Introdução a Demonstrações (cont.)

Matemática Discreta

Prof. Emanuel Estrada

centro de ciências computacionais

“Quando você elimina o impossível, o que sobra, por mais improvável que pareça, só pode ser a verdade.”

Arthur Conan Doyle

Demonstração por Contradição

- Supõe-se que a afirmação a ser provada é ***falsa***
- Usa-se premissas e outros fatos para mostrar que essa suposição leva a uma **contradição**, consequência absurda ou ridícula, *nonsense*...
- Conclui-se que a sentença a ser provada é verdadeira
- *Reductio ad absurdum* – Redução ao absurdo
- Podemos concluir que estávamos errado em assumir que a sentença era falsa, então a sentença original deve ser verdadeira

- Outro tipo de demonstração indireta

Demonstração por Contradição

- Este método não é limitado a provar somente sentenças condicionais
  - Esse método pode ser utilizado para provar qualquer tipo de sentença

Demonstração por Contradição

- Exemplo: Se $a, b \in \mathbb{Z}$, então $a^2 - 4b \neq 2$.

Supõe-se que

$$a^2 - 4b = 2$$

Negação

Demonstração por Contradição

- Exemplo: Se $a, b \in \mathbb{Z}$, então $a^2 - 4b \neq 2$.

Supõe-se que

$$a^2 - 4b = 2$$
$$a^2 = 4b + 2$$

Demonstração por Contradição

- Exemplo: Se $a, b \in \mathbb{Z}$, então $a^2 - 4b \neq 2$.

Supõe-se que

$$a^2 - 4b = 2$$
$$a^2 = 4b + 2$$
$$a^2 = 2(2b + 1)$$

$$a^2 = 2n$$
$$a = 2c$$

Demonstração por Contradição

- Exemplo: Se $a, b \in \mathbb{Z}$, então $a^2 - 4b \neq 2$.

Supõe-se que

$$a^2 - 4b = 2$$
$$a^2 = 4b + 2$$
$$a^2 = 2(2b + 1)$$
$$(2c)^2 - 4b = 2$$

$$a^2 = 2n$$
$$a = 2c$$

Demonstração por Contradição

- Exemplo: Se $a, b \in \mathbb{Z}$, então $a^2 - 4b \neq 2$.

<u>Supõe-se</u> que

$$a^2 - 4b = 2$$
$$a^2 = 4b + 2$$
$$a^2 = 2(2b + 1)$$
$$(2c)^2 - 4b = 2$$
$$4c^2 - 4b = 2$$

Demonstração por Contradição

- Exemplo: Se $a, b \in \mathbb{Z}$, então $a^2 - 4b \neq 2$.

Supõe-se que

$$a^2 - 4b = 2$$
$$a^2 = 4b + 2$$
$$a^2 = 2(2b + 1)$$
$$(2c)^2 - 4b = 2$$
$$4c^2 - 4b = 2$$
$$2(c^2 - b) = 1$$

Demonstração por Contradição

- Exemplo: Se $a, b \in \mathbb{Z}$, então $a^2 - 4b \neq 2$.

Supõe-se que

$$a^2 - 4b = 2$$
$$a^2 = 4b + 2$$
$$a^2 = 2(2b + 1)$$
$$(2c)^2 - 4b = 2$$
$$4c^2 - 4b = 2$$
$$2(c^2 - b) = 1$$
$$2d = 1$$

Demonstração por Contradição

- Exemplo: Se $a, b \in \mathbb{Z}$, então $a^2 - 4b \neq 2$.

Supõe-se que

$$a^2 - 4b = 2$$
$$a^2 = 4b + 2$$
$$a^2 = 2(2b + 1)$$
$$(2c)^2 - 4b = 2$$
$$4c^2 - 4b = 2$$
$$2(c^2 - b) = 1$$
$$2d = 1$$

Sabemos que 1 não é par, logo temos uma **contradição**.

Supomos erroneamente que a proposição $a^2 - 4b \neq 2$ é falsa. Portanto, a proposição é verdadeira.

