Fundamentos Teóricos da Computação

– Conceitos Matemáticos Preliminares –

Zenilton Kleber Gonçalves do Patrocínio Jr.

Ciência da Computação – PUC Minas

Belo Horizonte, Brasil

2025

PUC Minas

IM SCIENCE

Sumário

Teoria de Conjuntos

Conjunto

Abstação matemática que visa capturar o conceito do coleção (sequência não ordenada de elementos ou membros)

Simbologia

- $|A| \rightarrow$ número de elementos de A
- $\emptyset \rightarrow$ conjunto vazio
- $\in \rightarrow$ ser membro de
- $\notin \rightarrow$ não ser membro de
- $\subset, \supset, \subseteq, \supseteq, =, \cup, \cap, \ldots$

Teoria de Conjuntos

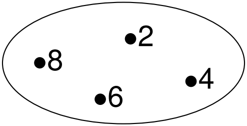
Definição explícita (ou por extensão)

$X = \{1, 2, 3\}$
$Y = \{a, b, c, d\}$

Definição implícita (ou por compreensão)

$Q = \{n \mid n = m^2 \text{ para todo número natural } m\}$

Diagrama de Venn



Teoria de Conjuntos

Relações básicas entre conjuntos

- **Subconjunto:** $A \subseteq B$ se e somente se $\forall x(x \in A \to x \in B)$
- **Subconjunto próprio:** $A \subset B$ se e somente se $A \subseteq B$ e $A \neq B$

Exemplos:

- $\emptyset \subseteq A$
- $\emptyset \subset A$ se $A \neq \emptyset$
- $\emptyset \not\subset \emptyset$

Teoria de Conjuntos

Operações básicas sobre conjuntos

- **União:** $A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$
- **Interseção:** $A \cap B = \{x \mid x \in A \text{ e } x \in B\}$
- **Diferença:** $A - B = \{x \mid x \in A \text{ e } x \notin B\}$
- **Complemento:** se $A \subseteq U$, então $C_U^A = U - A$ $\left(C_U^A = \overline{A} = A' \right)$

Teoria de Conjuntos

Exemplos de identidades

$A \cup B = B \cup A$

$A \cap B = B \cap A$

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$\overline{A \cup B} = \overline{A} \cap \overline{B}$

$\overline{A \cap B} = \overline{A} \cup \overline{B}$

$A - B = A \cap \overline{B}$

Teoria de Conjuntos

Igualdade

$A = B$ se e somente se $A \subseteq B$ e $B \subseteq A$

Prova de igualdade entre conjuntos

Para provar A = B:

1. Provar $A \subseteq B$;
2. Provar $B \subseteq A$.

Teoria de Conjuntos

Conjuntos disjuntos

A e B são disjuntos se e somente se $A \cap B = \emptyset$

União de n conjuntos

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n$$

Interseção de n conjuntos

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$$

Teoria de Conjuntos

Partição de um conjunto

Uma **partição** de A é o conjunto $\{A_1, A_2, \ldots, A_n\}$ tal que:

1. $A_i \neq \emptyset$ para $1 \leq i \leq n$;
2. $A_i \cap A_j = \emptyset$ para $1 \leq i < j \leq n$; e
3. $\bigcup_{i=1}^{n} A_i = A$.

Exemplo: Quais são as partições de $\{1, 2, 3\}$?

- $\{\{1\}, \{2\}, \{3\}\}$
- $\{\{1, 2\}, \{3\}\}$
- $\{\{1, 3\}, \{2\}\}$
- $\{\{1\}, \{2, 3\}\}$
- $\{\{1, 2, 3\}\}$

Teoria de Conjuntos

Partição de um conjunto

Uma **partição** de A é o conjunto $\{A_1, A_2, \ldots, A_n\}$ tal que:

1. $A_i \neq \emptyset$ para $1 \leq i \leq n$;
2. $A_i \cap A_j = \emptyset$ para $1 \leq i < j \leq n$; e
3. $\bigcup_{i=1}^{n} A_i = A$.

Exemplo: Quais são as partições de $\{1, 2, 3\}$?

- $\{\{1\}, \{2\}, \{3\}\}$
- $\{\{1, 2\}, \{3\}\}$
- $\{\{1, 3\}, \{2\}\}$
- $\{\{1\}, \{2, 3\}\}$
- $\{\{1, 2, 3\}\}$

Teoria de Conjuntos

Conjunto potência

Conjunto potência de A: $\mathcal{P}(A) = \{X \mid X \subseteq A\}$

Tamanho do conjunto potência

$|\mathcal{P}(A)| = 2^{|A|}$

Exemplo:

Qual é o tamanho e o conteúdo do conjunto $\mathcal{P}(\{1,2,3\})$?

- $|\mathcal{P}(\{1,2,3\})| = 2^{|\{1,2,3\}|} = 2^3 = 8$
- $\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

Teoria de Conjuntos

Conjunto potência

Conjunto potência de A: $\mathcal{P}(A) = \{X \mid X \subseteq A\}$

Tamanho do conjunto potência

$|\mathcal{P}(A)| = 2^{|A|}$

Exemplo:

Qual é o tamanho e o conteúdo do conjunto $\mathcal{P}(\{1, 2, 3\})$?

- $|\mathcal{P}(\{1, 2, 3\})| = 2^{|\{1,2,3\}|} = 2^3 = 8$
- $\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Teoria de Conjuntos

Conjunto potência

Conjunto potência de A: $\mathcal{P}(A) = \{X \mid X \subseteq A\}$

Tamanho do conjunto potência

$|\mathcal{P}(A)| = 2^{|A|}$

Exemplo:

Qual é o tamanho e o conteúdo do conjunto $\mathcal{P}(\{1,2,3\})$?

