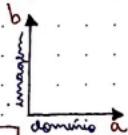


Relações

- definição \rightarrow como elementos de dois conjuntos se relacionam
- como representar essa relação? pares ordenados
 - $(a, b), (c, d), (e, f) \dots$
- escrita matemática \rightarrow uma relação é representada pelo conjunto $R = \{(a, b) \in \mathbb{Z} \times \mathbb{N} : \text{relação}\}$
- relação R de A para B é um subconjunto de $A \times B$
 - $A = B \rightarrow R$ é uma relação em A .
- domínio de uma relação $\rightarrow \text{dom}(R) = \{a \in A : \exists b \in B \ (a, b) \in R\}$
- imagem de uma relação $\rightarrow \text{img}(R) = \{b \in B : \exists a \in A \ (a, b) \in R\}$
- relação inversa \rightarrow para qualquer relação $R \subseteq A \times B$, $R^{-1} = \{(b, a) \in B \times A : (a, b) \in R\}$
 - exemplo da inversa da inversa $\rightarrow (R^{-1})^{-1} = R$
 \hookrightarrow por definição, $(a, b) \in R \Leftrightarrow (b, a) \in R^{-1} \Leftrightarrow (a, b) \in (R^{-1})^{-1}$
- composição de relações
 - se $R \subseteq A \times B \ \& \ S \subseteq B \times C$, pergunta-se que, indiretamente, $A \times C$ possuem alguma relação?
 - $S \circ R = \{(a, c) \in A \times C : \exists (a, b) \in R \wedge \exists (b, c) \in S\}$
 - \downarrow calculava com o domínio
 - \downarrow calculava com a imagem
- exemplo de composição de relações
 - opm $R + S$ relações em \mathbb{Z} definidas como $a R b \Leftrightarrow b = 3a$ e $a S b \Leftrightarrow b = a + 5$. Como será $S \circ R$?
nos temos que $(a, b) \in S \circ R$, sendo $a \in A \wedge b \in B \wedge c \in C$
Portanto, $(a, c) \in S \circ R \Leftrightarrow \exists b \in B \ (b = 3a \wedge b = a + 5) \ \wedge c = b$
 \hookrightarrow logo, $S \circ R = \{(a, c) \in \mathbb{Z} \times \mathbb{Z} : c = 3a + 5\}$
- relação identidade $\rightarrow I_A = \{(a, a) : a \in A\}$ \rightarrow notamos que compõe com a identidade não muda a relação. (Ex: se $R \subseteq A \times B$, então $R \circ I_A = I_B \circ R = R$)
 - porém $R \circ R \neq R \circ R^{-1} \neq I_A$



relação de ordem

- definição $\rightarrow R \subseteq A \times A$ é uma relação de ordem se...

1. reflexiva $\rightarrow \forall x \in A, (x,x) \in R$

2. antisimétrica $\rightarrow \forall (x,y) \in A, \text{ se } (x,y) \in R \wedge (y,x) \in R, \text{ então } x=y$

3. transitiva $\rightarrow \forall (x,y,z) \in A, \text{ se } (x,y) \in R \wedge (y,z) \in R, \text{ então } (x,z) \in R$

- neste caso, dizemos que A é um conjunto ordenado

- exemplo 1 \rightarrow relação "é subconjunto"

- seja $B = \{0, 1, 2\}$ e considere o conjunto das partes de B , isto é: $P(B) = \{X : X \subseteq B\}$

- então temos a seguinte relação em $P(B)$ $\rightarrow R = \{(x,y) \in P(B) \times P(B) : x \subseteq y\}$

- reflexividade \rightarrow como $X \subseteq X$ para qualquer subconjunto, temos que $(X,X) \in R$

- antisimétrica \rightarrow Para que $X \subseteq Y \wedge Y \subseteq X$, temos que $X=Y$

- transitiva \rightarrow se $X \subseteq Y \wedge Y \subseteq Z$, temos que $X \subseteq Z$

- diagrama de Hasse

- cada elemento do dom(R) é um nó

- arestas entre nós a e b indicam que $(a,b) \in R$

- elementos "mais" altos \rightarrow se $(a,b) \in R$, a é o alto de b

- ignoramos a reflexividade

- ignoramos a transitividade \rightarrow desenharmos arestas entre nós a e b e ignorarmos que exista $(c,b) \in R$

- relação total \rightarrow diagrama possui uma única ramificação, ou seja, todos os elementos são comparáveis entre si

• $\boxed{\forall (a,b) \in A \times A, \text{ temos que } (a,b) \in R \vee (b,a) \in R}$

- mínimo \rightarrow $a \in A$ tal que $a <^{\text{definição}}$ menor que todos os outros elementos (ele é único)

• $a = \text{mínimo}_R(A) \Leftrightarrow a \in A \wedge (\forall b \in A \setminus \{a\} (a, b) \in R)$

- minimal \rightarrow $a \in A$ tal que nenhum outro elemento é menor que a

• $\{a = \text{mínimo}_R(A) \Leftrightarrow a \in A \wedge (\nexists b \in A \setminus \{a\} (b, a) \in R)\}$

- máximo \rightarrow maior que todos os outros elementos

- maximal \rightarrow não existe um elemento maior na relação que ele participe

princípio da boa ordenação (PBO)