Demonstração por Contradição

- A ideia da prova por contradição é bastante antiga
- Remonta, pelo menos, a época de Pitágoras, que usou para provar que certos números são irracionais

Demonstração por Contradição

- Exemplo: Demonstrar que o número $\sqrt{2}$ é irracional.

Definição: Um número irracional não pode ser representado por uma fração de inteiros

Demonstração por Contradição

- Exemplo: Demonstrar que o número $\sqrt{2}$ é irracional.

Supõe-se que $\sqrt{2}$ é racional, então há inteiros a e b em que

$$\sqrt{2} = \frac{a}{b}$$

A fração a/b deve estar na forma canônica, ou seja, completamente reduzida. Desta forma, a e b não podem ser ambos pares.

Definição: Um número real é racional se $x = \frac{a}{b}$ para cada $a, b \in \mathbb{Z}$

Demonstração por Contradição

$$\sqrt{2} = \frac{a}{b}$$

Demonstração por Contradição

$$\sqrt{2} = \frac{a}{b}$$

$$\sqrt{2}^2 = \frac{a^2}{b^2}$$

Demonstração por Contradição

$$\sqrt{2} = \frac{a}{b}$$

$$\sqrt{2}^2 = \frac{a^2}{b^2}$$

$$a^2 = 2b^2$$

Demonstração por Contradição

$$\sqrt{2} = \frac{a}{b}$$

$$\sqrt{2}^2 = \frac{a^2}{b^2}$$

$$a^2 = 2b^2$$

$$\therefore a = 2c$$

a é par

Como a e b não podem ser ambos pares, assume-se que b deve ser **<u>ímpar</u>** para manter a forma canônica. Caso contrário, poderíamos dividir a e b por 2.

Demonstração por Contradição

Sabendo-se que $a = 2c$, ou seja, um número par, substituímos a na equação e esperamos obter um b ímpar.

$$a^2 = 2b^2$$

Demonstração por Contradição

Sabendo-se que $a = 2c$, ou seja, um número par, substituímos a na equação e esperamos obter um b ímpar.

$$a^2 = 2b^2$$
$$(2c)^2 = 2b^2$$

Demonstração por Contradição

Sabendo-se que $a = 2c$, ou seja, um número par, substituímos a na equação e esperamos obter um b ímpar.

$$a^2 = 2b^2$$

$$(2c)^2 = 2b^2$$

$$4c^2 = 2b^2$$

Demonstração por Contradição

Sabendo-se que $a = 2c$, ou seja, um número par, substituímos a na equação e esperamos obter um b ímpar.

$$a^2 = 2b^2$$

$$(2c)^2 = 2b^2$$

$$4c^2 = 2b^2$$

$$2c^2 = b^2$$

Demonstração por Contradição

Sabendo-se que $a = 2c$, ou seja, um número par, substituímos a na equação e esperamos obter um b ímpar.

$$a^2 = 2b^2$$
$$(2c)^2 = 2b^2$$
$$4c^2 = 2b^2$$
$$2c^2 = b^2$$
$$\therefore b = 2d$$

Encontramos que b é par, porém esperávamos que ele fosse ímpar. Assim, temos a **contradição** que b é ímpar e b é par.

Demonstração por Contradição

- Para apreciar o poder da demonstração por contradição, imagine tentar provar que $\sqrt{2}$ é irracional sem esse método.
- No exemplo anterior obtivemos a contradição (b é par) $\wedge$ (b é ímpar)
- Em geral, a contradição não precisa ter essa forma. Qualquer sentença que é claramente falsa é suficiente. Por exemplo, $\mathbf{2 \neq 2}$

Demonstração por Contradição

- Provando por contradição que $\boldsymbol{p} \rightarrow \boldsymbol{q}$
- Assume-se que $\neg(p \rightarrow q)$ é verdadeiro, obtendo-se uma contradição
- Sabe-se que $\neg(\boldsymbol{p} \rightarrow \boldsymbol{q}) \equiv (\boldsymbol{p} \wedge \neg \boldsymbol{q})$, então supõe-se p e $\neg q$ como verdadeiras e espera-se obter um contradição.

