Linguagens Formais, Autômatos e Gramáticas

Profa. Gina M. B. de Oliveira

Universidade Federal de Uberlândia

Esse material é baseado nos seguintes materiais:

• MENEZES. P. F. B. Linguagens Formais e Autômatos. Editora Sagra Luzzato, Porto Alegre, 4a ed., 2001.

• HOPCROFT, J. E.; ULLMAN, J. D. **Introduction to automata theory languages and computation.** Massachusetts: Addison-Wesley, 1979.

• Transparências de aula do Prof. Paulo F. B. Menezes.

• Transparências de aula da Profa. Gina M. B. de Oliveira

♦ Teoria das Linguagens Formais

- originariamente desenvolvida na década de 1950
- objetivo inicial
  - desenvolver teorias relacionadas com as linguagens naturais
- hoje
  - importante para o estudo de linguagens artificiais
  - em especial, para as linguagens originárias na Ciência da Computação

♦ Tipos do Formalismos usados

- Operacional
- Axiomático
- Denotacional

Operacional

- **Autômato ou máquina abstrata**
  - estados
  - instruções primitivas
  - como cada instrução modifica cada estado
- **Máquina abstrata**
  - suficientemente simples
    - não deve permitir dúvidas sobre seu funcionamento
  - também é dito um *Formalismo Reconhecedor*
    - análise de uma entrada para verificar se é *reconhecida* pela máquina
- **Principais máquinas**
  - Autômato Finito
  - Autômato com Pilha
  - Máquina e Turing

Axiomático

- **Associam-se regras às componentes da linguagem**
- **Regras**
  - permitem afirmar o que será verdadeiro
  - após a ocorrência de cada cláusula
  - considerando o que era verdadeiro antes da ocorrência
- **Formalismos axiomáticos**
  - Gramáticas Regulares
  - Gramáticas Livre do Contexto
  - Gramáticas Sensíveis ao Contexto
  - Gramáticas Irrestritas

- **Gramática também é dita um *Formalismo Gerador***
  - permite verificar se um determinado elemento da linguagem é *gerado*

Denotacional

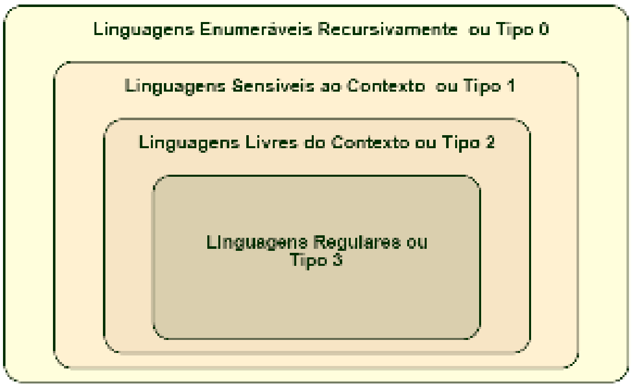
- **Ou *Formalismo Funcional***
- **Domínio (sintático)**
  - que permite a caracterização do conjunto de palavras admissíveis na linguagem
  - tratam-se de funções, as quais são, em geral, composicionais (horizontalmente)
    - o valor denotado por uma construção é especificado em termos dos valores denotados por suas subcomponentes

♦ Formalismo Denotacional

- Expressões Regulares
  - ∗ é simples inferir (*gerar*) aos elementos da linguagem
  - ∗ assim, freqüentemente também é denominado (de forma não muito precisa) como um Formalismo Gerador

♦ Hierarquia de Chomsky

- classifica as diversas classes de linguagens em uma ordem hierárquica
- inclusão própria entre as classes



Linguagens Formais e Autômatos

1 Revisão de Conceitos Básicos

2 Linguagens, Gramáticas e Reconhecedores

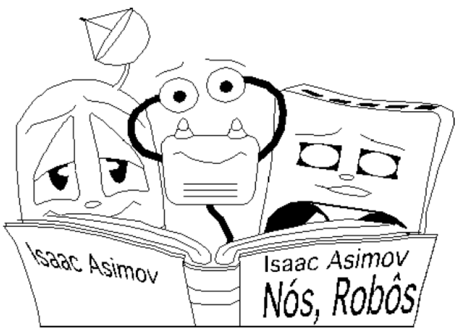
3 Linguagens Regulares
- Autômato Finito e Gramática Regular

4 Linguagens Livre do Contexto
- Autômato de Pilha e Gramática L. Contexto

5 Linguagens Enumeráveis Recursivamente
Máquina de Turing e Gramática Irrestrita

Cap. 1. Revisão de Conceitos Básicos
(livro do Paulo Blauth)

- **Conjuntos**
- **Relações**
- **Funções**
- **Lógica**



- **Técnicas de Demonstração**

1.1 Revisão: Conjuntos

- ***Conjunto* e *Elemento***
  - *Conjunto* é uma coleção de zero ou mais objetos distintos, denominados *Elementos* do conjunto.
  - número de elementos
    - finito
    - infinito

- conjunto finito
  - pode ser denotado por extensão
  - por exemplo, {a, b, c}
- conjunto vazio
  - sem elementos (ou seja, com zero elementos)
  - { } ou $\varnothing$
- conjunto (finito ou infinito) denotado por compreensão

$$\{ a \mid a \in A \text{ e } p(a) \} \quad \text{ou}$$

$$\{ a \in A \mid p(a) \} \quad \text{ou}$$

$$\{ a \mid p(a) \}$$

- $a \in A$, $a \notin A$
- $A \subseteq B$ ou $B \supseteq A$
  - * A *está contido* em B
  - * A é *subconjunto* de B
  - * B *contém* A
- $A \subset B$ ou $B \supset A$
  - * A *está contido propriamente* em B
  - * A é *subconjunto próprio* de B
  - * B *contém propriamente* A
- $A = B$
  - * $A \subseteq B$ e $B \subseteq A$