- ideia principal \rightarrow se $A \subseteq \mathbb{N}$ e $A \neq \emptyset$, então \exists mínimo (A)

o princípio da indução matemática

$$\bullet \text{ PIM} \Rightarrow \text{PBO}$$

• caso base $\rightarrow |A| = 1$, então $A = \{a\}$, e $a = \text{mínimo } (A)$. Logo, P(1) é válido

• hipótese indutiva $\rightarrow \exists k > 1$, tal que, se $|A| = k$, \exists mínimo (A)

• passo indutivo $\rightarrow |A| = k+1$

pelo caso base, temos que $\{a\} = 1$. Assim, $|A| = X \cup \{a\} = |X| + 1$

$\Rightarrow \exists m = \min(X)$. Assim, se $m < a$, $m = \min(A)$. Se $a < m$, $a = \min(A)$

- PBO \Leftrightarrow PIM \Leftrightarrow PIC \rightarrow os princípios são equivalentes e podem ser usados como axiomas.

- PBO na evitação de absurdos/contradição

1. definição de um conjunto S

2. visando uma contradição, assumimos $S \neq \emptyset$

3. por PBO, $\exists m = \text{mínimo } (S)$ (notar que $\exists x \in S$ tal que $x < m$)

4. agora, tentamos encontrar contradição (ou, partindo de $m-1 \notin S$, $m \notin S$)

- exemplo \rightarrow provar que $\forall n \in \mathbb{N}, \sum_{i=0}^n i = \frac{n(n+1)}{2}$

• seja $P(n) \Leftrightarrow \left(\sum_{i=0}^n i = \frac{n(n+1)}{2} \right)$. Seja $S = \{n \in \mathbb{N} : \neg P(n)\}$. Visando um absurdo, temos $S \neq \emptyset$

Logo PBO, temos que $\exists m = \text{mínimo } (S)$

Vemos que, para $n=0$, $\sum_{i=0}^0 i = 0$ e $\frac{0(0+1)}{2} = 0$. Logo, $P(0)$ vale. Então, $0 \notin S$.

Então, se $0 \notin S$, $m \geq 1$. Logo, $m-1 \in \mathbb{N}$. Como $m-1 < m$, $m = \text{mínimo } (S)$, $m-1 \notin S$.

Logo, necessariamente, $P(m-1)$ precisa valer. Assim, temos: $\sum_{i=0}^{m-1} i = \frac{(m-1)m}{2} = \frac{(m-1)(m-1+1)}{2}$

Somando m nos dois lados, $\sum_{i=0}^m i = m \left(\frac{m+m-1}{2} \right) = m \left(\frac{m+1}{2} \right)$

Portanto, $\forall n \in \mathbb{N}, \sum_{i=0}^n i = \frac{n(n+1)}{2}$

Ou seja $P(m)$ vale e m não pode pertencer a S , sendo $S = \emptyset$

relações de equivalência

→ matemática → às vezes, nós estamos interessados em classes de elementos que satisfazem uma propriedade

→ definição → se quisermos uma relação (binária) E que satisfaça a igualdade / equivalência precisamos

1. Elemento equivalente a si mesmo → reflexividade → $(x, x) \in E$

2. simetria → $(x, y) \in E \Leftrightarrow (y, x) \in E$

3. transitividade → se x é equivalente a y e y é equivalente a z , então $(x, z) \in E$

↳ nos permite agrupar os elementos em conjuntos / classes de equivalência

$$[X]_R = \{y \in A : x \text{ se relaciona com } y\}$$

• pela reflexividade, nenhuma classe de equivalência é vazia → ao menos $x \in [X]_R$

→ classe de equivalência → elementos que possuem algo em comum e são agrupados

• conjunto de todos as classes de equivalência → $A/R = \{[x]_R : x \in A\}$

• exemplo → sendo $R_k = \{\text{pessoas que compartilham idade } k\}$, $A/R = \{P_1, P_2, \dots, P_n\}$

→ exemplo 1 → considere a relação $R = \{(x, y) \in A \times R : x - y \in \mathbb{Z}\}$. Mostre que é uma RE.

• reflexividade → $x - x = 0 \in \mathbb{Z}$

• simétrica → $x - y \in \mathbb{Z} \Rightarrow y - x \in \mathbb{Z} \Rightarrow (y, x) \in R$

• transitiva → se $x - y \in \mathbb{Z}$ e $y - z \in \mathbb{Z}$, temos que $x = y + \text{número inteiro}$ e $y = z + \text{número inteiro}$
Logo, $x = (z + \text{nº}) + \text{nº}$. Portanto, $x - z \in \mathbb{Z} \Rightarrow (x, z) \in R$

→ classes de equivalência

• em geral, qualquer número real x pode ser escrito como $x = z + d$, sendo $\begin{cases} z \in \mathbb{Z} \\ d = x - z, d \in [0, 1[\end{cases}$

• então, $x \equiv y$ se x e y têm a mesma parte decimal ($x = z + d$ e $y = z' + d$)

• dessa forma, as classes de equivalência são, para todo $d \in [0, 1[$, $E_d = \{nº \text{ com decimal } d\}$

• logo, $A/R = \{E_d : d \in [0, 1[\}$

relações de equivalência

- algumas propriedades das classes de equivalência

1. a classe é independente do seu representante
2. duas classes são iguais se totalmente diferentes

