Teoria da Computação

MsC. Ana Carolina Siravenha
siravenha@ufpa.br Ou carolinaquintao@gmail.com
LaPS – Laboratório de Processamento de Sinais

Ementa

- Autômatos e Linguagens Formais.
- Linguagens regulares.
- Linguagens livres de contexto.
- Modelos computacionais universais.
- Computabilidade.

Bibliografia

- Cormen, T. H. Algoritmos – Teoria e Prática. Campus, 2002.
- Toscani, L. V. & Veloso, P. A. S Complexidade de Algoritmos. Sagra-Luzzzato, 2002.
- Sipser, Michael Introduction to the Theory of computation. PWS Publishing Company, 1997.
- MENEZES, Paulo F B: Linguagens Formais e Autômatos. P. Alegre: Sagra Luzzatto, 2004 (4a. Ed).
- HOPCROFT, J. E.; MOTWANI, R.; ULLMAN, J.D.: Introduction to Automata Theory, Languages, and Computation. New York: Addison-Wesley, 2004 (2a. Ed).
- LEWIS, H. R.; PAPPADIMITRIOU, C. H.: Elements of the Theory of Computation. Englewood Cliffs: Prentice-Hall, 1981.
- SHIELDS, M. W.: An Introduction to Automata Theory. Oxford: Blackwell Scientific Publications, 1987.
- SALOMA, A.: Formal Languages. New York: Academic Press, 1973.

Avaliação

- Três provas.
- Listas de exercícios.
- Poderemos ter trabalhos!
- Nota final é a média ponderada: (P*8 + LT*2)/10.

Introdução

Teoria da computação

- Computação: solução de um problema ou o cálculo de uma função, através de um algoritmo.
- A teoria da computação: subcampo da ciência da computação e matemática.
  - Busca determinar quais problemas podem ser computados em um dado modelo de computação.
  - Primeiros anos do século XX.
  - Definir o significado de um "método simples": um modelo formal da computação.

Teorias...

- Teoria da complexidade:
  - Problema computacionalmente fácil ou difícil.
  - Ordenação e alocação de aulas.
- Teoria da computabilidade:
  - Problemas não solúveis computacionalmente.
  - Se um enunciado é verdadeiro ou falso.
- Teoria dos autômatos:
  - Definições e propriedades de modelos matemáticos de computação.
    - A. Finito: processamento de texto, compiladores e desenho de hardware.
    - Gramática livre de contexto: linguagens de programação e IA.

Notações e terminologias

- Conjunto: A = {7,21,57}
  - $7 \in A \quad 15 \notin A$
- Sub-conjunto: B = {21}
  - $B \subseteq A$
- Conjunto vazio ($\emptyset$), União ($\cup$), Inteseção ($\cap$) e Complemento (A^C)...
- Sequência: objetos em alguma ordem.
  - {1,2,3}, {a, b,d,m,z} e $\{1,2,3\} \neq \{3,1,2\}$
  - Tuplas: sequência finita (3-tupla, 5-tupla)

Notações e terminologias

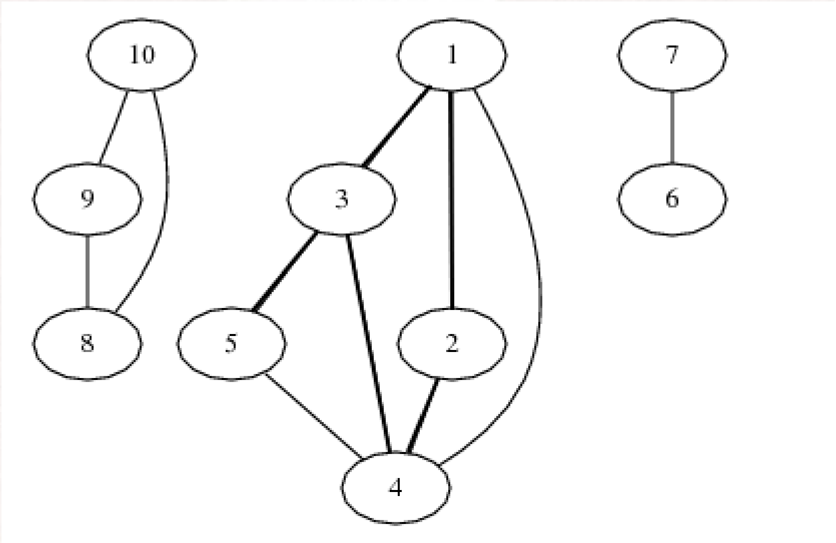
- Função: um objeto com relação entrada-saída (f(a)=b).
  - Domínio: possíveis entradas da função.
  - Contra-domínio: possíveis saídas da função.

