

# Conceitos Preliminares

Teoria da Computação – Ciência da Computação

Prof. Daniel Saad Nogueira Nunes



**INSTITUTO  
FEDERAL**

Brasília

---

Campus  
Taguatinga

# Sumário

Noções Matemáticas

Lógica

# Noções Matemáticas

- ▶ Antes de iniciar o nosso estudo em TC, precisamos revisar e abordar conceitos matemáticos básicos.
- ▶ Notações e ferramentas que vamos usar.

# Sumário

## Noções Matemáticas

Conjuntos

Sequências e Tuplas

Funções

Relações

Grafos

Linguagens e Cadeias

# Conjuntos

## Conjuntos

- ▶ Um conjunto é um grupo de objetos representado como uma unidade.
- ▶ Conjuntos podem ter objetos de tipos variados: números, símbolos, pessoas, ...
- ▶ Objetos que estão em um conjunto são denominados de elementos.
- ▶ Uma forma de descrever quais elementos estão em um conjunto é utilizar a notação de chaves:

$$\{7, 21, 57\}$$

# Conjuntos

## Notação (Pertinência)

- ▶ *Os símbolos  $\in$  e  $\notin$  são utilizados para denotar pertinência e não-pertinência de elementos em conjuntos.*
- ▶ *Ex:  $7 \in \{7, 21, 57\}$ .*
- ▶ *Ex:  $8 \notin \{7, 21, 57\}$*

# Conjuntos

## Notação ( $\subseteq$ )

- ▶ Dizemos que um conjunto  $A$  está contido em um conjunto  $B$ , se todo o elemento de  $A$  está em  $B$ .
- ▶ Representamos por  $A \subseteq B$ .

# Conjuntos

## Notação (Igualdade)

- ▶ *Dois conjuntos  $A$  e  $B$  são iguais se todo o elemento de  $A$  está em  $B$  e vice-versa.*
- ▶ *Em outras palavras,  $A = B$ , sse,  $A \subseteq B$  e  $B \subseteq A$ .*



# Conjuntos

## Notação ( $\subsetneq$ )

- ▶ Dizemos que um conjunto  $A$  está propriamente contido em um conjunto  $B$ , se todo o elemento de  $A$  está em  $B$ , mas  $B$  não é igual a  $A$ .
- ▶ Representamos por  $A \subsetneq B$ .

# Conjuntos

## Notação ( $\emptyset$ )

- ▶ *O conjunto vazio é aquele que não possui elementos.*
- ▶ *Representado por  $\emptyset$ .*

# Conjuntos

- ▶ A ordem na descrição não importa.
- ▶ Repetições também são ignoradas. Conjuntos são indistinguíveis considerando repetições.
- ▶ Ex:  $\{1, 2, 3\} = \{3, 2, 1\}$ .
- ▶ Ex:  $\{1, 1, 1, 1, 2, 3, 4\} = \{1, 2, 3, 4\}$ .
- ▶ **Multiconjuntos:** levam em consideração repetições.

# Conjuntos

## Definição (Cardinalidade)

- ▶ *A cardinalidade corresponde ao número de elementos que um conjunto possui.*
- ▶ *Denotamos por  $|A|$ .*
- ▶ *Em especial  $|\emptyset| = 0$ .*

# Conjuntos

- ▶ Alguns conjuntos são finitos.
- ▶ Alguns conjuntos são infinitos.
- ▶ Ex:  $|\{1, 2, 3, 4\}| = 4$ .
- ▶ Ex:  $\mathbb{N} = \{1, 2, 3, \dots\}$  é infinito.
- ▶ Ex:  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$  é infinito.
- ▶ Ex:  $\mathbb{R}$  é infinito.
- ▶ Curiosidade:  $|\mathbb{R}| > |\mathbb{Z}| = |\mathbb{N}|$ .

# Conjuntos

- ▶ Outra maneira de definir conjuntos, é colocando uma propriedade sobre os elementos.
- ▶ Conjunto dos pares:  $P = \{x | x = 2y \text{ com } y \in \mathbb{Z}\}$
- ▶ Conjunto dos ímpares:  $I = \{x | x = 2y + 1 \text{ com } y \in \mathbb{Z}\}$
- ▶ Conjunto dos primos:  $\Pi = \{x | x \in \mathbb{N} \wedge x > 1 \wedge \neg \exists y (1 < y < x \wedge x \bmod y = 0)\}$

# Conjuntos

## Definição (União)

*A união de dois conjuntos  $A$  e  $B$  corresponde a  $C = \{x | x \in A \text{ ou } x \in B\}$ .*

*A união de conjuntos é representada através do símbolo  $\cup$*

- ▶ Exemplo  $\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$ .
- ▶ Em especial  $A \cup \emptyset = A$ .

