

DCC638 - Introdução à Lógica Computacional  
2024.1

## Métodos de Demonstração

Área de Teoria DCC/UFMG

# Terminologia

- Uma sentença é **válida** se ela é *sempre* verdadeira.
- Um **axioma** é uma afirmação tida como válida sem uma demonstração.
- Resultados de demonstrações recebem diferentes nomes. Convencionalmente:
  - **Teorema**: resultado considerado interessante em si mesmo.
  - **Proposição**: resultado considerado “de menor interesse”.
  - **Lema**: resultado auxiliar, geralmente usado na demonstração de um teorema.
  - **Corolário**: resultado “imediato” a partir de outro resultado já demonstrado.
- Uma **conjectura** é uma afirmação que não é um axioma e para a qual uma demonstração não foi apresentada.

# Evidência versus demonstração

- Exemplo 1 Seja a fórmula  $p(n) = n^2 + n + 41$ .

**Conjectura:**  $\forall n \in \mathbb{N}. p(n)$  é primo.

# Evidência versus demonstração

- Exemplo 1 Seja a fórmula  $p(n) = n^2 + n + 41$ .

**Conjectura:**  $\forall n \in \mathbb{N}. p(n)$  é primo.

Temos evidências de que a conjectura *pode estar* certa.

Testando valores de  $n = 0, 1, \dots, 39$  a proposição é verdadeira, ou seja,  $p(n)$  é primo para  $0 \leq n \leq 39$ :

$n$	0	1	2	3	...	20	...	39
$p(n)$	41	43	47	53	...	461	...	1601

# Evidência versus demonstração

- Exemplo 1 Seja a fórmula  $p(n) = n^2 + n + 41$ .

**Conjectura:**  $\forall n \in \mathbb{N}$ .  $p(n)$  é primo.

Temos evidências de que a conjectura *pode estar* certa.

Testando valores de  $n = 0, 1, \dots, 39$  a proposição é verdadeira, ou seja,  $p(n)$  é primo para  $0 \leq n \leq 39$ :

$n$	0	1	2	3	...	20	...	39
$p(n)$	41	43	47	53	...	461	...	1601

Daí, podemos ficar tentados a concluir:

*Isto não pode ser uma coincidência! A hipótese deve ser válida!*

Mas não é:  $p(40) = 1681 = 41 \cdot 41$ , que não é primo!

Logo, a conjectura é falsa.

- Moral da história: evidência não é o mesmo que demonstração!

# Evidência versus demonstração

- Exemplo 2 Em 1769, Euler (1707–1783) conjecturou que

$$a^4 + b^4 + c^4 = d^4$$

não tem solução no conjunto dos números inteiros positivos.

Durante mais de dois séculos, ninguém conseguiu encontrar valores de  $a$ ,  $b$ ,  $c$  e  $d$  que satisfizessem a equação.

O insucesso de todos os matemáticos envolvidos era evidência de que a conjectura *podia ser* válida.

218 anos depois, em 1987, Noam Elkies proveu um contra-exemplo:

$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4.$$

Logo, esta conjectura também é falsa.

- Ausência de demonstração não é o mesmo que demonstração de ausência!

# Métodos de demonstração

- Construir uma demonstração é uma arte.

Cada caso é um caso: não existe uma “receita fechada” para construir demonstrações para todas as afirmações.

- Existem, entretanto, técnicas comuns para construir demonstrações:
  - demonstração direta;
  - demonstração por contraposição;
  - demonstração por contradição (ou demonstração por redução ao absurdo).
  - demonstração por exaustão e divisão em casos.
- Outros métodos de demonstração (e.g., demonstração por indução matemática) serão vistos mais adiante no curso.
- Existem também formas sistemáticas de construir demonstrações (*automatização de raciocínio*)

# Como escrever uma demonstração

- Escreva claramente qual a afirmação que se deseja demonstrar.  
(É comum preceder a afirmação com uma qualificação como **“Teorema”**, **“Lema”**, ou **“Proposição”**.)
- Delimite claramente o escopo da demonstração.  
Indique o início da demonstração com **“Demonstração.”**  
Indique o fim da demonstração com um marcador. Podem-se usar:
  - um quadradinho  $\square$ , ou
  - a abreviação **Q.E.D.** (do latim *“quod erat demonstrandum”*), ou
  - sua tradução em português, **C.Q.D.** (*“conforme queríamos demonstrar”*).
- Escreva a demonstração de tal forma que ela seja autocontida.
  - Use linguagem natural (português) de forma clara, empregando sentenças completas e bem estruturadas.
  - Utilize fórmulas matemáticas, equações, etc., quando necessário.

# Como escrever uma demonstração

- Identifique cada variável usada na demonstração juntamente com seu tipo.

Exs.:

- 1 Seja  $x$  um número real maior que 2.
- 2 Suponha que  $m$  e  $n$  sejam inteiros sem divisores comuns.

- Importante:

O objetivo principal de uma demonstração é convencer o leitor de que o resultado (teorema, proposição, lema) é válido.

Não basta que você mesmo esteja convencido!

Certifique-se de que está sendo conciso, mas claro.

# Demonstração direta

- Forma geral: “Supondo a premissa  $P$ , em uma série de *passos* derivarei a conclusão  $C$ ”.

- Em lógica de predicados:

1. Expresse a afirmação a ser demonstrada na forma:

$$\forall x \in D. (P(x) \rightarrow C(x))$$

2. Comece a demonstração supondo  $P(d)$ , sendo  $d$  um elemento *arbitrário* de  $D$ .

Ex.: “*Suponha que  $P(d)$  é verdadeiro, para um  $d \in D$  qualquer.*”

3. Mostre que a conclusão  $C(d)$  é verdadeira utilizando definições, resultados anteriores e regras de inferência.

- Importante: Como  $d \in D$  é escolhido arbitrariamente,

- ele não depende de nenhuma suposição especial sobre  $d$ , e,
- portanto, o resultado pode ser generalizado para todos os elementos de  $D$ .