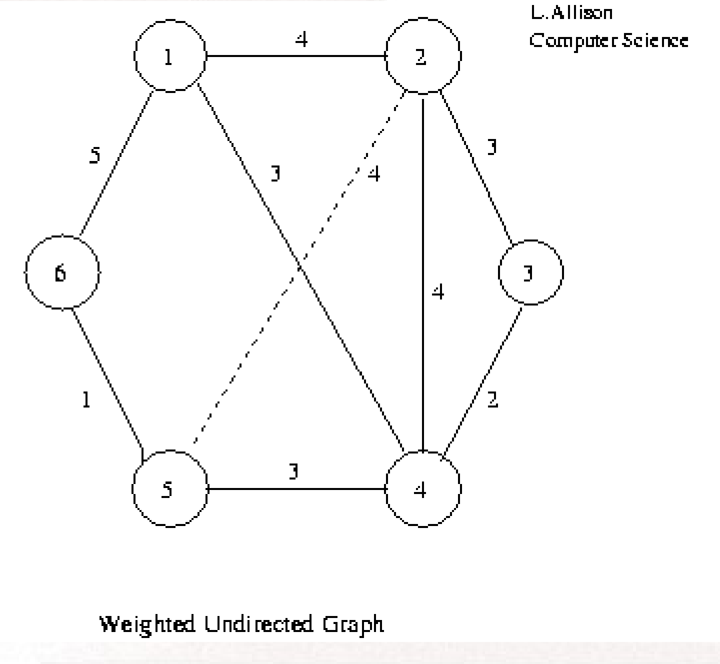
$$f : D \rightarrow CD$$

- Relações:
  - Reflexiva: para todo x, xRx.
  - Simétrica: para todo x e y, xRy sse yRx.
  - Transitiva: se xRy e yRz, implica em xRz.
  - Antissimétrica: se xRy e yRx, então x=y.

Grafos

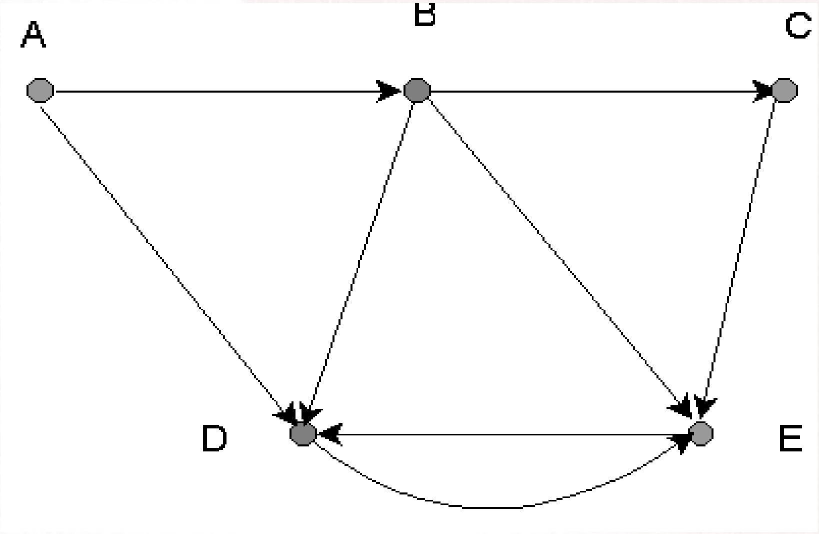
- Conjunto de pontos ligado por linhas.
  - Pontos: nós ou vértices.
  - Linhas: arcos.
  - Graus.
  - Sub-grafo.