# Conjuntos

## Definição (Interseção)

*A interseção de dois conjuntos  $A$  e  $B$  corresponde a  $C = \{x | x \in A \text{ e } x \in B\}$ .*

*A interseção de conjuntos é representada através do símbolo  $\cap$ .*

- ▶ Exemplo  $\{1, 2\} \cap \{2, 3\} = \{2\}$ .
- ▶ Em especial  $A \cap \emptyset = \emptyset$ .



# Conjuntos

## Definição (Complemento)

*O complemento de um conjunto  $A$  é outro conjunto cujos elementos em consideração são exatamente aqueles que não estão em  $A$ .*

*Denotamos o complemento de  $A$  por  $\bar{A}$ .*

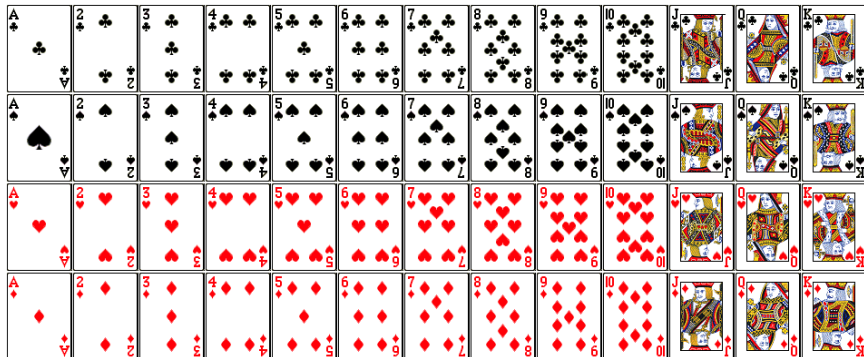
# Conjuntos

## Definição (Produto Cartesiano)

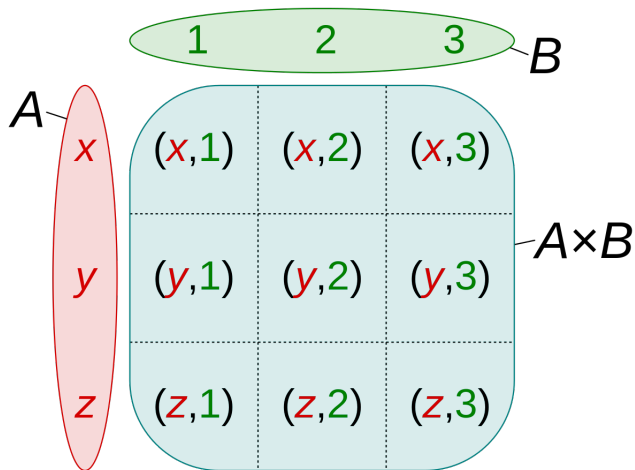
*Se  $A$  e  $B$  são conjuntos, o produto cartesiano de  $A$  por  $B$  é dado por:*

$$A \times B = \{(a, b) | a \in A \wedge b \in B\}$$

# Conjuntos



# Conjuntos



# Conjuntos

## Notação (Produto Cartesiano)

$$\underbrace{A \times A \times A \dots A}_k = A^k$$

- ▶ Ex:  $\mathbb{R}^2$ , o plano cartesiano.
- ▶ Ex:  $\mathbb{R}^3$ , espaço tridimensional.
- ▶ Ex:  $\mathbb{R}^n$ .
- ▶ Ex:  $\mathbb{N}^2 = \{(1, 1), (1, 2) \dots (2, 1), (2, 2) \dots\}$

# Conjuntos

## Definição (Partes de um Conjunto)

*As partes de um conjunto  $A$ , denotada por  $\mathcal{P}(A)$ , corresponde ao conjunto dos subconjuntos de  $A$ .*

Se  $|A| = n$ , então  $|\mathcal{P}(A)| = 2^n$

► Ex:  $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

# Sumário

## Noções Matemáticas

Conjuntos

**Sequências e Tuplas**

Funções

Relações

Grafos

Linguagens e Cadeias

# Sequências e Tuplas

## Definição (Sequências)

*Sequências de objetos são listas destes objetos. Diferentemente dos conjuntos, a ordem aqui importa, bem como as repetições.*



# Sequências e Tuplas

- ▶ Ex:  $F = (1, 1, 2, 3, 5, 8, \dots)$ .
- ▶ Ex:  $\Pi' = (2, 3, 5, 7, 11, \dots)$ .
- ▶ Ex:  $(1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \neq (1)$ .

