Métodos de prova

André Gustavo dos Santos[1]

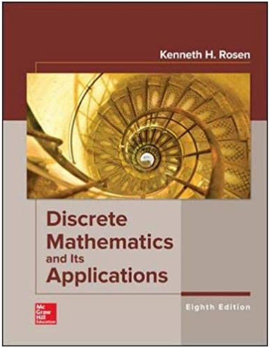
[1] Departamento de Informática
Universidade Federal de Viçosa

INF230 - 2021/1

UFV

Conteúdo

Os slides seguintes são baseados na seção 1.7 do livro texto da disciplina:



ROSEN, Kenneth H.
Discrete mathematics and its applications.
McGraw-Hill Education, 8th edition, 2018

Prova direta

- Queremos provar uma sentença condicional $p \to q$
- Na prova direta, assumimos p verdadeira e concluímos que q é verdadeira

Se n é um inteiro ímpar, então n^2 é ímpar

- $\forall n(P(n) \to Q(n))$
  - $P(n)$ é a sentença "n é um inteiro ímpar"
  - $Q(n)$ é a sentença "n^2 é ímpar"
- Assumindo que a hipótese seja válida, $n = 2k + 1$ para algum inteiro k
- Elevando-se os dois lados ao quadrado, $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$
- Então $n^2 = 2(2k^2 + 2k) + 1$
- Concluímos que n^2 é ímpar, pois é da forma $2\times$ (um número inteiro) $+1$

Outro exemplo

Se m e n são ambos quadrados perfeitos, então mn também é um quadrado perfeito

- $\forall n \forall m((P(n) \wedge P(m)) \rightarrow P(nm))$
  - $P(x)$ é a sentença "x é um quadrado perfeito"
- Assumindo que a hipótese seja válida, $n = r^2$ e $m = s^2$ para algum inteiro r e s
- Então $nm = r^2 s^2 = (rs)^2$
- Concluímos que nm é quadrado perfeito, pois é da forma (um número inteiro)^2

Outro exemplo

Se n é um inteiro, e $3n + 2$ é ímpar, então n é ímpar

- Assumindo que a hipótese seja válida, $3n + 2 = 2k + 1$ para algum inteiro k
- Como usar este fato para mostrar que n é ímpar?
- Se $3n + 2 = 2k + 1$, então $3n + 1 = 2k$
- ?...

- Como a tentativa por prova direta falhou, podemos tentar uma prova indireta

UFV

Prova por contraposição

- Queremos provar uma sentença condicional $p \rightarrow q$
- Na prova por contraposição, assumimos q falsa e concluímos que p é falsa
- Ou seja, assumimos $\neg q$ e concluímos $\neg p$
- Isso é válido porque $p \rightarrow q$ é equivalente à sua contrapositiva, $\neg q \rightarrow \neg p$

Se n é um inteiro, e $3n + 2$ é ímpar, então n é ímpar

- Assumindo que a conclusão seja falsa, ou seja, que n seja par
- Então $n = 2k$ para algum inteiro k
- Substituindo n por $2k$, temos que $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$
- Então $3n + 2$ é par, pois é da forma $2\times$ (um número inteiro)
- Isso é a negação da hipótese
- Concluímos que a negação da conclusão implica na negação da hipótese
- Provamos que a sentença original é verdadeira por contraposição

Outro exemplo

Se $n = ab$, em que a e b são inteiros positivos, então $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$

- Assumindo que a conclusão é falsa, ou seja que $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$ é falsa
- Equivalente a assumir que $(a > \sqrt{n}) \wedge (b > \sqrt{n})$ é verdadeira
- Multiplicando as inequações, e usando o fato que se $0 < s < t$ e $0 < u < v$ então $su < tv$, temos que $ab > \sqrt{n}\sqrt{n} = n$
- Então $ab \neq n$, que é a negação da hipótese
- Provamos que a sentença original é verdadeira por contraposição

Exercício 1

A soma de dois números racionais é um número racional

- Incluindo quantificadores, $\forall r \forall s((P(r) \wedge P(s)) \rightarrow P(r+s))$
  - $P(x)$ é a sentença "x é um número racional"

Prova direta

- Assumindo que r e s são racionais, i.e., existe inteiros p, q, t, u e $r = \frac{p}{q}$ e $s = \frac{t}{u}$
- Então $r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu+qt}{qu}$
- Como $q \neq 0$ e $u \neq 0$, então $qu \neq 0$
- Então $r + s$ pode ser expresso por $\frac{v}{w}$, $v = pu + qt$ e $w = qu$, dois inteiros e $w \neq 0$

UFV

Exercício 2

Se n é inteiro e n^2 é ímpar, então n é ímpar

Prova direta

- Assumindo que n^2 é inteiro ímpar, $n^2 = 2k + 1$ para algum inteiro k
- Então $n = \pm\sqrt{2k+1}$
- ?...