Grafos

- Conjunto de pontos ligado por linhas.
  - Caminhos:
    - Círculo
    - Árvore
  - Direcionado: ({A,B,C,D,E},{(A,B),(A,D),(B,C),(B,D),(B,E),(C,E),(E,D),(D,E)})



Palavra e linguagens

- Alfabeto: conjunto finito. O conjunto vazio também é um alfabeto!
- Símbolos: membros do alfabeto.
- Palavra de um alfabeto: sequência finita de símbolos de um alfabeto.
- $\Sigma^+ = \Sigma^* - \{\varepsilon\}$

$$\Sigma = 0,1$$

$$palavra_\Sigma : 0100111$$

$$|palavra_\Sigma| = 8$$

$$|\varepsilon| = 0$$

$$\Gamma = a, b, c, d, e, f, g, \ldots, u, v, x, y, w, z$$

$$palavra_\Gamma : abracadabra$$

$$|palavra_\Gamma| = 11$$

Prefixo, Sufixo e Subpalavra

- **Prefixo** de uma palavra é qualquer seqüência **inicial** de símbolos da palavra.
- **Sufixo** de uma palavra é qualquer seqüência **final** de símbolos da palavra.
- **Subpalavra** é qualquer seqüência **contígua** de símbolos da palavra.
- **Exemplo**: Identificar os prefixos, sufixos e subpalavras de “aaba”.

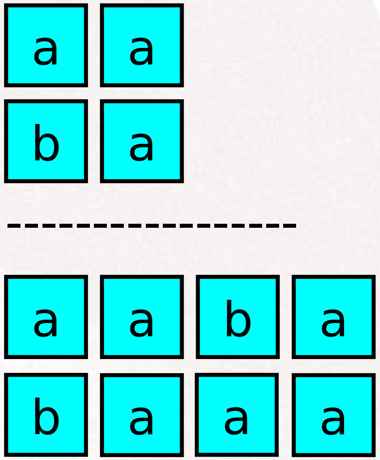
aaba:
ε, a, aa, aab, aaba
ε, a, ba, aba, aaba
ε, a, b, aa, ab, ba, aab, aba, aaba

Linguagem formal

- É um conjunto de palavras sobre um alfabeto.
- Exemplos: {}, {ε}, {a, b, aa, ab, ba, bb, aaa, ...}.
- Aplicações: Modelos dinâmicos, processos de automação, provadores de teoremas, interpretadores, compiladores, lógica temporal, automação, robótica, prototipação, etc.

Concatenação de palavras

- Operação binária, sem representação.
- É a justaposição de duas ou mais palavras
  - produz uma terceira que é formada pelos símbolos da primeira, na ordem em que ocorrem, seguidos pelos símbolos da segunda, também na ordem em que ocorrem e assim sucessivamente.
- Exemplo: Se v=aa e w=ba então x=vw=aaba e y=wv=baaa.



Propriedades da concatenação

- **Associatividade**: v(wt) = (vw)t.
- **Elemento Neutro**: εw = w = wε.

v=aa, w=b, t=a → v(wt) = (vw)t = aaba

u=aaba → εu = aaba = uε

Concatenação sucessiva

- De uma palavra repetidas vezes com ela mesma.
- Notação: w^n, onde $n \geq 0$ é o número de vezes que a palavra é repetida.
- w^3 = www.

  w^1 = w.

  $w^0 = \varepsilon$, para $w \neq \varepsilon$.

$(ab)^3$ = ababab
$(01)^4$ = 01010101

Gramática

- Uma gramática é uma quádrupla, G=(V, T, P, S), onde:
  - V é um conjunto de símbolos variáveis ou não-terminais.
  - T é um conjunto de símbolos terminais, disjunto de V.
  - P é um conjunto finito de regras de produção.
  - S é um elemento de V denominado “variável inicial”.

