

Parte I

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 1

Provas

1.1 Introdução

math:prf:int:
sec

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 φ a fórmula da forma $\psi \rightarrow \chi$ ” 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 φ a fórmula da forma $\psi \rightarrow \chi$ ”, você está provando algo apenas sobre todas as fórmulas de certo tipo (a saber, condicionais), e fica entendido que $\psi \rightarrow \chi$ é um condicional arbitrário sobre o qual sua prova falará.

1.2 Começando uma Prova

Mas por onde começar?

meth:prf:str:
sec

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.

1.3 Usando Definições

mod:prf:def:
sec

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 1.1. *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 1.2. 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 $A \cup B = B \cup A$. (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

¹Neste 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.

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 $x \in \{z : \dots z \dots\}$ sse $\dots x \dots$. Assim, desdobrando ainda mais a definição da notação $\{z : \dots z \dots\}$, 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 1.3. *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.

Problema 1.1. 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 “ $\emptyset$ ”.

1.4 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).

math:prf:pat:
sec

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, φ 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 1.4. *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 $x \in A \cup B$. $\square$

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 “distinguímos 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 “Distinguímos 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 1.5. *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 $x \in E$. Distinguímos 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 $x \in E$. $\square$

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 $\dots x \dots$ ”, isto é, que algum objeto tem a propriedade descrita por “ $\dots x \dots$ ”. 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 $x \dots$ ” (em que $\dots$ especifica qual objeto você tem em mente), possivelmente provando que $\dots$ de fato descreve um objeto que existe, e então passaria a mostrar que x tem a propriedade Q . Eis um exemplo simples.

Proposição 1.6. *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 $x \notin \emptyset$.

²Este 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.

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 $\subseteq$, $A \subseteq B$. $\square$

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 1.7. *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 disjuncto 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 $A \cup B \neq \emptyset$. $\square$

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?

1.5 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. mth:prf:ex1:sec

Proposição 1.8. *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 $z \in \{z : \dots z \dots\}$ sse $\dots z \dots$, 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 $z \in B$. Distinguímos 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 $z \in C$. Distinguímos 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 $z \in A \cup (B \cap C)$. □

1.6 Outro Exemplo

math:prf:ex2:
sec

Proposição 1.9. 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 conseqüente.

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 **mem-bros** 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 $A \cup (C \setminus A) = C$. □

1.7 Prova por Contradição

math:prf:con:
sec

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 1.10. *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. $\square$

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 1.11. $A \subseteq A \cup B$.

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, $A \not\subseteq A \cup B$.

Temos uma definição de $A \subseteq A \cup B$: todo $x \in A$ está também $\in A \cup B$. Para entender o que $A \not\subseteq A \cup B$ 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 $\notin A \cup B$. (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, $A \not\subseteq A \cup B$ 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 $x \notin A \cup B$. $\square$

Problema 1.2. Prove *indiretamente* que $A \cap B \subseteq A$.

Proposição 1.12. 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, $A \not\subseteq C$.

Como antes, raciocinamos que $A \not\subseteq C$ 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 $x \notin C$. $\square$

Proposição 1.13. 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 $A \not\subseteq B$ ou $B \not\subseteq A$. (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 $A \not\subseteq B$ ou $B \not\subseteq A$. Distinguimos casos.

No primeiro caso, supomos $A \not\subseteq B$, isto é, para algum x , $x \in A$ mas $x \notin B$. $A \cap B$ 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 $A \cap B = A \cup B$. $\square$

1.8 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.

[mth:prf:rea:sec](#)

Proposição 1.14 (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 $z \in A \cap (A \cup B)$. $\square$

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) $A \cap (A \cup B) \supseteq A$. (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)]. $\square$

Problema 1.3. 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 $\in A \cup (A \cap B)$. $\square$

1.9 Não Consigo Fazer Isso!

Todos nós chegamos a um ponto em que sentimos vontade de desistir. Mas *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. mth:prf:cnt:
sec

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.

1.10 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>

Capítulo 2

Indução

2.1 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. mth:ind:int:sec

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.

2.2 Indução em $\mathbb{N}$

math.ind.inN:
sec

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 2.1. *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. $\square$

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

$$\begin{aligned}s_0 &= 0 \\ s_{n+1} &= s_n + (n + 1)\end{aligned}$$

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 2.2. $s_n = n(n + 1)/2$.

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:

$$\begin{aligned} s_{k+1} &= \frac{k(k+1)}{2} + (k+1) = \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \\ &= \frac{k(k+1) + 2(k+1)}{2} = \\ &= \frac{(k+2)(k+1)}{2}. \end{aligned} \quad \square$$

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 .

2.3 Indução Forte

meth:ind:str:
sec 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 , $\forall x (\varphi(x) \rightarrow \psi(x))$ é verdadeiro se nenhum x satisfaz $\varphi(x)$. Neste caso, a

versão formalizada seria “ $\forall l (l < k \rightarrow P(l))$ ”—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 $l < k$.