♦ *Exemplo*

- $a \in \{b, a\}$ e $c \notin \{b, a\}$;
- $\{a, b\} = \{b, a\}$, $\{a, b\} \subseteq \{b, a\}$ e $\{a, b\} \subset \{a, b, c\}$;
- Os seguintes conjuntos são infinitos
  - * $\mathbb{N}$ conjuntos dos números naturais
  - * $\mathbb{Z}$ conjuntos dos números inteiros
  - * $\mathbb{Q}$ conjuntos dos números racionais
  - * $\mathbb{I}$ conjuntos dos números irracionais
  - * $\mathbb{R}$ conjuntos dos números reais
- $\{1, 2, 3\} = \{x \in \mathbb{N} \mid x > 0 \text{ e } x < 4\}$
- $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$;
- conjunto dos números pares

$$\{y \mid y = 2x \text{ e } x \in \mathbb{N}\}$$

Operações sobre Conjuntos

- ***União***
  - $A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$
- ***Intersecção***
  - $A \cap B = \{x \mid x \in A \text{ e } x \in B\}$
- ***Diferença***
  - $A - B = \{x \mid x \in A \text{ e } x \notin B\}$
- ***Complemento***
  - definida em relação a um conjunto fixo $\mathbb{U}$ denominado *universo*
  - $A' = \{x \mid x \in \mathbb{U} \text{ e } x \notin A\}$
- ***Conjunto das Partes***
  - $2^A = \{S \mid S \subseteq A\}$

- ***Produto Cartesiano***
  - $A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}$
  - notação usual de $A \times A$: A^2
- ***Par ordenado***
  - elemento de um produto cartesiano
  - denotado na forma (a, b)
  - não deve ser confundido com o conjunto $\{a, b\}$
    - a ordem é importante
    - as duas componentes são distinguidas
    - conceito é generalizado para n-upla ordenada, ou seja, com $n > 0$ componentes

- *Exemplo*
  - universo $\mathbb{N}$, $A = \{0, 1, 2\}$ e $B = \{2, 3\}$
    - $A \cup B = \{0, 1, 2, 3\}$
    - $A \cap B = \{2\}$
    - $A - B = \{0, 1\}$
    - $A' = \{x \in \mathbb{N} \mid x > 2\}$
    - $2^B = \{\varnothing, \{2\}, \{3\}, \{2, 3\}\}$
    - $A \times B = \{(0, 2), (0, 3), (1, 2), (1, 3), (2, 2), (2, 3)\}$

Algumas Propriedades

- **Suponha universo $\mathbb{U}$ e conjuntos A, B e C**
  - *idempotência* da união e intersecção
    - $A \cup A = A$
    - $A \cap A = A$
  - *associatividade* da união e intersecção
    - $A \cup (B \cup C) = (A \cup B) \cup C$
    - $A \cap (B \cap C) = (A \cap B) \cap C$
  - *comutatividade* da união e intersecção
    - $A \cup B = B \cup A$
    - $A \cap B = B \cap A$

- *distributividade* da união e intersecção
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- relativamente ao *complemento*
  - $(A')' = A$
  - $A \cup A' = \mathbb{U}$
  - $A \cap A' = \varnothing$
- *leis de Morgan*
  - $(A \cup B)' = A' \cap B'$
  - $(A \cap B)' = A' \cup B'$

1.2 Revisão: Relações

- ***Relação***
  - subconjunto de um produto cartesiano
  - $R \subseteq A \times B$
- **Notações**
  - A é denominado *domínio*
  - B é denominado *contra-domínio* ou *codomínio*
  - $a R b$ denota $(a, b) \in R$
  - relação *em* A: $R \subseteq A \times A$
    - domínio e o contra-domínio coincidem
    - normalmente denotada por (A, R)

Propriedades das Relações

- **Sejam**
  - A um conjunto e R uma relação em A
- ***Reflexiva***
  - se, para todo $a \in A$, $a R a$
- ***Simétrica***
  - se $a R b$, então $b R a$
- ***Antissimétrica***
  - se $a R b$ e $b R a$, então $a = b$
- ***Transitiva***
  - se $a R b$ e $b R c$, então $a R c$
- **Importante**
  - uma relação pode *não* ser simétrica nem antissimétrica: não são noções complementares
  - uma relação pode *ser simultaneamente* simétrica e antissimétrica

---

- *Exemplo*
  - conjunto não vazio A
  - $(\mathbb{N}, \leq)$ e $(2^A, \subseteq)$
    - * reflexivas
    - * antissimétricas
    - * transitivas
  - $(\mathbb{Z}, <)$ e $(2^A, \subset)$
    - * transitivas
  - $(\mathbb{Q}, =)$
    - * reflexiva
    - * simétrica
    - * antissimétrica
    - * transitiva

Relação de Ordem (R em A)

- ***Relação de Ordem***
  - se é transitiva
- ***Relação de Ordem Parcial***
  - se é reflexiva, antissimétrica e transitiva
- ***Relação de Ordem Total***
  - se é uma relação de ordem parcial e
  - para todo $a, b \in A$, ou $a R b$ ou $b R a$
- **Exemplo: considere um conjunto não vazio A**
  - relação de ordem
    - $(\mathbb{N}, \leq)$, $(2^A, \subseteq)$, $(\mathbb{Z}, <)$, $(2^A, \subset)$ e $(\mathbb{Q}, =)$
  - relação de ordem parcial
    - $(\mathbb{N}, \leq)$, $(2^A, \subseteq)$ e $(\mathbb{Q}, =)$
  - relação de ordem total
    - $(\mathbb{N}, \leq)$

Relação de Equivalência (R em A)

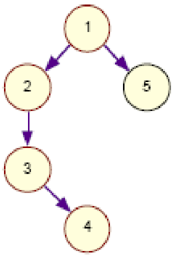
- ***Relação de Equivalência***
  - se for reflexiva, simétrica e transitiva
- **Importante resultado**
  - cada relação de equivalência induz um particionamento em *classes de equivalência*
    - particionamento do conjunto
    - em subconjuntos disjuntos e não vazios
- ***Exemplo***
  - $R = \{(a, b) \in \mathbb{N}^2 \mid a \text{ MOD } 2 = b \text{ MOD } 2\}$
  - MOD: resto da divisão inteira
  - R induz um particionamento de $\mathbb{N}$
    - subconjuntos dos pares (resto zero)
    - subconjuntos dos ímpares (resto um)