- $|\mathcal{P}(\{1,2,3\})| = 2^{|\{1,2,3\}|} = 2^3 = 8$
- $\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

Teoria de Conjuntos

Produto cartesiano de dois conjuntos

$$X \times Y = \{[x, y] \mid x \in X, y \in Y\}$$

Produto cartesiano de três conjuntos

$$X \times Y \times Z = \{[x, y, z] \mid x \in X, y \in Y, z \in Z\}$$

Produto cartesiano de *n* conjuntos

$$X_1 \times X_2 \times \ldots \times X_n = \{[x_1, x_2, \ldots, x_n] \mid x_i \in X_i, 1 \leq i \leq n\}$$

Obs.:
$X \times X = X^2, \quad X \times X \times X = X^3, \quad \ldots, \quad X \times X \times \ldots \times X = X^n$

Relações

Relações sobre dois conjuntos A_1 e A_2

É um subconjunto de $A_1 \times A_2$

Relações sobre n conjuntos $A_1, A_2, \ldots, A_n$

É um subconjunto de $A_1 \times A_2 \times \ldots \times A_n$

Relação binária: $R \subseteq A \times B$

Domínio: A
Contradomínio: B
Imagem: $\{y \mid [x, y] \in R \text{ para algum } x\}$

Notação: $[x, y] \in R$ é o mesmo que xRy

Relações

Exemplo de relação binária

Relação $< \subseteq \mathbb{N} \times \mathbb{N}$:

- **Domínio:** $\mathbb{N}$;
- **Contradomínio:** $\mathbb{N}$;
- **Imagem:** $\mathbb{N} - \{0\}$.

Relações

Inversa de relação binária

A relação inversa de R é $R^{-1} = \{[y, x] \mid [x, y] \in R\}$

Propriedades de uma relação binária $R \subseteq A \times A$

- **Reflexiva:** $\forall x \in A\, [xRx]$
- **Simétrica:** $\forall x, y \in A\, [xRy \rightarrow yRx]$
- **Transitiva:** $\forall x, y, z \in A\, [(xRy \wedge yRz) \rightarrow xRz]$

Relações

Exemplos

Considere as relações:

- $<$ sobre $\mathbb{N}^2$;
- $\leq$ sobre $\mathbb{N}^2$;
- $\subseteq$ sobre $\mathcal{P}(\mathbb{N})$;
- $\equiv$ sobre o conjunto das afirmativas da lógica proposicional.

Para cada uma diga se a mesma é reflexiva, simétrica e transitiva.

Relações

Relação de equivalência

Relação reflexiva, simétrica e transitiva é denominada relação de equivalência

$\Rightarrow$ Induz classes de equivalência

Exemplos:

- $(mod\ n) = \{[x, y] \in \mathbb{N}^2 \mid x\ mod\ n = y\ mod\ n\}$
- *fazem aniversário no mesmo dia*

Que classe de equivalência são induzidas por (*mod* 2)? E por (*mod* 10)? E por “*fazem anversário no mesmo dia*”?

Funções

Função parcial

Uma **função** $f : A \mapsto B$ é uma relação $f \subseteq A \times B$ tal que:

$$\text{se } [x, y] \in f \text{ e } [x, z] \in f \text{ então } y = z$$

- $[x, y] \in f$ é o mesmo que $f(x) = y$
- f é **indefinida** para x se não há y tal que $f(x) = y$
- Função **total**: é definida para todo argumento
- Função de n argumentos

$$f : A_1 \times A_2 \times \ldots \times A_n \mapsto B$$

Funções

Exemplos de funções

- $+ : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ (função total)
- $/ : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ (função parcial)

Funções

Composição de funções

$$g \circ f(x) = g(f(x))$$

Exemplo:

Sejam $f : \mathbb{Z} \mapsto \mathbb{N}$ tal que $f(n) = |n| + 1$
$g : \mathbb{N} \mapsto \mathbb{Z}$ tal que $g(n) = 1 - n$
Então:

- $g \circ f : \mathbb{Z} \mapsto \mathbb{Z}$ é tal que
  $(g \circ f)(n) = g(f(n)) = g(|n| + 1) = 1 - (|n| + 1) = -|n|$
- $f \circ g : \mathbb{N} \mapsto \mathbb{N}$ é tal que
  $(f \circ g)(n) = f(g(n)) = f(1 - n) = |1 - n| + 1$

Funções

Tipos de funções

Uma função total $f : A \mapsto B$ é:

- **Injetora:** se $\forall x, y[x \neq y \rightarrow f(x) \neq f(y)]$
  Ex: $f : \mathbb{N} \mapsto \mathbb{N}$ tal que $f(n) = 2n$
- **Sobrejetora:** se B é a imagem de f
  Ex: $f : \mathbb{Z} \mapsto \mathbb{N}$ tal que $f(n) = |n|$
- **Bijetora:** se for injetora e sobrejetora
  Ex: $f : \mathbb{Z} \mapsto \mathbb{N}$ tal que
  $$f(n) = \begin{cases} 2n & \text{se } n \geq 0 \\ -(2n+1) & \text{se } n < 0 \end{cases}$$

Cardinalidade

Teorema de Schröder-Bernstein

$card(A) = card(B)$ se existe uma função bijetora de A para B

$\Rightarrow card(A) = card(B)$ se $|A| = |B|$, caso A e B seja finitos

$\Rightarrow A$ é **infinito** se existe $X \subset A$ tal que $card(X) = card(A)$

Conjunto enumerável

A é conjunto enumerável se $card(A) = card(\mathbb{N})$

Conjunto **contável**: finito ou enumerável

Cardinalidade

Exemplo de conjunto enumerável

O conjunto $\mathbb{Z}$ é enumerável:

$$\begin{array}{cccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & \cdots \\
\updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
0 & -1 & 1 & -2 & 2 & -3 & 3 & \cdots
\end{array}$$

Cardinalidade

Corolário

A cardinalidade do conjunto X é menor ou igual a de Y se existir uma função injetora de X em Y

Teorema facilitador

As seguintes afirmativas são equivalentes:

1. A é contável;
2. Existe função injetora de A para $\mathbb{N}$;
3. $A = \emptyset$ ou existe função sobrejetora de $\mathbb{N}$ para A.