# Sequências e Tuplas

## Notação

*Tuplas Uma sequência de  $k$  elementos é denominado uma  $k$ -tupla.*

- ▶ *Ex:  $(7, 21, 57)$  é uma tripla.*
- ▶ *Ex:  $(1, 4)$  é um par.*
- ▶ *Ex:  $(1, 5, 3, 4, 7, 8, 1)$  é uma 7-tupla.*

# Sumário

## Noções Matemáticas

Conjuntos

Sequências e Tuplas

**Funções**

Relações

Grafos

Linguagens e Cadeias

# Funções

## Funções

Funções são objetos matemáticos que mapeia elementos de um conjunto em outro.

Se  $f$  mapeia elementos de  $D$  em  $CD$ , denotamos por:

$$f : D \rightarrow CD$$

$D$  é chamado de domínio e  $CD$  é chamado de contradomínio.

Para ser uma função, cada elemento de  $D$  deve ter exatamente 1 mapeamento.

# Funções

- ▶ Ex:  $f(x) : \mathbb{N} \rightarrow \mathbb{N}$  com  $x \mapsto x^2$ . Então  $f(2) = 4$ ,  $f(3) = 9$ ,  $f(20) = 400$ .
- ▶ Ex:  $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  com  $(x, y) \mapsto x$  mais  $y$ . Então  $+(2, 2) = 4$ ,  $+(1, 5) = 6$ .

# Funções

## Definição

### *Funções Injetoras*

- ▶ Se  $x \neq y \rightarrow f(x) \neq f(y)$  a função é dita injetora.
- ▶ Ou seja, elementos diferentes do domínio são mapeados em elementos diferentes no contradomínio.

# Funções

## Definição

### *Funções Sobrejetoras*

- ▶ *Seja  $f : D \rightarrow CD$  e o conjunto imagem  $I = \{f(x), x \in D\}$ .*
- ▶  *$f$  é dita sobrejetora quando  $|I| = |CD|$ , ou seja, todos os elementos do contradomínio foram mapeados.*

# Funções

## Definição

*Funções Bijetoras São aquelas que são Injetoras e Sobrejetoras.  
Mapeamento um para um.*



# Sumário

## Noções Matemáticas

Conjuntos

Sequências e Tuplas

Funções

**Relações**

Grafos

Linguagens e Cadeias

# Relações

## Definição (Relações)

*Uma relação ou predicado é um subconjunto de algum conjunto com alguma propriedade específica.*

# Relações

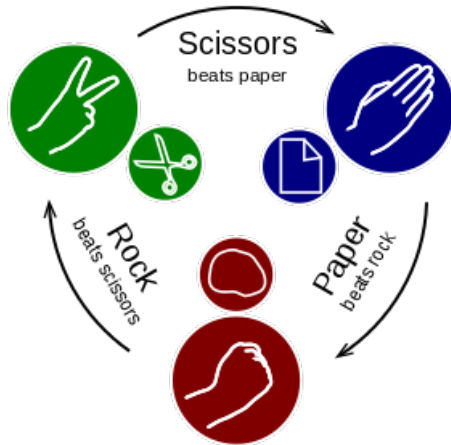
- ▶ Exemplos:  $P \subseteq \mathbb{N}$  e  $P := \{x | x \text{ é par}\}$ .
- ▶  $< \subseteq \mathbb{N} \times \mathbb{N}$  e  $< := \{(a, b) | a < b\}$ .

# Relações

## Notação

*Relações* Se  $R$  é uma relação e  $x \in R$ , dizemos que  $x$  vale,  $x$  é verdadeiro ou simplesmente  $x$  tem a propriedade  $R$ .

