CT 200 - Fundamentos de Autómatos e Linguagens Formais

Bibliografia

1. Introduction to Automata Theory, Language and Computation
JE Hopcroft e J.D. Ullman, Addison-Wesley

2. Languages and Machines - T. SudKamp, Addison-Wesley

3. Introduction to the Theory of Computation - M. Sipser
- PWS / Thomson

CT 200 Fundamentos de Autômatos e Linguagens Formais

4 meses

JFlap

Lista de Exercícios

Teoria dos conjuntos
Introdução

Prova

Lista de Exercícios

Conjuntos Regulares

Prova

~~Gramáticas~~
Conjuntos Livres de Contexto

Conjuntos Irrestritos

Lista de Exercícios

Prova

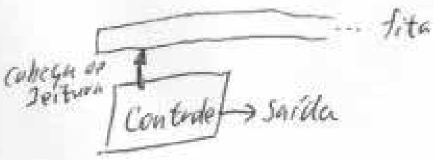
Trabalhos

3 Provas
1 Trabalho

Explicação do Curso

Linguagem Formal →

Autômato →



- produz saída de forma autônoma
- entrada ~~traduzida~~ em saída
- entrada aceita ou não

Para que serve?

- O que é um computador?
  (modelar o computador através de autômatos)
- Problemas: computáveis ou não? Teoria da Computabilidade
  (linguagens modelam problemas
  a solução de problemas é equivalente à interpretação
  de linguagens por autômatos)
- Problemas: fáceis ou difíceis de se resolver num computador?

Teoria da Complexidade

Aplicações Diretas

- projeto de hardware (circuitos sequenciais / circuitos de chaveamento)
- processamento de texto
  (corretor ortográfico) (T9 do celular)
- compiladores
  (análise léxica, sintética, geração de código)
- análise de padrões

1	abc 2	def 3
ghi 4	jkl 5	mno 6
mrs 7	tuv 8	wxyz 9

Soletrar 76538
Polegar 76534
Roleta 765382

Sol
Polenta

Motivação (Importância do formalismo, aprender a demonstrar teoremas)

- Demonstrar que nem todo problema pode ser resolvido computacionalmente

1 - Assumir que para cada função computável há um programa de computador finito

2 - Assim, O conjunto de todos programas de computador (possíveis de se escrever) é infinito, mas contável

3 - ~~Suponha que todo problema~~ Consideramos os problemas que consistem de responder sim ou não para um determinado número inteiro. (Exemplo: O número é par? O número é primo? é perfeito?)

4 - ~~Esses problemas~~ Um problema assim pode ser modelado como uma função $f(n)$ que retorne 0 ou 1.

5 - Suponha que cada problema desse possa ser numerado, assim temos funções $f_0, f_1, \dots, f_i, \dots$ - conjunto contável e infinito

6 - A função $f(n) = \begin{cases} 0, & \text{se } f_n(n) = 1 \\ 1, & \text{caso contrário} \end{cases}$ não pode corresponder a nenhum inteiro. Veja que $f_j(j) = \begin{cases} 0, & \text{se } f_j(j) = 1 \\ 1, & \text{caso contrário} \end{cases}$

7 - ~~Logo~~, o conjunto de problemas é infinito e incontável (maior, portanto que o conjunto do possíveis programas)

Problema não computável:

halting : TodosProgramas $\rightarrow \mathbb{N}$

haltinp(p) = 1 , se a execução de p vai parar

0 , caso contrário

Outro:

Verificar se um programa é correto (faz o que deve fazer)

Teorema de Gödel

Postulado da paralela de Euclides não pode ser demonstrado a partir dos 4 axiomas

1. dados 2 ptos existe uma reta que os contém

2. a reta que passa por 2 pontos é única

3. nem todo ponto está sobre a mesma reta

4. uma reta contém infinitos pontos

Notação de Conjunto

$A = \{1, 3, 7, 10\}$

$\hookrightarrow$ a ordem não importa $\{2,3\} = \{3,2\}$

$B = \{x \mid x \text{ é par}\}$ notação Zermelo-Fraenkel

$\hookrightarrow$ condição ou expressão lógica

$P = \{x \mid x \text{ é o nome de um rio e } x \text{ está no Brasil}\}$

Pertinência

$x \in A$

$x \notin A$

elemento

conjunto

no caso acima $1 \in A$

$2 \notin A$

$C = \{2, 4, 6, 8, \dots\} \to$ conjunto infinito

Conjunto Vazio ou nulo

$\emptyset = \{\}$

$B = \{x \mid x^2 = 4 \text{ e } x \text{ é impar}\} = \emptyset$

$x \notin \emptyset, \forall x$

$\hookrightarrow$ qualquer que seja x

Universo de discurso

U conjunto de todos elementos

$x \in U, \forall x$

Subconjuntos

$A = \{1, 3, 7\}$

são subconjuntos de A: $\emptyset$, $\{1\}$, $\{3\}$, $\{7\}$, $\{1,3\}$, $\{1,7\}$, $\{3,7\}$, $\underbrace{\{1,3,7\}}_{\text{o próprio } A}$

$\{1, 3\} \subset A$ → está contido (é subconjunto de)

$\{1, 7\} \subsetneq A$ → é subconjunto próprio de A, isto é, é subconjunto de A, mas é diferente de A

$A \subsetneq A$ → falso

Inclusão e Comparabilidade

$\emptyset \subset A$, $\forall$ conjunto A

$A \subset B \Rightarrow B \supset A$

$\underset{\text{então}}{\Rightarrow}$ $\quad \underset{\text{contém}}{\supset}$

Se $A \subset B$ ou $B \subset A$, então A e B são comparáveis

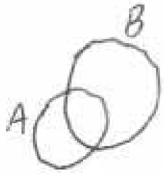
Se $A \not\subset B$ e $B \not\subset A$, então A e B não são comparáveis