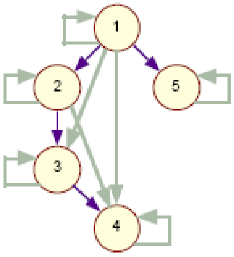
- **Freqüentemente**
  - desejável estender uma relação de forma a satisfazer determinado conjunto de propriedades
- ***Fecho de uma Relação***
  - R uma relação e P um conjunto de propriedades
  - *Fecho* de R em relação ao P
    - denotado por FECHO-P(R)
    - menor relação que contém R e que satisfaz às propriedades em P
- **Dois fechos importantes**
  - Transitivo
  - Transitivo e Reflexivo

- ***Fecho Transitivo***
  - P = {transitiva}
  - denotado por R^+ = FECHO-P(R)
  - definido como segue
    - se $(a, b) \in R$, então $(a, b) \in R^+$
    - se $(a, b) \in R^+$ e $(b, c) \in R^+$, então $(a, c) \in R^+$
    - os únicos elementos de R^+ são os construídos como acima
- ***Fecho Transitivo e Reflexivo***
  - P = {transitiva, reflexiva}
  - denotado por R^*, é tal que:
    - $R^* = R^+ \cup \{ (a, a) \mid a \in A \}$

◆ *Exemplo: Grafo (direto)*

- pode ser definido como uma
  - relação (binária) A (de arestas)
  - em um conjunto V (de vértices)
- A = {(1, 2), (2, 3), (3, 4), (1, 5)}
  - é um grafo em V = {1, 2, 3, 4, 5}
- A* = {(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4), (5, 5)}





1.3 Revisão: Funções

◆ ***Função Parcial***

- relação $f \subseteq A \times B$ tal que
  - se $(a, b) \in f$ e $(a, c) \in f$, então $b = c$
  - cada elemento do domínio está relacionado com, no máximo, um elemento do contra-domínio
- notação $f: A \to B$
- $f(a) = b$ denota $(a, b) \in f$
  - f está definida para a
  - b é *imagem* de a
- $\{b \in B \mid \text{existe } a \in A \text{ tal que } f(a) = b\}$
  - *conjunto imagem* de f
  - denotado por f(A) ou Img(f)

♦ *Função (Total)* ou *Aplicação*

- função parcial $f: A \to B$ onde
  - para todo $a \in A$ existe $b \in B$ tal que $f(a) = b$
- ou seja:
  - função parcial
  - definida para todos os elementos do domínio

♦ *Exemplo*

- *Adição nos naturais*
  - $ad: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tq $ad(a, b) = a + b$
  - função (total)
- *Divisão nos inteiros*
  - $div: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ tq $div(a, b) = a/b$
  - função parcial
  - não é definida para $(a, 0) \in \mathbb{Z} \times \mathbb{Z}$

♦ *Composição de Funções*

- Sejam $f: A \to B$ e $g: B \to C$ funções
- $g \circ f: A \to C$ tal que
  - $(g \circ f)(a) = g(f(a))$
  - aplicação da função f ao elemento a e, na seqüência, da função g à imagem $f(a)$

♦ *Exemplo*

- $ad: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- $quadrado: \mathbb{N} \to \mathbb{N}$ tq $quadrado(a) = a^2$
- $quadrado \circ ad: \mathbb{N}^2 \to \mathbb{N}$
  - $(quadrado \circ ad)(3, 1) =$
  - $quadrado(ad(3, 1)) =$
  - $quadrado(4) =$
  - 16

Tipos de Funções

- **Uma função $f: A \to B$ é**
- ***Injetora***
  - se, para todo $b \in B$, existe no máximo um $a \in A$ tal que $f(a) = b$
  - se cada elemento do contra-domínio é imagem de, no máximo, um elemento do domínio
- ***Sobrejetora***
  - se, para todo $b \in B$, existe pelo menos um $a \in A$ tal que $f(a) = b$
  - se todo elemento do contra-domínio é imagem de pelo menos um elemento do domínio
- ***Bijetora***
  - se é injetora e sobrejetora
  - se todo elemento do contra-domínio é imagem de exatamente um elemento do domínio

- *Exemplo*
  - inclusão: $\mathbb{N} \to \mathbb{Z}$ tq inclusão(a) = a é injetora
  - módulo: $\mathbb{Z} \to \mathbb{N}$ tq módulo(a) = $|a|$ é sobrejetora
  - $f: \mathbb{Z} \to \mathbb{N}$ tq
    - $f(a) = 2a$ se $a \geq 0$
    - $f(a) = |2a| - 1$ se $a < 0$
    - é bijetora

Cardinalidade de Conjuntos

- *Cardinalidade*
  - de um conjunto
  - é uma medida de seu tamanho
  - definida usando funções bijetoras
  - de um conjunto A, é representada por #A
- *Cardinalidade Finita*
  - se existe uma bijeção de A com
    - $\{1, 2, 3, ..., n\}$, $n \in \mathbb{N}$
    - $\#A = n$
  - ou seja
    - é possível representar por extensão
- *Cardinalidade* **Infinita**
  - se existe uma bijeção entre A com
    - um subconjunto próprio de A
  - ou seja
    - retirando elementos de A
    - pode-se estabelecer uma bijeção com A

- *Exemplo*
  - $f: \mathbb{Z} \rightarrow \mathbb{N}$ tal que
    - $f(a) = 2a$ se $a \geq 0$
    - $f(a) = |2a| - 1$ se $a < 0$
    - é bijetora
  - $\mathbb{N}$ é subconjunto próprio de $\mathbb{Z}$
  - então $\mathbb{Z}$ é infinito
- **Importante**
  - nem todos os conjuntos infinitos possuem a mesma cardinalidade
  - cardinal do conjunto dos números naturais $\mathbb{N}$
    - denotado por $\aleph_0$
    - $\aleph$ ("alef") é a primeira letra do alfabeto hebráico

- ***Conjunto Contável* ou *Contavelmente Infinito***
  - se existe uma bijeção
    - com um subconjunto infinito de $\mathbb{N}$
    - denominada *Enumeração* de A
  - um conjunto é contável
    - pode-se enumerar seus elementos
    - como uma seqüência na forma a_0, a_1, a_2, ...
  - cardinal de qualquer conjunto contável
    - $\aleph_0$
- ***Conjunto (Infinito) Não-Contável***
  - caso contrário
- ***Exemplo***
  - $\mathbb{Z}$ e $\mathbb{Q}$ são contáveis
  - $\mathbb{I}$ e $\mathbb{R}$
    - são não-contáveis
    - cardinal é $2^{\aleph_0}$