# Relações



# Sumário

## Noções Matemáticas

Conjuntos

Sequências e Tuplas

Funções

Relações

**Grafos**

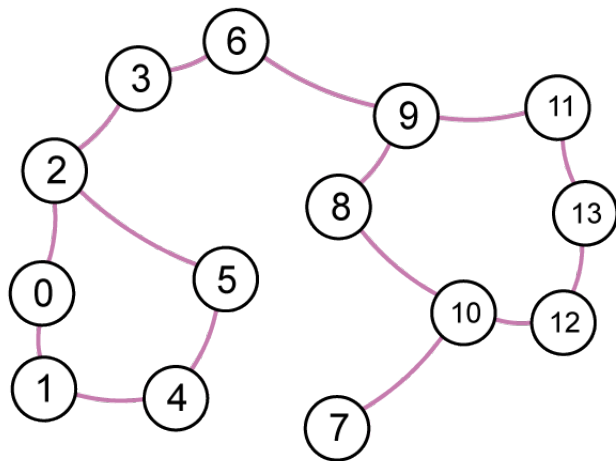
Linguagens e Cadeias

# Grafo Simples

## Definição (Grafo simples)

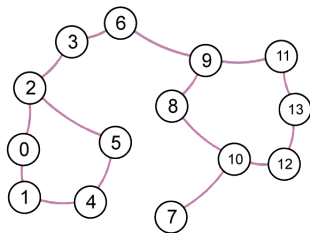
*Um grafo simples, é uma dupla  $G = (V, E)$  sendo  $V$  o conjunto de vértices e  $E \subseteq \{\{u, v\} \mid u, v \in V, u \neq v\}$  as arestas.*

# Grafos





# Grafos



► Neste exemplo temos:

$$V = \{0, 1, 2, \dots, 13\}$$

e

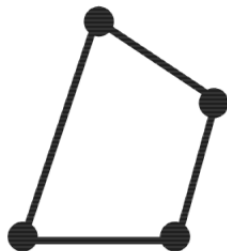
$$E = \left\{ \begin{array}{l} \{0, 1\}, \{0, 2\}, \{1, 4\}, \{4, 5\}, \{5, 2\}, \{2, 3\}, \{3, 6\}, \{6, 9\}, \\ \{9, 8\}, \{9, 11\}, \{8, 10\}, \{10, 12\}, \{12, 13\}, \{13, 11\}, \{10, 7\} \end{array} \right\}$$

# Grafos

## Definição (Subgrafo)

$G' = (V', E')$  é um subgrafo de  $G = (V, E)$ , quando  $V' \subseteq V$  e  $E' \subseteq E$ .

# Grafos



# Grafos

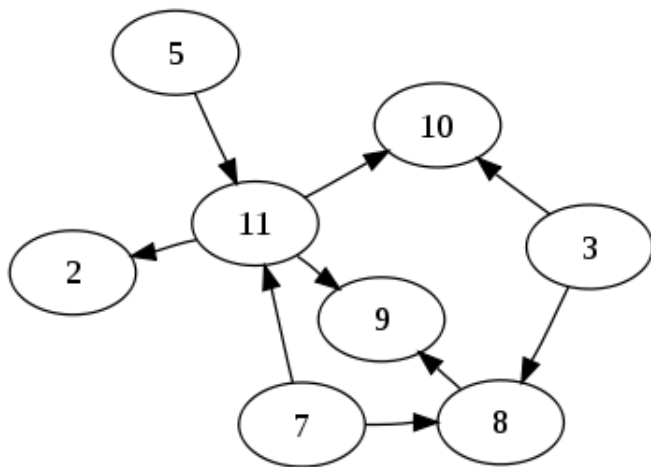
- ▶ Grafos também podem ser direcionados.
- ▶ Neste caso, a orientação das arestas faz diferença.

# Grafos

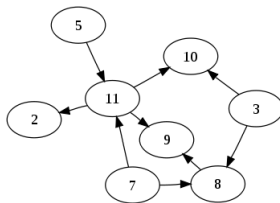
## Definição (Grafo direcionado)

*Um grafo direcionado, é uma dupla  $G = (V, E)$  sendo  $V$  o conjunto de vértices e  $E \subseteq V^2$  o conjunto de arestas.*

# Grafos



# Grafos



► Neste exemplo temos:

$$V = \{2, 3, 5, 7, 8, 9, 10, 11\}$$

e

$$E = \left\{ (5, 11), (11, 2), (11, 10), (11, 9), (3, 10), (3, 8), (8, 9), (7, 11), (7, 8) \right\}$$

# Grafos

- ▶ Modelam vários problemas práticos.
- ▶ Teoria dos grafos estuda estes objetos.



# Sumário

## Noções Matemáticas

Conjuntos

Sequências e Tuplas

Funções

Relações

Grafos

Linguagens e Cadeias

# Linguagens e Cadeias

## Definição (Alfabeto)

*Um alfabeto é qualquer conjunto não vazio e finito de símbolos.*

- ▶ Ex:  $\Sigma = \{0, 1\}$ .
- ▶ Ex:  $\Sigma = \{a, \dots, z, A, \dots, Z\}$ .
- ▶ Ex:  $\Gamma = \{0, 1, x, y, z\}$ .