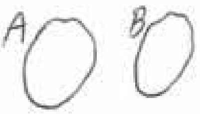
Diagramas de Venn

$\rightarrow x \in A$

$\rightarrow x \notin A$

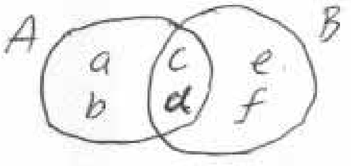
$\rightarrow A \subset B$



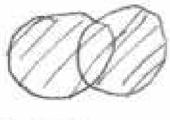


$\rightarrow$ Conjuntos disjuntos

$A = \{a, b, c, d\}$ $\quad B = \{c, d, e, f\}$

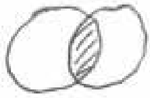


União $A \cup B = \{a, b, c, d, e, f\}$



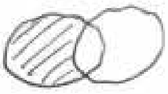
$\{x \mid x \in A \text{ ou } x \in B\}$

Intersecção $A \cap B = \{c, d\}$



$\{x \mid x \in A \text{ e } x \in B\}$

Diferença $A - B = \{a, b\}$



$\{x \mid x \in A \text{ e } x \notin B\}$

Diferença Simétrica $A \ominus B = (A-B) \cup (B-A)$

$= \{a, b, e, f\}$

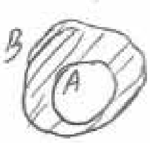
$\{x \mid x \in A \text{ XOR } x \in B\}$

XOR ↓ ou-exclusivo

$\{x \mid (x \in A) \neq (x \in B)\}$

Complemento $\bar{A} = \{x \mid x \notin A\}$

Complemento Relativo $\bar{A}^B = B - A$



Expressões Lógicas

Valores: Verdadeiro e Falso

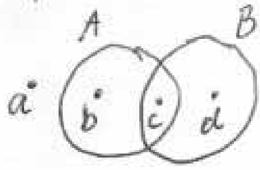
Proposição: uma afirmação que pode assumir um desses valores

$p \wedge q$ → conjunção (operação e)

Tabela verdade

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Exemplo



$p = a \in A \rightarrow F$

$q = a \in B \rightarrow F$

$p \wedge q \rightarrow F$

$p \vee q$ → disjunção (operação ou)

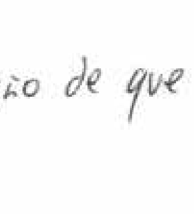
p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

$\neg p$ → negação (afirmação de que p é falsa)

p	$\neg p$
V	F
F	V

$p \rightarrow q$ → implicação ou condicional

$= q \vee \neg p$



$a \in A \rightarrow a \in B$

(é verdadeiro isso? sim)

quando $A \subset B$

$p \leftrightarrow q$ → bicondicional

$a \in A \leftrightarrow a \in B$

(só se $A = B$)

Leis de De Morgan

$\neg(p \vee q) = \neg p \wedge \neg q \longrightarrow \overline{A \cup B} = \bar{A} \cap \bar{B}$

$\neg(p \wedge q) = \neg p \vee \neg q \longrightarrow \overline{A \cap B} = \bar{A} \cup \bar{B}$

EPC - Demonstrar De Morgan (por exemplo, utilizando uma tabela-verdade)

Quantificadores

$p(x)$ "sentença aberta" - depende de x

exemplo $p(x) = x \in A$

se $A = \{1, 2, 3\}$, $p(1)$ é verdadeira, $p(4)$ é falsa

Quantificador Universal $\forall$ (qualquer)

$\forall x \in B,\ p(x) \rightarrow$ verdade se $B \subset A$

Quantificador existencial $\exists$ (existe)

$\exists x \in B,\ p(x) \rightarrow$ verdade se A e B não são disjuntos

Construindo Conjuntos com quantificadores

Exemplo

$B = \{3, 5, 7\}$

$A = \{x \mid \exists y \in B, y < x \text{ e } x < 10\} = \{4, 5, 6, 7, 8, 9\}$

$C = \{x \mid \forall y \in B, y < x \text{ e } x < 10\} = \{8, 9\}$

Cardinalidade de um conjunto finito

é o número de elementos de um conjunto

$A = \{2, 3, 7, 8\}$

$|A| = 4$

Conjunto das Partes

2^A é o conjunto de todos subconjuntos de A

$A = \{1, 2\}$

$2^A = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

$|2^A| = 2^{|A|}$ → Associar a cada elemento a_i de A uma proposição $p_i(x)$

$p_i(x) = a_i \in X$

que pode ser verdadeira ou falsa

Para $A = \{1, 2, 3\}$

- $1 \in X$
  - sim: $2 \in X$
    - sim: $3 \in X$ — sim: $\{1,2,3\}$; não: $\{1,2\}$
    - não: $3 \in X$ — sim / não
  - não: $2 \in X$
    - sim: $3 \in X$ — sim / não
    - não: $3 \in X$ — sim / não: $\emptyset$

⋮

→ $2^{\text{nº de elementos em } A}$

1	2	3
V/F	V/F	V/F

$2 \cdot 2 \cdot 2 = 8$

Pares Ordenados

$(a,b) = \{\{a\}, \{a,b\}\}$

↳ a ordem importa

$(a,b) = (c,d)$ sse $a = c$ e $b = d$

Produto Cartesiano

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

Exemplo $A = \{1,2,3\}$ $B = \{x,y\}$

$A \times B = \{(1,x), (1,y), (2,x), (2,y), (3,x), (3,y)\}$

$|A \times B| = ?$ $\rightarrow |A| \cdot |B|$

$A \times B$ não é necessáriamente igual a $B \times A$

Tuplas

$(a,b,c) = ((a,b),c)$

Assim $(a,b,c) = (d,e,f) \iff a=d, b=e$ e $c=f$

Produto cartesiano de vários conjuntos $A \times B \times C \cdots$

Relações

Uma relação nos conjuntos $A_1, A_2, \cdots, A_n$ é um conjunto qualquer de tuplas de elementos de $A_1, A_2, \cdots, A_n$