Demonstração por Contradição

- **Exemplo**: Prove que se $3n + 5$ é par então n é ímpar

Demonstração por Contradição

- **Exemplo**: Prove que se $3n + 5$ é par então n é ímpar

p: $3n + 5$ é par
q: n é ímpar
$p \rightarrow q$

Demonstração por Contradição

- **Exemplo**: Prove que se $3n + 5$ é par então n é ímpar
- Demonstração por contradição

Assume-se que $3n + 5$ é par e $\boldsymbol{n}$ **é par**.

p: $3n + 5$ é par
q: n é ímpar
$p \rightarrow q$

$p \land \neg q$

Demonstração por Contradição

- **Exemplo**: Prove que se $3n + 5$ é par então n é ímpar
- Demonstração por contradição

Assume-se que $3n + 5$ é par e $\boldsymbol{n}$ **é par**.

$n = 2k$

p: $3n + 5$ é par
q: n é ímpar
$p \rightarrow q$

$p \wedge \neg q$

Demonstração por Contradição

- **Exemplo**: Prove que se $3n + 5$ é par então n é ímpar
- Demonstração por contradição

Assume-se que $3n + 5$ é par e $\boldsymbol{n}$ **é par**.

$n = 2k$

$3n + 5 = 3(2k) + 5 = 6k + 4 + 1 = 2(3k + 2) + 1$

p: $3n + 5$ é par
q: n é ímpar
$p \rightarrow q$

$p \land \neg q$

Demonstração por Contradição

- **Exemplo**: Prove que se $3n + 5$ é par então n é ímpar
- Demonstração por contradição

$p: 3n + 5$ é par
$q: n$ é ímpar
$p \rightarrow q$

Assume-se que $3n + 5$ é par e $\boldsymbol{n}$ **é par**.

$p \wedge \neg q$

$n = 2k$

$3n + 5 = 3(2k) + 5 = 6k + 4 + 1 = 2(3k + 2) + 1$

Sendo $m = 3k + 2$

$3n + 5 = 2m + 1$

Demonstração por Contradição

- **Exemplo**: Prove que se $3n + 5$ é par então n é ímpar
- Demonstração por contradição

Assume-se que $3n + 5$ é par e $\boldsymbol{n}$ **é par**.

$n = 2k$

$3n + 5 = 3(2k) + 5 = 6k + 4 + 1 = 2(3k + 2) + 1$

Sendo $m = 3k + 2$

$3n + 5 = 2m + 1$

Portanto, "$3n + 5$ é ímpar"

p: $3n + 5$ é par
q: n é ímpar
$p \rightarrow q$

$p \wedge \neg q$

Demonstração por Contradição

- **Exemplo**: Prove que se $3n + 5$ é par então n é ímpar
- Demonstração por contradição

p: $3n + 5$ é par
q: n é ímpar
$p \rightarrow q$

Assume-se que $3n + 5$ é par e $\boldsymbol{n}$ **é par**.

$p \wedge \neg q$

$n = 2k$

$3n + 5 = 3(2k) + 5 = 6k + 4 + 1 = 2(3k + 2) + 1$

Sendo $m = 3k + 2$

$3n + 5 = 2m + 1$

Portanto, "$3n + 5$ é ímpar"

Por contradição, se $3n + 5$ é par, então n é ímpar.

Demonstração por Contradição

- **Exemplo** 2: Prove que se n^2 é ímpar então n é ímpar

Demonstração por Contradição

- **Exemplo** 2: Prove que se n^2 é ímpar então n é ímpar
- Demonstração por contradição

Assume-se que n^2 é ímpar e $\boldsymbol{n}$ **é par**.

$n = 2k$

Demonstração por Contradição

- **Exemplo** 2: Prove que se n^2 é ímpar então n é ímpar
- Demonstração por contradição

Assume-se que n^2 é ímpar e $\boldsymbol{n}$ **é par**.