# Linguagens e Cadeias

## Definição (Cadeias, Palavras ou Strings)

*Cadeias, palavras ou strings são sequências finitas de símbolos de alfabetos.*

- ▶ Supondo  $\Sigma = \{0, 1\}$ , então  $w = 01101101$  é uma cadeia válida.
- ▶ Suponho  $\Sigma = \{a, \dots, z\}$ , então  $w = \textit{abracadabra}$  é uma cadeia válida.

# Linguagens e Cadeias

## Notação (Tamanho de Cadeias)

*Seja  $w = w_1w_2w_3 \dots w_n$  uma cadeia sobre o alfabeto  $\Sigma$ . Denotamos  $|w| = n$  como o tamanho de  $n$ .*

*Em particular, a cadeia vazia,  $\varepsilon$ , tem tamanho  $|\varepsilon| = 0$ .*

# Linguagens e Cadeias

## Notação (Concatenação)

*Suponha cadeias  $x = x_1x_2 \dots x_n$  e  $y = y_1y_2 \dots y_m$  sobre o alfabeto  $\Sigma$ .*

*$xy = x_1x_2 \dots x_ny_1y_2 \dots y_m$  denota a concatenação de  $x$  com  $y$ .*

*Em especial  $\underbrace{xxx \dots x}_k = x^k$ .*

# Linguagens e Cadeias

## Notação (Inverso)

*Seja  $w = w_1w_2 \dots w_n$  uma cadeia sobre o alfabeto  $\Sigma$ .  $w^R = w_nw_{n-1} \dots w_1$  denota o inverso de  $w$ .*

# Linguagens e Cadeias

## Definição (Ordem lexicográfica)

*A ordem lexicográfica de cadeias da precedência para cadeias menores, e em caso de empate, segue-se a ordem do dicionário.*

- ▶ Para  $\Sigma = \{0, 1\}$ , a ordem lexicográfica sobre todas as palavras sobre o alfabeto  $\Sigma$  é:

$$(\varepsilon, 0, 1, 00, 01, 10, 11, 000, \dots)$$

# Linguagens e Cadeias

## Definição (Linguagem)

*Uma linguagem  $L$  é um conjunto de palavras.*

- ▶ Ex:  $L_1 = \{ww^R \mid w \text{ é uma cadeia sobre } \Sigma\}$
- ▶ Ex:  $L_2 = \{w \mid w = w^R\}$



# Linguagens e Cadeias

## Notação ( $\Sigma^*$ )

$\Sigma^*$  é a linguagem formada por todas as cadeias sobre o alfabeto  $\Sigma$ .

- ▶ Para  $\Sigma = \{0, 1\}$ ,  $\Sigma^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, \dots\}$ .
- ▶ Para  $\Sigma = \{A, C, G, T\}$ ,  $\Sigma^* = \{\varepsilon, A, C, G, T, AA, AC, AG, AT, \dots\}$ .

# Sumário

Noções Matemáticas

Lógica

# Lógica

- ▶ Por que a lógica é importante?

# Lógica

- ▶ Utilizamos lógica no dia a dia, na vida profissional e na pessoal.
- ▶ Elaboramos conceitos.
- ▶ Fazemos observações.
- ▶ Formalizamos teorias.
- ▶ Utilizamos **raciocínio lógico** para derivar conclusões a partir de premissas.
- ▶ Utilizamos **demonstrações** ou **provas** para convencer os outros que estamos corretos.

# Proposições

- ▶ Na matemática, uma **proposição** é uma sentença que pode ser **falsa** ou **verdadeira**, mas nunca as duas.
- ▶ Por exemplo:
  - ▶ “6 é par” é uma proposição verdadeira.
  - ▶ “4 é ímpar” é uma proposição falsa.

# Sumário

## Lógica

- Operadores Lógicos

- Quantificadores

- Definições

- Teoremas

- Provas

- Técnicas de Prova

# Operadores lógicos

- ▶ Podemos combinar proposições para criar outras mais complexas através dos operadores lógicos.

# Operadores lógicos

## Negação

Sejam  $p$  uma proposição.

- ▶ Não  $p$  ( $\neg p$ ) é verdadeiro quando  $p$  é falso.
- ▶ Não  $p$  ( $\neg p$ ) é falso quando  $p$  é verdadeiro.



# Operadores lógicos

## Conjunção

Sejam,  $p$  e  $q$  proposições.