# Demonstração direta

- **Definição:**

- (i) Um inteiro  $n$  é **par** se existe um inteiro  $k$  tal que  $n = 2k$ .

- (ii) Um inteiro  $n$  é **ímpar** se existe um inteiro  $k$  tal que  $n = 2k + 1$ .

- Exemplo 3 Mostre que se  $n$  é um inteiro ímpar, então  $n^2$  é ímpar.

# Demonstração direta

- **Definição:**

- (i) Um inteiro  $n$  é **par** se existe um inteiro  $k$  tal que  $n = 2k$ .

- (ii) Um inteiro  $n$  é **ímpar** se existe um inteiro  $k$  tal que  $n = 2k + 1$ .

- Exemplo 3 Mostre que se  $n$  é um inteiro ímpar, então  $n^2$  é ímpar.

**Demonstração.** Queremos mostrar que

$$\forall n. (P(n) \rightarrow Q(n)),$$

em que

- $P(n)$  é o predicado “ $n$  é um inteiro ímpar”, e
- $Q(n)$  é o predicado “ $n^2$  é ímpar”.

Para produzir uma demonstração direta, supomos que para um inteiro  $k$  a hipótese da implicação,  $P(k)$ , seja verdadeira, ou seja, que  $k$  é ímpar.

Então, pela definição de número ímpar, existe um inteiro  $k'$  tal que  $k = 2k' + 1$ .

# Demonstração direta

- Exemplo 3 (Continuação)

Queremos mostrar que a conclusão da implicação,  $Q(k)$ , é verdadeira, ou seja, que  $k^2$  também é ímpar.

Para isto podemos calcular

$$\begin{aligned}k^2 &= (2k' + 1)^2 \\ &= 4k'^2 + 4k' + 1 \\ &= 2(2k'^2 + 2k') + 1.\end{aligned}$$

Mas note que isso significa que

$$k^2 = 2k'' + 1,$$

em que  $k'' = 2k'^2 + 2k'$  é um inteiro.

Logo, pela definição de número ímpar,  $k^2$  também é ímpar e está concluída nossa demonstração. □

# Demonstração direta

- **Definição:** Um inteiro  $a$  é um **quadrado perfeito** se existe um inteiro  $b$  tal que  $a = b^2$ .
- **Exemplo 4** Mostre que se  $m$  e  $n$  são quadrados perfeitos, então  $mn$  é um quadrado perfeito.

**Demonstração.** Para demonstrar esta proposição, vamos supor que  $m$  e  $n$  sejam quadrados perfeitos. Pela definição de quadrado perfeito, devem existir inteiros  $s$  e  $t$  tais que  $m = s^2$  e  $n = t^2$ .

O objetivo da demonstração é mostrar que  $mn$  será um quadrado perfeito quando  $m$  e  $n$  o forem. Para ver isto, podemos calcular

$$mn = s^2 t^2 = (st)^2.$$

Mas é claro que  $st$  também é um inteiro, logo  $mn$  satisfaz a definição de quadrado perfeito (já que  $mn = (st)^2$ ), e a conclusão da implicação também é verdadeira.

Logo concluímos a demonstração de que a afirmação é válida. □

# Demonstração direta

- **Definição:**

- (i) Um número real  $n$  é **racional** quando existem inteiros  $p$  e  $q$ , com  $q \neq 0$ , tais que  $n = p/q$ .
- (ii) Um número real  $n$  é **irracional** quando ele não é racional.

- Exemplo 5 Mostre que a soma de dois números racionais é um número racional.

# Demonstração direta

- **Definição:**

- (i) Um número real  $n$  é **racional** quando existem inteiros  $p$  e  $q$ , com  $q \neq 0$ , tais que  $n = p/q$ .
- (ii) Um número real  $n$  é **irracional** quando ele não é racional.

- **Exemplo 5** Mostre que a soma de dois números racionais é um número racional.

**Demonstração.** Formalmente, queremos mostrar que para todo número real  $r$  e todo número real  $s$ , se  $r$  e  $s$  são racionais, então  $r + s$  também é racional.

Para dar uma demonstração direta desta afirmação, vamos supor que  $r$  e  $s$  sejam racionais. Pela definição de número racional, devem existir então inteiros  $p$  e  $q$ , com  $q \neq 0$ , tais que  $r = p/q$ , e devem existir também inteiros  $t$  e  $u$ , com  $u \neq 0$ , tais que  $s = t/u$ .

# Demonstração direta

- Exemplo 5 (Continuação)

Para mostrar que  $r + s$  também será racional quando  $r$  e  $s$  o forem, podemos calcular

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

Note que, por hipótese,  $q$  e  $u$  são diferentes de zero e, portanto,  $qu \neq 0$ .

Consequentemente  $r + s$  pode ser expresso como a razão de dois inteiros ( $pu + qt$  e  $qu$ , com  $qu \neq 0$ ) e, portanto,  $r + s$  satisfaz a definição de número racional.

Logo a afirmação é válida. □

# Demonstração por contraposição

- Forma geral: “Supondo o oposto da conclusão, i.e.,  $\neg C$ , mostrarei o oposto da premissa, i.e.,  $\neg P$ .”

- Em lógica de predicados:

1. Exprese a afirmação a ser demonstrada na forma:

$$\forall x \in D. (P(x) \rightarrow C(x))$$

2. Encontre a afirmação contrapositiva da afirmação a ser demonstrada:

$$\forall x \in D. (\neg C(x) \rightarrow \neg P(x))$$

3. Suponha que a conclusão  $C(d)$  é falsa, i.e.,  $\neg C(d)$  é verdadeira, sendo  $d$  um elemento *arbitrário* de  $D$ .
4. Mostre que a premissa  $P(d)$  é falsa, i.e.,  $\neg P(d)$  é verdadeira, utilizando definições, resultados anteriores e regras de inferência.

# Demonstração por contraposição

- Exemplo 6 Mostre que se  $n$  é um inteiro e  $3n + 2$  é ímpar, então  $n$  é ímpar.