3. A/R é uma partição de A $\left\{ \begin{array}{l} \bigcup_{x \in A/R} X = A \\ (\forall x, y \in A) \wedge x \neq y \Rightarrow x \cap y = \emptyset \end{array} \right.$

4. Se A é finito, $A/R = \{x_1, x_2, \dots, x_n\}$

construindo conjuntos a partir de relações de equivalência

- construção dos racionais

- define a seguinte relação sobre $\mathbb{Z} \times \mathbb{Z}^*$: $R = \{(a,b), (c,d) \in A \times A : ad = bc\}$

- podemos ver que R é uma relação de equivalência

| |
|---|
| $a/b = c/d$ (necessidade) $ad = bc \Leftrightarrow cb = da$ $\text{se } ad = bc \text{ e } cf = de, \frac{a}{b} = \frac{c}{f} = \frac{e}{d}$ $\therefore a/b = c/d \Rightarrow (a,b) \equiv (c,d)$ |
|---|

- operação para a conjunto de equivalência $B = A/R = \{[(a,b)]_R : (a,b) \in A\}$

- soma $\rightarrow [(a,b)]_R + [(c,d)]_R = [(ad+bc, bd)]_R$

- produto $\rightarrow [(a,b)]_R \cdot [(c,d)]_R = [(ac, bd)]_R$

- subtração $\rightarrow = [(a,b)]_R + [(-1,1)]_R - [(c,d)]_R$

- divisão $\rightarrow = [(a,b)]_R \cdot [(d,c)]_R$

multiplicação de classes de equivalência

- lembrando a definição $\rightarrow [(a,b)]_R \cdot [(c,d)]_R = [(ac, bd)]_R$

- como $b, d \in \mathbb{Z}^*, bd \neq 0$. logo, $(ac, bd) \in A \Rightarrow [(ac, bd)]_R$ é uma classe de equivalência válida
- se $(a,b) \equiv (x,y)$, e $(c,d) \equiv (w,z)$, mostraremos que $(a,b) \cdot (c,d) \equiv (x,y) \cdot (w,z)$, podemos finalmente dizer que $\mathbb{Q} = A/R$

o conjunto dos inteiros módulo n via relações de equivalência

- operações modulares e relações de equivalência

$$\bullet R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : n \mid (a - b)\} = [a]_n = a \equiv b \pmod{n}$$

- teorema \rightarrow para todo natural $n \geq 2$ e inteiros a, b , temos que $a \equiv b \pmod{n}$ se, e somente se, o resto da divisão de a por n é igual ao resto da divisão de b por n .

- exemplo $\rightarrow n=3$

- o resto pode ser 0, 1, 2.

$$\bullet [0]_3 = \{-6, -3, 0, 3, 6, \dots\} = 3\mathbb{Z}$$

$$\bullet [2]_3 = \{-7, -4, -1, 2, 5, 8, \dots\} = 3\mathbb{Z} + 2$$

$$\bullet [1]_3 = \{-5, -2, 1, 4, 7, \dots\} = 3\mathbb{Z} + 1$$

• os quocientes de \mathbb{Z} por esta relação é: $\mathbb{Z}_3 = \mathbb{Z}/R = \{[0]_3, [1]_3, [2]_3\}$ inteiros módulo n

- operações

$$\bullet \text{ soma} \rightarrow [a]_n + [b]_n = [a+b]_n$$

$$\bullet \text{ produto} \rightarrow [a]_n \cdot [b]_n = [a \cdot b]_n$$

impresso multiplicativo módulo n

- como podemos definir divisão?

$$\bullet a \cdot b \equiv 1 \pmod{n}$$

\hookrightarrow inverso como a^{-1} \rightarrow inverso multiplicativo

$$\bullet \text{ exemplo} \rightarrow n=7$$

$$\begin{cases} a=1 & \rightarrow a^{-1}=1 \\ a=2 & \rightarrow a^{-1}=4 \\ a=3 & \rightarrow a^{-1}=5 \\ a=4 & \rightarrow a^{-1}=2 \end{cases}$$

- teorema \rightarrow se n um inteiro maior ou igual a 2, para todo $x \in \mathbb{Z}$,

$$\bullet \exists x^{-1} \in \mathbb{Z} : x \cdot x^{-1} \equiv 1 \pmod{n} \Leftrightarrow \text{mdc}(x, n) = 1$$

Operações módulo n e soluções de equações

- inteiros módulo n com inverso

- assim como em \mathbb{R}^* , nomeamos o elemento que não tem inverso (multiplicativo) → o zéro.

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : \exists x^{-1} \in \mathbb{Z}_n\}$$

- número divisível → um inteiro X é divisível por n se, e somente se, $X \equiv 0 \pmod{n}$

- para mostrar que uma expressão é divisível por algum número, podemos mapear a expressão em \mathbb{Z}_n e mostrar que ela é igual a zero.
- se uma equação com coeficientes em \mathbb{Z} tem solução inteira, então ela tem solução em \mathbb{Z}_n , para $n \geq 2$.
- contrapositiva → se existe $n \geq 2$ tal que a equação não tem solução em \mathbb{Z}_n , então ela não tem solução inteira.

Funções

- totalidade e funcionalidade → para $R \subseteq X \times Y$...