- ▶  $p$  e  $q$  ( $p \wedge q$ ) é verdadeiro quando  $p$  e  $q$  são verdadeiros.
- ▶ Caso contrário,  $p \wedge q$  é falso.

# Operadores lógicos

## Disjunção

Sejam  $p$  e  $q$  proposições.

- ▶  $p$  ou  $q$  ( $p \vee q$ ) é verdadeiro quando  $p$  **ou**  $q$  são verdadeiros.
- ▶ Caso contrário,  $p \vee q$  é falso.

# Operadores lógicos

## Implicação

Sejam  $p$  e  $q$  proposições.

- ▶ Se  $p$  então  $q$  ( $p \Rightarrow q$ ) é verdadeiro quando  $p$  é falso **ou**  $q$  é verdadeiro.
- ▶ Caso contrário,  $p \Rightarrow q$  é falso.

# Operadores lógicos

## Implicação

Sejam  $p$  e  $q$  proposições.

- ▶ Se  $p$  então  $q$  ( $p \Rightarrow q$ ) é verdadeiro quando  $p$  é falso **ou**  $q$  é verdadeiro.
- ▶ Caso contrário,  $p \Rightarrow q$  é falso.
- ▶ Se  $p$  é falso, dizemos que  $p \Rightarrow q$  é *vacuamente* verdadeiro.

# Operadores lógicos

## Bi-implicação

Sejam  $p$  e  $q$  proposições.

- ▶  $p$  se, e somente se,  $q$  ( $p \Leftrightarrow q$ ) é verdadeiro quando  $p$  e  $q$  são falsos ou  $p$  e  $q$  são verdadeiros.
- ▶ Caso contrário,  $p \Leftrightarrow q$  é falso.
- ▶ Se  $p \Leftrightarrow q$  é verdadeiro, dizemos que  $p$  e  $q$  são equivalentes.

# Sumário

## Lógica

Operadores Lógicos

**Quantificadores**

Definições

Teoremas

Provas

Técnicas de Prova

# Quantificadores

- ▶ Considere a afirmação “ $x$  é par”.
- ▶ Não podemos dizer se esta afirmação é verdadeira ou falsa, pois não sabemos quem é  $x$ .

# Quantificadores

- ▶ Existem três maneiras básicas de conseguir obter um valor verdade para a afirmação.
  1. Dizer quem é  $x$ .  $x = 6$  por exemplo tornaria a afirmação verdadeira.
  2. Para todo  $x$  inteiro,  $x$  é par. O que tornaria a afirmação incorreta, pois nem todo inteiro é par.
  3. Existe  $x$  inteiro,  $x$  é par. O que tornaria a afirmação correta, pois existe inteiros pares.



# Quantificadores

- ▶ As frases “para todo” e “existe” são chamados de quantificadores.
- ▶ Podemos utilizar os símbolos  $\forall$  e  $\exists$  para representá-los de maneira mais compacta.

# Quantificadores

- ▶ Talvez as coisas fiquem mais claras com uma definição matemática.

# Quantificadores

## Definição (Número par)

*Um número  $x$  é dito par se e somente se existe um inteiro  $y$  tal que  $x = 2y$ .*

# Quantificadores

- ▶ Ou seja, estamos definido que um inteiro  $x$  é par, se e somente se existe algum  $y$  que multiplicado por 2 é igual a  $x$ .

# Quantificadores

- ▶ Utilizando a mesma estratégia, podemos definir os números ímpares.

# Quantificadores e Relações

## Definição (Número ímpar)

*Um número  $x$  é dito ímpar se e somente se existe um inteiro  $y$  tal que  $x = 2y + 1$ .*

# Quantificadores

- ▶ Os quantificadores podem ser aplicados à propriedades (relações).
- ▶ Seja  $P \subseteq \mathbb{N}$  a relação dos inteiros pares e  $I \subseteq \mathbb{N}$  a relação dos números ímpares.
  - ▶ Podemos dizer que  $\exists x P(x)$  é verdadeiro?
  - ▶ Podemos dizer que  $\exists x I(x)$  é verdadeiro?
  - ▶ Podemos dizer que  $\forall x P(x)$  é verdadeiro?
  - ▶ Podemos dizer que  $\forall x I(x)$  é verdadeiro?

# Quantificadores e Relações

Considerando os inteiros:

- ▶ O que  $\forall x \exists y (x = 2y)$  quer dizer?
- ▶ O que  $\exists x \exists y (x = 2y)$  quer dizer?
- ▶ O que  $\forall x (\exists y (x = 2y) \vee \exists y (x = 2y + 1))$  quer dizer?