2.4 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 seqüências 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 $[\text{ e }]$, 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. mth:ind:idf:
sec

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 2.3 (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 $\circ$ 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,

a, b, c, d

No segundo passo, aplicamos (2) aos termos que construímos. Obteremos

$$[a \circ a], [a \circ b], [b \circ a], \dots, [d \circ d]$$

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 $[a \circ [a \circ a]]$ —em que t é a do passo 1 e s é $[a \circ a]$ do passo 2—e $[[b \circ c] \circ [d \circ b]]$ construído a partir dos dois termos $[b \circ c]$ e $[d \circ b]$ 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 o 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 2.4. *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 $[, \circ,]$). 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. $\square$

Problema 2.1. 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 $\leq n/2 + 1$.

2.5 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 $x \mapsto x + 1$.

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 2.5. *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 $o(s_1, s_2)$. $\square$

Problema 2.2. Prove, por indução estrutural, que nenhum termo bonito começa com $]$.

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.

meth:ind:sti: **Proposição 2.6.** *Todo segmento inicial próprio de um termo bonito t tem mais $[$ do que $]$.*
prop:initial

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 $]$. $\square$

2.6 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 2.7. 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 $a \sqsubseteq [b \circ a]$. Pois (2) diz que $a \sqsubseteq [b \circ a]$ sse $a = [b \circ a]$, ou $a \sqsubseteq b$, ou $a \sqsubseteq a$. As duas primeiras são falsas: a claramente não é idêntico a $[b \circ a]$, 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 2.8. 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 , $b \circ d$, $b \circ a \circ b$. Agora, se definíssemos “subtermo” para termos sem colchetes do modo como fizemos acima, a segunda cláusula diria

Se $t_2 = s_1 \circ s_2$, então $t_1 \sqsubseteq t_2$ sse $t_1 = t_2$, $t_1 \sqsubseteq s_1$, ou $t_1 \sqsubseteq s_2$.

Agora, $b \circ a \circ b$ é da forma $s_1 \circ s_2$ com

$$s_1 = b \text{ e}$$

$$s_2 = a \circ b.$$

Ele também é da forma $r_1 \circ r_2$ com

$$r_1 = b \circ a \text{ e}$$

$$r_2 = b.$$

Agora, $a \circ b$ é um subtermo de $b \circ a \circ b$? 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 2.9. *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 2.6**, isso é impossível se s_1 e r_1 são ambos termos bonitos. Mas se $s_1 = r_1$, então claramente também $s_2 = r_2$. $\square$

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 2.10. *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,

$$\begin{aligned} f([a \circ b]) &= \max(f(a), f(b)) + 1 = \\ &= \max(0, 0) + 1 = 1, \text{ e} \\ f([[a \circ b] \circ c]) &= \max(f([a \circ b]), f(c)) + 1 = \\ &= \max(1, 0) + 1 = 2. \end{aligned}$$

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 $a \circ b \circ c \circ d$. Ele pode ser lido de mais de um modo, por exemplo, como $s_1 \circ s_2$ com

$$s_1 = a \text{ e } s_2 = b \circ c \circ d,$$

ou como $r_1 \circ r_2$ com

$$r_1 = a \circ b \text{ e } r_2 = c \circ d.$$

Calcular g de acordo com o primeiro modo de lê-lo daria

$$\begin{aligned} g(s_1 \circ s_2) &= \max(g(a), g(b \circ c \circ d)) + 1 = \\ &= \max(0, 2) + 1 = 3 \end{aligned}$$

enquanto, de acordo com a outra leitura, obtemos

$$\begin{aligned} g(r_1 \circ r_2) &= \max(g(a \circ b), g(c \circ d)) + 1 = \\ &= \max(1, 1) + 1 = 2 \end{aligned}$$

Mas uma função deve sempre produzir um valor único; então nossa “definição” de g não define função alguma.

Problema 2.3. Dê uma definição indutiva da função l , em que $l(t)$ é o número de símbolos no termo bonito t .

Problema 2.4. 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 2.10](#)).

Créditos das Imagens

Referências Bibliográficas

- Cheng, Eugenia. 2004. How to write proofs: A quick guide. URL <https://eugeniacheng.com/wp-content/uploads/2017/02/cheng-proofguide.pdf>.
- Hammack, Richard. 2013. *Book of Proof*. Richmond, VA: Virginia Commonwealth University. URL <http://www.people.vcu.edu/~rhammack/BookOfProof/BookOfProof.pdf>.
- Hutchings, Michael. 2003. Introduction to mathematical arguments. URL <https://math.berkeley.edu/~hutching/teach/proofs.pdf>.
- Sandstrum, Ted. 2019. *Mathematical Reasoning: Writing and Proof*. Allendale, MI: Grand Valley State University. URL <https://scholarworks.gvsu.edu/books/7/>.
- 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.
- Velleman, Daniel J. 2019. *How to Prove It: A Structured Approach*. Cambridge: Cambridge University Press, 3rd ed.