1.4 Revisão: Lógica

- **Lógica Booleana**
  - o estudo dos princípios e métodos usados para distinguir sentenças verdadeiras de falsas
- ***Proposição***
  - sentença declarativa
  - possui valor lógico
    - *verdadeiro*
    - *falso*
  - usualmente denotados por V e F
- ***Proposição Sobre*** $\mathbb{U}$
  - considere um conjunto universo $\mathbb{U}$
  - proposição cujo valor lógico depende de $x \in \mathbb{U}$
  - usualmente denotada por p(x)

- p sobre $\mathbb{U}$
  - induz uma partição de $\mathbb{U}$ em duas classes de equivalências
    - {x | p(x) é verdadeira}: *conjunto verdade* de p
    - {x | p(x) é falsa}: *conjunto falsidade* de p
- ***Tautologia***
  - se p(x) é V para qq $x \in \mathbb{U}$
- ***Contradição***
  - se p(x) é F para qq $x \in \mathbb{U}$
- ***Exemplo***
  - $3 + 4 > 5$ é uma *proposição*
  - para a proposição $n! < 10$ sobre $\mathbb{N}$
    - {0, 1, 2, 3} é o *conjunto verdade*
    - $\{n \in \mathbb{N} \mid n > 3\}$ é o *conjunto falsidade*
  - $n + 1 > n$ sobre $\mathbb{N}$ é uma *tautologia*
  - "2n é ímpar" sobre $\mathbb{N}$ é uma *contradição*

- ***Operador***
  - função da forma $op: A^n \to A$
- ***Operador Lógico* ou *Conetivo***
  - operador sobre o conjunto das proposições $\mathbb{P}$
- ***Proposição Atômica* ou *Átomo***
  - proposição que não contém conetivos
- ***Tabela Verdade***
  - descreve os valores lógicos de uma proposição
  - em termos das possíveis combinações dos valores lógicos das proposições componentes

♦ Operadores Lógicos

- Operador $\neg$ *Negação*
- Operador $\wedge$ *E*
- Operador $\vee$ *Ou*
- Operador $\rightarrow$ *Se-Então*
- Operador $\leftrightarrow$ *Se-Somente-Se*

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
V	V	F	V	V	V	V
V	F	F	F	V	F	F
F	V	V	F	V	V	F
F	F	V	F	F	V	V

♦ Operadores $\rightarrow$ e $\leftrightarrow$ induzem

- Relação de Implicação
- Relação de Equivalência

♦ *Relação de Implicação*

- $\Rightarrow$
- $\{(p, q) \in \mathbb{P}^2 \mid p \rightarrow q$ é uma tautologia$\}$

♦ *Relação de Equivalência*

- $\Leftrightarrow$
- $\{(p, q) \in \mathbb{P}^2 \mid p \leftrightarrow q$ é uma tautologia$\}$

♦ $\Rightarrow$ e $\Leftrightarrow$

- $\Rightarrow$ é relação de ordem
- $\Leftrightarrow$ é relação de equivalência

♦ *Exemplo*

- $p \Rightarrow p \vee q$
- $p \wedge q \Rightarrow p$

p	q	$p \vee q$	$p \to (p \vee q)$	$p \wedge q$	$(p \wedge q) \to p$
V	V	V	V	V	V
V	F	V	V	F	V
F	V	V	V	F	V
F	F	F	V	F	V

- $p \to q \Leftrightarrow \neg q \to \neg p$

$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$	$p \to q \leftrightarrow \neg q \to \neg p$
F	F	V	V	V
F	V	F	F	V
V	F	V	V	V
V	V	V	V	V

♦ **Exemplo**

- $p \to q \Leftrightarrow (p \wedge \neg q) \to F$

p	q	$\neg q$	$p \to q$	$p \wedge \neg q$	$p \to q \leftrightarrow (p \wedge \neg q) \to F$
V	V	F	V	F	V
V	F	V	F	V	V
F	V	F	V	F	V
F	F	V	V	F	V

1.4 Revisão: Técnicas de Demonstração

- ***Teorema***
  - proposição $p \rightarrow q$
    - prova-se ser uma tautologia
    - ou seja, $p \Rightarrow q$
  - p: hipótese
  - q: tese
- ***Corolário***
  - teorema que é uma conseqüência quase direta de um outro já demonstrado
  - ou seja, cuja prova é trivial ou imediata
- ***Lema***
  - teorema auxiliar que possui um resultado importante para a prova de um outro

---

- **Hipótese e Tese**
  - antes de iniciar uma demonstração deve-se identificar claramente
    - hipótese
    - tese
- ***Exemplo***
  - hipótese e tese?

    $\cap$ distribui-se sobre a $\cup$, ou seja,
    $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - reescrita identificando a hipótese e a tese

    se A, B *e* C *são conjuntos quaisquer,*
    então $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

- **Teorema na forma $p \leftrightarrow q$**
  - $p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \land (q \rightarrow p)$
  - demonstra-se
    - "ida" ($\rightarrow$)
    - "volta" ($\leftarrow$)
- *Exemplo*

A é contável sse
existe uma função bijetora entre A e o
conjunto dos números pares

- "ida" e "volta"

se um conjunto A é contável,
então existe uma função bijetora entre A e o
conjunto dos números pares

e

se existe uma função bijetora entre A e o
conjunto dos números pares,
então A é contável

- **Algumas técnicas para demonstrar um teorema $p \rightarrow q$**
  - direta
  - contraposição
  - redução ao absurdo
  - indução

Prova Direta

- **Técnica**
  - supor a hipótese é V
  - a partir da hipótese provar que a tese é V
- ***Exemplo***
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - lembre-se que
    - $X = Y$ sse $X \subseteq Y$ e $Y \subseteq X$
    - $X \subseteq Y$ sse todos os elementos de X também são elementos de Y
  - é fácil verificar que
    - $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$
  - Para provar que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
    - $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$
    - $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$

- **Prova Direta**
  - *Caso 1:* $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
    - Suponha que $x \in A \cap (B \cup C)$