- relação total → se $\forall x \in X (\exists y \in Y (x, y) \in R)$; logo, dom(R) = X
- relação funcional → se $\forall x \in X (\exists y_1, y_2 \in R) \wedge (x, y_1) \in R \wedge (x, y_2) \in R \Rightarrow y_1 = y_2$
- relação total e funcional → $\forall x \in X (\exists! y \in Y ((x, y) \in R)) \rightarrow f(x) = y$

composição de funções

- teorema de composição de funções

- considere duas funções $f \subseteq X \times Y$ e $g \subseteq Y \times Z \rightarrow$ a composição $g \circ f$ é uma função X para Z

- inversa de uma função → relação inversa

- $f \subseteq X \times Y \Rightarrow f^{-1} = \{(y, x) \in Y \times X : (x, y) \in f\}$.

- atégoria → a inversa de uma função não necessariamente é uma função

- compor com a inversa gera a identidade → seja $f \subseteq X \times Y$, $f^{-1} \circ f = \text{Id}_X$ e $f \circ f^{-1} = \text{Id}_Y$

funções

- função injetora

- para $f \subseteq X \times Y$, $\forall x, x' \in X$ ($f(x) = f(x') \Rightarrow x = x'$) $\rightarrow f^{-1}$ é funcional

- função sobrejetora

- para $f \subseteq X \times Y$, $\forall y \in Y \exists x \in X, f(x) = y$

- $\text{im} (f) = Y \rightarrow f^{-1}$ é total

- bijeção (função invertível)

- uma função é bijetora se for injetora e sobrejetora

- uma função f é bijetora se, e somente se, f^{-1} é uma função

- exemplos de funções

- função piso $\rightarrow x - 1 < \lfloor x \rfloor \leq x$ e $f(x) = \max\{z \in \mathbb{Z} : z \leq x\}$

- função teto $\rightarrow x \leq \lceil x \rceil < x + 1$ e $f(x) = \min\{z \in \mathbb{Z} : x \leq z\}$

bijecões e cardinalidades

- mesma cardinalidade

- para quaisquer conjuntos X e Y , digamos que $|X| = |Y|$ se existe uma função bijetora de X para Y
- cada $x \in X$ se relaciona com um $y \in Y$ e vice-versa (y se relaciona com $x = f^{-1}(y)$)
- $|X| \leq |Y|$ se existe uma função injetora de X para Y
- $|Y| \leq |X|$ se existe uma função sobrejetora de X para Y

- teorema schröder - bernstein

- se A e B são conjuntos tal que $|A| \leq |B|$ e $|B| \leq |A|$, então $|A| = |B|$

- conjuntos finitos

- se X e Y são finitos e ambos tem n elementos, então $X = \{x_1, \dots, x_n\}$ e $Y = \{y_1, \dots, y_n\}$
- $f(x_i) = y_i$ é uma bijeção de X para Y .

Bijesões e cardinalidades

- conjuntos infinitos e conjuntos contáveis

- um conjunto é contável se for finito ou se tiver a mesma cardinalidade que \mathbb{N} .

- conjunto contável = conjunto que pode ser listado

- deixa um elemento, e possível dizer qual é o próximo.

↳ se $a \in A$ e $f(i) = a$, então o próximo elemento depois de a é b , tal que $f(i+1) = b$.

- exemplo de conjunto contável

- seja $f: \mathbb{N} \rightarrow \mathbb{Z}$ tal que $f(x) = \begin{cases} \frac{x}{2}, & se\ x \in \text{par} \\ -\frac{(x+1)}{2}, & se\ x \in \text{ímpar} \end{cases}$
- sejam $x, \hat{x} \in \mathbb{N}$ tais que $f(x) = f(\hat{x})$.

- temos 3 casos diferentes:

1. x, \hat{x} são pares $\Rightarrow f(x) = f(\hat{x}) \Rightarrow \frac{x}{2} = \frac{\hat{x}}{2} \Rightarrow x = \hat{x}$

2. x, \hat{x} são ímpares $\Rightarrow f(x) = f(\hat{x}) \Rightarrow -\frac{(x+1)}{2} = -\frac{(\hat{x}+1)}{2} \Rightarrow x = \hat{x}$

3. paridades diferentes $\Rightarrow f(x) = f(\hat{x}) \Rightarrow \frac{x}{2} = -\frac{\hat{x}+1}{2} \Rightarrow \hat{x}+1 = x \Rightarrow x = -\hat{x}-1$, mas $x, \hat{x} \in \mathbb{N}$, então reia impossível.

- logo, temos que a função f é injetora \rightarrow nenhum par de números naturais diferentes tem a mesma imagem em \mathbb{Z} .

- paralelamente, ela é sobrejetora, pois $\frac{x}{2} = -\frac{(x+1)}{2}$ cobrem todos os \mathbb{Z} .

- portanto, concluímos que \mathbb{Z} é um conjunto contável, pois possui a mesma cardinalidade que \mathbb{N} .

- conjuntos incontáveis

- se a cardinalidade é esteticamente maior que $|\mathbb{N}|$, dizemos que o conjunto é incontável.

- não é possível contar, ou listar, os elementos.

- exemplo de conjunto não contável \rightarrow diagonalização de Cantor

- visando uma contradição, vamos supor que $]\mathbb{0}, 1[$ é um conjunto contável. Ou seja, $f:]\mathbb{0}, 1[\rightarrow \mathbb{N}$ é uma bijeção.

