Técnicas de Prova

Profa. Sheila Morais de Almeida

DAINF-UTFPR-PG

junho - 2018

Este material é preparado usando como referências os textos dos seguintes livros.

GERSTING, Judith L.,*Mathematical Structures For Computer Science: A Modern Approach to Discrete Mathematics, 6th ed., 2007.*

ROSEN, Kenneth H., Discrete Mathematics and its applications, 6th ed., 2007.

Terminologia

Teoremas são enunciados matemáticos que podem ser provados, geralmente expressos na forma $P \to Q$.

P é chamada de **hipótese**.

Q é chamada de **conclusão**.

Geralmente os teoremas são os resultados mais importantes de um estudo.

Outros enunciados que podem ser provados para auxiliar na prova de um teorema são chamados de **Proposição** ou **Lema**.

Técnicas de Prova

Definição

Uma prova é um argumento válido que mostra a veracidade de um enunciado matemático.

Para provar algo, pode-se assumir como verdade:

- a hipótese,
- axiomas,
- resultados que tenham sido provados anteriormente.

Com esses fatos, equivalências lógicas e regras de inferência, resta mostrar a validade do enunciado.

Terminologia

Axiomas são verdades absolutas, não precisam ser provados.

Corolários são consequências diretas de teoremas que já foram provados.

Conjecturas são hipóteses que ainda não foram provadas, mas que acredita-se que sejam verdadeiras devido a algumas evidências parciais ou intuição de algum especialista no assunto.

Terminologia

Sobre conjecturas:

- Quando uma conjectura é provada, ela se torna um teorema.
- Se um contraexemplo para uma conjectura for apresentado, a conjectura é falsa e não é um teorema.

Terminologia

Exemplo:

Conjectura

Se x é um número inteiro positivo, então $2^x > x!$.

Vamos averiguar alguns casos, para conferir se vale a pena nos dedicarmos a provar esta conjectura.

Conjectura

Se x é um número inteiro positivo, então $2^x > x!$.

Vamos averiguar alguns casos, para conferir se vale a pena nos dedicar a provar esta conjectura.

Quando $x = 1$, tem-se $2^1 > 1!$, ou seja, $2 > 1$.

Quando $x = 2$, tem-se $2^2 > 2!$, ou seja, $4 > 2$.

Terminologia

Conjectura

Se x é um número inteiro positivo, então $2^x > x!$.

Vamos averiguar alguns casos, para conferir se vale a pena nos dedicar a provar esta conjectura.

Quando $x = 1$, tem-se $2^1 > 1!$, ou seja, $2 > 1$.

Quando $x = 2$, tem-se $2^2 > 2!$, ou seja, $4 > 2$.

Quando $x = 3$, tem-se $2^3 > 3!$, ou seja, $8 > 6$.

Quando $x = 4$, tem-se $2^4 > 4!$, ou seja $16 > 24$. Falso!

Conjectura

Se x é um número inteiro positivo, então $2^x > x!$.

A conjectura é falsa! **Contraexemplo:** $x = 4$.

Um **contraexemplo** é um caso que satisfaz as hipóteses, mas para o qual a conclusão é falsa.

Um único contraexemplo é suficiente para garantir que uma conjectura é falsa.

Forneça contra-exemplos para as seguintes sentenças:

- Se n é um inteiro par, então n não é primo.
- Se n^2 é ímpar, então n é múltiplo de 3.

Terminologia

Forneça contra-exemplos para as seguintes sentenças:

- Se n é um inteiro par, então n não é primo. $n = 2$
- Se n^2 é ímpar, então n é múltiplo de 3. $n = 1$

Terminologia

Quando avaliamos a conjectura em vários casos e não encontramos contraexemplos, nos sentimos mais encorajados a provar sua validade.

Conjectura

Se x e y são números reais positivos e $x > y$, então $x^2 > y^2$.

Alguns testes:

Para $x = \frac{1}{2}$ e $y = \frac{1}{3}$, tem-se: $\left(\frac{1}{2}\right)^2 > \left(\frac{1}{3}\right)^2$, ou seja, $\frac{1}{4} > \frac{1}{9}$.