# Demonstração por contraposição

- Exemplo 6 Mostre que se  $n$  é um inteiro e  $3n + 2$  é ímpar, então  $n$  é ímpar.

**Demonstração.** Queremos mostrar que  $\forall n \in \mathbb{N}. (P(n) \rightarrow Q(n))$ , onde  $P(n)$  é “ $3n + 2$  é ímpar”, e  $Q(x)$  é “ $n$  é ímpar”.

Para produzir uma demonstração por contraposição, vamos demonstrar que  $\forall n \in \mathbb{N}. (\neg Q(n) \rightarrow \neg P(n))$ . Ou seja, vamos mostrar que se um número inteiro  $n$  não é ímpar, então  $3n + 2$  também não é ímpar.

Se  $n$  não é ímpar, é porque  $n$  é par e, pela definição de número par,  $n = 2k$  para algum  $k \in \mathbb{N}$ . Portanto podemos derivar

$$\begin{aligned} 3n + 2 &= 3(2k) + 2 \\ &= 6k + 2 \\ &= 2(3k + 1), \end{aligned}$$

de onde concluímos que  $3n + 2$  satisfaz a definição de número par.

Como mostramos que sempre que a conclusão da implicação é falsa, a hipótese também é falsa, concluímos com sucesso a demonstração por contraposição . □

# Demonstração por contraposição

- **Exemplo 7** Mostre que se  $n = ab$  onde  $a$  e  $b$  são inteiros positivos, então  $a \leq \sqrt{n}$  ou  $b \leq \sqrt{n}$ .

**Demonstração.** Em primeiro lugar, note que o resultado que queremos demonstrar pode ser formalizado como

$$\forall n, a, b \in \mathbb{Z}^+. (n = ab \rightarrow a \leq \sqrt{n} \vee b \leq \sqrt{n}) .$$

Para produzir uma demonstração por contraposição, vamos demonstrar que sempre que a conclusão da implicação é falsa, sua hipótese também é falsa.

A conclusão da implicação é  $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$ , logo por de Morgan, sua negação é

$$\begin{aligned} \neg((a \leq \sqrt{n}) \vee (b \leq \sqrt{n})) &\equiv \neg(a \leq \sqrt{n}) \wedge \neg(b \leq \sqrt{n}) \\ &\equiv (a > \sqrt{n}) \wedge (b > \sqrt{n}). \end{aligned}$$

Já a hipótese da implicação é  $n = ab$ , e sua negação é  $n \neq ab$ .

# Demonstração por contraposição

- Exemplo 7 (Continuação)

Queremos mostrar a contrapositiva da proposição original, ou seja, que para todos inteiros positivos  $a, b, n$  se  $(a > \sqrt{n}) \wedge (b > \sqrt{n})$  então  $n \neq ab$ .

Para isto, note que se  $(a > \sqrt{n}) \wedge (b > \sqrt{n})$  podemos derivar o seguinte

$$\begin{aligned} ab &> \sqrt{n} \cdot b && \text{(pois } a > \sqrt{n}\text{)} \\ &> \sqrt{n} \cdot \sqrt{n} && \text{(pois } b > \sqrt{n}\text{)} \\ &= n, \end{aligned}$$

de onde se conclui que  $ab > n$  e, portanto,  $ab \neq n$ .

Como mostramos que sempre que a conclusão da implicação é falsa, a hipótese também é falsa, a demonstração por contraposição é concluída com sucesso. □

# Demonstração por vacuidade

- Forma geral: “Se a premissa nunca é verdadeira, ela permite demonstrar qualquer conclusão.”

- Em lógica de predicados:

1. Exprese a afirmação a ser demonstrada na forma:

$$\forall x \in D. (P(x) \rightarrow C(x))$$

2. Mostre que não existem elementos  $d \in D$  tais que  $P(d)$  seja verdadeiro.

3. Conclua que  $\forall x \in D. (P(x) \rightarrow C(x))$  é verdadeira, pelas definições de  $\rightarrow$  e  $\forall$ .

- O nome **demonstração por vacuidade** segue de demonstrarmos que a premissa da implicação é “vácua”, ou seja, falsa.
- Com isso nem precisamos analisar a conclusão para garantir que toda a implicação é válida.

# Demonstração por vacuidade

- **Definição:** Um inteiro  $a$  é um **cubo perfeito** se existe um inteiro  $b$  tal que  $a = b^3$ .
- **Exemplo 8** Mostre que se  $n$  é um inteiro, com  $10 \leq n \leq 15$ , tal que  $n$  é um quadrado perfeito, então  $n$  é também um cubo perfeito.

# Demonstração por vacuidade

- **Definição:** Um inteiro  $a$  é um **cubo perfeito** se existe um inteiro  $b$  tal que  $a = b^3$ .
- **Exemplo 8** Mostre que se  $n$  é um inteiro, com  $10 \leq n \leq 15$ , tal que  $n$  é um quadrado perfeito, então  $n$  é também um cubo perfeito.

## Demonstração.

Note que queremos mostrar a seguinte implicação para todo inteiro  $n$ : se  $10 \leq n \leq 15$  e  $n$  é um quadrado perfeito, então  $n$  é um cubo perfeito.

Mas note que a hipótese da implicação é falsa: como  $3^2 = 9$  e o próximo quadrado perfeito é  $4^2 = 16$ , não existe nenhum quadrado perfeito  $n$  tal que  $10 \leq n \leq 15$ .

Consequentemente, a implicação a ser demonstrada é verdadeira, por vacuidade, para todos os inteiros  $n$ .



# Demonstração trivial

- Forma geral: “Se a conclusão é sempre verdadeira, ela é demonstrável independentemente de premissas.”

- Em lógica de predicados:

1. Exprese a afirmação a ser demonstrada na forma:

$$\forall x \in D. (P(x) \rightarrow C(x))$$

2. Mostre que a conclusão  $C(d)$  é verdadeira, sendo  $d$  um elemento *arbitrário* de  $D$ .
3. Conclua que  $\forall x \in D. (P(x) \rightarrow C(x))$  é verdadeira.

