conjuntos que caem fora da hierarquia. Por conseguinte, devemos acrescentar um novo axioma, que assegura que todo o conjunto surge em algum lugar da hierarquia.

Uma vez que os $V_\alpha$ são os nossos estágios, poderíamos simplesmente considerar acrescentar o seguinte como axioma:

> *Regularidade.* $\forall A \exists \alpha\ A \subseteq V_\alpha$

Seria uma abordagem perfeitamente razoável. Contudo, por razões que se explicarão adiante, adotaremos antes um axioma alternativo:

**Fundação (Fundação).** $(\forall A \neq \emptyset)(\exists B \in A) A \cap B = \emptyset$.

Com algum trabalho, podemos mostrar (em $\mathbf{ZF}^-$) que a Fundação implica a Regularidade:

**Definição 68.10.** Para cada conjunto $A$, definimos:

$$\begin{aligned} \mathrm{cl}_0(A) &= A, \\ \mathrm{cl}_{n+1}(A) &= \bigcup \mathrm{cl}_n(A), \\ \mathrm{trcl}(A) &= \bigcup_{n<\omega} \mathrm{cl}_n(A). \end{aligned}$$

Chamamos a $\mathrm{trcl}(A)$ o *fecho transitivo* de $A$.

O nome «fecho transitivo» é adequado:

**Proposição 68.11.** *$A \subseteq \mathrm{trcl}(A)$ e $\mathrm{trcl}(A)$ é um conjunto transitivo.*

*Prova.* Evidentemente $A = \mathrm{cl}_0(A) \subseteq \mathrm{trcl}(A)$. E se $x \in b \in \mathrm{trcl}(A)$, então $b \in \mathrm{cl}_n(A)$ para algum $n$, logo $x \in \mathrm{cl}_{n+1}(A) \subseteq \mathrm{trcl}(A)$. □

**Lema 68.12.** *Se $A$ é um conjunto transitivo, então existe algum $\alpha$ tal que $A \subseteq V_\alpha$.*

*Prova.* Recordando a definição de «$\mathrm{lsub}(X)$» em Definição 67.32, definimos dois conjuntos:

$$D = \{x \in A : \forall \delta\ x \nsubseteq V_\delta\}$$
$$\alpha = \mathrm{lsub}\{\delta : (\exists x \in A)(x \subseteq V_\delta \wedge (\forall \gamma \in \delta) x \nsubseteq V_\gamma)\}$$

Suponhamos $D = \emptyset$. Se $x \in A$, então existe algum $\delta$ tal que $x \subseteq V_\delta$ e, pela boa ordenação dos ordinais, $(\forall \gamma \in \delta) x \nsubseteq V_\gamma$; logo $\delta \in \alpha$ e assim $x \in V_\alpha$ por Lema 68.7. Logo $A \subseteq V_\alpha$, como pretendido.

Basta pois mostrar que $D = \emptyset$. Por redução ao absurdo, suponhamos o contrário. Pela Fundação, existe algum $B \in D \subseteq A$ tal que $D \cap B = \emptyset$. Se $x \in B$ então $x \in A$, pois $A$ é transitivo, e como $x \notin D$, segue que $\exists \delta\ x \subseteq V_\delta$. Seja agora

$$\beta = \mathrm{lsub}\{\delta : (\exists x \in B)(x \subseteq V_\delta \wedge (\forall \gamma < \delta) x \nsubseteq V_\gamma)\}.$$

Como antes, $B \subseteq V_\beta$, contradizendo a afirmação de que $B \in D$. □

**Teorema 68.13.** *A Regularidade vale.*

*Prova.* Fixemos $A$; agora $A \subseteq \mathrm{trcl}(A)$ por Proposição 68.11, que é transitivo. Logo existe algum $\alpha$ tal que $A \subseteq \mathrm{trcl}(A) \subseteq V_\alpha$ por Lema 68.12 □

Estes resultados mostram que $\mathbf{ZF}^-$ prova a implicação *Fundação* $\Rightarrow$ *Regularidade*. Em Proposição 68.22, mostraremos que $\mathbf{ZF}^-$ prova *Regularidade* $\Rightarrow$ *Fundação*. Como tal, a Fundação e a Regularidade são *equivalentes* (módulo $\mathbf{ZF}^-$). Mas isto significa que, dado $\mathbf{ZF}^-$, podemos justificar a Fundação notando que é equivalente à Regularidade. E podemos justificar a Regularidade de imediato com base em *Estágios-são-chave*.

## 68.5 Z e ZF: um marco

Com a Fundação, atingimos outro marco importante. Consideramos as teorias $\mathbf{Z}^-$ e $\mathbf{ZF}^-$, que dissemos ser certas teorias «menos» alguma coisa. Essa coisa é a Fundação. Logo:

**Definição 68.14.** A teoria **Z** acrescenta a Fundação a $\mathbf{Z}^-$. Os seus axiomas são Extensionalidade, União, Pares, Conjuntos das Partes, Infinito, Fundação, e todas as instâncias do esquema de Separação.

A teoria **ZF** acrescenta a Fundação a $\mathbf{ZF}^-$. Por outras palavras, **ZF** acrescenta todas as instâncias de Substituição a **Z**.

Ainda assim, uma pergunta pode ter surgido. Se a Regularidade é equivalente sobre $\mathbf{ZF}^-$ à Fundação, e a justificação da Regularidade é clara, por que dar voltas e tomar a Fundação como axioma básico, em vez da Regularidade?

Deixando de lado razões históricas (quem formulou o quê e quando), a razão essencial é que a Fundação pode ser apresentada sem recorrer à definição dos $V_\alpha$. Essa definição dependeu de todo o trabalho na Seção 68.2: foi preciso provar a recursão transfinita, para mostrar que era legítima. Mas a nossa prova da recursão transfinita usou o *Esquema de Substituição*. Logo, embora a Fundação e a Regularidade sejam equivalentes módulo $\mathbf{ZF}^-$, não são equivalentes módulo $\mathbf{Z}^-$.

De fato, a questão é mais grave do que esta observação simples sugere. Embora ultrapasse o âmbito deste livro, verifica-se que tanto $\mathbf{Z}^-$ como **Z** são demasiado fracas para definir os $V_\alpha$. Logo, se se trabalha apenas em **Z**, então a Regularidade (tal como a formulamos) nem sequer faz *sentido*. É por isso que o nosso axioma oficial é a Fundação, e não a Regularidade.

Daqui em diante, trabalharemos em **ZF** (salvo indicação em contrário), sem mais comentários.

## 68.6 Posto

Tendo definido os estágios como os $V_\alpha$ e sabendo que todo o conjunto é subconjunto de algum estágio, podemos definir o *posto* de um conjunto. Intuitivamente, o posto de $A$ é o primeiro momento em que $A$ é formado. Com mais precisão:

**Definição 68.15.** Para cada conjunto $A$, $\text{posto}(A)$ é o menor ordinal $\alpha$ tal que $A \subseteq V_\alpha$.

**Proposição 68.16.** $\text{posto}(A)$ *existe, para qualquer* $A$.

*Prova.* Fica como exercício. □

A boa ordenação dos postos permite provar alguns resultados importantes:

**Proposição 68.17.** *Para qualquer ordinal* $\alpha$, $V_\alpha = \{x : \text{posto}(x) \in \alpha\}$.

*Prova.* Se $\text{posto}(x) \in \alpha$ então $x \subseteq V_{\text{posto}(x)} \in V_\alpha$, logo $x \in V_\alpha$ pois $V_\alpha$ é potente (invocando Lema 68.7 várias vezes). Reciprocamente, se $x \in V_\alpha$ então $x \subseteq V_\alpha$, logo $\text{posto}(x) \leq \alpha$; agora uma indução transfinita simples mostra que $x \notin V_\alpha$. □

**Proposição 68.18.** *Se $B \in A$, então* $\text{posto}(B) \in \text{posto}(A)$.

*Prova.* $A \subseteq V_{\text{posto}(A)} = \{x : \text{posto}(x) \in \text{posto}(A)\}$ por Proposição 68.17. □

Com este fato, podemos estabelecer um resultado que nos permite provar afirmações sobre *todos os conjuntos* por uma forma de indução:

**Teorema 68.19 (Esquema de indução-$\in$).** *Para qualquer fórmula $\varphi$:*

$$\forall A((\forall x \in A)\varphi(x) \to \varphi(A)) \to \forall A \varphi(A).$$

*Prova.* Provaremos a contrapositiva. Suponhamos, pois, $\neg\forall A\varphi(A)$. Pela indução transfinita (Teorema 67.16), existe algum não-$\varphi$ de posto mínimo possível; isto é, algum $A$ tal que $\neg\varphi(A)$ e $\forall x(\text{posto}(x) \in \text{posto}(A) \to \varphi(x))$. Ora, se $x \in A$ então $\text{posto}(x) \in \text{posto}(A)$, por Proposição 68.18, logo $\varphi(x)$; isto é, $(\forall x \in A)\varphi(x) \wedge \neg\varphi(A)$. □

Eis uma forma informal de interpretar este resultado poderoso. Digamos que $\varphi$ é *hereditária* sse sempre que todo o membro de um conjunto é $\varphi$, o próprio conjunto é $\varphi$. Então a indução-$\in$ diz o seguinte: se $\varphi$ é hereditária, todo o conjunto é $\varphi$.

Para concluir a discussão dos postos (por agora), provaremos algumas afirmações que já antecipamos várias vezes.

**Proposição 68.20.** $\text{posto}(A) = \text{lsub}_{x\in A} \text{posto}(x)$.

*Prova.* Seja $\alpha = \text{lsub}_{x\in A} \text{posto}(x)$. Por Proposição 68.18, $\alpha \leq \text{posto}(A)$. Mas se $x \in A$ então $\text{posto}(x) \in \alpha$, logo $x \in V_\alpha$ por Proposição 68.17, e portanto $A \subseteq V_\alpha$, isto é, $\text{posto}(A) \leq \alpha$. Logo $\text{posto}(A) = \alpha$. □

**Corolário 68.21.** *Para qualquer ordinal $\alpha$,* $\text{posto}(\alpha) = \alpha$.

*Prova.* Suponhamos, por indução transfinita, que $\text{posto}(\beta) = \beta$ para todo o $\beta \in \alpha$. Ora, $\text{posto}(\alpha) = \text{lsub}_{\beta\in\alpha} \text{posto}(\beta) = \text{lsub}_{\beta\in\alpha} \beta = \alpha$ por Proposição 68.20.□

Finalmente, eis uma prova rápida do resultado prometido no fim de Seção 68.4, a saber que $\mathbf{ZF}^-$ prova a implicação *Regularidade* $\Rightarrow$ *Fundação*. (Notemos que a noção de «posto» e Proposição 68.18 estão disponíveis para uso nesta prova pois—como indicamos no início deste texto—podem ser apresentadas usando $\mathbf{ZF}^- + \text{Regularidade}$.)

**Proposição 68.22 (trabalhando em $\mathbf{ZF}^- + \mathbf{Regularidade}$).** *A Fundação vale.*

*Prova.* Fixemos $A \neq \emptyset$, e algum $B \in A$ de posto mínimo possível. Se $c \in B$ então $\text{posto}(c) \in \text{posto}(B)$ por Proposição 68.18, logo $c \notin A$ pela escolha de $B$. □

## Problemas

**Problema 68.1.** Prove Proposição 68.16.

**Problema 68.2.** Complete a indução transfinita simples mencionada na Proposição 68.17.

# Capítulo 69

# Substituição

## 69.1 Introdução

A Substituição é o esquema axiomático que distingue **ZF** de **Z**. Recorremos a ele ao longo de Capítulos 67 a 68. Neste capítulo, abordaremos finalmente a questão: a Substituição está justificada?

Para tornar a questão precisa, convém observar que a Substituição é realmente bastante *forte*. Teremos uma ideia de quão forte é ao longo deste capítulo (e de novo na Seção 72.5). Isto sugere que uma justificação é de fato necessária.

Discutiremos dois tipos de justificação. Em traços largos: uma justificação *extrínseca* é uma tentativa de justificar um axioma pelos seus frutos; uma justificação *intrínseca* é uma tentativa de justificar um axioma sugerindo que ele é vindicado pelos conceitos matemáticos em causa. Teremos uma ideia mais clara do que isto significa ao longo deste capítulo, mas não passa da ponta de um icebergue. Para mais pormenores, veja em particular Maddy (1988a e 1988b).

## 69.2 A Força da Substituição

Começamos com uma observação simples sobre a força da Substituição: a menos que ultrapassemos **Z**, não podemos provar a existência de qualquer ordinal de von Neumann maior ou igual a $\omega + \omega$.

Eis um esboço do porquê. Trabalhando em **ZF**, consideremos o conjunto $V_{\omega+\omega}$. Este conjunto serve como domínio de um *modelo* para **Z**. Para ver isto, introduzimos alguma notação para a *relativização* de uma fórmula:

**Definição 69.1.** Para qualquer conjunto $M$, e qualquer fórmula $\varphi$, seja $\varphi^M$ a fórmula que resulta de restringir todos os quantificadores de $\varphi$ a $M$. Isto é, substituir "$\exists x$" por "$(\exists x \in M)$", e substituir "$\forall x$" por "$(\forall x \in M)$".

Pode mostrar-se que, para todo o axioma $\varphi$ de **Z**, tem-se $\mathbf{ZF} \vdash \varphi^{V_{\omega+\omega}}$. Mas $\omega + \omega$ não está *em* $V_{\omega+\omega}$, por Corolário 68.21. Logo **Z** é consistente com a não existência de $\omega + \omega$.

Foi por isso que dissemos, na Seção 67.7, que Teorema 67.26 não pode ser provado sem Substituição. Pois é fácil, dentro de **Z**, definir uma boa ordenação explícita que intuitivamente *deveria* ter tipo de ordem $\omega + \omega$. De fato, demos um exemplo informal disto em Seção 67.2, quando apresentamos a ordenação nos números naturais dada por:

$$\begin{gathered} n \lessdot m \text{ sse ou } n < m \text{ e } m - n \text{ é par,} \\ \text{ou } n \text{ é par e } m \text{ é ímpar.} \end{gathered}$$

Mas se $\omega + \omega$ não existe, esta boa ordenação não é isomorfa a nenhum ordinal. Logo **Z** *não* prova Teorema 67.26.

Invertendo o prisma: a Substituição permite provar a existência de $\omega + \omega$, e portanto tem de permitir provar a existência de $V_{\omega+\omega}$. E não só. Para *qualquer* boa ordenação que possamos definir, Teorema 67.26 nos diz que existe algum $\alpha$ isomorfo com essa boa ordenação, e portanto que $V_\alpha$ existe. De forma direta, então, a Substituição garante que a hierarquia de conjuntos tem de ser *muito alta*.

Nas próximas partes do capítulo, e de novo em Seção 72.5, teremos uma ideia mais clara de quão *alta* a Substituição força a hierarquia a ser. O ponto simples, por agora, é que a Substituição *precisa* mesmo de justificação!

## 69.3 Considerações Extrínsecas sobre a Substituição

Começamos por considerar uma tentativa *extrínseca* de justificar a Substituição. Boolos sugere uma, como segue.

> [...] a razão para adotar os axiomas da substituição é bastante simples: têm muitas consequências desejáveis e (aparentemente) nenhuma indesejável. Para além de teoremas sobre a concepção iterativa, as consequências incluem uma teoria satisfatória, embora não ideal, dos números infinitos, e um resultado altamente desejável que justifica definições indutivas em relações bem fundadas. (Boolos, 1971, 229)

A ideia central de Boolos é que devemos justificar a Substituição pelos seus frutos. E os frutos específicos que menciona são os que temos discutido nos últimos capítulos. A Substituição permitiu-nos provar que os ordinais de von Neumann eram excelentes sucedâneos da ideia de um tipo de boa ordenação (isto é a nossa "teoria satisfatória, embora não ideal, dos números infinitos"). A Substituição permitiu-nos também definir os $V_\alpha$, estabelecer a noção de posto e provar a indução-$\in$ (isto corresponde aos nossos "teoremas sobre a

concepção iterativa"). Por fim, a Substituição permite provar o teorema de recursão transfinita (isto são as "definições indutivas em relações bem fundadas").

São, de fato, consequências desejáveis. Mas estas consequências desejáveis bastam para *justificar* a Substituição? *Não*. Ou pelo menos, não de forma direta.

Eis um problema simples. Embora tenhamos enunciado algumas consequências desejáveis da Substituição, muitas delas poderiam ter sido obtidas por outras vias. Isto não é tão conhecido como devia, pelo que convém explicar a situação.

Existe uma teoria simples de conjuntos, a Teoria dos Níveis, ou **LT** abreviadamente.[1] Os axiomas de **LT** são apenas Extensionalidade, Separação e a afirmação de que todo o conjunto é subconjunto de algum *nível*, onde "nível" é definido de modo astuto para que os níveis se comportem como os nossos amigos, os $V_\alpha$. Logo **ZF** prova **LT**; mas **LT** é *muito* mais fraca que **ZF**. De fato, **LT** não dá Pares, Conjuntos potencia, Infinito nem Substituição. Seja **Zr** o resultado de acrescentar Infinito e Conjuntos potencia a **LT**; isto fornece também Pares, logo **Zr** é pelo menos tão forte quanto **Z**. Mas, de fato, **Zr** é estritamente mais forte que **Z**, pois acrescenta a afirmação de que todo o conjunto tem posto (daí a sugestão de o chamar **Zr**). De fato, **Zr** fornece: uma teoria perfeitamente satisfatória dos ordinais; resultados que estratificam a hierarquia em estágios bem ordenados; uma prova da indução-$\in$; e uma *versão* da recursão transfinita.

Em resumo: embora Boolos não soubesse disto, todas as consequências desejáveis que menciona poderiam ter sido obtidas *sem* Substituição; bastaria usar **Zr** em vez de **Z**.

(Diante disto, por que seguimos a rota convencional, ensinando-lhe **ZF** em vez de **LT** e **Zr**? Há duas razões. Primeiro: por razões puramente históricas, começar por **LT** é pouco standard; queríamos dotá-lo de ferramentas para ler discussões mais standard de teoria de conjuntos. Segundo: quando estiver preparado para apreciar **LT** e **Zr**, pode simplesmente ler Potter 2004 e Button 2021.)

Naturalmente, como **Zr** é estritamente mais fraca que **ZF**, há resultados que **ZF** prova e que **Zr** deixa em aberto. Logo alguém poderia tentar justificar a Substituição em bases extrínsecas apontando para um desses resultados. Mas, uma vez que saiba usar **Zr**, é bastante difícil encontrar muitos exemplos de coisas que (a) ficam decididas pela Substituição mas não de outro modo, e (b) são intuitivamente verdadeiras. (Para mais sobre isto, veja Potter 2004, §13.2.)

[1] As primeiras versões de **LT** são apresentadas por Montague (1965) e Scott (1974); foi simplificada e recebeu tratamento de livro por Potter (2004); e Button (2021) simplificou recentemente ainda mais **LT**.

A conclusão é esta. Para fornecer uma justificação extrínseca convincente da Substituição, seria preciso encontrar um resultado que *não* possa ser obtido sem Substituição. E isso não é empresa fácil.

Consideremos um problema adicional que surge para qualquer tentativa de oferecer uma justificação puramente extrínseca da Substituição. (Este problema é talvez mais fundamental que o primeiro.) Boolos não se limita a observar que a Substituição tem muitas consequências desejáveis. Afirma também que a Substituição "(aparentemente) não tem" consequências indesejáveis. Mas esta ressalva entre parênteses, "aparentemente", é seguramente absolutamente crucial.

Relembre como chegamos aqui: a Compreensão ingênua encontrou inconsistência, e respondemos a essa inconsistência abraçando a concepção cumulativa-iterativa de conjunto. Esta concepção vem equipada com uma narrativa que, esperamos, nos assegura a sua consistência. Mas se não pudermos justificar a Substituição dentro dessa narrativa, então não temos (ainda) razão para crer que **ZF** é consistente. Ou melhor: não temos razão para crer que **ZF** é consistente, para além do fato (talvez meramente contingente) de que ninguém descobriu ainda uma contradição. Exatamente nesse sentido, o comentário de Boolos parece reduzir-se a isto: "(aparentemente) **ZF** é consistente". Deveríamos exigir maior garantia de consistência do que isto.

Esta questão afecta qualquer tentativa *puramente* extrínseca de justificar a Substituição, isto é, qualquer justificação formulada unicamente em termos das consequências (conhecidas) de **ZF**. Como tal, convém procurar uma justificação *intrínseca* da Substituição, isto é, uma justificação que sugira que a narrativa que contamos sobre conjuntos de algum modo "já" nos compromete com a Substituição.

## 69.4 Limitação de Tamanho

Talvez a tentativa mais comum de oferecer uma justificação "intrínseca" da Substituição passe pela seguinte noção:

> *Limitação-de-tamanho*. Quaisquer coisas formam um conjunto, desde que não haja demasiadas.

Este princípio vindicará de imediato a Substituição. Afinal, qualquer conjunto formado por Substituição não pode ser maior do que o conjunto a partir do qual foi formado. Enunciado com precisão: suponha que forma um conjunto $\tau[A] = \{\tau(x) : x \in A\}$ usando Substituição; então $\tau[A] \preceq A$; logo, se os membroos de $A$ não eram demasiado numerosos para formar um conjunto, as suas imagens não são demasiado numerosas para formar $\tau[A]$.

A dificuldade óbvia em invocar *Limitação-de-tamanho* para justificar a Substituição é que *ainda* não estabelecemos qualquer princípio como *Limitação-de-tamanho*.

Além disso, quando contamos a nossa história sobre a concepção cumulativa-iterativa de conjunto em Capítulos 65 a 66, nada *sugeriu* a direção de *Limitação-de-tamanho*. Isto é, de fato, precisamente a razão pela qual Boolos escreveu num dado momento: "Talvez se possa concluir que há pelo menos dois pensamentos 'por detrás' da teoria de conjuntos" (1989, p. 19). Por um lado, as ideias em torno da concepção cumulativa-iterativa de conjunto destinam-se a vindicar **Z**. Por outro, *Limitação-de-tamanho* visa vindicar a Substituição.

Mas a questão não é apenas termos estado até aqui *em silêncio* sobre *Limitação-de-tamanho*. Antes, a questão é que *Limitação-de-tamanho* (tal como acabamos de o formular) parece assentar mal com a noção cumulativa-iterativa de conjunto. Afinal, não menciona nada sobre a ideia de conjuntos formados em *estágios*.

Isto não surpreende muito, dada a história destes "dois pensamentos" (isto é, a concepção cumulativa-iterativa de conjunto, e *Limitação-de-tamanho*). Estes "dois pensamentos" acabam por ser dois projetos bastante diferentes para bloquear os paradoxos da teoria de conjuntos. A noção cumulativa-iterativa de conjunto bloqueia o paradoxo de Russell dizendo, em traços largos: *nunca deveríamos ter esperado que existisse um conjunto de Russell, porque não seria "formado" em nenhum estágio*. Por contraste, *Limitação-de-tamanho* visa excluir o conjunto de Russell, dizendo, em traços largos: *nunca deveríamos ter esperado que existisse um conjunto de Russell, porque seria demasiado grande*.

Posto assim, sejamos diretos: considerada como resposta aos paradoxos, *Limitação-de-tamanho* carece de *muito* mais justificação. Considere, por exemplo, esta versão do paradoxo de Russell: *nenhum pug fareja exatamente os pugs que não se cheiram a si próprios* (ver Seção 65.2). Se perguntar "por que não há tal pug?", não é boa resposta dizer-lhe que tal pug teria de cheirar demasiados pugs. Logo por que seria boa explicação intuitiva, da não existência de um conjunto de Russell, que teria de ser "demasiado grande" para existir?

Em suma, é perdoável estar um pouco perplexo quanto à motivação "intuitiva" para *Limitação-de-tamanho*.

## 69.5 Substituição e "Infinito Absoluto"

Deixamos agora *Limitação-de-tamanho* para trás e exploramos uma outra família de tentativas (intrínsecas) de justificar a Substituição, que levam a sério a ideia de conjuntos formados em estágios.

Quando delineamos pela primeira vez o processo iterativo, oferecemos alguns princípios que explicam o que acontece em cada estágio. Foram *Estágios-são-chave*, *Estágios-são-ordenados*, e *Estágios-acumulam*. Mais tarde, acrescentamos alguns princípios que nos dizem algo sobre o número de estágios: *Estágios-prosseguem* disse-nos que o processo de formação de conjuntos nunca termina, e *Estágios-atingem-o-infinito* disse-nos que o processo passa por um estágio infinito-ésimo.

É razoável sugerir que estes dois últimos princípios decorrem de algum princípio mais amplo, como:

> *Estágios-são-inesgotáveis*. Há absolutamente infinitamente muitos estágios; a hierarquia é tão alta quanto possível.

Obviamente isto é um princípio informal. Mas mesmo que não seja imediatamente *implicado* pela concepção cumulativa-iterativa de conjunto, certamente parece *consonante* com ela. Pelo menos, e ao contrário de *Limitação-de-tamanho*, retém a ideia de que os conjuntos são formados estágio a estágio.

A esperança, agora, é alavancar *Estágios-são-inesgotáveis* numa justificação da Substituição. Vejamos como isso poderia fazer-se.

Na Seção 67.2, vimos que é fácil construir uma boa ordenação que (moralmente) deveria ser isomorfa a $\omega + \omega$. Dito de outro modo, podemos facilmente imaginar um processo iterativo estágio a estágio, cujo tipo de ordem (moralmente) é $\omega + \omega$. Como tal, se aceitamos *Estágios-são-inesgotáveis*, então deveríamos certamente aceitar que há pelo menos um estágio $\omega + \omega$-ésimo da hierarquia, isto é, $V_{\omega+\omega}$, pois a hierarquia seguramente *poderia* continuar até aqui.

Este pensamento generaliza-se como segue: para qualquer boa ordenação, o processo de construir a hierarquia iterativa deveria correr pelo menos tão longe quanto essa boa ordenação. E poderíamos garantir isto tratando Teorema 67.26 como um *axioma*. Isto diria-nos que toda a boa ordenação é isomorfa a um ordinal de von Neumann. Como cada ordinal de von Neumann será igual ao seu próprio posto, Teorema 67.26 dir-nos-á então que, sempre que possamos descrever uma boa ordenação na nossa teoria de conjuntos, o processo iterativo de formação de conjuntos tem de ultrapassar essa boa ordenação.

Esta ideia parece certamente um corolário de *Estágios-são-inesgotáveis*. Infelizmente, se o nosso objetivo é extrair a Substituição desta ideia, enfrentamos um obstáculo simples e técnico: a Substituição é estritamente mais forte que Teorema 67.26. (Esta observação é feita por Potter (2004, §13.2); prová-lo-emos na Seção 69.8.)

A conclusão é que, se vamos entender *Estágios-são-inesgotáveis* de modo a obter a Substituição, então não pode *meramente* dizer que a hierarquia ultrapassa qualquer boa ordenação. Tem de fazer uma afirmação mais forte. Com este fim, Shoenfield (1977) propôs um reforço muito natural da ideia, como segue: a hierarquia não é *cofinal* com nenhum conjunto.[2] Com um pouco mais de pormenor: se $\tau$ é um mapeamento que envia conjuntos para estágios da hierarquia, a imagem de qualquer conjunto $A$ sob $\tau$ não esgota a hierarquia. Dito de outro modo (esquematicamente):

[2] Gödel parece ter proposto um pensamento semelhante; ver Potter (2004, p. 223). Para discussão de Gödel e Shoenfield, ver Incurvati (2020, 90–5).

> *Estágios-são-supercofinais*. Se $A$ é um conjunto e $\tau(x)$ é um estágio para todo o $x \in A$, então existe um estágio que vem depois de cada $\tau(x)$ para $x \in A$.

É óbvio que **ZF** prova uma versão adequadamente formalizada de *Estágios-são-supercofinais*. Reciprocamente, podemos argumentar informalmente que *Estágios-são-supercofinais* justifica a Substituição.[3] De fato, suponha $(\forall x \in A)\exists! y\, \varphi(x,y)$. Então, para cada $x \in A$, seja $\sigma(x)$ o $y$ tal que $\varphi(x,y)$, e seja $\tau(x)$ o estágio em que $\sigma(x)$ é formado pela primeira vez. Por *Estágios-são-supercofinais*, existe um estágio $V$ tal que $(\forall x \in A)\tau(x) \in V$. Ora, como cada $\tau(x) \in V$ e $\sigma(x) \subseteq \tau(x)$, por Separação podemos obter $\{y \in V : (\exists x \in A)\sigma(x) = y\} = \{y : (\exists x \in A)\varphi(x,y)\}$.

Logo *Estágios-são-supercofinais* vindica a Substituição. E é pelo menos plausível que *Estágios-são-inesgotáveis* vindique *Estágios-são-supercofinais*. De fato, suponha que *Estágios-são-supercofinais* falha. Logo a hierarquia é cofinal com algum conjunto $A$, isto é, temos uma aplicação $\tau$ tal que para qualquer estágio $S$ existe algum $x \in A$ tal que $S \in \tau(x)$. Nesse caso, temos de fato uma forma de apreender o suposto "infinito absoluto" da hierarquia: ele é *esgotado* pela imagem de $\tau$ aplicada a $A$. E isso compromete a ideia de que a hierarquia é "absolutamente infinita". Contrapondo: *Estágios-são-inesgotáveis* implica *Estágios-são-supercofinais*, que por sua vez justifica a Substituição.

Isto representa uma tentativa genuinamente promissora de fornecer uma justificação intrínseca da Substituição. Mas se funciona ultimamente ou não, teremos de deixar para si decidir.

## 69.6 Substituição e Reflexão

A nossa última tentativa de justificar a Substituição, via *Estágios-são-inesgotáveis*, começa com um resultado profundo e elegante:[4]

**Teorema 69.2 (Esquema de reflexão).** *Para qualquer fórmula $\varphi$:*

$$\forall \alpha \exists \beta > \alpha (\forall x_1 \ldots, x_n \in V_\beta)(\varphi(x_1, \ldots, x_n) \leftrightarrow \varphi^{V_\beta}(x_1, \ldots, x_n))$$

Como na Definição 69.1, $\varphi^{V_\beta}$ é o resultado de restringir todos os quantificadores de $\varphi$ ao conjunto $V_\beta$. Assim, intuitivamente, a Reflexão diz o seguinte: se $\varphi$ é verdadeira em toda a hierarquia, então $\varphi$ é verdadeira em arbitrariamente muitos *segmentos iniciais* da hierarquia.

Montague (1961) e Lévy (1960) mostraram que (formulações adequadas da) Substituição e da Reflexão são equivalentes, módulo **Z**, de modo que

[3] Seria mais difícil provar a Substituição usando alguma formalização de *Estágios-são-supercofinais*, pois **Z** por si só não é forte o suficiente para definir os estágios, logo não é claro como se formalizaria *Estágios-são-supercofinais*. Uma opção, contudo, é trabalhar nalguma extensão de **LT**, como discutido na Seção 69.3.

[4] Lembrete: todas as fórmulas podem ter parâmetros (salvo indicação explícita em contrário).

acrescentar qualquer uma delas dá **ZF**. (Provamos estes resultados na Seção 69.7.) Dada esta equivalência, poder-se-á esperar justificar a Reflexão e a Substituição via *Estágios-são-inesgotáveis* do seguinte modo: dado *Estágios-são-inesgotáveis*, a hierarquia deverá ser muito, muito alta; tão alta, de fato, que nada do que podemos dizer sobre ela é suficiente para limitar a sua altura. E podemos entender isto como a ideia de que, se qualquer sentença $\varphi$ é verdadeira em toda a hierarquia, então é verdadeira em arbitrariamente muitos segmentos iniciais da hierarquia. E isso é precisamente a Reflexão.

De novo, isto parece uma tentativa genuinamente promissora de fornecer uma justificação intrínseca da Substituição. Mas há demasiado a dizer sobre o assunto aqui. Cabe-lhe agora decidir por si se tem êxito.[5]

## 69.7 Apêndice: Resultados sobre Substituição

A seguir, provaremos a Reflexão dentro de **ZF**. Provaremos também em que sentido a Reflexão é equivalente à Substituição. E provaremos uma consequência interessante de tudo isto, relativa à força da Reflexão/Substituição. *Aviso: isto é, de longe, a parte mais avançada de matemática deste manual.*

Começamos com um lema que, por brevidade, recorre ao expediente notacional do *sobrelinhado* para lidar com sequências de variáveis ou objetos. Assim: "$\overline{a}_k$" abrevia "$a_{k_1}, \ldots, a_{k_n}$", onde $n$ é determinado pelo contexto.

**Lema 69.3.** *Para cada $1 \leq i \leq k$, seja $\varphi_i(\overline{v}_i, x)$ uma fórmula. Então, para cada $\alpha$ existe algum $\beta > \alpha$ tal que, para quaisquer $\overline{a}_1, \ldots, \overline{a}_k \in V_\beta$ e cada $1 \leq i \leq k$:*

$$\exists x \varphi_i(\overline{a}_i, x) \to (\exists x \in V_\beta)\varphi_i(\overline{a}_i, x)$$

*Prova.* Definimos um termo $\mu$ como segue: $\mu(\overline{a}_1, \ldots, \overline{a}_k)$ é o estágio mínimo, $V$, que satisfaz todos os seguintes condicionais, para $1 \leq i \leq k$:

$$\exists x \varphi_i(\overline{a}_i, x) \to (\exists x \in V)\varphi_i(\overline{a}_i, x))$$

É fácil verificar que $\mu(\overline{a}_1, \ldots, \overline{a}_k)$ existe para todos $\overline{a}_1, \ldots, \overline{a}_k$. Ora, usando a Substituição e o nosso teorema de recursão, definimos:

$$\begin{aligned} S_0 &= V_{\alpha+1} \\ S_{n+1} &= S_n \cup \bigcup \{\mu(\overline{a}_1, \ldots, \overline{a}_k) : \overline{a}_1, \ldots, \overline{a}_k \in S_n\} \\ S &= \bigcup_{m<\omega} S_n. \end{aligned}$$

Cada $S_n$, e portanto o próprio $S$, é um estágio depois de $V_\alpha$. Fixemos $\overline{a}_1$, $\ldots$, $\overline{a}_k \in S$; logo existe algum $n < \omega$ tal que $\overline{a}_1$, $\ldots$, $\overline{a}_k \in S_n$. Fixemos algum $1 \leq i \leq k$, e suponhamos que $\exists x \varphi_i(\overline{a}_i, x)$. Então $(\exists x \in \mu(\overline{a}_1, \ldots, \overline{a}_k))\varphi_i(\overline{a}_i, x)$ por construção, logo $(\exists x \in S_{n+1})\varphi_i(\overline{a}_i, x)$ e portanto $(\exists x \in S)\varphi_i(\overline{a}_i, x)$. Logo $S$ é o nosso $V_\beta$. □

[5] Poderá, no entanto, querer continuar lendo Incurvati (2020, 95–100).

Podemos agora provar Teorema 69.2 de forma bastante direta:

*Prova.* Fixemos $\alpha$. Sem perda de generalidade, podemos assumir que os únicos conectivos de $\varphi$ são $\exists$, $\neg$ e $\wedge$ (pois estes são expressivamente adequados). Sejam $\psi_1, \ldots, \psi_k$ uma enumeração de cada uma das subfórmulas de $\varphi$ por ordem de complexidade, de modo que $\psi_k = \varphi$. Por Lema 69.3, existe um $\beta > \alpha$ tal que, para qualquer $\overline{a}_i \in V_\beta$ e cada $1 \leq i \leq k$:

$$\exists x \psi_i(\overline{a}_i, x) \to (\exists x \in V_\beta)\psi_i(\overline{a}_i, x) \tag{*}$$

Por indução na complexidade de $\psi_i$, mostraremos que $\psi_i(\overline{a}_i) \leftrightarrow \psi_i^{V_\beta}(\overline{a}_i)$, para qualquer $\overline{a}_i \in V_\beta$. Se $\psi_i$ é atómica, isto é trivial. A bicondicional estabelece também que, quando $\psi_i$ é uma negação ou conjunção de subfórmulas que satisfazem esta propriedade, a própria $\psi_i$ satisfaz esta propriedade. Logo o único caso interessante é o da quantificação. Fixemos $\overline{a}_i \in V_\beta$; então:

$$\begin{aligned}
(\exists x \psi_i(\overline{a}_i, x))^{V_\beta} &\text{ sse } (\exists x \in V_\beta)\psi_i^{V_\beta}(\overline{a}_i, x) && \text{por definição} \\
&\text{sse } (\exists x \in V_\beta)\psi_i(\overline{a}_i, x) && \text{por hipótese} \\
&\text{sse } \exists x \psi_i(\overline{a}_i, x) && \text{por (*)}
\end{aligned}$$

Isto completa a indução; o resultado segue pois $\psi_k = \varphi$. □

Provamos a Reflexão em **ZF**. A nossa prova seguiu essencialmente Montague (1961). Queremos agora provar em **Z** que a Reflexão implica a Substituição. A prova segue Lévy (1960), com uma simplificação.

Como trabalhamos em **Z**, não podemos apresentar a Reflexão exatamente na forma dada acima. Afinal, formulamos a Reflexão usando a notação "$V_\alpha$", e isso não pode ser definido em **Z** (ver Seção 68.5). Em vez disso, ofereceremos uma formulação aparentemente mais fraca da Substituição, como segue:

> *Reflexão fraca.* Para qualquer fórmula $\varphi$, existe um conjunto transitivo $S$ tal que $0$, $1$ e quaisquer parâmetros de $\varphi$ são membroos de $S$, e $(\forall \overline{x} \in S)(\varphi \leftrightarrow \varphi^S)$.

Para usar isto na prova da Substituição, seguiremos primeiro Lévy (1960, primeira parte do Teorema 2) e mostraremos que podemos "refletir" duas fórmulas de uma vez:

**Lema 69.4 (em Z + Reflexão fraca.).** *Para quaisquer fórmulas $\psi, \chi$, existe um conjunto transitivo $S$ tal que $0$ e $1$ (e quaisquer parâmetros das fórmulas) são membroos de $S$, e $(\forall \overline{x} \in S)((\psi \leftrightarrow \psi^S) \wedge (\chi \leftrightarrow \chi^S))$.*

*Prova.* Seja $\varphi$ a fórmula $(z = 0 \wedge \psi) \vee (z = 1 \wedge \chi)$.

Aqui usamos uma abreviatura; devemos explicitar "$z = 0$" como "$\forall t\, t \notin z$" e "$z = 1$" como "$\forall s(s \in z \leftrightarrow \forall t\, t \notin s)$". Mas como $0, 1 \in S$ e $S$ é transitivo, estas fórmulas são *absolutas* para $S$; isto é, aplicam-se ao mesmo objeto quer restrinjamos os seus quantificadores a $S$.[6]

Pela Reflexão fraca, temos algum $S$ adequado tal que:

$$\begin{aligned}
&(\forall z, \overline{x} \in S)(\varphi \leftrightarrow \varphi^S)\\
\text{isto é } &(\forall z, \overline{x} \in S)(((z = 0 \wedge \psi) \vee (z = 1 \wedge \chi)) \leftrightarrow\\
&\qquad ((z = 0 \wedge \psi) \vee (z = 1 \wedge \chi))^S)\\
\text{isto é } &(\forall z, \overline{x} \in S)(((z = 0 \wedge \psi) \vee (z = 1 \wedge \chi)) \leftrightarrow\\
&\qquad ((z = 0 \wedge \psi^S) \vee (z = 1 \wedge \chi^S)))\\
\text{isto é } &(\forall \overline{x} \in S)((\psi \leftrightarrow \psi^S) \wedge (\chi \leftrightarrow \chi^S))
\end{aligned}$$

A segunda afirmação implica a terceira porque "$z = 0$" e "$z = 1$" são absolutas para $S$; a quarta segue pois $0 \neq 1$. □

Podemos agora obter a Substituição, seguindo e simplificando Lévy (1960, Teorema 6):

**Teorema 69.5 (em Z + Reflexão fraca).** *Para qualquer fórmula $\varphi(v, w)$, e qualquer $A$, se $(\forall x \in A)\exists! y\, \varphi(x, y)$, então $\{y : (\exists x \in A)\varphi(x, y)\}$ existe.*

*Prova.* Fixemos $A$ tal que $(\forall x \in A)\exists! y\, \varphi(x, y)$, e definimos fórmulas:

$$\begin{aligned}
&\psi \text{ é } (\varphi(x, z) \wedge A = A)\\
&\chi \text{ é } \exists y\, \varphi(x, y)
\end{aligned}$$

Usando Lema 69.4, como $A$ é um parâmetro de $\psi$, existe um conjunto transitivo $S$ tal que $0, 1, A \in S$ (juntamente com quaisquer outros parâmetros), e tal que:

$$(\forall x, z \in S)((\psi \leftrightarrow \psi^S) \wedge (\chi \leftrightarrow \chi^S))$$

Logo, em particular:

$$\begin{aligned}
&(\forall x, z \in S)(\varphi(x, z) \leftrightarrow \varphi^S(x, z))\\
&(\forall x \in S)(\exists y \varphi(x, y) \leftrightarrow (\exists y \in S)\varphi^S(x, y))
\end{aligned}$$

Combinando isto, e observando que $A \subseteq S$ pois $A \in S$ e $S$ é transitivo:

$$(\forall x \in A)(\exists y \varphi(x, y) \leftrightarrow (\exists y \in S)\varphi(x, y))$$

Ora, $(\forall x \in A)(\exists! y \in S)\varphi(x, y)$, porque $(\forall x \in A)\exists! y\, \varphi(x, y)$. Ora, a Separação dá $\{y \in S : (\exists x \in A)\varphi(x, y)\} = \{y : (\exists x \in A)\varphi(x, y)\}$. □

[6] Mais formalmente, seja $\xi$ qualquer uma destas fórmulas; então $\xi(z) \leftrightarrow \xi^S(z)$.