Para $x = \frac{1}{4}$ e $y = \frac{1}{5}$, tem-se: $\left(\frac{1}{4}\right)^2 > \left(\frac{1}{5}\right)^2$, ou seja, $\frac{1}{16} > \frac{1}{25}$.

Para $x = 2$ e $y = 1$, tem-se: $2^2 > 1^2$, ou seja, $4 > 1$.

Para $x = 3$ e $y = 2$, tem-se: $3^2 > 2^2$, ou seja, $9 > 4$.

Conjectura

Se x e y são números reais positivos e $x > y$, então $x^2 > y^2$.

Para provar essa conjectura, podemos assumir que as hipóteses são verdadeiras:

- x é um número real positivo;
- y é um número real positivo;
- $x > y$.

Terminologia

Além das hipóteses, podemos usar como axiomas algumas propriedades dos números reais:

1. Se $x > y$, então $xx > xy$.
2. Da mesma forma, se $x > y$, então $xy > yy$.
3. De (1) e (2), pode-se concluir que $xx > xy > yy$.
4. Portanto, $xx > yy$. $\square$

Terminologia

Partindo da hipótese e de propriedades conhecidas (que são axiomas, lemas, proposições e teoremas já provados), usamos regras de inferência para garantir a conclusão de uma Conjectura.

(No exemplo, levam a concluir que $x^2 > y^2$.)

Ao chegar nessa conclusão, desde que as regras de derivação sejam válidas e tenham se baseado em premissas verdadeiras, a Conjectura está provada, ou seja, agora pode ser chamada de Lema ou Teorema.

Teorema

Se x e y são números reais positivos e $x > y$, então $x^2 > y^2$.

Terminologia

Conjectura

Se um número n é divisível por 6, então n é divisível por 3.

Podemos testar vários casos:
12 é divisível por 6 $\rightarrow 12 = 3 \times 4$
42 é divisível por 6 $\rightarrow 42 = 3 \times 14$
48 é divisível por 6 $\rightarrow 48 = 3 \times 16$

Quanto mais casos encontramos satisfazendo as condições, mais confiantes ficamos de que é possível provar a conjectura.

Concluir algo baseado na experiência é um processo chamado de **Raciocínio Indutivo**.

Terminologia

Conjectura

Se um número n é divisível por 6, então n é divisível por 3.

Mas alguns casos não bastam para termos certeza de que a conjectura é sempre verdadeira.

Para prová-la, todo o universo que seu enunciado abrange deve ser verificado.

(Nesse caso, para qualquer que seja o número divisível por 6, a conjectura precisa ser verdadeira).

Apresentar uma prova ou um contraexemplo para a conjectura, é um processo chamado de **Raciocínio Dedutivo**.

Prova por Exaustão

Considere uma conjectura $P \to Q$.

Se o domínio de P for suficientemente restrito, podemos verificar todos os casos possíveis para mostrar que a conjectura é verdadeira.

Conjectura: Se $x \in \{0, 1, 2, 3\}$, então $2^x \geq x!$.

Prova por exaustão:

$2^0 \geq 1!$, ou seja, $1 \geq 1$.

$2^1 \geq 1!$, ou seja, $2 \geq 1$.

$2^2 \geq 2!$, ou seja, $4 \geq 2$.

$2^3 \geq 3!$, ou seja, $8 \geq 6$. $\square$

Técnicas de Prova

Para provar uma conjectura $A \to B$, lembre-se das tabela verdade da implicação:

$A \to B$ é verdade, a menos que A seja verdade e B seja falso.

A	B	$A \to B$
V	V	V
V	F	F
F	V	V
F	F	V

Então para provar que $A \to B$ é verdade, só precisamos provar que quando A é verdade, B também é verdade.

Prova Direta

Para construir uma prova direta para uma afirmação do tipo $A \to B$:

- suponha que A é verdade;
- os passos seguintes são construídos utilizando-se axiomas, lemas, equivalências lógicas e regras de derivação;
- a última regra de inferência deve implicar que B também é verdade.

Prova Direta

Definição

Um número inteiro n é divisível por um número k se $n = ky$, para algum inteiro y.