Exemplo:

$$G = (\ V = \{S, X\},\ T = \{a, b\},\ P = \{S \rightarrow a \mid aX,\ X \rightarrow b \mid bX\},\ S).$$

Regras de produção

- São pares do tipo (a, b), representados por $a \rightarrow b$, onde $a \in (V \cup T)^+$ e $b \in (V \cup T)^*$.
- Definem as condições de geração das palavras da linguagem.
- Abreviação: $a \rightarrow b_1$, $a \rightarrow b_2$, ..., $a \rightarrow b_n$ por $a \rightarrow b_1 | b_2 | \ldots | b_n$.
- A aplicação de uma regra de produção chama-se uma *derivação*.

$P = \{S \rightarrow aX | bX,\ X \rightarrow a | b | X\}$

Derivação

- Seja G=(V,T,P,S) uma gramática. Uma *derivação* é um par da relação denotada por ➔, com domínio em $(V \cup T)^+$ e contradomínio em $(V \cup T)^*$.
- Um par (a,b) da relação é denotado de forma infixa: a➔b.

Seqüência de Derivação

Seja G=(V,T,P,S)=({S,X},{a,b},{S→aS|X,X→ba|X},S).

Uma *seqüência de derivação* para produzir a palavra "aaba" nesta gramática é: S ➔ aS ➔ aaS ➔ aaX ➔ aaba.

Definição de derivação (intuitiva)

- Para toda produção da forma S→b, onde S é o símbolo inicial de G, tem-se que S➔b.
- Para todo par a→b, onde b=uvw, se v→t é regra de P, então a➔utw.
- Portanto uma derivação é a substituição de uma subpalavra, de acordo com uma regra de produção.
- Notação:

$\Rightarrow^*$ Zero ou mais passos de derivação sucessivos.

$\Rightarrow^+$ Um ou mais passos de derivação sucessivos.

$\Rightarrow^n$ Exatamente n passos de derivação sucessivos.

Linguagem gerada

- Uma gramática é um formalismo *gerador*, pois permite derivar (gerar) todas as palavras da linguagem que representa.
- Seja G = (V, T, P, S) uma gramática.
- A linguagem gerada pela gramática G, denotada por L(G) ou GERA(G), é composta por todas as palavras formadas por símbolos terminais deriváveis a partir do símbolo inicial S.
- $L(G) = \{w \in T^* \mid S \Rightarrow^{+} w\}$.
- Exemplo: $G=(V,T,P,S)=(\{S, D\}, \{0,1,...,9\}, \{S \rightarrow D \mid DS, D \rightarrow 0|1|...|9\}, S)$.

Linguagem gerada

- A gramática abaixo gera o conjunto dos números naturais:
- G=(V,T,P,S)=({S, D}, {0,1,...,9}, {S→D|DS, D→0|1|...|9}, S).

Por exemplo, gerar 593:

S→ DS → 5S → 5DS → 59S → 59D → 593

- Duas gramáticas, G1 e G2 são ditas ser *equivalentes* se e somente se geram a mesma linguagem, isto é:
  - GERA(G1) = GERA(G2).

Indução

- Silogismo estatístico: 90% dos estudantes de EngComp são criativos. José é estudante de EngComp; logo, José é criativo.
- Generalização estatística: 63% de uma amostra de 3.845 pessoas escolhidas ao acaso em todo país são presidencialistas; logo, 63% dos brasileiros são presidencialistas

Indução matemática

- Aplica-se a conjuntos enumeráveis.
- *Base de indução*: Mostrar que P é verdadeira para X=0 ou X=1.
- *Hipótese de Indução*: Assumir que P é verdadeira para X=N.
- *Passo de Indução*: Mostrar que P é verdadeira para X=N+1.