## 69.8 Apêndice: Axiomatizabilidade finita

Terminamos este capítulo extraindo alguns resultados da Substituição. O primeiro resultado é devido a Montague (1961); note que não é uma prova *dentro* de **ZF**, mas uma prova *sobre* **ZF**:

**Teorema 69.6.** **ZF** *não é finitamente axiomatizável. Mais geralmente: se* **T** *é finita e* $\mathbf{T} \vdash \mathbf{ZF}$*, então* **T** *é inconsistente.*

*(Aqui nos restringimos tacitamente a sentenças de primeira ordem cujo único primitivo não lógico é* $\in$*, e escrevemos* $\mathbf{T} \vdash \mathbf{ZF}$ *para indicar que* $\mathbf{T} \vdash \varphi$ *para todo o* $\varphi \in \mathbf{ZF}$*.)*

*Prova.* Fixemos **T** finita tal que $\mathbf{T} \vdash \mathbf{ZF}$. Logo **T** prova a Reflexão, isto é, Teorema 69.2. Como **T** é finita, podemos reescrevê-la como uma única conjunção, $\theta$. Refletindo com esta fórmula, $\mathbf{T} \vdash \exists \beta(\theta \leftrightarrow \theta^{V_\beta})$. Como trivialmente $\mathbf{T} \vdash \theta$, obtemos $\mathbf{T} \vdash \exists \beta\, \theta^{V_\beta}$.

Ora, seja $\psi(X)$ uma abreviatura de:

$$\theta^X \wedge X \text{ é transitivo} \wedge (\forall Y \in X)(Y \text{ é transitivo} \to \neg\theta^Y)$$

isto diz, em traços largos: $X$ é um modelo transitivo de $\theta$, e $\in$-minimal a esse respeito. Ora, recordando que $\mathbf{T} \vdash \exists \beta\, \theta^{V_\beta}$, por fatos básicos sobre postos dentro de **ZF** e portanto dentro de **T**, temos:

$$\mathbf{T} \vdash \exists M \psi(M). \tag{*}$$

Usando o primeiro conjunto de $\psi(X)$, sempre que $\mathbf{T} \vdash \sigma$, temos $\mathbf{T} \vdash \forall X(\psi(X) \to \sigma^X)$. Logo, por (*):

$$\mathbf{T} \vdash \forall X(\psi(X) \to (\exists N \psi(N))^X)$$

Usando isto, e (*) de novo:

$$\mathbf{T} \vdash \exists M(\psi(M) \wedge (\exists N \psi(N))^M)$$

Em particular, então:

$$\mathbf{T} \vdash \exists M(\psi(M) \wedge (\exists N \in M)((N \text{ é transitivo})^N \wedge (\theta^N)^M))$$

Logo, por raciocínio elementar sobre transitividade:

$$\mathbf{T} \vdash \exists M(\psi(M) \wedge (\exists N \in M)(N \text{ é transitivo} \wedge \theta^N))$$

Logo **T** é inconsistente.[7] □

[7] Este "raciocínio elementar" envolve provar certos "fatos de absolutidade" para conjuntos transitivos.

Eis um resultado semelhante, assinalado por Potter (2004, 223):

**Proposição 69.7.** *Seja* **T** *uma extensão de* **Z** *com um número finito de novos axiomas. Se* $\mathbf{T} \vdash \mathbf{ZF}$*, então* **T** *é inconsistente. (Aqui usamos as mesmas restrições tácitas que para Teorema 69.6.)*

*Prova.* Usemos $\theta$ para a conjunção de todos os axiomas de **T** *exceto* as (infinitas) instâncias de Separação. Definindo $\psi$ a partir de $\theta$ como no Teorema 69.6, podemos mostrar que $\mathbf{T} \vdash \exists M \psi(M)$.

Como no Teorema 69.6, podemos estabelecer o esquema de que, sempre que $\mathbf{T} \vdash \sigma$, temos $\mathbf{T} \vdash \forall X(\psi(X) \to \sigma^X)$. Terminamos a prova exatamente como no Teorema 69.6.

No entanto, estabelecer o esquema envolve um pouco mais de trabalho do que no Teorema 69.6. Afinal, as instâncias de Separação estão em **T**, mas não são conjuntos de $\theta$. Contudo, podemos ultrapassar este obstáculo provando que $\mathbf{T} \vdash \forall X(X \text{ é transitivo} \to \sigma^X)$, para toda a instância de Separação $\sigma$. Deixamos isto ao leitor. □

Como observamos na Seção 69.5, isto mostra que a Substituição é estritamente mais forte que Teorema 67.26. Ou, um pouco mais precisamente: se **Z** + "toda a boa ordenação é isomorfa a um ordinal único" for consistente, então não prova alguma instância da Substituição.

## Problemas

**Problema 69.1.** Apresente uma formalização de *Estágios-são-supercofinais* em **ZF**.

**Problema 69.2.** Mostre que, para toda a instância de Separação $\sigma$, tem-se: $\mathbf{Z} \vdash \forall X(X \text{ é transitivo} \to \sigma^X)$. (Usamos este esquema na Proposição 69.7.)

**Problema 69.3.** Mostre que, para todo o $\varphi \in \mathbf{Z}$, tem-se $\mathbf{ZF} \vdash \varphi^{V_{\omega+\omega}}$.

**Problema 69.4.** Confirme os restantes resultados esquemáticos invocados nas provas de Teorema 69.6 e Proposição 69.7.

# Capítulo 70

# Aritmética Ordinal

## 70.1 Introdução

No Capítulo 67, desenvolvemos uma teoria dos números ordinais. Vimos no Capítulo 68 que podemos pensar nos ordinais como uma espinha dorsal em torno da qual se constrói o restante da hierarquia. Mas esse não é o único papel dos ordinais. Há também a tarefa de efetuar a aritmética ordinal.

Já aludimos a isto, em Seção 67.2, quando falamos de $\omega$, $\omega + 1$ e $\omega + \omega$. Na altura falamos informalmente; chegou a altura de o expor com rigor. Devemos contudo mencionar que não há muita filosofia neste capítulo; apenas desenvolvimentos técnicos, juntamente com uma observação (ligeiramente) interessante de que podemos fazer a mesma coisa de duas maneiras diferentes.

## 70.2 Adição Ordinal

Suponha-se que se pretende somar $\alpha$ e $\beta$. Pode simplesmente colocar-se uma cópia de $\beta$ imediatamente a seguir a uma cópia de $\alpha$. (É preciso tomar *cópias*, pois sabemos por Proposição 67.22 que ou $\alpha \subseteq \beta$ ou $\beta \subseteq \alpha$.) O efeito intuitivo disto é percorrer uma $\alpha$-sucessão de passos, *e depois* percorrer uma $\beta$-sucessão. A sucessão resultante fica bem ordenada; logo, por Teorema 67.26 é isomorfa a um ordinal (único). Esse ordinal pode considerar-se a *soma* de $\alpha$ e $\beta$.

Esta é a ideia intuitiva por detrás da adição ordinal. Para a definir com rigor, começa-se pela ideia de tomar *cópias* de conjuntos. A ideia é usar etiquetas arbitrárias, 0 e 1, para saber de onde veio cada objeto:

**Definição 70.1.** A *soma disjunta* de $A$ e $B$ é $A \sqcup B = (A \times \{0\}) \cup (B \times \{1\})$.

Define-se em seguida uma ordem em pares de ordinais:

**Definição 70.2.** Para quaisquer ordinais $\alpha_1, \alpha_2, \beta_1, \beta_2$, diga-se que:

$$\langle \alpha_1, \alpha_2 \rangle \lhd \langle \beta_1, \beta_2 \rangle \text{ sse ou } \alpha_2 \in \beta_2$$
$$\text{ou tanto } \alpha_2 = \beta_2 \text{ como } \alpha_1 \in \beta_1$$

Trata-se de uma ordem *lexicográfica inversa*, pois ordena-se pelo segundo elemento e depois pelo primeiro. Recorde-se que se pretendia definir $\alpha + \beta$ como o tipo de ordem de uma cópia de $\alpha$ seguida de uma cópia de $\beta$. Para o conseguir, define-se:

**Definição 70.3.** Para quaisquer ordinais $\alpha$, $\beta$, a sua soma é $\alpha + \beta = \mathrm{ord}(\alpha \sqcup \beta, \lhd)$.

Note-se que aqui se abusou ligeiramente da notação; estritamente deveria escrever-se "$\{\langle x, y\rangle \in \alpha \sqcup \beta : x \lhd y\}$" em lugar de "$\lhd$". Por brevidade, contudo, continuaremos a abusar da notação deste modo no que se segue.

O resultado seguinte, juntamente com Teorema 67.26, confirma que a nossa definição está bem formada:

**Lema 70.4.** *$\langle \alpha \sqcup \beta, \lhd \rangle$ é um bom ordenamento, para quaisquer ordinais $\alpha$ e $\beta$.*

*Prova.* Obviamente $\lhd$ é conexa em $\alpha \sqcup \beta$. Para mostrar que é bem fundada, fixe-se um $X \subseteq \alpha \sqcup \beta$ não vazio. Seja $Y$ o subconjunto de $X$ cuja segunda coordenada é a menor possível, isto é, $Y = \{\langle \gamma, i\rangle \in X : (\forall \langle \delta, j\rangle \in X) i \leq j\}$. Escolha-se agora o elemento de $Y$ com menor primeira coordenada. □

Temos assim uma definição explícita e clara da adição ordinal. Eis um fato não surpreendente (recorde-se que $1 = \{0\}$, por Definição 66.7):

**Proposição 70.5.** *$\alpha + 1 = \alpha^+$, para qualquer ordinal $\alpha$.*

*Prova.* Considere-se o isomorfismo $f$ de $\alpha^+ = \alpha \cup \{\alpha\}$ para $\alpha \sqcup 1 = (\alpha \times \{0\}) \sqcup (\{0\} \times \{1\})$ dado por $f(\gamma) = \langle \gamma, 0\rangle$ para $\gamma \in \alpha$, e $f(\alpha) = \langle 0, 1\rangle$. □

Além disso, é fácil mostrar que a adição obedece a certas condições recursivas:

**Lema 70.6.** *Para quaisquer ordinais $\alpha, \beta$, tem-se:*

$$\begin{aligned} \alpha + 0 &= \alpha \\ \alpha + (\beta + 1) &= (\alpha + \beta) + 1 \\ \alpha + \beta &= \operatorname{lsub}_{\delta < \beta}(\alpha + \delta) \qquad \text{se } \beta \text{ é um ordinal limite} \end{aligned}$$

*Prova.* Verifica-se caso a caso; primeiro:

$$\begin{aligned}
\alpha + 0 &= \operatorname{ord}((\alpha \times \{0\}) \cup (0 \times \{1\}), \lhd) \\
&= \operatorname{ord}((\alpha \times \{0\}) \cup \{0\}, \lhd) \\
&= \alpha \\
\alpha + (\beta + 1) &= \operatorname{ord}((\alpha \times \{0\}) \cup (\beta^+ \times \{1\}), \lhd) \\
&= \operatorname{ord}((\alpha \times \{0\}) \cup (\beta \times \{1\}), \lhd) + 1 \\
&= (\alpha + \beta) + 1
\end{aligned}$$

Seja agora $\beta \neq \emptyset$ um limite. Se $\delta < \beta$ então também $\delta + 1 < \beta$, logo $\alpha + \delta$ é um segmento inicial próprio de $\alpha + \beta$. Logo $\alpha + \beta$ é um majorante estrito de $X = \{\alpha + \delta : \delta < \beta\}$. Além disso, se $\alpha \leq \gamma < \alpha + \beta$, então claramente $\gamma = \alpha + \delta$ para algum $\delta < \beta$. Logo $\alpha + \beta = \operatorname{lsub}_{\delta<\beta}(\alpha + \delta)$. □

Mas eis um fato marcante. Para definir a adição ordinal, poder-se-ia *em alternativa* ter usado simplesmente o teorema da recursão transfinita, e estipulado as equações recursivas, exatamente como em Lema 70.6 (embora com "$\beta^+$" em vez de "$\beta + 1$").

Há, pois, duas maneiras diferentes de definir operações nos ordinais. Podem definir-se *sinteticamente*, construindo explicitamente um conjunto bem ordenado e considerando o seu tipo de ordem. Ou podem definir-se *recursivamente*, apenas estipulando as equações recursivas. Feito corretamente, porém, o resultado é idêntico. De fato, Teorema 67.26 garante que estas equações recursivas determinam ordinais *únicos*.

Em muitos aspectos, a aritmética ordinal comporta-se como a adição dos números naturais. Por exemplo, pode provar-se o seguinte:

**Lema 70.7.** *Se $\alpha, \beta, \gamma$ são ordinais, então:*

1. *se $\beta < \gamma$, então $\alpha + \beta < \alpha + \gamma$*
2. *se $\alpha + \beta = \alpha + \gamma$, então $\beta = \gamma$*
3. *$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, isto é, a adição é associativa*
4. *Se $\alpha \leq \beta$, então $\alpha + \gamma \leq \beta + \gamma$*

*Prova.* Provamos (3), deixando o resto como exercício. A prova é por indução transfinita simples em $\gamma$, usando Lema 70.6. Quando $\gamma = 0$:

$$(\alpha + \beta) + 0 = \alpha + \beta = \alpha + (\beta + 0)$$

Quando $\gamma = \delta + 1$, suponha-se por indução que $(\alpha + \beta) + \delta = \alpha + (\beta + \delta)$; usando Lema 70.6 três vezes:

$$\begin{aligned}(\alpha + \beta) + (\delta + 1) &= ((\alpha + \beta) + \delta) + 1 \\ &= (\alpha + (\beta + \delta)) + 1 \\ &= \alpha + ((\beta + \delta) + 1) \\ &= \alpha + (\beta + (\delta + 1))\end{aligned}$$

Quando $\gamma$ é um ordinal limite, suponha-se por indução que se $\delta \in \gamma$ então $(\alpha + \beta) + \delta = \alpha + (\beta + \delta)$; então:

$$\begin{aligned}(\alpha + \beta) + \gamma &= \operatorname{lsub}_{\delta<\gamma}((\alpha + \beta) + \delta) \\ &= \operatorname{lsub}_{\delta<\gamma}(\alpha + (\beta + \delta)) \\ &= \alpha + \operatorname{lsub}_{\delta<\gamma}(\beta + \delta) \\ &= \alpha + (\beta + \gamma)\end{aligned}$$

□

Deste modo, a adição ordinal deve parecer muito familiar. Há contudo um ponto crucial em que a adição ordinal *não* se parece com a adição nos naturais.

**Proposição 70.8.** *A adição ordinal* não *é comutativa;* $1 + \omega = \omega < \omega + 1$.

*Prova.* Note-se que $1 + \omega = \operatorname{lsub}_{n<\omega}(1 + n) = \omega \in \omega \cup \{\omega\} = \omega^+ = \omega + 1$.□

Embora isto possa surpreender à primeira vista, *não devia*. Por um lado, ao considerar $1 + \omega$, pensa-se no tipo de ordem que se obtém colocando um elemento extra *antes* de todos os números naturais. Raciocinando como com o Hotel de Hilbert em Seção 6.1, intuitivamente esse primeiro elemento extra não altera o tipo de ordem global. Por outro lado, ao considerar $\omega + 1$, pensa-se no tipo de ordem que se obtém colocando um elemento extra *depois* de todos os números naturais. E isso é algo radicalmente diferente!

## 70.3 Usando Adição Ordinal

Com a adição nos ordinais, podemos calcular explicitamente os postos de vários conjuntos, no sentido de Definição 68.15:

**Lema 70.9.** *Se* $\operatorname{posto}(A) = \alpha$ *e* $\operatorname{posto}(B) = \beta$, *então:*

1. $\operatorname{posto}(\wp(A)) = \alpha + 1$
2. $\operatorname{posto}(\{A, B\}) = \max(\alpha, \beta) + 1$
3. $\operatorname{posto}(A \cup B) = \max(\alpha, \beta)$

4. $\text{posto}(\langle A, B\rangle) = \max(\alpha, \beta) + 2$
5. $\text{posto}(A \times B) \leq \max(\alpha, \beta) + 2$
6. $\text{posto}(\bigcup A) = \alpha$ *quando* $\alpha$ *é vazio ou limite;* $\text{posto}(\bigcup A) = \gamma$ *quando* $\alpha = \gamma + 1$

*Prova.* Ao longo de todo o raciocínio, invocamos repetidamente Proposição 68.20.

*(1).* Se $x \subseteq A$ então $\text{posto}(x) \leq \text{posto}(A)$. Logo $\text{posto}(\wp(A)) \leq \alpha + 1$. Como em particular $A \in \wp(A)$, tem-se $\text{posto}(\wp(A)) = \alpha + 1$.

*(2).* Por Proposição 68.20

*(3).* Por Proposição 68.20.

*(4).* Por (2), duas vezes.

*(5).* Note-se que $A \times B \subseteq \wp(\wp(A \cup B))$, e invoque (4).

*(6).* Se $\alpha = \gamma + 1$, existe algum $c \in A$ com $\text{posto}(c) = \gamma$, e nenhum membro de $A$ tem posto superior; logo $\text{posto}(\bigcup A) = \gamma$. Se $\alpha$ é um ordinal limite, então $A$ tem membros com posto arbitrariamente próximo (mas estritamente inferior) de $\alpha$, pelo que $\bigcup A$ também tem membros com posto arbitrariamente próximo (mas estritamente inferior) de $\alpha$, e portanto $\text{posto}(\bigcup A) = \alpha$. □

Deixamos como exercício mostrar por que (5) envolve uma *des*igualdade.

Estamos também agora em condições de mostrar que várias noções razoáveis do que possa significar descrever um ordinal como "finito" ou "infinito" coincidem:

**Lema 70.10.** *Para qualquer ordinal* $\alpha$*, as seguintes afirmações são equivalentes:*

1. $\alpha \notin \omega$*, isto é,* $\alpha$ *não é um número natural*
2. $\omega \leq \alpha$
3. $1 + \alpha = \alpha$
4. $\alpha \approx \alpha + 1$*, isto é,* $\alpha$ *e* $\alpha + 1$ *são equipotentes*
5. $\alpha$ *é infinito de Dedekind*

Temos assim cinco formas provavelmente equivalentes de precisar o que exige que um ordinal seja (in)finito.

*Prova.* *(1)* $\Rightarrow$ *(2).* Por tricotomia.

*(2)* $\Rightarrow$ *(3).* Fixe $\alpha \geq \omega$. Por indução transfinita, existe um ordinal $\gamma$ mínimo (possivelmente 0) tal que existe um ordinal limite $\beta$ com $\alpha = \beta + \gamma$. Ora:

$$1 + \alpha = 1 + (\beta + \gamma) = (1 + \beta) + \gamma = \operatorname*{lsub}_{\delta < \beta}(1 + \delta) + \gamma = \beta + \gamma = \alpha.$$

*(3)* $\Rightarrow$ *(4).* Existe claramente uma bijeção $f \colon (\alpha \sqcup 1) \to (1 \sqcup \alpha)$. Se $1 + \alpha = \alpha$, existe um isomorfismo $g \colon (1 \sqcup \alpha) \to \alpha$. Considere-se $g \circ f$.

*(4)* ⇒ *(5)*. Se $\alpha \approx \alpha + 1$, existe uma bijeção $f\colon (\alpha \sqcup 1) \to \alpha$. Defina $g(\gamma) = f(\gamma, 0)$ para cada $\gamma < \alpha$; esta injeção mostra que $\alpha$ é infinito de Dedekind, pois $f(0,1) \in \alpha \setminus \mathrm{Im}(g)$.

*(5)* ⇒ *(1)*. Isto é Proposição 66.8. □

## 70.4 Multiplicação Ordinal

Passamos agora à multiplicação ordinal, abordando-a de forma muito semelhante à adição ordinal. Suponha-se que se pretende multiplicar $\alpha$ por $\beta$. Pode imaginar-se uma grelha retangular, com largura $\alpha$ e altura $\beta$; o produto de $\alpha$ e $\beta$ é então o resultado de percorrer cada linha e depois passar à linha seguinte… até percorrer toda a grelha. Dito de outro modo, o produto de $\alpha$ e $\beta$ obtém-se substituindo *cada* elemento de $\beta$ por uma cópia de $\alpha$.

Para formalizar, usa-se simplesmente a ordem lexicográfica inversa no produto cartesiano de $\alpha$ e $\beta$:

**Definição 70.11.** Para quaisquer ordinais $\alpha, \beta$, o seu produto $\alpha \cdot \beta = \mathrm{ord}(\alpha \times \beta, \lhd)$.

É preciso de novo confirmar que esta definição está bem formada:

**Lema 70.12.** *$\langle \alpha \times \beta, \lhd \rangle$ é um bom ordenamento, para quaisquer ordinais $\alpha$ e $\beta$.*

*Prova.* Exatamente como para Lema 70.4. □

E não é difícil provar que a multiplicação se comporta assim:

**Lema 70.13.** *Para quaisquer ordinais $\alpha, \beta$:*

$$\begin{aligned} \alpha \cdot 0 &= 0 \\ \alpha \cdot (\beta + 1) &= (\alpha \cdot \beta) + \alpha \\ \alpha \cdot \beta &= \operatorname{lsub}_{\delta < \beta}(\alpha \cdot \delta) \qquad \text{quando } \beta \text{ é um ordinal limite.} \end{aligned}$$

*Prova.* Deixado como exercício. □

De fato, tal como no caso da adição, poderíamos ter definido a multiplicação ordinal por estas equações recursivas, em vez de dar uma definição direta. Tal como na adição, certo comportamento é familiar:

**Lema 70.14.** *Se $\alpha, \beta, \gamma$ são ordinais, então:*

1. *se $\alpha \neq 0$ e $\beta < \gamma$, então $\alpha \cdot \beta < \alpha \cdot \gamma$;*
2. *se $\alpha \neq 0$ e $\alpha \cdot \beta = \alpha \cdot \gamma$, então $\beta = \gamma$;*
3. *$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$;*

4. *Se* $\alpha \leq \beta$, *então* $\alpha \cdot \gamma \leq \beta \cdot \gamma$;
5. $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$.

*Prova.* Deixado como exercício. □

Pode provar-se (ou consultar) outros resultados, à vontade. Mas, dado Proposição 70.8, o que se segue não deve surpreender:

**Proposição 70.15.** *A multiplicação ordinal não é comutativa:* $2 \cdot \omega = \omega < \omega \cdot 2$

*Prova.* $2 \cdot \omega = \text{lsub}_{n<\omega}(2 \cdot n) = \omega \in \text{lsub}_{n<\omega}(\omega + n) = \omega + \omega = \omega \cdot 2$. □

De novo, a justificação intuitiva é direta. Para calcular $2 \cdot \omega$, substitui-se cada número natural por duas entidades. Obtém-se o mesmo tipo de ordem se simplesmente se inserirem todos os números "meios" nos naturais, isto é, se se considerar a ordem natural em $\{n/2 : n \in \omega\}$. Assim posto, o tipo de ordem é claramente o mesmo que o de $\omega$ em si. Mas, para calcular $\omega \cdot 2$, dispõem-se duas cópias de $\omega$, uma a seguir à outra.

## 70.5 Exponenciação Ordinal

Passamos agora à exponenciação ordinal. Infelizmente, não há uma definição *simpática* sintética para a exponenciação ordinal.

Certo que *existem* definições sintéticas explícitas. Eis uma. Seja $\text{finfun}(\alpha, \beta)$ o conjunto de todas as funções $f\colon \alpha \to \beta$ tais que $\{\gamma \in \alpha : f(\gamma) \neq 0\}$ é equipotente a algum número natural. Defina-se um bom ordenamento em $\text{finfun}(\alpha, \beta)$ por $f \sqsubset g$ sse $f \neq g$ e $f(\gamma_0) < g(\gamma_0)$, onde $\gamma_0 = \max\{\gamma \in \alpha : f(\gamma) \neq g(\gamma)\}$. Então pode definir-se $\alpha^{(\beta)}$ como $\text{ord}(\text{finfun}(\alpha, \beta), \sqsubset)$. Potter usa esta definição explícita e explica de seguida:

> A escolha desta ordenação determina-se unicamente pelo desejo de obter uma definição da exponenciação ordinal que obedeça à condição recursiva adequada. . . , e é muito mais difícil de visualizar do que a soma ou o produto ordenados. (Potter, 2004, p. 199)

Exatamente. Explicamos a adição como "uma cópia de $\alpha$ seguida de uma cópia de $\beta$", e a multiplicação como "uma $\beta$-sucessão de cópias de $\alpha$". Mas não temos nada de sucinto a dizer sobre $\text{finfun}(\alpha, \gamma)$. Por isso, apresentaremos a definição da exponenciação ordinal apenas *por* recursão transfinita, isto é:

**Definição 70.16.**

$$\begin{aligned} \alpha^{(0)} &= 1 \\ \alpha^{(\beta+1)} &= \alpha^{(\beta)} \cdot \alpha \\ \alpha^{(\beta)} &= \bigcup_{\delta<\beta} \alpha^{(\delta)} && \text{quando } \beta \text{ é um ordinal limite} \end{aligned}$$

Se trabalhássemos *como* teoristas de conjuntos, poderíamos querer explorar algumas propriedades da exponenciação ordinal. Mas pouco mais temos a acrescentar, salvo notar o fato pouco surpreendente de que a exponenciação ordinal não comuta. Assim $2^{(\omega)} = \bigcup_{\delta<\omega} 2^{(\delta)} = \omega$, enquanto $\omega^{(2)} = \omega \cdot \omega$. Mas então não se deve *esperar* que comute, pois já não comuta nos naturais: $2^{(3)} = 8 < 9 = 3^{(2)}$.

## Problemas

**Problema 70.1.** Prove o resto de Lema 70.7.

**Problema 70.2.** Exiba conjuntos $A$ e $B$ tais que $\text{posto}(A \times B) = \max(\text{posto}(A), \text{posto}(B))$.
Exiba conjuntos $A$ e $B$ tais que $\text{posto}(A \times B) = \max(\text{posto}(A), \text{posto}(B)) + 2$.
São possíveis outros postos?

**Problema 70.3.** Prove Lema 70.12, Lema 70.13, e Lema 70.14

**Problema 70.4.** Usando indução transfinita, prove que, se se define $\alpha^{(\beta)} = \text{ord}(\text{finfun}(\alpha, \beta), \sqsubset)$, obtêm-se as equações recursivas de Definição 70.16.

# Capítulo 71

# Cardinais

## 71.1 Princípio de Cantor

Volte o pensamento a Seção 67.5. Estávamos a discutir conjuntos bem ordenados e sugerimos que seria desejável ter objetos que funcionem como representantes dos bons ordenamentos. Com isto em mente, introduzimos os ordinais e depois mostramos em Corolário 67.28 que estes se comportam como desejamos, isto é:

$$\mathrm{ord}(A, <) = \mathrm{ord}(B, \lessdot) \text{ sse } \langle A, < \rangle \cong \langle B, \lessdot \rangle.$$

Volte ainda mais atrás, a Seção 4.8. Ali, trabalhando ingenuamente, introduzimos a noção de "tamanho" de um conjunto. Especificamente, dissemos que dois conjuntos são equipotentes, $A \approx B$, precisamente quando existe uma bijeção $f\colon A \to B$. Esta noção é intrinsecamente mais simples do que a de um bom ordenamento: interessam-nos apenas as bijeções, e não (como com os isomorfismos de ordem) se as bijeções "preservam alguma estrutura".

Tudo isto sugere um pensamento óbvio. Tal como introduzimos certos objetos, *ordinais*, para calibrar bons ordenamentos, podemos introduzir certos objetos, *cardinais*, para calibrar tamanho. Esse é o objetivo deste capítulo.

Antes de dizer o que serão estes cardinais, convém enunciar um princípio que devem satisfazer. Escrevendo $|X|$ para a cardinalidade do conjunto $X$, desejaríamos que obedecessem a:

$$|A| = |B| \text{ sse } A \approx B.$$

Chamaremos a isto o Princípio *de Cantor*, já que Cantor foi provavelmente o primeiro a tê-lo claramente presente. (Diremos mais sobre a sua relação com o Princípio de *Hume* na Seção 71.5.) O nosso objetivo é definir $|X|$, para cada $X$, de modo a que satisfaça o Princípio de Cantor.

## 71.2 Cardinais como Ordinais

De fato, a nossa teoria dos cardinais fará uso (descarado) da nossa teoria dos ordinais. Ou seja: definiremos os cardinais como certos ordinais específicos. Em particular, proporemos o seguinte:

**Definição 71.1.** Se $A$ pode ser bem ordenado, então $|A|$ é o menor ordinal $\gamma$ tal que $A \approx \gamma$. Para qualquer ordinal $\gamma$, diz-se que $\gamma$ é um *cardinal* sse $\gamma = |\gamma|$.

Acabamos de usar a locução "$A$ pode ser bem ordenado". Como quase sempre em matemática, a locução modal aqui é apenas um atalho para uma asserção existencial: dizer "$A$ pode ser bem ordenado" é dizer "existe uma relação que bem ordena $A$".

Há contudo um problema com Definição 71.1. Gostaríamos que *todo* o conjunto tivesse um tamanho, isto é, que $|A|$ existisse para todo $A$. A definição que acabamos de dar, porém, começa por uma condicional: "*Se* $A$ pode ser bem ordenado…". Se existir algum conjunto $A$ que não possa ser bem ordenado, a nossa definição simplesmente deixa de definir um objeto $|A|$.

Logo, para usar Definição 71.1, precisamos de uma garantia de que todo o conjunto pode ser bem ordenado. Infelizmente, essa garantia não está disponível em **ZF**. Assim, se queremos usar Definição 71.1, não há alternativa senão acrescentar um novo axioma, tal como:

**Bom ordenamento (Bom ordenamento).** Todo o conjunto pode ser bem ordenado.

Discutiremos se o axioma do bom ordenamento é aceitável em Capítulo 73. Daqui em diante, porém, simplesmente o admitiremos. E, com ele, é bastante direto provar que os cardinais (tal como definidos na Definição 71.1) existem e comportam-se bem:

**Lema 71.2.** *Para todo o conjunto $A$:*

1. *$|A|$ existe e é único;*
2. *$|A| \approx A$;*
3. *$|A|$ é um cardinal, isto é, $|A| = ||A||$;*

*Prova.* Fixe $A$. Pelo Bom ordenamento, existe um bom ordenamento $\langle A, R\rangle$. Por Teorema 67.26, $\langle A, R\rangle$ é isomorfo a um único ordinal, $\beta$. Logo $A \approx \beta$. Por indução transfinita, existe um único ordinal mínimo, $\gamma$, tal que $A \approx \gamma$. Logo $|A| = \gamma$, o que estabelece (1) e (2). Para (3), note-se que se $\delta \in \gamma$ então $\delta \prec A$, pela escolha de $\gamma$, logo também $\delta \prec \gamma$ pois a equipotência é uma relação de equivalência (Proposição 4.20). Logo $\gamma = |\gamma|$. □

O resultado seguinte garante o Princípio de Cantor, e mais ainda. (Note-se que os cardinais herdam a ordem dos ordinais, isto é, $\mathfrak{a} < \mathfrak{b}$ sse $\mathfrak{a} \in \mathfrak{b}$. Ao formular isto, usaremos letras Fraktur para objetos que sabemos serem cardinais. Isto é bastante usual. Uma alternativa comum é usar letras gregas, já que os cardinais são ordinais, escolhendo-as do meio do alfabeto, por exemplo $\kappa, \lambda$.):

**Lema 71.3.** *Para quaisquer conjuntos $A$ e $B$:*

$$A \approx B \text{ sse } |A| = |B|$$
$$A \preceq B \text{ sse } |A| \leq |B|$$
$$A \prec B \text{ sse } |A| < |B|$$

*Prova.* Provaremos o sentido da esquerda para a direita da segunda afirmação (os outros casos são semelhantes e ficam como exercício). Considere-se o diagrama seguinte:

$$\begin{array}{ccc} A & \longrightarrow & B \\ \updownarrow & & \updownarrow \\ |A| & \dashrightarrow & |B| \end{array}$$

As setas duplas indicam bijeções, cuja existência é garantida por Lema 71.2. Ao supor $A \preceq B$, existe uma injeção $A \to B$. Seguindo as setas de $|A|$ para $A$, para $B$ e para $|B|$, obtém-se uma injeção $|A| \to |B|$ (a seta tracejada). □

Pode ainda usar-se Lema 71.3 para voltar a provar Cantor–Bernstein. Trata-se da afirmação de que se $A \preceq B$ e $B \preceq A$ então $A \approx B$. A enunciamos como Teorema 4.25, mas a provamos primeiro—com algum esforço—em Seção 6.5. Considere-se:

*Nova prova de Schröder-Bernstein.* Se $A \preceq B$ e $B \preceq A$, então $|A| \leq |B|$ e $|B| \leq |A|$ por Lema 71.3. Logo $|A| = |B|$ e $A \approx B$ por tricotomia e Lema 71.3. □

Embora seja uma prova muito simples, apoia-se implicitamente na Substituição (para assegurar Teorema 67.26) e no Bom ordenamento (para garantir Lema 71.3). Em contraste, a prova na Seção 6.5 era muito mais autônoma (de fato, pode efetuar-se em $\mathbf{Z}^-$).

## 71.3 ZFC: um marco

Com a adição do axioma do bom ordenamento, atingimos o último marco teórico. Dispomos agora de todos os axiomas necessários para **ZFC**. Em detalhe:

**Definição 71.4.** A teoria **ZFC** tem estes axiomas: Extensionalidade, União, Pares, Conjuntos potência, Infinitude, Fundação, Bom ordenamento e todas as instâncias dos esquemas de Separação e Substituição. Dito de outro modo, **ZFC** acrescenta o Bom ordenamento a **ZF**.

**ZFC** significa teoria de conjuntos de *Zermelo–Fraenkel* com *Escolha*. Isto pode parecer ligeiramente estranho, pois o axioma que adicionamos se chama "Bom ordenamento", não "Escolha". Mas, quando mais tarde formularmos a *Escolha*, verificar-se-á que o Bom ordenamento lhe é equivalente (módulo **ZF**) (ver Teorema 73.6). Logo, qual tomar como axioma "básico" é indiferente. E o nome "**ZFC**" é inteiramente standard na literatura.

## 71.4 Finito, Enumerável, Não Enumerável

Agora que fomos introduzidos aos cardinais, vale a pena dedicar um pouco de tempo a variedades de cardinais; nomeadamente, cardinais finitos, enumerável e não enumerável.

Os nossos dois primeiros resultados implicam que os cardinais finitos serão exatamente os ordinais finitos, que definimos como os nossos *números naturais* em Definição 66.7:

**Proposição 71.5.** *Sejam $n, m \in \omega$. Então $n = m$ sse $n \approx m$.*

*Prova.* O sentido *da esquerda para a direita* é trivial. Para provar *da direita para a esquerda*, suponha-se $n \approx m$ embora $n \neq m$. Por tricotomia, ou $n \in m$ ou $m \in n$; suponha-se, sem perda de generalidade, $n \in m$. Então $n \subsetneq m$ e existe uma bijeção $f : m \to n$, logo $m$ é infinito de Dedekind, o que contradiz Proposição 66.8. □

**Corolário 71.6.** *Se $n \in \omega$, então $n$ é um cardinal.*

*Prova.* Imediato. □

Segue-se também que várias noções razoáveis do que possa significar descrever um cardinal como "finito" ou "infinito" coincidem:

**Teorema 71.7.** *Para qualquer conjunto $A$, as seguintes afirmações são equivalentes:*

1. *$|A| \notin \omega$, isto é, $A$ não é um número natural;*
2. *$\omega \leq |A|$;*
3. *$A$ é infinito de Dedekind.*

*Prova.* Por Lema 70.10, Lema 71.3, e Corolário 71.6. □

Isto autoriza a seguinte *definição* de algumas noções que usamos de forma informal na Parte I:

**Definição 71.8.** Diz-se que $A$ é *finito* sse $|A|$ é um número natural, isto é, $|A| \in \omega$. Caso contrário, diz-se que $A$ é *infinito*.

Note-se que esta definição é apresentada no contexto de **ZFC**. Afinal, precisamos do Bom ordenamento para garantir que todo o conjunto tem uma cardinalidade. E, de fato, sem o Bom ordenamento, pode existir um conjunto que nem é finito nem infinito de Dedekind. Voltaremos a este tipo de questão no Capítulo 73. Por ora, continuamos a assumir o Bom ordenamento.

Passemos agora dos cardinais finitos aos cardinais infinitos. Eis dois pontos elementares:

**Corolário 71.9.** *$\omega$ é o menor cardinal infinito.*

*Prova.* $\omega$ é um cardinal, pois $\omega$ é infinito de Dedekind e se $\omega \approx n$ para algum $n \in \omega$ então $n$ seria infinito de Dedekind, contrariando Proposição 66.8. Ora, $\omega$ é o menor cardinal infinito por definição. □

**Corolário 71.10.** *Todo o cardinal infinito é um ordinal limite.*

*Prova.* Seja $\alpha$ um ordinal sucessor infinito, logo $\alpha = \beta + 1$ para algum $\beta$. Por Proposição 71.5, $\beta$ também é infinito, logo $\beta \approx \beta + 1$ por Lema 70.10. Ora, $|\beta| = |\beta + 1| = |\alpha|$ por Lema 71.3, logo $\alpha \neq |\alpha|$. □

Já na Definição 4.27, assinalamos que podemos distinguir conjuntos infinitos enumerável de conjuntos infinitos não enumerável. Essa definição conduz naturalmente ao seguinte:

**Proposição 71.11.** *$A$ é enumerável sse $|A| \leq \omega$, e $A$ é não enumerável sse $\omega < |A|$.*

*Prova.* Por tricotomia, as duas afirmações são equivalentes, bastando provar que $A$ é enumerável sse $|A| \leq \omega$. Para *da direita para a esquerda*: se $|A| \leq \omega$, então $A \preceq \omega$ por Lema 71.3 e Corolário 71.9. Para *da esquerda para a direita*: suponha-se $A$ enumerável; então, por Definição 4.27, há três casos possíveis:

1. se $A = \emptyset$, então $|A| = 0 \in \omega$, por Corolário 71.6 e Lema 71.3.
2. se $n \approx A$, então $|A| = n \in \omega$, por Corolário 71.6 e Lema 71.3.
3. se $\omega \approx A$, então $|A| = \omega$, por Corolário 71.9.

Em todos os casos, $|A| \leq \omega$. □

De fato, $\omega$ tem um lugar especial. Embora existam muitos ordinais contáveis:

**Corolário 71.12.** *$\omega$ é o único cardinal infinito enumerável.*

*Prova.* Seja $\mathfrak{a}$ um cardinal infinito enumerável. Como $\mathfrak{a}$ é infinito, $\omega \leq \mathfrak{a}$. Como $\mathfrak{a}$ é um cardinal infinito enumerável, $\mathfrak{a} = |\mathfrak{a}| \leq \omega$. Logo $\mathfrak{a} = \omega$ por tricotomia. □

Claro que existem infinitos cardinais. Poderíamos perguntar: *Quantos cardinais há?* Os resultados seguintes mostram que convém reconsiderar essa pergunta.

