

prf.1 Padrões de Inferência

mth:prf:pat:
sec

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, 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 prf.1. *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 “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 prf.2. *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 $x \in E$.¹

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 $\dots x \dots$ ”, 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

¹Este 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.

provando que ... de fato descreve um objeto que existe, e então passaria a mostrar que x tem a propriedade Q . Eis um exemplo simples.

Proposição prf.3. *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 $\subseteq$, $A \subseteq B$. $\square$

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 prf.4. *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 disjuntivo 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?

Créditos das Imagens

Referências Bibliográficas