MC358 - Fundamentos matemáticos da computação

Prof. Dr. Hilder Vitor Lima Pereira

Instituto de computação

UNICAMP

09 de agosto de 2023

Provas matemáticas

Prova: visão geral

Uma prova matemática é argumento *formal* que mostra a validade de uma implicação do tipo

$$A \wedge H \Rightarrow C$$

onde A é a conjunção dos axiomas, H é a hipótese e C é a conclusão.

Prova: visão geral

Uma prova matemática é argumento *formal* que mostra a validade de uma implicação do tipo

$$A \wedge H \Rightarrow C$$

onde A é a conjunção dos axiomas, H é a hipótese e C é a conclusão. Como axiomas são assumidos como verdadeiro, são omitidos e a prova é escrita apenas como

$$H \Rightarrow C$$

Prova: visão geral

Note que provar

$$H \Rightarrow C$$

não significa que H é verdade!
O que provamos é que *quando/se* H é verdade, então C é verdade.

Prova: visão geral

Note que provar

$$H \Rightarrow C$$

não significa que H é verdade!
O que provamos é que *quando/se* H é verdade, então C é verdade.
Exemplo: última aula:

$$\underbrace{A \cup B = \emptyset}_{H} \Rightarrow \underbrace{A = B = \emptyset}_{C}.$$

$A \cup B$ não é vazio sempre. Mas quando for, então podemos concluir C.

Derivando a conclusão

Usamos regras da inferência lógica, axiomas e resultados conhecidos para concluir C a partir da hipótese H.
Há várias formas de se provar $H \Rightarrow C$, e todas são equivalentes, graças às equivalências lógicas que já vimos.

- Prova direta
- Contrapositiva
- Redução ao absurdo

Prova direta

Prova direta

Para provar $H \Rightarrow C$, provamos uma sequência de implicações que termina em C.
Cada passo da prova deve ser justificado:

$$
\begin{aligned}
H &\Rightarrow R_1 && \text{(justificativa 1)} \\
&\Rightarrow R_2 && \text{(justificativa 2)} \\
&\vdots && \vdots \\
&\Rightarrow R_n && \text{(justificativa } n\text{)}
\end{aligned}
$$

No final, devemos ter $R_n = C$.

Exemplo de prova direta simples

Teorema

Sejam A e B dois conjuntos. Suponha que $C = (A \cup B)$ e $D = C \setminus B$. Então $D \subseteq A$.

Exemplo de prova direta simples

Teorema

Sejam A e B dois conjuntos. Suponha que $C = (A \cup B)$ e $D = C \setminus B$. Então $D \subseteq A$.

Antes de começar uma prova, se pergunte sempre:

- Quais são as hipóteses?
- O que se conclui imediatamente das hipóteses?
- O que exatamente queremos provar? Ache uma (ou mais) expressão(ões) precisa(s) para a conclusão a ser provada.

Exemplo de prova direta simples

Teorema

Sejam A e B dois conjuntos. Suponha que $C = (A \cup B)$ e $D = C \setminus B$. Então $D \subseteq A$.

Antes de começar uma prova, se pergunte sempre:

- Quais são as hipóteses?
- O que se conclui imediatamente das hipóteses?
- O que exatamente queremos provar? Ache uma (ou mais) expressão(ões) precisa(s) para a conclusão a ser provada.

Prova na lousa.

Segundo exemplo de prova direta

Teorema

Sejam x e y números reais. Suponha que $x > 3$ e $y < 2$. Então,

$$x^2 - 2y > 5.$$

Segundo exemplo de prova direta

Teorema

Sejam x e y números reais. Suponha que $x > 3$ e $y < 2$. Então,

$$x^2 - 2y > 5.$$

- Quais são as hipóteses?
- Como escrever essa afirmação usando quantificadores e predicados?