Cardinalidade

Outro exemplo de conjunto enumerável

O conjunto dos racionais não-negativos $\mathbb{Q}^+$ é enumerável:

	1	2	3	4	5	$\cdots$
0	0	1	3	6	10	
1	2	4	7	11		
2	5	8	12			
3	9	13				
4	14					
$\vdots$						

$f(i,j) = (i+j)(i+j-1)/2 + i$ é bijetora. Logo existe uma função sobrejetora de $\mathbb{N}$ para $\mathbb{Q}^+$

Cardinalidade

Outros resultados importantes

1. Todo subconjuto de conjunto contável é contável
2. Se A e B são contáveis, então $A \cup B$ é contável
3. Se A e B são contáveis, então $A \times B$ é contável

Cardinalidade

Teorema de Cantor

Para todo número cardinal $\alpha, \alpha < 2^{\alpha}$

Corolário

Seja X um conj. infinito, é de se esperar que $\mathcal{P}(X)$ seja maior que X.
Seja $\eta_0 = \mathcal{P}(X)$, então η_0 é muito maior que X
Se $\eta_1 = \mathcal{P}(\eta_0)$, então η_1 é maior que η_0 e assim sucessivamente...
Logo, existe um sistema de numeração em que:

$$card(\eta_0) < card(\eta_1) < card(\eta_2) < \dots$$

ou seja **os infinitos possuem tamanhos diferentes!**

Corolário

$\mathcal{P}(\mathbb{N})$ é incontável

Definições

Definições

Definições descrevem os objetos e noções que usamos de forma precisa e clara.

$\Rightarrow$ Ao se definir um objeto deve-se deixar claro o que constitui aquele objeto e o que não o constitui.

Uma definição pode ser:

- simples (por exemplo, a definição de um conjunto); ou
- complexa (por exemplo, a definição de segurança em um sistema criptográfico.

Definições Recursivas

Definição Recursiva

Uma propriedade importante de conjuntos enumeráveis é que eles podem ser definidos por meio de uma *definição recursiva* (ou *indutiva*). Uma **definição recursiva** espefica como um conjunto contável pode ser *gerado* a partir de um subconjunto do mesmo aplicando-se determinadas *operações* um número finito de vezes.

Partes da definição recursiva do conjunto A

1. **base:** especificação de um conjunto base $B \subset A$;
2. **passo recursivo:** especificação de um conjunto de operações que, se aplicadas a elementos de A, geram elementos de A;
3. **fechamento:** afirmação de que os únicos elementos de A são aqueles que podem ser obtidos a partir dos elementos de B aplicando-se um número finito de vezes as operações especificadas em (2).

Definições Recursivas

Observação

O conjunto B deve ser contável, podendo ser definido recursivamente.

Exemplo:

O conjunto $\mathbb{N}$ pode ser definido recursivamente da seguinte forma:

1. **base:** $0 \in \mathbb{N}$;
2. **passo recursivo:** se $n \in \mathbb{N}$, então $s(n) \in \mathbb{N}$, em que $s(n)$ representa o sucessor de n;
3. **fechamento:** só pertence a $\mathbb{N}$ o número que pode ser obtido de acordo com (1) e (2).

Pode-se omitir o item (3) de uma definição recursiva e dizer que o conjunto definido é o *menor conjunto* que pode ser obtido por meio de (1) e (2).

Definições Recursivas

Outro exemplo:

A função fatorial *fat* : $\mathbb{N} \mapsto \mathbb{N}$ é definida recursivamente por:

1. $fat(0) = 1$;
2. $fat(n) = n \times fat(n-1)$, para $n \geq 1$.

Evidentemente, a definição poderia ser colocada no formato anterior:

1. **base:** $(0, 1) \in fat$;
2. **passo recursivo:** se $n \geq 1$ e $(n-1, k) \in fat$, então $(n, nk) \in fat$;
3. **fechamento:** só pertence a *fat* o par que pode ser obtido conforme (1) e (2).

Enunciados Matemáticos

Enunciados Matemáticos

Enunciados matemáticos expressam que algum objeto possui uma certa propriedade.

$\Rightarrow$ Como uma definição, um enunciado deve ser preciso – não deve haver ambiguidade sobre seu significado.

Um enunciado pode ser:

- verdadeiro; ou
- falso.

Provas

Prova

Prova é um argumento lógico convincente de que um enunciado é verdadeiro.

Teorema

Teorema é um enunciado matemático demonstrado como verdadeiro – geralmente enunciados de especial interesse.

Lema

Lema é um enunciado que é interessante somente porque ajuda na prova de outro enunciado mais significativo.

Corolário

Corolário é um enunciado que pode ser facilmente demonstrado verdadeiro a partir de um outro teorema (ou de sua prova).

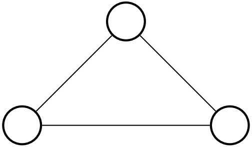
Encontrando Provas

- Não há “receita” para se produzir provas;
- Existem estratégias gerais que podem ser úteis;
- Deve-se procurar um sentimento intuitivo da razão que torna um enunciado verdadeiro;
- Experimentar com exemplos é especialmente útil – ajuda a identificar um **contra-exemplo**;
- As dificuldades de se obter um contra-exemplo podem ajudar a entender porque o enunciado é verdadeiro;
- Tente provar um(alguns) caso(s) especial(is) e vá generalizando para depois enteder o caso mais geral;
- A prova deve ser escrita apropriadamente – uma prova bem escrita é uma sequência de enunciados, na qual cada um segue por simples raciocínio lógico dos enunciados anteriores na sequência.