# Quantificadores e Relações

- ▶ A ordem dos quantificadores também é muito importante.

# Quantificadores e Relações

Considerando  $<$  como a relação de menor entre inteiros:

- ▶  $\forall x \exists y (x < y)$  é verdadeiro?
- ▶  $\exists x \forall y (x < y)$  é verdadeiro?

# Sumário

## Lógica

Operadores Lógicos

Quantificadores

**Definições**

Teoremas

Provas

Técnicas de Prova

# Definições

## Definição (Definições)

*Definições descrevem os objetos e noções que utilizamos. Uma definição pode ser simples, como a de conjuntos que utilizamos, ou complexa, como a de segurança em sistemas criptográficos.*

*Ao definir devemos utilizar uma linguagem livre de ambiguidades, para que ser bem claro sobre o que estamos falando.*

# Afirmações

## Definição (Afirmações)

*Afirmações matemáticas expressam que determinado objeto possui determinada propriedade.*

*Independente de serem verdadeiras ou falsas, também devem ser precisas.*

# Prova

## Definição (Prova)

*Uma prova é uma sequência válida de passos dedutivos chegando a uma conclusão.*

# Sumário

## Lógica

Operadores Lógicos

Quantificadores

Definições

**Teoremas**

Provas

Técnicas de Prova

# Teoremas

## Definição (Teoremas)

*Teoremas são enunciados matemáticos verdadeiros e que podem ser provados.*



# Lemas

- ▶ Existem teoremas complexos de obter a prova.
- ▶ Para facilitar, podemos provar afirmações menores.
- ▶ Estas afirmações são chamadas de Lemas.
- ▶ Utilizamos Lemas para concluir os teoremas de maneira mais simples.

# Corolário

- ▶ Corolários são afirmações verdadeiras que decorrem imediatamente de um teorema.

# Sumário

## Lógica

Operadores Lógicos

Quantificadores

Definições

Teoremas

**Provas**

Técnicas de Prova

# Provas

- ▶ Uma prova ou demonstração matemática pode ser vista como um argumento para convencer outra pessoa que algo é verdadeiro.
- ▶ Uma boa prova deve ser a mais didática possível.
- ▶ Algumas estruturas são comuns dependendo da afirmação a qual se quer provar.

# Estrutura de provas

Queremos provar que  $p$  é verdadeiro:

- ▶ Prove diretamente que  $p$  é verdadeiro.
- ▶ Assuma que  $p$  é falso e chegue em uma contradição.

# Estrutura de provas

Queremos provar que  $p \wedge q$  é verdadeiro:

- Prove diretamente que  $p$  vale e prove que  $q$  vale.

# Estrutura de provas

Queremos provar que  $p \vee q$  é verdadeiro:

- ▶ Assuma que  $p$  é falso e deduza que  $q$  obrigatoriamente tem que ser verdadeiro.
- ▶ Assuma  $q$  falso e deduza que  $p$  obrigatoriamente tem que ser verdadeiro.
- ▶ Prove que  $p$  é verdadeiro.
- ▶ Prove que  $q$  é verdadeiro.

# Estrutura de provas

Queremos provar que  $p \Rightarrow q$  é verdadeiro:

- ▶ Assuma que  $p$  vale e deduza que  $q$  também vale.
- ▶ Assuma  $q$  falso e deduza que  $p$  tem que ser falso também.



# Estrutura de provas

Queremos provar que  $p \Leftrightarrow q$  é verdadeiro:

- Prove  $p \Rightarrow q$  e prove  $q \Rightarrow p$ .

# Estrutura de provas

Queremos provar que  $\exists x P(x)$  é verdadeiro:

- ▶ Basta encontrar um  $x$  que satisfaça a propriedade.

# Estrutura de provas

Queremos provar que  $\forall x P(x)$  é verdadeiro:

- ▶ Não assuma nada sobre  $x$  e prove que  $P(x)$  vale.

# Provas

- ▶ Por exemplo, vamos provar que, para todo inteiro  $x$ , se  $x$  é ímpar, então  $x + 1$  é par.

# Provas

- ▶ Como queremos mostrar que o resultado vale para qualquer  $x$ , não podemos assumir absolutamente nada sobre ele.
- ▶ Como o teorema diz respeito a uma implicação (se, então), assumimos a primeira parte e tentamos provar a segunda.

# Provas

## Demonstração.

Assuma  $x$  ímpar.