Assim

$R \subset A_1 \times A_2 \times \cdots \times A_n$ $\longrightarrow$ $\prod_{i=1}^{n} A_i$

Quando $n=2$, a relação é binária

É comum haver relações binárias sobre o mesmo conjunto A

$R \subset A \times A$

Exemplo

A relação $<$ no conjunto $\{1, 2, 3\}$

$$R_1 = \{(1,2), (1,3), (2,3)\}$$

$1 R_1 2 \rightarrow$ verdadeira
$2 R_1 1 \rightarrow$ falsa

A relação $\leq$ no mesmo conjunto

$$R_2 = \{(1,2), (1,3), (2,3), (1,1), (2,2), (3,3)\}$$

A relação "é o dobro de" no mesmo conjunto

$$R_3 = \{(2,1)\}$$

Relação vazia

$$R_4 = \emptyset$$

Relação conversa

R^c é o converso de uma relação R

$$R^c = \{(x,y) \mid (y,x) \in R\}$$

Qual o converso de "<"?

Funções

Uma relação f ~~em~~ $A \times B$ é uma função com domínio A e codomínio B (ou contra-domínio) se para cada $x \in A$ existe um único y em B tal que $(x,y) \in f$. Em outros termos,

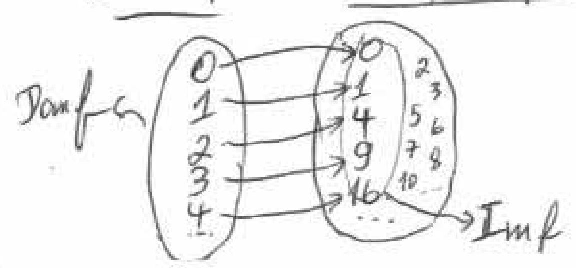
$$(x,y) \in f \text{ e } (x,z) \in f \rightarrow y = z$$

Imagem ou amplitude de f

$$\{y \in B \mid \exists x \in A, f(x) = y\}$$

Exemplo: função quadrado

$$f: \mathbb{N} \rightarrow \mathbb{N} \qquad \text{ou } f(x) = x^2$$
$$x \mapsto x^2$$



- Qual a cardinalidade de uma função?
  = a cardinalidade do domínio

Partições

Seja $A = \{1, 2, 3, \ldots, 10\}$

e os subconjuntos $B_1 = \{1, 3\}$, $B_2 = \{7, 8, 10\}$, $B_3 = \{2, 5, 6\}$,

$B_4 = \{4, 9\}$

$\mathcal{B} = \{B_1, B_2, B_3, B_4\}$ família de conjuntos com as propriedades:

- $A = \bigcup\limits_{B \in \mathcal{B}} B = \bigcup\limits_{i=1}^{4} B_i = B_1 \cup B_2 \cup B_3 \cup B_4$

- ~~B_i~~ Para quaisquer conjuntos B_i, B_j em $\mathcal{B}$ com $i \neq j$

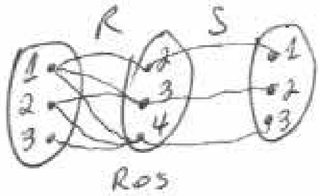
$$B_i \cap B_j = \emptyset$$

$$(\forall B_i, B_j \in \mathcal{B},\ B_i = B_j \vee B_i \cap B_j = \emptyset)$$

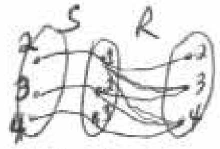
$\mathcal{B}$ é então uma partição de A

e cada B_i é um bloco de A

Composição de Relações



RoS



SoR

$$R_1 \subset X \times Z, \quad R_2 \subset Z \times Y$$

$$x(R_1 R_2)y \iff \exists z \in Z, \ xR_1z \text{ e } zR_2y$$

Relação de Equivalência

A relação R em X é chamada uma relação de equivalência sse R for

1) reflexiva: $\forall x \in X, \ xRx$
2) simétrica: $\forall x,y \in X, \ xRy \to yRx$
3) transitiva: $\forall x,y,z \in X, \ xRy$ e $yRz \to xRz$

Se R é uma relação de equivalência, a classe de equivalência contendo x é:

$$R[x] = \{y \mid y \in X \text{ e } xRy\}$$

Uma relação de equivalência em X particiona X em classes de equivalência disjuntas

Suponha que $x \in R[y]$ e $x \in R[z]$

$$\Downarrow \qquad\qquad \Downarrow$$

$$yRx \qquad\qquad zRx$$

R Simétrica $\Rightarrow xRz$, ~~compondo~~:

R Transitiva $\Rightarrow yRx, xRz \to yRz \Rightarrow y \in R[z]$

Assim $\left.\begin{array}{l} R[y] \subset R[z] \\ R[z] \subset R[y] \end{array}\right\} \Rightarrow R[y] = R[z]$

Além disso, $\forall x, \ x \in R[x] \to$ a partição cobre todo conjunto X

O ranque de R é o número de classes de equivalência

~~Características de Funções~~

Correspondências

Dados dois conjuntos A e B e uma função $f: A \to B$

f é injetora, biunívoca ou "1 para 1" se
nunca mapeia elementos diferentes para
o mesmo lugar, ou seja

$$a \neq b \to f(a) \neq f(b)$$

f é sobrejetora, "sobre" ou "onto" se
atinge todos elementos de B, ou seja

$$\forall b \in B, \ \exists a \in A \mid f(a) = b$$

$\mathrm{Im}\, f = B$

f é bijetora ou uma "Correspondência" se
for injetora e sobrejetora

Uma bijeção num conjunto finito pode ser associada a uma
permutação ou a uma rerotulação

Inversa $\quad f: A \to B$

Se f é injetora, contém uma inversa f^{-1}

Se f for também sobrejetora, o domínio de f^{-1} é B

Se f^c for $\underbrace{\text{uma função,}}_{\text{existe a inversa } f^{-1} \text{ e}}$ $f^{-1} = f^c$

Cardinalidade (geral) definição

Dois conjuntos tem o mesmo tamanho se existe uma correspondência (1:1 e onto) entre eles.