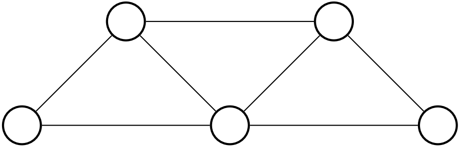
Encontrando Provas

Suponha que se deseje provar o enunciado: *para todo grafo G, a soma dos graus de todos os nós em G é um número par*.

Primeiro, examine uns grafos e observe se o enunciado é ou não verdadeiro. Eis dois exemplos:



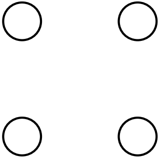
$$\text{soma} = 2 + 2 + 2 = 6$$



$$\text{soma} = 2 + 3 + 4 + 3 + 2 = 14$$

Encontrando Provas

A seguir, tente encontrar um **contra-exemplo**, ou seja, um grafo no qual a soma seja um número ímpar.

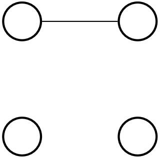


$$soma = 0$$

Agora, você começa a perceber que o enunciado deve ser verdadeiro e como pode prová-lo.

Encontrando Provas

A seguir, tente encontrar um **contra-exemplo**, ou seja, um grafo no qual a soma seja um número ímpar.

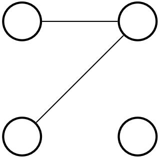


$soma = 2$

Agora, você começa a perceber que o enunciado deve ser verdadeiro e como pode prová-lo.

Encontrando Provas

A seguir, tente encontrar um **contra-exemplo**, ou seja, um grafo no qual a soma seja um número ímpar.

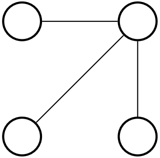


$soma = 4$

Agora, você começa a perceber que o enunciado deve ser verdadeiro e como pode prová-lo.

Encontrando Provas

A seguir, tente encontrar um **contra-exemplo**, ou seja, um grafo no qual a soma seja um número ímpar.

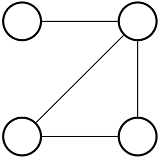


$soma = 6$

Agora, você começa a perceber que o enunciado deve ser verdadeiro e como pode prová-lo.

Encontrando Provas

A seguir, tente encontrar um **contra-exemplo**, ou seja, um grafo no qual a soma seja um número ímpar.

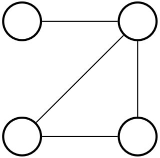


$soma = 8$

Agora, você começa a perceber que o enunciado deve ser verdadeiro e como pode prová-lo.

Encontrando Provas

A seguir, tente encontrar um **contra-exemplo**, ou seja, um grafo no qual a soma seja um número ímpar.



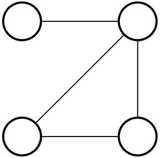
$soma = 8$

Toda vez que uma aresta é adicionada, a soma de graus aumenta de dois.

Agora, você começa a perceber que o enunciado deve ser verdadeiro e como pode prová-lo.

Encontrando Provas

A seguir, tente encontrar um **contra-exemplo**, ou seja, um grafo no qual a soma seja um número ímpar.



$soma = 8$

Toda vez que uma aresta é adicionada, a soma de graus aumenta de dois.

Agora, você começa a perceber que o enunciado deve ser verdadeiro e como pode prová-lo.

Encontrando Provas

Teorema

Para todo grafo G, a soma dos graus dos nós em G é um número par.

Prova

Toda aresta em G está conectada a dois nós.

Cada aresta contribui com 01 para o grau de cada nó ao qual ela está conectada.

Portanto, cada aresta contribui com 02 para a soma dos graus de todos os nós.

Logo, se G contém e arestas, então a soma dos graus de todos os nós de G é $2e$ – que é um número par.

Encontrando Provas

Teorema

Para todo grafo G, a soma dos graus dos nós em G é um número par.

Prova

Toda aresta em G está conectada a dois nós.

Cada aresta contribui com 01 para o grau de cada nó ao qual ela está conectada.

Portanto, cada aresta contribui com 02 para a soma dos graus de todos os nós.

Logo, se G contém e arestas, então a soma dos graus de todos os nós de G é $2e$ – que é um número par.

Encontrando Provas

Teorema

Para todo grafo G, a soma dos graus dos nós em G é um número par.

Prova

Toda aresta em G está conectada a dois nós.

Cada aresta contribui com 01 para o grau de cada nó ao qual ela está conectada.

Portanto, cada aresta contribui com 02 para a soma dos graus de todos os nós.

Logo, se G contém e arestas, então a soma dos graus de todos os nós de G é $2e$ – que é um número par.

Encontrando Provas

Teorema

Para todo grafo G, a soma dos graus dos nós em G é um número par.

Prova

Toda aresta em G está conectada a dois nós.

Cada aresta contribui com 01 para o grau de cada nó ao qual ela está conectada.

Portanto, cada aresta contribui com 02 para a soma dos graus de todos os nós.

Logo, se G contém e arestas, então a soma dos graus de todos os nós de G é $2e$ – que é um número par.

Encontrando Provas

Teorema

Para todo grafo G, a soma dos graus dos nós em G é um número par.

Prova

Toda aresta em G está conectada a dois nós.

Cada aresta contribui com 01 para o grau de cada nó ao qual ela está conectada.

Portanto, cada aresta contribui com 02 para a soma dos graus de todos os nós.

Logo, se G contém e arestas, então a soma dos graus de todos os nós de G é $2e$ – que é um número par.

Encontrando Provas

Tipos de Prova

- Prova por construção;
- Prova por contradição;
- Prova por indução;
- ...