      $x \in A \cap (B \cup C) \Rightarrow$

      $x \in A \wedge x \in (B \cup C) \Rightarrow$

      $x \in A \wedge (x \in B \vee x \in C) \Rightarrow$

      $(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \Rightarrow$

      $x \in (A \cap B) \vee x \in (A \cap C) \Rightarrow$

      $x \in (A \cap B) \cup (A \cap C)$
    - Portanto, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$
  - *Caso 2:* $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$
    - Suponha que $x \in (A \cap B) \cup (A \cap C)$

      $x \in (A \cap B) \cup (A \cap C) \Rightarrow$

      $(x \in (A \cap B)) \vee (x \in A \cap C) \Rightarrow$

      $(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \Rightarrow$

      $x \in A \wedge (x \in B \vee x \in C) \Rightarrow$

      $x \in A \wedge x \in (B \cup C) \Rightarrow$

      $x \in A \cap (B \cup C)$
    - Portanto, $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.
  - Logo, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Prova por Contraposição

- **Técnica**

$$p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$$

- *Exemplo*

$$n! > n + 1 \rightarrow n > 2$$

  - pode-se, equivalentemente, demonstrar por contraposição que

$$n \leq 2 \rightarrow n! \leq n + 1$$

  - prova de que $n \leq 2 \rightarrow n! \leq n$?
    - é suficiente testar para $n = 0$, $n = 1$ e $n = 2$

Prova por Redução ao Absurdo

- **Técnica**

$$p \rightarrow q \Leftrightarrow (p \wedge \neg q) \rightarrow F$$

  - supor a hipótese p
  - supor a negação da tese $\neg q$
  - concluir uma contradição
    - em geral, $q \wedge \neg q$

- **Prova por Contra-Exemplo**
  - em uma demonstração por absurdo
    - construção da contradição $q \wedge \neg q$
    - apresentação de um *contra-exemplo*

- *Exemplo*

0 é o único elemento neutro da adição em $\mathbb{N}$

  - reescrevendo na forma de $p \rightarrow q$

se 0 é elemento neutro da adição em $\mathbb{N}$, então 0 é o único elemento neutro da adição em $\mathbb{N}$

Prova por Absurdo

- suponha que 0 é o neutro da adição em $\mathbb{N}$
- suponha que não é o único
- seja e um neutro da adição em $\mathbb{N}$ tq $e \neq 0$
- como 0 é neutro
  - para qualquer $n \in \mathbb{N}$ tem-se que $n = 0 + n$
  - em particular, para $n = e$, tem-se que $e = 0 + e$
- como e é elemento
  - para qualquer $n \in \mathbb{N}$, tem-se que $n = n + e$
  - em particular, para $n = 0$, tem-se que $0 = 0 + e$
- portanto
  - como $e = 0 + e$ e $0 = 0 + e$, tem-se que $e = 0$
  - contradição!!! pois foi suposto que $e \neq 0$
- Logo, é absurdo supor que o elemento neutro da adição em $\mathbb{N}$ não é único

Prova por Indução

Importante

- é usada com freqüência
- é usada em proposições que dependem de $\mathbb{N}$

Princípio da Indução Matemática

- seja $p(n)$ uma proposição sobre $\mathbb{N}$
- $p(0)$ é V
- se, para qualquer $k \in \mathbb{N}$, $p(k) \to p(k + 1)$ então, para qualquer $n \in \mathbb{N}$, $p(n)$ é V

Nomenclatura

- $p(0)$: *base de indução.*
- $p(k)$: *hipótese de indução*
- $p(k) \to p(k + 1)$: *passo de indução*

♦ Técnica

- demonstrar a base de indução $p(0)$
- fixado um k, supor V a hipótese de indução $p(k)$
- demonstrar o passo de indução
- na realidade
  - * o princípio da indução matemática pode ser aplicado a qualquer proposição que dependa de um conjunto para o qual exista uma bijeção com os naturais

♦ *Exemplo*

para qualquer $n \in N$ *tq* $n \geq 0$, *tem-se que*

$$1 + 2 + \ldots + n = (n^2 + n)/2$$

♦ Prova por Indução

- ***Base de Indução***

  Seja $n = 0$. Então:

  $(0^2 + 0)/2 = (0 + 0)/2 = 0/2 = 0$

  Portanto, $1 + 2 + \ldots + n = (n^2 + n)/2$ é V para $n = 0$

- ***Hipótese de Indução***

  Suponha que, para algum n fixo tq $n \geq 0$

  $1 + 2 + \ldots + n = (n^2 + n)/2$

- ***Passo de Indução***.

  Prova para $1 + 2 + \ldots + n + (n + 1)$

  $1 + 2 + \ldots + n + (n + 1) =$

  $(1 + 2 + \ldots + n) + (n + 1) =$

  $(n^2 + n)/2 + (n + 1) =$

  $(n^2 + n)/2 + (2n + 2)/2 =$

  $(n^2 + n + 2n + 2)/2 =$

  $((n^2 + 2n + 1) + (n + 1))/2 =$

  $((n + 1)^2 + (n + 1))/2$

  Portanto, $1 + 2 + \ldots + (n + 1) = ((n + 1)^2 + (n + 1))/2$

- Logo, para qq $n \in \mathbb{N}$ tq $n \geq 0$, tem-se que

  $1 + 2 + \ldots + n = (n^2 + n)/2$

- **Princípio da Indução Matemática × Definições**
  - o princípio da indução matemática pode ser usado para definições
  - é dita *indutivamente definida*
  - ou *recursivamente definida*
  - exemplo
    - definição de Fecho

Cap. 2 Linguagens, Gramáticas e Reconhecedores

- ***Definição: Símbolo, Caractere***
  - entidades abstratas básica
  - não definida formalmente
- ***Exemplo: Símbolo***
    - letras
    - dígitos
- ***Definição: Alfabeto***
  - conjunto *finito* de símbolos
- ***Exemplo: Alfabeto***
  - $\Sigma_1 = \{a, b, c\}$
  - $\Sigma_2 = \{0, 1, ..., 9\}$
  - $\Sigma_3 = \{\ \}$

♦ *Definição: Palavra, Cadeia de Caracteres, Sentença*

- sobre um alfabeto
- seqüência finita de símbolos justapostos

♦ *Exemplo: Palavra*

- a, abcb são palavras sobre {a, b, c}
- ε
  - palavra vazia - sem símbolos
  - é palavra sobre qualquer alfabeto