- entao, seja $x_i = f(i) \in]\mathbb{0}, 1[$. logo, $x_i = 0, d_{i1}, d_{i2}, d_{i3}, \dots$, onde $d_{ij} \in \{0, 1, 2, \dots, 9\}$

- considere $x \in]\mathbb{0}, 1[$ definido como $x = 0, d_0, d_1, d_2, \dots$, onde $d_i = \begin{cases} 2, & se\ d_{ii}=0 \\ 1, & se\ d_{ii}\neq0 \end{cases}$

- como f é sobrejetora, $\exists k \in \mathbb{N}: f(k) = x_k = x, \nexists d_{kk} \neq d_k$

- mas note que $]\mathbb{0}, 1[\times \mathbb{N}$

notação assintótica para funções

- introdução

- vários algoritmos podem resolver o mesmo problema, mas quase sempre, normalmente, o algoritmo que executa menos operações

- não ligamos tanto para as constantes \rightarrow podemos agrupar funções com o mesmo comportamento para grande

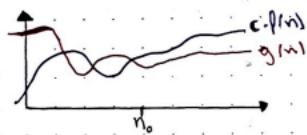
- funções assintoticamente positivas

- funções que se mantêm não negativas à medida que sua entrada (domínio) se aproxima do infinito

- limiteite superior assintótico, big-Oh

- $O(f(n)) = \{g(n) : g(n) cresce mais lentamente que f(n)\}$

$$O(f(n)) = \{g(n) : \exists (n_0, c) \in \mathbb{N} \times \mathbb{R} > 0 \quad (\forall n \geq n_0, g(n) \leq c \cdot f(n))\}$$



- exemplo \rightarrow para cada $f(n)$, mostrare que $f(n) \in O(n^2)$.

- $f(n) = 4n^2$

tomando $c=4$ e $n_0=0$, temos $4n^2 \leq cn^2$ para todo $n \geq n_0$.

Logo, $4n^2 \in O(n^2)$

- $f(n) = 4n^2 + 2n$

vamos decompor: $4n^2 \leq cn^2$ (nátilo) $(2n \leq cn^2)$

vamos que todo natural n , $2n \leq 2n^2$, logo, $4n^2 + 2n \leq 2n^2 + 4n^2 = 6n^2$

$4n^2 + 2n \leq 6n^2$. logo, tomamos $c=6$ e $n_0=0$.

- prova ou refute que $0,000001 \cdot n^2 \in O(n^2)$

- $\exists (c, n_0) \in \mathbb{R}_+ \times \mathbb{N} : \forall n \geq n_0, \quad En^2 \leq n^2 \rightarrow \forall n > 0, \quad E \cdot n^2 \leq n^2$, mas isso é falso para $n > \frac{E}{E}$

notação assintótica

\rightarrow omega \rightarrow limite inferior assintótico

- $\Omega(f(n)) = \{g(n) : g(n) \text{ está por cima de } f(n)\}$

$$\hookrightarrow \Omega(f(n)) = \{g(n) : \exists (n_0, c) \in \mathbb{N} \times \mathbb{R}_{>0}, (\forall n \geq n_0, g(n) \geq c f(n))\}$$

\rightarrow exemplo de omega \rightarrow para cada $f(n) \in g(n)$, prove ou refute que $f(n) \in \Omega(g(n))$

- $f(n) = 4n^2 + 2n + 100 \quad \text{e} \quad g(n) = n^2$

$$\forall n \in \mathbb{N}, 4n^2 \geq n^2, 2n \geq 0 \quad \text{e} \quad 100 > 0.$$

$$\text{Logo, } 4n^2 + 2n + 100 \geq n^2$$

- $f(n) = \frac{n^2}{4} - 2n - 100 \quad \text{e} \quad g(n) = n^2$

$$f(n) = \frac{n^2}{12} + \frac{n^2}{12} + \frac{n^2}{12} - 2n - 100 \Rightarrow \frac{n^2}{12} + \left(\frac{n^2}{12} - 2n \right) + \left(\frac{n^2}{12} - 100 \right)$$

$$\begin{array}{c} \nearrow 0 \\ \downarrow \\ n \geq 24 \end{array} \quad \begin{array}{c} \nearrow 0 \\ \downarrow \\ n \geq 1200 \end{array}$$

$$\hookrightarrow c = \frac{1}{12} \quad \text{e} \quad n_0 \geq 1200 \text{ (extremamente grande)}$$

$$\text{Seja } (n_0, c) = (1200, \frac{1}{12}). \text{ Então, } \forall n \geq n_0, \text{ temos } n^2 \geq 1200, \text{ então } \frac{n^2}{12} \geq 100 \Rightarrow \frac{n^2}{12} - 100 \geq 0$$

$$\text{Similarmente, } n^2 \geq n_0 \Rightarrow \frac{n^2}{12} - 2n \geq 0$$

$$\text{Assim, } \forall n \geq n_0, \frac{n^2}{4} - 2n - 100 = \frac{n^2}{12} + \left(\frac{n^2}{12} - 2n \right) + \left(\frac{n^2}{12} - 100 \right) \geq \frac{n^2}{12} = cn^2$$