Dizemos também que n é múltiplo de k.

Exemplo 1

Conjectura: Se um número n é divisível por 6, então n é divisível por 3.

Prova Direta: Seja n um número divisível por 6.

Então, por definição, $n = 6y$, para algum inteiro y.

Como $6 = 3 \times 2$, podemos escrever $n = 6y = 3 \cdot 2 \cdot y = 3(2y)$.

Então $n = 3z$, onde $z = 2y$ é um inteiro. Então, por definição, n é divisível por 3. $\square$

Prova Direta

Definição

Um número inteiro n é par se existe um inteiro k tal que $n = 2k$.

Definição

Um número inteiro n é ímpar se existe um inteiro k tal que $n = 2k + 1$.

Note que um inteiro ou é par ou é ímpar, e nenhum inteiro é par e ímpar.

Exemplo 2

Conjectura: Se n é um inteiro ímpar, então n^2 é ímpar.

Demonstração: Suponha que a hipótese é verdadeira, ou seja, n é ímpar.

Pela definição de um inteiro ímpar, tem-se $n = 2k + 1$, onde k é algum inteiro.

Nós queremos mostrar que n^2 também é ímpar.

(Podemos elevar os dois lados da equação $n = 2k + 1$ ao quadrado para obter uma nova equação que expressa n^2.)

Então, $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Como k é inteiro, $2k^2 + 2k$ é um número inteiro.

Vamos chamar $2k^2 + 2k$ de z.

Então $n^2 = 2z + 1$.

Por definição de número ímpar, podemos concluir que n^2 é ímpar.
(n^2 é duas vezes um inteiro mais 1.)

Portanto, se n é um inteiro ímpar, então n^2 é ímpar. $\square$

Exemplo 3

Conjectura: Se m e n são números pares, então mn também é par.

Demonstração: Para produzir uma prova direta desse teorema, suponha que a hipótese é verdadeira, ou seja, considere que n e m são números pares.

Pela definição de números pares, sabemos que existem dois números inteiros s e t tais que $m = 2s$ e $n = 2t$.

(O objetivo dessa prova é mostrar que mn é par quando m e n são pares.)

Prova Direta

Para conseguir uma equação com mn, vamos multiplicar as duas equações $m = 2s$ e $n = 2t$.

Com essa multiplicação, obtemos $mn = 2s \cdot 2t$, o que implica que $mn = 2s \cdot 2t = 2(2st)$.

Pela definição de número par, isso implica que mn também é par, pois é um número inteiro $(2st)$ multiplicado por 2.

Portanto, se m e n são pares, então mn também é par. $\square$

Exemplos de Provas

Definição

Um número real r é **racional** se existem inteiros p e q com $q \neq 0$ tais que $r = \frac{p}{q}$.

Definição

Um número real que não é racional é um número **irracional**.

Exemplo 4

Conjectura: A soma de dois números racionais é racional.

(Note que nós queremos provar que:
"Se r e s são quaisquer números racionais, então $r + s$ é racional.".)

Demonstração: Considere que r e s são números racionais.

Pela definição de números racionais, isso implica que:

- existem números inteiros, p e q, com $q \neq 0$, tais que $r = \frac{p}{q}$,
- existem inteiros t e u, com $u \neq 0$, tais que $s = \frac{t}{u}$.

(Podemos usar essa informação para mostrar que $r + s$ é racional?)

Prova Direta

Somando $r = \frac{p}{q}$ e $s = \frac{t}{u}$, obtém-se:

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu}.$$

Como $q \neq 0$ e $u \neq 0$, isso implica que $qu \neq 0$.

Consequentemente, pode-se expressar $r + s$ como uma fração de dois inteiros, $pu + qt$ e qu, onde $qu \neq 0$.

Então, pela definição de números racionais, $r + s$ é racional.

Portanto, a soma de dois números racionais é racional. $\square$

Provas Indiretas

Foi Visto

Provas diretas assumem que a hipótese é verdadeira e usam regras de derivação para mostrar que a conclusão é verdadeira.

Definição

Provas indiretas são provas que não começam assumindo que a hipótese é verdadeira para mostrar que a conclusão é verdadeira.