Prova por contraposição

- Assumindo que n seja par, $n = 2k$ para algum inteiro k
- Então $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
- Então n^2 também é par
- Provamos que a sentença original é verdadeira por contraposição

Prova por contradição

- Queremos provar que uma proposição p é verdadiera
- Suponha que podemos achar uma contradição q tal que $\neg p \rightarrow q$ é verdadeira
- Como q é falsa, mas $\neg p \rightarrow q$ é verdadeira, então $\neg p$ é falsa, logo p é verdadeira
- Como podemos achar uma contradição q para provar p desta forma?
- Sabemos que se r é uma proposição, $r \wedge \neg r$ é uma contradição
- Na prova por contradição, mostramos que $\neg p \rightarrow (r \wedge \neg r)$ é verdade para algum r

Pelo menos 4 de um conjunto qualquer de 22 dias caem no mesmo dia da semana

- Seja p tal proposição e assuma $\neg p$ verdadeira
- Ou seja, no máximo 3 dias de um conjunto de 22 caem no mesmo dia da semana
- Como há 7 dias na semana, então tal conjunto pode ter no máximo 21 dias
- Isto contradiz a premissa que estamos considerando 22 dias
- Ou seja, se r é a sentença “escolhemos 22 dias”, então $\neg p \rightarrow (r \wedge \neg r)$
- Consequentemente, p é verdadeira

Prova por contradição

- Também pode ser usada para provar uma sentença condicional $p \rightarrow q$
- Para isso usamos a negação da conclusão e a equivalência de $p \rightarrow q$ e $p \wedge \neg q \rightarrow \mathit{False}$

Prova por contradição

- Podemos reescrever uma prova por contraposição como prova por contradição
- Na prova de $p \to q$ por contraposição, assumimos $\neg q$ e concluímos $\neg p$
- Para reescrever em prova por contradição, assumimos p e $\neg q$ como verdadeiras
- Usamos os passos da prova $\neg q \to \neg p$ para mostrar que $\neg p$ é verdade
- Isto leva à contradição $p \wedge \neg p$, que completa a prova.

Se n é um inteiro, e $3n + 2$ é ímpar, então n é ímpar

- Seja p a sentença "$3n + 2$ é ímpar" e q a sentença "n é ímpar"
- Assumindo que p e $\neg q$ sejam falsas, ou seja, $3n + 2$ é ímpar e q não é ímpar
- Como n não é ímpar, então n é par, i.e., $n = 2k$ para algum inteiro k
- Então $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$, que é par ($2t$, para $t = 3k + 1$)
- Logo $\neg p$ é verdade, e chegamos à contradição $p \wedge \neg p$

Prova por contradição

- Podemos reescrever uma prova direta como prova por contradição
- Na prova direta de $p \to q$, assumimos p e concluímos q
- Para reescrever em prova por contradição, assumimos p e $\neg q$ como verdadeiras
- Usamos os passos da prova para mostrar que q é verdade
- Isto leva à contradição $q \wedge \neg q$.

Contraexemplo

- Para provar que $\forall x P(x)$ é falsa, basta achar um x tal que $P(x)$ seja falsa
- Se achamos que $\forall x P(x)$ é falsa, ou tenha resistido a muitas tentativas de prova, procuramos um contraexemplo

Todo inteiro positivo pode ser escrito como a soma de dois quadrados perfeitos

- Contraexemplo: 3

Vacuidade e Trivialidade

Vacuidade

$p \rightarrow q$ é verdadeira se p é falsa

- Se mostramos que p é sempre falsa, então por vacuidade $p \rightarrow q$ é verdadeira

Trivialidade

$p \rightarrow q$ é verdadeira se q é verdadeira

- Se mostramos que q é sempre verdadeira, então por trivialidade $p \rightarrow q$ é verdadeira

Exemplos

Seja $P(n)$ a sentença "Se $n > 1$, então $n^2 > n$". Mostre que $P(0)$ é verdadeira.