- O nome **demonstração trivial** segue de demonstrarmos que a conclusão da implicação é sempre verdadeira, sem usar a premissa.

- Exemplo 9 Mostre que se um inteiro  $n$  é par, então  $n \leq n$ .

## **Demonstração.**

Como todo inteiro é menor ou igual a si mesmo, a implicação vale independentemente da premissa.

Consequentemente, a implicação a ser demonstrada é válida, trivialmente.



# Demonstração por contradição ou por redução ao absurdo

- Forma geral: “Suponha o contrário do resultado a ser demonstrado. Se isto for absurdo, demonstra-se o resultado.”
- Em lógica proposicional
  1. Para demonstrar que a afirmação  $p$  é verdadeira, suponha que sua negação  $\neg p$  seja verdadeira.
  2. Mostre que  $\neg p$  leva a uma contradição, ou seja, que

$$\neg p \rightarrow \perp.$$

Conclua que  $p$  é verdadeira.

# Demonstração por contradição ou por redução ao absurdo

- Exemplo 10 Mostre que em qualquer grupo de 22 dias (consecutivos ou não), ao menos 4 dias caem no mesmo dia da semana.

**Demonstração.** Seja  $F$  a proposição “Em qualquer grupo de 22 dias (consecutivos ou não), ao menos 4 dias caem no mesmo dia da semana”.

Suponha que  $\neg F$  seja verdadeiro, ou seja, que “Existe um grupo de 22 dias (consecutivos ou não) em que no máximo 3 dias caem no mesmo dia da semana”.

Mas note que existem apenas 7 dias na semana. Logo, se no máximo 3 dias caem no mesmo dia da semana, o grupo de dias pode ter no máximo 21 dias. Isso contradiz a premissa de que o grupo tem 22 dias.

Em outras palavras, se  $G$  é a proposição “22 dias são escolhidos para fazer parte do grupo”, teríamos  $\neg F \rightarrow (G \wedge \neg G)$ , ou seja,  $\neg F \rightarrow \perp$ .

Logo,  $\neg F$  não pode nunca ser verdadeiro, ou seja,  $F$  é sempre verdadeiro.  $\square$

# Demonstração por contradição ou por redução ao absurdo

- Exemplo 11 Mostre que se  $3n + 2$  é ímpar, então  $n$  é ímpar.

**Demonstração.** Queremos mostrar a proposição “se  $3n + 2$  é ímpar, então  $n$  é ímpar”. Podemos escrever esta proposição como  $p \rightarrow q$ .

Para demonstrar por contradição, vamos supor que  $p \rightarrow q$  seja falso. Isso quer dizer que estamos supondo  $p \wedge \neg q$ , ou seja, que “ $3n + 2$  é ímpar e  $n$  não é ímpar”.

Mas se  $n$  não é ímpar, é porque  $n$  é par e existe um inteiro  $k$  tal que  $n = 2k$ . Podemos, então, derivar

$$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1),$$

o que implica que  $3n + 2$  é par. Mas isto significa que concluímos exatamente que  $p$  é falso, o que contradiz a hipótese de que  $p$  é verdadeiro.

Logo, não é possível ter  $p \wedge \neg q$  sem cair em contradição, e, portanto, se  $3n + 2$  é ímpar então  $n$  é ímpar. □

# Demonstração por contradição ou por redução ao absurdo

- Exemplo 12 Vamos mostrar que  $\sqrt{2}$  é irracional.

# Demonstração por contradição ou por redução ao absurdo

- Exemplo 12 Vamos mostrar que  $\sqrt{2}$  é irracional.

**Demonstração.** Para atingir uma contradição, suponha o contrário do que queremos demonstrar, ou seja, que  $\sqrt{2}$  seja racional.

# Demonstração por contradição ou por redução ao absurdo

- Exemplo 12 Vamos mostrar que  $\sqrt{2}$  é irracional.

**Demonstração.** Para atingir uma contradição, suponha o contrário do que queremos demonstrar, ou seja, que  $\sqrt{2}$  seja racional.

Neste caso, existem  $p, q \in \mathbb{Z}$ , com  $\text{mdc}(p, q) = 1$ , tais que  $\sqrt{2} = p/q$ .  
Elevando os dois lados ao quadrado, obtemos  $2 = p^2/q^2$ , ou seja,  $p^2 = 2q^2$ .  
Note que  $2q^2$  é par, portanto pela igualdade acima  $p^2$  também tem que ser par. Isto implica que  $p$  deve ser par.

# Demonstração por contradição ou por redução ao absurdo

- Exemplo 12 Vamos mostrar que  $\sqrt{2}$  é irracional.

**Demonstração.** Para atingir uma contradição, suponha o contrário do que queremos demonstrar, ou seja, que  $\sqrt{2}$  seja racional.

Neste caso, existem  $p, q \in \mathbb{Z}$ , com  $\text{mdc}(p, q) = 1$ , tais que  $\sqrt{2} = p/q$ . Elevando os dois lados ao quadrado, obtemos  $2 = p^2/q^2$ , ou seja,  $p^2 = 2q^2$ . Note que  $2q^2$  é par, portanto pela igualdade acima  $p^2$  também tem que ser par. Isto implica que  $p$  deve ser par.

Agora, já que  $p$  é par, existe algum  $s \in \mathbb{Z}$  tal que  $p = 2s$ . Isso implica que  $2q^2 = p^2 = (2s)^2 = 4s^2$ , o que resulta em  $q^2 = 2s^2$ . Note que então  $q^2$  é par, portanto  $q$  deve ser par.

# Demonstração por contradição ou por redução ao absurdo

- Exemplo 12 Vamos mostrar que  $\sqrt{2}$  é irracional.

**Demonstração.** Para atingir uma contradição, suponha o contrário do que queremos demonstrar, ou seja, que  $\sqrt{2}$  seja racional.