♦ *Definição: Tamanho, Comprimento* de uma palavra

- número de símbolos que compõem a palavra
- representação
  - $|w|$
  - w denota uma palavra

♦ *Exemplo: Tamanho de uma palavra*

- $|abcb| = 4$
- $|\varepsilon| = 0$

♦ *Definição: Concatenação*

- operação binária, definida sobre uma linguagem
- palavra formada pela justaposição das palavras
- notação
  - * justaposição dos símbolos que representam as palavras componentes
- satisfaz às seguintes propriedades:
  - * associatividade: $v(wt) = (vw)t$
  - * elemento neutro (esq/dir): $\varepsilon w = w = w\varepsilon$

♦ *Exemplo: Concatenação*

- para $v = ab$ e $w = cd$
  - * $vw = abcd$

♦ *Definição: Prefixo, Sufixo, Subpalavra*

- prefixo (sufixo)
  - * qq seqüência de símbolos inicial (final) de uma palavra
- subpalavra
  - * qq seqüência de símbolos contígüa de uma palavra

♦ *Exemplo: para a palavra* abcb

- prefixos: ε, a, ab, abc, abcb
- sufixos: ε, b, cb, bcb, abcb
- prefixos e sufixos são subpalavras

♦ *Definição: Concatenação Sucessiva*

- concatenação sucessiva de uma palavra com ela mesma
- indefinida para ε^0

w^n : concatenação sucessiva de w, por ela mesma, onde *n* indica o numero de concatenações.

♦ *Exemplo: Concatenação Sucessiva*

- w^3 = www
- w^1 = w
- a^5 = aaaaa
- a^n = aaa...a (a repetido n vezes)
- $w^0 = \varepsilon$ para $w \neq \varepsilon$

Definição: Produto de Conjunto de Palavras

Sejam V e W conjuntos de palavras sobre Σ.

$$VW = \{vw \mid v \in V \text{ e } w \in W\}$$

Exemplo:

Σ = {0, 1, 2, 3} V = {00, 11} W = {222, 333}

VW = {00222, 00333, 11222, 11333}

VV = V^2 = {0000, 0011, 1100, 1111}

$V^0 = \{\varepsilon\}$, por definição

V^3 = {000000, ..., 111111}

V^4 = {00000000, ..., 1^8}

Definição: Fechamento de Kleene

Seja W um conjunto de palavras sobre Σ

$W^* = \bigcup_{i \geq 0} W^i$

$W^* = W^0 \cup W^1 \cup W^2 \cup W^3 \ldots$

Conjunto de todas as concatenações possíveis de W, incluindo ε.

Exemplos:

V = {00, 11} V^* = { ε, 00, 11, 0011, 1100, 1111, 000000, ...}

Σ = {0, 1} Σ^* = {ε, 0, 1, 00, 01, 11, 000, 001, 01, 011, ...}

Definição: Fechamento Positivo.

Seja W um conjunto de palavras sobre Σ,

$W^+ = \bigcup_{i \geq 1} W^i \rightarrow$ igual a W^*, exceto ε.

$W^+ = W^1 \cup W^2 \cup W^3 \ldots$

Conjunto de todas as concatenações possíveis de W, excluindo ε.

Exemplos:

V = {00, 11} V^+ = {00, 11, 0000, 0011, 1100, 1111, 000000, ...}

Σ = {0, 1} Σ^+ = {0, 1, 00, 11, 01, 10, 0000, ...}

- ***Definição: Linguagem Formal***

Uma Linguagem L é um conjunto de palavras sobre um alfabeto Σ, ou seja, $L \subset \Sigma^*$.

- ***Exemplo: Ling. Formal sobre Σ = {a, b}***
  - conjunto vazio
  - conjunto formado pela palavra vazia
    - note-se que { } ≠ {ε}
  - conjunto das palíndromos
    - palavras que têm a mesma leitura da esquerda para a direita e vice-versa
    - linguagem infinita
    - ε, a, b, aa, bb, aaa, aba, bab, bbb, aaaa,... são palíndromos

Como representar uma linguagem formal L?

Se L é finito, basta listar todas as palavras.

Se L é infinito, existem 2 formalismos principais:

- ***Formalismo Gerador: Gramática***
- ***Formalismo Reconhecedor: Autômato***

♦ ***Definição: Gramática***

$G = (V, T, P, S)$:

- V
  - conjunto finito de símbolos
  - *variáveis* ou *não-terminais*
- T
  - conjunto finito de símbolos
  - *terminais*
  - disjunto de V
- P
  - conjunto finito de pares (α, β)
  - *regra de produção*
  - α é palavra de $(V \cup T)^+$
  - β é palavra de $(V \cup T)^*$
- S
  - elemento de V
  - *variável inicial*

♦ **Notação de (α, β)**

- $\alpha \rightarrow \beta$
- notação abreviada para $\alpha \rightarrow \beta_1, \ldots, \alpha \rightarrow \beta_n$
  - $\alpha \rightarrow \beta_1 \mid \ldots \mid \beta_n$

- ***Definição: Derivação***
  - $G = (V, T, P, S)$ uma gramática
  - *Derivação* é um par da relação denotada por $\Rightarrow$
    - com domínio em $(V \cup T)^+$
    - contra-domínio em $(V \cup T)^*$
    - representação de forma infixada

$$\alpha \Rightarrow \beta$$

  - $\Rightarrow$ é indutivamente definida
  - para qq produção $S \rightarrow \beta$
    - S é o símbolo inicial

$$S \Rightarrow \beta$$

  - para qq par $\alpha \Rightarrow \beta$
    - onde $\beta = \beta_u \beta_v \beta_w$
    - se $\beta_v \rightarrow \beta_t$ é regra de P então

$$\beta \Rightarrow \beta_u \beta_t \beta_w$$

- **Portanto, derivação**
  - substituição de uma subpalavra de acordo com uma regra de produção

- **Sucessivos Passos de Derivações**
  - $\Rightarrow^*$
    - fecho transitivo e reflexivo da relação $\Rightarrow$
    - zero ou mais passos de derivações sucessivos
  - $\Rightarrow^+$
    - fecho transitivo da relação $\Rightarrow$
    - um ou mais passos de derivações sucessivos
  - $\Rightarrow^i$
    - exatos i passos de derivações sucessivos
    - i é número natural