Prova por Construção

Prova por Construção

Muitos teoremas enunciam que um tipo particular de objeto existe. Uma maneira de provar um desses teoremas é demonstrar como construir o objeto – técnica conhecida como **prova por construção**.

$\Rightarrow$ Exemplo de prova por construção

Definição

Definimos um grafo como k-**regular** se todo nó do grafo tem grau k.

Teorema

Para cada número par n maior que 2, existe um grafo 3-**regular** com n nós.

Prova por Construção

$\Rightarrow$ Exemplo de prova por construção (cont.)

Prova

Seja n um número par maior que 2. Construa o grafo $G = (V, E)$ com n nós da seguinte forma.

O conj. de nós de G é $V = \{0, 1, \ldots, n-1\}$ e o conj. de arestas de G é

$$E = \{[i, i+1] \mid 0 \leq i \leq n-2\} \cup \{[n-1, 0]\}$$

$$\cup \{[i, i+n/2] \mid 0 \leq i \leq n/2 - 1\}.$$

Verifique a construção desenhando os nós desse grafo consecutivamente ao redor da circunferência de um círculo. As arestas definidas na 1^a linha ligam pares adjacentes ao longo do círculo, já as descritas na 2^a linha ligam nós em lados opostos do círculo.

Prova por Construção

$\Rightarrow$ Exemplo de prova por construção (cont.)

Prova

Seja n um número par maior que 2. Construa o grafo $G = (V, E)$ com n nós da seguinte forma.

O conj. de nós de G é $V = \{0, 1, \ldots, n-1\}$ e o conj. de arestas de G é

$$E = \{[i, i+1] \mid 0 \leq i \leq n-2\} \cup \{[n-1, 0]\}$$

$$\cup \{[i, i+n/2] \mid 0 \leq i \leq n/2-1\}.$$

Verifique a construção desenhando os nós desse grafo consecutivamente ao redor da circunferência de um círculo. As arestas definidas na 1^a linha ligam pares adjacentes ao longo do círculo, já as descritas na 2^a linha ligam nós em lados opostos do círculo.

Prova por Construção

⇒ Exemplo de prova por construção (cont.)

Prova

Seja n um número par maior que 2. Construa o grafo $G = (V, E)$ com n nós da seguinte forma.

O conj. de nós de G é $V = \{0, 1, \ldots, n-1\}$ e o conj. de arestas de G é

$$E = \{[i, i+1] \mid 0 \leq i \leq n-2\} \cup \{[n-1, 0]\}$$

$$\cup\{[i, i+n/2] \mid 0 \leq i \leq n/2 - 1\}.$$

Verifique a construção desenhando os nós desse grafo consecutivamente ao redor da circunferência de um círculo. As arestas definidas na 1^a linha ligam pares adjacentes ao longo do círculo, já as descritas na 2^a linha ligam nós em lados opostos do círculo.

Prova por Construção

$\Rightarrow$ Exemplo de prova por construção (cont.)

Prova

Seja n um número par maior que 2. Construa o grafo $G = (V, E)$ com n nós da seguinte forma.

O conj. de nós de G é $V = \{0, 1, \ldots, n-1\}$ e o conj. de arestas de G é

$$E = \{[i, i+1] \mid 0 \leq i \leq n-2\} \cup \{[n-1, 0]\}$$

$$\cup\{[i, i+n/2] \mid 0 \leq i \leq n/2-1\}.$$

Verifique a construção desenhando os nós desse grafo consecutivamente ao redor da circunferência de um círculo. As arestas definidas na 1^a linha ligam pares adjacentes ao longo do círculo, já as descritas na 2^a linha ligam nós em lados opostos do círculo.

Prova por Contradição

Prova por Contradição

Em uma forma comum de argumento para se provar um teorema, assumimos que o teorema é falso e, em seguida, mostramos que essa suposição leva a uma consequência obviamente falsa – chamada **contradição**.

$\Rightarrow$ Exemplo de prova por contradição (frequente no cotidiano)

Prova

Pedro vê Ana que acaba de chegar da rua.

Observando que ela está completamente enxuta, ele conclui que não está chovendo.

Sua "prova" de que não está chovendo é que, **se estivesse chovendo** (a suposição de que o enunciado é falso), **Ana estaria molhada** (a consequência, obviamente falsa).

Portanto, não pode estar chovendo.

Prova por Contradição

Prova por Contradição

Em uma forma comum de argumento para se provar um teorema, assumimos que o teorema é falso e, em seguida, mostramos que essa suposição leva a uma consequência obviamente falsa – chamada **contradição**.

$\Rightarrow$ Exemplo de prova por contradição (frequente no cotidiano)

Prova

Pedro vê Ana que acaba de chegar da rua.

Observando que ela está completamente enxuta, ele conclui que não está chovendo.

Sua "prova" de que não está chovendo é que, **se estivesse chovendo** (a suposição de que o enunciado é falso), **Ana estaria molhada** (a consequência, obviamente falsa).

Portanto, não pode estar chovendo.

Prova por Contradição

Prova por Contradição

Em uma forma comum de argumento para se provar um teorema, assumimos que o teorema é falso e, em seguida, mostramos que essa suposição leva a uma consequência obviamente falsa – chamada **contradição**.

$\Rightarrow$ Exemplo de prova por contradição (frequente no cotidiano)

Prova

Pedro vê Ana que acaba de chegar da rua.

Observando que ela está completamente enxuta, ele conclui que não está chovendo.

Sua “prova” de que não está chovendo é que, **se estivesse chovendo** (a suposição de que o enunciado é falso), **Ana estaria molhada** (a consequência, obviamente falsa).

Portanto, não pode estar chovendo.

Prova por Contradição

Prova por Contradição

Em uma forma comum de argumento para se provar um teorema, assumimos que o teorema é falso e, em seguida, mostramos que essa suposição leva a uma consequência obviamente falsa – chamada **contradição**.