- Note que $P(0)$ é a sentença "Se $0 > 1$, então $0^2 > 0$"
- Mas a hipótese $(0 > 1)$ é falsa, então $P(0)$ é verdadeira por vacuidade.

Seja $P(n)$ "Se a e b são inteiros positivos com $a \geq b$, então $a^n \geq b^n$". Mostre que $P(0)$ é verdadeira.

- Note que $P(0)$ é a proposição "Se $a \geq b$, então $a^0 \geq b^0$"
- Mas a conclusão $(a^0 \geq b^0)$ é verdadeira $(1 \geq 1)$, então $P(0)$ é verdadeira por trivialidade.

Exemplo (citado na wikipedia)

“Se Londres está na França, então a Torre Eiffel está na Bolívia.”

- $p \rightarrow q$
  - p é a sentença “Londres está na França”
  - q é a sentença “a Torre Eiffel está na Bolívia”
- p é falsa, então $p \rightarrow q$ é verdadeira por vacuidade
- Atenção: isso não diz que q é verdadeira (ou falsa)!
  só diz que $p \rightarrow q$ é verdadeira (lembre-se que só é falsa se p verdadeira e q falsa)

UFV

Exercício 3

Se n é um inteiro tal que $10 \leq n \leq 15$ que é quadrado perfeito, então n é cubo perfeito.

- a hipótese é falsa (não há quadrados perfeitos entre 10 e 15)
- então a proposição é verdadeira por vacuidade

Provas de Equivalência

Para provar $p \leftrightarrow q$

- deve-se provar $p \to q$ e provar $q \to p$
- alternativamente pode-se provar $p \to q$, provar $q \to r$ e provar $r \to q$ para alguma proposição r

O que há de errado?

1 = 2

- Sejam a e b dois inteiros positivos iguais
  1. $a = b$
  2. $a^2 = ab$
  3. $a^2 - b^2 = ab - b^2$
  4. $(a - b)(a + b) = b(a - b)$
  5. $(a + b) = b$
  6. $2b = b$
  7. $2 = 1$

UFV

O que há de errado?

1 = 2

- Sejam a e b dois inteiros positivos iguais
  1. $a = b$
  2. $a^2 = ab$
  3. $a^2 - b^2 = ab - b^2$
  4. $(a - b)(a + b) = b(a - b)$
  5. $(a + b) = b$
  6. $2b = b$
  7. $2 = 1$

Do passo 4 para o 5 houve divisão por 0.

UFV

O que há de errado?

Se n^2 é positivo, então n é positivo

- Suponha que n^2 seja positivo
- Sabemos que se n é positivo, então n^2 é positivo
- Portanto, n é positivo

Se n não é positivo, então n^2 não é positivo

- Suponha que n não seja positivo
- Sabemos que se n é positivo, então n^2 é positivo
- Portanto, n^2 não é positivo

O que há de errado?

Se n^2 é positivo, então n é positivo

- Suponha que n^2 seja positivo
- Sabemos que se n é positivo, então n^2 é positivo
- Portanto, n é positivo

Está usando a oposta $q \rightarrow p$, que não é equivalente a $p \rightarrow q$.

Se n não é positivo, então n^2 não é positivo

- Suponha que n não seja positivo
- Sabemos que se n é positivo, então n^2 é positivo
- Portanto, n^2 não é positivo

Está usando a inversa $\neg p \rightarrow \neg q$, que não é equivalente a $p \rightarrow q$.

O que há de errado?

Seja n um inteiro. Se n^2 é par, então n é par

- Suponha que n^2 seja par
- Então $n^2 = 2k$ para algum inteiro k
- Seja $n = 2l$ para algum inteiro l
- Então n é par.

O que há de errado?

Seja n um inteiro. Se n^2 é par, então n é par

- Suponha que n^2 seja par
- Então $n^2 = 2k$ para algum inteiro k
- Seja $n = 2l$ para algum inteiro l
- Então n é par.

Apesar da proposição ser verdadeira, a prova está incorreta. A terceira sentença (supor $n = 2l$) é equivalente à supor que n é par, que é o que se quer demonstrar. É um raciocínio circular.