Gramática é um formalismo

- Axiomático
- de Geração
  - permite derivar ("gerar") todas as palavras da linguagem que representa

Definição: Linguagem Gerada

- $G = (V, T, P, S)$ uma gramática
- *Linguagem Gerada* por G'

$$L(G) \text{ ou } GERA(G)$$

- todas as palavras de símbolos terminais deriváveis a partir do símbolo inicial S

$$L(G) = \{w \in T^* \mid S \Rightarrow^+ w\}$$

Exemplo: números naturais

- $G = (V, T, P, S)$
  - $V = \{S, D\}$
  - $T = \{0, 1, 2,..., 9\}$
  - $P = \{S \to D, S \to DS, D \to 0 \mid 1 \mid ... \mid 9\}$
- uma derivação do número 243

$$S \Rightarrow DS \Rightarrow 2S \Rightarrow 2DS \Rightarrow 24S \Rightarrow 24D \Rightarrow 243$$

- portanto

$$S \Rightarrow^* 243$$

$$S \Rightarrow^+ 243$$

$$S \Rightarrow^6 243$$

- logo GERA(G)
  - o conjunto dos números naturais

♦ *Definição: Equivalência de Gramáticas*

- G_1 e G_2 são equivalentes sse

$$GERA(G_1) = GERA(G_2)$$

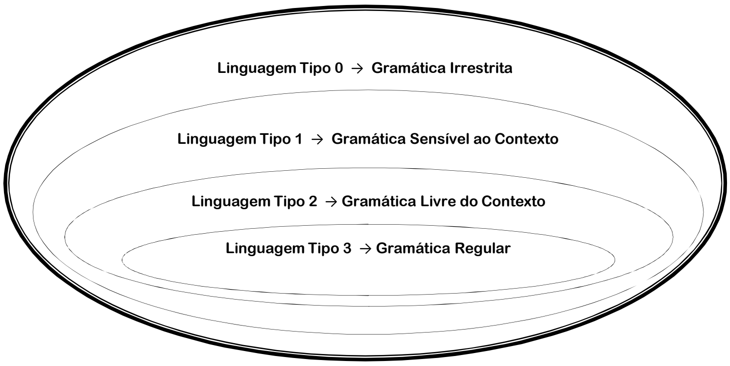
♦ Convenções:

- A, B, C,..., S, T símbolos variáveis
- a, b, c,..., s, t símbolos terminais
- u, v, w, x, y, z palavras de símbolos terminais
- α, ß,... palavras de símbolos variáveis e/ou terminais

Definição: Hierarquia de Chomsky

Define 4 tipos de gramática:

- •Gramática tipo 3 (regular):
- •Gramática tipo 2 (livre de contexto):
- •Gramática tipo 1 (sensíveis ao contexto):
- •Gramática tipo 0 (irrestrita):



Gramática tipo 3 (regular):

G = (V, T, P, S) é do tipo 3, se toda produção em P é da forma:

$A \to wB$ ou $A \to Bw$ ou $A \to w$ com $A \in V$, $B \in V$ e $w \in T^*$, ou seja:

Uma variável à esquerda e no máximo uma variável à direita (a variável a direita não pode ser precedida e sucedida ao mesmo tempo por terminais).

Ex1. Seja G1 = (V, T, P, S) com:

$V = \{S, A, B\}$
$T = \{a,b\}$
$P = \{S \to aA, A \to bB|\varepsilon, B \to aA\}$

Derivações

$S \Rightarrow a\underline{A} \Rightarrow a$ ou $S \overset{2}{\Rightarrow} a$ ou $S \overset{*}{\Rightarrow} a$ ou $S \overset{+}{\Rightarrow} a$

$S \Rightarrow a\underline{A} \Rightarrow ab\underline{B} \Rightarrow aba\underline{A} \Rightarrow aba$

Linguagem Gerada

L(G1) = {a, aba, ababa, abababa, ….}
L(G1) = {w є {a,b}* | w tem prefixo "a" seguido de 0 ou mais ba's}

Hierarquia: Tipo 3 ou Regular

Ex2.

Seja G2 = (V, T, P, S) com:

$V = \{S\}$
$T = \{a,b\}$
$P = \{S \to Sba \mid a\}$

Derivações

$S \Rightarrow a$

$S \Rightarrow \underline{S}ba \Rightarrow aba$

$S \Rightarrow \underline{S}ba \Rightarrow \underline{S}baba \Rightarrow \underline{S}bababa \Rightarrow abababa$

Linguagem Gerada

L(G2) = {a, aba, ababa, abababa, ….}
L(G2) = {w є {a,b}* | w tem prefixo "a" seguido de 0 ou mais ba's}

Portanto, a gramática do exemplo 2 gera exatamente a mesma linguagem da gramática do exemplo 1. Nesse caso, dizemos que as gramáticas são equivalentes.

Hierarquia: Tipo 3 ou Regular

Gramática tipo 2 (livre de contexto):

G = (V, T, P, S) é do tipo 2 se toda regra em P é da forma:

$$A \rightarrow \alpha, \quad \text{com} \quad A \in V \ \text{e} \ \alpha \in (V \cup T)^*,$$

ou seja, basta ter <u>uma variável à esquerda.</u>

Ex3.

Seja G3 = (V, T, P, S) com:

V = {S, B}

T = {0,1}

P = {S → 0B | 0SB, B → 1 }

Derivações

$S \Rightarrow 0\underline{B} \Rightarrow 01$

$S \Rightarrow 0\underline{S}B \Rightarrow 00\underline{B}B \Rightarrow 001\underline{B} \Rightarrow 0011$

Linguagem Gerada

$L(G3) = \{01, 0011, 000111, \ldots, 0^{100}1^{100}, \ldots\}$

L(G3) = {w ε {0,1}* | w possui N 0's concatenados com N 1's, para N ≥ 1}

$L(G3) = \{w \in \{0,1\}^* \mid w = 0^N1^N, N \geq 1\}$

Hierarquia: Tipo 2 ou Livre de Contexto

Ex4.