(isto é, os dois conjuntos são equivalentes, cardinalidades iguais definem classes de equivalência entre os conjuntos)

Conjunto Infinito

Um conjunto é infinito sempre que for equivalente a um subconjunto próprio de si mesmo.
Caso contrário, o conjunto é finito.

Conjunto Infinito Contável

É aquele para o qual existe uma correspondência com o conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

Diz-se que sua cardinalidade é $\aleph_0$

Correspondência

Dados dois conjuntos A e B e uma função $f: A \to B$

ou injetora ou biunívoca
f é um-para-um se nunca mapeia elementos diferentes para o mesmo lugar, ou seja

$f(a) \neq f(b)$ sempre que $a \neq b$

$a \neq b \to f(a) \neq f(b)$

ou sobrejetora
f é onto se atinge todos elementos de B, ou seja

$\forall b \in B, \exists a \in A \mid f(a) = b$

A e B tem o mesmo tamanho se há uma função $f: A \to B$ que seja um-para-um e onto (uma correspondência)

Exemplo

Seja $\mathbb{N}^*$ o conjunto dos naturais positivos $\{1, 2, 3, \dots\}$ e $\mathcal{E}$ o conjunto dos naturais pares. Mostrar que tem o mesmo tamanho.

→ Determinar $f(n) = 2 \cdot n$

(como demonstro que f é injetora e bijetora?)

$f(a) = 2 \cdot a$
$f(b) = 2 \cdot b$
Se $f(a) \neq f(b) \Rightarrow 2 \cdot a \neq 2 \cdot b \Rightarrow a \neq b$
(não é ao contrário?)
Se $a \neq b \Rightarrow 2a \neq 2b \Rightarrow f(a) \neq f(b)$

Conjunto contável é o que tem o mesmo tamanho que $\mathbb{N}$

Exemplo

$\mathbb{Q}^+$: racionais positivos

$\mathbb{Q}^+ = \{ \frac{m}{n} \mid m, n \in \mathbb{N} \}$

Provar que $\mathbb{Q}$ tem o mesmo tamanho que $\mathbb{N}$!!!

→ Encontrar uma função que associe a cada elemento de $\mathbb{Q}$, um de $\mathbb{N}$

Construir uma matriz com $\frac{i}{j}$, onde i = linha, j = coluna

$$
\begin{array}{cccccc}
\frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \cdots \\
\frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \\
\frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \\
\frac{4}{1} & \frac{4}{2} & & & & \\
\frac{5}{1} & \vdots & & & &
\end{array}
$$

Transformar a matriz numa lista (listando na diagonal)

- pular elementos repetidos

$\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{5}{1}, \frac{1}{5}, \ldots$

Exemplo

$\mathbb{R}$ é incontável

(por contradição)

Supor $f: \mathbb{N} \to \mathbb{R}$ uma correspondência

Encontrar $x \in \mathbb{R}$, $x \neq n \; \forall n \in \mathbb{N}$, considerar $0 < x < 1$, assim $x = 0, \ldots$

Para que $x \neq f(1)$, o primeiro dígito decimal de x é feito diferente do primeiro de $f(1)$

Para que $x \neq f(2)$, o segundo " "

Não utilizar dígitos 0 ou 9 para construir x

$x \neq f(n)$ para qualquer n, porque o nº dígito é diferente

Exemplo

$\mathbb{R}$ tem o mesmo tamanho que $2^{\mathbb{N}}$

escrevendo um número real entre 0 e 1 na forma binária:

$$r = \underbrace{0{,}d_1\, d_2\, d_3\, d_4 \cdots}_{\text{infinitos dígitos}}$$

cada dígito corresponde a um número natural

~~ao número real pode ser correspondida uma função~~

a correspondência é dada pela função $f: 2^{\mathbb{N}} \to [0,1]$

$$f(c) = 0{,}d_1\, d_2\, d_3\, d_4 \cdots \mid d_i = \begin{cases} 1 & \text{se } i \in c \\ 0 & \text{caso contrário} \end{cases}$$

basta agora encontrar uma correspondência $g: [0,1] \to \mathbb{R}$

EPC O conjunto $\mathbb{N} \times \mathbb{N}$ é enumerável (contável)
→ construção como no caso de $\mathbb{Q}$

EPC O conjunto $2^{\mathbb{N}}$ não é um conjunto enumerável
→ diagonalização como no caso de $\mathbb{R}$

Supor $2^{\mathbb{N}}$ enumerável
$f: \mathbb{N} \to 2^{\mathbb{N}}$ sobrejetora
$X = \{ j \in \mathbb{N} \mid j \notin f(j) \}$
escolhendo k
se $k \in f(k) \Rightarrow k \notin X$
se $k \notin f(k) \Rightarrow k \in X$
contradição

EPC A cardinalidade do intervalo $[0,1]$ é igual à cardinalidade de $\mathbb{R}$
→ basta achar uma função inversível $[0,1] \to \mathbb{R}$

PROG

$F_1((i,j,k)) = 2^i 3^j 5^k$

$F_2((i,j,k)) = g(\,(i, g((j,k)))\,)$ $\quad g((i,j)) = 2^i 3^j$

Verificar se $F((a,b,c)) = F((d,e,f))$ qsq $a=d$, $b=e$ e $c=f$

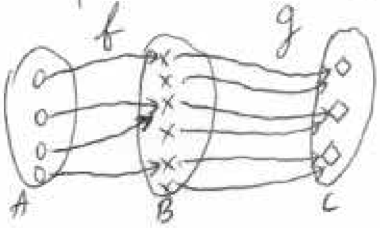
EPC Fechamento da composição de relações no caso de funções

$$(x,z) \in h \Leftrightarrow \exists\, y \in B \mid (x,y) \in f \text{ e } (y,z) \in g$$

f é função : $A \to B$

g é função : $B \to C$

Provar que h é função $h = f \circ g : A \to C$



Provar que

$$(x,y) \in h \text{ e } (x,z) \in h \to y = z$$

$$(x,y) \in h \to \exists\, K \in B \mid (x,K) \in f \text{ e } (K,y) \in g$$

$$(x,z) \in h \to \exists\, l \in B \mid (x,l) \in f \text{ e } (l,z) \in g$$

$$(x,l) \in f \text{ e } (x,K) \in f \text{ e } f \text{ função} \to l = K$$

$$(K,y) \in g \text{ e } \underbrace{(l,z) \in g}_{(K,z) \in g} \text{ e } g \text{ função} \to y = z$$

C.q.d.