**Proposição 71.13.** *Se todo o membro de $X$ é um cardinal, então $\bigcup X$ é um cardinal.*

*Prova.* É fácil verificar que $\bigcup X$ é um ordinal. Seja $\alpha \in \bigcup X$ um ordinal; então $\alpha \in \mathfrak{b} \in X$ para algum cardinal $\mathfrak{b}$. Como $\mathfrak{b}$ é um cardinal, $\alpha \prec \mathfrak{b}$. Como $\mathfrak{b} \subseteq \bigcup X$, tem-se $\mathfrak{b} \preceq \bigcup X$, e portanto $\alpha \not\approx \bigcup X$. Generalizando, $\bigcup X$ é um cardinal. □

**Teorema 71.14.** *Não existe um cardinal máximo.*

*Prova.* Para qualquer cardinal $\mathfrak{a}$, o teorema de Cantor (Teorema 4.24) e Lema 71.2 implicam que $\mathfrak{a} < |\wp(\mathfrak{a})|$. □

**Teorema 71.15.** *O conjunto de todos os cardinais não existe.*

*Prova.* Por redução ao absurdo, suponha-se $C = \{\mathfrak{a} : \mathfrak{a} \text{ é um cardinal}\}$. Ora, $\bigcup C$ é um cardinal por Proposição 71.13, logo por Teorema 71.14 existe um cardinal $\mathfrak{b} > \bigcup C$. Por definição $\mathfrak{b} \in C$, logo $\mathfrak{b} \subseteq \bigcup C$, donde $\mathfrak{b} \leq \bigcup C$, uma contradição. □

Compare isto com o paradoxo de Russell e com Burali-Forti.

## 71.5 Apêndice: Princípio de Hume

Na Seção 71.1, descrevemos o Princípio de Cantor. Era:

$$|A| = |B| \text{ sse } A \approx B.$$

Isto é muito semelhante ao que hoje se chama *Princípio de Hume*, que diz:

$$\#x\, F(x) = \#x\, G(x) \text{ sse } F \sim G$$

onde '$F \sim G$' abrevia que há tantos $F$ quantos $G$, isto é, os $F$ podem pôr-se em bijeção com os $G$, isto é:

$$\begin{aligned}\exists R(&\forall v \forall y (Rvy \to (Fv \wedge Gy)) \wedge \\ &\forall v (Fv \to \exists! y\, Rvy) \wedge \\ &\forall y (Gy \to \exists! v\, Rvy))\end{aligned}$$

Mas há uma diferença de tipo entre o Princípio de Hume e o Princípio de Cantor. No enunciado do Princípio de Cantor, as variáveis "$A$" e "$B$" são termos de primeira ordem que denotam *conjuntos*. No enunciado do Princípio de Hume, "$F$", "$G$" e "$R$" *não* são termos de primeira ordem; estão em *posição de predicado*. (Talvez denotem *propriedades*.) Assim, o Princípio de Hume pode parafrasear-se em português: o número de $F$s é o número de $G$s sse os $F$s estão em bijeção com os $G$s. Chama-se *Princípio de Hume* porque Hume escreveu o seguinte:

> Quando dois números se combinam de tal modo que a cada unidade de um corresponde sempre uma unidade do outro, dizemos que são iguais. (Hume, 1740, Pt.III Bk.1 §1)

E o Princípio de Hume foi trazido à proeminência matemático-lógica contemporânea por Frege (1884, §63), que citou esta passagem de Hume antes de (em efeito) esboçar (o que chamamos) Princípio de Hume.

Note a semelhança estrutural entre o Princípio de Hume e a Lei Básica V. A formulamos na Seção 65.6 do seguinte modo:

$$\epsilon x\, F(x) = \epsilon x\, G(x) \text{sse } \forall x\, (F(x) \leftrightarrow G(x)).$$

E, neste ponto, alguns comentários e comparações podem ajudar.

Há duas maneiras de entender um princípio como o Princípio de Hume ou a Lei Básica V: *predicativamente* ou *impredicativamente* (recorde Seção 65.3). Na leitura impredicativa da Lei Básica V, para cada $F$, o objeto $\epsilon x\, F(x)$ pertence ao domínio de quantificação usado na própria formulação da Lei Básica V. Do mesmo modo, na leitura impredicativa do Princípio de Hume, para cada $F$, o objeto $\#x\, F(x)$ pertence ao domínio de quantificação usado na formulação do Princípio de Hume. Em contraste, na compreensão *predicativa*, os objetos $\epsilon x\, F(x)$ e $\#x\, F(x)$ seriam entidades de um domínio *diferente*.

Agora, se a Lei Básica V se lê impredicativamente, conduz à inconsistência, via Compreensão ingênua (para pormenores, ver Seção 65.6). Tal como a Compreensão ingênua, pode tornar-se consistente se se lê *predicativamente*. Mas provavelmente não fará tudo o que desejávamos.

O Princípio de Hume, porém, *pode* ser lido de modo consistente impredicativamente. E, assim lido, é bastante poderoso.

Para ilustrar: considere-se o predicado "$x \neq x$", que obviamente nada satisfaz. O Princípio de Hume fornece agora um objeto $\#x(x \neq x)$. Podemos tratá-lo como o número 0. Agora, na compreensão *impredicativa*—mas *só* na impredicativa—esta entidade 0 pertence ao nosso domínio original de quantificação. Logo podemos aplicar sensatamente o Princípio de Hume com o predicado "$x = 0$" para obter um objeto $\#x(x = 0)$. Podemos tratá-lo como o número 1. Além disso, o Princípio de Hume implica que $0 \neq 1$, pois não pode haver bijeção dos objetos não auto-idênticos para os objetos idênticos a

0 (não há dos primeiros, mas há um dos segundos). Agora, de novo impredicativamente, 1 pertence ao domínio original de quantificação. Logo podemos aplicar o Princípio de Hume com o predicado "$(x = 0 \vee x = 1)$" para obter um objeto $\#x(x = 0 \vee x = 1)$. Podemos tratá-lo como o número 2, e mostrar que $0 \neq 2$ e $1 \neq 2$, e assim por diante.

Em suma, tomado impredicativamente, o Princípio de Hume implica que há *infinitamente muitos objetos*. E isto encorajou os *logicistas neo-fregeanos* a tomar o Princípio de Hume como fundação da aritmética.

O próprio Frege, contudo, não tomou o Princípio de Hume como fundação da aritmética. Em vez disso, Frege provou o Princípio de Hume a partir de uma definição explícita: $\#x\, F(x)$ é definido como a extensão do conceito $F \sim \Phi$. Em termos modernos, poder-se-ia tentar render isto como $\#x\, F(x) = \{G : F \sim G\}$; mas isto volta a arrastar-nos para os problemas da Compreensão ingênua.

# Capítulo 72

# Aritmética Cardinal

## 72.1 Definindo as Operações Básicas

Como não precisamos de controlar a ordem, a aritmética cardinal é bastante mais fácil de definir do que a aritmética ordinal. Definiremos adição, multiplicação e exponenciação simultaneamente.

**Definição 72.1.** Quando $\mathfrak{a}$ e $\mathfrak{b}$ são cardinais:

$$\begin{aligned} \mathfrak{a} \oplus \mathfrak{b} &= |\mathfrak{a} \sqcup \mathfrak{b}| \\ \mathfrak{a} \otimes \mathfrak{b} &= |\mathfrak{a} \times \mathfrak{b}| \\ \mathfrak{a}^{\mathfrak{b}} &= \left|{}^{\mathfrak{b}}\mathfrak{a}\right| \end{aligned}$$

onde ${}^{X}Y = \{f : f \text{ é uma função } X \to Y\}$. (É fácil mostrar que ${}^{X}Y$ existe para quaisquer conjuntos $X$ e $Y$; deixamos isto como exercício.)

Pode ajudar explicar esta definição. Quanto à adição: usa-se a noção de soma disjunta, $\sqcup$, tal como definida em Definição 70.1; e é fácil ver que esta definição dá o resultado certo nos casos finitos. Quanto à multiplicação: Proposição 1.27 nos diz que, se $A$ tem $n$ membros e $B$ tem $m$ membros, então $A \times B$ tem $n \cdot m$ membros, pelo que a nossa definição generaliza simplesmente a ideia à multiplicação transfinita. A exponenciação é semelhante: estamos simplesmente a generalizar o pensamento do finito para o transfinito. De fato, sob certos aspectos, a aritmética cardinal transfinita parece muito mais a aritmética "ordinária" do que a aritmética ordinal transfinita:

**Proposição 72.2.** *$\oplus$ e $\otimes$ são comutativas e associativas.*

*Prova.* Para a comutatividade, por Lema 71.3 basta observar que $(\mathfrak{a} \sqcup \mathfrak{b}) \approx (\mathfrak{b} \sqcup \mathfrak{a})$ e $(\mathfrak{a} \times \mathfrak{b}) \approx (\mathfrak{b} \times \mathfrak{a})$. Deixamos a associatividade como exercício. □

**Proposição 72.3.** *$A$ é infinito se e só se $|A| \oplus 1 = 1 \oplus |A| = |A|$.*

*Prova.* Como em Teorema 71.7, a partir de Lema 70.10 e Lema 71.3. □

Isto explica porque precisamos de símbolos distintos para adição/multiplicação ordinal versus cardinal: são operações genuinamente *diferentes*. Este par de resultados mostra que a exponenciação ordinal versus cardinal também são operações distintas. (Recordar que Definição 66.7 implica que $2 = \{0, 1\}$):

**Lema 72.4.** $|\wp(A)| = 2^{|A|}$, *para qualquer* $A$.

*Prova.* Para cada subconjunto $B \subseteq A$, seja $\chi_B \in {}^A2$ dado por:

$$\chi_B(x) = \begin{cases} 1 & \text{se } x \in B \\ 0 & \text{caso contrário.} \end{cases}$$

Seja agora $f(B) = \chi_B$; isto define uma bijeção $f\colon \wp(A) \to {}^A2$. Logo $\wp(A) \approx {}^A2$. Daí $\wp(A) \approx {}^{|A|}2$, pelo que $|\wp(A)| = \left|{}^{|A|}2\right| = 2^{|A|}$. □

Esta prova sucinta subsume essencialmente a discussão em Seção 4.13. Ali, mostramos como "reduzir" a não enumerabilidade de $\wp(\omega)$ à não enumerabilidade do conjunto das sequências binárias infinitas, $\mathbb{B}^\omega$. Na prática, $\mathbb{B}^\omega$ é apenas ${}^\omega 2$; e a prova precedente mostrou que o raciocínio que seguimos na Seção 4.13 continua a valer usando qualquer conjunto $A$ no lugar de $\omega$. O resultado também fornece um fato rápido sobre exponenciação cardinal:

**Corolário 72.5.** $\mathfrak{a} < 2^{\mathfrak{a}}$ *para qualquer cardinal* $\mathfrak{a}$.

*Prova.* Pelo Teorema de Cantor (Teorema 4.24) e Lema 72.4. □

Logo $\omega < 2^\omega$. Mas nota: isto é um resultado sobre exponenciação *cardinal*. Deve contrastar-se com a exponenciação *ordinal*, pois neste último caso $\omega = 2^{(\omega)}$ (ver Seção 70.5).

Enquanto estamos no tema da exponenciação cardinal, podemos também ser um pouco mais precisos sobre a "maneira" pela qual $\mathbb{R}$ é não enumerável.

**Teorema 72.6.** $|\mathbb{R}| = 2^\omega$

*Esboço de prova.* Há muitas maneiras de provar isto. A mais direta é argumentar que $\wp(\omega) \preceq \mathbb{R}$ e $\mathbb{R} \preceq \wp(\omega)$, e depois usar Schröder-Bernstein para inferir que $\mathbb{R} \approx \wp(\omega)$, e Lema 72.4 para inferir que $|\mathbb{R}| = 2^\omega$. Deixamos como exercício (esclarecedor) definir injecções $f\colon \wp(\omega) \to \mathbb{R}$ e $g\colon \mathbb{R} \to \wp(\omega)$. □

## 72.2 Simplificando Adição e Multiplicação

Acontece que a adição e a multiplicação cardinais transfinitas são *extremamente* fáceis. Isto segue do fato de os cardinais serem (certos) ordinais, logo bem ordenados, e poderem ser manipulados de certa forma. Mostrar isto, porém, *não* é tão fácil. Para começar, precisamos de uma definição hábil:

**Definição 72.7.** Definimos uma *ordenação canónica*, $\lhd$, em pares de ordinais, estipulando que $\langle \alpha_1, \alpha_2 \rangle \lhd \langle \beta_1, \beta_2 \rangle$ se e só se se verifica uma das seguintes condições:

1. $\max(\alpha_1, \alpha_2) < \max(\beta_1, \beta_2)$; ou
2. $\max(\alpha_1, \alpha_2) = \max(\beta_1, \beta_2)$ e $\alpha_1 < \beta_1$; ou
3. $\max(\alpha_1, \alpha_2) = \max(\beta_1, \beta_2)$ e $\alpha_1 = \beta_1$ e $\alpha_2 < \beta_2$

**Lema 72.8.** *$\langle \alpha \times \alpha, \lhd \rangle$ é uma boa ordem, para qualquer ordinal $\alpha$.*

*Prova.* Evidentemente $\lhd$ é conexa em $\alpha \times \alpha$. De fato, suponhamos que nem $\langle \alpha_1, \alpha_2 \rangle$ nem $\langle \beta_1, \beta_2 \rangle$ é menor do que a outra no sentido de $\lhd$. Então $\max(\alpha_1, \alpha_2) = \max(\beta_1, \beta_2)$ e $\alpha_1 = \beta_1$ e $\alpha_2 = \beta_2$, pelo que $\langle \alpha_1, \alpha_2 \rangle = \langle \beta_1, \beta_2 \rangle$.

Para mostrar que é boa ordem, seja $X \subseteq \alpha \times \alpha$ não vazio. Como $\alpha$ é um ordinal, algum $\delta$ é o menor membro de $\{\max(\gamma_1, \gamma_2) : \langle \gamma_1, \gamma_2 \rangle \in X\}$. Descartemos agora todos os pares de $\{\langle \gamma_1, \gamma_2 \rangle \in X : \max(\gamma_1, \gamma_2) = \delta\}$ exceto os de primeira coordenada mínima; entre estes, o par de segunda coordenada mínima é o elemento $\lhd$-mínimo de $X$. □

Segue-se uma observação mínima, mas simples:

**Proposição 72.9.** *Se $\alpha \approx \beta$, então $\alpha \times \alpha \approx \beta \times \beta$.*

*Prova.* Basta deixar que $f : \alpha \to \beta$ induza $\langle \gamma_1, \gamma_2 \rangle \mapsto \langle f(\gamma_1), f(\gamma_2) \rangle$. □

E agora aplicaremos tudo isto para provar um lema crucial:

**Lema 72.10.** *$\alpha \approx \alpha \times \alpha$, para qualquer ordinal infinito $\alpha$*

*Prova.* Por redução ao absurdo, seja $\alpha$ o menor ordinal infinito para o qual isto falha. Proposição 4.12 mostra que $\omega \approx \omega \times \omega$, logo $\omega \in \alpha$. Além disso, $\alpha$ é um cardinal: suponhamos o contrário, por redução ao absurdo; então $|\alpha| \in \alpha$, pelo que $|\alpha| \approx |\alpha| \times |\alpha|$, por hipótese; e $|\alpha| \approx \alpha$ por definição; logo $\alpha \approx \alpha \times \alpha$ por Proposição 72.9.

Ora, para cada $\langle \gamma_1, \gamma_2 \rangle \in \alpha \times \alpha$, consideremos o segmento:

$$\mathrm{Seg}(\gamma_1, \gamma_2) = \{\langle \delta_1, \delta_2 \rangle \in \alpha \times \alpha : \langle \delta_1, \delta_2 \rangle \lhd \langle \gamma_1, \gamma_2 \rangle\}$$

Seja $\gamma = \max(\gamma_1, \gamma_2)$; note-se que $\langle \gamma_1, \gamma_2\rangle \lhd \langle \gamma+1, \gamma+1\rangle$. Assim, quando $\gamma$ é infinito, observe-se:

$$\begin{aligned}\operatorname{Seg}(\gamma_1, \gamma_2) &\preceq ((\gamma+1)\cdot(\gamma+1))\\ &\approx (\gamma\cdot\gamma), \text{ por Lema 70.10 e Proposição 72.9}\\ &\approx \gamma, \text{ pela hipótese de indução}\\ &\prec \alpha, \text{ pois } \alpha \text{ é um cardinal}\end{aligned}$$

Logo $\operatorname{ord}(\alpha\times\alpha, \lhd) \leq \alpha$, e portanto $\alpha\times\alpha \preceq \alpha$. Como obviamente $\alpha \preceq \alpha\times\alpha$, o resultado segue por Schröder-Bernstein. □

Finalmente, chegamos ao nosso resultado simplificador:

**Teorema 72.11.** *Se $\mathfrak{a}, \mathfrak{b}$ são cardinais infinitos, então:*

$$\mathfrak{a}\otimes\mathfrak{b} = \mathfrak{a}\oplus\mathfrak{b} = \max(\mathfrak{a},\mathfrak{b}).$$

*Prova.* Sem perda de generalidade, suponhamos $\mathfrak{a} = \max(\mathfrak{a},\mathfrak{b})$. Então, invocando Lema 72.10, $\mathfrak{a}\otimes\mathfrak{a} = \mathfrak{a} \leq \mathfrak{a}\oplus\mathfrak{b} \leq \mathfrak{a}\oplus\mathfrak{a} \leq \mathfrak{a}\otimes\mathfrak{a}$. □

Do mesmo modo, se $\mathfrak{a}$ é infinito, uma união de cardinalidade $\mathfrak{a}$ de conjuntos de cardinalidade $\leq \mathfrak{a}$ tem cardinalidade $\leq \mathfrak{a}$:

**Proposição 72.12.** *Seja $\mathfrak{a}$ um cardinal infinito. Para cada ordinal $\beta\in\mathfrak{a}$, seja $X_\beta$ um conjunto com $|X_\beta| \leq \mathfrak{a}$. Então $\left|\bigcup_{\beta\in\mathfrak{a}} X_\beta\right| \leq \mathfrak{a}$.*

*Prova.* Para cada $\beta\in\mathfrak{a}$, fixe uma injeção $f_\beta\colon X_\beta \to \mathfrak{a}$.[1] Defina uma injeção $g\colon \bigcup_{\beta\in\mathfrak{a}} X_\beta \to \mathfrak{a}\times\mathfrak{a}$ por $g(v) = \langle\beta, f_\beta(v)\rangle$, onde $v\in X_\beta$ e $v\notin X_\gamma$ para qualquer $\gamma\in\beta$. Ora, $\bigcup_{\beta\in\mathfrak{a}} X_\beta \preceq \mathfrak{a}\times\mathfrak{a} \approx \mathfrak{a}$ por Teorema 72.11. □

## 72.3 Algumas Simplificações com Exponenciação Cardinal

Embora definir $\lhd$ fosse um pouco trabalhoso, o resultado é um teorema útil sobre adição e multiplicação cardinais, Teorema 72.11. A exponenciação transfinita, porém, não se simplifica tão diretamente. Para explicar por que, começamos por um resultado que prolonga um padrão familiar do caso finitário (embora a sua prova esteja a um nível elevado de abstração):

**Proposição 72.13.** $\mathfrak{a}^{\mathfrak{b}\oplus\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}}\otimes\mathfrak{a}^{\mathfrak{c}}$ *e* $(\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}\otimes\mathfrak{c}}$, *para quaisquer cardinais* $\mathfrak{a},\mathfrak{b},\mathfrak{c}$.

*Prova.* Para a primeira afirmação, considere-se uma função $f\colon (\mathfrak{b}\sqcup\mathfrak{c}) \to \mathfrak{a}$. Ora, "parta-se" isto, definindo $f_{\mathfrak{b}}(\beta) = f(\beta, 0)$ para cada $\beta\in\mathfrak{b}$, e $f_{\mathfrak{c}}(\gamma) = f(\gamma, 1)$ para cada $\gamma\in\mathfrak{c}$. A aplicação $f \mapsto (f_{\mathfrak{b}}\times f_{\mathfrak{c}})$ é uma bijeção ${}^{\mathfrak{b}\sqcup\mathfrak{c}}\mathfrak{a} \to ({}^{\mathfrak{b}}\mathfrak{a}\times{}^{\mathfrak{c}}\mathfrak{a})$.

[1] Como são estes "fixos"? Ver Seção 73.5.

Para a segunda afirmação, considere-se uma função $f\colon \mathfrak{c} \to ({}^{\mathfrak{b}}\mathfrak{a})$; assim, para cada $\gamma \in \mathfrak{c}$ temos alguma função $f(\gamma)\colon \mathfrak{b} \to \mathfrak{a}$. Ora, defina-se $f^*(\beta,\gamma) = (f(\gamma))(\beta)$ para cada $\langle \beta,\gamma\rangle \in \mathfrak{b}\times\mathfrak{c}$. A aplicação $f \mapsto f^*$ é uma bijeção ${}^{\mathfrak{c}}({}^{\mathfrak{b}}\mathfrak{a}) \to {}^{\mathfrak{b}\otimes\mathfrak{c}}\mathfrak{a}$. □

O que gostaríamos *mesmo* era de uma maneira fácil de calcular $\mathfrak{a}^{\mathfrak{b}}$ quando tratamos de cardinais infinitos. Eis um passo útil nessa direção:

**Proposição 72.14.** *Se* $2 \leq \mathfrak{a} \leq \mathfrak{b}$ *e* $\mathfrak{b}$ *é infinito, então* $\mathfrak{a}^{\mathfrak{b}} = 2^{\mathfrak{b}}$

*Prova.*

$$\begin{aligned} 2^{\mathfrak{b}} &\leq \mathfrak{a}^{\mathfrak{b}}, \text{ pois } 2 \leq \mathfrak{a} \\ &\leq (2^{\mathfrak{a}})^{\mathfrak{b}}, \text{ por Lema 72.4} \\ &= 2^{\mathfrak{a}\otimes\mathfrak{b}}, \text{ por Proposição 72.13} \\ &= 2^{\mathfrak{b}}, \text{ por Teorema 72.11} \end{aligned}$$ □

Não devemos esperar poder simplificar mais além disto, pois $\mathfrak{b} < 2^{\mathfrak{b}}$ por Lema 72.4. Contudo, isto não nos diz o que afirmar sobre $\mathfrak{a}^{\mathfrak{b}}$ quando $\mathfrak{b} < \mathfrak{a}$. Naturalmente, se $\mathfrak{b}$ é *finito*, sabemos o que fazer.

**Proposição 72.15.** *Se* $\mathfrak{a}$ *é infinito e* $n \in \omega$*, então* $\mathfrak{a}^n = \mathfrak{a}$

*Prova.* $\mathfrak{a}^n = \mathfrak{a}\otimes\mathfrak{a}\otimes\ldots\otimes\mathfrak{a} = \mathfrak{a}$, por Teorema 72.11. □

Adicionalmente, nalguns outros casos, podemos controlar o tamanho de $\mathfrak{a}^{\mathfrak{b}}$:

**Proposição 72.16.** *Se* $2 \leq \mathfrak{b} < \mathfrak{a} \leq 2^{\mathfrak{b}}$ *e* $\mathfrak{b}$ *é infinito, então* $\mathfrak{a}^{\mathfrak{b}} = 2^{\mathfrak{b}}$

*Prova.* $2^{\mathfrak{b}} \leq \mathfrak{a}^{\mathfrak{b}} \leq (2^{\mathfrak{b}})^{\mathfrak{b}} = 2^{\mathfrak{b}\otimes\mathfrak{b}} = 2^{\mathfrak{b}}$, raciocinando como na Proposição 72.14.□

Para além deste ponto, as coisas tornam-se bastante mais subtis.

## 72.4 A Hipótese do Contínuo

O resultado anterior sugere (corretamente) que a exponenciação cardinal seria bastante *fácil*, se os cardinais infinitos estivessem garantidos a "comportar-se de forma simples" com potências de 2, isto é, (por Lema 72.4) com a operação de tomar conjuntos potência. Mas não podemos supor que os cardinais infinitos *se comportem* de forma simples com os conjuntos potência.

Começando a desdobrar isto, introduzimos uma notação conveniente.

**Definição 72.17.** Onde $\mathfrak{a}^{\oplus}$ é o menor cardinal estritamente maior do que $\mathfrak{a}$, definimos duas sequências infinitas:

$$\begin{aligned} \aleph_0 &= \omega & \beth_0 &= \omega \\ \aleph_{\alpha+1} &= (\aleph_\alpha)^{\oplus} & \beth_{\alpha+1} &= 2^{\beth_\alpha} \\ \aleph_\alpha &= \bigcup_{\beta<\alpha} \aleph_\beta & \beth_\alpha &= \bigcup_{\beta<\alpha} \beth_\beta \end{aligned} \qquad \text{quando } \alpha \text{ é um ordinal limite.}$$

A definição de $\mathfrak{a}^{\oplus}$ faz sentido, pois Teorema 71.14 nos diz que, para cada cardinal $\mathfrak{a}$, existe algum cardinal maior do que $\mathfrak{a}$, e a Indução Transfinita garante que existe um cardinal *mínimo* maior do que $\mathfrak{a}$. O resto da definição é fornecido pela recursão transfinita.

Cantor introduziu esta notação "$\aleph$"; trata-se do *alef*, a primeira letra do alfabeto hebraico e a primeira letra da palavra hebraica para "infinito". Peirce introduziu a notação "$\beth$"; trata-se do *beth*, a segunda letra do alfabeto hebraico.[2] Estas notações fornecem-nos cardinais infinitos.

**Proposição 72.18.** *$\aleph_\alpha$ e $\beth_\alpha$ são cardinais, para todo o ordinal $\alpha$.*

*Prova.* Ambos os resultados valem por uma indução transfinita simples. $\aleph_0 = \beth_0 = \omega$ é um cardinal por Corolário 71.9. Supondo que $\aleph_\alpha$ e $\beth_\alpha$ são ambos cardinais, $\aleph_{\alpha+1}$ e $\beth_{\alpha+1}$ estão explicitamente definidos como cardinais. E a união de um conjunto de cardinais é um cardinal, por Proposição 71.13. □

Além disso, todo o cardinal infinito é um $\aleph$:

**Proposição 72.19.** *Se $\mathfrak{a}$ é um cardinal infinito, então $\mathfrak{a} = \aleph_\gamma$ para um certo $\gamma$ único.*

*Prova.* Por indução transfinita nos cardinais. Para a indução, suponhamos que se $\mathfrak{b} < \mathfrak{a}$ então $\mathfrak{b} = \aleph_{\gamma_\mathfrak{b}}$. Se $\mathfrak{a} = \mathfrak{b}^{\oplus}$ para algum $\mathfrak{b}$, então $\mathfrak{a} = (\aleph_{\gamma_\mathfrak{b}})^{\oplus} = \aleph_{\gamma_\mathfrak{b}+1}$. Se $\mathfrak{a}$ não é o sucessor de nenhum cardinal, então, por serem os cardinais ordinais, $\mathfrak{a} = \bigcup_{\mathfrak{b}<\mathfrak{a}} \mathfrak{b} = \bigcup_{\mathfrak{b}<\mathfrak{a}} \aleph_{\gamma_\mathfrak{b}}$, logo $\mathfrak{a} = \aleph_\gamma$ onde $\gamma = \bigcup_{\mathfrak{b}<\mathfrak{a}} \gamma_\mathfrak{b}$. □

Como todo o cardinal infinito é um $\aleph$, surge naturalmente a pergunta: será que todo o cardinal infinito é um $\beth$? Certamente que, se isso *se verificasse*, os cardinais infinitos "comportar-se-iam de forma simples" com a operação de tomar conjuntos potência. De fato, teríamos o seguinte:

> *Hipótese Generalizada do Contínuo* (HGC). $\aleph_\alpha = \beth_\alpha$, para todo o $\alpha$.

[2] Peirce usou esta notação numa carta a Cantor de dezembro de 1900. Infelizmente, Peirce também apresentou ali um mau argumento de que $\beth_\alpha$ não existe para $\alpha \geq \omega$.

Além disso, se a HGC valesse, poderíamos simplificar bastante a exponenciação cardinal. Em particular, poderíamos mostrar que, quando $\mathfrak{b} < \mathfrak{a}$, o valor de $\mathfrak{a}^{\mathfrak{b}}$ fica encerrado entre $\mathfrak{a} \leq \mathfrak{a}^{\mathfrak{b}} \leq \mathfrak{a}^{\oplus}$. Poderíamos então dar condições precisas que determinam qual das duas possibilidades se verifica (isto é, se $\mathfrak{a} = \mathfrak{a}^{\mathfrak{b}}$ ou $\mathfrak{a}^{\mathfrak{b}} = \mathfrak{a}^{\oplus}$).[3]

Mas a HGC é uma *hipótese*, não um *teorema*. De fato, Gödel (1938) provou que, se **ZFC** for consistente, então também o é **ZFC** + HGC. Mas mais tarde verificou-se que podemos acrescentar igualmente ¬HGC a **ZFC**. De fato, considere-se a *instância* não trivial mais simples da HGC, nomeadamente:

*Hipótese do Contínuo* (HC). $\aleph_1 = \beth_1$.

Cohen (1963) provou que, se **ZFC** for consistente, então também o é **ZFC** + ¬HC. Logo a Hipótese do Contínuo é independente de **ZFC**.

A Hipótese do Contínuo chama-se assim porque "o contínuo" é outro nome para a reta real, $\mathbb{R}$. Teorema 72.6 nos diz que $|\mathbb{R}| = \beth_1$. Assim, a Hipótese do Contínuo afirma que não há cardinal entre a cardinalidade dos números naturais, $\aleph_0 = \beth_0$, e a cardinalidade do contínuo, $\beth_1$.

Dada a *independência* da (H)HC relativamente a **ZFC**, o que devemos dizer sobre a sua *verdade*? Há *muito* a dizer. De fato, muito trabalho recente e fecundo em teoria dos conjuntos tem sido dedicado a estas questões. Mas dois pontos rápidos valem certamente a pena enfatizar.

Primeiro: não se segue *imediatamente* destes resultados formais de independência que a HGC ou a HC sejam *indeterminadas* no valor de verdade. Afinal, talvez bastem mais axiomas, que nos pareçam naturais, para decidir a questão num sentido ou noutro. O próprio Gödel sugeriu que essa era a resposta adequada.

Segundo: a independência da HC relativamente a **ZFC** é certamente *notável*, mas não é *inacreditável* (no sentido literal). O ponto é simplesmente que, para tudo o que **ZFC** nos diz, passar de um cardinal ao seu sucessor pode envolver uma ferramenta menos direta do que simplesmente tomar conjuntos potência.

Feitas estas duas observações, quem quiser saber mais terá de recorrer aos vários filósofos e matemáticos com cavalos na corrida.[4]

## 72.5 Pontos Fixos de $\aleph$

No Capítulo 68, sugerimos que o Esquema de Substituição carece de justificação, pois força a hierarquia a ser bastante alta. Tendo feito alguma aritmética cardinal, podemos dar uma pequena ilustração da altura da hierarquia.

[3] A condição é ditada pela *cofinalidade*.

[4] Embora possa querer começar por ler Potter (2004, §15.6).

Evidentemente $0 < \aleph_0$, e $1 < \aleph_1$, e $2 < \aleph_2 \ldots$ e, de fato, a diferença de tamanho só fica *maior* a cada passo. Assim, é tentador conjecturar que $\kappa < \aleph_\kappa$ para todo o ordinal $\kappa$.

Mas esta conjectura é *falsa*, em **ZFC**. De fato, podemos provar que existem *pontos fixos de* $\aleph$, isto é, cardinais $\kappa$ tais que $\kappa = \aleph_\kappa$.

**Proposição 72.20.** *Existe um ponto fixo de* $\aleph$.

*Prova.* Por recursão, defina-se:

$$\begin{aligned} \kappa_0 &= 0 \\ \kappa_{n+1} &= \aleph_{\kappa_n} \\ \kappa &= \bigcup_{n<\omega} \kappa_n \end{aligned}$$

Ora, $\kappa$ é um cardinal por Proposição 71.13. Mas então:

$$\kappa = \bigcup_{n<\omega} \kappa_{n+1} = \bigcup_{n<\omega} \aleph_{\kappa_n} = \bigcup_{\alpha<\kappa} \aleph_\alpha = \aleph_\kappa$$

□

Boolos escreveu um artigo sobre precisamente o ponto fixo de $\aleph$ que acabamos de construir. Depois de notar a existência de $\kappa$, no início do artigo, disse:

> [$\kappa$ é] um número *bastante grande*, aos olhos de quem não teve contato prévio com a teoria dos conjuntos, tão grande, me parece, que põe em causa a verdade de qualquer teoria que, entre as suas afirmações, inclua a de que existem pelo menos $\kappa$ objetos. (Boolos, 2000, p. 257)

E concluiu o artigo perguntando:

> [será que] suspeitamos que, seja qual for o começo da história, quando chegamos tão longe as rodas giram no vazio e já não estamos a ouvir uma descrição de coisa alguma que seja o caso? (Boolos, 2000, p. 268)

Se, de fato, ultrapassamos "qualquer coisa que seja o caso", então devemos apontar o dedo da culpa diretamente ao Esquema de Substituição. Pois é este axioma que permite a nossa prova funcionar. Nesse caso, supõe-se, Boolos teria de rever a afirmação que fizera, décadas antes, de que a Substituição não tem consequências "indesejáveis" (ver Seção 69.3).

Mas será a existência de $\kappa$ assim tão má? Pode ajudar, aqui, considerar o *paradoxo de Tristram Shandy* de Russell. Tristram Shandy documenta a sua vida no diário, mas demora um ano a registrar um único dia. A cada ano que passa, Tristram fica cada vez mais atrasado: passado um ano, só registrou um dia, e viveu 364 dias por registrar; passados dois anos, só registrou dois dias, e viveu

728 dias por registrar; passados três anos, só registrou três dias, e viveu 1092 dias por registrar ...[5] Ainda assim, se Tristram é *imortal*, conseguirá registrar todos os dias, pois registrará o $n$-ésimo dia no $n$-ésimo ano da sua vida. E assim, "no fim dos tempos", Tristram terá um diário completo.

Porque é que isto difere tanto da ideia de que $\alpha$ é menor do que $\aleph_\alpha$—e, de fato, cada vez mais, desesperadamente menor—até $\kappa$, onde nos "apanhamos" e $\kappa = \aleph_\kappa$?

Deixando isto de lado, e supondo que aceitamos **ZFC**, fechemos com um pouco mais de diversão sobre construções de pontos fixos. Os três resultados seguintes estabelecem, intuitivamente, que existe um ponto (não trivial) em que a hierarquia é tão larga como alta:

**Proposição 72.21.** *Existe um ponto fixo de $\beth$, isto é, um $\kappa$ tal que $\kappa = \beth_\kappa$.*

*Prova.* Como na Proposição 72.20, usando "$\beth$" no lugar de "$\aleph$". □

**Proposição 72.22.** *$|V_{\omega+\alpha}| = \beth_\alpha$. Se $\omega \cdot \omega \leq \alpha$, então $|V_\alpha| = \beth_\alpha$.*

*Prova.* A primeira afirmação vale por uma indução transfinita simples. A segunda segue-se, pois se $\omega \cdot \omega \leq \alpha$ então $\omega + \alpha = \alpha$. Para o estabelecer, usamos fatos sobre aritmética ordinal de Capítulo 70. Note-se primeiro que $\omega \cdot \omega = \omega \cdot (1 + \omega) = (\omega \cdot 1) + (\omega \cdot \omega) = \omega + (\omega \cdot \omega)$. Ora, se $\omega \cdot \omega \leq \alpha$, isto é, $\alpha = (\omega \cdot \omega) + \beta$ para algum $\beta$, então $\omega + \alpha = \omega + ((\omega \cdot \omega) + \beta) = (\omega + (\omega \cdot \omega)) + \beta = (\omega \cdot \omega) + \beta = \alpha$. □

**Corolário 72.23.** *Existe um $\kappa$ tal que $|V_\kappa| = \kappa$.*

*Prova.* Seja $\kappa$ um ponto fixo de $\beth$, dado por Proposição 72.21. Claramente $\omega \cdot \omega < \kappa$. Logo $|V_\kappa| = \beth_\kappa = \kappa$ por Proposição 72.22. □

Há tantos estágios abaixo de $V_\kappa$ quantos membros de $V_\kappa$. Intuitivamente, então, $V_\kappa$ é tão largo como alto. Isto é muito à maneira de Tristram Shandy: passamos de um estágio ao seguinte tomando *conjuntos potência*, tornando a hierarquia *muito* maior a cada passo. Mas "no fim", isto é, no estágio $\kappa$, a largura da hierarquia alcança a altura.

Alguém pode perguntar: *Com que frequência a largura da hierarquia coincide com a altura?* A resposta é: *Tantas vezes quantos os ordinais.* Mas isto precisa de uma pequena explicação.

Definimos um termo $\tau$ do seguinte modo. Para qualquer $A$, seja:

$$\begin{aligned} \tau_0(A) &= |A| \\ \tau_{n+1}(A) &= \beth_{\tau_n(A)} \\ \tau(A) &= \bigcup_{n<\omega} \tau_n(A) \end{aligned}$$

[5] Ignorando anos bissextos.

Como na Proposição 72.21, $\tau(A)$ é um ponto fixo de $\beth$ para qualquer $A$, e trivialmente $|A| < \tau(A)$. Considere-se então esta definição recursiva:

$$\begin{aligned} W_0 &= 0 \\ W_{\alpha+1} &= \tau(W_\alpha) \\ W_\alpha &= \bigcup_{\beta<\alpha} W_\beta, \text{ quando } \alpha \text{ é limite} \end{aligned}$$

A construção está definida para todos os ordinais. Intuitivamente, então, $W$ é "uma injeção" dos ordinais nos pontos fixos de $\beth$. E, exatamente como antes, $V_{W_\alpha}$ é tão largo como alto, para qualquer $\alpha$.

## Problemas

**Problema 72.1.** Prove em $\mathbf{Z}^-$ que ${}^X Y$ existe para quaisquer conjuntos $X$ e $Y$. Trabalhando em **ZF**, calcule $\text{posto}({}^X Y)$ a partir de $\text{posto}(X)$ e $\text{posto}(Y)$, à maneira de Lema 70.9.

**Problema 72.2.** Prove que $\oplus$ e $\otimes$ são associativas.

**Problema 72.3.** Complete a prova de Teorema 72.6, mostrando que $\wp(\omega) \preceq \mathbb{R}$ e $\mathbb{R} \preceq \wp(\omega)$.

# Capítulo 73

# Escolha

## 73.1 Introdução

Em Capítulos 71 a 72, desenvolvemos uma teoria de cardinais tratando os cardinais como ordinais. Essa abordagem depende do Axioma da Boa Ordenação. Verifica-se que a Boa Ordenação é equivalente a outro princípio—o Axioma da Escolha—e houve discussão filosófica séria sobre a sua aceitabilidade. As questões deste capítulo são: Como é que o Axioma é usado, e pode ser justificado?

## 73.2 O Truque de Tarski–Scott

Na Definição 71.1, definimos cardinais como ordinais. Para isso, assumimos o Axioma da Boa Ordenação. Fizemo-lo apenas porque é o "padrão da indústria".

Antes de discutir questões filosóficas em torno da Boa Ordenação, importa deixar claro que *podemos* afastar-nos desse padrão e desenvolver uma teoria de cardinais *sem* assumir a Boa Ordenação. Continuamos a poder usar as definições de $A \approx B$, $A \preceq B$ e $A \prec B$, tal como apareceram no Capítulo 4. Só precisamos de uma nova noção de *cardinal*.

Uma ideia ingênua seria tentar definir a cardinalidade de $A$ assim:

$$\{x : A \approx x\}.$$

Talvez queira comparar isto com a definição fregeana de $\#xFx$, esboçada no final de Seção 71.5. E, pelas razões que ali adumbramos, esta definição falha. Qualquer conjunto singular é equipotente com $\{\emptyset\}$. Mas novos singulares são formados em cada estágio sucessor da hierarquia (basta considerar o singular do estágio anterior). Logo $\{x : A \approx x\}$ não existe, pois não pode ter posto.

Para contornar o problema, usamos um truque devido a Tarski e Scott:[1]

[1] Lembrete: todas as fórmulas podem ter parâmetros (salvo indicação em contrário).

**Definição 73.1 (Tarski–Scott).** Para qualquer fórmula $\varphi(x)$, seja $[x : \varphi(x)]$ o conjunto de todos os $x$, de posto mínimo possível, tais que $\varphi(x)$ (ou $\varnothing$, se não houver $\varphi$s).