Neste caso, existem  $p, q \in \mathbb{Z}$ , com  $\text{mdc}(p, q) = 1$ , tais que  $\sqrt{2} = p/q$ . Elevando os dois lados ao quadrado, obtemos  $2 = p^2/q^2$ , ou seja,  $p^2 = 2q^2$ . Note que  $2q^2$  é par, portanto pela igualdade acima  $p^2$  também tem que ser par. Isto implica que  $p$  deve ser par.

Agora, já que  $p$  é par, existe algum  $s \in \mathbb{Z}$  tal que  $p = 2s$ . Isso implica que  $2q^2 = p^2 = (2s)^2 = 4s^2$ , o que resulta em  $q^2 = 2s^2$ . Note que então  $q^2$  é par, portanto  $q$  deve ser par.

Mas se ambos  $p$  e  $q$  são pares, isto contradiz a suposição de que o  $\text{mdc}(p, q) = 1$ : encontramos uma contradição.

# Demonstração por contradição ou por redução ao absurdo

- Exemplo 12 Vamos mostrar que  $\sqrt{2}$  é irracional.

**Demonstração.** Para atingir uma contradição, suponha o contrário do que queremos demonstrar, ou seja, que  $\sqrt{2}$  seja racional.

Neste caso, existem  $p, q \in \mathbb{Z}$ , com  $\text{mdc}(p, q) = 1$ , tais que  $\sqrt{2} = p/q$ . Elevando os dois lados ao quadrado, obtemos  $2 = p^2/q^2$ , ou seja,  $p^2 = 2q^2$ . Note que  $2q^2$  é par, portanto pela igualdade acima  $p^2$  também tem que ser par. Isto implica que  $p$  deve ser par.

Agora, já que  $p$  é par, existe algum  $s \in \mathbb{Z}$  tal que  $p = 2s$ . Isso implica que  $2q^2 = p^2 = (2s)^2 = 4s^2$ , o que resulta em  $q^2 = 2s^2$ . Note que então  $q^2$  é par, portanto  $q$  deve ser par.

Mas se ambos  $p$  e  $q$  são pares, isto contradiz a suposição de que o  $\text{mdc}(p, q) = 1$ : encontramos uma contradição.

Logo podemos concluir que não existem  $p, q \in \mathbb{Z}$ , com  $q \neq 0$  e  $\text{mdc}(p, q) = 1$ , tais que  $\sqrt{2} = p/q$ . Portanto  $\sqrt{2}$  é irracional. □

# Demonstração de equivalências

- Forma geral:
  - ① Para mostrar que  $p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_n$ , mostre, separadamente, cada uma das implicações

$$p_1 \rightarrow p_2$$

$$p_2 \rightarrow p_3$$

$$\dots \rightarrow \dots$$

$$p_n \rightarrow p_1$$

- Importante: A demonstração não está completa se não se fechar o ciclo de implicações, demonstrando que a última proposição implica de volta na primeira:  $p_n \rightarrow p_1$ .
- Note que este resultado depende da seguinte tautologia:

$$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$$

# Demonstração de equivalências

- Exemplo 13 Mostre que as seguintes afirmações sobre um inteiro  $n$  são equivalentes:

$p_1$  : “ $n$  é par”

$p_2$  : “ $n - 1$  é ímpar”

$p_3$  : “ $n^2$  é par”

# Demonstração de equivalências

- Exemplo 13 Mostre que as seguintes afirmações sobre um inteiro  $n$  são equivalentes:

$p_1$  : “ $n$  é par”

$p_2$  : “ $n - 1$  é ímpar”

$p_3$  : “ $n^2$  é par”

## Demonstração.

Vamos demonstrar que as três afirmações são equivalentes mostrando que as três implicações são verdadeiras:  $p_1 \rightarrow p_2$ ,  $p_2 \rightarrow p_3$ , e  $p_3 \rightarrow p_1$ .

- $p_1 \rightarrow p_2$  : Vamos usar uma demonstração direta.

Se  $n$  é par, então  $n = 2k$  para algum inteiro  $k$ . Logo:

$$n - 1 = 2k - 1 = 2(k - 1) + 1 ,$$

e, portanto  $n - 1$  é ímpar, por ser da forma  $2m + 1$  para o inteiro  $m = k - 1$ .

# Demonstração de equivalências

- Exemplo 13 (Continuação)

- $p_2 \rightarrow p_3$  : Vamos usar uma demonstração direta.

Se  $n - 1$  é ímpar, então  $n - 1 = 2k + 1$  para algum inteiro  $k$ . Logo:

$$n = (2k + 1) + 1 = 2k + 2 .$$

Portanto podemos derivar

$$n^2 = (2k + 2)^2 = 4k^2 + 8k + 4 = 2(k^2 + 4k + 2) ,$$

de onde concluímos que  $n^2$  é par por ser da forma  $n = 2m$  para o inteiro  $m = k^2 + 4k + 2$ .

- $p_3 \rightarrow p_1$  : Vamos usar uma demonstração por contraposição.

Mas note que a contraposição desejada,  $\neg p_1 \rightarrow \neg p_3$ , é a afirmação “Se  $n$  é ímpar, então  $n^2$  é ímpar”, que já demonstramos em um exemplo anterior.

Concluídas as demonstrações das três implicações, as equivalências desejadas estão estabelecidas.



# Contra-exemplos

- Contra-exemplos evidenciam que conjecturas são inválidas.

- Em lógica de predicados:

1. Exprese a afirmação a ser demonstrada na forma:

$$\forall x \in D. P(x)$$

2. Encontre um  $d \in D$  tal que  $P(d)$  seja falso.
3. Conclua que a afirmação em questão é inválida.

# Contra-exemplos

- Exemplo 14 Seja  $f(n) = n^2 + n + 41$ . Demonstre que, para todo inteiro  $n$ ,  $f(n)$  é primo.

# Contra-exemplos

- Exemplo 14 Seja  $f(n) = n^2 + n + 41$ . Demonstre que, para todo inteiro  $n$ ,  $f(n)$  é primo.