Veremos duas técnicas de provas indiretas:

- contraposição;
- e contradição.

Prova por Contraposição

A prova por contraposição faz uso do fato de que a proposição $A \to B$ é equivalente à sua contrapositiva $\neg B \to \neg A$.

A	B	$A \to B$	$\neg B$	$\neg A$	$\neg B \to \neg A$
V	V	V	F	F	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

Prova por Contraposição

Observação

Pela equivalência entre essas proposições, $A \to B$ pode ser provada mostrando-se que sua contrapositiva, $\neg B \to \neg A$, é verdade.

Em uma prova por contraposição de $A \to B$, deve-se:

1. considerar que $\neg B$ é verdade,
2. usar axiomas, definições e teoremas já provados, junto com equivalências lógicas e regras de inferência,
3. e concluir que $\neg A$ é verdade.

Exemplo 5

Conjectura: Seja n um número inteiro. Se $3n + 2$ é ímpar, então n é ímpar.

Por contraposição, vamos provar que $\neg B \rightarrow \neg A$.

1. considerar que $\neg B$ é verdade,
2. usar axiomas, definições e teoremas já provados, junto com regras de inferência e equivalências lógicas e
3. concluir que $\neg A$ é verdade.

Prova por Contraposição

Exemplo 5

Conjectura: Seja n um número inteiro. Se $3n + 2$ é ímpar, então n é ímpar.

Demonstração: Por contraposição, suponha que n não é ímpar. Como n é um número inteiro, conclui-se que n é par.

Então, por definição de número par, $n = 2k$ para algum inteiro k.

Consequentemente, $3n + 2 = 3(2k) + 2$.

Então $3n + 2 = 6k + 2 = 2(3k + 1)$ e, como k é inteiro, $3k + 1$ é inteiro.

Portanto, $3n + 2$ é par (pois é um múltiplo de dois), e então não é ímpar. $\square$

"Portanto, $3n + 2$ é par (pois é um múltiplo de dois)."

Isso é uma negação da hipótese! Provamos que $\neg A$ é verdade, concluindo o teorema.

Exemplo 6

Conjectura: Seja n um número inteiro. Se n é divisível por 6, então n é divisível por 3.

Demonstração: Seja n um número inteiro. Por contraposição, suponha que n não é divisível por 3.

Então, para todo k inteiro $n \neq 3k$.

Então, mesmo se k for par, $n \neq 3k$. Ou seja, $n \neq 3(2y)$, para todo y inteiro.

Então, $n \neq 6y$, para todo y inteiro. Ou seja, ão existe y inteiro tal que $n = 6y$.

Portanto n não é divisível por 6. $\square$

Equivalência entre Implicações

Observe que a proposição $A \rightarrow B$ não é equivalente a $B \rightarrow A$.

A	B	$A \rightarrow B$	$B \rightarrow A$
V	V	V	V
V	F	F	V
F	V	V	F
F	F	V	V

Observe: a implicação "Se $a > 5$, então $a > 2$" é verdadeira.

A sua recíproca "Se $a > 2$, então $a > 5$" é falsa.

Cuidado!

Provas por contraposição de $A \rightarrow B$ mostram que $\neg B \rightarrow \neg A$.

Provar que $B \rightarrow A$, não é logicamente equivalente.

Prova por Contradição

Queremos provar que uma proposição P é verdadeira.

Suponha que existe uma contradição $(C \wedge \neg C)$ tal que $\neg P \rightarrow (C \wedge \neg C)$ é verdade.

Você se lembra da definição de contradição?

Definição

Uma **contradição** é uma proposição que é sempre falsa (para qualquer combinação de valores-verdade de suas variáveis).

Como $(C \wedge \neg C)$ é falsa e $\neg P \rightarrow (C \wedge \neg C)$ é verdade, concluímos que $\neg P$ é falsa.

Portanto, P é verdade.

Prova por Contradição

Considere que queremos provar a proposição P e que $P : A \to B$.

Observe: $C \wedge \neg C$ é uma contradição, para qualquer proposição C.

Então, pode-se provar que P é verdade mostrando-se que $\neg P \to (C \wedge \neg C)$.