Propriedades ~~Potenciais~~ (em potencial)

- Para relações

1) $\forall x \in S,\ xRx$ reflexiva

2) $\forall x,y \in S,\ xRy$ e $yRx \Rightarrow x=y$ antissimétrica

3) $\forall x,y,z \in S,\ xRy$ e $yRz \Rightarrow xRz$ transitiva

4) $\forall x,y \in S,\ xRy$ ou yRx "comparabilidade"

5) $\forall x,y \in S,\ xRy \Rightarrow yRx$ simétrica

- Para operações

6) $\forall x,y,z \in S \quad x \circ (y \circ z) = (x \circ y) \circ z$ associativa

7) $\exists! e \in S,\ \forall x \in S,\ x \circ e = e \circ x = x$ elemento neutro ou identidade

existe um único

8) $\forall x \in S, \exists y \in S,\ x \circ y = y \circ x = e$ existência do inverso

9) $\forall x,y \in S,\ x \circ y = y \circ x$ comutativa

10) $\forall x,y,z \in S \quad x \circ (y \,\square\, z) = (x \circ y) \,\square\, (x \circ z)$ distributiva à esquerda

11) $\forall x,y,z \in S \quad (y \,\square\, z) \circ x = (y \circ x) \,\square\, (z \circ x)$ distributiva à direita

Ordenação

Um sistema $\langle P, \leq \rangle$ é parcialmente ordenado sse satisfaz as propriedades "antissimétrica", "reflexiva" e "transitiva"

Se satisfaz a propriedade de "comparabilidade" diz-se que o sistema é totalmente ordenado.

Exemplos $\langle 2^{\{1,2,3\}}, \subset \rangle$ - parcial

$\langle \mathbb{Z}, \leq \rangle$ - total

Fechos de Relações

$R \subset S \times S$

Fecho transitivo de R é R^+:

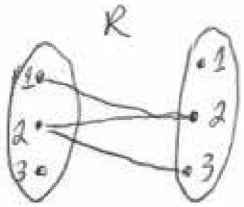
1) $a R b \to a R^+ b$
2) $(a,b) \in R^+$ e $(b,c) \in R \to (a,c) \in R^+$
3) Nada mais em R^+ que não venha de (1) ou de (2)

R^+ inclui R, é transitivo e é mínimo

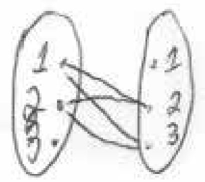
Fecho reflexivo e transitivo R^* de R:

$R^+ \cup \{(a,a) \mid a \in S\}$

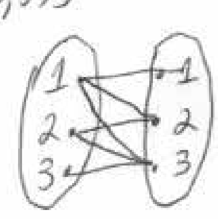
Exemplo $R = \{(1,2), (2,2), (2,3)\}$ $\quad S = \{1,2,3\}$



$R^+ = \{(1,2), (2,2), (2,3), (1,3)\}$



$R^* = \{(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$



Tipos de Demonstração

1 - Demonstração por Construção

2 - Demonstração por Contradição

$\sqrt{2}$ é irracional

1 - Supor $\sqrt{2}$ racional, assim posso escrever $\sqrt{2}$ na forma $\frac{m}{n}$ fração irredutível (m, n inteiros)

2 - $\sqrt{2} = \frac{m}{n} \Rightarrow n \cdot \sqrt{2} = m \Rightarrow 2n^2 = m^2$

3 - m^2 é par, assim m também é par porque o quadrado de um número ímpar é sempre ímpar

4 - $m = 2K$, K inteiro

5 - Substituindo $m = 2K$

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

$$n^2 = 2K^2$$

6 - n é par

7 - $\frac{m}{n}$ não é irredutível, pois m e n são pares

8 - $\sqrt{2}$ não pode ser racional

3- Demonstração por Indução

Demonstrar que $P(n): \sum_{i=0}^{n} i^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$

a) Demonstro $P(0)$

$$P(0): \sum_{i=0}^{0} i^2 = 0 \quad , \quad \frac{0 \cdot (0+1)(0+1)}{6} = 0$$

b) Demonstro $P(n)$, supondo $P(n-1)$ verdade

$$P(n-1): \sum_{i=0}^{n-1} i^2 = \frac{(n-1)(n)(2n-2+1)}{6}$$

Somar n^2 dos dois lados

$$\sum_{i=0}^{n} i^2 = \frac{2n^3 - 2n^2 - n^2 - n + 6n^2}{6} = \frac{2n^3 + 3n^2 + n}{6}$$

$$= \frac{n(2n^2 + 3n + 1)}{6} = \frac{n(2n+1)(n+1)}{6}$$

Teorema → Afirmação matemática provada verdadeira. Geralmente, de interesse particular.

Lema → Como o teorema, mas com significado de resultado intermediário.

Corolário → Como o teorema, mas com significado de resultado decorrente de uma afirmação mais importante.