$\Rightarrow$ Exemplo de prova por contradição (frequente no cotidiano)

Prova

Pedro vê Ana que acaba de chegar da rua.

Observando que ela está completamente enxuta, ele conclui que não está chovendo.

Sua "prova" de que não está chovendo é que, **se estivesse chovendo** (a suposição de que o enunciado é falso), **Ana estaria molhada** (a consequência, obviamente falsa).

Portanto, não pode estar chovendo.

Prova por Contradição

Prova por Contradição

Em uma forma comum de argumento para se provar um teorema, assumimos que o teorema é falso e, em seguida, mostramos que essa suposição leva a uma consequência obviamente falsa – chamada **contradição**.

$\Rightarrow$ Exemplo de prova por contradição (frequente no cotidiano)

Prova

Pedro vê Ana que acaba de chegar da rua.

Observando que ela está completamente enxuta, ele conclui que não está chovendo.

Sua "prova" de que não está chovendo é que, **se estivesse chovendo** (a suposição de que o enunciado é falso), **Ana estaria molhada** (a consequência, obviamente falsa).

Portanto, não pode estar chovendo.

Prova por Contradição

⇒ Outro exemplo de prova por contradição

Definição

Um número racional r é igual a razão de dois inteiros m e n, isto é, $r = m/n$.

Teorema

$\sqrt{2}$ é irracional.

Prova

Suponha que $\sqrt{2}$ é racional. Logo, $\sqrt{2} = \frac{m}{n}$ em que ambos, m e n, são inteiros.

Se ambos m e n são divisíveis pelo mesmo inteiro maior que um, divida ambos por esse inteiro. Isso não muda o valor da fração, contudo, pelo menos um, dentre m e n, não é um número par.

Multiplicando ambos os lados da equação por n e obtemos $n\sqrt{2} = m$.

Prova por Contradição

$\Rightarrow$ Outro exemplo de prova por contradição

Definição

Um número racional r é igual a razão de dois inteiros m e n, isto é, $r = m/n$.

Teorema

$\sqrt{2}$ é irracional.

Prova

Suponha que $\sqrt{2}$ é racional. Logo, $\sqrt{2} = \frac{m}{n}$ em que ambos, m e n, são inteiros.

Se ambos m e n são divisíveis pelo mesmo inteiro maior que um, divida ambos por esse inteiro. Isso não muda o valor da fração, contudo, pelo menos um, dentre m e n, não é um número par.

Multiplicando ambos os lados da equação por n e obtemos $n\sqrt{2} = m$.

Prova por Contradição

$\Rightarrow$ Outro exemplo de prova por contradição

Definição

Um número racional r é igual a razão de dois inteiros m e n, isto é, $r = m/n$.

Teorema

$\sqrt{2}$ é irracional.

Prova

Suponha que $\sqrt{2}$ é racional. Logo, $\sqrt{2} = \frac{m}{n}$ em que ambos, m e n, são inteiros.

Se ambos m e n são divisíveis pelo mesmo inteiro maior que um, divida ambos por esse inteiro. Isso não muda o valor da fração, contudo, pelo menos um, dentre m e n, não é um número par.

Multiplicando ambos os lados da equação por n e obtemos $n\sqrt{2} = m$.

Prova por Contradição

$\Rightarrow$ Outro exemplo de prova por contradição

Definição

Um número racional r é igual a razão de dois inteiros m e n, isto é, $r = m/n$.

Teorema

$\sqrt{2}$ é irracional.

Prova

Suponha que $\sqrt{2}$ é racional. Logo, $\sqrt{2} = \frac{m}{n}$ em que ambos, m e n, são inteiros.

Se ambos m e n são divisíveis pelo mesmo inteiro maior que um, divida ambos por esse inteiro. Isso não muda o valor da fração, contudo, pelo menos um, dentre m e n, não é um número par.

Multiplicando ambos os lados da equação por n e obtemos $n\sqrt{2} = m$.

Prova por Contradição

$\Rightarrow$ Outro exemplo de prova por contradição (cont.)

Prova (cont.)

Elevamos ao quadrado ambos os lados e teremos $2n^2 = m^2$.

Em virtude de m^2 ser 2 vezes o inteiro n^2, sabemos que m^2 é par. Logo, m também é par, pois o quadrado de um número ímpar é sempre ímpar.

Portanto, podemos escrever $m = 2k$ para algum inteiro k. Substituindo m por $2k$, obtemos $2n^2 = m^2 = (2k)^2 = 4k^2$.

Dividindo ambos os lados por 2 obtemos $n^2 = 2k^2$.

Porém, esse resultado mostra que n^2 é par e, assim, n é par. Dessa forma, estabelecemos que tanto m quanto n são pares.

Mas tínhamos reduzido m e n de forma que eles não fossem ambos pares. Isso é uma contradição (ou absurdo). Logo, a suposição inicial é falsa, ou ainda, $\sqrt{2}$ não é racional.

Prova por Contradição

$\Rightarrow$ Outro exemplo de prova por contradição (cont.)

Prova (cont.)

Elevamos ao quadrado ambos os lados e teremos $2n^2 = m^2$.

Em virtude de m^2 ser 2 vezes o inteiro n^2, sabemos que m^2 é par. Logo, m também é par, pois o quadrado de um número ímpar é sempre ímpar.

Portanto, podemos escrever $m = 2k$ para algum inteiro k. Substituindo m por $2k$, obtemos $2n^2 = m^2 = (2k)^2 = 4k^2$.

Dividindo ambos os lados por 2 obtemos $n^2 = 2k^2$.

Porém, esse resultado mostra que n^2 é par e, assim, n é par. Dessa forma, estabelecemos que tanto m quanto n são pares.