Devemos verificar que esta definição é legítima. Trabalhando em **ZF**, Teorema 68.13 garante que $\operatorname{posto}(x)$ existe para todo o $x$. Agora, se houver entidades que satisfazem $\varphi$, podemos deixar $\alpha$ ser o posto mínimo tal que $(\exists x \subseteq V_\alpha)\varphi(x)$, isto é, $(\forall \beta \in \alpha)(\forall x \subseteq V_\beta)\neg\varphi(x)$. Podemos então definir $[x : \varphi(x)]$ por Separação como $\{x \in V_{\alpha+1} : \varphi(x)\}$.

Tendo justificado o truque de Tarski–Scott, podemos usá-lo para definir uma noção de cardinalidade:

**Definição 73.2.** A TS-cardinalidade de $A$ é $\operatorname{tsc}(A) = [x : A \approx x]$.

A definição de TS-cardinal não usa a Boa Ordenação. Mas, mesmo sem esse Axioma, podemos mostrar que os TS-*cardinais* se comportam de modo semelhante aos *cardinais* tal como definidos na Definição 71.1. Por exemplo, se reformularmos Lema 71.3 e Lema 72.4 em termos de TS-cardinais, as provas funcionam em **ZF**, sem assumir a Boa Ordenação.

Enquanto estamos no assunto, vale a pena notar que também podemos desenvolver uma teoria de ordinais usando o truque de Tarski–Scott. Onde $\langle A, < \rangle$ é uma boa ordenação, seja $\operatorname{tso}(A, <) = [\langle X, R\rangle : \langle A, <\rangle \cong \langle X, R\rangle]$. Para mais sobre este tratamento de cardinais e ordinais, ver Potter (2004, chs. 9–12).

## 73.3 Comparabilidade e Lema de Hartogs

Isto é o lado positivo. Eis o lado negativo. Sem Escolha, as coisas ficam *complicadas*. Para ver por que, eis um belo resultado devido a Hartogs (1915):

**Lema 73.3 (*em* ZF).** *Para qualquer conjunto $A$, existe um ordinal $\alpha$ tal que $\alpha \not\preccurlyeq A$*

*Prova.* Se $B \subseteq A$ e $R \subseteq B^2$, então $\langle B, R\rangle \subseteq V_{\operatorname{posto}(A)+4}$ por Lema 70.9. Logo, usando Separação, considere-se:

$$C = \{\langle B, R\rangle \in V_{\operatorname{posto}(A)+5} : B \subseteq A \text{ e } \langle B, R\rangle \text{ é uma boa ordenação}\}$$

Usando Substituição e Teorema 67.26, forme-se o conjunto:

$$\alpha = \{\operatorname{ord}(B, R) : \langle B, R\rangle \in C\}.$$

Por Corolário 67.19, $\alpha$ é um ordinal, pois é um conjunto transitivo de ordinais. De fato, se $\gamma \in \beta \in \alpha$, então $\beta = \operatorname{ord}(B, R)$ para algum $B \subseteq R$, donde $\gamma = \operatorname{ord}(B_b, R_b)$ para algum $b \in B$ por Lema 67.10, logo $\gamma \in \alpha$.

Por redução ao absurdo, suponhamos que existe uma injeção $f : \alpha \to A$. Então, onde:

$$B = \mathrm{Im}(f)$$
$$R = \{\langle f(\alpha), f(\beta)\rangle \in A \times A : \alpha \in \beta\}.$$

Claramente $\alpha = \mathrm{ord}(B, R)$ e $\langle B, R\rangle \in C$. Logo $\alpha \in \alpha$, o que é contradição. □

Isto implica um resultado profundo:

**Teorema 73.4 (*em* ZF).** *As afirmações seguintes são equivalentes:*

1. *O Axioma da Boa Ordenação*
2. *Ou $A \preceq B$ ou $B \preceq A$, para quaisquer conjuntos $A$ e $B$*

*Prova.* *(1) ⇒ (2).* Fixem-se $A$ e $B$. Invocando (1), existem boas ordenações $\langle A, R\rangle$ e $\langle B, S\rangle$. Invocando Teorema 67.26, sejam $f : \alpha \to \langle A, R\rangle$ e $g : \beta \to \langle B, S\rangle$ isomorfismos. Por Proposição 67.22, ou $\alpha \subseteq \beta$ ou $\beta \subseteq \alpha$. Se $\alpha \subseteq \beta$, então $g \circ f^{-1} : A \to B$ é uma injeção, logo $A \preceq B$; analogamente, se $\beta \subseteq \alpha$ então $B \preceq A$.

*(2) ⇒ (1).* Fixe-se $A$; por Lema 73.3 existe algum ordinal $\beta$ tal que $\beta \not\preceq A$. Invocando (2), temos $A \preceq \beta$. Logo existe alguma injeção $f : A \to \beta$, e podemos usar esta injecção para bem ordenar os elementos de $A$, definindo uma ordem $\{\langle a, b\rangle \in A \times A : f(a) \in f(b)\}$. □

Como consequência imediata: se a Boa Ordenação falha, então alguns conjuntos são *literalmente incomparáveis* quanto ao tamanho. Assim, se a Boa Ordenação falha, a aritmética cardinal transfinita ficará complicada. Por exemplo, teremos de abandonar a ideia de que, se $A$ e $B$ são infinitos, então $A \sqcup B \approx A \times B \approx M$, onde $M$ é o maior de $A$ e $B$ (ver Teorema 72.11). O problema é simples: se não podemos *comparar* o tamanho de $A$ e $B$, então não faz sentido perguntar qual é o maior.

## 73.4 O Problema da Boa Ordenação

Evidentemente que muito depende de aceitarmos ou não a Boa Ordenação. Mas a discussão deste princípio tendeu a concentrar-se num equivalente, o Axioma da Escolha. Voltemos então a atenção para esse axioma (e provemos a equivalência).

Em 1883, Cantor exprimiu o seu apoio ao Axioma da Boa Ordenação, chamando-lhe "uma lei do pensamento que me parece fundamental, rica nas suas consequências e particularmente notável pela sua generalidade" (citado em Potter 2004, p. 243). Mas Cantor acabou por convencer-se de que o "Axioma" precisava de prova. A comunidade matemática também.

O problema foi "resolvido" por Zermelo em 1904. Para explicar a solução, precisamos de algumas definições.

**Definição 73.5.** Uma função $f$ é uma *função de escolha* sse $f(x) \in x$ para todo o $x \in \mathrm{dom}(f)$. Dizemos que $f$ é uma *função de escolha para* $A$ sse $f$ é uma função de escolha com $\mathrm{dom}(f) = A \setminus \{\emptyset\}$.

Intuitivamente, para cada conjunto (não vazio) $x \in A$, uma função de escolha para $A$ *escolhe* um elemento particular, $f(x)$, de $x$. O Axioma da Escolha é então:

**Escolha (Escolha).** Todo o conjunto tem uma função de escolha.

Zermelo mostrou que a Escolha implica a boa ordenação, e vice-versa:

**Teorema 73.6 (em ZF).** *A Boa Ordenação e a Escolha são equivalentes.*

*Prova. Da esquerda para a direita.* Seja $A$ um conjunto de conjuntos. Então $\bigcup A$ existe pelo Axioma da União, e logo, pela Boa Ordenação, existe alguma relação $<$ que bem ordena $\bigcup A$. Seja agora $f(x) =$ o membro $<$-mínimo de $x$. Isto é uma função de escolha para $A$.

*Da direita para a esquerda.* Fixe-se $A$. Pela Escolha, existe uma função de escolha, $f$, para $\wp(A) \setminus \{\emptyset\}$. Usando Recursão Transfinita, defina-se uma função:

$$g(0) = f(A)$$
$$g(\alpha) = \begin{cases} \text{parar!} & \text{se } A = g[\alpha] \\ f(A \setminus g[\alpha]) & \text{caso contrário} \end{cases}$$

A indicação "parar!" é apenas uma abreviatura para o que seria de outro modo uma definição mais longa. Ou seja, quando $A = g[\alpha]$ pela primeira vez, seja $g(\delta) = A$ para todo o $\delta \leq \alpha$. Agora, em primeiro lugar, só podemos ter a certeza de que isto define um *termo* (ver as observações após Teorema 68.4); mas mostraremos que de fato temos uma função.

Como $f$ é função de escolha, para cada $\alpha$ (quando definido) temos $g(\alpha) = f(A \setminus g[\alpha]) \in A \setminus g[\alpha]$; isto é, $g(\alpha) \notin g[\alpha]$. Logo, se $g(\alpha) = g(\beta)$ então $g(\beta) \notin g[\alpha]$, isto é, $\beta \notin \alpha$, e analogamente $\alpha \notin \beta$. Logo $\alpha = \beta$, por Tricotomia. Assim, $g$ é injetiva.

Observe-se a seguir que de fato paramos!, isto é, que existe algum ordinal mínimo $\alpha$ tal que $A = g[\alpha]$. De fato, suponhamos o contrário; então, como $g$ é injetiva, teríamos $\alpha \prec \wp(A) \setminus \{\emptyset\}$ para todo o ordinal $\alpha$, contradizendo Lema 73.3. Daí também $\mathrm{Im}(g) = A$.

Reunindo estes fatos, $g$ é uma bijeção de algum ordinal para $A$. Agora, $g$ pode ser usada para bem ordenar $A$. □

Assim, a Boa Ordenação e a Escolha estão de pé ou caem juntas. Mas a questão permanece: estão de pé ou caem?

## 73.5 Escolha Enumerável

É fácil provar, sem usar Escolha/Boa Ordenação, que:

**Lema 73.7 (em $\mathbf{Z}^-$).** *Todo o conjunto finito tem uma função de escolha.*

*Prova.* Seja $a = \{b_1, \ldots, b_n\}$. Suponhamos, por simplicidade, que cada $b_i \neq \emptyset$. Logo existem objetos $c_1, \ldots, c_n$ tais que $c_1 \in b_1, \ldots, c_n \in b_n$. Agora, por Proposição 66.5, o conjunto $\{\langle b_1, c_1\rangle, \ldots, \langle b_n, c_n\rangle\}$ existe; e isto é uma função de escolha para $a$. □

Mas a situação complica-se logo que consideramos conjuntos infinitos. Por exemplo, considere-se esta extensão "mínima" do resultado acima:

> *Escolha Enumerável.* Todo o conjunto *enumerável* tem uma função de escolha.

Isto é um caso particular da Escolha. E verifica-se que este princípio foi invocado com alguma frequência, sem uma consciência óbvia do seu uso. Eis dois bons exemplos.[2]

**Exemplo 73.8.** Eis um pensamento natural: para qualquer conjunto $A$, ou $\omega \preceq A$, ou $A \approx n$ para algum $n \in \omega$. Esta é uma maneira de exprimir a ideia intuitiva de que todo o conjunto é finito ou infinito. Cantor, e muitos outros matemáticos, fizeram esta afirmação sem a provar. Com a cautela que nos caracteriza, a provamos em Teorema 71.7. Mas nessa prova estávamos a trabalhar em **ZFC**, pois assumíamos que qualquer conjunto $A$ pode ser bem ordenado, e logo que $|A|$ está garantidamente definido. Ou seja: assumimos explicitamente a Escolha.

De fato, Dedekind (1888) ofereceu a sua própria prova desta afirmação, do seguinte modo:

**Teorema 73.9 (em $\mathbf{Z}^-$ + Escolha Enumerável).** *Para qualquer $A$, ou $\omega \preceq A$ ou $A \approx n$ para algum $n \in \omega$.*

*Prova.* Suponhamos $A \not\approx n$ para todo o $n \in \omega$. Então, em particular, para cada $n < \omega$ existe um subconjunto $A_n \subseteq A$ com exatamente $2^n$ elementos. Usando esta sequência $A_0, A_1, A_2, \ldots$, definimos para cada $n$:

$$B_n = A_n \setminus \bigcup_{i<n} A_i.$$

[2] Devidos a Potter (2004, §9.4) e Luca Incurvati.

Note-se o seguinte

$$\begin{aligned}\left|\bigcup_{i<n} A_n\right| &\leq |A_0| + |A_1| + \ldots + |A_{n-1}| \\ &= 1 + 2 + \ldots + 2^{n-1} \\ &= 2^n - 1 \\ &< 2^n = |A_n|\end{aligned}$$

Logo cada $B_n$ tem pelo menos um membro, $c_n$. Além disso, os $B_n$ são dois a dois disjuntos; assim, se $c_n = c_m$ então $n = m$. Mas cada $c_n \in A$. Logo a função $f(n) = c_n$ é uma injecção $\omega \to A$. □

Dedekind não assinalou que tinha usado a Escolha Enumerável. Mas reparou o leitor no seu uso? Olhe de novo. (De fato: *olhe de novo*.)

A prova usou a Escolha Enumerável duas vezes. A usamos uma vez, para obter a nossa sequência de conjuntos $A_0$, $A_1$, $A_2$, ... Voltamos a usá-la para seleccionar os elementos $c_n$ de cada $B_n$. Além disso, este uso da Escolha é irredutível. Cohen (1966, p. 138) provou que o resultado falha se não tivermos qualquer versão da Escolha. Ou seja: é consistente com **ZF** que existam conjuntos *incomparáveis* com $\omega$.

**Exemplo 73.10.** Em 1878, Cantor afirmou que uma união enumerável de conjuntos enumeráveis é enumerável. Não apresentou prova, talvez por considerar a prova óbvia. Agora, com a nossa cautela, provamos uma versão mais geral deste resultado em Proposição 72.12. Mas a nossa prova assumiu explicitamente a Escolha. E mesmo a prova do resultado menos geral requer a Escolha Enumerável.

**Teorema 73.11 (em $\mathbf{Z}^- +$ Escolha Enumerável).** *Se $A_n$ é enumerável para cada $n \in \omega$, então $\bigcup_{n<\omega} A_n$ é enumerável.*

*Prova.* Sem perda de generalidade, suponhamos que cada $A_n \neq \emptyset$. Logo, para cada $n \in \omega$ existe uma sobrejeção $f_n \colon \omega \to A_n$. Defina-se $f \colon \omega \times \omega \to \bigcup_{n<\omega} A_n$ por $f(m,n) = f_n(m)$. O resultado segue porque $\omega \times \omega$ é enumerável (Proposição 4.12) e $f$ é uma sobrejeção. □

Notou o uso da Escolha Enumerável? Serve para escolher a nossa sequência de funções $f_0$, $f_1$, $f_2$, ...[3] E, de novo, o resultado falha na ausência de qualquer princípio de Escolha. Especificamente, Feferman and Levy (1963) provou que é consistente com **ZF** que uma união enumerável de conjuntos enumeráveis tenha cardinalidade $\beth_1$. Mas eis uma formulação bem mais divertida do ponto, de Russell:

[3] Um uso semelhante da Escolha ocorreu em Proposição 72.12, quando demos a instrução "Para cada $\beta \in \mathfrak{a}$, fixe uma injeção $f_\beta$".

> Isto ilustra-se com o milionário que comprava um par de meias sempre que comprava um par de botas, e nunca noutra ocasião, e que tinha tal paixão por comprar ambos que acabou por ter $\aleph_0$ pares de botas e $\aleph_0$ pares de meias... Nas botas podemos distinguir direita e esquerda, e portanto podemos fazer uma seleção de uma em cada par, nomeadamente, podemos escolher todas as botas direitas ou todas as esquerdas; mas com as meias não se impõe qualquer princípio de seleção, e não podemos ter a certeza, a menos que assumamos o axioma multiplicativo [isto é, em efeito, a Escolha], de que existe alguma classe constituída por uma meia de cada par. (Russell, 1919, p. 126)

Em suma, alguma forma de Escolha é necessária para provar o seguinte: se tem uma quantidade enumerável de pares de meias, então tem (apenas) uma quantidade enumerável de meias. E, de fato, sem a Escolha Enumerável (ou algo equivalente), uma união enumerável de conjuntos enumeráveis pode deixar de ser enumerável.

A moral é que a Escolha Enumerável foi usada repetidamente, sem grande consciência por parte de quem a usava. A questão filosófica é: como poderíamos *justificar* a Escolha Enumerável?

Uma tentativa de justificação intuitiva poderia apelar a uma super-tarefa. Suponhamos que fazemos a primeira escolha em $1/2$ minuto, a segunda em $1/4$ minuto, ..., a $n$-ésima em $1/2^n$ minuto, ... Então, dentro de 1 minuto, teremos feito uma $\omega$-sequência de escolhas, e definido uma função de escolha.

Mas que poderia realmente dizer-nos um tal experimento mental? Para começar, depende de tomar a ideia de "escolher" de modo bastante literal. Para além disso, parece atar a matemática a possibilidades metafísicas.

Mais importante: não nos dará justificação para a Escolha *sem reservas*, em vez da *mera* Escolha Enumerável. Porque, se precisarmos que *todo* o conjunto tenha função de escolha, então precisaremos de poder realizar uma "supertarefa de comprimento ordinal arbitrário." Sem rodeios, essa ideia é risível.

## 73.6 Considerações Intrínsecas sobre a Escolha

A questão mais ampla, então, é se a Boa Ordenação, ou a Escolha, ou de fato a comparabilidade de todos os conjuntos quanto ao tamanho—não importa qual—podem ser justificadas.

Eis uma tentativa de justificação *intrínseca*. De volta a Seção 66.1, introduzimos vários princípios sobre a hierarquia. Um deles merece ser repetido:

> *Estágios-acumulam*. Para qualquer estágio $S$, e para quaisquer conjuntos que foram formados *antes* do estágio $S$: forma-se no estágio $S$ um conjunto cujos membros são exatamente esses conjuntos. Nada mais se forma no estágio $S$.

De fato, muitos autores sugeriram que o Axioma da Escolha pode ser justificado via (algo como) este princípio. Daremos brevemente um resumo dessa abordagem.

Começamos por um resultado simples, que oferece *mais uma* formulação equivalente da Escolha:

**Teorema 73.12 (em ZF).** *A Escolha é equivalente ao princípio seguinte. Se os membros de $A$ são disjuntos dois a dois e não vazios, então existe algum $C$ tal que $C \cap x$ é um singular para todo o $x \in A$. (Chamamos a tal $C$ um conjunto de escolha para $A$.)*

A prova deste resultado é direta, e a deixamos como exercício para o leitor.

O ponto essencial é que um conjunto de escolha para $A$ é precisamente o contradomínio de uma função de escolha para $A$. Assim, para justificar a Escolha, podemos simplesmente tentar justificar a sua formulação equivalente, em termos da existência de conjuntos de escolha. E é exatamente isso que faremos agora.

Sejam os membros de $A$ disjuntos dois a dois e não vazios. Por *Estágios-são-chave* (ver Seção 66.1), $A$ é formado em algum estágio $S$. Note-se que todos os membros de $\bigcup A$ estão disponíveis antes do estágio $S$. Agora, por *Estágios-acumulam*, para *quaisquer* conjuntos formados antes de $S$, forma-se um conjunto cujos membros são exatamente esses conjuntos. Dito de outro modo: toda a *possível* coleção de conjuntos disponíveis mais cedo existirá em $S$. Mas é certamente *possível* seleccionar objetos que possam ser reunidos num conjunto de escolha para $A$; isso é apenas um certo subconjunto muito específico de $\bigcup A$. Logo: existe tal conjunto de escolha, como requerido.

Bem, esta é uma tentativa *muito* rápida de oferecer uma justificação da Escolha por razões intrínsecas. Mas, para aprofundar esta ideia, deve ler o desenvolvimento elegante de Potter (2004, §14.8).

## 73.7 Paradoxo de Banach–Tarski

Também podemos tentar justificar a Escolha, como Boolos tentou justificar a Substituição, apelando a considerações *extrínsecas* (ver Seção 69.3). Afinal, adotar a Escolha tem muitas consequências desejáveis: poder comparar qualquer par de cardinais; poder bem ordenar qualquer conjunto; poder tratar os cardinais como um tipo particular de ordinal; etc.

Por vezes, contudo, afirma-se que a Escolha tem consequências *indesejáveis*. Na maior parte dos casos, isso deve-se a um resultado de Banach and Tarski (1924).

**Teorema 73.13 (Paradoxo de Banach–Tarski (em ZFC)).** *Qualquer bola pode ser decomposta num número finito de peças, que podem ser remontadas (por rotação e transporte) de modo a formar duas cópias dessa bola.*

À primeira vista, isto surpreende. Claramente as duas bolas têm *o dobro* do volume da bola original. Mas os movimentos rígidos—rotação e transporte—não alteram o volume. Parece assim que Banach–Tarski nos permite fazer aparecer matéria nova por magia.

Pior ainda.[4] Raciocínio semelhante mostra que uma ervilha pode ser cortada num número finito de peças, que depois podem ser remontadas (por rotação e transporte) de modo a formar um objeto com a forma e o tamanho do Big Ben.

Nada disto, porém, vale em **ZF** isoladamente.[5] Logo temos de decidir: rejeitar a Escolha, ou aprender a viver com o "paradoxo".

Sugerimos que devemos aprender a viver com o "paradoxo". De fato, não nos parece propriamente um paradoxo. Em particular, não vemos por que haveria de ser mais ou menos paradoxal do que qualquer um dos resultados seguintes:[6]

1. Há tantos pontos no intervalo $(0,1)$ como em $\mathbb{R}$.
   *Prova*: considere-se $\tan(\pi(r - 1/2))$.

2. Há tantos pontos numa reta como num quadrado.
   Ver Seção 77.3 e Seção 77.5.

3. Existem curvas que preenchem o espaço.
   Ver Seção 77.3 e Seção 77.6.

Nenhum destes três resultados requer a Escolha. De fato, já os tratamos simplesmente como matemática surpreendente e bela. Talvez devêssemos adotar a mesma atitude perante o Paradoxo de Banach–Tarski.

Com certeza, é necessária aqui uma observação técnica; mas basta manter a cabeça fria. Os movimentos rígidos preservam volume. Consequentemente, as cinco[7] peças em que a bola é decomposta não podem todas ser *mensuráveis*. Grosso modo, não faz sentido atribuir volume a estas peças individualmente. Deve pensar nelas como dispersões infinitas de pontos impossíveis de visualizar. Agora, pode ser "estranho" conceber tais conjuntos "infinitamente dispersos". Mas a sua existência parece seguir da injunção, incorporada em *Estágios-acumulam*, de que se formem *todas* as coleções possíveis de conjuntos disponíveis mais cedo.

Se nada disto convence, eis um último argumento (extrínseco) a favor de abraçar o Paradoxo de Banach–Tarski. Ele implica de imediato a melhor piada matemática de sempre:

[4] Ver Tomkowicz and Wagon (2016, Theorem 3.12).

[5] Embora Banach–Tarski possa ser provado com princípios estritamente mais fracos do que a Escolha; ver Tomkowicz and Wagon (2016, 303).

[6] Potter (2004, 276–7), Weston (2003, 16), Tomkowicz and Wagon (2016, 31, 308–9) fazem pontos semelhantes, com outros exemplos.

[7] Enunciamos o Paradoxo em termos de "número finito de peças". De fato, Robinson (1947) provou que a decomposição pode ser feita com *cinco* peças (mas não menos). Para uma prova, ver Tomkowicz and Wagon (2016, pp. 66–7).

*Pergunta*. O que é um anagrama de "Banach–Tarski"?

*Resposta*. "Banach–Tarski Banach–Tarski".

## 73.8 Apêndice: Paradoxo de Vitali

Para ter uma ideia real de se a construção de Banach–Tarski é aceitável ou não, devíamos examinar a sua *prova*. Infelizmente, isso exigiria muito mais álgebra do que podemos apresentar aqui. Contudo, podemos oferecer algumas observações rápidas que talvez esclareçam a prova de Banach–Tarski,[8] concentrando-nos no resultado seguinte:

**Teorema 73.14 (Paradoxo de Vitali (em ZFC)).** *Qualquer círculo pode ser decomposto numa quantidade enumerável de peças, que podem ser remontadas (por rotação e transporte) de modo a formar duas cópias desse círculo.*

O Paradoxo de Vitali é muito mais fácil de provar do que o Paradoxo de Banach–Tarski. Chamamos-lhe "Paradoxo de Vitali", pois segue-se da construção, em 1905, de um conjunto não mensurável. Mas os aspectos conjuntistas da prova do Paradoxo de Vitali e do Paradoxo de Banach–Tarski são muito semelhantes. A diferença essencial entre os resultados é que Banach–Tarski considera uma decomposição *finita*, enquanto o Paradoxo de Vitali considera uma decomposição *enumerável infinita*. Como Weston (2003) diz, o Paradoxo de Vitali "certamente não é tão notável como o paradoxo de Banach–Tarski, mas ilustra que paradoxos geométricos podem ocorrer mesmo em situações 'simples'."

O Paradoxo de Vitali trata de uma figura bidimensional, um círculo. Logo trabalhamos no plano, $\mathbb{R}^2$. Seja $R$ o conjunto das rotações (no sentido dos ponteiros do relógio) de pontos em torno da origem por valores em radianos *racionais* no intervalo $[0, 2\pi)$. Eis alguns fatos algébricos sobre $R$ (se não compreender o enunciado do resultado, a prova esclarecerá o seu significado):

**Lema 73.15.** *$R$ forma um grupo abeliano sob a composição de funções.*

*Prova.* Escrevendo $0_R$ para a rotação por 0 radianos, este é um elemento neutro para $R$, pois $\rho \circ 0_R = 0_R \circ \rho = \rho$ para qualquer $\rho \in R$.

Todo o elemento tem inverso. Onde $\rho \in R$ roda por $r$ radianos, $\rho^{-1} \in R$ roda por $2\pi - r$ radianos, de modo que $\rho \circ \rho^{-1} = 0_R$.

A composição é associativa: $(\tau \circ \sigma) \circ \rho = \tau \circ (\sigma \circ \rho)$ para quaisquer $\rho, \sigma, \tau \in R$

A composição é comutativa: $\sigma \circ \rho = \rho \circ \sigma$ para quaisquer $\rho, \sigma \in R$. □

[8] Para um tratamento bem mais completo, ver Weston (2003) ou Tomkowicz and Wagon (2016).

De fato, podemos partir o nosso grupo $R$ ao meio e depois usar qualquer metade para recuperar o grupo inteiro:

**Lema 73.16.** *Existe uma partição de $R$ em dois conjuntos disjuntos, $R_1$ e $R_2$, ambos dos quais são uma base para $R$.*

*Prova.* Seja $R_1$ o conjunto das rotações por valores racionais em radianos em $[0, \pi)$; seja $R_2 = R \setminus R_1$. Por álgebra elementar, $\{\rho \circ \rho : \rho \in R_1\} = R$. Um resultado semelhante obtém-se para $R_2$. □

Usaremos este fato sobre grupos para estabelecer Teorema 73.14. Seja $\mathbf{S}$ o círculo unitário, isto é, o conjunto dos pontos exatamente a 1 unidade da origem do plano, isto é, $\{\langle r, s\rangle \in \mathbb{R}^2 : \sqrt{r^2 + s^2} = 1\}$. Partiremos $\mathbf{S}$ em partes considerando a relação seguinte em $\mathbf{S}$:

$$r \sim s \text{ sse } (\exists \rho \in R)\rho(r) = s.$$

Ou seja, os pontos de $\mathbf{S}$ estão ligados por esta relação sse se pode passar de um para o outro por uma rotação de valor racional em torno da origem. Sem surpresa:

**Lema 73.17.** *$\sim$ é uma relação de equivalência.*

*Prova.* Trivial, usando Lema 73.15. □

Invocamos agora a Escolha para obter um conjunto, $C$, contendo exatamente um membro de cada classe de equivalência de $\mathbf{S}$ sob $\sim$. Ou seja, consideramos uma função de escolha $f$ no conjunto das classes de equivalência,[9]

$$E = \{[r]_\sim : r \in \mathbf{S}\},$$

e seja $C = \mathrm{Im}(f)$. Para cada rotação $\rho \in R$, o conjunto $\rho[C]$ consiste nos pontos obtidos ao aplicar a rotação $\rho$ a cada ponto de $C$. Os dois resultados seguintes mostram que estes conjuntos cobrem o círculo por completo e sem sobreposição:

**Lema 73.18.** $\mathbf{S} = \bigcup_{\rho \in R} \rho[C]$.

*Prova.* Fixe-se $s \in \mathbf{S}$; existe algum $r \in C$ tal que $r \in [s]_\sim$, isto é, $r \sim s$, isto é, $\rho(r) = s$ para algum $\rho \in R$. □

**Lema 73.19.** *Se $\rho_1 \neq \rho_2$ então $\rho_1[C] \cap \rho_2[C] = \emptyset$.*

[9] Como $R$ é enumerável, cada membro de $E$ é enumerável. Como $\mathbf{S}$ é não enumerável, segue-se de Lema 73.18 e Proposição 72.12 que $E$ é não enumerável. Logo isto é um uso de Escolha *não* enumerável.

*Prova.* Suponhamos $s \in \rho_1[C] \cap \rho_2[C]$. Logo $s = \rho_1(r_1) = \rho_2(r_2)$ para alguns $r_1, r_2 \in C$. Daí $\rho_2^{-1}(\rho_1(r_1)) = r_2$, e $\rho_2^{-1} \circ \rho_1 \in R$, logo $r_1 \sim r_2$. Logo $r_1 = r_2$, pois $C$ selecciona exatamente um membro de cada classe de equivalência sob $\sim$. Logo $s = \rho_1(r_1) = \rho_2(r_1)$, e portanto $\rho_1 = \rho_2$. □

Aplicamos agora os fatos algébricos anteriores ao nosso círculo:

**Lema 73.20.** *Existe uma partição de* **S** *em dois conjuntos disjuntos, $D_1$ e $D_2$, tal que $D_1$ pode ser particionado numa quantidade enumerável de conjuntos que podem ser rodados de modo a formar uma cópia de* **S** *(e analogamente para $D_2$).*

*Prova.* Usando $R_1$ e $R_2$ de Lema 73.16, seja:

$$D_1 = \bigcup_{\rho \in R_1} \rho[C] \qquad\qquad D_2 = \bigcup_{\rho \in R_2} \rho[C]$$

Isto é uma partição de **S**, por Lema 73.18, e $D_1$ e $D_2$ são disjuntos por Lema 73.19. Por construção, $D_1$ pode ser particionado numa quantidade enumerável de conjuntos, $\rho[C]$ para cada $\rho \in R_1$. E estes podem ser rodados de modo a formar uma cópia de **S**, pois $\mathbf{S} = \bigcup_{\rho \in R} \rho[C] = \bigcup_{\rho \in R_1} (\rho \circ \rho)[C]$ por Lema 73.16 e Lema 73.18. O mesmo raciocínio vale para $D_2$. □

Isto implica de imediato o Paradoxo de Vitali. Pois podemos gerar *duas* cópias de **S** a partir de **S**, apenas partindo-o numa quantidade enumerável de peças (os vários $\rho[C]$) e depois movendo-as rigidamente (basta rodar cada peça de $D_1$, e primeiro transportar e depois rodar cada peça de $D_2$).

Recapitulemos a estratégia de prova. Começamos com fatos algébricos sobre o grupo de rotações no plano. Usamos este grupo para partir **S** em classes de equivalência. Chegamos então a um "paradoxo", usando a Escolha para seleccionar elementos de cada classe.

Usamos exatamente a mesma estratégia para provar Banach–Tarski. A principal diferença é que os fatos algébricos usados na prova de Banach–Tarski são bastante mais complicados do que os usados no Paradoxo de Vitali. Mas esses fatos algébricos nada têm a ver com a Escolha. Resumimos-os rapidamente.

Para provar Banach–Tarski, começamos por estabelecer um análogo de Lema 73.16: qualquer *grupo livre* pode ser partido em quatro peças que, intuitivamente, podemos "mover" de modo a recuperar duas cópias do grupo inteiro.[10] Mostramos depois que podemos usar duas rotações particulares em torno da origem de $\mathbb{R}^3$ para gerar um grupo livre de rotações, $F$.[11] (Ainda sem Escolha.) Consideramos agora pontos na superfície da esfera como "semelhantes" sse um pode obter-se do outro por uma rotação em $F$. *Usamos*

[10] O fato de podermos usar *quatro* peças deve-se a Robinson (1947). Para uma prova recente, ver Tomkowicz and Wagon (2016, Theorem 5.2). Seguimos Weston (2003, p. 3) ao descrever isto como "mover" as peças do grupo.

[11] Ver Tomkowicz and Wagon (2016, Theorem 2.1).

*então a Escolha* para seleccionar exatamente um ponto de cada classe de equivalência de pontos "semelhantes". Aplicando a nossa divisão de $F$ à superfície da esfera, como em Lema 73.20, partimos essa superfície em quatro peças, que podemos "mover" de modo a obter duas cópias da superfície da esfera. E isto estabelece (Hausdorff, 1914):

**Teorema 73.21 (Paradoxo de Hausdorff (em ZFC)).** *A superfície de qualquer esfera pode ser decomposta num número finito de peças, que podem ser remontadas (por rotação e transporte) de modo a formar duas cópias disjuntas dessa esfera.*

Ainda são precisos alguns truques algébricos para obter o Teorema completo de Banach–Tarski (que não diz só respeito à superfície da esfera, mas também ao seu interior). Francamente, porém, isto é apenas a cereja no topo do bolo algébrico. Por isso Weston escreve:

> [...] o resultado sobre grupos livres é o passo *chave* na prova do paradoxo de Banach–Tarski. Deste ponto de vista, o paradoxo de Banach–Tarski não é tanto uma afirmação sobre $\mathbb{R}^3$ quanto uma afirmação sobre a complexidade do grupo [das translações e rotações em $\mathbb{R}^3$]. (Weston, 2003, p. 16)

Ou seja: podermos ou não oferecer uma decomposição *finita* (como em Banach–Tarski) ou uma decomposição *enumerável infinita* (como no Paradoxo de Vitali) resume-se a certos fatos de teoria dos grupos sobre trabalhar em duas ou três dimensões.

Admitidamente, esta última observação estraga ligeiramente a piada no final de Seção 73.7. Por ser bidimensional, "Banach–Tarski" tem de ser dividido numa *infinidade* enumerável de peças, se se quiserem rearranjar essas peças de modo a formar "Banach–Tarski Banach–Tarski". Para consertar a piada, é preciso escrever em três dimensões. Deixamos isto como exercício para o leitor.

Um último comentário. Na Seção 73.7, mencionamos que as "peças" da esfera que se obtêm não podem ser *mensuráveis*, mas têm de ser dispersões infinitas impossíveis de visualizar. O mesmo vale para o nosso uso da Escolha ao obter Lema 73.20. E tudo isto merece explicação.

De novo, devemos esboçar alguma base (mas isto é *apenas* um esboço; talvez queira consultar uma entrada de manual sobre *medida*). Definir uma medida para um conjunto $X$ é atribuir um valor $\mu(E) \in \mathbb{R}$ a cada $E$ nalguma "$\sigma$-álgebra" sobre $X$. Os detalhes aqui não são essenciais, exceto que a função $\mu$ deve obedecer ao princípio da aditividade enumerável: a medida de uma união enumerável de conjuntos disjuntos é a soma das medidas individuais, isto é, $\mu(\bigcup_{n<\omega} X_n) = \sum_{n<\omega} \mu(X_n)$ sempre que os $X_n$ são disjuntos. Dizer que um conjunto é "não mensurável" é dizer que nenhuma medida pode ser atribuída de modo adequado. Agora, usando o nosso $R$ de antes:

**Corolário 73.22 (Vitali).** *Seja $\mu$ uma medida tal que $\mu(\mathbf{S}) = 1$, e tal que $\mu(X) = \mu(Y)$ se $X$ e $Y$ são congruentes. Então $\rho[C]$ é não mensurável para todo o $\rho \in R$.*

*Prova.* Por redução ao absurso, suponhamos o contrário. Seja então $\mu(\sigma[C]) = r$ para algum $\sigma \in R$ e algum $r \in \mathbb{R}$. Para qualquer $\rho \in R$, $\rho[C]$ e $\sigma[C]$ são congruentes, logo $\mu(\rho[C]) = r$ para qualquer $\rho \in R$. Por Lema 73.18 e Lema 73.19, $\mathbf{S} = \bigcup_{\rho\in R} \rho[C]$ é uma união enumerável de conjuntos disjuntos dois a dois. Logo a aditividade enumerável dita que $\mu(\mathbf{S}) = 1$ é a soma das medidas de cada $\rho[C]$, isto é,

$$1 = \mu(\mathbf{S}) = \sum_{\rho\in R} \mu(\rho[C]) = \sum_{\rho\in R} r$$

Mas se $r = 0$ então $\sum_{\rho\in R} r = 0$, e se $r > 0$ então $\sum_{\rho\in R} r = \infty$. □

## Problemas

**Problema 73.1.** Prove Teorema 73.12. Se tiver dificuldades, encontrará uma prova em (Potter, 2004, pp. 242–3).

# Parte XVI

# Methods

This part covers general and methodological material, especially explanations of various proof methods a non-mathematics student may be unfamiliar with. It currently contains a chapter on how to write proofs, and a chapter on induction, but additional sections for those, exercises, and a chapter on mathematical terminology is also planned.

# Capítulo 74

# Provas

## 74.1 Introdução

Com base em suas experiências na lógica introdutória, você talvez se sinta à vontade com um sistema de derivação—provavelmente um sistema de derivação de dedução natural ou no estilo Fitch, ou talvez um sistema de árvores de prova. Você provavelmente se lembra de fazer provas nesses sistemas, seja provando a fórmula, seja mostrando que um dado argumento é válido. Para fazer isso, você aplicava as regras do sistema até obter o resultado final desejado. Ao raciocinar *sobre* lógica, também provamos coisas, mas na maioria dos casos não estamos usando um sistema de derivação. De fato, a maior parte das provas que consideramos é feita em português (talvez com alguma linguagem simbólica inserida) e não inteiramente na linguagem da lógica de primeira ordem. Ao construir tais provas, você pode a princípio ficar perdido—como provo algo sem um sistema de derivação? Como começo? Como sei se minha prova está correta?

Antes de tentar uma prova, é importante saber o que é uma prova e como construir uma. Como o nome sugere, uma *prova* destina-se a mostrar que algo é verdadeiro. Você pode pensar nisso em termos de um diálogo—alguém lhe pergunta se algo é verdadeiro, digamos, se todo primo diferente de dois é um número ímpar. Responder "sim" não é suficiente; a pessoa pode querer saber *por quê*. Nesse caso, você lhe daria uma prova.

No discurso cotidiano, pode ser suficiente esboçar uma resposta, ou dar uma resposta incompleta. Na lógica e na matemática, porém, queremos uma prova rigorosa—queremos mostrar que algo é verdadeiro além de *qualquer* dúvida. Isso significa que cada passo de nossa prova deve ser justificado, e a justificativa deve ser convincente (isto é, a suposição que você está usando é de fato assumida no enunciado do teorema que você está provando, as definições que você aplica devem ser aplicadas corretamente, as justificativas invocadas devem ser inferências corretas, etc.).

Em geral, estamos provando algum enunciado. Chamamos os enunciados

que provamos por vários nomes: proposições, teoremas, lemas ou corolários. Uma proposição é um enunciado básico digno de prova: importante o suficiente para ser registrado, mas talvez não particularmente profundo nem aplicado com frequência. Um teorema é uma proposição significativa e importante. Sua prova é frequentemente dividida em vários passos, e às vezes recebe o nome da pessoa que primeiro o provou (por exemplo, o Teorema de Cantor, o teorema de Löwenheim–Skolem) ou do fato de que trata (por exemplo, o teorema da completude). Um lema é uma proposição ou teorema usado na prova de um resultado mais importante. De modo confuso, às vezes os lemas são resultados importantes em si mesmos, e também recebem o nome da pessoa que os introduziu (por exemplo, o Lema de Zorn). Um corolário é um resultado que decorre facilmente de outro.

Um enunciado a ser provado frequentemente contém suposições que esclarecem sobre quais tipos de coisas estamos provando algo. Ele pode começar com "Seja $\varphi$ a fórmula da forma $\psi \to \chi$" ou "Suponha $\Gamma \vdash \varphi$" ou algo do gênero. Essas são as *hipóteses* da proposição, teorema ou lema, e você pode assumi-las como verdadeiras em sua prova. Elas restringem o que estamos provando e também introduzem alguns nomes para os objetos sobre os quais estamos falando. Por exemplo, se sua proposição começa com "Seja $\varphi$ a fórmula da forma $\psi \to \chi$", você está provando algo apenas sobre todas as fórmulas de certo tipo (a saber, condicionais), e fica entendido que $\psi \to \chi$ é um condicional arbitrário sobre o qual sua prova falará.