Outro exemplo Indução

Prove que 3 é um fator de $n^3 - n + 3$, $\forall n \in \mathbb{N}$

i) Para $n = 0$ (base da indução)

$$0^3 - 0 + 3 = 3$$

ii) (passo indutivo)

$$n^3 - n + 3 = K \cdot 3$$

$$(n+1)^3 - (n+1) + 3 = n^3 + 3n^2 + 2n + 3$$

$$= \underbrace{n^3 - n + 3} + \underbrace{(n^2 + n)} \cdot 3$$

$$= K \cdot 3 + \ell \cdot 3$$

$$= (K + \ell) \cdot 3$$

Seqüências

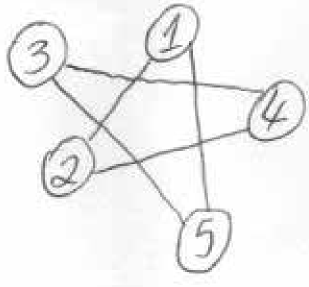
$(7, 21, 57) \rightarrow$ Tupla (no caso uma 3-tupla ou tripla)
seqüência finita

$(2, 4, 6, 8, 10, \dots) \rightarrow$ seqüência infinita

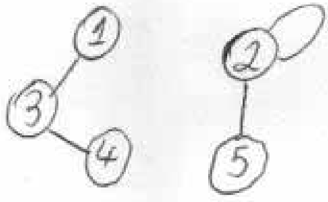
Diferentemente de conjuntos, a ordem dos elementos é importante e pode haver repetições de elementos.

Grafos

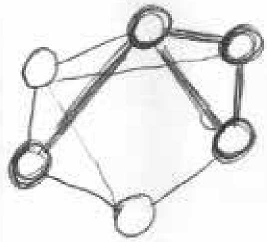
$G = (V, E)$ V: conjunto de vértices
$E \subset V \times V$: conjunto de arestas que conectam 2 vértices



$V = \{1, 2, 3, 4, 5\}$
$E = \{(1,2), (2,3), (3,4), (4,5), (5,1)\}$ (Fecho Simétrico?)

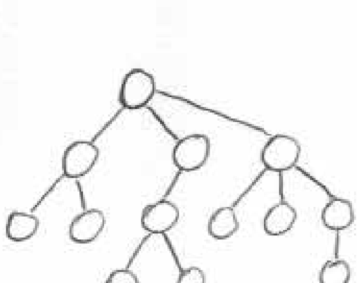


$V = \{1, 2, 3, 4, 5\}$
$E = \{(n, m) \mid n+m = 4$ ou $n+m = 7\}$



Sub-grafo: Subconjunto de V e de E que também é um grafo

Caminho: seqüência de vértices $v_1, v_2, \dots v_K$, $K \geq 1$
tais que existam arestas (v_i, v_{i+1}) $1 \leq i < K$
O comprimento do caminho é $K-1$



Ciclo: Caminho com $v_1 = v_K$

árvore: grafo sem ciclos

Conectividade

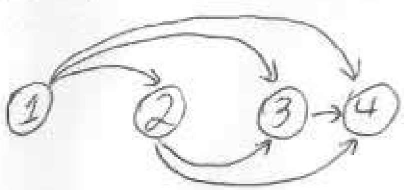
Grafo é conexo se existe caminho de um nó a qualquer outro

(conectividade de nós → fecho transitivo)
↳ relação de equivalência → classes de equivalência

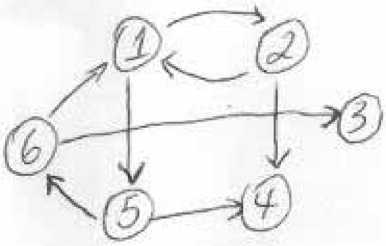
Grafos disjuntos: não existe caminho para dois nós escolhidos

Grafo Direcionado (Digrafo)

Pares ordenados $N_1 \rightarrow N_2$ formam as arestas ou arcos



$(\{1,2,3,4\}, \{i \rightarrow j \mid i<j\})$



$V = \{1,2,3,4,5,6\}$

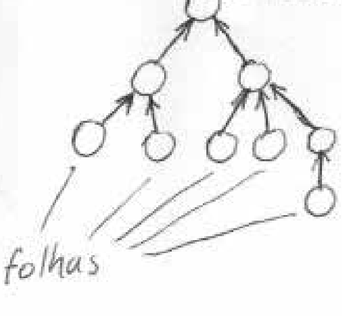
$E = \{(1,2), (1,5), (2,1), (2,4), (5,4), (5,6), (6,1), (6,3)\}$

Grau do nó: número de arestas ligadas ao nó

grau de entrada do nó (fan-in): número de arcos destinados ao nó

grau de saída do nó (fan-out): número de arcos originados no nó

Árvore com raiz e indução de direções



A escolha de uma raiz na árvore induz um direcionamento das arestas, representando a relação "é filho de"

Árvore binária: máximo de filhos por nó é 2

Os filhos podem ser ordenados (exemplo: filho à esquerda e filho à direita

Cadeias de Símbolos e Linguagens

Strings, cadeias ou fitas: são seqüências finitas de símbolos

Símbolos são entidades primitivas

Alfebeto é um conjunto de símbolos

$\Sigma_1 = \{0,1\}$ $\quad \Sigma_2 = \{a,b,c,d,e,\cdots,z\}$

Uma String de um alfabeto Σ é uma seqüência finita de símbolos do alfabeto Σ

01001 é uma cadeia do alfabeto $\Sigma = \{0,1\}$

Se $\underline{w}$ é uma cadeia, o comprimento de $\underline{w}$ é escrito $|\underline{w}|$ e é o número de símbolos que $\underline{w}$ contem

A cadeia vazia tem tamanho zero e é escrita ϵ (ou λ)

Sub-string $\underline{z}$ de $\underline{w}$ se $\underline{z}$ aparece de forma consecutiva dentro de $\underline{w}$ (cad é substring de abracadabra)

$\underline{w} = w_1 w_2 \cdots w_n \quad , \; w_i \in \Sigma$

Concatenação de $\underline{x} = x_1 x_2 \cdots x_n$ e $\underline{y} = y_1 y_2 \cdots y_m$