**Solução.** Tome o valor  $n = 40$ . Neste caso temos  $f(n) = 1681 = 41 \cdot 41$ , que não é primo. Logo  $n = 40$  é um contra-exemplo e a afirmação não pode ser demonstrada. □

# Demonstração por exaustão ou divisão em casos

- Forma geral: “Se o número de casos é finito, mostre para cada caso que a afirmação é verdadeira.”
- Em lógica proposicional:

1. Se deve-se mostrar que

$$p_1 \vee p_2 \vee \dots \vee p_n \rightarrow q$$

2. Mostre, separadamente, cada uma das implicações

$$p_1 \rightarrow q$$

$$p_2 \rightarrow q$$

$$\dots \rightarrow \dots$$

$$p_n \rightarrow q$$

3. Conclua que  $p \rightarrow q$ .

# Demonstração por exaustão ou divisão em casos

- Exemplo 15 Mostre que, dados dois números reais  $x, y$ ,  
 $\min(x, y) + \max(x, y) = x + y$ .

# Demonstração por exaustão ou divisão em casos

- **Exemplo 15** Mostre que, dados dois números reais  $x, y$ ,  
 $\min(x, y) + \max(x, y) = x + y$ .

**Demonstração.** Há somente três possibilidades para  $x$  e  $y$ :

$$x < y \quad \text{ou} \quad x = y \quad \text{ou} \quad x > y$$

Vamos analisar cada caso separadamente:

- Se  $x < y$ , então  $\min(x, y) + \max(x, y) = x + y$ .
- Se  $x = y$ , então  $\min(x, y) + \max(x, y) = x + y$ .
- Se  $x > y$ , então  $\min(x, y) + \max(x, y) = y + x = x + y$ .

Logo, podemos concluir que sempre teremos  
 $\min(x, y) + \max(x, y) = x + y$ .



# Demonstração por exaustão ou divisão em casos

- **Definição:** Dado um número real  $a$ , seu **valor absoluto**  $|a|$  é definido como  $|a| = a$  quando  $a \geq 0$ , e como  $|a| = -a$  quando  $a < 0$ .
- **Exemplo 16** Mostre que  $|xy| = |x||y|$ , em que  $x$  e  $y$  são números reais.

**Demonstração.** Note que podemos identificar cinco casos exaustivos para a combinação de  $x$  e  $y$ :

1. pelo menos um entre  $x$  e  $y$  é zero,
2.  $x$  e  $y$  são ambos positivos,
3.  $x$  é positivo e  $y$  é negativo,
4.  $x$  é negativo e  $y$  é positivo, ou
5.  $x$  e  $y$  são ambos negativos.

# Demonstração por exaustão ou divisão em casos

- Exemplo 16 (Continuação)

Vamos analisar cada caso separadamente:

1. Se pelo menos um entre  $x$  e  $y$  é zero, então  $xy = 0$  e pelo menos um entre  $|x|$  e  $|y|$  é zero e, portanto, temos

$$|xy| = 0 = |x||y|.$$

2. Se  $x$  e  $y$  são ambos positivos, então  $xy > 0$  e temos

$$|xy| = xy = |x||y|.$$

3. Se  $x$  é positivo e  $y$  é negativo, então  $xy < 0$  e temos

$$|xy| = -xy = x(-y) = |x||y|.$$

4. Se  $x$  é negativo e  $y$  é positivo, então  $xy < 0$  e temos

$$|xy| = -xy = (-x)y = |x||y|.$$

5. Se  $x$  e  $y$  são ambos negativos, então  $xy > 0$  e temos

$$|xy| = xy = (-x)(-y) = |x||y|.$$

Logo, podemos concluir que a afirmação é sempre verdadeira. □

# Demonstração de existência

- Uma demonstração de um teorema do tipo  $\exists x \in D. P(x)$  é chamada de **demonstração de existência**.
- Uma demonstração de existência pode ser **construtiva**
  - Para *algum* elemento  $d \in D$  mostra-se que  $P(d)$  é verdadeiro.
  - O elemento  $d$  é chamado de **testemunha** da demonstração.
- Uma demonstração de existência pode ser **não-construtiva**
  - Não produz uma testemunha.
  - Demonstra-se  $\exists x. P(x)$  de outra maneira.
  - Uma maneira é por exemplo por redução ao absurdo.

# Demonstração de existência: construtiva

- **Exemplo 17** Mostre que existe um inteiro positivo que pode ser escrito como a soma de cubos de inteiros positivos de duas maneiras distintas.

**Demonstração.** Após uma busca trabalhosa (por exemplo, usando um programa de computador), encontramos que

$$1729 = 10^3 + 9^3 = 12^3 + 1^3.$$



- A demonstração acima é construtiva porque ela produz uma testemunha (o número 1729 junto com suas decomposições) que atesta a existência desejada.

## Demonstração de existência: não-construtiva

- Exemplo 18 Existem números irracionais  $x$  e  $y$  tais que  $x^y$  é racional.

# Demonstração de existência: não-construtiva

- Exemplo 18 Existem números irracionais  $x$  e  $y$  tais que  $x^y$  é racional.

**Demonstração.** Sabemos que  $\sqrt{2}$  é irracional (já demonstramos isto).

Considere o número  $\sqrt{2}^{\sqrt{2}}$ . Há duas possibilidades para este número:

1. Ele é racional. Neste caso temos dois números irracionais  $x = \sqrt{2}$  e  $y = \sqrt{2}$  tais que  $x^y$  é racional.
2. Ele é irracional. Neste caso podemos calcular que

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2,$$

é um número racional. Assim temos dois números irracionais  $x = \sqrt{2}^{\sqrt{2}}$  e  $y = \sqrt{2}$  tais que  $x^y$  é racional. □

- A demonstração acima é não-construtiva porque ela não produz uma testemunha que atesta a existência desejada.

Sabemos que ou o par  $x = \sqrt{2}$ ,  $y = \sqrt{2}$  ou o par  $x = \sqrt{2}^{\sqrt{2}}$ ,  $y = \sqrt{2}$  satisfaz a propriedade, mas não sabemos qual destes dois pares é o certo!