Mas tínhamos reduzido m e n de forma que eles não fossem ambos pares. Isso é uma contradição (ou absurdo). Logo, a suposição inicial é falsa, ou ainda, $\sqrt{2}$ não é racional.

Prova por Contradição

⇒ Outro exemplo de prova por contradição (cont.)

Prova (cont.)

Elevamos ao quadrado ambos os lados e teremos $2n^2 = m^2$.

Em virtude de m^2 ser 2 vezes o inteiro n^2, sabemos que m^2 é par. Logo, m também é par, pois o quadrado de um número ímpar é sempre ímpar.

Portanto, podemos escrever $m = 2k$ para algum inteiro k. Substituindo m por $2k$, obtemos $2n^2 = m^2 = (2k)^2 = 4k^2$.

Dividindo ambos os lados por 2 obtemos $n^2 = 2k^2$.

Porém, esse resultado mostra que n^2 é par e, assim, n é par. Dessa forma, estabelecemos que tanto m quanto n são pares.

Mas tínhamos reduzido m e n de forma que eles não fossem ambos pares. Isso é uma contradição (ou absurdo). Logo, a suposição inicial é falsa, ou ainda, $\sqrt{2}$ não é racional.

Prova por Contradição

$\Rightarrow$ Outro exemplo de prova por contradição (cont.)

Prova (cont.)

Elevamos ao quadrado ambos os lados e teremos $2n^2 = m^2$.

Em virtude de m^2 ser 2 vezes o inteiro n^2, sabemos que m^2 é par. Logo, m também é par, pois o quadrado de um número ímpar é sempre ímpar.

Portanto, podemos escrever $m = 2k$ para algum inteiro k. Substituindo m por $2k$, obtemos $2n^2 = m^2 = (2k)^2 = 4k^2$.

Dividindo ambos os lados por 2 obtemos $n^2 = 2k^2$.

Porém, esse resultado mostra que n^2 é par e, assim, n é par. Dessa forma, estabelecemos que tanto m quanto n são pares.

Mas tínhamos reduzido m e n de forma que eles não fossem ambos pares. Isso é uma contradição (ou absurdo). Logo, a suposição inicial é falsa, ou ainda, $\sqrt{2}$ não é racional.

Prova por Contradição

⇒ Outro exemplo de prova por contradição (cont.)

Prova (cont.)

Elevamos ao quadrado ambos os lados e teremos $2n^2 = m^2$.

Em virtude de m^2 ser 2 vezes o inteiro n^2, sabemos que m^2 é par. Logo, m também é par, pois o quadrado de um número ímpar é sempre ímpar.

Portanto, podemos escrever $m = 2k$ para algum inteiro k. Substituindo m por $2k$, obtemos $2n^2 = m^2 = (2k)^2 = 4k^2$.

Dividindo ambos os lados por 2 obtemos $n^2 = 2k^2$.

Porém, esse resultado mostra que n^2 é par e, assim, n é par. Dessa forma, estabelecemos que tanto m quanto n são pares.

Mas tínhamos reduzido m e n de forma que eles não fossem ambos pares. Isso é uma contradição (ou absurdo). Logo, a suposição inicial é falsa, ou ainda, $\sqrt{2}$ não é racional.

Prova por Contradição

$\Rightarrow$ Outro exemplo de prova por contradição (cont.)

Prova (cont.)

Elevamos ao quadrado ambos os lados e teremos $2n^2 = m^2$.

Em virtude de m^2 ser 2 vezes o inteiro n^2, sabemos que m^2 é par. Logo, m também é par, pois o quadrado de um número ímpar é sempre ímpar.

Portanto, podemos escrever $m = 2k$ para algum inteiro k. Substituindo m por $2k$, obtemos $2n^2 = m^2 = (2k)^2 = 4k^2$.

Dividindo ambos os lados por 2 obtemos $n^2 = 2k^2$.

Porém, esse resultado mostra que n^2 é par e, assim, n é par. Dessa forma, estabelecemos que tanto m quanto n são pares.

Mas tínhamos reduzido m e n de forma que eles não fossem ambos pares. Isso é uma contradição (ou absurdo). Logo, a suposição inicial é falsa, ou ainda, $\sqrt{2}$ não é racional.

Prova por Contradição

⇒ Outro exemplo de prova por contradição (cont.)

Prova (cont.)

Elevamos ao quadrado ambos os lados e teremos $2n^2 = m^2$.

Em virtude de m^2 ser 2 vezes o inteiro n^2, sabemos que m^2 é par. Logo, m também é par, pois o quadrado de um número ímpar é sempre ímpar.

Portanto, podemos escrever $m = 2k$ para algum inteiro k. Substituindo m por $2k$, obtemos $2n^2 = m^2 = (2k)^2 = 4k^2$.

Dividindo ambos os lados por 2 obtemos $n^2 = 2k^2$.

Porém, esse resultado mostra que n^2 é par e, assim, n é par. Dessa forma, estabelecemos que tanto m quanto n são pares.

Mas tínhamos reduzido m e n de forma que eles não fossem ambos pares. Isso é uma contradição (ou absurdo). Logo, a suposição inicial é falsa, ou ainda, $\sqrt{2}$ não é racional.

Prova por Indução

Princípio de Indução Matemática

Seja uma propriedade P sobre os números naturais. Então, caso

- P se verifique para o número 0, e
- para um número natural n, se P se verifica para n, então P se verifica para $n + 1$,

pode-se concluir que P se verifica para todo número natural.

Passos para provar por indução sobre $n \in \mathbb{N}$

1. **base da indução:** provar que P se verifica para o número zero;
2. **hipótese de indução:** supor que P se verifica para n, em que n representa um número natural arbitrário; e
3. **passo indutivo:** provar que P se verifica para $n + 1$.