$\underline{xy} = x_1 x_2 \cdots x_n y_1 y_2 \cdots y_m$

Concatenação múltipla de $\underline{x}$ com si próprio

$\underline{x}^k = \underbrace{\underline{x}\underline{x}\cdots\underline{x}}_{k \text{ vezes}}$

Ordem lexicográfica

"Ordem do dicionário", strings mais curtas precedem strings mais longas

$(\epsilon, 0, 1, 00, 01, 10, 11, 000, \cdots)$

Linguagens

Linguagem é um conjunto de strings de um alfabeto

$\emptyset$ é uma linguagem

$\{\epsilon\}$ é uma linguagem

O conjunto dos palindromos no alfabeto $\{0,1\}$ é uma linguagem

$\{\epsilon, 0, 1, 00, 11, 000, 101, 010, 111, \cdots\}$

O conjunto de todas as strings sobre o alfabeto Σ

é designada por Σ^*

Para $\Sigma = \{a\}$, $\Sigma^* = \{\epsilon, a, aa, aaa, \cdots\}$

Para $\Sigma = \{0,1\}$, $\Sigma^* = ?$ $\{\epsilon, 0, 1, 00, 01, 10, 11, 000, \cdots\}$

Definição

i) $\epsilon \in \Sigma^*$

ii) Se $\underline{w} \in \Sigma^*$ e $a \in \Sigma$, então $\underline{w}a \in \Sigma^*$

iii) $\underline{w} \in \Sigma^*$ apenas se puder ser obtida por um número finito de aplicações de (ii) a partir de ϵ

Uma linguagem L sobre Σ é um subconjunto de Σ^*

Concatenação de Strings

Sejam $\underline{u}$ e $\underline{v} \in \Sigma^*$. A concatenação $\underline{uv}$ é uma operação binária definida em Σ^* da seguinte forma

(i) Se $|\underline{v}| = 0 \Rightarrow \underline{uv} = \underline{u}$

(ii) Seja v de comprimento $= n > 0$. $\underline{v} = \underline{w}\, a$, onde $\underline{w}$ é string de tamanho $n-1$ e $a \in \Sigma$, e $\underline{uv} = (\underline{uw})a$

→ Concatenação é associativa, com elemento neutro ϵ

Reverso

$\underline{u}^R = (u_n u_{n-1} \cdots u_1)$ onde $\underline{u} = (u_1 u_2 \cdots u_n)$

Definição Recursiva:

(i) Se $|\underline{u}| = 0 \Rightarrow \underline{u}^R = \varepsilon$

(ii) Se $|\underline{u}| = n > 0$, então $\underline{u} = \underline{w}a$ para alguma string $\underline{w}$, $|\underline{w}| = n-1$ e $a \in \Sigma$, e $\underline{u}^R = a\underline{w}^R$

Propriedade: $(\underline{u}\underline{v})^R = \underline{v}^R \underline{u}^R$

Demonstr.

Base Indução: $|\underline{v}| = 0 \Rightarrow \underline{v} = \varepsilon$, $(\underline{u}\underline{v})^R = \underline{u}^R$

Analogamente, $\underline{v}^R \underline{u}^R = \varepsilon \underline{u}^R = \underline{u}^R$

Passo Indutivo:

$|\underline{v}| = n+1$, provar $(\underline{u}\underline{v})^R = \underline{v}^R \underline{u}^R$

$\underline{v} = \underline{w}a$, $|\underline{w}| = n$ e $a \in \Sigma$

$$(\underline{u}\,\underline{v})^R = (\underline{u}(\underline{w}a))^R = ((\underline{u}\underline{w})a)^R = a(\underline{u}\underline{w})^R = a(\underline{w}^R\underline{u}^R)$$
$$= (a\underline{w}^R)\underline{u}^R = (\underline{w}a)^R\underline{u}^R = \underline{v}^R\underline{u}^R$$

Especificações Finitas de Linguagens

(expressão lógica) • $L_1 = \{\underline{x} \in \Sigma_1^* \mid \underline{x} = \underline{w}a$, $\underline{w} \in \Sigma_1^*$ e $a \in \{1,3,5,7,9\}\}$ $\quad \Sigma = \{0,1,2,3,\dots,9\}$

(representação recursiva) • $\Sigma_2 = \{a, b\}$ $\longrightarrow$ Strings de comprimento par começando por a

(i) aa e $ab \in L_2$

(ii) Se $\underline{u} \in L_2$, então $\underline{u}aa$, $\underline{u}ab$, $\underline{u}ba$ e $\underline{u}bb \in L_2$

(iii) $\underline{u} \in L_2$ apenas se pode ser obtida ~~pelos~~ a partir dos elementos em (i) por um número finito de aplicações de (ii)

- $\Sigma_3 = \{a, b\}$ $\rightarrow$ Cada b é imediatamente precedido por uma a

  (i) $\varepsilon \in L_3$

  (ii) $\underline{u} \in L_3 \Rightarrow \underline{u}a, \underline{u}ab \in L$

  (iii) $\underline{u} \in L_3$ apenas se obtido a partir de ε por um número finito de aplicações do passo recursivo (ii)

Concatenação de Linguagens

A concatenação das linguagens X e Y, denotada XY, é a linguagem

$$XY = \{\underline{u}\underline{v} \mid \underline{u} \in X \text{ e } \underline{v} \in Y\}$$

A concatenação de X consigo n vezes é denotada X^n. $X^0 = \{\varepsilon\}$

Exemplo:

$X = \{a, b, c\}$ e $Y = \{abb, ba\}$, então

$XY = \{aabb, babb, cabb, aba, bba, cba\}$

$X^0 = \{\varepsilon\}$

$X^1 = X = \{a, b, c\}$

$X^2 = XX = \{aa, ab, ac, ba, bb, bc, ca, cb, cc\}$

$X \cup Y = \{a, b, c, abb, ba\}$

Fechamento de Kleene

Se X é um conjunto, então

$$X^* = \bigcup_{i=0}^{\infty} X^i \quad \text{e} \quad X^+ = \bigcup_{i=1}^{\infty} X^i \quad \left(\begin{array}{c}\text{Notar que} \\ X^+ = XX^*\end{array}\right)$$