$n = 2k$

$n^2 = 4k^2 = 2(2k^2)$

Demonstração por Contradição

- **Exemplo** 2: Prove que se n^2 é ímpar então n é ímpar
- Demonstração por contradição

Assume-se que n^2 é ímpar e $\boldsymbol{n}$ **é par**.

$n = 2k$

$n^2 = 4k^2 = 2(2k^2)$

Sendo $m = 2k^2$

$n^2 = 2m$

Demonstração por Contradição

- **Exemplo** 2: Prove que se n^2 é ímpar então n é ímpar
- Demonstração por contradição

Assume-se que n^2 é ímpar e $\boldsymbol{n}$ **é par**.

$n = 2k$

$n^2 = 4k^2 = 2(2k^2)$

Sendo $m = 2k^2$

$n^2 = 2m$

Portanto, “n^2 é par”

Definindo-se c como “n^2 é ímpar”

$c \wedge \neg c$ é uma contradição

Por contradição, se n^2 é ímpar, então n é ímpar.

Demonstração por Contradição

- Mesmo a demonstração por contradição sendo um método poderoso de prova, é aconselhável usá-la somente quando o método direto e o por contraposição não funcionarem
- Muita vezes a prova por contradição pode ter oculta uma prova por contraposição
- Ex.: Supondo que $a \in \mathbb{Z}$. Se $a^2 - 2a + 7$ é par, então a é impar.

Demonstração por Contradição

- Ex.: Supondo que $a \in \mathbb{Z}$. Se $a^2 - 2a + 7$ é par, então a é ímpar.

$$\left.\begin{array}{l} p\colon a^2 - 2a + 7 \text{ é par} \\ q\colon a \text{ é ímpar} \end{array}\right\} p \to q$$

$$\left.\begin{array}{l} \neg p\colon a^2 - 2a + 7 \text{ é ímpar} \\ \neg q\colon a \text{ é par} \end{array}\right\} \neg q \to \neg p$$

Demonstração por Contradição

- Ex.: Supondo que $a \in \mathbb{Z}$. Se $a^2 - 2a + 7$ é par, então a é ímpar.

$$a = 2k$$
$$a^2 - 2a + 7 = (2k)^2 - 2(2k) + 7$$
$$a^2 - 2a + 7 = 4k^2 - 4k + 7$$
$$a^2 - 2a + 7 = 4k^2 - 4k + 6 + 1$$
$$a^2 - 2a + 7 = 2(2k^2 - 2k + 3) + 1$$
$$a^2 - 2a + 7 = 2t + 1$$

Demonstração por Contradição

- Exercício – Demonstre por contradição:
  a) Suponha que n seja um número inteiro. Se n ímpar, então $n + 11$ é par.
  b) Suponha que n seja um número inteiro. Se n^3+5 é impar, então n é par.
  c) Se a e b são números inteiros, então $a^2 - 4b - 2 \neq 0$

Demonstração Não Condicional

- Como provar que $p \leftrightarrow q$?
- Provando que:
  - $p \to q$
  - $q \to p$

Demonstração Não Condicional

- Ex.: n é ímpar se e somente se n^2 é ímpar.

Demonstração por Equivalência

- Como provar que $p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n$?

$$p_1 \leftrightarrow p_2 \leftrightarrow \cdots p_n \equiv$$
$$(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \ldots \wedge (p_{n-1} \rightarrow p_n) \wedge (p_n \rightarrow p_1)$$

Demonstração por Equivalência

- Mostre que as sentenças sobre um inteiro *n* são equivalentes

p: *n* é ímpar

q: *n*+1 é par

r: n^2 é ímpar

- Como provar?
- $p \leftrightarrow q \leftrightarrow r \equiv (p \rightarrow q) \wedge (q \rightarrow r) \wedge (r \rightarrow p)$

Demonstração por Equivalência

- Mostre que as sentenças sobre um inteiro *n* são equivalentes

p: *n* é ímpar

q: *n*+1 é par

r: n^2 é ímpar

- Demonstração:

1. $p \rightarrow q$: se *n* é ímpar, então n+1 é par. (demonstração direta)

n é ímpar: $n = 2k + 1$

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

$n + 1 = 2m$ (*n*+1 é par)