## 74.2 Começando uma Prova

Mas por onde começar?

Foi-lhe dado algo a provar, de modo que isso deveria ser a última coisa mencionada na prova (você pode, obviamente, *anunciar* que vai prová-lo no começo, mas não convém usá-lo como suposição). Escreva o que você está tentando provar no rodapé de uma folha de papel em branco—assim você não perde de vista seu objetivo.

Em seguida, você pode ter algumas suposições que pode usar (isso ficará mais claro quando falarmos sobre o *tipo* de prova que você está fazendo na próxima seção). Escreva-as no topo da página e certifique-se de sinalizar que são suposições (isto é, se você está supondo $p$, escreva "suponha que $p$" ou "assuma que $p$"). Por fim, pode haver na questão algumas definições que você precisa conhecer. Pode ser que lhe digam para usar uma definição específica, ou pode haver várias definições nas suposições ou na conclusão para a qual você está trabalhando. *Anote-as e certifique-se de entender o que significam.*

A forma como você organiza sua prova também dependerá da forma da questão. A próxima seção fornece detalhes sobre como organizar sua prova com base no tipo de sentença.

## 74.3 Usando Definições

Mencionamos que você deve estar familiarizado com todas as definições que possam ser usadas na prova, e que saiba aplicá-las corretamente. Esse é um ponto realmente importante, e vale a pena examiná-lo em um pouco mais de detalhe. As definições são usadas para abreviar propriedades e relações, de modo que possamos falar delas de forma mais sucinta. A abreviação introduzida é chamada de *definiendum*, e aquilo que ela abrevia é o *definiens*. Em provas, com frequência temos que voltar a como o definiendum foi introduzido, porque temos que explorar a estrutura lógica do definiens (a versão longa da qual o termo definido é a abreviação) para concluir nossa prova. Ao desdobrar as definições, você garante que está chegando ao cerne de onde a ação lógica acontece.

Começaremos com um exemplo. Suponha que você queira provar o seguinte:

**Proposição 74.1.** *Para quaisquer conjuntos $A$ e $B$, $A \cup B = B \cup A$.*

Para sequer iniciar a prova, precisamos saber o que significa que dois conjuntos sejam idênticos; isto é, precisamos saber o que o "$=$" naquela equação significa para conjuntos. Os conjuntos são definidos como idênticos sempre que têm os mesmos membros. Assim, a definição que temos que desdobrar é:

**Definição 74.2.** Os conjuntos $A$ e $B$ são *idênticos*, $A = B$, sse todo membro de $A$ é um membro de $B$, e vice-versa.

Esta definição usa $A$ e $B$ como marcadores de posição para conjuntos arbitrários. O que ela define—o *definiendum*—é a expressão "$A = B$", dando a condição sob a qual $A = B$ é verdadeira. Essa condição—"todo membro de $A$ é um membro de $B$, e vice-versa"—é o *definiens*.[1] A definição especifica que $A = B$ é verdadeira se, e somente se (abreviamos isso por "sse") a condição vale.

Quando você aplica a definição, tem que fazer corresponder o $A$ e o $B$ da definição ao caso de que está tratando. No nosso caso, isso significa que, para que $A \cup B = B \cup A$ seja verdadeira, cada $z \in A \cup B$ também deve estar em $B \cup A$, e vice-versa. A expressão $A \cup B$ na proposição faz o papel de $A$ na definição, e $B \cup A$, o de $B$. Como $A$ e $B$ são usados tanto na definição quanto no enunciado da proposição que estamos provando, mas em usos diferentes, você precisa ter cuidado para não confundir os dois. Por exemplo, seria um erro pensar que você poderia provar a proposição mostrando que todo membro de $A$ é um membro de $B$, e vice-versa—isso mostraria que $A = B$, não que

[1] Neste caso particular—e de modo bastante confuso!—quando $A = B$, os conjuntos $A$ e $B$ são apenas um único e mesmo conjunto, ainda que usemos letras diferentes para ele do lado esquerdo e do lado direito. Mas os modos pelos quais esse conjunto é identificado podem ser diferentes, e isso torna a definição não trivial.

$A \cup B = B \cup A$. (Além disso, como $A$ e $B$ podem ser quaisquer dois conjuntos, você não chegaria muito longe, pois, se nada for suposto sobre $A$ e $B$, eles bem podem ser conjuntos diferentes.)

Dentro da prova, estamos lidando com noções da teoria dos conjuntos, como união, e portanto também precisamos conhecer os significados do símbolo $\cup$ a fim de entender como a prova deve prosseguir. E, às vezes, desdobrar a definição dá origem a outras definições a desdobrar. Por exemplo, $A \cup B$ é definido como $\{z : z \in A \text{ ou } z \in B\}$. Então, se você quer provar que $x \in A \cup B$, desdobrar a definição de $\cup$ lhe diz que você tem que provar $x \in \{z : z \in A \text{ ou } z \in B\}$. Agora você também tem que lembrar que $x \in \{z : \ldots z \ldots\}$ sse $\ldots x \ldots$. Assim, desdobrando ainda mais a definição da notação $\{z : \ldots z \ldots\}$, o que você tem que mostrar é: $x \in A$ ou $x \in B$. Assim, "todo membro de $A \cup B$ é também um membro de $B \cup A$" significa, na verdade: "para todo $x$, se $x \in A$ ou $x \in B$, então $x \in B$ ou $x \in A$." Se desdobramos completamente as definições na proposição, vemos que o que temos que mostrar é isto:

**Proposição 74.3.** *Para quaisquer conjuntos $A$ e $B$: (a) para todo $x$, se $x \in A$ ou $x \in B$, então $x \in B$ ou $x \in A$, e (b) para todo $x$, se $x \in B$ ou $x \in A$, então $x \in A$ ou $x \in B$.*

O que importa é que desdobrar definições é uma parte necessária da construção de uma prova. Fazê-lo corretamente é às vezes difícil: você deve ter cuidado para distinguir e fazer corresponder as variáveis da definição e os termos na afirmação que está provando. Para ter sucesso, você deve saber o que a questão está pedindo e o que todos os termos usados na questão significam—muitas vezes você precisará desdobrar mais de uma definição. Em provas simples como as que seguem, a solução decorre quase imediatamente das próprias definições. É claro que nem sempre será assim tão simples.

## 74.4 Padrões de Inferência

As provas são compostas de inferências individuais. Quando fazemos uma inferência, normalmente a indicamos usando uma palavra como "então," "assim," ou "portanto." A inferência muitas vezes se apoia em um ou dois fatos que já temos disponíveis em nossa prova—pode ser algo que supusemos, ou algo que concluímos por uma inferência anterior. Para deixar claro, podemos rotular essas coisas, e na inferência indicamos quais outras afirmações estamos usando na inferência. Uma inferência muitas vezes também conterá uma explicação de *por que* nossa nova conclusão decorre das coisas que a precedem. Há alguns padrões comuns de inferência que são usados com muita frequência em provas; percorreremos alguns deles abaixo. Alguns padrões de inferência, como as provas por indução, são mais elaborados (e serão discutidos mais adiante).

Já discutimos um padrão de inferência: desdobrar, ou aplicar, uma definição. Quando desdobramos uma definição, apenas reenunciamos algo que envolve o definiendum usando o definiens. Por exemplo, suponha que já tenhamos estabelecido no curso de uma prova que $D = E$ (a). Então podemos aplicar a definição de $=$ para conjuntos e inferir: "Assim, por definição, de (a), todo membro de $D$ é um membro de $E$ e vice-versa."

De modo um tanto confuso, muitas vezes não escrevemos a justificativa de uma inferência quando de fato a fazemos, mas antes. Suponha que ainda não tenhamos provado que $D = E$, mas queremos. Se $D = E$ é a conclusão que buscamos, então podemos reenunciar esse objetivo também aplicando a definição: para provar $D = E$ temos que provar que todo membro de $D$ é um membro de $E$ e vice-versa. Assim, nossa prova terá a forma: (a) provar que todo membro de $D$ é um membro de $E$; (b) todo membro de $E$ é um membro de $D$; (c) portanto, de (a) e (b), pela definição de $=$, $D = E$. Mas normalmente não escreveríamos desse jeito. Em vez disso, poderíamos escrever algo como,

> Queremos mostrar $D = E$. Pela definição de $=$, isso equivale a mostrar que todo membro de $D$ é um membro de $E$ e vice-versa.
>
> (a) ... (uma prova de que todo membro de $D$ é um membro de $E$)
> ...
>
> (b) ... (uma prova de que todo membro de $E$ é um membro de $D$)
> ...

### Usando uma Conjunção

Talvez o padrão de inferência mais simples seja o de tirar como conclusão uma das conjuntivas de uma conjunção. Em outras palavras: se supusemos ou já provamos que $p$ e $q$, então temos o direito de inferir que $p$ (e também que $q$). Essa é uma inferência tão básica que muitas vezes não é mencionada. Por exemplo, uma vez que tenhamos desdobrado a definição de $D = E$, estabelecemos que todo membro de $D$ é um membro de $E$ e vice-versa. Disso podemos concluir que todo membro de $E$ é um membro de $D$ (essa é a parte do "vice-versa").

### Provando uma Conjunção

Às vezes, o que lhe pedirão para provar terá a forma de uma conjunção; pedirão a você que "prove $p$ e $q$." Nesse caso, você simplesmente tem que fazer duas coisas: provar $p$, e então provar $q$. Você poderia dividir sua prova em duas seções e, para maior clareza, rotulá-las. Quando estiver fazendo suas primeiras anotações, você pode escrever "(1) Provar $p$" no topo da página, e "(2) Provar $q$" no meio da página. (É claro que você pode não ser explicitamente solicitado a provar uma conjunção, mas descobrir que sua prova exige que você prove uma conjunção. Por exemplo, se lhe pedem para provar

que $D = E$, você descobrirá que, após desdobrar a definição de $=$, você tem que provar: todo membro de $D$ é um membro de $E$ *e* todo membro de $E$ é um membro de $D$).

### Provando uma Disjunção

Quando o que você está provando assume a forma de uma disjunção (isto é, é uma afirmação da forma "$p$ ou $q$"), basta mostrar que um dos disjuntos é verdadeiro. No entanto, basicamente nunca acontece de qualquer um dos disjuntos simplesmente decorrer das suposições do seu teorema. Mais frequentemente, as suposições do seu teorema são elas próprias disjuntivas, ou você está mostrando que todas as coisas de certo tipo têm uma de duas propriedades, mas algumas das coisas têm uma e outras têm a outra propriedade. É aqui que a prova por casos é útil (veja abaixo).

### Prova Condicional

Muitos teoremas que você encontrará estão na forma condicional (isto é, mostre que se $p$ vale, então $q$ também é verdadeiro). Esses casos são bons e fáceis de montar—basta supor o antecedente do condicional (neste caso, $p$) e provar a conclusão $q$ a partir dele. Então, se o seu teorema diz "Se $p$ então $q$," você começa sua prova com "suponha $p$" e, ao final, você deve ter provado $q$.

Os condicionais podem ser enunciados de maneiras diferentes. Assim, em vez de "Se $p$ então $q$," um teorema pode afirmar que "$p$ somente se $q$," "$q$ se $p$," ou "$q$, desde que $p$." Todos eles significam o mesmo e exigem supor $p$ e provar $q$ a partir dessa suposição. Lembre-se de que um bicondicional ("$p$ se e somente se (sse) $q$") é, na verdade, dois condicionais postos juntos: se $p$ então $q$, e se $q$ então $p$. Tudo o que você tem que fazer, então, são duas instâncias de prova condicional: uma para o primeiro condicional e outra para o segundo. Às vezes, no entanto, é possível provar uma afirmação "sse" encadeando um monte de outras afirmações "sse", de modo que você comece com "$p$" e termine com "$q$"—mas, nesse caso, você tem que garantir que cada passo realmente seja um "sse."

### Afirmações Universais

Usar uma afirmação universal é simples: se algo é verdadeiro para qualquer coisa, é verdadeiro para cada coisa particular. Então, se, digamos, a hipótese da sua prova é $A \subseteq B$, isso significa (desdobrando a definição de $\subseteq$) que, para todo $x \in A$, $x \in B$. Assim, se você já sabe que $z \in A$, você pode concluir $z \in B$.

Provar uma afirmação universal pode parecer um pouco complicado. Normalmente essas afirmações assumem a seguinte forma: "Se $x$ tem $P$, então ele tem $Q$" ou "Todos os $P$ são $Q$." É claro que pode não se ajustar a essa forma

perfeitamente, e é preciso um pouco de prática para descobrir o que exatamente lhe pedem para provar. Mas: muitas vezes temos que provar que todos os objetos com alguma propriedade têm uma certa outra propriedade.

A maneira de provar uma afirmação universal é introduzir nomes ou variáveis para as coisas que têm uma propriedade e então mostrar que elas também têm a outra propriedade. Poderíamos expressar isso dizendo que, para provar algo para *todos* os $P$, você tem que prová-lo para um *$P$ arbitrário*. E o nome introduzido é um nome para um $P$ arbitrário. Normalmente usamos letras isoladas como esses nomes para coisas arbitrárias, e as letras costumam seguir convenções: por exemplo, usamos $n$ para números naturais, $\varphi$ para fórmulas, $A$ para conjuntos, $f$ para funções, etc.

O truque é manter a generalidade ao longo da prova. Você começa supondo que um objeto arbitrário ("$x$") tem a propriedade $P$, e mostra (com base apenas em definições ou no que lhe é permitido supor) que $x$ tem a propriedade $Q$. Como você não estipulou o que $x$ é especificamente, a não ser que ele tem a propriedade $P$, então você pode afirmar que tudo que tem $P$ tem a propriedade $Q$. Em suma, $x$ é um substituto para *todas* as coisas com a propriedade $P$.

**Proposição 74.4.** *Para todos os conjuntos $A$ e $B$, $A \subseteq A \cup B$.*

*Prova.* Sejam $A$ e $B$ conjuntos arbitrários. Queremos mostrar que $A \subseteq A \cup B$. Pela definição de $\subseteq$, isso equivale a: para todo $x$, se $x \in A$ então $x \in A \cup B$. Então seja $x \in A$ um membro arbitrário de $A$. Temos que mostrar que $x \in A \cup B$. Como $x \in A$, $x \in A$ ou $x \in B$. Assim, $x \in \{x : x \in A \vee x \in B\}$. Mas isso, pela definição de $\cup$, significa $x \in A \cup B$. □

### Prova por Casos

Suponha que você tenha uma disjunção como suposição ou como conclusão já estabelecida—você supôs ou provou que $p$ ou $q$ é verdadeira. Você quer provar $r$. Você faz isso em dois passos: primeiro você supõe que $p$ é verdadeira, e prova $r$, e depois supõe que $q$ é verdadeira e prova $r$ novamente. Isso funciona porque supomos ou sabemos que uma das duas alternativas vale. Os dois passos estabelecem que qualquer uma delas é suficiente para a verdade de $r$. (Se ambas são verdadeiras, temos não uma, mas duas razões para que $r$ seja verdadeira. Não é necessário provar separadamente que $r$ é verdadeira supondo tanto $p$ quanto $q$.) Para indicar o que estamos fazendo, anunciamos que "distinguimos casos." Por exemplo, suponha que saibamos que $x \in B \cup C$. $B \cup C$ é definido como $\{x : x \in B \text{ ou } x \in C\}$. Em outras palavras, por definição, $x \in B$ ou $x \in C$. Provaríamos que $x \in A$ a partir disso supondo primeiro que $x \in B$, e provando $x \in A$ a partir dessa suposição, e então supondo $x \in C$, e novamente provando $x \in A$ a partir disso. Você escreveria "Distinguimos casos" sob a suposição, depois "Caso (1): $x \in B$" abaixo, e "Caso (2): $x \in C$" na

metade da página. Então você prosseguiria preenchendo a metade superior e a metade inferior da página.

A prova por casos é especialmente útil se o que você está provando é, ele mesmo, disjuntivo. Eis um exemplo simples:

**Proposição 74.5.** *Suponha $B \subseteq D$ e $C \subseteq E$. Então $B \cup C \subseteq D \cup E$.*

*Prova.* Suponha (a) que $B \subseteq D$ e (b) $C \subseteq E$. Por definição, qualquer $x \in B$ também está $\in D$ (c) e qualquer $x \in C$ também está $\in E$ (d). Para mostrar que $B \cup C \subseteq D \cup E$, temos que mostrar que se $x \in B \cup C$ então $x \in D \cup E$ (pela definição de $\subseteq$). $x \in B \cup C$ sse $x \in B$ ou $x \in C$ (pela definição de $\cup$). De modo semelhante, $x \in D \cup E$ sse $x \in D$ ou $x \in E$. Então, temos que mostrar: para qualquer $x$, se $x \in B$ ou $x \in C$, então $x \in D$ ou $x \in E$.

> Até aqui só desdobramos definições! Reformulamos nossa proposição sem $\subseteq$ e $\cup$ e ficamos tentando provar uma afirmação condicional universal. Pelo que discutimos acima, isso é feito supondo que $x$ é algo a respeito do qual supomos que a parte do "se" é verdadeira, e passaremos a mostrar que a parte do "então" também é verdadeira. Em outras palavras, suporemos que $x \in B$ ou $x \in C$ e mostraremos que $x \in D$ ou $x \in E$.[2]

Suponha que $x \in B$ ou $x \in C$. Temos que mostrar que $x \in D$ ou $x \in E$. Distinguimos casos.

Caso 1: $x \in B$. Por (c), $x \in D$. Assim, $x \in D$ ou $x \in E$. (Aqui fizemos a inferência discutida na subseção anterior!)

Caso 2: $x \in C$. Por (d), $x \in E$. Assim, $x \in D$ ou $x \in E$. □

### Provando uma Afirmação de Existência

Quando lhe pedem para provar uma afirmação de existência, a questão normalmente será da forma "prove que há um $x$ tal que $\ldots x \ldots$", isto é, que algum objeto tem a propriedade descrita por "$\ldots x \ldots$". Nesse caso, você terá que identificar um objeto adequado e mostrar que ele tem a propriedade exigida. Isso parece direto, mas uma prova desse tipo pode ser complicada. Tipicamente, ela envolve *construir* ou *definir* um objeto e provar que o objeto assim definido tem a propriedade exigida. Encontrar o objeto certo pode ser difícil, provar que ele tem a propriedade exigida pode ser difícil, e às vezes é até complicado mostrar que você teve sucesso em definir um objeto!

Em geral, você escreveria isso especificando o objeto, por exemplo, "seja $x \ldots$" (em que $\ldots$ especifica qual objeto você tem em mente), possivelmente provando que $\ldots$ de fato descreve um objeto que existe, e então passaria a mostrar que $x$ tem a propriedade $Q$. Eis um exemplo simples.

[2] Este parágrafo apenas explica o que estamos fazendo—não é parte da prova, e você não precisa entrar em todo esse detalhe quando escreve suas próprias provas.

**Proposição 74.6.** *Suponha que $x \in B$. Então há um $A$ tal que $A \subseteq B$ e $A \neq \emptyset$.*

*Prova.* Suponha $x \in B$. Seja $A = \{x\}$.

> Aqui definimos o conjunto $A$ enumerando seus membros. Como supomos que $x$ é um objeto, e sempre podemos formar um conjunto enumerando seus membros, não temos que mostrar que tivemos sucesso em definir um conjunto $A$ aqui. No entanto, ainda temos que mostrar que $A$ tem as propriedades exigidas pela proposição. A prova não está completa sem isso!

Como $x \in A$, $A \neq \emptyset$.

> Isso se apoia na definição de $A$ como $\{x\}$ e nos fatos óbvios de que $x \in \{x\}$ e $x \notin \emptyset$.

Como $x$ é o único membro de $\{x\}$, e $x \in B$, todo membro de $A$ é também um membro de $B$. Pela definição de $\subseteq$, $A \subseteq B$. □

### Usando Afirmações de Existência

Suponha que você saiba que alguma afirmação de existência é verdadeira (você a provou, ou ela é uma hipótese que você pode usar), digamos, "para algum $x$, $x \in A$" ou "há um $x \in A$." Se você quiser usá-la em sua prova, você pode simplesmente fingir que tem um nome para uma das coisas que sua hipótese diz existir. Como $A$ contém pelo menos uma coisa, há coisas a que esse nome poderia se referir. É claro que você pode não ser capaz de escolher uma ou de descrevê-la mais (a não ser que ela é $\in A$). Mas, para os fins da prova, você pode fingir que a escolheu e dar-lhe um nome. É importante escolher um nome que você ainda não tenha usado (ou que apareça nas suas hipóteses), caso contrário as coisas podem dar errado. Em sua prova, você indica isso passando de "para algum $x$, $x \in A$" para "Seja $a \in A$." Agora você pode raciocinar sobre $a$, usar algumas outras hipóteses, etc., até chegar a uma conclusão, $p$. Se $p$ não menciona mais $a$, $p$ é independente da suposição de que $a \in A$, e você mostrou que ele decorre apenas da suposição "para algum $x$, $x \in A$."

**Proposição 74.7.** *Se $A \neq \emptyset$, então $A \cup B \neq \emptyset$.*

*Prova.* Suponha $A \neq \emptyset$. Então, para algum $x$, $x \in A$.

> Aqui apenas reenunciamos a hipótese da proposição. Essa hipótese, isto é, $A \neq \emptyset$, esconde uma afirmação existencial, à qual você só chega desdobrando algumas definições. A definição de $=$ nos diz que $A = \emptyset$ sse todo $x \in A$ também está $\in \emptyset$ e todo $x \in \emptyset$ também está $\in A$. Negando ambos os lados, obtemos: $A \neq \emptyset$ sse ou algum

> $x \in A$ está $\notin \emptyset$ ou algum $x \in \emptyset$ está $\notin A$. Como nada está $\in \emptyset$, o segundo disjunto nunca pode ser verdadeiro, e "$x \in A$ e $x \notin \emptyset$" se reduz a apenas $x \in A$. Então $A \neq \emptyset$ sse, para algum $x$, $x \in A$. Essa é uma afirmação de existência. Agora usamos essa afirmação de existência introduzindo um nome para um dos membros de $A$:

Seja $a \in A$.

> Agora introduzimos um nome para uma das coisas $\in A$. Continuaremos a argumentar sobre $a$, mas teremos o cuidado de supor apenas que $a \in A$ e nada mais:

Como $a \in A$, $a \in A \cup B$, pela definição de $\cup$. Então, para algum $x$, $x \in A \cup B$, isto é, $A \cup B \neq \emptyset$.

> Naquele último passo, fomos de "$a \in A \cup B$" para "para algum $x$, $x \in A \cup B$." Isso não menciona mais $a$, então sabemos que "para algum $x$, $x \in A \cup B$" decorre de "para algum $x$, $x \in A$" apenas. Mas isso significa que $A \cup B \neq \emptyset$. □

Talvez seja boa prática manter variáveis ligadas como "$x$" separadas de nomes hipotéticos como $a$, como fizemos. Na prática, porém, muitas vezes não o fazemos e apenas usamos $x$, assim:

> Suponha $A \neq \emptyset$, isto é, há um $x \in A$. Pela definição de $\cup$, $x \in A \cup B$. Então $A \cup B \neq \emptyset$.

No entanto, quando você faz isso, tem que ter um cuidado extra para usar $x$ e $y$ diferentes para afirmações existenciais diferentes. Por exemplo, a seguinte *não* é uma prova correta de "Se $A \neq \emptyset$ e $B \neq \emptyset$ então $A \cap B \neq \emptyset$" (o que não é verdade).

> Suponha $A \neq \emptyset$ e $B \neq \emptyset$. Então, para algum $x$, $x \in A$ e também, para algum $x$, $x \in B$. Como $x \in A$ e $x \in B$, $x \in A \cap B$, pela definição de $\cap$. Então $A \cap B \neq \emptyset$.

Você consegue identificar onde ocorre o passo incorreto e explicar por que o resultado não vale?

## 74.5 Um Exemplo

Nosso primeiro exemplo é o seguinte fato simples sobre uniões e interseções de conjuntos. Ele ilustrará o desdobramento de definições, provas de conjunções, de afirmações universais, e a prova por casos.

**Proposição 74.8.** *Para quaisquer conjuntos $A$, $B$ e $C$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$*

Vamos prová-la!

*Prova.* Queremos mostrar que, para quaisquer conjuntos $A$, $B$ e $C$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

> Primeiro desdobramos a definição de "=" no enunciado da proposição. Lembre-se de que provar que conjuntos são idênticos significa mostrar que os conjuntos têm os mesmos membros. Isto é, todos os membros de $A \cup (B \cap C)$ são também membros de $(A \cup B) \cap (A \cup C)$, e vice-versa. O "vice-versa" significa que também todo membro de $(A \cup B) \cap (A \cup C)$ deve ser um membro de $A \cup (B \cap C)$. Assim, ao desdobrar a definição, vemos que temos que provar uma conjunção. Vamos registrar isso:

Por definição, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ sse todo membro de $A \cup (B \cap C)$ é também um membro de $(A \cup B) \cap (A \cup C)$, e todo membro de $(A \cup B) \cap (A \cup C)$ é um membro de $A \cup (B \cap C)$.

> Como isso é uma conjunção, devemos provar cada conjuntiva separadamente. Vamos começar pela primeira: vamos provar que todo membro de $A \cup (B \cap C)$ é também um membro de $(A \cup B) \cap (A \cup C)$.
>
> Esta é uma afirmação universal, e por isso consideramos um membro arbitrário de $A \cup (B \cap C)$ e mostramos que ele também deve ser um membro de $(A \cup B) \cap (A \cup C)$. Vamos escolher uma variável para chamar esse membro arbitrário, digamos, $z$. Nossa prova continua:

Primeiro, provamos que todo membro de $A \cup (B \cap C)$ é também um membro de $(A \cup B) \cap (A \cup C)$. Seja $z \in A \cup (B \cap C)$. Temos que mostrar que $z \in (A \cup B) \cap (A \cup C)$.

> Agora é hora de desdobrar a definição de $\cup$ e $\cap$. Por exemplo, a definição de $\cup$ é: $A \cup B = \{z : z \in A \text{ ou } z \in B\}$. Quando aplicamos a definição a "$A \cup (B \cap C)$," o papel do "$B$" na definição passa a ser desempenhado por "$B \cap C$," de modo que $A \cup (B \cap C) = \{z : z \in A \text{ ou } z \in B \cap C\}$. Então nossa suposição de que $z \in A \cup (B \cap C)$ equivale a: $z \in \{z : z \in A \text{ ou } z \in B \cap C\}$. E $z \in \{z : \ldots z \ldots\}$ sse $\ldots z \ldots$, isto é, neste caso, $z \in A$ ou $z \in B \cap C$.

Pela definição de $\cup$, ou $z \in A$ ou $z \in B \cap C$.

> Como isso é uma disjunção, será útil aplicar a prova por casos. Tomamos os dois casos, e mostramos que, em cada um, a conclusão que buscamos (a saber, "$z \in (A \cup B) \cap (A \cup C)$") se obtém.

Caso 1: Suponha que $z \in A$.

> Não há muito mais com que trabalhar a partir das nossas suposições. Então vamos olhar para o que temos com que trabalhar na conclusão. Queremos mostrar que $z \in (A \cup B) \cap (A \cup C)$. Com base na definição de $\cap$, se queremos mostrar que $z \in (A \cup B) \cap (A \cup C)$, temos que mostrar que ele está tanto em $(A \cup B)$ quanto em $(A \cup C)$. Mas $z \in A \cup B$ sse $z \in A$ ou $z \in B$, e já temos (como a suposição do caso 1) que $z \in A$. Pelo mesmo raciocínio—trocando $C$ por $B$—$z \in A \cup C$. Esse argumento foi na direção inversa, então vamos registrar nosso raciocínio na direção necessária à nossa prova.

Como $z \in A$, $z \in A$ ou $z \in B$, e logo, pela definição de $\cup$, $z \in A \cup B$. De modo semelhante, $z \in A \cup C$. Mas isso significa que $z \in (A \cup B) \cap (A \cup C)$, pela definição de $\cap$.

> Isso completa o primeiro caso da prova por casos. Agora queremos derivar a conclusão no segundo caso, em que $z \in B \cap C$.

Caso 2: Suponha que $z \in B \cap C$.

> Novamente, estamos trabalhando com a interseção de dois conjuntos. Vamos aplicar a definição de $\cap$:

Como $z \in B \cap C$, $z$ deve ser um membro tanto de $B$ quanto de $C$, pela definição de $\cap$.

> É hora de olhar de novo para a nossa conclusão. Temos que mostrar que $z$ está tanto em $(A \cup B)$ quanto em $(A \cup C)$. E, novamente, a solução é imediata.

Como $z \in B$, $z \in (A \cup B)$. Como $z \in C$, também $z \in (A \cup C)$. Então, $z \in (A \cup B) \cap (A \cup C)$.

> Aqui aplicamos as definições de $\cup$ e $\cap$ novamente, mas como já relembramos essas definições, e já mostramos que, se $z$ está em um de dois conjuntos, ele está na união deles, não precisamos ser tão explícitos no que fizemos.
>
> Completamos o segundo caso da prova por casos, então agora podemos afirmar nossa primeira conclusão.

Então, se $z \in A \cup (B \cap C)$, então $z \in (A \cup B) \cap (A \cup C)$.

> Agora queremos apenas mostrar a outra direção, que todo membro de $(A \cup B) \cap (A \cup C)$ é um membro de $A \cup (B \cap C)$. Como antes, provamos essa afirmação universal supondo que temos um membro arbitrário do primeiro conjunto e mostrando que ele deve estar no segundo conjunto. Vamos declarar o que estamos prestes a fazer.

Agora, suponha que $z \in (A \cup B) \cap (A \cup C)$. Queremos mostrar que $z \in A \cup (B \cap C)$.

> Estamos agora trabalhando a partir da hipótese de que $z \in (A \cup B) \cap (A \cup C)$. Esperamos que não seja confuso demais estarmos usando o mesmo $z$ aqui que na primeira parte da prova. Quando terminamos aquela parte, todas as suposições que fizemos ali deixaram de estar em vigor, então agora podemos fazer novas suposições sobre o que $z$ é. Se isso for confuso para você, basta substituir $z$ por uma variável diferente no que segue.
>
> Sabemos que $z$ está tanto em $A \cup B$ quanto em $A \cup C$, pela definição de $\cap$. E, pela definição de $\cup$, podemos desdobrar isso ainda mais em: ou $z \in A$ ou $z \in B$, e também ou $z \in A$ ou $z \in C$. Isso parece uma prova por casos de novo—exceto que o "e" a torna confusa. Você poderia pensar que isso equivale a haver três possibilidades: $z$ está ou em $A$, $B$ ou $C$. Mas isso seria um erro. Temos que ter cuidado, então vamos considerar cada disjunção por vez.

Pela definição de $\cap$, $z \in A \cup B$ e $z \in A \cup C$. Pela definição de $\cup$, $z \in A$ ou $z \in B$. Distinguimos casos.

> Como estamos nos concentrando na primeira disjunção, ainda não obtivemos nossa segunda disjunção (do desdobramento de $A \cup C$). De fato, ainda não precisamos dela. O primeiro caso é $z \in A$, e um membro de um conjunto é também um membro da união desse conjunto com qualquer outro. Então o caso 1 é fácil:

Caso 1: Suponha que $z \in A$. Segue-se que $z \in A \cup (B \cap C)$.

> Agora, para o segundo caso, $z \in B$. Aqui desdobraremos o segundo $\cup$ e faremos outra prova por casos:

Caso 2: Suponha que $z \in B$. Como $z \in A \cup C$, ou $z \in A$ ou $z \in C$. Distinguimos os casos ainda mais:

Caso 2a: $z \in A$. Então, novamente, $z \in A \cup (B \cap C)$.

> Ok, isso foi um pouco estranho. Na verdade, não precisamos da suposição de que $z \in B$ para este caso, mas tudo bem.

Caso 2b: $z \in C$. Então $z \in B$ e $z \in C$, de modo que $z \in B \cap C$, e consequentemente, $z \in A \cup (B \cap C)$.

> Isso conclui ambas as provas por casos, e assim terminamos a segunda metade.

Então, se $z \in (A \cup B) \cap (A \cup C)$, então $z \in A \cup (B \cap C)$. □

## 74.6 Outro Exemplo

**Proposição 74.9.** *Se $A \subseteq C$, então $A \cup (C \setminus A) = C$.*

*Prova.* Suponha que $A \subseteq C$. Queremos mostrar que $A \cup (C \setminus A) = C$.

> Começamos observando que esta é uma afirmação condicional. Ela está tacitamente quantificada universalmente: a proposição vale para todos os conjuntos $A$ e $C$. Assim, $A$ e $C$ são variáveis para conjuntos arbitrários. Para provar tal afirmação, supomos o antecedente e provamos o consequente.
>
> Continuamos usando a suposição de que $A \subseteq C$. Vamos desdobrar a definição de $\subseteq$: a suposição significa que todos os membros de $A$ são também membros de $C$. Vamos anotar isto—é um fato importante que usaremos ao longo da prova.

Pela definição de $\subseteq$, como $A \subseteq C$, para todo $z$, se $z \in A$, então $z \in C$.

> Desdobramos todas as definições que nos são dadas na suposição. Agora podemos passar à conclusão. Queremos mostrar que $A \cup (C \setminus A) = C$, e por isso montamos uma prova de modo semelhante ao último exemplo: mostramos que todo membro de $A \cup (C \setminus A)$ é também um membro de $C$ e, reciprocamente, todo membro de $C$ é um membro de $A \cup (C \setminus A)$. Podemos abreviar isso para: $A \cup (C \setminus A) \subseteq C$ e $C \subseteq A \cup (C \setminus A)$. (Aqui estamos fazendo o oposto de desdobrar uma definição, mas isso torna a prova um pouco mais fácil de ler.) Como isso é uma conjunção, temos que provar ambas as partes. Para mostrar a primeira parte, isto é, que todo membro de $A \cup (C \setminus A)$ é também um membro de $C$, supomos que $z \in A \cup (C \setminus A)$ para um $z$ arbitrário e mostramos que $z \in C$. Pela definição de $\cup$, podemos concluir que $z \in A$ ou $z \in C \setminus A$ a partir de $z \in A \cup (C \setminus A)$. Você já deve estar pegando o jeito disso.

$A \cup (C \setminus A) = C$ sse $A \cup (C \setminus A) \subseteq C$ e $C \subseteq (A \cup (C \setminus A)$. Primeiro provamos que $A \cup (C \setminus A) \subseteq C$. Seja $z \in A \cup (C \setminus A)$. Então, ou $z \in A$ ou $z \in (C \setminus A)$.

> Chegamos a uma disjunção, e a partir dela queremos provar que $z \in C$. Fazemos isso usando a prova por casos.

Caso 1: $z \in A$. Como, para todo $z$, se $z \in A$, $z \in C$, temos que $z \in C$.

> Aqui usamos o fato registrado anteriormente, que decorreu da hipótese da proposição de que $A \subseteq C$. O primeiro caso está completo, e passamos ao segundo caso, $z \in (C \setminus A)$. Lembre-se de que $C \setminus A$ denota a *diferença* dos dois conjuntos, isto é, o conjunto de todos os membros de $C$ que não são membros de $A$. Mas qualquer

> membro de $C$ que não esteja em $A$ é, em particular, um membro de $C$.

Caso 2: $z \in (C \setminus A)$. Isso significa que $z \in C$ e $z \notin A$. Então, em particular, $z \in C$.

> Ótimo, provamos a primeira direção. Agora a segunda direção. Aqui provamos que $C \subseteq A \cup (C \setminus A)$. Então supomos que $z \in C$ e provamos que $z \in A \cup (C \setminus A)$.

Agora seja $z \in C$. Queremos mostrar que $z \in A$ ou $z \in C \setminus A$.

> Como todos os membros de $A$ são também membros de $C$, e $C \setminus A$ é o conjunto de todas as coisas que são membros de $C$ mas não de $A$, segue-se que $z$ está ou em $A$ ou em $C \setminus A$. Isso pode ser um pouco obscuro se você ainda não souber por que o resultado é verdadeiro. Seria melhor prová-lo passo a passo. Ajudará usar um fato simples que podemos enunciar sem prova: $z \in A$ ou $z \notin A$. Isso é chamado de "princípio do terceiro excluído:" para qualquer afirmação $p$, ou $p$ é verdadeira ou sua negação é verdadeira. (Aqui, $p$ é a afirmação de que $z \in A$.) Como isso é uma disjunção, podemos novamente usar a prova por casos.

Ou $z \in A$ ou $z \notin A$. No primeiro caso, $z \in A \cup (C \setminus A)$. No segundo caso, $z \in C$ e $z \notin A$, de modo que $z \in C \setminus A$. Mas então $z \in A \cup (C \setminus A)$.

> Nossa prova está completa: mostramos que $A \cup (C \setminus A) = C$. □

## 74.7 Prova por Contradição

Em primeira instância, a prova por contradição é um padrão de inferência usado para provar afirmações negativas. Suponha que você queira mostrar que alguma afirmação $p$ é *falsa*, isto é, você quer mostrar $\neg p$. A estratégia mais promissora é (a) supor que $p$ é verdadeira, e (b) mostrar que essa suposição leva a algo que você sabe ser falso. "Algo que se sabe ser falso" pode ser um resultado que entra em conflito com—contradiz—o próprio $p$, ou alguma outra hipótese da afirmação geral que você está considerando. Por exemplo, uma prova de "se $q$ então $\neg p$" envolve supor que $q$ é verdadeira e provar $\neg p$ a partir disso. Se você prova $\neg p$ por contradição, isso significa supor $p$ além de $q$. Se você consegue provar $\neg q$ a partir de $p$, mostrou que a suposição $p$ leva a algo que contradiz sua outra suposição $q$, já que $q$ e $\neg q$ não podem ser ambas verdadeiras. É claro que você tem que usar outros padrões de inferência em sua prova da contradição, bem como desdobrar definições. Vamos considerar um exemplo.

**Proposição 74.10.** *Se $A \subseteq B$ e $B = \emptyset$, então $A$ não tem membros.*

*Prova.* Suponha $A \subseteq B$ e $B = \emptyset$. Queremos mostrar que $A$ não tem membros.

> Como esta é uma afirmação condicional, supomos o antecedente e queremos provar o consequente. O consequente é: $A$ não tem membros. Podemos tornar isso um pouco mais explícito: não é o caso de que haja um $x \in A$.

$A$ não tem membros sse não é o caso de que haja um $x$ tal que $x \in A$.

> Então determinamos que o que queremos provar é, na verdade, uma afirmação negativa $\neg p$, a saber: não é o caso de que haja um $x \in A$. Para usar a prova por contradição, temos que supor a afirmação positiva correspondente $p$, isto é, há um $x \in A$, e provar uma contradição a partir dela. Indicamos que estamos fazendo uma prova por contradição escrevendo "por absurdo, suponha" ou mesmo apenas "suponha que não," e então enunciamos a suposição $p$.

Suponha que não: há um $x \in A$.

> Esta é agora a nova suposição que usaremos para obter uma contradição. Temos mais duas suposições: que $A \subseteq B$ e que $B = \emptyset$. A primeira nos dá que $x \in B$:

Como $A \subseteq B$, $x \in B$.

> Mas como $B = \emptyset$, todo membro de $B$ (por exemplo, $x$) também deve ser um membro de $\emptyset$.

Como $B = \emptyset$, $x \in \emptyset$. Isso é uma contradição, já que, por definição, $\emptyset$ não tem membros.

> Isso já completa a prova: chegamos ao que precisávamos (uma contradição) a partir das suposições que montamos, e isso significa que as suposições não podem ser todas verdadeiras. Como as duas primeiras suposições ($A \subseteq B$ e $B = \emptyset$) não são contestadas, deve ser a última suposição introduzida (há um $x \in A$) que tem que ser falsa. Mas, se quisermos ser minuciosos, podemos explicitar isso.

Assim, nossa suposição de que há um $x \in A$ tem que ser falsa, logo, $A$ não tem membros, por prova por contradição. □

Toda afirmação positiva é trivialmente equivalente a uma afirmação negativa: $p$ sse $\neg\neg p$. Assim, as provas por contradição também podem ser usadas para estabelecer afirmações positivas "indiretamente," como segue: Para provar $p$, leia-o como a afirmação negativa $\neg\neg p$. Se conseguirmos provar uma

contradição a partir de $\neg p$, estabelecemos $\neg\neg p$ por prova por contradição, e portanto $p$.