# Demonstração de unicidade

- Alguns teoremas afirmam a existência de um único objeto com uma certa propriedade.
- Forma geral: “Existe um objeto para o qual a propriedade vale e *para todos os outros* ela é falsa.”
  1. **Demonstração de existência:** Mostre que um objeto  $x$  com a propriedade deseja existe.
  2. **Demonstração de unicidade:** Mostre que se dois objetos  $x$  e  $y$  apresentam ambos a mesma propriedade desejada, então  $x = y$ .
- Em lógica de predicados:

$$\exists x. (P(x) \wedge \forall y. (P(y) \rightarrow y = x))$$

# Demonstração de unicidade

- Exemplo 19 Mostre que se  $a$  e  $b$  são números reais tais que  $a \neq 0$ , então existe um único número real  $r$  tal que  $ar + b = 0$ .

# Demonstração de unicidade

- **Exemplo 19** Mostre que se  $a$  e  $b$  são números reais tais que  $a \neq 0$ , então existe um único número real  $r$  tal que  $ar + b = 0$ .

## Demonstração.

Primeiro mostramos a existência de um real  $r$  com a propriedade desejada.

Para isto, fazemos  $r = -b/a$  e verificamos que neste caso

$$ar + b = a \left( \frac{-b}{a} \right) + b = -b + b = 0.$$

Em seguida, mostramos que  $r = -b/a$  é o único real satisfazendo a propriedade.

Para isto, suponha que exista um número real  $s$  tal que  $as + b = 0$ .

Então  $ar + b = as + b$ , com  $r = -b/a$ . Daí concluímos:

$$\begin{aligned} ar + b = as + b &\rightarrow ar = as && \text{(subtraindo } b \text{ dos dois lados)} \\ &\rightarrow r = s && \text{(dividindo os dois lados por } a) \end{aligned}$$



# Erros comuns em demonstrações

- Existem muitos erros comuns na construção de demonstrações matemáticas.
- Entre os erros mais comuns estão os erros algébricos básicos.
- Além disso, cada etapa de uma demonstração matemática precisa estar correta e a conclusão precisa seguir logicamente das etapas que a precedem.

# Erros comuns em demonstrações

- Muitos erros resultam da introdução de um passo que não segue logicamente daqueles que o precedem (falácias formais).
- Exemplo 20** Qual o erro na seguinte “demonstração” de que  $1 = 2$ ?

## Passo

- $\exists x, y \in \mathbb{R}. x = y$
- $a = b$
- $a^2 = ab$
- $a^2 - b^2 = ab - b^2$
- $(a + b)(a - b) = b(a - b)$
- $a + b = b$
- $2b = b$
- $2 = 1$

## Justificativa

- Premissa
- Instanciação existencial de (1)
- Multiplicando ambos os lados de (2) por  $a$
- Subtraindo  $b^2$  de ambos os lados de (3)
- Fatorando ambos os lados de (4)
- Dividindo ambos os lados de (5) por  $(a - b)$
- Substituindo (2) em (6) e simplificando
- Dividindo ambos os lados de (7) por  $b$

# Erros comuns em demonstrações

- Muitos erros resultam da introdução de um passo que não segue logicamente daqueles que o precedem (falácias formais).
- Exemplo 20 Qual o erro na seguinte “demonstração” de que  $1 = 2$ ?

## Passo

1.  $\exists x, y \in \mathbb{R}. x = y$
2.  $a = b$
3.  $a^2 = ab$
4.  $a^2 - b^2 = ab - b^2$
5.  $(a + b)(a - b) = b(a - b)$
6.  $a + b = b$
7.  $2b = b$
8.  $2 = 1$

## Justificativa

- Premissa
- Instanciação existencial de (1)
- Multiplicando ambos os lados de (2) por  $a$
- Subtraindo  $b^2$  de ambos os lados de (3)
- Fatorando ambos os lados de (4)
- Dividindo ambos os lados de (5) por  $(a - b)$
- Substituindo (2) em (6) e simplificando
- Dividindo ambos os lados de (7) por  $b$

# Erros comuns em demonstrações

- Exemplo 20 (Continuação)

## Solução.

Todos os passos na “demonstração” estão corretos, exceto pelo passo (6) e pelo passo (8).

Como  $a = b$  (pelo passo (2)), temos que  $a - b = 0$  e, portanto, a divisão de um real por  $(a - b)$  não pode ser realizada.

Além disso, no passo (8) não sabemos se  $b \neq 0$ , logo não podemos dividir por  $b$ .



# Erros comuns em demonstrações

- Outro erro comum em demonstrações é argumentar a partir de exemplos.
- Exemplo 21 **Teorema:** “Se  $m + n$  é par então  $m - n$  é par.”

**Demonstração incorreta:** Se  $m = 14$  e  $n = 6$  então  $m + n = 20$ , que é par, e  $m - n = 8$ , que também é par.

Logo se  $m + n$  é par então  $m - n$  é par. □

# Erros comuns em demonstrações

- Mais um tipo comum de erro é pular para uma conclusão, ou alegar a verdade de alguma coisa sem dar uma razão adequada.
- Exemplo 22 **Teorema:** “Se  $m + n$  é par então  $m - n$  é par.”

**Demonstração incorreta:** Suponha que  $m$  e  $n$  sejam inteiros e que  $m + n$  é par. Pela definição de par,  $m + n = 2k$  para algum inteiro  $k$ . Então  $m = 2k - n$  e assim  $m - n$  é par. □

# Erros comuns em demonstrações

- Mais um tipo comum de erro é pular para uma conclusão, ou alegar a verdade de alguma coisa sem dar uma razão adequada.

- Exemplo 22 **Teorema:** “Se  $m + n$  é par então  $m - n$  é par.”

**Demonstração incorreta:** Suponha que  $m$  e  $n$  sejam inteiros e que  $m + n$  é par. Pela definição de par,  $m + n = 2k$  para algum inteiro  $k$ . Então  $m = 2k - n$  e assim  $m - n$  é par. □

- Exemplo 23 Corrija as demonstrações acima, demonstrando corretamente a afirmação “Se  $m + n$  é par então  $m - n$  é par”.