\rightarrow teorema

- $\underbrace{g(n) \in \Omega(f(n))}_{c f(n) \leq g(n)} \Leftrightarrow \underbrace{f(n) \in O(g(n))}_{f(n) \leq c g(n)} \quad \text{e} \quad f(n) \leq g(n)$

$\rightarrow \Theta \rightarrow$ assintoticamente equivalente

- $\Theta(f(n)) = \{g(n) : g(n) \text{ está por cima e por baixo de } f(n)\}$

$$\hookrightarrow \Theta(f(n)) = \{g(n) : \exists (n_0, c_0, c_1) \in \mathbb{N} \times \mathbb{R}_{>0} \times \mathbb{R}_{>0} / (\forall n \geq n_0, c_0 f(n) \leq g(n) \leq c_1 f(n))\}$$

- $g(n) \in \Theta(f(n)) \Leftrightarrow g(n) \in O(f(n)) \wedge g(n) \in \Omega(f(n))$

→ soma na notação assintótica

- seja K uma constante e $f_0(n), \dots, f_K(n) \in O(g(n))$. Seja, $f_0(n) + f_1(n) + \dots + f_K(n) \in O(g(n))$
- com esse teorema, podemos simplificar a análise assintótica: $\underbrace{2n^3 + n \log n}_{O(n^3)} + \underbrace{(\log n)^2}_{O(n)} \in \underbrace{O(n^3)}_{O(n^3)}$

→ funções típicas ordenadas assintoticamente

- elas → cada conjunto está contido no próximo

Tipos de crescimento / complexidade

1 constante $\rightarrow O(1)$

2 logarítmica $\rightarrow O(\log n)$

polilogarítmica $\rightarrow O(\log^k n)$, onde $k \in \mathbb{N}^*$ é constante

sublinear $\rightarrow O(n^\epsilon)$, onde $\epsilon \in]0, 1[$ é constante

linear $\rightarrow O(n)$

linearétrica $\rightarrow O(n \log n)$

polinomial $\rightarrow O(n^k)$, onde $k \in \mathbb{N}^*$ é constante

exponencial $\rightarrow O(2^n)$

+ factorial $\rightarrow O(n!)$

→ teorema

- $\log(n!) \in \Theta(n \log n)$

→ propriedades dos logaritmos

• logaritmo do produto $\rightarrow \log_a(b \cdot c) = \log_a b + \log_a c$

• logaritmo do quociente $\rightarrow \log_a\left(\frac{b}{c}\right) = \log_a b - \log_a c$

• logaritmo da potência $\rightarrow \log_a b^c = c \cdot \log_a b$

• logaritmo de base com potência $\rightarrow \log_a b = \frac{1}{c} \log_a b^c$

• mudança de base $\rightarrow \log_b a = \frac{\log_a a}{\log_a b}$

Vetópées: assimptóticas com inequações estitas

→ assimptoticamente estritamente menor → ojinho

- $\Theta(f(n)) = \{g(n) : g(n) \text{ cresce estritamente mais devagar que } f(n)\}$

- definição formal $\Theta(f(n)) = \{g(n) : \forall c \in \mathbb{R}_{>0} \exists n_0 \in \mathbb{N}, (\forall n > n_0, g(n) \leq c \cdot f(n))\}$

→ assimptoticamente estritamente maior → omegão

- $\Omega(f(n)) = \{g(n) : g(n) \text{ cresce estritamente mais rapidamente que } f(n)\}$

- definição formal $\Omega(f(n)) = \{g(n) : \forall c \in \mathbb{R}_{>0} \exists n_0 \in \mathbb{N}, (\forall n > n_0, g(n) \geq c \cdot f(n))\}$

→ teorema

$$g(n) \in \Theta(f(n)) \Leftrightarrow f(n) \in \Theta(g(n))$$

| resumo das vetópées | |
|-------------------------|------------------|
| $f(n) \in O(g(n))$ | $f(n) \leq g(n)$ |
| $f(n) \in \omega(g(n))$ | $f(n) > g(n)$ |
| $f(n) \in \Theta(g(n))$ | $f(n) = g(n)$ |
| $f(n) \in \Theta(g(n))$ | $f(n) \leq g(n)$ |
| $f(n) \in \Omega(g(n))$ | $f(n) > g(n)$ |

Algoritmos

→ sequências definidas recursivamente

- sequências ou funções que são definidas com respeito a si próprias, mas incluem um caso base

→ exemplo

- considere $f(n) = \begin{cases} 2, & \text{se } n=0 \\ 2(f(n-1)) + 1, & \text{se } n \geq 1 \end{cases}$. Calcule $f(3)$.

$$\bullet f(3) = 2(f(2)) + 1 = 2(2(f(1)) + 1) + 1 = 2(2(2(f(0)) + 1) + 1) + 1 =$$

$$2(2(2(2+1)+1)+1) = 2(2(5)+1)+1 = 2(11)+1 = 23$$

recorrências

→ fórmula fechada

- muitas vezes, é possível achar uma fórmula não recursiva para uma função que tem recorrência

- exemplo

$$\text{fazemos } \begin{cases} 2 & , \text{ se } n=0 \\ 2 \cdot f(n-1) + 1 & , \text{ se } n>1 \end{cases}$$

↳ aplicamos a definição da função algumas vezes para tentar obter um candidato para o termo geral.