Prova por Indução

$\Rightarrow$ Exemplo de prova por indução

Teorema

Para todo $n \in \mathbb{N}, \sum_{k=0}^{n} k = n(n+1)/2$.

Prova

Base: Inicialmente, veja que $\sum_{k=0}^{0} k = 0(0+1)/2 = 0$.

Hipótese de indução: Suponha que $\sum_{k=0}^{n} k = n(n+1)/2$ para um n arbitrário.

Passo indutivo: Basta provar que $\sum_{k=0}^{n+1} k = (n+1)(n+2)/2$.

Temos que $\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = n(n+1)/2 + (n+1)$ (hipótese indução).

Daí, temos que:

$n(n+1)/2 + (n+1) = [n(n+1) + 2(n+1)]/2 = (n^2 + 3n + 2)/2 = (n+1)(n+2)/2$.

Logo, pelo princípio da indução, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova por Indução

⇒ Exemplo de prova por indução

Teorema

Para todo $n \in \mathbb{N}, \sum_{k=0}^{n} k = n(n+1)/2$.

Prova

Base: Inicialmente, veja que $\sum_{k=0}^{0} k = 0(0+1)/2 = 0$.

Hipótese de indução: Suponha que $\sum_{k=0}^{n} k = n(n+1)/2$ para um n arbitrário.

Passo indutivo: Basta provar que $\sum_{k=0}^{n+1} k = (n+1)(n+2)/2$.

Temos que $\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = n(n+1)/2 + (n+1)$ (hipótese indução).

Daí, temos que:

$n(n+1)/2 + (n+1) = [n(n+1) + 2(n+1)]/2 = (n^2 + 3n + 2)/2 = (n+1)(n+2)/2.$

Logo, pelo princípio da indução, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova por Indução

⇒ Exemplo de prova por indução

Teorema

Para todo $n \in \mathbb{N}$, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova

Base: Inicialmente, veja que $\sum_{k=0}^{0} k = 0(0+1)/2 = 0$.

Hipótese de indução: Suponha que $\sum_{k=0}^{n} k = n(n+1)/2$ para um n arbitrário.

Passo indutivo: Basta provar que $\sum_{k=0}^{n+1} k = (n+1)(n+2)/2$.

Temos que $\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = n(n+1)/2 + (n+1)$ (hipótese indução).

Daí, temos que:

$n(n+1)/2 + (n+1) = [n(n+1) + 2(n+1)]/2 = (n^2 + 3n + 2)/2 = (n+1)(n+2)/2$.

Logo, pelo princípio da indução, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova por Indução

⇒ Exemplo de prova por indução

Teorema

Para todo $n \in \mathbb{N}$, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova

Base: Inicialmente, veja que $\sum_{k=0}^{0} k = 0(0+1)/2 = 0$.

Hipótese de indução: Suponha que $\sum_{k=0}^{n} k = n(n+1)/2$ para um n arbitrário.

Passo indutivo: Basta provar que $\sum_{k=0}^{n+1} k = (n+1)(n+2)/2$.

Temos que $\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = n(n+1)/2 + (n+1)$ (hipótese indução).

Daí, temos que:

$n(n+1)/2 + (n+1) = [n(n+1) + 2(n+1)]/2 = (n^2 + 3n + 2)/2 = (n+1)(n+2)/2$.

Logo, pelo princípio da indução, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova por Indução

⇒ Exemplo de prova por indução

Teorema

Para todo $n \in \mathbb{N}$, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova

Base: Inicialmente, veja que $\sum_{k=0}^{0} k = 0(0+1)/2 = 0$.

Hipótese de indução: Suponha que $\sum_{k=0}^{n} k = n(n+1)/2$ para um n arbitrário.

Passo indutivo: Basta provar que $\sum_{k=0}^{n+1} k = (n+1)(n+2)/2$.

Temos que $\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = n(n+1)/2 + (n+1)$ (hipótese indução).

Daí, temos que:

$n(n+1)/2 + (n+1) = [n(n+1) + 2(n+1)]/2 = (n^2 + 3n + 2)/2 = (n+1)(n+2)/2.$

Logo, pelo princípio da indução, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova por Indução

$\Rightarrow$ Exemplo de prova por indução

Teorema

Para todo $n \in \mathbb{N}$, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova

Base: Inicialmente, veja que $\sum_{k=0}^{0} k = 0(0+1)/2 = 0$.

Hipótese de indução: Suponha que $\sum_{k=0}^{n} k = n(n+1)/2$ para um n arbitrário.

Passo indutivo: Basta provar que $\sum_{k=0}^{n+1} k = (n+1)(n+2)/2$.

Temos que $\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = n(n+1)/2 + (n+1)$ (hipótese indução).

Daí, temos que:

$n(n+1)/2 + (n+1) = [n(n+1) + 2(n+1)]/2 = (n^2 + 3n + 2)/2 = (n+1)(n+2)/2$.

Logo, pelo princípio da indução, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova por Indução

⇒ Exemplo de prova por indução

Teorema

Para todo $n \in \mathbb{N}$, $\sum_{k=0}^{n} k = n(n+1)/2$.

Prova

Base: Inicialmente, veja que $\sum_{k=0}^{0} k = 0(0+1)/2 = 0$.

Hipótese de indução: Suponha que $\sum_{k=0}^{n} k = n(n+1)/2$ para um n arbitrário.

Passo indutivo: Basta provar que $\sum_{k=0}^{n+1} k = (n+1)(n+2)/2$.

Temos que $\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + (n+1) = n(n+1)/2 + (n+1)$ (hipótese indução).

Daí, temos que:

$n(n+1)/2 + (n+1) = [n(n+1) + 2(n+1)]/2 = (n^2 + 3n + 2)/2 = (n+1)(n+2)/2$.

Logo, pelo princípio da indução, $\sum_{k=0}^{n} k = n(n+1)/2$.