**Solução.** Exercício para o(a) estudante! •

# Regras de inferência

# Regras de inferência para proposições quantificadas

- Vamos discutir regras de inferência para proposições quantificadas.
  - Muito usadas em argumentos matemáticos, muitas vezes de forma implícita.
- Regras de inferência importantes para lógica de predicados:

Nome	Inferência	Condição
Instanciação universal	$\frac{\forall x. P(x)}{P(c)} \quad I_{\forall}$	para qualquer $c$ do domínio do $x$
Generalização universal	$\frac{P(c)}{\forall x. P(x)} \quad G_{\forall}$	se $c$ é um elemento arbitrário do domínio
Instanciação existencial	$\frac{\exists x. P(x)}{P(c)} \quad I_{\exists}$	para algum $c$ do domínio
Generalização existencial	$\frac{P(c)}{\exists x. P(x)} \quad G_{\exists}$	para algum $c$ do domínio

# Regras de inferência para proposições quantificadas

- Exemplo 24 Mostre que as premissas
  - Ⓐ *“Todos os matriculados em Introdução à Lógica Computacional são estudantes dedicados”*
  - e
  - Ⓑ *“Felipe está matriculado em Introdução à Lógica Computacional”*
  - implicam a conclusão
  - Ⓒ *“Felipe é um estudante dedicado”*

# Regras de inferência para proposições quantificadas

- Exemplo 24 Mostre que as premissas
  - Ⓐ *“Todos os matriculados em Introdução à Lógica Computacional são estudantes dedicados”*
  - e
  - Ⓑ *“Felipe está matriculado em Introdução à Lógica Computacional”*
  - implicam a conclusão
  - Ⓒ *“Felipe é um estudante dedicado”*

**Solução.** Vamos definir os seguintes predicados, tendo como domínio o conjunto de todas os estudantes:

- $M(x)$  : *“x está matriculado em Introdução à Lógica Computacional.”*
- $D(x)$  : *“x é um estudante dedicado.”*

# Regras de inferência para proposições quantificadas

- Exemplo 24 (Continuação)

As premissas do argumento são, então:

(a)  $\forall x : ( M(x) \rightarrow D(x) )$

(b)  $M(\text{Felipe})$

A conclusão do argumento é:

(c)  $D(\text{Felipe})$

A derivação da conclusão a partir das premissas pode ser feita assim:

## Passo

## Justificativa

1.  $\forall x. ( M(x) \rightarrow D(x) )$

Premissa (a)

2.  $M(\text{Felipe}) \rightarrow D(\text{Felipe})$

Instanciação universal de (1)

3.  $M(\text{Felipe})$

Premissa (b)

4.  $D(\text{Felipe})$

Modus ponens usando (2) e (3)



# Regras de inferência para proposições quantificadas

- Exemplo 25 Mostre que as premissas
  - Ⓐ *“Um estudante de Introdução à Lógica Computacional não leu o livro-texto”, e*
  - Ⓑ *“Todos os estudantes de Introdução à Lógica Computacional foram bem na prova”*implicam a conclusão
  - Ⓒ *“Algum estudante de Introdução à Lógica Computacional que foi bem na prova não leu o livro-texto”*

# Regras de inferência para proposições quantificadas

- Exemplo 25 Mostre que as premissas

- (a) *“Um estudante de Introdução à Lógica Computacional não leu o livro-texto”, e*

- (b) *“Todos os estudantes de Introdução à Lógica Computacional foram bem na prova”*

implicam a conclusão

- (c) *“Algum estudante de Introdução à Lógica Computacional que foi bem na prova não leu o livro-texto”*

**Solução.** Vamos definir os seguintes predicados, tendo como domínio o conjunto de todas as pessoas:

- $M(x)$  : *“x é estudante de Introdução à Lógica Computacional.”*

- $L(x)$  : *“x leu o livro-texto.”*

- $P(x)$  : *“x foi bem na prova.”*

# Regras de inferência para proposições quantificadas

- Exemplo 25 (Continuação)

As premissas do argumento são, então:

$$(a) \exists x. (M(x) \wedge \neg L(x))$$

$$(b) \forall x. (M(x) \rightarrow P(x))$$

A conclusão do argumento é:

$$(c) \exists x. (M(x) \wedge \neg L(x) \wedge P(x))$$

# Regras de inferência para proposições quantificadas

- Exemplo 25 (Continuação)

A derivação da conclusão a partir das premissas pode ser feita assim:

## Passo

1.  $\exists x. (M(x) \wedge \neg L(x))$

2.  $M(c) \wedge \neg L(c)$

3.  $\forall x. (M(x) \rightarrow P(x))$

4.  $M(c) \rightarrow P(c)$

5.  $M(c)$

6.  $P(c)$

7.  $M(c) \wedge \neg L(c) \wedge P(c)$

8.  $\exists x. (M(c) \wedge \neg L(c) \wedge P(c))$

## Justificativa

Premissa (a)

Instanciação existencial de (1)

Premissa (b)

Instanciação universal de (3)

Simplificação conjuntiva de (2)

Modus ponens de (4) e (5)

Adição conjuntiva de (2) e (6)

Generalização existencial de (7)



# Combinando regras de inferência para proposições e predicados quantificados

- Como MP e  $I_{\forall}$  são combinadas com frequência, podemos usar a seguinte regra conhecida como **modus ponens universal**:

$$\frac{\forall x. P(x) \rightarrow Q(x) \quad P(c)}{Q(c)} \text{MP}_{\forall}$$

- Exemplo 26 Assuma que a seguinte premissa seja verdadeira:

*“Para todo inteiro positivo  $n$ , se  $n > 4$ , então  $n^2 < 2^n$ ”.*

Sabemos que a proposição “ $10 > 4$ ” é verdadeira.

Por modus ponens universal, podemos concluir que “ $10^2 < 2^{10}$ ”.