Indução matemática

- Seja p(n) uma proposição sobre N:
  - p(0) é verdadeira;
  - Para qualquer $k \in \mathbb{N}, p(k) \rightarrow p(k+1)$ é verdadeira.
  - Então, para qualquer $n \in \mathbb{N}$, p(n) é verdadeira.
- p(0), p(n) e a proposição $p(k) \rightarrow p(k+1)$ denominam-se: base de indução, hipótese de indução e passo de indução, respectivamente.

Indução matemática

- Em uma demonstração por indução, deve-se demonstrar a base de indução p(0) e, fixado um k, supor verdadeira a hipótese de indução p(k) e demonstrar o passo de indução.
- Exemplo:Para qualquer $n \in \mathbb{N}$, tem-se que $1+2+...+n = (n^2+n)/2$
  - Base de indução: Seja n=0, logo: $(0^2+0)/2 = 0$
    - Assim,para n=0 a proposta é V. Note: $1+2+...+n = 0+1+2+...+n$.

Indução matemática

- Hipótese da indução: Suponha que para algum $n \in \mathbb{N}$ tem-se que: $1+2+...+n=(n^2+n)/2$.
- Passo de indução: Prova para $1 + 2 +...+ n + (n + 1)$:
  - $1 + 2 +...+ n + (n + 1) =$
    $(1 + 2 +...+ n) + (n + 1) =$
    $(n^2 + n)/2 + (n + 1) =$
    $(n^2 + n)/2 + (n*2 + 1*2)/2 =$
    $(n^2 + n + 2n + 2)/2 =$
    $((n^2 + 2n + 1) + (n + 1))/2 =$
    $((n + 1)^2 + (n+1))/2.$
  - Assim, $1 + 2 +...+ n + (n + 1) = ((n + 1)^2 + (n+1))/2$ e para todo $n \in \mathbb{N}$ tem-se que $1+2+...+n=(n^2+n)/2$

Exercícios

- Marque os conjuntos que são alfabetos:

  a) Conjunto dos números naturais; [ ]

  b) Conjunto dos números primos; [ ]

  c) Conjunto das letras do alfabeto brasileiro; [ ]

  d) Conjunto dos algarismos arábicos; [ ]

  e) Conjunto dos algarismos romanos; [ ]

  f) Conjunto { a, b, c, d }; [ ]

  g) Conjunto das partes de { a, b, c }; [ ]

  h) Conjunto das vogais; [ ]

  i) Conjunto das letras gregas. [ ]

Exercícios

- Marque os conjuntos que são alfabetos:

  a) Conjunto dos números naturais [ ]

  b) Conjunto dos números primos [ ]

  c) Conjunto das letras do alfabeto brasileiro [x]

  d) Conjunto dos algarismos arábicos [x]

  e) Conjunto dos algarismos romanos [x]

  f) Conjunto { a, b, c, d } [x]

  g) Conjunto das vogais [x]

  h) Conjunto das letras gregas [x]

Exercícios

- Dê os possíveis prefixos e sufixos de cada uma das seguintes palavras:

  a) teoria

  b) universidade

  c) aaa

  d) abccba

  e) abcabc

Exercícios

- Dê os possíveis prefixos e sufixos de cada uma das seguintes palavras:

  a) teoria

    - P: t, te, teo...
    - S: a, ia, ria...

  b) universidade

    - P:u, un, uni...
    - S:e, de, ade...

Exercícios

1.2 Para $A = \{1\}$, $B = \{1, 2\}$ e $C = \{\{1\}, 1\}$, discuta a validade das seguintes proposições:

a) $A \subset B$, $A \subseteq B$, $A \in B$, $A = B$

b) $A \subset C$, $A \subseteq C$, $A \in C$, $A = C$

c) $1 \in A$, $1 \in C$, $\{1\} \in A$, $\{1\} \in C$

1.17 Prove por indução que, para qualquer $n \in \mathbb{N}$, tem-se que:

$$1 + 8 + \ldots + n^3 = (1 + 2 + \ldots + n)^2$$

Sugestão: para verificar a base de indução ($n = 0$), lembre-se que zero é o elemento neutro da adição.