Provas desse tipo são chamadas de **Provas por Contradição**.

Provas por contradição são um outro tipo de prova indireta.

Prova por Contradição

Lembre-se:

1. $P : A \rightarrow B$.
2. Vamos provar que $\neg P \rightarrow (C \wedge \neg C)$.
3. $\neg P \equiv \neg(A \rightarrow B) \equiv \neg(\neg A \vee B) \equiv \neg(\neg A) \wedge \neg B \equiv A \wedge \neg B$.

Então, queremos provar que $(A \wedge \neg B) \rightarrow (C \wedge \neg C)$, para alguma proposição C qualquer.

Observe que, com isso, mostramos que $(A \wedge \neg B)$ implica falso.
Então, quando A é verdade, B obrigatoriamente é verdade, provando P.

Prova por Contradição

Estratégia da Prova por Contradição

Para provar que $A \rightarrow B$ por contradição, deve-se:

- Assumir $A \wedge \neg B$ como hipótese.
- Usar lemas, teoremas, equivalências lógicas e regras de inferência para concluir $C \wedge \neg C$, para alguma proposição C.
- Uma vez que $(C \wedge \neg C)$ não pode ser verdade, concluímos que $A \wedge \neg B$ é absurdo e, portanto, $A \rightarrow B$.

Exemplo 7

Conjectura: Seja n um número inteiro. Se $3n + 2$ é ímpar, então n é ímpar.

Demonstração: Por contradição, suponha que $3n + 2$ é ímpar e n não é ímpar.

Como n é inteiro e não é ímpar, então n é par.

Seja $n = 2k$, para algum k inteiro.

Isso implica que $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.

Como $3n + 2$ é duas vezes um número inteiro, $3n + 2$ é par.

Prova por Contradição

Como $3n + 2$ é ímpar e par, temos uma contradição.

Então, se $3n + 2$ é ímpar, como assumimos no início, n tem que ser ímpar.

Isso completa a prova por contradição. $\square$

Exemplo 7

Conjectura: Se um número adicionado a ele mesmo resulta em nele próprio, então este número é zero.

Observe que podemos escrever esta conjectura mais formalmente:

Conjectura: Se $x + x = x$, então $x = 0$.

Prova por Contradição

Exemplo 7

Conjectura: Se $x + x = x$, então $x = 0$.

Demontração: Por contradiação, suponha que x é um número tal que $x + x = x$ e que $x \neq 0$.

Como $x + x = x$, pode-se subtrair x de ambos os lados da igualdade, obtendo-se $x + x - x = x - x$.

Ou seja, $x = 0$, uma contradição, já que assumimos que $x \neq 0$.

Portanto, se $x + x = x$, não é possível que $x \neq 0$, então $x = 0$. $\square$

Prova por Contradição

Exemplo 8

Conjectura: $\sqrt{2}$ é um número irracional.

Exemplo 8

Conjectura: $\sqrt{2}$ é um número irracional.

Demonstração: Suponha por contradição que $\sqrt{2}$ é racional.

Então existem dois números inteiros p e q, tal que $q \neq 0$ e $\sqrt{2} = \frac{p}{q}$.

Podemos assumir que esta fração $\frac{p}{q}$ já está simplificada.

(Se a fração não estiver, simplifique a fração e tome os valores da fração simplificada para serem p e q.)

Então, $(\sqrt{2})^2 = \left(\frac{p}{q}\right)^2$. Ou seja, $2q^2 = p^2$.

Como q^2 é inteiro, p^2 é par.

Prova por Contradição

Como q^2 é inteiro, p^2 é par.

Então, p é par, pois só um par ao quadrado resulta em par.

Portanto, considere que $p = 2t$, para algum t inteiro.

Como $2q^2 = p^2$, sabemos que $2q^2 = (2t)^2 = 4t$.

Então, $q^2 = 2t$. Ou seja, q^2 é par.

Consequentemente, q é par.

Então a fração $\frac{p}{q}$ pode ser simplificada por 2, um absurdo, pois já é uma fração simplificada.

Como chegamos a uma contradição, $\sqrt{2}$ não pode ser racional. $\square$