No último exemplo, buscávamos provar uma afirmação negativa, a saber, que $A$ não tem membros, e por isso a suposição que fizemos para os fins da prova por contradição (isto é, que há um $x \in A$) era uma afirmação positiva. Ela nos deu algo com que trabalhar, a saber, o hipotético $x \in A$ sobre o qual continuamos a raciocinar até chegarmos a $x \in \emptyset$.

Ao provar uma afirmação positiva indiretamente, a suposição que você faria para os fins da prova por contradição seria negativa. Mas muito frequentemente você pode facilmente reformular uma afirmação positiva como uma afirmação negativa, e uma afirmação negativa como uma afirmação positiva. Nossa prova anterior teria sido essencialmente a mesma se tivéssemos provado "$A = \emptyset$" em vez do consequente negativo "$A$ não tem membros." (Pela definição de $=$, "$A = \emptyset$" é uma afirmação geral, já que ela se desdobra em "todo membro de $A$ é um membro de $\emptyset$ e vice-versa".) Mas é facilmente visto que ela é equivalente à afirmação negativa "não: há um $x \in A$."

Então, às vezes é mais fácil trabalhar com $\neg p$ como suposição do que provar $p$ diretamente. Mesmo quando uma prova direta é igualmente simples ou até mais simples (como nos próximos exemplos), algumas pessoas preferem proceder indiretamente. Se a dupla negação o confunde, pense em uma prova por contradição de alguma afirmação como uma prova de uma contradição a partir da afirmação *oposta*. Assim, uma prova por contradição de $\neg p$ é uma prova de uma contradição a partir da suposição $p$; e a prova por contradição de $p$ é uma prova de uma contradição a partir de $\neg p$.

**Proposição 74.11.** $A \subseteq A \cup B$.

*Prova.* Queremos mostrar que $A \subseteq A \cup B$.

> À primeira vista, esta é uma afirmação positiva: todo $x \in A$ está também em $A \cup B$. A negação disso é: algum $x \in A$ está $\notin A \cup B$. Então podemos provar a afirmação indiretamente supondo essa afirmação negada, e mostrando que ela leva a uma contradição.

Suponha que não, isto é, $A \nsubseteq A \cup B$.

> Temos uma definição de $A \subseteq A \cup B$: todo $x \in A$ está também $\in A \cup B$. Para entender o que $A \nsubseteq A \cup B$ significa, temos que usar alguma manipulação lógica elementar sobre a definição desdobrada: é falso que todo $x \in A$ esteja também $\in A \cup B$ sse há *algum* $x \in A$ que está $\notin C$. (Este é um ponto em que você quer ser muito cuidadoso: muitas tentativas de prova por contradição de estudantes falham porque eles analisam a negação de uma afirmação como "todos os $A$ são $B$" incorretamente.) Em outras palavras, $A \nsubseteq A \cup B$ sse há um $x$ tal que $x \in A$ e $x \notin A \cup B$. A partir daí, é fácil.

Então, há um $x \in A$ tal que $x \notin A \cup B$. Pela definição de $\cup$, $x \in A \cup B$ sse $x \in A$ ou $x \in B$. Como $x \in A$, temos $x \in A \cup B$. Isso contradiz a suposição de que $x \notin A \cup B$. □

**Proposição 74.12.** *Se $A \subseteq B$ e $B \subseteq C$ então $A \subseteq C$.*

*Prova.* Suponha $A \subseteq B$ e $B \subseteq C$. Queremos mostrar $A \subseteq C$.

> Vamos proceder indiretamente: supomos a negação do que queremos estabelecer.

Suponha que não, isto é, $A \nsubseteq C$.

> Como antes, raciocinamos que $A \nsubseteq C$ sse nem todo $x \in A$ está também $\in C$, isto é, algum $x \in A$ está $\notin C$. Não se preocupe, com prática você não terá mais que pensar muito para desdobrar negações como esta.

Em outras palavras, há um $x$ tal que $x \in A$ e $x \notin C$.

> Agora podemos usar isso para chegar à nossa contradição. É claro que teremos que usar as outras duas suposições para fazê-lo.

Como $A \subseteq B$, $x \in B$. Como $B \subseteq C$, $x \in C$. Mas isso contradiz $x \notin C$. □

**Proposição 74.13.** *Se $A \cup B = A \cap B$ então $A = B$.*

*Prova.* Suponha $A \cup B = A \cap B$. Queremos mostrar que $A = B$.

> O começo é agora rotineiro:

Suponha, por absurdo, que $A \neq B$.

> Nossa suposição para a prova por contradição é que $A \neq B$. Como $A = B$ sse $A \subseteq B$ e $B \subseteq A$, obtemos que $A \neq B$ sse $A \nsubseteq B$ *ou* $B \nsubseteq A$. (Note como é importante ter cuidado ao manipular negações!) Para provar uma contradição a partir dessa disjunção, usamos uma prova por casos e mostramos que, em cada caso, uma contradição se segue.

$A \neq B$ sse $A \nsubseteq B$ ou $B \nsubseteq A$. Distinguimos casos.

> No primeiro caso, supomos $A \nsubseteq B$, isto é, para algum $x$, $x \in A$ mas $\notin B$. $A \cap B$ é definido como aqueles membros que $A$ e $B$ têm em comum, então, se algo não está em um deles, não está na interseção. $A \cup B$ é $A$ junto com $B$, então qualquer coisa em um ou outro está também na união. Isso nos diz que $x \in A \cup B$ mas $x \notin A \cap B$, e logo que $A \cap B \neq A \cup B$.

Caso 1: $A \not\subseteq B$. Então, para algum $x$, $x \in A$ mas $x \notin B$. Como $x \notin B$, então $x \notin A \cap B$. Como $x \in A$, $x \in A \cup B$. Então, $A \cap B \neq A \cup B$, contradizendo a suposição de que $A \cap B = A \cup B$.

Caso 2: $B \not\subseteq A$. Então, para algum $y$, $y \in B$ mas $y \notin A$. Como antes, temos $y \in A \cup B$ mas $y \notin A \cap B$, e assim $A \cap B \neq A \cup B$, novamente contradizendo $A \cap B = A \cup B$. □

## 74.8 Lendo Provas

As provas que você encontra em livros-texto e artigos muito raramente fornecem todos os detalhes que incluímos até agora em nossos exemplos. Os autores frequentemente não chamam a atenção para quando distinguem casos, quando dão uma prova indireta, ou não mencionam que usam uma definição. Assim, quando você lê uma prova em um livro-texto, muitas vezes terá de preencher esses detalhes por conta própria para entender a prova. Fazer isso também é um bom exercício para pegar o jeito dos vários passos que você tem de dar em uma prova. Vejamos um exemplo.

**Proposição 74.14 (Absorção).** *Para todos os conjuntos $A$, $B$,*

$$A \cap (A \cup B) = A$$

*Prova.* Se $z \in A \cap (A \cup B)$, então $z \in A$, logo $A \cap (A \cup B) \subseteq A$. Agora suponha $z \in A$. Então também $z \in A \cup B$, e portanto também $z \in A \cap (A \cup B)$. □

A prova precedente da lei da absorção é muito condensada. Não há menção a quaisquer definições usadas, nenhum "temos de provar que" antes de prová-lo, etc. Vamos desempacotá-la. A proposição provada é uma afirmação geral sobre quaisquer conjuntos $A$ e $B$, e quando a prova menciona $A$ ou $B$, estes são variáveis para conjuntos arbitrários. As afirmações gerais que a prova estabelece são o que se exige para provar a identidade de conjuntos, isto é, que todo membro do lado esquerdo da identidade é um membro do direito e vice-versa.

"Se $z \in A \cap (A \cup B)$, então $z \in A$, logo $A \cap (A \cup B) \subseteq A$."

Esta é a primeira metade da prova da identidade: ela estabelece que, se um $z$ arbitrário é um membro do lado esquerdo, ele também é um membro do direito, isto é, $A \cap (A \cup B) \subseteq A$. Assuma que $z \in A \cap (A \cup B)$. Como $z$ é um membro da interseção de dois conjuntos se, e somente se, é um membro de ambos os conjuntos, podemos concluir que $z \in A$ e também $z \in A \cup B$. Em particular, $z \in A$, que é o que queríamos mostrar. Como isso é tudo o que precisa ser feito para a primeira metade, sabemos que o restante da prova deve ser uma prova da segunda metade, isto é, uma prova de que $A \subseteq A \cap (A \cup B)$.

> "Agora suponha $z \in A$. Então também $z \in A \cup B$, e portanto também $z \in A \cap (A \cup B)$."

Começamos assumindo que $z \in A$, já que estamos mostrando que, para qualquer $z$, se $z \in A$ então $z \in A \cap (A \cup B)$. Para mostrar que $z \in A \cap (A \cup B)$, temos de mostrar (pela definição de "$\cap$") que (i) $z \in A$ e também (ii) $z \in A \cup B$. Aqui (i) é justamente nossa suposição, então não há mais nada a provar, e é por isso que a prova não a menciona novamente. Para (ii), lembre-se de que $z$ é um membro de uma união de conjuntos se, e somente se, é um membro de pelo menos um desses conjuntos. Como $z \in A$, e $A \cup B$ é a união de $A$ e $B$, este é o caso aqui. Então $z \in A \cup B$. Mostramos ambos (i) $z \in A$ e (ii) $z \in A \cup B$, logo, pela definição de "$\cap$," $z \in A \cap (A \cup B)$. A prova não menciona essas definições; presume-se que o leitor já as tenha internalizado. Se você não as internalizou, terá de voltar e relembrar quais são. Então também terá de reconhecer por que decorre de $z \in A$ que $z \in A \cup B$, e de $z \in A$ e $z \in A \cup B$ que $z \in A \cap (A \cup B)$.

Eis outra versão da prova acima, com tudo tornado explícito:

*Prova.* [Pela definição de $=$ para conjuntos, $A \cap (A \cup B) = A$, temos de mostrar (a) $A \cap (A \cup B) \subseteq A$ e (b) $A \cap (A \cup B) \subseteq A$. (a): Pela definição de $\subseteq$, temos de mostrar que se $z \in A \cap (A \cup B)$, então $z \in A$.] Se $z \in A \cap (A \cup B)$, então $z \in A$ [já que pela definição de $\cap$, $z \in A \cap (A \cup B)$ se, e somente se, $z \in A$ e $z \in A \cup B$], logo $A \cap (A \cup B) \subseteq A$. [(b): Pela definição de $\subseteq$, temos de mostrar que se $z \in A$, então $z \in A \cap (A \cup B)$.] Agora suponha [(1)] $z \in A$. Então também [(2)] $z \in A \cup B$ [já que por (1) $z \in A$ ou $z \in B$, o que pela definição de $\cup$ significa $z \in A \cup B$], e portanto também $z \in A \cap (A \cup B)$ [já que a definição de $\cap$ requer que $z \in A$, isto é, (1), e $z \in A \cup B$), isto é, (2)]. □

## 74.9 Não Consigo Fazer Isso!

Todos nós chegamos a um ponto em que sentimos vontade de desistir. Mas você *consegue* fazer isso. Seu professor e o monitor, bem como seus colegas, podem ajudar. Peça ajuda a eles! Aqui estão algumas dicas para ajudá-lo a evitar uma crise, e o que fazer se você sentir vontade de desistir.

Para garantir que você consiga resolver os problemas com sucesso, faça o seguinte:

1. *Comece com a maior antecedência possível.* Ficamos ocupados ao longo do semestre e muitos de nós lutam com a procrastinação; uma das melhores coisas que você pode fazer é começar as tarefas de casa cedo. Dessa forma, se você travar, terá tempo para procurar uma solução (que não seja chorar).

2. *Converse com seus colegas de turma.* Você não está sozinho. Outros na turma também podem ter dificuldades—mas podem ter dificuldades

com coisas diferentes. Conversar sobre o assunto com seus colegas pode lhe dar uma perspectiva diferente sobre o problema que pode levar a um avanço. É claro, não copie simplesmente a solução deles: peça uma dica, ou explique onde você travou e peça o próximo passo. E quando você conseguir, retribua. Ajudar outra pessoa, e explicar as coisas, ajudará você a entender melhor também.

3. *Peça ajuda.* Você tem muitos recursos à sua disposição—seu professor e o monitor estão lá por você e *querem* que você tenha sucesso. Eles devem ser capazes de ajudá-lo a resolver um problema e identificar em que ponto do processo você está com dificuldade.

4. *Faça uma pausa.* Se você travar, *pode* ser porque ficou olhando para o problema por tempo demais. Faça uma pausa curta, tome uma xícara de chá, ou trabalhe em um problema diferente por um tempo, depois volte ao problema com a mente renovada. Durma sobre o assunto.

Percebe como essas estratégias exigem que você tenha começado a trabalhar na prova com bastante antecedência? Se você começou a prova às 2 da madrugada do dia anterior à entrega, elas talvez não sejam tão úteis.

Isso pode soar como pessimismo e desgraça, mas resolver uma prova é um desafio que compensa no final. Algumas pessoas fazem isso como profissão—portanto deve haver algo de prazeroso nisso. Como praticamente tudo, resolver problemas e fazer provas é algo que exige prática. Você pode ver colegas que acham isso fácil: provavelmente eles apenas já tiveram muita prática. Tente não ceder com facilidade demais.

Se você ficar mesmo sem tempo (ou sem paciência) em um problema específico: tudo bem. Isso não significa que você seja burro ou que nunca vá conseguir. Descubra (com seu professor ou outro estudante) como se faz, e identifique onde você errou ou travou, para poder evitar fazer isso da próxima vez que encontrar uma questão semelhante. Depois tente fazê-lo sem olhar a solução. E na próxima vez, comece (e peça ajuda) mais cedo.

## 74.10 Outros Recursos

Há muitos livros sobre como fazer provas em matemática que podem ser úteis. Confira em particular *How to Read and do Proofs: An Introduction to Mathematical Thought Processes* (Solow, 2013) e *How to Prove It: A Structured Approach* (Velleman, 2019). O *Book of Proof* (Hammack, 2013) e o *Mathematical Reasoning* (Sandstrum, 2019) são livros sobre provas que estão disponíveis gratuitamente online. Filósofos podem achar *More Precisely: The Math you need to do Philosophy* (Steinhart, 2018) uma boa introdução ao raciocínio matemático.

Há também vários guias mais curtos sobre provas disponíveis na internet; por exemplo, "Introduction to Mathematical Arguments" (Hutchings, 2003) e "How to write proofs" (Cheng, 2004).

### Vídeos Motivacionais

Sente que não tem motivação para fazer sua tarefa de casa? Desanimado? Estes vídeos podem ajudar!

- https://www.youtube.com/watch?v=ZXsQAXx_ao0
- https://www.youtube.com/watch?v=BQ4yd2W50No
- https://www.youtube.com/watch?v=StTqXEQ2l-Y

## Problemas

**Problema 74.1.** Suponha que lhe peçam para provar que $A \cap B \neq \emptyset$. Desdobre todas as definições que ocorrem aqui, isto é, reenuncie isto de um modo que não mencione "$\cap$", "=", ou "$\emptyset$".

**Problema 74.2.** Prove *indiretamente* que $A \cap B \subseteq A$.

**Problema 74.3.** Expanda a seguinte prova de $A \cup (A \cap B) = A$, mencionando todos os padrões de inferência usados, por que cada passo decorre de suposições ou afirmações estabelecidas antes dele, e onde temos de apelar para quais definições.

*Prova.* Se $z \in A \cup (A \cap B)$ então $z \in A$ ou $z \in A \cap B$. Se $z \in A \cap B$, $z \in A$. Qualquer $z \in A$ está também $\in A \cup (A \cap B)$. □

# Capítulo 75

# Indução

## 75.1 Introdução

A indução é uma técnica de prova importante, usada, em diferentes formas, em quase todas as áreas da lógica, da ciência da computação teórica e da matemática. Ela é necessária para provar muitos dos resultados em lógica.

A indução é frequentemente contrastada com a dedução, e caracterizada como a inferência do particular para o geral. Por exemplo, se observamos muitas esmeraldas verdes, e nada que chamaríamos de esmeralda que não seja verde, poderíamos concluir que todas as esmeraldas são verdes. Essa é uma inferência indutiva, no sentido de que procede de muitos casos particulares (esta esmeralda é verde, aquela esmeralda é verde, etc.) a uma afirmação geral (todas as esmeraldas são verdes). A indução *matemática* também é uma inferência que conclui uma afirmação geral, mas é de um tipo muito diferente dessa "indução simples."

De modo bem aproximado, uma prova indutiva em matemática conclui que todos os objetos matemáticos de certo tipo têm uma certa propriedade. No caso mais simples, os objetos matemáticos com que uma prova indutiva se ocupa são os números naturais. Nesse caso, uma prova indutiva é usada para estabelecer que todos os números naturais têm alguma propriedade, e faz isso mostrando que

1. 0 tem a propriedade, e

2. sempre que um número $k$ tem a propriedade, também $k + 1$ a tem.

A indução sobre os números naturais pode então, também, ser frequentemente usada para provar afirmações gerais sobre objetos matemáticos aos quais se podem atribuir números. Por exemplo, conjuntos finitos têm, cada um, um número finito $n$ de elementos, e se pudermos usar a indução para mostrar que todo número $n$ tem a propriedade "todos os conjuntos finitos de

tamanho $n$ são ..." então teremos mostrado algo sobre todos os conjuntos finitos.

A indução também pode ser generalizada para objetos matemáticos que são *definidos indutivamente*. Por exemplo, as expressões de uma linguagem formal, como as da lógica de primeira ordem, são definidas indutivamente. A *indução estrutural* é um modo de provar resultados sobre todas essas expressões. A indução estrutural, em particular, é muito útil—e amplamente usada—em lógica.

## 75.2 Indução em $\mathbb{N}$

Em sua forma mais simples, a indução é uma técnica usada para provar resultados para todos os números naturais. Ela usa o fato de que, começando em 0 e somando 1 repetidamente, eventualmente alcançamos todo número natural. Assim, para provar que algo é verdadeiro para todo número, podemos (1) estabelecer que é verdadeiro para 0 e (2) mostrar que, sempre que é verdadeiro para um número $n$, também é verdadeiro para o número seguinte $n + 1$. Se abreviarmos "o número $n$ tem a propriedade $P$" por $P(n)$ (e "o número $k$ tem a propriedade $P$" por $P(k)$, etc.), então uma prova por indução de que $P(n)$ para todo $n \in \mathbb{N}$ consiste em:

1. uma prova de $P(0)$, e

2. uma prova de que, para qualquer $k$, se $P(k)$ então $P(k + 1)$.

Para deixar isso bem claro, suponha que tenhamos tanto (1) quanto (2). Então (1) nos diz que $P(0)$ é verdadeiro. Se também tivermos (2), sabemos em particular que, se $P(0)$, então $P(0 + 1)$, isto é, $P(1)$. Isso decorre da afirmação geral "para qualquer $k$, se $P(k)$ então $P(k + 1)$" ao pôr 0 no lugar de $k$. Então, por modus ponens, temos que $P(1)$. De (2) novamente, agora tomando 1 por $n$, temos: se $P(1)$ então $P(2)$. Como acabamos de estabelecer $P(1)$, por modus ponens, temos $P(2)$. E assim por diante. Para qualquer número $n$, depois de fazer isso $n$ vezes, eventualmente chegamos a $P(n)$. Então (1) e (2) juntos estabelecem $P(n)$ para qualquer $n \in \mathbb{N}$.

Vejamos um exemplo. Suponha que queiramos descobrir quantas somas diferentes podemos lançar com $n$ dados. Embora possa parecer bobo, vamos começar com 0 dados. Se você não tem dados, há apenas uma soma possível que você pode "lançar": nenhum ponto, que soma 0. Assim, o número de lançamentos possíveis diferentes é 1. Se você tem apenas um dado, isto é, $n = 1$, há seis valores possíveis, de 1 a 6. Com dois dados, podemos lançar qualquer soma de 2 a 12, ou seja, 11 possibilidades. Com três dados, podemos lançar qualquer número de 3 a 18, isto é, 16 possibilidades diferentes. 1, 6, 11, 16: parece um padrão: talvez a resposta seja $5n + 1$? É claro que $5n + 1$ é o máximo possível, pois há apenas $5n + 1$ números entre $n$, o menor valor que

você pode lançar com $n$ dados (todos 1) e $6n$, o maior que você pode lançar (todos 6).

**Teorema 75.1.** *Com n dados pode-se lançar todos os* $5n + 1$ *valores possíveis entre n e* $6n$*.*

*Prova.* Seja $P(n)$ a afirmação: "É possível lançar qualquer número entre $n$ e $6n$ usando $n$ dados." Para usar a indução, provamos:

1. A *base da indução* $P(1)$, isto é, com apenas um dado, você pode lançar qualquer número entre 1 e 6.

2. O *passo da indução*, para todo $k$, se $P(k)$ então $P(k + 1)$.

(1) é provado inspecionando um dado de 6 lados. Ele tem todos os 6 lados, e todo número entre 1 e 6 aparece em um dos lados. Então é possível lançar qualquer número entre 1 e 6 usando um único dado.

Para provar (2), supomos o antecedente do condicional, isto é, $P(k)$. Essa suposição é chamada de *hipótese indutiva*. Nós a usamos para provar $P(k + 1)$. A parte difícil é encontrar um modo de pensar sobre os valores possíveis de um lançamento de $k + 1$ dados em termos dos valores possíveis de lançamentos de $k$ dados, somados aos lançamentos do dado extra, o $(k + 1)$-ésimo—é isso, porém, que temos que fazer, se quisermos usar a hipótese indutiva.

A hipótese indutiva diz que podemos obter qualquer número entre $k$ e $6k$ usando $k$ dados. Se lançamos um 1 com nosso $(k + 1)$-ésimo dado, isso acrescenta 1 ao total. Então podemos lançar qualquer valor entre $k + 1$ e $6k + 1$ lançando $k$ dados e depois rolando um 1 com o $(k + 1)$-ésimo dado. O que falta? Os valores de $6k + 2$ a $6k + 6$. Podemos obtê-los rolando $k$ dados em 6 e depois um número entre 2 e 6 com nosso $(k + 1)$-ésimo dado. Juntos, isso significa que, com $k + 1$ dados, podemos lançar qualquer um dos números entre $k + 1$ e $6(k + 1)$, isto é, provamos $P(k + 1)$ usando a suposição $P(k)$, a hipótese indutiva. □

Muito frequentemente usamos a indução quando queremos provar algo sobre uma série de objetos (números, conjuntos, etc.) que é, ela própria, definida "indutivamente," isto é, definindo o $(n + 1)$-ésimo objeto em termos do $n$-ésimo. Por exemplo, podemos definir a soma $s_n$ dos números naturais até $n$ por

$$s_0 = 0$$
$$s_{n+1} = s_n + (n + 1)$$

Esta definição dá:

$$\begin{aligned} s_0 &= 0, \\ s_1 &= s_0 + 1 && = 1, \\ s_2 &= s_1 + 2 && = 1 + 2 = 3 \\ s_3 &= s_2 + 3 && = 1 + 2 + 3 = 6, \text{ etc.} \end{aligned}$$

Agora podemos provar, por indução, que $s_n = n(n+1)/2$.

**Proposição 75.2.** *$s_n = n(n+1)/2$.*

*Prova.* Temos que provar (1) que $s_0 = 0 \cdot (0+1)/2$ e (2) se $s_k = k(k+1)/2$ então $s_{k+1} = (k+1)(k+2)/2$. (1) é óbvio. Para provar (2), supomos a hipótese indutiva: $s_k = k(k+1)/2$. Usando-a, temos que mostrar que $s_{k+1} = (k+1)(k+2)/2$.

O que é $s_{k+1}$? Pela definição, $s_{k+1} = s_k + (k+1)$. Pela hipótese indutiva, $s_k = k(k+1)/2$. Podemos substituir isso na equação anterior, e então só precisamos de um pouco de aritmética de frações:

$$\begin{aligned} s_{k+1} &= \frac{k(k+1)}{2} + (k+1) = \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \\ &= \frac{k(k+1) + 2(k+1)}{2} = \\ &= \frac{(k+2)(k+1)}{2}. \end{aligned}$$

□

A lição importante aqui é que, se você está provando algo sobre alguma sequência definida indutivamente $a_n$, a indução é o caminho óbvio a seguir. E, mesmo quando não é (como no caso das possibilidades de lançamentos de dados), você pode usar a indução se conseguir, de alguma forma, relacionar o caso para $k+1$ ao caso para $k$.

## 75.3 Indução Forte

No princípio de indução discutido acima, provamos $P(0)$ e também que, se $P(k)$, então $P(k+1)$. Na segunda parte, assumimos que $P(k)$ é verdadeiro e usamos essa suposição para provar $P(k+1)$. De forma equivalente, é claro, poderíamos assumir $P(k-1)$ e usá-la para provar $P(k)$—o importante é que sejamos capazes de realizar a inferência de qualquer número para seu sucessor; que possamos provar a afirmação em questão para qualquer número sob a suposição de que ela vale para seu antecessor.

Há uma variante do princípio de indução em que não apenas assumimos que a afirmação vale para o antecessor $k-1$ de $k$, mas para todos os números

menores que $k$, e usamos essa suposição para estabelecer a afirmação para $k$. Isso também nos dá a afirmação $P(n)$ para todo $n \in \mathbb{N}$. Pois, uma vez que tenhamos estabelecido $P(0)$, teremos com isso estabelecido que $P$ vale para todos os números menores que 1. E se sabemos que, se $P(l)$ para todo $l < k$, então $P(k)$, sabemos isso em particular para $k = 1$. Então podemos concluir $P(1)$. Com isso provamos $P(0)$ e $P(1)$, isto é, $P(l)$ para todo $l < 2$, e como temos também o condicional, se $P(l)$ para todo $l < 2$, então $P(2)$, podemos concluir $P(2)$, e assim por diante.

De fato, se conseguirmos estabelecer o condicional geral "para todo $k$, se $P(l)$ para todo $l < k$, então $P(k)$," não temos mais de estabelecer $P(0)$, já que ele decorre disso. Pois lembre-se de que uma afirmação geral como "para todo $l < k$, $P(l)$" é verdadeira se não houver nenhum $l < k$. Este é um caso de quantificação vazia: "todos os $A$s são $B$s" é verdadeiro se não houver nenhum $A$, $\forall x\,(\varphi(x) \to \psi(x))$ é verdadeiro se nenhum $x$ satisfaz $\varphi(x)$. Neste caso, a versão formalizada seria "$\forall l\,(l < k \to P(l))$"—e isso é verdadeiro se não houver nenhum $l < k$. E se $k = 0$ esse é exatamente o caso: não há nenhum $l < 0$, logo "para todo $l < 0$, $P(0)$" é verdadeiro, qualquer que seja $P$. Uma prova de "se $P(l)$ para todo $l < k$, então $P(k)$" estabelece assim automaticamente $P(0)$.

Esta variante é útil se estabelecer a afirmação para $k$ não puder ser feito de modo a apenas se apoiar na afirmação para $k - 1$, mas puder exigir a suposição de que ela é verdadeira para um ou mais $l < k$.

## 75.4 Definições Indutivas

Em lógica, muito frequentemente definimos tipos de objetos *indutivamente*, isto é, especificando regras para o que conta como um objeto do tipo a ser definido, que explicam como obter novos objetos desse tipo a partir de objetos antigos desse tipo. Por exemplo, frequentemente definimos tipos especiais de sequências de símbolos, como os termos e fórmulas de uma linguagem, por indução. Para um exemplo simples, considere cadeias compostas das letras a, b, c, d, do símbolo $\circ$, e dos colchetes [ e ], como "[[c $\circ$ d][", "[a[]$\circ$]", "a" ou "[[a $\circ$ b] $\circ$ d]". Você provavelmente sente que há algo "errado" com as duas primeiras cadeias: os colchetes não "se equilibram" de modo algum na primeira, e você pode sentir que o "$\circ$" deveria "conectar" expressões que elas próprias façam sentido. A terceira e a quarta cadeia parecem melhores: para todo "[" há um "]" de fechamento (se houver algum), e para qualquer $\circ$ podemos encontrar expressões "bonitas" de cada lado, cercadas por um par de parênteses.

Gostaríamos de especificar precisamente o que conta como um "termo bonito." Em primeiro lugar, toda letra isolada é bonita. Qualquer coisa que não seja apenas uma letra isolada deve ser da forma "$[t \circ s]$" em que $s$ e $t$ são, eles próprios, bonitos. Reciprocamente, se $t$ e $s$ são bonitos, então podemos formar um novo termo bonito pondo um $\circ$ entre eles e cercando-os por um

par de colchetes. Poderíamos usar essas operações para *definir* o conjunto dos termos bonitos. Esta é uma *definição indutiva*.

**Definição 75.3 (Termos bonitos).** O conjunto dos *termos bonitos* é definido indutivamente como segue:

1. Qualquer letra a, b, c, d é um termo bonito.
2. Se $s_1$ e $s_2$ são termos bonitos, então também o é $[s_1 \circ s_2]$.
3. Nada mais é um termo bonito.

Esta definição nos diz que algo conta como um termo bonito sse ele pode ser construído de acordo com as duas condições (1) e (2) em algum número finito de passos. No primeiro passo, construímos todos os termos bonitos compostos apenas por letras isoladas, isto é,

$$\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}$$

No segundo passo, aplicamos (2) aos termos que construímos. Obteremos

$$[\mathrm{a} \circ \mathrm{a}], [\mathrm{a} \circ \mathrm{b}], [\mathrm{b} \circ \mathrm{a}], \ldots, [\mathrm{d} \circ \mathrm{d}]$$

para todas as combinações de duas letras. No terceiro passo, aplicamos (2) novamente, a quaisquer dois termos bonitos que construímos até agora. Obtemos novos termos bonitos como $[\mathrm{a} \circ [\mathrm{a} \circ \mathrm{a}]]$—em que $t$ é a do passo 1 e $s$ é $[\mathrm{a} \circ \mathrm{a}]$ do passo 2—e $[[\mathrm{b} \circ \mathrm{c}] \circ [\mathrm{d} \circ \mathrm{b}]]$ construído a partir dos dois termos $[\mathrm{b} \circ \mathrm{c}]$ e $[\mathrm{d} \circ \mathrm{b}]$ do passo 2. E assim por diante. A cláusula (3) impede que qualquer coisa não construída desse modo se infiltre no conjunto dos termos bonitos.

Note que ainda não provamos que toda sequência de símbolos que "parece" bonita é bonita de acordo com esta definição. No entanto, deve ficar claro que tudo o que podemos construir de fato "parece bonito": os colchetes estão equilibrados, e $\circ$ conecta partes que são, elas próprias, bonitas.

A característica-chave das definições indutivas é que, se você quer provar algo sobre todos os termos bonitos, a definição lhe diz quais casos você deve considerar. Por exemplo, se lhe é dito que $t$ é um termo bonito, a definição indutiva lhe diz com o que $t$ pode se parecer: $t$ pode ser uma letra, ou pode ser $[s_1 \circ s_2]$ para algum par de termos bonitos $s_1$ e $s_2$. Por causa da cláusula (3), essas são as únicas possibilidades.

Ao provar afirmações sobre todo um conjunto definido indutivamente, a forma forte da indução torna-se particularmente importante. Por exemplo, suponha que queiramos provar que, para todo termo bonito de comprimento $n$, o número de [ nele é $< n/2$. Isso pode ser visto como uma afirmação sobre todos os $n$: para todo $n$, o número de [ em qualquer termo bonito de comprimento $n$ é $< n/2$.

**Proposição 75.4.** *Para qualquer $n$, o número de [ em um termo bonito de comprimento $n$ é $< n/2$.*

*Prova.* Para provar esse resultado por indução (forte), temos que mostrar que a seguinte afirmação condicional é verdadeira:

> Se, para todo $l < k$, qualquer termo bonito de comprimento $l$ tem $< l/2$ [, então qualquer termo bonito de comprimento $k$ tem $< k/2$ [.

Para mostrar este condicional, suponha que seu antecedente é verdadeiro, isto é, suponha que, para qualquer $l < k$, termos bonitos de comprimento $l$ contêm $< l/2$ [. Chamamos essa suposição de hipótese indutiva. Queremos mostrar que o mesmo vale para termos bonitos de comprimento $k$.

Então suponha que $t$ é um termo bonito de comprimento $k$. Como os termos bonitos são definidos indutivamente, temos dois casos: (1) $t$ é uma letra isolada, ou (2) $t$ é $[s_1 \circ s_2]$ para alguns termos bonitos $s_1$ e $s_2$.

1. $t$ é uma letra. Então $k = 1$, e o número de [ em $t$ é 0. Como $0 < 1/2$, a afirmação vale.

2. $t$ é $[s_1 \circ s_2]$ para alguns termos bonitos $s_1$ e $s_2$. Sejam $l_1$ o comprimento de $s_1$ e $l_2$ o comprimento de $s_2$. Então o comprimento $k$ de $t$ é $l_1 + l_2 + 3$ (os comprimentos de $s_1$ e $s_2$ mais três símbolos [, ∘, ]). Como $l_1 + l_2 + 3$ é sempre maior que $l_1$, $l_1 < k$. De modo semelhante, $l_2 < k$. Isso significa que a hipótese de indução se aplica aos termos $s_1$ e $s_2$: o número $m_1$ de [ em $s_1$ é $< l_1/2$, e o número $m_2$ de [ em $s_2$ é $< l_2/2$.

   O número de [ em $t$ é o número de [ em $s_1$, mais o número de [ em $s_2$, mais 1, isto é, é $m_1 + m_2 + 1$. Como $m_1 < l_1/2$ e $m_2 < l_2/2$, temos:

$$m_1 + m_2 + 1 < \frac{l_1}{2} + \frac{l_2}{2} + 1 = \frac{l_1 + l_2 + 2}{2} < \frac{l_1 + l_2 + 3}{2} = k/2.$$

Em cada caso, mostramos que o número de [ em $t$ é $< k/2$ (com base na hipótese indutiva). Por indução forte, a proposição se segue. □

## 75.5 Indução Estrutural

Até aqui usamos a indução para estabelecer resultados sobre todos os números naturais. Mas um princípio correspondente pode ser usado diretamente para provar resultados sobre todos os membros de um conjunto definido indutivamente. Isso é frequentemente chamado de indução *estrutural*, porque depende da estrutura dos objetos definidos indutivamente.

Em geral, uma definição indutiva é dada por (a) uma lista de membros "iniciais" do conjunto e (b) uma lista de operações que produzem novos membros do conjunto a partir de antigos. No caso dos termos bonitos, por exemplo, os objetos iniciais são as letras. Temos apenas uma operação: as operações são

$$o(s_1, s_2) = [s_1 \circ s_2]$$

Você pode até pensar nos próprios números naturais $\mathbb{N}$ como sendo dados por uma definição indutiva: o objeto inicial é 0, e a operação é a função sucessor $x + 1$.

Para provar algo sobre todos os elementos de um conjunto definido indutivamente, isto é, que todo membro do conjunto tem uma propriedade $P$, devemos:

1. Provar que os objetos iniciais têm $P$
2. Provar que, para cada operação $o$, se os argumentos têm $P$, o resultado também tem.

Por exemplo, para provar algo sobre todos os termos bonitos, nós provaríamos que é verdadeiro para todas as letras, e que é verdadeiro para $[s_1 \circ s_2]$ desde que seja verdadeiro de $s_1$ e $s_2$ individualmente.

**Proposição 75.5.** *O número de* [ *é igual ao número de* ] *em qualquer termo bonito $t$.*

*Prova.* Usamos a indução estrutural. Os termos bonitos são definidos indutivamente, com as letras como objetos iniciais e a operação $o$ para construir novos termos bonitos a partir de antigos.

1. A afirmação é verdadeira para toda letra, já que o número de [ em uma letra isolada é 0 e o número de ] nela também é 0.
2. Suponha que o número de [ em $s_1$ é igual ao número de ], e o mesmo é verdadeiro para $s_2$. O número de [ em $o(s_1, s_2)$, isto é, em $[s_1 \circ s_2]$, é a soma do número de [ em $s_1$ e $s_2$ mais um. O número de ] em $o(s_1, s_2)$ é a soma do número de ] em $s_1$ e $s_2$ mais um. Assim, o número de [ em $o(s_1, s_2)$ é igual ao número de ] em $o(s_1, s_2)$. □

Vamos dar outra prova por indução estrutural: um segmento inicial próprio de uma cadeia $t$ de símbolos é qualquer cadeia $s$ que concorda com $t$ símbolo por símbolo, lida da esquerda, mas $t$ é mais longa. Assim, por exemplo, $[a \circ$ é um segmento inicial próprio de $[a \circ b]$, mas nem $[b \circ$ (discordam no segundo símbolo) nem $[a \circ b]$ (têm o mesmo comprimento) o são.

**Proposição 75.6.** *Todo segmento inicial próprio de um termo bonito $t$ tem mais* [ *do que* ].

*Prova.* Por indução em $t$:

1. $t$ é uma letra isolada: Então $t$ não tem segmentos iniciais próprios.
2. $t = [s_1 \circ s_2]$ para alguns termos bonitos $s_1$ e $s_2$. Se $r$ é um segmento inicial próprio de $t$, há várias possibilidades:
   a) $r$ é apenas $[$: Então $r$ tem um $[$ a mais do que $]$.
   b) $r$ é $[r_1$ em que $r_1$ é um segmento inicial próprio de $s_1$: Como $s_1$ é um termo bonito, por hipótese de indução, $r_1$ tem mais $[$ do que $]$, e o mesmo é verdadeiro para $[r_1$.
   c) $r$ é $[s_1$ ou $[s_1 \circ$: Pelo resultado anterior, o número de $[$ e $]$ em $s_1$ é igual; então o número de $[$ em $[s_1$ ou $[s_1 \circ$ é um a mais do que o número de $]$.
   d) $r$ é $[s_1 \circ r_2$ em que $r_2$ é um segmento inicial próprio de $s_2$: Por hipótese de indução, $r_2$ contém mais $[$ do que $]$. Pelo resultado anterior, o número de $[$ e de $]$ em $s_1$ é igual. Então o número de $[$ em $[s_1 \circ r_2$ é maior do que o número de $]$.
   e) $r$ é $[s_1 \circ s_2$: Pelo resultado anterior, o número de $[$ e $]$ em $s_1$ é igual, e o mesmo para $s_2$. Então há um $[$ a mais em $[s_1 \circ s_2$ do que há $]$. □

## 75.6 Relações e Funções

Quando definimos um conjunto de objetos (como os números naturais ou os termos bonitos) indutivamente, também podemos definir *relações sobre* esses objetos por indução. Por exemplo, considere a seguinte ideia: um termo bonito $t_1$ é um subtermo de um termo bonito $t_2$ se ocorre como parte dele. Vamos usar um símbolo para isso: $t_1 \sqsubseteq t_2$. Todo termo bonito é, é claro, um subtermo de si mesmo: $t \sqsubseteq t$. Podemos dar uma definição indutiva dessa relação como segue:

**Definição 75.7.** A relação de um termo bonito $t_1$ ser um subtermo de $t_2$, $t_1 \sqsubseteq t_2$, é definida por indução em $t_2$ como segue:

1. Se $t_2$ é uma letra, então $t_1 \sqsubseteq t_2$ sse $t_1 = t_2$.
2. Se $t_2$ é $[s_1 \circ s_2]$, então $t_1 \sqsubseteq t_2$ sse $t_1 = t_2$, $t_1 \sqsubseteq s_1$, ou $t_1 \sqsubseteq s_2$.

Esta definição, por exemplo, nos dirá que a $\sqsubseteq$ [b ∘ a]. Pois (2) diz que a $\sqsubseteq$ [b ∘ a] sse a = [b ∘ a], ou a $\sqsubseteq$ *b*, ou a $\sqsubseteq$ a. As duas primeiras são falsas: a claramente não é idêntico a [b ∘ a], e por (1), a $\sqsubseteq$ b sse a = b, o que também é falso. No entanto, também por (1), a $\sqsubseteq$ a sse a = a, o que é verdadeiro.

É importante observar que o sucesso desta definição depende de um fato que ainda não provamos: todo termo bonito $t$ ou é uma letra isolada, ou existem termos bonitos *univocamente determinados* $s_1$ e $s_2$ tais que $t = [s_1 \circ s_2]$.

"Univocamente determinados" aqui significa que, se $t = [s_1 \circ s_2]$, ele não é *também* $= [r_1 \circ r_2]$ com $s_1 \neq r_1$ ou $s_2 \neq r_2$. Se este fosse o caso, então a cláusula (2) poderia entrar em conflito consigo mesma: lendo $t_2$ como $[s_1 \circ s_2]$ poderíamos obter $t_1 \sqsubseteq t_2$, mas se lermos $t_2$ como $[r_1 \circ r_2]$ poderíamos obter não $t_1 \sqsubseteq t_2$. Antes de provarmos que isso não pode acontecer, vejamos um exemplo em que ele *pode* acontecer.