$X = \{a, b, c\} \Rightarrow X^* = \{\varepsilon, a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, aaa, \ldots\}$

X^+ não contém o ε

Reversão de Linguagem $X^R = \{\underline{u}^R \mid \underline{u} \in X\}$

Representação de Linguagens com Operadores

Linguagem das strings que contém a substring bb

$\{a,b\}^*\{bb\}\{a,b\}^*$

Cadeias que começam e terminam com a e que contém pelomenos um b

$\{a\}\{a,b\}^*\{b\}\{a,b\}^*\{a\}$

Cadeias sobre $\{a,b\}$ começando com ~~a~~ aa ou terminando com bb

$\{aa\}\{a,b\}^* \cup \{a,b\}^*\{bb\}$

Cadeias sobre $\{a,b\}$ de comprimento par

$\{aa, bb, ab, ba\}^*$

Conjuntos Regulares

$\emptyset$, $\{\epsilon\}$, $\{a\}$ $\forall a \in \Sigma$ e conjuntos formados por união, concatenação e fechamento de Kleene.

Definição Recursiva:

(i) $\emptyset$, $\{\epsilon\}$ e $\{a\}$, $\forall a \in \Sigma$ são conjuntos regulares sobre Σ

(ii) Sejam X e Y conjuntos regulares sobre Σ.
Os conjuntos $X \cup Y$, XY e X^* são conjuntos regulares sobre Σ

(iii) X é regular sobre Σ apenas se pode ser obtido pelos elementos básicos com aplicação de um número finito de vezes do passo recursivo

Exemplo: $\{a,b\}^*\{bb\}\{a,b\}^*$ é regular

$\{a\}$ e $\{b\}$ são regulares $\Rightarrow \{a\} \cup \{b\} = \{a,b\}$ é regular $\Rightarrow \{a,b\}^*$ é regular

$\Rightarrow \{b\}\{b\} = \{bb\}$ é regular

$\Rightarrow \{a,b\}^*\{bb\}\{a,b\}^*$ é regular

Expressões Regulares

Forma abreviada para representar conjuntos regulares

Seja Σ um alfabeto, as expressões regulares sobre Σ são definidas recursivamente como:

(i) $\emptyset$, ε e a para qualquer $a \in \Sigma$ são expressões regulares sobre Σ

(ii) Sejam $\underline{u}$ e $\underline{v}$ expressões regulares sobre Σ.

As expressões

$(\underline{u} \cup \underline{v})$

$(\underline{u}\underline{v})$

$(\underline{u}^*)$

São expressões regulares sobre Σ

(iii) $\underline{u}$ é uma expressão regular sobr Σ somente se pode ser obtida a partir dos elementos de (i) com aplicação de (ii) um número finito de vezes.

Parenteses podem ser omitidos:

- união e concatenação são associativas
- regra de precedência: $*$, concatenação, $\cup$

$\underline{u}^+$ é o mesmo que $\underline{u}\underline{u}^*$

$\underline{u}^2$ equivale a $\underline{u}\underline{u}$

Identidades para Expressões Regulares

1. $\emptyset u = u\emptyset = \emptyset$
2. $\varepsilon u = u\varepsilon = u$ — elemento neutro
3. $\emptyset^* = \varepsilon$
4. $\varepsilon^* = \varepsilon$
5. $u \cup v = v \cup u$ — comutatividade
6. $u \cup \emptyset = u$ — elemento neutro
7. $u \cup u = u$
8. $u^* = (u^*)^*$ — idem potência
9. $u(v \cup w) = uv \cup uw$ — distributividade à esquerda
10. $(u \cup v)w = uw \cup vw$ — distributividade à direita
11. $(uv)^*u = u(vu)^*$
12. $(u \cup v)^* = (u^* \cup v)^*$
$$= u^*(u \cup v)^* = (u \cup vu^*)^*$$
$$= (u^*v^*)^* = u^*(vu^*)^*$$
$$= (u^*v)^*u^*$$

Exemplos

O conjunto regular $\{ba\underline{w}ab \mid \underline{w} \in \{a,b\}^*\}$ expresso por $ba(a \cup b)^*ab$

$(a \cup b)^*aa(a \cup b)^* \cup (a \cup b)^*bb(a \cup b)^* \rightarrow$ strings de $\{a,b\}^*$ contendo aa ou bb

$a^*ba^*ba^* \rightarrow$ strings que contém exatamente 2 b's

$(a \cup b)^*b(a \cup b)^*b(a \cup b)^* \rightarrow$ strings que contém 2 ou mais b's

ou

$a^*ba^*b(a \cup b)^*$

EPC Provar por Indução (em i) que

$$(\underline{w}^R)^i = (\underline{w}^i)^R \ , \ \forall \text{ string } \underline{w} \ , \ \forall \ i \geq 0$$

EPC O conjunto de palíndromos é definido como

$$\{ \underline{w} \mid \underline{w} = \underline{w}^R \}$$

Dê uma definição recursiva equivalente

EPC Dê uma expressão regular que represente

a) O conjunto de strings sobre $\{a, b, c\}$ em que todo a precede algum b, todo b precede algum c

b) O conjunto de strings sobre $\{a, b\}$ de tamanho 2 ou maior em que todo a precede b

c) O conjunto de strings sobre $\{a, b, c\}$ que não contém a substring aa

d) O conjunto de strings sobre $\{a, b\}$ em que todo a é ou imediatamente precedido ou imediatamente seguido por um b, por exemplo, baab, aba e b

e) O conjunto de strings de tamanho ímpar sobre $\{a, b\}$ que contém a substring bb