Segundo exemplo de prova direta

Teorema

Sejam x e y números reais. Suponha que $x > 3$ e $y < 2$. Então,

$$x^2 - 2y > 5.$$

- Quais são as hipóteses?
- Como escrever essa afirmação usando quantificadores e predicados?
- Qual a diferença entre (1.) e (2.)?
  1. $\forall x, y \in \mathbb{R}\,(P(x, y) \rightarrow Q(x, y))$
  2. $\forall x, y \in \mathbb{R}\,(P(x, y) \Rightarrow Q(x, y))$

Segundo exemplo de prova direta

Teorema

Sejam x e y números reais. Suponha que $x > 3$ e $y < 2$. Então,

$$x^2 - 2y > 5.$$

- Quais são as hipóteses?
- Como escrever essa afirmação usando quantificadores e predicados?
- Qual a diferença entre (1.) e (2.)?
  1. $\forall x, y \in \mathbb{R}\,(P(x, y) \rightarrow Q(x, y))$
  2. $\forall x, y \in \mathbb{R}\,(P(x, y) \Rightarrow Q(x, y))$

Para provar, usamos resultados conhecidos, como

- Lema 1: Se $x < a$, então $-x > -a$.
- Lema 2: Se $x > a$ e $b > 0$, então $xb > ab$.
- Lema 3: Se $x > a > 0$, então $x^2 > a^2$.
- Lema 4: Se $x > a$ e $y > b$, então $x + y > a + b$.

Note que nossa prova tem a forma

$$P(x,y) \Rightarrow A_1(x,y) \wedge B_1(x,y) \Rightarrow A_1(x,y) \wedge B_2(x,y) \Rightarrow Q(x,y)$$

Não precisamos repetir as duas ramificações em cada linha.

Note que nossa prova tem a forma

$$P(x,y) \Rightarrow A_1(x,y) \wedge B_1(x,y) \Rightarrow A_1(x,y) \wedge B_2(x,y) \Rightarrow Q(x,y)$$

Não precisamos repetir as duas ramificações em cada linha.

$$\begin{tikzcd}[arrows=Rightarrow]
 & P(x,y) \arrow[dl] \arrow[dr] & \\
\color{blue}{A_1(x,y)} \arrow[ddr] & & \color{purple}{B_1(x,y)} \arrow[d] \\
 & & \color{purple}{B_2(x,y)} \arrow[dl] \\
 & Q(x,y) &
\end{tikzcd}$$

Se as "subprovas" forem complicadas (longas ramificações), crie lemas e use-os na prova (lembre-se de funções na programação)

Terceiro exemplo: prova direta usando lemas

Teorema

Seja n um inteiro par, maior que ou igual a 4. Então $2^n - 1$ não é primo.

Terceiro exemplo: prova direta usando lemas

Teorema

Seja n um inteiro par, maior que ou igual a 4. Então $2^n - 1$ não é primo.

Hipóteses:

- Quais são as hipóteses?
- O que podemos concluir imediatamente das hipóteses?

Terceiro exemplo: prova direta usando lemas

Teorema

Seja n um inteiro par, maior que ou igual a 4. Então $2^n - 1$ não é primo.

Hipóteses:

- Quais são as hipóteses?
- O que podemos concluir imediatamente das hipóteses?
- $n = 2a$ para algum $a \geq 2$.

Terceiro exemplo: prova direta usando lemas

Teorema

Seja n um inteiro par, maior que ou igual a 4. Então $2^n - 1$ não é primo.

Hipóteses:

- Quais são as hipóteses?
- O que podemos concluir imediatamente das hipóteses?
- $n = 2a$ para algum $a \geq 2$.

O que queremos provar exatamente?

- Se $x := 2^n - 1$ é primo, então os divisores de x são $\{\pm 1, \pm x\}$
- i.e., x não é primo $\Leftrightarrow \exists p, q \in \mathbb{Z}\,((x = pq) \wedge (1 < p < x))$.