↳ temos $f(n) = 2^n \cdot f(n-1) + 2^n - 1$

↳ usamos a case base para obter uma expressão para f(n) → $n=k \Rightarrow f(n) = 2^k f(0) + 2^k - 1 = 3 \cdot 2^k - 1$

↳ usamos indução matemática / P.B.O. para provar que $f(n)$ é, de fato, uma fórmula fechada.

↳ $P(n) \Leftrightarrow f(n) = 3 \cdot 2^n - 1, \forall n \in \mathbb{N}, P(n)$

case base: para $n=0$, $f(0)=2$, por definição, e $3 \cdot 2^0 - 1 = 2$.

Hipótese Indutiva: $\exists k \in \mathbb{N}, P(k)$

passo: como $k+1 \geq 1$, temos que $f(k+1) = 2 f(k) + 1$

por H.I., temos que $f(k+1) = 2(3 \cdot 2^k - 1) + 1 = 3 \cdot 2^{k+1} - 1$

ou seja, $P(k+1)$ vale.

resolvendo recorrências

→ passo a passo

- iteração e substituição

- equação característica

- estimativa assintótica

→ prova com notação $O(f(n))$

- Nós provas que $2^n + n^2 \in O(2^n)$
- considere $n_0 = 16 + c = 2$.
- então, $\forall n \geq n_0$, temos $\sqrt{n} \geq 4$ e também $\sqrt{n} \geq \log \sqrt{n}$
- portanto, $n = \sqrt{n} \cdot \sqrt{n} \geq 4 \cdot \log \sqrt{n} = \log n^2$.
- como a função exponencial é crescente, temos $2^n \geq 2^{\log(n^2)} = n^2$
- Portanto, para $n \geq n_0$, $2^n + n^2 \leq 2^n + 2^n = c \cdot 2^n$, sendo $c = 2$
- Isto significa que $2^n + n^2 \in O(2^n)$.

→ prove que $\log(n^3 + 10n - 10) \in O(\log(n^3))$

- Sabendo que $10n^3 \geq 10n$ para qualquer $n \in \mathbb{N}$ e que a função logarítmica é crescente, temos:
 $\log(n^3 + 10n - 10) \leq \log(n^3 + 10n^3 - 10) = \log(11n^3 - 10)$
- Cuidado quando de fato de dizer ser crescente, $\log(11n^3 - 10) \leq \log(11n^3)$.
- Assim, temos que $\log(n^3 + 10n - 10) \leq \log(11n^3)$.
- Temos que $11n^3 \leq n^4$, $\forall n \geq 11$. Assim, temos que $\log(11n^3) = \log(11n^3) \leq \log(n^4)$.
- Por fim, para mostrar que $\log(n^3 + 10n - 10) \in O(\log(n^3))$, precisamos encontrar c tal que
 $\log(n^3 + 10n - 10) \leq c \cdot \log(n^3)$.
- Como visto anteriormente, $\log(n^3 + 10n - 10) \leq \log(11n^3) \leq \log(n^4)$ para $n \geq 11$.
- Dessa forma, temos $\leq 2 \log(n^3)$, mostrando que $c \geq 2$.
- Em suma, com $n_0 = 11 + c = 2$, temos que $\log(n^3 + 10n - 10) \in O(\log(n^3))$.

Solução de recorrências via equação característica

→ recorrência com dois termos recursivos.

- Vamos considerar a recorrência $a_0 = 1, a_1 = 3, a_n = a_{n-1} + 2 \cdot a_{n-2}$.
- considere soluções do tipo $a_n = cX^n$ para algum $(c, X) \in \mathbb{R}^2$. Se isso funcionasse, teríamos que $cX^n = cX^{n-1} + 2cX^{n-2} \Leftrightarrow X^2 - X - 2 = 0$.
↳ solução da recorrência está conectada aos raízes do polinômio.
- suponha que o polinômio tinha 2 raízes distintas $r_1 \neq r_2$. Logo, $r_1^2 \neq r_2^2$ satisfazem a equação.
↳ combinação linear delas também é solução $\Rightarrow a_1r_1^2 + a_2r_2^2$.

→ Teorema para soluções de recorrências lineares homogêneas de grau 2?

- sejam c_1, c_2 constantes não nulas. Considere a recorrência $f(n) = \begin{cases} i_0 & , \text{ se } n=0 \\ i_1 & , \text{ se } n=1 \\ c_1f(n-1) + c_2f(n-2) & , \text{ se } n \geq 2 \end{cases}$
- defina o polinômio $p(x) = x^2 - c_1x - c_2$.

- se $p(x)$ tem duas raízes diferentes $r_1 \neq r_2$, então, para todo $n \in \mathbb{N}$, $f(n) = a_1r_1^n + a_2r_2^n$, onde a_1 e a_2 são constantes determinadas por i_0 e i_1 .

→ condições de teorema

- lineares → não há: $f(n-1)^2, f(n-2)/n, \sqrt{f(n-1)}, \log(f(n-2))$, etc.
- grau 2 → não há: $f(n-3), f(n-4), f(n-5)$, etc.
- homogênea → não há termo constante nem multiplicador $f(n-1)$ ou $f(n-2)$.