**Definição 75.8.** Defina *termos sem colchetes* indutivamente por

1. Toda letra é um termo sem colchetes.
2. Se $s_1$ e $s_2$ são termos sem colchetes, então $s_1 \circ s_2$ é um termo sem colchetes.
3. Nada mais é um termo sem colchetes.

Termos sem colchetes são, por exemplo, a, b ∘ d, b ∘ a ∘ b. Agora, se definíssemos "subtermo" para termos sem colchetes do modo como fizemos acima, a segunda cláusula diria

$$\text{Se } t_2 = s_1 \circ s_2, \text{ então } t_1 \sqsubseteq t_2 \text{ sse } t_1 = t_2, t_1 \sqsubseteq s_1, \text{ ou } t_1 \sqsubseteq s_2.$$

Agora, b ∘ a ∘ b é da forma $s_1 \circ s_2$ com

$$s_1 = \text{b e} \qquad\qquad s_2 = \text{a} \circ \text{b}.$$

Ele também é da forma $r_1 \circ r_2$ com

$$r_1 = \text{b} \circ \text{a e} \qquad\qquad r_2 = \text{b}.$$

Agora, a ∘ b é um subtermo de b ∘ a ∘ b? A resposta é sim, se seguirmos a primeira leitura, e não, se seguirmos a segunda.

A propriedade de que o modo como um termo bonito é construído a partir de outros termos bonitos é único é chamada de *leitura única*. Como definições indutivas de relações para tais objetos definidos indutivamente são importantes, temos que provar que ela vale.

**Proposição 75.9.** *Suponha que t é um termo bonito. Então ou t é uma letra isolada, ou existem termos bonitos univocamente determinados $s_1$, $s_2$ tais que $t = [s_1 \circ s_2]$.*

*Prova.* Se $t$ é uma letra isolada, a condição é satisfeita. Então suponha que $t$ não é uma letra isolada. Podemos perceber, pela definição indutiva, que então $t$ deve ser da forma $[s_1 \circ s_2]$ para alguns termos bonitos $s_1$ e $s_2$. Resta mostrar que estes são univocamente determinados, isto é, se $t = [r_1 \circ r_2]$, então $s_1 = r_1$ e $s_2 = r_2$.

Então suponha $t = [s_1 \circ s_2]$ e também $t = [r_1 \circ r_2]$ para termos bonitos $s_1$, $s_2$, $r_1$, $r_2$. Temos que mostrar que $s_1 = r_1$ e $s_2 = r_2$. Primeiro, $s_1$ e $r_1$

devem ser idênticos, pois, caso contrário, um é um segmento inicial próprio do outro. Mas, por Proposição 75.6, isso é impossível se $s_1$ e $r_1$ são ambos termos bonitos. Mas se $s_1 = r_1$, então claramente também $s_2 = r_2$. □

Também podemos definir funções indutivamente: por exemplo, podemos definir a função $f$ que mapeia qualquer termo bonito na profundidade máxima de aninhamento de $[\dots]$ nele como segue:

**Definição 75.10.** A *profundidade* de um termo bonito, $f(t)$, é definida indutivamente como segue:

$$f(t) = \begin{cases} 0 & \text{se } t \text{ é uma letra} \\ \max(f(s_1), f(s_2)) + 1 & \text{se } t = [s_1 \circ s_2]. \end{cases}$$

Por exemplo,

$$\begin{aligned} f([\mathrm{a} \circ \mathrm{b}]) &= \max(f(\mathrm{a}), f(\mathrm{b})) + 1 = \\ &= \max(0,0) + 1 = 1, \text{ e} \\ f([[\mathrm{a} \circ \mathrm{b}] \circ \mathrm{c}]) &= \max(f([\mathrm{a} \circ \mathrm{b}]), f(\mathrm{c})) + 1 = \\ &= \max(1,0) + 1 = 2. \end{aligned}$$

Aqui, é claro, supomos que $s_1$ e $s_2$ são termos bonitos, e fazemos uso do fato de que todo termo bonito ou é uma letra ou é da forma $[s_1 \circ s_2]$. É novamente importante que ele possa ser dessa forma de apenas um modo. Para ver por quê, considere novamente os termos sem colchetes que definimos antes. A "definição" correspondente seria:

$$g(t) = \begin{cases} 0 & \text{se } t \text{ é uma letra} \\ \max(g(s_1), g(s_2)) + 1 & \text{se } t = s_1 \circ s_2. \end{cases}$$

Agora considere o termo sem colchetes $\mathrm{a} \circ \mathrm{b} \circ \mathrm{c} \circ \mathrm{d}$. Ele pode ser lido de mais de um modo, por exemplo, como $s_1 \circ s_2$ com

$$s_1 = \mathrm{a} \text{ e} \qquad\qquad s_2 = \mathrm{b} \circ \mathrm{c} \circ \mathrm{d},$$

ou como $r_1 \circ r_2$ com

$$r_1 = \mathrm{a} \circ b \text{ e} \qquad\qquad r_2 = \mathrm{c} \circ \mathrm{d}.$$

Calcular $g$ de acordo com o primeiro modo de lê-lo daria

$$\begin{aligned} g(s_1 \circ s_2) &= \max(g(\mathrm{a}), g(\mathrm{b} \circ \mathrm{c} \circ \mathrm{d})) + 1 = \\ &= \max(0,2) + 1 = 3 \end{aligned}$$

enquanto, de acordo com a outra leitura, obtemos

$$\begin{aligned} g(r_1 \circ r_2) &= \max(g(\mathrm{a} \circ \mathrm{b}), g(\mathrm{c} \circ \mathrm{d})) + 1 = \\ &= \max(1, 1) + 1 = 2 \end{aligned}$$

Mas uma função deve sempre produzir um valor único; então nossa "definição" de $g$ não define função alguma.

## Problemas

**Problema 75.1.** Defina o conjunto dos termos superbonitos por

1. Qualquer letra a, b, c, d é um termo superbonito.
2. Se $s$ é um termo superbonito, então também o é $[s]$.
3. Se $s_1$ e $s_2$ são termos superbonitos, então também o é $[s_1 \circ s_2]$.
4. Nada mais é um termo superbonito.

Mostre que o número de [ em um termo superbonito $t$ de comprimento $n$ é $\leq n/2 + 1$.

**Problema 75.2.** Prove, por indução estrutural, que nenhum termo bonito começa com ].

**Problema 75.3.** Dê uma definição indutiva da função $l$, em que $l(t)$ é o número de símbolos no termo bonito $t$.

**Problema 75.4.** Prove, por indução estrutural sobre termos bonitos $t$, que $f(t) < l(t)$ (em que $l(t)$ é o número de símbolos em $t$ e $f(t)$ é a profundidade de $t$ tal como definida em Definição 75.10).

# Parte XVII

# History

# Capítulo 76

# Biografias

## 76.1 Georg Cantor

Uma biografia inicial de Georg Cantor (GAY-org KAHN-tor) afirmava que ele tinha nascido e sido encontrado num navio que seguia para São Petersburgo, na Rússia, e que seus pais eram desconhecidos. Isto, porém, não é verdade; embora ele tivesse nascido em São Petersburgo em 1845.

Figura 76.1: Georg Cantor

Cantor se doutorou em matemática na Universidade de Berlim em 1867. É conhecido por seu trabalho em teoria dos conjuntos e é considerado o fundador da teoria dos conjuntos como disciplina de pesquisa distinta. Foi o primeiro a provar que existem conjuntos infinitos de tamanhos diferentes. Suas teorias, e sobretudo a teoria dos infinitos, provocaram muito debate entre os matemáticos da época, e seu trabalho foi controverso.

As convicções religiosas de Cantor e seu trabalho matemático estavam inextricavelmente ligados; ele chegou a afirmar que a teoria dos números transfinitos lhe tinha sido comunicada diretamente por Deus. Mais tarde, Cantor sofreu de doença mental. A partir de 1894, e com maior frequência nos últimos anos, Cantor foi internado. As fortes críticas a seu trabalho, incluindo um rompimento com o matemático Leopold Kronecker, levaram à depressão e à perda de interesse pela matemática. Durante episódios depressivos, Cantor se dedicava à filosofia e à literatura, e

chegou a publicar uma teoria de que Francis Bacon era o autor das peças de Shakespeare.

Cantor morreu em 6 de janeiro de 1918, num sanatório em Halle.

**Leitura complementar** Para biografias completas de Cantor, ver Dauben (1990) e Grattan-Guinness (1971). As visões radicais de Cantor são também descritas no programa da BBC Radio 4 *A Brief History of Mathematics* (du Sautoy, 2014). Se quiser ouvir as teorias de Cantor em forma de rap, ver Rose (2012).

## 76.2 Alonzo Church

Figura 76.2: Alonzo Church

Alonzo Church nasceu em Washington, DC, em 14 de junho de 1903. Na primeira infância, um acidente com uma arma de ar comprimido deixou Church cego de um olho. Ele concluiu o ensino preparatório em Connecticut em 1920 e iniciou sua formação universitária em Princeton naquele mesmo ano. Concluiu seus estudos de doutorado em 1927. Após alguns anos no exterior, Church retornou a Princeton. Church era conhecido por ser extremamente educado e cuidadoso. Sua escrita no quadro-negro era impecável, e ele preservava artigos importantes cobrindo-os cuidadosamente com cimento Duco (uma cola transparente). Fora de suas atividades acadêmicas, gostava de ler revistas de ficção científica e não tinha receio de escrever aos editores caso identificasse quaisquer imprecisões nos textos.

As realizações acadêmicas de Church foram notáveis. Junto com seus alunos Stephen Kleene e Barkley Rosser, ele desenvolveu uma teoria da calculabilidade efetiva, o cálculo lambda, independentemente do desenvolvimento da máquina de Turing por Alan Turing. As duas definições de computabilidade são equivalentes e dão origem ao que hoje é conhecido como a *Tese de Church–Turing*: a de que uma função dos números naturais é efetivamente computável se e somente se for computável por meio de uma máquina de Turing (ou do cálculo lambda). Ele também provou o que hoje é conhecido como o *Teorema de Church*: o problema da decisão para a validade de fórmulas de primeira ordem é insolúvel.

Church continuou seu trabalho até a velhice. Em 1967, deixou Princeton para ir à UCLA, onde foi professor até se aposentar, em 1990. Church faleceu

em 1º de agosto de 1995, aos 92 anos.

**Leitura complementar** Para uma breve biografia de Church, veja Enderton (2019). Os escritos originais de Church sobre o cálculo lambda e o Entscheidungsproblem (Tese de Church) são Church (1936a,b). Aspray (1984) registra uma entrevista com Church sobre a comunidade matemática de Princeton na década de 1930. Church escreveu uma série de resenhas de livros para o *Journal of Symbolic Logic* de 1936 até 1979. Todas estão arquivadas no site de John MacFarlane (MacFarlane, 2015).

## 76.3 Gerhard Gentzen

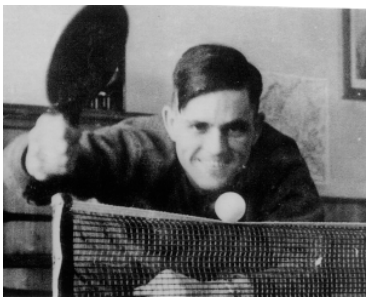


Figura 76.3: Gerhard Gentzen

Gerhard Gentzen é conhecido principalmente como o criador da teoria estrutural da prova e, especificamente, pela criação dos sistemas de derivação de dedução natural e de cálculo de sequentes. Ele nasceu em 24 de novembro de 1909 em Greifswald, na Alemanha. Gerhard foi educado em casa por três anos antes de frequentar o ensino preparatório, onde estava atrás da maioria de seus colegas em termos de instrução. Apesar disso, era um aluno brilhante e demonstrava forte aptidão para a matemática. Seus interesses eram variados e ele, por exemplo, também escrevia poemas para a mãe e peças para o teatro da escola.

Gentzen começou seus estudos universitários na Universidade de Greifswald, mas passou por Göttingen, Munique e Berlim. Recebeu seu doutorado em 1933 pela Universidade de Göttingen, sob a orientação de Hermann Weyl. (Paul Bernays supervisionou a maior parte de seu trabalho, mas foi demitido da universidade pelos nazistas.) Em 1934, Gentzen começou a trabalhar como assistente de David Hilbert. Nesse mesmo ano, desenvolveu os sistemas de derivação de cálculo de sequentes e de dedução natural, em seus artigos *Untersuchungen über das logische Schließen I–II [Investigações sobre a Dedução Lógica I–II]*. Ele provou a consistência dos axiomas de Peano em 1936.

A relação de Gentzen com os nazistas é complicada. Ao mesmo tempo em que seu mentor Bernays foi forçado a deixar a Alemanha, Gentzen ingressou no braço universitário da SA, a organização paramilitar nazista. Como muitos alemães, foi membro do partido nazista. Durante a guerra, serviu como oficial de telecomunicações na unidade de inteligência aérea. No entanto, em 1942 foi dispensado do serviço devido a um colapso nervoso. Não está claro se as

lealdades de Gentzen estavam com o partido nazista ou se ele ingressou no partido a fim de garantir sucesso acadêmico.

Em 1943, foi oferecida a Gentzen uma posição acadêmica no Instituto Matemático da Universidade Alemã de Praga, que ele aceitou. No entanto, em 1945 os cidadãos de Praga se revoltaram contra a ocupação alemã. As forças soviéticas chegaram à cidade e prenderam todos os professores da universidade. Por causa de sua filiação a organizações nazistas, Gentzen foi levado a um campo de trabalhos forçados. Ele morreu de desnutrição em sua cela em 4 de agosto de 1945, aos 35 anos.

**Leitura complementar** Para uma biografia completa de Gentzen, veja Menzler-Trott (2007). Uma leitura interessante sobre matemáticos sob o regime nazista, que traz uma breve nota sobre a vida de Gentzen, é dada por Segal (2014). Os artigos de Gentzen sobre dedução lógica estão disponíveis no alemão original (Gentzen, 1935a,b). Traduções para o inglês dos artigos de Gentzen foram reunidas em um único volume por Szabo (1969), que também inclui um esboço biográfico.

## 76.4 Kurt Gödel

Kurt Gödel (GER-dle) nasceu em 28 de abril de 1906 em Brünn, no império austro-húngaro (hoje Brno, na República Tcheca). Devido a seu espírito inquisitivo e brilhante, o jovem Kurtele era muitas vezes chamado "Der kleine Herr Warum" (o Pequeno Senhor Porquê) pela família. Destacou-se nos estudos desde a escola primária, tendo obtido menos do que a nota mais alta apenas em matemática. Gödel faltava frequentemente à escola por causa da frágil saúde e estava isento de educação física. Foi diagnosticado com febre reumática durante a infância. Ao longo da vida, acreditou que isso tinha afetado permanentemente seu coração, apesar dos pareceres médicos em contrário.

Figura 76.4: Kurt Gödel

Gödel começou a estudar na Universidade de Viena em 1924 e concluiu o doutorado em 1929. Inicialmente pretendia estudar física, mas seus interesses se deslocaram rapidamente para a matemática e sobretudo para a lógica, em parte devido à influência do filósofo Rudolf Carnap. Sua dissertação, ori-

entada por Hans Hahn, provava o teorema de completude da lógica de predicados de primeira ordem com identidade (Gödel, 1929). Apenas um ano depois, obteve seus resultados mais famosos—o primeiro e o segundo teorema da incompletude (publicados em Gödel 1931). Durante o período em Viena, Gödel participou intensamente no Círculo de Viena, um grupo de filósofos de orientação científica que incluía Carnap, cujo trabalho foi especialmente influenciado pelos resultados de Gödel.

Em 1938, Gödel se casou com Adele Nimbursky. Os pais não ficaram contentes: não só ela era seis anos mais velha e já divorciada, como trabalhava como bailarina num clube noturno. As pressões sociais não afetaram Gödel, contudo, e permaneceram felizmente casados até sua morte.

Depois de a Alemanha Nazi ter anexado a Áustria em 1938, Gödel e Adele emigraram para os Estados Unidos, onde ele assumiu um lugar no Institute for Advanced Study em Princeton, Nova Jersey. Apesar da introversão e do caráter excêntrico, o período de Gödel em Princeton foi colaborativo e frutuoso. Publicou ensaios em teoria dos conjuntos, filosofia e física. Notavelmente, estabeleceu uma amizade particularmente forte com o colega no IAS, Albert Einstein.

Nos últimos anos, a saúde mental de Gödel se deteriorou. A internação da esposa em 1977 fez com que ela não pudesse mais cozinhar as refeições dele. Tendo sofrido de problemas de saúde mental ao longo da vida, sucumbiu à paranoia. Com medo mortal de ser envenenado, Gödel se recusou a comer. Morreu de inanição em 14 de janeiro de 1978, em Princeton.

**Leitura complementar** Para uma biografia completa da vida de Gödel, ver John Dawson (1997). Para outros textos biográficos, bem como ensaios sobre as contribuições de Gödel para a lógica e a filosofia, ver Wang (1990), Baaz et al. (2011), Takeuti et al. (2003), e Sigmund et al. (2007).

A tese de doutorado de Gödel está disponível no alemão original (Gödel, 1929). O texto original dos teoremas da incompletude é (Gödel, 1931). Todas as publicações e textos não publicados de Gödel, bem como uma seleção de correspondência, estão disponíveis em inglês em seus *Collected Papers* Feferman et al. (1986, 1990).

Para um tratamento detalhado dos teoremas da incompletude de Gödel, ver Smith (2013). Para uma discussão informal e filosófica dos teoremas de Gödel, ver o podcast de Mark Linsenmayer (Linsenmayer, 2014).

## 76.5 Emmy Noether

Emmy Noether (NER-ter) nasceu em Erlangen, na Alemanha, em 23 de março de 1882, em uma família erudita de classe média alta. Aclamada como a "mãe da álgebra moderna", Noether fez contribuições inovadoras tanto para a matemática quanto para a física, apesar das significativas barreiras à educação

das mulheres. Na Alemanha daquela época, esperava-se que as meninas fossem educadas nas artes e elas não tinham permissão para frequentar escolas preparatórias para a faculdade. No entanto, após assistir como ouvinte às aulas nas Universidades de Göttingen e Erlangen (onde seu pai era professor de matemática), Noether finalmente conseguiu se matricular como aluna em Erlangen em 1904, quando a política da instituição foi atualizada para permitir estudantes do sexo feminino. Ela recebeu seu doutorado em matemática em 1907.

Apesar de suas qualificações, Noether enfrentou muita resistência durante sua carreira. De 1908 a 1915, ela lecionou em Erlangen sem remuneração. Durante esse período, chamou a atenção de David Hilbert, um dos mais eminentes matemáticos do mundo na época, que a convidou para Göttingen. No entanto, as mulheres eram proibidas de obter cátedras, e ela só pôde lecionar sob o nome de Hilbert, novamente sem remuneração. Foi nesse período que ela provou o que hoje é conhecido como o teorema de Noether, que ainda é usado na física teórica atualmente. Noether finalmente recebeu o direito de lecionar em 1919. A resposta de Hilbert à resistência contínua de seus colegas de universidade teria sido: "Senhores, o conselho da faculdade não é uma casa de banhos."

Figura 76.5: Emmy Noether

No final da década de 1920, ela concentrou-se no trabalho em álgebra abstrata, e suas contribuições revolucionaram o campo. Em suas provas, ela frequentemente fazia uso da chamada condição de cadeia ascendente, que afirma que não há cadeia infinita estritamente crescente de certos conjuntos. Por exemplo, certas estruturas algébricas hoje conhecidas como anéis noetherianos têm a propriedade de que não há sequências infinitas de ideais $I_1 \subsetneq I_2 \subsetneq \dots$. A condição pode ser generalizada para qualquer ordem parcial (na álgebra, ela diz respeito ao caso especial de ideais ordenados pela relação de subconjunto), e também podemos considerar a condição dual de cadeia descendente, na qual toda sequência estritamente *de*crescente em uma ordem parcial eventualmente termina. Se uma ordem parcial satisfaz a condição de cadeia descendente, é possível usar indução ao longo dessa ordem de maneira semelhante àquela em que podemos usar indução ao longo da ordem $<$ sobre $\mathbb{N}$. Tais ordens são chamadas *bem fundadas* ou *noetherianas*, e o princípio

de prova correspondente, *indução noetheriana*.

Noether era judia e, quando os nazistas chegaram ao poder em 1933, ela foi demitida de seu cargo. Felizmente, Noether conseguiu emigrar para os Estados Unidos para ocupar uma posição temporária em Bryn Mawr, na Pensilvânia. Durante seu tempo lá, ela também lecionou em Princeton, embora considerasse a universidade pouco acolhedora para as mulheres (Dick, 1981, 81). Em 1935, Noether passou por uma operação para remover um tumor uterino. Ela morreu de uma infecção decorrente da cirurgia e foi enterrada em Bryn Mawr.

**Leitura complementar** Para uma biografia de Noether, veja Dick (1981). O Perimeter Institute for Theoretical Physics disponibiliza on-line suas palestras sobre a vida e a influência de Noether (Institute, 2015). Se você estiver cansado de ler, *Stuff You Missed in History Class* tem um podcast sobre a vida e a influência de Noether (Frey and Wilson, 2015). As obras reunidas de Noether estão disponíveis no alemão original (Jacobson, 1983).

## 76.6 Bertrand Russell

Bertrand Russell é celebrado como um dos fundadores da filosofia analítica moderna. Nascido em 18 de maio de 1872, Russell não era conhecido apenas pelo trabalho em filosofia e lógica, mas escreveu muitos livros de divulgação em diversas áreas. Foi também um ardente ativista político ao longo da vida.

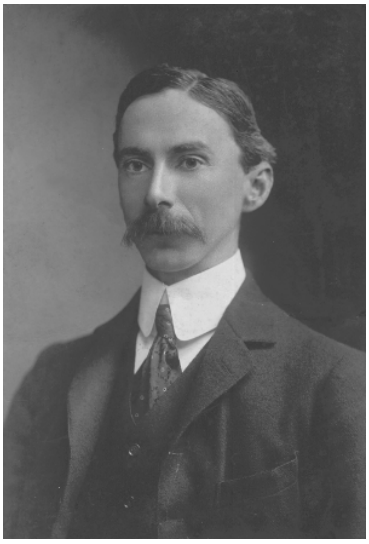


Figura 76.6: Bertrand Russell

Russell nasceu em Trellech, Monmouthshire, no País de Gales. Os pais pertenciam à nobreza britânica. Eram livre-pensadores e chegaram a travar amizade com os radicais de Boston da época. Infelizmente, os pais de Russell morreram quando ele era ainda criança, e Russell foi viver com os avós. Ali recebeu uma educação religiosa (algo que os pais tinham querido evitar a todo custo). A avó era muito rigorosa em todas as questões de moralidade. Na adolescência foi sobretudo educado em casa por professores particulares.

A influência de Russell na filosofia analítica, e sobretudo na lógica, é enorme. Estudou matemática e filosofia no Trinity College, em Cambridge, onde foi influenciado pelo matemático e filósofo Alfred North Whitehead. Em 1910,

Russell e Whitehead publicaram o primeiro volume de *Principia Mathematica*, defendendo a ideia de que a matemática é redutível à lógica. Seguiu-se a publicação de centenas de livros, ensaios e panfletos políticos. Em 1950, ganhou o Prêmio Nobel de Literatura.

Russell se encontrava profundamente envolvido na política e no ativismo social. Durante a Primeira Guerra Mundial foi preso e condenado a seis meses de prisão por atividades pacifistas e protesto. Na prisão pôde escrever e ler, e afirma ter achado a experiência "bastante agradável." Permaneceu pacifista ao longo da vida, e voltou a ser detido por participar num comício pelo desarmamento nuclear em 1961. Sobreviveu também a um acidente de avião em 1948, no qual os únicos sobreviventes eram os que estavam sentados na área de fumantes. Por isso, Russell declarou que devia a vida ao tabagismo. Russell se casou quatro vezes, mas tinha fama de manter relações extraconjugais. Morreu em 2 de fevereiro de 1970, aos 97 anos, em Penrhyndeudraeth, no País de Gales.

**Leitura complementar** Russell escreveu uma autobiografia em três partes, que abrange sua vida de 1872 a 1967 (Russell, 1967, 1968, 1969). O Bertrand Russell Research Centre na McMaster University alberga os arquivos de Bertrand Russell. Ver o site em Duncan (2015), para informação sobre os volumes de suas obras reunidas (incluindo índices pesquisáveis) e projetos de arquivo. O artigo de Russell *On Denoting* (Russell, 1905) é um clássico da filosofia analítica do século XX.

A entrada da Stanford Encyclopedia of Philosophy sobre Russell (Irvine, 2015) inclui excertos de áudio de Russell a falar sobre Desejo e teoria política. Estão disponíveis online muitas entrevistas em vídeo com Russell. Para o ouvir falar de tabagismo e do envolvimento num acidente de avião, ver, por exemplo, Russell (n.d.). Algumas obras de Russell, incluindo a *Introduction to Mathematical Philosophy*, estão disponíveis como audiolivros gratuitos em LibriVox (n.d.).

## 76.7 Alfred Tarski

Alfred Tarski nasceu em 14 de janeiro de 1901 em Varsóvia, na Polônia (então parte do Império Russo). Descrito como "napoleônico", Tarski era ruidoso, falador e intenso. Sua energia se refletia muitas vezes nas aulas—chegou a incendiar um cesto de lixo ao jogar fora um cigarro durante uma aula, e foi proibido de lecionar novamente naquele edifício.

Tarski tinha sede de conhecimento desde cedo. Mais tarde diria aos estudantes que estudara lógica porque era a única disciplina em que tivera um B, mas os registros do colégio mostram que tinha notas máximas em tudo—até em lógica. Estudou na Universidade de Varsóvia de 1918 a 1924. Tarski pretendia inicialmente estudar biologia, mas se interessou por matemática, filoso-

fia e lógica, pois a universidade era o centro da Escola de Lógica e Filosofia de Varsóvia. Tarski se doutorou em 1924 sob orientação de Stanisław Leśniewski.

Antes de emigrar para os Estados Unidos em 1939, Tarski completou parte de seu trabalho mais importante enquanto professor de ensino secundário em Varsóvia. O trabalho sobre consequência lógica e verdade lógica foi escrito nesse período. Em 1939, Tarski se encontrava nos Estados Unidos numa turnê de palestras. Durante a visita, a Alemanha invadiu a Polônia, e, por causa da ascendência judaica, Tarski não pôde retornar. A esposa e os filhos permaneceram na Polônia até o fim da guerra, mas depois também puderam emigrar para os Estados Unidos. Tarski lecionou em Harvard, no College of the City of New York, no Institute for Advanced Study em Princeton, e finalmente na Universidade da Califórnia, em Berkeley. Ali fundou o programa multidisciplinar em Lógica e Metodologia da Ciência. Tarski morreu em 26 de outubro de 1983, aos 82 anos.

Figura 76.7: Alfred Tarski

**Leitura complementar** Para mais sobre a vida de Tarski, ver a biografia *Alfred Tarski: Life and Logic* (Feferman and Feferman, 2004). As obras fundadoras de Tarski sobre consequência lógica e verdade estão disponíveis em inglês em (Corcoran, 1983). Todas as obras originais de Tarski foram reunidas numa série de quatro volumes, (Tarski, 1981).

## 76.8 Alan Turing

Alan Turing nasceu em Maida Vale, Londres, em 23 de junho de 1912. É considerado o pai da ciência da computação teórica. O interesse de Turing pelas ciências físicas e pela matemática começou em tenra idade. No entanto, quando menino, seus interesses não eram bem contemplados nas escolas que frequentava, onde a ênfase recaía sobre a literatura e os clássicos. Consequentemente, ele teve um desempenho fraco na escola e foi repreendido por muitos de seus professores.

Turing estudou no King's College, em Cambridge, na graduação, onde estudou matemática. Em 1936, Turing desenvolveu (o que hoje se chama) a máquina de Turing como uma tentativa de definir precisamente a noção de função computável e de provar a indecidibilidade do problema da decisão.

Ele foi superado no resultado por Alonzo Church, que o provou por meio de seu próprio cálculo lambda. Ainda assim, o artigo de Turing foi publicado com referência ao resultado de Church. Church convidou Turing para Princeton, onde ele passou de 1936 a 1938 e obteve um doutorado sob a orientação de Church.

Figura 76.8: Alan Turing

Apesar de seu interesse pela lógica, os interesses anteriores de Turing pelas ciências físicas permaneceram predominantes. Suas habilidades práticas foram postas em prática durante seu serviço no departamento britânico de criptanálise em Bletchley Park durante a Segunda Guerra Mundial. Turing foi uma figura central na quebra da cifra usada nas comunicações navais alemãs—o código Enigma. A expertise de Turing em estatística e criptografia, juntamente com a introdução de maquinário eletrônico, deu à equipe a capacidade de quebrar o código por meio da criação de uma máquina de descriptografia chamada "bombe". Suas ideias também ajudaram na criação do primeiro computador eletrônico programável do mundo, o Colossus, também usado em Bletchley Park para quebrar a cifra alemã Lorenz.

Turing era homossexual. Mesmo assim, em 1942 ele pediu Joan Clarke em casamento, uma de suas colegas de equipe em Bletchley Park, mas depois rompeu o noivado e confessou a ela que era homossexual. Teve vários amantes ao longo da vida, embora os atos homossexuais fossem, então, crimes no Reino Unido. Em 1952, a casa de Turing foi assaltada por um amigo de seu amante da época e, ao prestar queixa à polícia, Turing admitiu ter um relacionamento homossexual, sob a impressão de que o governo estava a caminho de legalizar os atos homossexuais. Isso não era verdade, e ele foi acusado de grave indecência. Em vez de ir para a prisão, Turing optou por um tratamento hormonal que reduzia a libido. Turing foi encontrado morto em 8 de junho de 1954, de uma overdose de cianeto—muito provavelmente suicídio. Ele recebeu um perdão real da Rainha Elizabeth II em 2013.

**Leitura complementar** Para uma biografia abrangente de Alan Turing, veja Hodges (2014). A vida e a obra de Turing inspiraram uma peça, *Breaking the Code*, que foi produzida em 1996 para a TV, com Derek Jacobi no papel de Turing. *The Imitation Game*, um filme indicado ao Oscar, com Bendict Cumberbatch e Kiera Knightley, também é baseado livremente na vida de Alan

Turing e em seu período em Bletchley Park (Tyldum, 2014).

Radiolab (2012) tem vários podcasts sobre a vida e a obra de Turing. O documentário *The Strange Life and Death of Dr. Turing*, da BBC Horizon, está disponível para assistir on-line (Sykes, 1992). (Theelen, 2012) é um vídeo curto de uma Máquina de Turing de LEGO em funcionamento—feito para homenagear o centenário de Turing em 2012.

O artigo original de Turing sobre máquinas de Turing e o problema da decisão é Turing (1937).

## 76.9 Ernst Zermelo

Figura 76.9: Ernst Zermelo

Ernst Zermelo nasceu em 27 de julho de 1871 em Berlim, na Alemanha. Tinha cinco irmãs, embora a família sofresse de frágil saúde e apenas três sobrevivessem à idade adulta. Os pais também faleceram quando ele era jovem, deixando-o órfão, com os irmãos, aos dezessete anos. Zermelo tinha um profundo interesse pelas artes, e sobretudo pela poesia. Era conhecido por ser perspicaz, espirituoso e crítico. Entre suas conquistas matemáticas mais celebradas estão a introdução do axioma da escolha (em 1904) e sua axiomatização da teoria dos conjuntos (em 1908).

Os interesses de Zermelo na universidade eram variados. Frequentou cursos de física, matemática e filosofia. Sob orientação de Hermann Schwarz, Zermelo concluiu a dissertação *Investigations in the Calculus of Variations* em 1894 na Universidade de Berlim. Em 1897, decidiu prosseguir estudos na Universidade de Göttingen, onde foi fortemente influenciado pelo trabalho fundacional de David Hilbert. Em 1899 tornou-se elegível para uma cátedra, mas só obteve uma onze anos depois—possivelmente devido a seu comportamento estranho e à "pressa nervosa."

Zermelo obteve finalmente uma cátedra remunerada na Universidade de Zurique em 1910, mas foi forçado a se aposentar em 1916 por causa da tuberculose. Depois da recuperação, foi nomeado professor honorário na Universidade de Freiburg em 1921. Nesse período dedicou-se à matemática fundacional. Irritou-se com os trabalhos de Thoralf Skolem e Kurt Gödel, e criticou publicamente suas abordagens em seus artigos. Foi demitido do cargo em

Freiburg em 1935, devido a sua impopularidade e à oposição à ascensão de Hitler ao poder na Alemanha.

Os últimos anos da vida de Zermelo foram marcados pelo isolamento. Depois da demissão em 1935, abandonou a matemática. Mudou-se para o campo, onde viveu modestamente. Casou-se em 1944 e ficou completamente dependente da esposa à medida que ia ficando cego. Zermelo perdeu totalmente a visão por volta de 1951. Faleceu em Günterstal, na Alemanha, em 21 de maio de 1953.

**Leitura complementar** Para uma biografia completa de Zermelo, ver Ebbinghaus (2015). Os artigos fundadores de 1904 e 1908 de Zermelo podem ser lidos no alemão original (Zermelo, 1904, 1908b). As obras reunidas de Zermelo, incluindo os escritos sobre física, estão disponíveis em tradução inglesa em Ebbinghaus et al. (2010); Ebbinghaus and Kanamori (2013).

# Capítulo 77

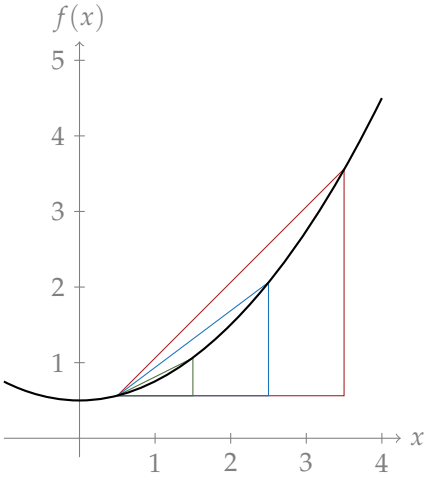
# História e Mitologia da Teoria dos Conjuntos

This chapter includes the historical prelude from Tim Button's Open Set Theory text.

## 77.1 Infinitesimais e Diferenciação

Newton e Leibniz descobriram o cálculo (independentemente) no fim do século XVII. Uma aplicação particularmente importante do cálculo era a *diferenciação*. Grosso modo, a diferenciação pretende dar uma noção da "taxa de variação", ou gradiente, de uma função num ponto.

Eis uma forma vívida de ilustrar a ideia. Considere a função $f(x) = {}^{x^2}/_4 + {}^1/_2$, representada a preto abaixo:



Suponhamos que queremos encontrar o gradiente da função em $c = 1/2$. Começamos por desenhar um triângulo cuja hipotenusa aproxima o gradiente nesse ponto, talvez o triângulo vermelho acima. Quando $\beta$ é o comprimento da base do nosso triângulo, a sua altura é $f(1/2 + \beta) - f(1/2)$, de modo que o gradiente da hipotenusa é:

$$\frac{f(1/2 + \beta) - f(1/2)}{\beta}.$$

Assim, o gradiente do nosso triângulo vermelho, com base de comprimento 3, é exatamente 1. A hipotenusa de um triângulo menor, o triângulo azul com base de comprimento 2, dá uma melhor aproximação; o seu gradiente é $3/4$. Um triângulo ainda menor, o verde com base de comprimento 1, dá uma aproximação ainda melhor, com gradiente $1/2$.

Triângulos cada vez menores dão-nos aproximações cada vez melhores. Por isso poderíamos dizer algo deste gênero: a hipotenusa de um triângulo com comprimento de base *infinitesimal* nos dá o próprio gradiente em $c = 1/2$. Deste modo, obteríamos uma fórmula para a (primeira) derivada da função $f$ no ponto $c$:

$$f'(c) = \frac{f(c + \beta) - f(c)}{\beta} \text{ onde } \beta \text{ é infinitesimal.}$$

E, grosso modo, foi isto que Newton e Leibniz disseram.

Contudo, uma vez que o disseram, devemos perguntar-lhes: o que é um *infinitesimal*? Surge um dilema sério. Se $\beta = 0$, então $f'$ fica mal definida, pois envolve dividir por 0. Mas se $\beta > 0$, obtemos apenas uma *aproximação* ao gradiente, e não o próprio gradiente.

Esta não é uma preocupação anacrônica. Eis Berkeley, a criticar os seguidores de Newton:

> Admito que os signos possam ser feitos para denotar qualquer coisa ou nada: e consequentemente que, na notação original $c + \beta$, $\beta$ poderia ter significado um incremento ou nada. Mas então, seja qual for o significado atribuído a $\beta$, é preciso argumentar de modo consistente com essa significação, e não proceder com duplo sentido: o que seria um sofismo manifesto. (Berkeley 1734, §XIII, variáveis alteradas para coincidir com o texto precedente)

Para defender o cálculo infinitesimal face a Berkeley, poder-se-ia responder que a linguagem dos "infinitesimais" é meramente figurada. Poder-se-ia dizer que, desde que tomemos um triângulo *bem pequeno*, obteremos uma aproximação *suficientemente boa* à tangente. Berkeley tinha também uma resposta para isto: embora isso pudesse bastar para a engenharia, minava o *estatuto* da matemática, pois

> dizem-nos que *in rebus mathematicis errores quàm minimi non sunt contemnendi*. [No caso da matemática, os menores erros não devem ser desprezados.] (Berkeley, 1734, §IX)

A passagem em itálico é uma citação quase literal do próprio Newton na *Quadrature of Curves* (1704).

As objeções filosóficas de Berkeley são profundamente incisivas. Não obstante, o cálculo foi uma empresa enormemente bem-sucedida, e os matemáticos continuaram a usá-lo sem incorrer em erro.

## 77.2 Definição Rigorosa de Limites

Hoje em dia, a solução padrão ao problema anterior é livrar-se dos infinitesimais. Eis como.

Já vimos que, à medida que $\beta$ fica menor, obtemos melhores aproximações do gradiente. De fato, à medida que $\beta$ se aproxima arbitrariamente de 0, o valor de $f'(c)$ "tende sem limite" para o gradiente que queremos. Assim, em vez de considerar o que acontece *em* $\beta = 0$, precisamos apenas considerar a *tendência* de $f'(c)$ quando $\beta$ se aproxima de 0.

Posto deste modo, o desafio geral é dar sentido a afirmações desta forma:

> À medida que $x$ se aproxima de $c$, $g(x)$ tende sem limite para $\ell$.

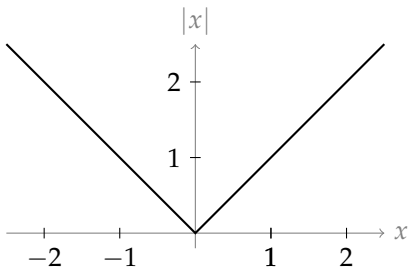
que podemos escrever de forma mais compacta assim:

$$\lim_{x \to c} g(x) = \ell.$$

No século XIX, sobre trabalho anterior de Cauchy, Weierstrass deu uma definição perfeitamente rigorosa desta expressão. A ideia é, de fato, que podemos tornar $g(x)$ tão próxima quanto queiramos de $\ell$, tornando $x$ adequadamente próximo de $c$. Mais precisamente, estipulamos que $\lim_{x \to c} g(x) = \ell$ significará:

$$(\forall \varepsilon > 0)(\exists \delta > 0) \forall x \left( |x - c| < \delta \to |g(x) - \ell| < \varepsilon \right).$$

As barras verticais indicam aqui valor absoluto. Isto é, $|x| = x$ quando $x \geq 0$, e $|x| = -x$ quando $x < 0$; pode representar-se *essa* função como se segue:



A definição diz portanto, grosso modo, o seguinte: pode tornar o seu "erro" inferior a $\varepsilon$ (isto é, $|g(x) - \ell| < \varepsilon$) escolhendo argumentos que distem no máximo $\delta$ de $c$ (isto é, $|x - c| < \delta$).

Tendo definido a noção de limite, podemos usá-la para evitar por completo os infinitesimais, estipulando que o gradiente de $f$ em $c$ é dado por:

$$f'(c) = \lim_{x \to 0} \left( \frac{f(c+x) - f(c)}{x} \right) \text{ quando um limite existe.}$$

É importante, no entanto, compreender por que a nossa definição precisa da ressalva "quando um limite existe". Para um exemplo simples, considere $f(x) = |x|$, cujo gráfico acabamos de ver. Evidentemente, $f'(0)$ está mal definida: se nos aproximamos de 0 "pela direita", o gradiente é sempre 1; se nos aproximamos "pela esquerda", o gradiente é sempre $-1$; logo o limite não está definido. Como tal, podemos acrescentar que uma função $f$ é *diferenciável* em $x$ se e só se tal limite existe.