Terceiro exemplo: prova direta usando lemas

Teorema

Seja n um inteiro par, maior que ou igual a 4. Então $2^n - 1$ não é primo.

Hipóteses:

- Quais são as hipóteses?
- O que podemos concluir imediatamente das hipóteses?
- $n = 2a$ para algum $a \geq 2$.

O que queremos provar exatamente?

- Se $x := 2^n - 1$ é primo, então os divisores de x são $\{\pm 1, \pm x\}$
- i.e., x não é primo $\Leftrightarrow \exists p, q \in \mathbb{Z}\,((x = pq) \wedge (1 < p < x))$.

Como podemos provar?

Terceiro exemplo: prova direta usando lemas

Note que

$$x := 2^{2a} - 1 = (2^a)^2 - 1^2 = \underbrace{(2^a - 1)}_{p}\underbrace{(2^a + 1)}_{q}.$$

Isso nos dá dois fatores de x.

Terceiro exemplo: prova direta usando lemas

Note que

$$x := 2^{2a} - 1 = (2^a)^2 - 1^2 = \underbrace{(2^a - 1)}_{p}\underbrace{(2^a + 1)}_{q}.$$

Isso nos dá dois fatores de x.

Para completar a prova, temos que provar que ao menos um desses fatores não é trivial.

Podemos escrever

- Lema 1: $a \geq 2 \Rightarrow 2^a - 1 < x$
- Lema 2: $a \geq 2 \Rightarrow 2^a - 1 > 1$

Finalmente, usar a observação acima e os lemas para provar o teorema.

Quarto exemplo de prova direta: divisibilidade por 3

Teorema

Seja x um inteiro positivo divisível por 3. Então a soma dos seus dígitos (na base 10) também é divisível por 3.

Quarto exemplo de prova direta: divisibilidade por 3

Teorema

Seja x um inteiro positivo divisível por 3. Então a soma dos seus dígitos (na base 10) também é divisível por 3.

Hipóteses:

- Quais são as hipóteses?
- O que podemos concluir imediatamente das hipóteses?

Quarto exemplo de prova direta: divisibilidade por 3

Teorema

Seja x um inteiro positivo divisível por 3. Então a soma dos seus dígitos (na base 10) também é divisível por 3.

Hipóteses:

- Quais são as hipóteses?
- O que podemos concluir imediatamente das hipóteses?
- $n = 3\alpha$ para algum $\alpha \in \mathbb{N}$.

Quarto exemplo de prova direta: divisibilidade por 3

Teorema

Seja x um inteiro positivo divisível por 3. Então a soma dos seus dígitos (na base 10) também é divisível por 3.

Hipóteses:

- Quais são as hipóteses?
- O que podemos concluir imediatamente das hipóteses?
- $n = 3\alpha$ para algum $\alpha \in \mathbb{N}$.

O que queremos provar exatamente?

- Se $x = x_0 + 10 \cdot x_1 + 10^2 \cdot x_2 + ... + 10^{n-1} \cdot x_{n-1}$, então a soma

  $$x_0 + x_1 + ... + x_{n-1}$$

  é divisível por 3

Quarto exemplo de prova direta: divisibilidade por 3

Teorema

Seja x um inteiro positivo divisível por 3. Então a soma dos seus dígitos (na base 10) também é divisível por 3.

Hipóteses:

- Quais são as hipóteses?
- O que podemos concluir imediatamente das hipóteses?
- $n = 3\alpha$ para algum $\alpha \in \mathbb{N}$.

O que queremos provar exatamente?

- Se $x = x_0 + 10 \cdot x_1 + 10^2 \cdot x_2 + ... + 10^{n-1} \cdot x_{n-1}$, então a soma

  $$x_0 + x_1 + ... + x_{n-1}$$

  é divisível por 3
- i.e., $\sum_{i=0}^{n-1} x_i = 3\beta$ para algum $\beta \in \mathbb{Z}$

Perguntas, observações, comentários?