Demonstração por Equivalência

- Mostre que as sentenças sobre um inteiro *n* são equivalentes

p: *n* é ímpar

q: *n*+1 é par

r: n^2 é ímpar

- Demonstração:

2. $q \rightarrow r$: se *n*+1 é par, então n^2 é ímpar. (demonstração direta)

n+1 é par: $n + 1 = 2k$

$n = 2k - 1$

$n^2 = 4k^2 - 4k + 1 = 2(2k^2 - 2k) + 1$

$n^2 = 2m + 1$ (n^2 é ímpar)

Demonstração por Equivalência

- Mostre que as sentenças sobre um inteiro *n* são equivalentes

p: *n* é ímpar

q: *n*+1 é par

r: n^2 é ímpar

- Demonstração:

3. $r \rightarrow p$: se n^2 é ímpar, então n é ímpar. (já demonstrado por contradição)

Demonstração por Equivalência

- Prove por equivalência $p \leftrightarrow q \leftrightarrow r$

  p: “*n* é par”

  q: “*n*-5 é ímpar”

  r: “n^2 é par”

Demonstração por Equivalência

- Prove por equivalência $p \leftrightarrow q \leftrightarrow r$

  p: "*n* é par"

  q: "*n*-5 é ímpar"

  r: "n^2 é par"

Demonstração:

1. $p \rightarrow q$: Se n é par, então $n - 5$ é ímpar (demonstração direta)

$n = 2k$

$n - 5 = 2k - 5 = 2k - 6 + 1$

$n - 5 = 2(k - 3) + 1 = 2t + 1$ ($n - 5$ é ímpar)

Demonstração por Equivalência

- Prove por equivalência $p \leftrightarrow q \leftrightarrow r$

  p: "*n* é par"

  q: "*n*-5 é ímpar"

  r: "n^2 é par"

Demonstração:

2. $q \rightarrow r$: Se $n - 5$ é ímpar, então n^2 é par (demonstração direta)

$n - 5 = 2k + 1$

$n = 2k + 6 = 2(k + 3) = 2m$

$n^2 = (2m)^2 = 4m^2 = 2(2m^2) = 2t$ (n^2 é par)

Demonstração por Equivalência

- Prove por equivalência $p \leftrightarrow q \leftrightarrow r$

  p: “*n* é par”

  q: “*n*-5 é ímpar”

  r: “n^2 é par”

Demonstração:

3. $r \rightarrow p$: Se n^2 é par, então n é par (demonstração por contraposição)

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

$n^2 = 2t + 1$

Demonstração por Contraexemplo

- Como demonstrar que $\forall x P(x)$ é falsa?

  Encontrando um contraexemplo ☺

Demonstração por Contraexemplo

- Exemplo: demonstre que “todo positivo inteiro é a soma dos quadrados de dois inteiros” é falso.

Demonstração:

O número 3 não pode ser escrito pela soma dos quadrados de dois inteiros.

Por causa que os únicos quadrados que não excedem 3 são $0^2=0$ e $1^2=1$.

Não há uma forma de obter-se 3 pela soma destes quadrados.

Demonstração por Contraexemplo

- Exemplo: Sendo a e b são números reais, se $a^2 = b^2$, então $a = b$

Contraexemplo:

$a = 1$ e $b = -1$

Demonstração por Contraexemplo

- Exemplo: Seja $p(n) = n^2 + n + 41$.

Conjectura: Sendo n é qualquer número natural, então $p(n)$ é primo.

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

Achamos uma fórmula para qualquer número primo???

Definição: Um número natural n é **primo** se ele tem exatamente dois divisores positivos, 1 e n.

Demonstração por Contraexemplo

- Exemplo: Seja $p(n) = n^2 + n + 41$.

Conjectura: Sendo n é qualquer número natural, então $p(n)$ é primo.

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

Achamos uma fórmula para qualquer número primo???

"Só que não..." $p(40) = 1681$, que não é primo.

Definição: Um número natural n é **primo** se ele tem exatamente dois divisores positivos, 1 e n.