Já vimos como tratar a diferenciação usando a noção de *limite*. Podemos usar a mesma noção para definir a ideia de função *contínua*. (Bolzano tinha, com efeito, percebido isto já por 1817.) O tratamento Cauchy–Weierstrass da continuidade é o seguinte. Grosso modo: uma função $f$ é contínua (num ponto) desde que, ao exigir um certo grau de precisão relativamente à saída da função, se possa garantir essa precisão insistindo num certo grau de precisão relativamente à entrada da função. Mais precisamente: $f$ é contínua em $c$ desde que, à medida que $x$ tende para zero, a diferença entre $f(c+x)$ e $f(c)$ tenda para 0. De outro modo: $f$ é *contínua* em $c$ se e só se $f(c) = \lim_{x \to c} f(x)$.

Ir mais longe levar-nos-ia apenas para a análise real, quando o nosso tema é a teoria dos conjuntos. Por isso, agora devemos fazer uma pausa e enunciar a moral. Durante o século XIX, os matemáticos aprenderam a passar sem infinitesimais, invocando uma noção rigorosamente definida de *limite*.

## 77.3 Patologias

Contudo, a definição de um *limite* acabou por permitir construções bastante "patológicas".

Por volta da década de 1830, Bolzano descobriu uma função que era *contínua em todo o lado*, mas *não diferenciável em parte nenhuma*. (Infelizmente, Bolzano nunca publicou isto; a ideia foi pela primeira vez encontrada pelos matemáticos em 1872, graças à descoberta independente de Weierstrass da mesma ideia.)[1] Isto era, no mínimo, bastante surpreendente. É fácil encontrar funções, como $|x|$, que são contínuas em todo o lado mas não diferenciáveis num dado ponto. Mas uma função contínua em todo o lado e *não diferenciável em parte nenhuma*

[1] A história está documentada em notas de rodapé extremamente minuciosas do artigo da Wikipédia sobre a função de Weierstrass.

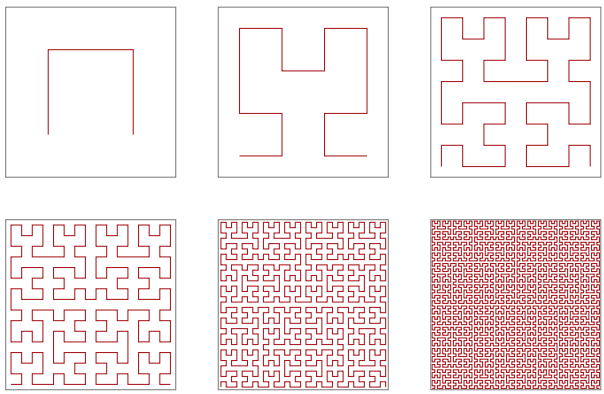
é uma criatura muito diferente. Considere, por um momento, como tentaria desenhar tal função. Para garantir que é contínua, deve conseguí-la desenhar sem nunca levantar a caneta da página; mas para garantir que não é diferenciável em nenhum ponto, teria de mudar abruptamente a direção da caneta, constantemente.

Seguiram-se mais "patologias". A 5 de janeiro de 1874, Cantor escreveu uma carta a Dedekind, colocando o problema:

> Poderá uma superfície (digamos um quadrado incluindo o seu contorno) estar correlacionada biunivocamente com uma linha (digamos uma reta incluindo as extremidades) de modo que a cada ponto da superfície corresponda um ponto da linha e, reciprocamente, a cada ponto da linha corresponda um ponto da superfície?
>
> Ainda me parece, de momento, que a resposta a esta questão é muito difícil—embora aqui também se esteja tão impelido a dizer *não* que se queira considerar quase supérflua a prova. [Citado em Gouvêa 2011]

Mas, em 1877, Cantor provou que estivera errado. De fato, uma linha e um quadrado têm exatamente o mesmo número de pontos. Escreveu a 29 de junho de 1877 a Dedekind "*je le vois, mais je ne le crois pas*"; isto é, "eu vejo, mas não acredito". Na "história recebida" da matemática, isto é frequentemente tomado como indicador de quão *literalmente incríveis* eram estes novos resultados para os matemáticos da época. (A correspondência é apresentada em Gouvêa (2011), e voltaremos a ela em Seção 77.4. A prova de Cantor está esboçada em Seção 77.5.)

Inspirado pelo resultado de Cantor, Peano começou a considerar se seria possível mapear suavemente uma linha sobre um plano. Isto seria uma *curva que preenche o espaço*. Em 1890, Peano construiu precisamente tal curva. Isto é verdadeiramente contraintuitivo: Euclides tinha definido uma linha como "comprimento sem largura" (Livro I, Definição 2), mas Peano mostrara que, enrolando adequadamente uma linha, o seu comprimento pode transformar-se em largura. Em 1891, Hilbert descreveu uma curva preenchedora de espaço ligeiramente mais intuitiva, juntamente com algumas figuras que a ilustram. A curva é construída em sequência, e eis as primeiras seis fases da construção:



No limite—uma noção que, entretanto, recebera definição rigorosa—todo o quadrado fica inteiramente preenchido na cor vermelho. E, de passagem, a

curva de Hilbert é contínua em todo o lado mas não diferenciável em parte nenhuma; intuitivamente porque, no limite infinito, a função muda abruptamente de direção a cada instante. (Esboçaremos a construção de Hilbert com mais pormenor na Seção 77.6.)

Para o bem ou para o mal, estas construções geométricas "patológicas" foram tratadas como motivo para duvidar de apelos à intuição geométrica. Tornaram-se algo próximo de *propaganda* por uma nova forma de fazer matemática, que culminaria na teoria dos conjuntos. Na construção posterior do mito em torno do assunto, repetia-se, frequentemente, que estes resultados eram ao mesmo tempo perfeitamente rigorosos e perfeitamente chocantes. Serviam portanto um duplo propósito: como aviso contra confiar na intuição geométrica, e como uma demonstração da fertilidade de novas formas de pensar.

## 77.4 Mais Mito do que História?

Com mais de um século de perspectiva, ao olhar para estes acontecimentos, devemos ter cuidado para não tomar estes veredictos por adquiridos. Os resultados eram certamente novos, entusiasmantes e surpreendentes. Mas quão verdadeiramente chocantes eram? E demonstraram realmente que não devemos confiar na intuição geométrica?

Quanto ao choque, Gouvêa (2011) observa que a célebre nota de Cantor a Dedekind, "*je le vois, mais je ne le crois pas*" é tirada um tanto fora de contexto. Eis mais desse contexto (citado de Gouvêa):

> Peço desculpa pelo meu zelo pelo assunto se lhe faço tantas exigências à sua bondade e paciência; as comunicações que ultimamente lhe enviei são mesmo para mim tão inesperadas, tão novas, que não posso ter paz de espírito até obter de si, amigo honrado, uma decisão sobre a sua correcção. Enquanto não concordar comigo, só posso dizer: *je le vois, mais je ne le crois pas.*

Cantor sabia que o seu resultado era "tão inesperado, tão novo". Mas é duvidoso que alguma vez achasse o seu resultado *inacreditável*. Como Gouvêa observa, estava simplesmente a pedir a Dedekind que verificasse a prova que oferecera.

Quanto à intuição geométrica: Peano publicou a sua curva preenchedora de espaço sem incluir quaisquer diagramas. Mas quando Hilbert publicou a sua curva, explicou o seu propósito: daria aos leitores um modo claro de compreender o resultado de Peano, se "se servirem da seguinte intuição geométrica"; após o que incluiu uma série de *diagramas* tal como os fornecidos em Seção 77.3.

De modo mais geral: embora os diagramas tenham caído um tanto em desuso nas provas publicadas, não há como escapar ao fato de que os matemáticos *com frequência* usam diagramas ao provar resultados. (Grosso modo: bons matemáticos sabem quando podem confiar na intuição geométrica.)

Em suma: não acredite na *exaltação*; ou, pelo menos, não a aceite por adquirido. Para mais sobre isto, pode ler Giaquinto (2007).

## 77.5 Cantor na Reta e no Plano

Algumas circunstâncias em torno da prova de Schröder-Bernstein relacionam-se com a história que discutimos em Seção 77.3. Recordemos que, em 1877, Cantor provou que há tantos pontos num quadrado quanto num dos seus lados. Aqui apresentaremos a sua prova (primeira tentativa).

Seja L o intervalo unitário, isto é, o conjunto de pontos $[0, 1]$. Seja S o quadrado unitário, isto é, o conjunto de pontos $\mathrm{L} \times \mathrm{L}$. Nestes termos, Cantor provou que $\mathrm{L} \approx \mathrm{S}$. Escreveu uma nota a Dedekind, que continha essencialmente o seguinte argumento.

**Teorema 77.1.** *$L \approx S$*

*Prova: primeira parte..* Fixemos $a, b \in \mathrm{L}$. Escrevamos $a$ e $b$ em notação binária, de modo que temos sequências infinitas de 0s e 1s, $a_1, a_2, \ldots$, e $b_1, b_2, \ldots$, tais que:

$$a = 0.a_1a_2a_3a_4\ldots$$
$$b = 0.b_1b_2b_3b_4\ldots$$

Consideremos a função $f : \mathrm{S} \to \mathrm{L}$ dada por

$$f(a, b) = 0.a_1b_1a_2b_2a_3b_3a_4b_4\ldots$$

A função $f$ é uma injeção, pois se $f(a, b) = f(c, d)$, então $a_n = c_n$ e $b_n = d_n$ para todo $n \in \mathbb{N}$, logo $a = c$ e $b = d$. □

Infelizmente, como Dedekind apontou a Cantor, isto não responde à questão original. Considere-se $0.\dot{1}\dot{0} = 0.1010101010\ldots$. Para que $f(a, b) = 0.\dot{1}\dot{0}$, seria preciso:

$$a = 0.\dot{1}\dot{1} = 0.111111\ldots$$
$$b = 0$$

Mas $a = 0.\dot{1}\dot{1} = 1$. Assim, quando dizemos "escrever $a$ e $b$ em notação binária", temos de escolher *qual* notação usar; e, como $f$ deve ser uma *função*, só podemos usar *uma* das duas notações possíveis. Mas se, por exemplo, usarmos a notação simples e escrevermos $a$ como "$1.000\ldots$", então não existe par $\langle a, b\rangle$ tal que $f(a, b) = 0.\dot{1}\dot{0}$.

Em resumo: Dedekind observou que, dada a possibilidade de certas expansões binárias periódicas, a função $f$ de Cantor é uma injeção mas *não* é uma sobrejeção. Cantor tinha mostrado apenas que $\mathrm{S} \preceq \mathrm{L}$ e *não* que $\mathrm{S} \approx \mathrm{L}$.

Cantor respondeu a Dedekind quase de imediato, sugerindo essencialmente que a prova poderia completar-se assim:

*Prova: completada..* Mostramos que $S \preceq L$. Mas é óbvio que existe uma injeção de L para S: basta "deitar" a reta sobre um lado do quadrado. Logo $L \preceq S$ e $S \preceq L$. Pelo teorema de Schröder–Bernstein (Teorema 4.25), $L \approx S$. □

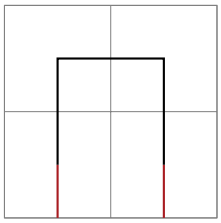
Claro que Cantor não podia justificar a última linha nestes termos, pois o teorema de Schröder-Bernstein ainda não estava provado. De fato, embora Cantor viesse a formulá-lo como conjectura geral, só viria a ser provado de modo satisfatório em 1897. (E assim, mais tarde em 1877, Cantor deu outra prova de Teorema 77.1, que não passava por Schröder–Bernstein.)

## 77.6 Apêndice: Curvas Preenchedoras de Espaço de Hilbert

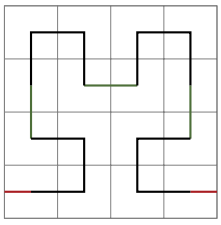
No capítulo Seção 77.3, mencionamos que a prova de Cantor de que uma reta e um quadrado têm exatamente o mesmo número de pontos (Teorema 77.1) levou Peano a perguntar se poderia existir uma *curva* que preenchesse o espaço. Obteve resposta afirmativa em 1890. Nesta secção explicamos (de modo informal) como construir a curva preenchedora de espaço de Hilbert (com um pequeno ajuste).[2]

Temos de definir uma função, $h$, como limite de uma sequência de funções $h_1$, $h_2$, $h_3$, ... Primeiro descrevemos a construção. Depois mostramos que preenche o espaço. Depois mostramos que é uma curva.

Tomaremos a imagem de $h$ como sendo o quadrado unitário, S. Eis a nossa primeira aproximação a $h$, isto é, $h_1$:



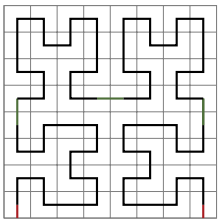
Para orientação, impusemos uma grelha $2 \times 2$ ao quadrado. Podemos pensar na curva como começando no quadrante inferior esquerdo, indo para o superior esquerdo, depois para o superior direito e finalmente para o inferior direito. Eis a segunda etapa da construção, isto é, $h_2$:



[2] Para uma explicação mais rigorosa, ver Rose (2010). O ajuste consiste em incluir as partes vermelhas das curvas abaixo. Isto torna ligeiramente mais fácil verificar que a curva é contínua.

As cores diferentes ajudam a explicar como $h_2$ foi construída. Colocamos primeiro cópias reduzidas do troço não-vermelho de $h_1$ no inferior esquerdo, superior esquerdo, superior direito e inferior direito do quadrado (traçadas a preto). Depois ligamos estas quatro figuras (com linhas verde). Por fim, ligamos a figura ao contorno do quadrado (com linhas vermelho).

Passamos a $h_3$. Tal como $h_2$ foi feita a partir de quatro cópias ligadas e reduzidas do troço não vermelho de $h_1$, $h_3$ compõe-se de quatro cópias reduzidas do troço não vermelho de $h_2$ (a preto), que depois se unem (com linhas verde) e se ligam ao contorno do quadrado (com linhas vermelho).



Agora vê-se o padrão geral para definir $h_{n+1}$ a partir de $h_n$. Por fim definimos a curva *h em si* considerando o limite ponto a ponto destas funções sucessivas $h_1, h_2, \ldots$ Isto é, para cada $x \in \mathrm{S}$:

$$h(x) = \lim_{n\to\infty} h_n(x)$$

Mostramos agora que esta curva preenche o espaço. Ao traçar $h_n$, impomos uma grelha $2^n \times 2^n$ sobre S. Pelo teorema de Pitágoras, a diagonal de cada célula da grelha tem comprimento:

$$\sqrt{(1/2^n)^2 + (1/2^n)^2} = 2^{(\frac{1}{2}-n)}$$

e é evidente que $h_n$ passa por todas as células. Logo cada ponto de S está *a uma distância no máximo* $2^{(\frac{1}{2}-n)}$ de algum ponto de $h_n$. Mas $h$ é definida como o limite das funções $h_1, h_2, h_3, \ldots$ Assim, a distância máxima de qualquer ponto a $h$ é dada por:

$$\lim_{n\to\infty} 2^{(\frac{1}{2}-n)} = 0.$$

Ou seja: todo o ponto de S está à distância 0 de $h$. Em outras palavras, todo o ponto de S situa-se *sobre* a curva. Logo $h$ preenche o espaço!

Resta mostrar que $h$ é, de fato, uma *curva*. Para isso é preciso definir o conceito. A definição moderna baseia-se na de Jordan, de 1887 (isto é, poucos anos antes da primeira curva preenchedora de espaço):

**Definição 77.2.** Uma curva é uma aplicação contínua de L para $\mathbb{R}^2$.

Isto é bastante intuitivo: uma curva é, intuitivamente, uma aplicação "suave" que leva uma reta canônica para o plano $\mathbb{R}^2$. A nossa função $h$ é de fato

uma aplicação de L para $\mathbb{R}^2$. Logo só precisamos de mostrar que $h$ é contínua. Definimos continuidade em Seção 77.2 com a notação $\varepsilon/\delta$. Em linguagem corrente, queremos estabelecer o seguinte: *Se especificar um ponto p em S, juntamente com qualquer nível de precisão ε, podemos encontrar um intervalo aberto de L tal que, dado qualquer x nesse intervalo, $h(x)$ fica a uma distância inferior a ε de p.*

Assim: suponhamos que $p$ e $\varepsilon$ estão fixos. Isto corresponde, em efeito, a traçar um círculo com centro $p$ e raio $\varepsilon$ sobre S. (O círculo pode sair para fora de S, mas não importa.) Recordemos que, ao descrever $h_n$, traçamos uma grelha $2^n \times 2^n$ sobre S. É óbvio que, por pequeno que seja $\varepsilon$, existe algum $n$ tal que alguma célula individual da grelha $2^n \times 2^n$ sobre S fica inteiramente dentro do círculo com centro $p$ e raio $\varepsilon$.

Tomemos esse $n$, e seja $I$ a maior parte aberta de L que $h_n$ mapeia inteiramente para a célula relevante. (É claro que $I$ existe, pois já notamos que $h_n$ passa por todas as células da grelha $2^n \times 2^n$.) Basta agora mostrar que, sempre que $x \in I$, o ponto $h(x)$ pertence à mesma célula. E, para *isso*, basta mostrar que $h_m(x)$ pertence à mesma célula, para qualquer $m > n$. Mas isto é óbvio. Se considerarmos o que acontece com $h_m$ para $m > n$, vemos que exatamente a "mesma parte" do intervalo unitário é mapeada para a mesma célula; apenas a descrevemos de modo cada vez mais esticado e sinuoso.

# Parte XVIII

# Reference

This part collects various lists of alphabets, notations, definitions, rules, etc., for inclusion as appendices in a textbook.

## Capítulo 78

# O Alfabeto Grego

| | | | | | |
|---|---|---|---|---|---|
| Alfa | $\alpha$ | $A$ | Niu | $\nu$ | $N$ |
| Beta | $\beta$ | $B$ | Xi | $\xi$ | $\Xi$ |
| Gama | $\gamma$ | $\Gamma$ | Ômicron | $o$ | $O$ |
| Delta | $\delta$ | $\Delta$ | Pi | $\pi$ | $\Pi$ |
| Épsilon | $\varepsilon$ | $E$ | Rô | $\rho$ | $P$ |
| Zeta | $\zeta$ | $Z$ | Sigma | $\sigma$ | $\Sigma$ |
| Eta | $\eta$ | $H$ | Tau | $\tau$ | $T$ |
| Teta | $\theta$ | $\Theta$ | Ípsilon | $\upsilon$ | $\Upsilon$ |
| Iota | $\iota$ | $I$ | Fi | $\varphi$ | $\Phi$ |
| Capa | $\kappa$ | $K$ | Qui | $\chi$ | $X$ |
| Lambda | $\lambda$ | $\Lambda$ | Psi | $\psi$ | $\Psi$ |
| Mi | $\mu$ | $M$ | Ômega | $\omega$ | $\Omega$ |

## Capítulo 79

# The Fraktur Alphabet

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A | 𝔄 | a | 𝔞 | N | 𝔑 | n | 𝔫 |
| B | 𝔅 | b | 𝔟 | O | 𝔒 | o | 𝔬 |
| C | ℭ | c | 𝔠 | P | 𝔓 | p | 𝔭 |
| D | 𝔇 | d | 𝔡 | Q | 𝔔 | q | 𝔮 |
| E | 𝔈 | e | 𝔢 | R | ℜ | r | 𝔯 |
| F | 𝔉 | f | 𝔣 | S | 𝔖 | s | 𝔰 |
| G | 𝔊 | g | 𝔤 | T | 𝔗 | t | 𝔱 |
| H | ℌ | h | 𝔥 | U | 𝔘 | u | 𝔲 |
| I | ℑ | i | 𝔦 | V | 𝔙 | v | 𝔳 |
| J | 𝔍 | j | 𝔧 | W | 𝔚 | w | 𝔴 |
| K | 𝔎 | k | 𝔨 | X | 𝔛 | x | 𝔵 |
| L | 𝔏 | l | 𝔩 | Y | 𝔜 | y | 𝔶 |
| M | 𝔐 | m | 𝔪 | Z | ℨ | z | 𝔷 |

# Créditos das Imagens

Georg Cantor, p. 541: Retrato de Georg Cantor por Otto Zeth, cortesia do Arquivo Universitário, Martin-Luther-Universität Halle–Wittenberg. UAHW Rep. 40-VI, Nr. 3 Bild 102.

Kurt Gödel, p. 544: Retrato de Kurt Gödel, c. 1925, fotógrafo desconhecido. Do Shelby White and Leon Levy Archives Center, Institute for Advanced Study, Princeton, NJ, EUA, em depósito na Biblioteca da Universidade de Princeton, Divisão de Manuscritos, Departamento de Livros Raros e Coleções

Especiais, Kurt Gödel Papers, (C0282), Box 14b, #110000. O *Open Logic Project* obteve permissão do Arquivo do Instituto para usar esta imagem em materiais derivados do OLP não comerciais. É necessária autorização do Arquivo para qualquer outro uso.

Bertrand Russell, p. 547: Retrato de Bertrand Russell, c. 1907, cortesia da Divisão William Ready de Arquivos e Coleções de Investigação, Biblioteca da McMaster University. Arquivos Bertrand Russell, Box 2, f. 4.

Alfred Tarski, p. 549: Fotografia de passaporte de Alfred Tarski, 1939. Recortada e restaurada a partir de digitalização do passaporte de Tarski por Joel Fuller. Original cortesia da Biblioteca Bancroft, University of California, Berkeley. Alfred Tarski Papers, Banc MSS 84/49. O *Open Logic Project* obteve permissão para usar esta imagem em materiais derivados do OLP não comerciais. É necessária autorização da Biblioteca Bancroft para qualquer outro uso.

Ernst Zermelo, p. 551: Retrato de Ernst Zermelo, c. 1922, cortesia da Abteilung für Handschriften und Seltene Drucke, Niedersächsische Staats- und Universitätsbibliothek Göttingen, Cod. Ms. D. Hilbert 754, Bl. 6 Nr. 25.

# Referências Bibliográficas


Aspray, William. 1984. The Princeton mathematics community in the 1930s: Alonzo Church. URL http://www.princeton.edu/mudd/finding_aids/mathoral/pmc05.htm. Interview.

Baaz, Matthias, Christos H. Papadimitriou, Hilary W. Putnam, Dana S. Scott, and Charles L. Harper Jr. 2011. *Kurt Gödel and the Foundations of Mathematics: Horizons of Truth*. Cambridge: Cambridge University Press.

Banach, Stefan and Alfred Tarski. 1924. Sur la décomposition des ensembles de points en parties respectivement congruentes. *Fundamenta Mathematicae* 6: 244–77.

Benacerraf, Paul. 1965. What numbers could not be. *The Philosophical Review* 74(1): 47–73.

Berkeley, George. 1734. *The Analyst; or, a Discourse Adressed to an Infidel Mathematician*.

Boolos, George. 1971. The iterative conception of set. *The Journal of Philosophy* 68(8): 215–31.

Boolos, George. 1989. Iteration again. *Philosophical Topics* 17(2): 5–21.

Boolos, George. 2000. Must we believe in set theory? In *Between Logic and Intuition: Essays in Honor of Charles Parsons*, eds. Gila Sher and Richard Tieszen, 257–68. Cambridge: Cambridge University Press.

Burali-Forti, Cesare. 1897. Una questione sui numeri transfiniti. *Rendiconti del Circolo Matematico di Palermo* 11: 154–64.

Button, Tim. 2021. Level theory, part 1: Axiomatizing the bare idea of a cumulative hierarchy of sets. *The Bulletin of Symbolic Logic* 27(4): 436–460.

Cantor, Georg. 1878. Ein Beitrag zur Mannigfaltigkeitslehre. *Journal für die reine und angewandte Mathematik* 84: 242–58.

Cantor, Georg. 1883. *Grundlagen einer allgemeinen Mannigfaltigkeitslehre. Ein mathematisch-philosophischer Versuch in der Lehre des Unendlichen*. Leipzig: Teubner.

Cantor, Georg. 1892. Über eine elementare Frage der Mannigfaltigkeitslehre. *Jahresbericht der deutschen Mathematiker-Vereinigung* 1: 75–8.

Cheng, Eugenia. 2004. How to write proofs: A quick quide. URL `https://eugeniacheng.com/wp-content/uploads/2017/02/cheng-proofguide.pdf`.

Church, Alonzo. 1936a. A note on the Entscheidungsproblem. *The Journal of Symbolic Logic* 1: 40–41.

Church, Alonzo. 1936b. An unsolvable problem of elementary number theory. *American Journal of Mathematics* 58: 345–363.

Cohen, Paul J. 1963. The independence of the continuum hypothesis. *Proceedings of the National Academy of Sciences of the United States of America* 24: 556–557.

Cohen, Paul J. 1966. *Set Theory and the Continuum Hypothesis*. Reading, MA: Benjamin.

Conway, John. 2006. The power of mathematics. In *Power*, eds. Alan Blackwell and David MacKay, Darwin College Lectures. Cambridge: Cambridge University Press. URL `http://www.cs.toronto.edu/~mackay/conway.pdf`.

Corcoran, John. 1983. *Logic, Semantics, Metamathematics*. Indianapolis: Hackett, 2nd ed.

Dauben, Joseph. 1990. *Georg Cantor: His Mathematics and Philosophy of the Infinite*. Princeton: Princeton University Press.

Dedekind, Richard. 1888. *Was sind und was sollen die Zahlen?* Braunschweig: Vieweg.

Dick, Auguste. 1981. *Emmy Noether 1882–1935*. Boston: Birkhäuser.

du Sautoy, Marcus. 2014. A brief history of mathematics: Georg Cantor. URL `http://www.bbc.co.uk/programmes/b00ss1j0`. Audio Recording.

Duncan, Arlene. 2015. The Bertrand Russell Research Centre. URL `http://russell.mcmaster.ca/`.

Ebbinghaus, Heinz-Dieter. 2015. *Ernst Zermelo: An Approach to his Life and Work*. Berlin: Springer-Verlag.

Ebbinghaus, Heinz-Dieter, Craig G. Fraser, and Akihiro Kanamori. 2010. *Ernst Zermelo. Collected Works*, vol. 1. Berlin: Springer-Verlag.

Ebbinghaus, Heinz-Dieter and Akihiro Kanamori. 2013. *Ernst Zermelo: Collected Works*, vol. 2. Berlin: Springer-Verlag.

Enderton, Herbert B. 2019. Alonzo Church: Life and Work. In *The Collected Works of Alonzo Church*, eds. Tyler Burge and Herbert B. Enderton. Cambridge, MA: MIT Press.

Feferman, Anita and Solomon Feferman. 2004. *Alfred Tarski: Life and Logic*. Cambridge: Cambridge University Press.

Feferman, Solomon, John W. Dawson Jr., Stephen C. Kleene, Gregory H. Moore, Robert M. Solovay, and Jean van Heijenoort. 1986. *Kurt Gödel: Collected Works. Vol. 1: Publications 1929–1936*. Oxford: Oxford University Press.

Feferman, Solomon, John W. Dawson Jr., Stephen C. Kleene, Gregory H. Moore, Robert M. Solovay, and Jean van Heijenoort. 1990. *Kurt Gödel: Collected Works. Vol. 2: Publications 1938–1974*. Oxford: Oxford University Press.

Feferman, Solomon and Azriel Levy. 1963. Independence results in set theory by Cohen's method II. *Notices of the American Mathematical Society* 10: 593.

Fraenkel, Abraham. 1922. Über den Begriff 'definit' und die Unabhängigkeit des Auswahlaxioms. *Sitzungsberichte der Preussischen Akadademie der Wissenschaften, Physikalisch-mathematische Klasse* 253–257.

Frege, Gottlob. 1884. *Die Grundlagen der Arithmetik: Eine logisch mathematische Untersuchung über den Begriff der Zahl*. Breslau: Wilhelm Koebner. Translation in Frege (1953).

Frege, Gottlob. 1953. *Foundations of Arithmetic*, ed. J. L. Austin. Oxford: Basil Blackwell & Mott, 2nd ed.

Frey, Holly and Tracy V. Wilson. 2015. Stuff you missed in history class: Emmy Noether, mathematics trailblazer. URL `https://www.iheart.com/podcast/stuff-you-missed-in-history-cl-21124503/episode/emmy-noether-mathematics-trailblazer-30207491/`. Podcast audio.

Gentzen, Gerhard. 1935a. Untersuchungen über das logische Schließen I. *Mathematische Zeitschrift* 39: 176–210. English translation in Szabo (1969), pp. 68–131.

Gentzen, Gerhard. 1935b. Untersuchungen über das logische Schließen II. *Mathematische Zeitschrift* 39: 176–210, 405–431. English translation in Szabo (1969), pp. 68–131.

Giaquinto, Marcus. 2007. *Visual Thinking in Mathematics*. Oxford: Oxford University Press.

Gödel, Kurt. 1929. Über die Vollständigkeit des Logikkalküls [On the completeness of the calculus of logic]. Dissertation, Universität Wien. Reprinted and translated in Feferman et al. (1986), pp. 60–101.

Gödel, Kurt. 1931. über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme I [On formally undecidable propositions of *Principia Mathematica* and related systems I]. *Monatshefte für Mathematik und Physik* 38: 173–198. Reprinted and translated in Feferman et al. (1986), pp. 144–195.

Gödel, Kurt. 1938. The consistency of the axiom of choice and the generalized continuum hypothesis. *Proceedings of the National Academy of Sciences of the United States of America* 50: 1143–8.

Gouvêa, Fernando Q. 2011. Was Cantor surprised? *American Mathematical Monthly* 118(3): 198–209.

Grattan-Guinness, Ivor. 1971. Towards a biography of Georg Cantor. *Annals of Science* 27(4): 345–391.

Hammack, Richard. 2013. *Book of Proof*. Richmond, VA: Virginia Commonwealth University. URL `http://www.people.vcu.edu/~rhammack/BookOfProof/BookOfProof.pdf`.

Hartogs, Friedrich. 1915. Über das Problem der Wohlordnung. *Mathematische Annalen* 76: 438–43.

Hausdorff, Felix. 1914. Bemerkung über den Inhalt von Punktmengen. *Mathematische Annalen* 75: 428–34.

Heck, Richard Kimberly. 2012. *Reading Frege's Grundgesetze*. Oxford: Oxford University Press.

Heijenoort, Jean van. 1967. *From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931*. Cambridge, MA: Harvard University Press.

Hilbert, David. 1891. Über die stetige Abbildung einer Linie auf ein Flächenstück. *Mathematische Annalen* 38(3): 459–460.

Hilbert, David. 2013. *David Hilbert's Lectures on the Foundations of Arithmetic and Logic 1917–1933*, eds. William Bragg Ewald and Wilfried Sieg. Heidelberg: Springer.

Hodges, Andrew. 2014. *Alan Turing: The Enigma*. London: Vintage.

Hume, David. 1740. *A Treatise of Human Nature*. London.

Hutchings, Michael. 2003. Introduction to mathematical arguments. URL https://math.berkeley.edu/~hutching/teach/proofs.pdf.

Incurvati, Luca. 2020. *Conceptions of Set and the Foundations of Mathematics*. Cambridge: Cambridge University Press.

Institute, Perimeter. 2015. Emmy Noether: Her life, work, and influence. URL https://www.youtube.com/watch?v=tNNyAyMRsgE. Video Lecture.

Irvine, Andrew David. 2015. Sound clips of Bertrand Russell speaking. URL http://plato.stanford.edu/entries/russell/russell-soundclips.html.

Jacobson, Nathan. 1983. *Emmy Noether: Gesammelte Abhandlungen—Collected Papers*. Berlin: Springer-Verlag.

John Dawson, Jr. 1997. *Logical Dilemmas: The Life and Work of Kurt Gödel*. Boca Raton: CRC Press.

Katz, Karin Usadi and Mikhail G. Katz. 2012. Stevin numbers and reality. *Foundations of Science* 17(2): 109–23.

Kunen, Kenneth. 1980. *Set Theory: An Introduction to Independence Proofs*. New York: North Holland.

Lévy, Azriel. 1960. Axiom schemata of strong infinity in axiomatic set theory. *Pacific Journal of Mathematics* 10(1): 223–38.

LibriVox. n.d. Bertrand Russell. URL https://librivox.org/author/1508?primary_key=1508&search_category=author&search_page=1&search_form=get_results. Collection of public domain audiobooks.

Linnebo, Øystein. 2010. Predicative and impredicative definitions. *Internet Encyclopedia of Philosophy* URL http://www.iep.utm.edu/predicat/.

Linsenmayer, Mark. 2014. The partially examined life: Gödel on math. URL http://www.partiallyexaminedlife.com/2014/06/16/ep95-godel/. Podcast audio.

MacFarlane, John. 2015. Alonzo Church's JSL reviews. URL http://johnmacfarlane.net/church.html.

Maddy, Penelope. 1988a. Believing the axioms I. *The Journal of Symbolic Logic* 53(2): 481–511.

Maddy, Penelope. 1988b. Believing the axioms II. *The Journal of Symbolic Logic* 53(3): 736–64.

Magnus, P. D., Tim Button, J. Robert Loftis, Aaron Thomas-Bolduc, Robert Trueman, and Richard Zach. 2021. *Forall x: Calgary. An Introduction to Formal Logic*. Calgary: Open Logic Project, f21 ed. URL https://forallx.openlogicproject.org/.

Menzler-Trott, Eckart. 2007. *Logic's Lost Genius: The Life of Gerhard Gentzen*. Providence: American Mathematical Society.

Montague, Richard. 1961. Semantic closure and non-finite axiomatizability I. In *Infinitistic Methods: Proceedings of the Symposium on Foundations of Mathematics (Warsaw 1959)*, 45–69. New York: Pergamon.

Montague, Richard. 1965. Set theory and higher-order logic. In *Formal systems and recursive functions*, eds. John Crossley and Michael Dummett, 131–48. Amsterdam: North-Holland. Proceedings of the Eight Logic Colloquium, July 1963.

O'Connor, John J. and Edmund F. Robertson. 2005. The real numbers: Stevin to Hilbert URL http://www-history.mcs.st-and.ac.uk/HistTopics/Real_numbers_2.html.

Peano, Giuseppe. 1890. Sur une courbe, qui remplit toute une aire plane. *Mathematische Annalen* 36(1): 157–60.

Potter, Michael. 2004. *Set Theory and its Philosophy*. Oxford: Oxford University Press.

Radiolab. 2012. The Turing problem. URL http://www.radiolab.org/story/193037-turing-problem/. Podcast audio.

Ramsey, Frank Plumpton. 1925. The foundations of mathematics. *Proceedings of the London Mathematical Society* 25: 338–384.

Robinson, Raphael. 1947. On the decomposition of spheres. *Fundamenta Mathematicae* 34(1): 246–60.

Rose, Daniel. 2012. A song about Georg Cantor. URL https://www.youtube.com/watch?v=QUP5Z4Fb5k4. Audio Recording.

Rose, Nicholas J. 2010. Hilbert-type space-filling curves. URL https://web.archive.org/web/20151010184939/http://www4.ncsu.edu/~njrose/pdfFiles/HilbertCurve.pdf.

Russell, Bertrand. 1905. On denoting. *Mind* 14: 479–493.

Russell, Bertrand. 1919. *Introduction to Mathematical Philosophy*. London: Allen & Unwin.

Russell, Bertrand. 1967. *The Autobiography of Bertrand Russell*, vol. 1. London: Allen and Unwin.

Russell, Bertrand. 1968. *The Autobiography of Bertrand Russell*, vol. 2. London: Allen and Unwin.

Russell, Bertrand. 1969. *The Autobiography of Bertrand Russell*, vol. 3. London: Allen and Unwin.

Russell, Bertrand. n.d. Bertrand Russell on smoking. URL `https://www.youtube.com/watch?v=80oLTiVW_lc`. Video Interview.

Sandstrum, Ted. 2019. *Mathematical Reasoning: Writing and Proof*. Allendale, MI: Grand Valley State University. URL `https://scholarworks.gvsu.edu/books/7/`.

Scott, Dana. 1974. Axiomatizing set theory. In *Axiomatic Set Theory II*, ed. Thomas Jech, 207–14. American Mathematical Society. Proceedings of the Symposium in Pure Mathematics of the American Mathematical Society, July–August 1967.

Segal, Sanford L. 2014. *Mathematicians under the Nazis*. Princeton: Princeton University Press.

Shoenfield, Joseph R. 1977. Axioms of set theory. In *Handbook of Mathematical Logic*, ed. Jon Barwise, 321–44. London: North-Holland.

Sigmund, Karl, John Dawson, Kurt Mühlberger, Hans Magnus Enzensberger, and Juliette Kennedy. 2007. Kurt Gödel: Das Album–The Album. *The Mathematical Intelligencer* 29(3): 73–76.

Skolem, Thoralf. 1922. Einige Bemerkungen zur axiomatischen Begründung der Mengenlehre. In *Wissenschaftliche Vorträge gehalten auf dem fünften Kongress der skandanivschen Mathematiker in Helsingfors vom 4. bis zum 7. Juli 1922*, 137–52. Akademiska Bokhandeln.

Smith, Peter. 2013. *An Introduction to Gödel's Theorems*. Cambridge: Cambridge University Press.

Smullyan, Raymond M. 1968. *First-Order Logic*. New York, NY: Springer. Corrected reprint, New York, NY: Dover, 1995.

Solow, Daniel. 2013. *How to Read and Do Proofs*. Hoboken, NJ: Wiley.

Steinhart, Eric. 2018. *More Precisely: The Math You Need to Do Philosophy*. Peterborough, ON: Broadview, 2nd ed.

Sykes, Christopher. 1992. BBC Horizon: The strange life and death of Dr. Turing. URL `https://www.youtube.com/watch?v=gyusnGbBSHE`.

Szabo, Manfred E. 1969. *The Collected Papers of Gerhard Gentzen*. Amsterdam: North-Holland.

Takeuti, Gaisi, Nicholas Passell, and Mariko Yasugi. 2003. *Memoirs of a Proof Theorist: Gödel and Other Logicians*. Singapore: World Scientific.

Tarski, Alfred. 1981. *The Collected Works of Alfred Tarski*, vol. I–IV. Basel: Birkhäuser.

Theelen, Andre. 2012. Lego turing machine. URL `https://www.youtube.com/watch?v=FTSAiF9AHN4`.

Tomkowicz, Grzegorz and Stan Wagon. 2016. *The Banach-Tarski Paradox*. Cambridge: Cambridge University Press.

Turing, Alan M. 1937. On computable numbers, with an application to the "Entscheidungsproblem". *Proceedings of the London Mathematical Society, 2nd Series* 42: 230–265.

Tyldum, Morten. 2014. The imitation game. Motion picture.

Velleman, Daniel J. 2019. *How to Prove It: A Structured Approach*. Cambridge: Cambridge University Press, 3rd ed.

Vitali, Giuseppe. 1905. *Sul problema della misura dei gruppi di punti di una retta*. Bologna: Gamberini e Parmeggiani.

von Neumann, John. 1925. Eine Axiomatisierung der Mengenlehre. *Journal für die reine und angewandte Mathematik* 154: 219–40.

Wang, Hao. 1990. *Reflections on Kurt Gödel*. Cambridge: MIT Press.

Weston, Tom. 2003. The Banach-Tarski paradox URL `http://people.math.umass.edu/~weston/oldpapers/banach.pdf`.

Whitehead, Alfred North and Bertrand Russell. 1910. *Principia Mathematica*, vol. 1. Cambridge: Cambridge University Press.

Zermelo, Ernst. 1904. Beweis, daß jede Menge wohlgeordnet werden kann. *Mathematische Annalen* 59: 514–516. English translation in (Ebbinghaus et al., 2010, pp. 115–119).

Zermelo, Ernst. 1908a. Untersuchungen über die Grundlagen der Mengenlehre I. *Mathematische Annalen* 65: 261–81.

Zermelo, Ernst. 1908b. Untersuchungen über die Grundlagen der Mengenlehre I. *Mathematische Annalen* 65(2): 261–281. English translation in (Ebbinghaus et al., 2010, pp. 189-229).

Zuckerman, Martin M. 1973. Formation sequences for propositional formulas. *Notre Dame Journal of Formal Logic* 14(1): 134–138.