Como  $x$  é ímpar, temos que existe um  $y$  tal que  $x = 2y + 1$ .

Adicionando 1 a ambos os lados, temos que  $x + 1 = 2y + 2$ .

Tome  $w = y + 1$ , substituindo temos:  $x + 1 = 2w$ .

Portanto  $x + 1$  é par.



# Sumário

## Lógica

Operadores Lógicos

Quantificadores

Definições

Teoremas

Provas

Técnicas de Prova

# Prova por casos

## Prova por casos

A prova por casos divide a prova em diversos casos, transformando-a em múltiplas provas mais simples.



# Prova por casos

- ▶ Vamos pegar o seguinte teorema para ilustrar a técnica de prova por casos:

## Teorema

*Para qualquer inteiro  $x$ , o inteiro  $x(x + 1)$  é par.*

- ▶ Temos dois casos:  $x$  é par ou  $x$  é ímpar.

# Prova por casos

## Demonstração.

Caso 1:  $x$  é par.

- ▶ Como  $x$  é par, temos que existe um  $y$  tal que  $x = 2y$ .
- ▶ Assim, temos que:

$$x(x + 1) = 2y(2y + 1)$$

- ▶ Tome  $w = y(2y + 1)$ .
- ▶ Assim:

$$x(x + 1) = 2y(2y + 1) = 2w$$

- ▶ Logo  $x(x + 1)$  é par.



# Prova por casos

## Demonstração.

Caso 2:  $x$  é ímpar.

- ▶ Como  $x$  é ímpar, temos que existe um  $y$  tal que  $x = 2y + 1$ .
- ▶ Assim, temos que:

$$x(x + 1) = (2y + 1)(2y + 2) = (2y + 1)(y + 1)2$$

- ▶ Tome  $w = (2y + 1)(y + 1)$ .
- ▶ Assim:

$$x(x + 1) = (2y + 1)(2y + 2) = (2y + 1)(y + 1)2 = 2w$$

- ▶ Logo  $x(x + 1)$  é par.



## Prova por Construção

Muitos teoremas afirmam a existência de um tipo particular de objeto.

Provas por construção mostram que é possível construir um objeto do referido tipo.

## Exemplo

Um grafo  $k$ -regular é aquele que todos os nós tem grau  $k$ .

### Teorema

*Para qualquer  $n > 2$  par, existe um grafo 3-regular com  $n$  nós.*

### Demonstração.

$$E = \{\{i, i + 1\} | 0 \leq i \leq n - 2\} \cup \{n - 1, 0\} \cup \{(i, i + n/2) | 0 \leq i \leq n/2 - 1\}$$



# Prova por Contradição

## Prova por Contradição

Assume-se que um teorema é falso. Uma vez concluído o absurdo, podemos concluir que o teorema é de fato verdadeiro.

# Exemplo I

Teorema

$\sqrt{2}$  é *irracional*.

Demonstração.

## Exemplo II

Suponha  $\sqrt{2}$  racional.

Logo  $\sqrt{2} = \frac{n}{m}$ , uma fração reduzida. Obviamente,  $n$  ou  $m$  é ímpar.

Elevando os dois lados ao quadrado temos:

$2 = \frac{n^2}{m^2}$ , e portanto  $n^2 = 2m^2$ , então  $n^2$  é par, e  $n$  também é.

Se  $n$  é par, temos  $n = 2k$  para algum  $k$ .

Substituindo, temos  $n^2 = (2k)^2 = 4k^2$ . Logo  $4k^2 = 2m^2$  e portanto  $m^2 = 2k^2$  o que torna  $m^2$  par e consequentemente  $m$  par. Mas  $n$  e  $m$  não podem ser simultaneamente pares. Contradição.

$\sqrt{2}$  tem que ser irracional.





# Prova por Indução

## Prova por Indução

Prova-se o caso base. Assume que a propriedade vale para todo  $k < n$ . Tentamos provar que vale para  $n$  utilizando as hipóteses de indução e o caso base.

# Prova por Indução

## Teorema

*O  $n$  ésimo termo de uma P.A de razão  $r$  é  $a_0 + rn$ .*

## Demonstração.

Para  $n = 0$ ,  $a_0 = a_0$ . Suponha que a propriedade vale para todo  $k < n$ .

Sabemos que  $a_n = a_{n-1} + r$ , pela definição da P.A. Aplicando a hipótese de indução sobre  $a_{n-1}$ , temos:

$$a_n = a_0 + r(n - 1) + r = a_0 + rn$$