→ Fórmula fechada para a sequência de Fibonacci

- a sequência é definida como $F_n = F_{n-1} + F_{n-2}$, com condição inicial $\begin{cases} F_0 = 0 \\ F_1 = 1 \end{cases}$.
- como é uma equação homogênea linear e de grau 2, podemos aplicar o teorema.
 $x^n = x^{n-1} + x^{n-2} \Leftrightarrow x^2 = x + 1 \Leftrightarrow x = \frac{1 \pm \sqrt{5}}{2}$ e, assim, $F_n = a_1 \left(\frac{1 + \sqrt{5}}{2} \right)^n + a_2 \left(\frac{1 - \sqrt{5}}{2} \right)^n$.
- para obter os valores de a_1 e a_2 , aplicamos nos casos base $F_0 = F_1$, obtendo $a_1 = 1 = -a_2$.

→ Teorema

- para a recorrência, definiu o polinômio $p(x) = x^2 - c_1x - c_2$. Se $p(x)$ tem uma raiz de multiplicidade 2, $(p(x) = (x-r)^2)$, então $f(n) = a_2 \cdot r^n + a_3 \cdot n \cdot r^n$.

Solução de recorrências via equação característica

→ exemplo

- considere a relação de recorrência $a_0=1, a_1=0, a_n=6a_{n-1}-9a_{n-2}$ para $n \geq 2$
- ela é homogênea, linear e de grau 2, logo, podemos aplicar qualquer um dos teoremas
- polinômio associado $\rightarrow P(x)=x^2-6x+9 \rightarrow$ a raiz é única $\rightarrow (x-3)^2$
- $a_n = c_1 3^n + c_2 n 3^n$
- a partir das condições iniciais, encontramos $c_1=1 \rightarrow c_2=-1$
- logo, $a_n = 3^n - 3^n \cdot n$

→ generalizações para grau maior que 2 e para recorrências lineares não homogêneas

- utilizam métodos similares

estimativas assintóticas para relações de recorrência

- solução exata X assintótica

- com uma solução exata, é trivial achar uma estimativa assintótica.
↳ mas, achar uma fórmula fechada pode ser desencorajante/trabalhoso.

- fizemos que $f(n) = 2f(n-1) + 1 \in O(2^n)$

- então, se natural, achar que $g(n) = 2(g(n-1)) - 1 \in O(2^n)$ \rightarrow COMO PROVAR?

↳ considere $g(0)=1$ e provemos, por indução matemática, que $g(n) \in O(2^n)$ para $n \geq 1$

↳ 1º, fazemos um raciocínio de passo indutivo e de base para achar $c \in \mathbb{N}$

↳ 2º, fazemos usando indução, que para $\forall n \in \mathbb{N}$ e $n \geq n_0$, $f(n) \leq g(n) \leq 2^n$ vale

- (PROVA) Sup. $f(n) \leq g(n) \leq 1 \cdot 2^n$

case base \rightarrow para $n=0$, temos $g(0)=1 \leq 2^0=1$. Logo, $f(0)$ vale

Hipótese Indutiva $\rightarrow \exists k \in \mathbb{N}$, $f(k)$ vale. Isto sign., $g(k) \leq 2^k$

passo induutivo $\rightarrow g(k+1) = 2g(k) - 1$, pois $k+1 \geq 0$. Logo, $g(k+1) \leq 2^k \cdot 2 - 1 = 2^{k+1} - 1 \leq 2^{k+1}$

Logo, para qualquer $n \geq 0$, $g(n) \leq 2^n$. Isto sign., $g(n) \in O(2^n)$

Estimativas assintóticas com variável extra

- mais uma variável = mais padrão

- "fortalecemos" a hipótese de indução supondo algo como $f(n) \leq c g(n) + d(n)$

- exemplo

ajustamos $d(n)$ para obter o que queremos, incertezas

- vamos provar que $f(n) \in O(n^2)$, onde $f(n) = \begin{cases} 1 & \text{se } n \leq 1 \\ 4f(\lfloor n/2 \rfloor) + n & \text{se } n > 1 \end{cases}$
- sejamos $P(n) \Leftrightarrow f(n) \leq c \cdot n^2 + d(n)$, onde $d(n) = -n$ e $c = 11$
- caso base $\rightarrow P(1) = 10 \leq 11 \cdot 1^2 - 1 = 10 = 10$
- hipótese indução $\rightarrow \exists k \in \mathbb{N}: k-1 \geq 1 \Rightarrow P(1), \dots, P(k-1)$ vale
- passo \rightarrow como $k \geq 2$, temos
$$P(k) = 4P(\lfloor \frac{k}{2} \rfloor) + k \leq 4 \left(c \left(\lfloor \frac{k}{2} \rfloor \right)^2 + d \left(\lfloor \frac{k}{2} \rfloor \right) \right) + k, \text{ pois } k \geq 2, \text{ logo } \lfloor \frac{k}{2} \rfloor \leq k-1, \text{ então } P\left(\lfloor \frac{k}{2} \rfloor\right) \text{ vale}\right. \\ \left. \leq 4c \left(\lfloor \frac{k}{2} \rfloor \right)^2 + 4d \left(\lfloor \frac{k}{2} \rfloor \right) + k = ck^2 - k \quad \text{pois } \lfloor \frac{k}{2} \rfloor \leq k \right)$$

 \Rightarrow em suma, $P(k)$ vale