Seja G_4 = (V, T, P, S) com:

V = {S,Z,U}

T = {0,1}

P = {S → ε | Z | U | 0SZ | 1SU, Z→0, U→1}

Derivações

$S \Rightarrow \varepsilon$ $\quad S \Rightarrow Z \Rightarrow 0$ $\quad S \Rightarrow U \Rightarrow 1$

$S \Rightarrow 0\underline{S}Z \Rightarrow 01\underline{S}UZ \Rightarrow 01UUZ \Rightarrow 01110$

Linguagem Gerada

$L(G_4) = \{\varepsilon, 0, 1, 00, 11, 000, 010, 101, 111, 0000, 0110, 1001, 1111, \ldots\}$

$L(G_4)$ = {w ε {0,1}* | w é uma palíndrome}

Hierarquia: Tipo 2 ou Livre de Contexto

Ex5.

Seja G_5 = (V, T, P, E) com:

V = {E}
T = {+,*,(,),x}
P = {E → E+E | E*E | (E) | x}

Derivações

Linguagem Gerada

Hierarquia: Tipo 2 ou Livre de Contexto

Gramática tipo 1 (sensíveis ao contexto):

G = (V, T, P, S) é tipo 1 se P é da forma:

$S \rightarrow \varepsilon$ ou $\alpha \rightarrow \beta$, com $|\beta| \geq |\alpha|$, $\alpha \in (V \cup T)^*$ e $\beta \in (V \cup T)^+$

Existe uma forma normal dessa gramática, de onde deriva o nome da mesma, onde P é da forma:

$S \rightarrow \varepsilon$ ou

$\alpha A \varphi \rightarrow \alpha \beta \varphi$, sendo $\alpha \in (V \cup T)^*$, $\varphi \in (V \cup T)^*$ e $\beta \in (V \cup T)^+$

Dizemos que a variável A é substituída por β, no contexto α A φ.

Ex6.

Seja G_6 = (V, T, P, S) com:

V = {S, X, Y, A, B, C, D, E, F}
T = {a,b}
P = { S → XY | aa | bb | ε,
X → XaA | XbB | aaC | abD | baE | bbF,
Aa → aA, Ab → bA, AY → Ya, Ba → aB, Bb → bB, BY → Yb,
Ca → aC, Cb → bC, CY → aa, Da → aD, Db → bD, DY → ab,
Ea → aE, Eb → bE, EY → ba, Fa → aF, Fb → bF, FY → bb}

Ex7.

Seja G_7 = (V, T, P, S) com:

V = {S, C}
T = {a, b, c}
P = {S → abc | ε, ab → aabbC, Cb → bC, Cc → cc}

Derivações

S ⇒ ε   S ⇒ abc   S ⇒ abc ⇒ aabbCc ⇒ aabbcc

S ⇒ abc ⇒ aabbCc ⇒ aabbcc ⇒ aaabbCbcc ⇒ aaabbbCcc ⇒ aaabbbccc

Linguagem Gerada

$L(G_7)$ = {ε, abc, aabbcc, aaabbbccc, ….}

$L(G_7) = \{w \in \{a,b,c\}^* \mid w = a^N b^N c^N, N \geq 0\}$

Hierarquia: Tipo 1 ou Sensível ao Contexto

Gramática tipo 0 (irrestrita):

G = (V, T, P, S) é uma gramática sem nenhuma restrição adicional em P, apenas:

$\alpha \rightarrow \beta$, sendo $\alpha \in (V \cup T)^+$ e $\beta \in (V \cup T)^*$, conforme vimos na definição geral de gramática.

Ex8.

Seja G_8 = (V, T, P, S) com:

V = {S, A, B, C, D, E}
T = {a}
P = {S → ACaB, Ca → aaC, CB → DB | E, aD → Da, AD → AC,
aE → Ea, AE → ε}

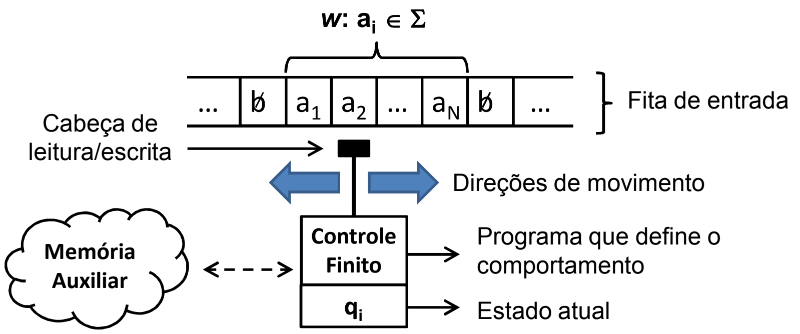
Definição: Reconhecedor de Linguagem

Um reconhecedor de uma linguagem ***L*** é a representação de um procedimento que quando apresentado a uma cadeia ***w***, após um número finito de passos:

- Pára e responde **SIM**, se a cadeia ***w*** pertença a ***L***.
- Caso ***w*** não pertença a ***L***:

    1. Ele pára e responde **NÃO.**
    2. Ele não pára.

Simbolicamente:



Uma configuração do reconhecedor é:

(a) estado de controle finito
(b) conteúdo da fita de entrada e posição da cabeça
(c) conteúdo da memória

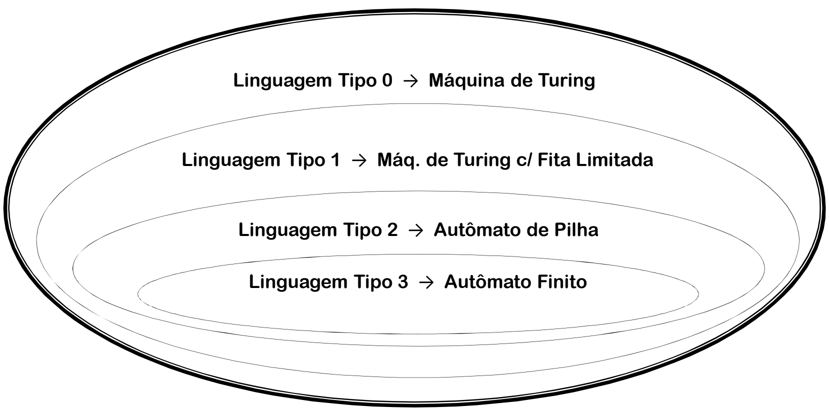
Um reconhecedor aceita (ou reconhece) ***w*** se:

- (i) Partindo de uma configuração inicial;
- (ii) faz seqüência finita de movimentos;
- (iii) e termina numa configuração final.

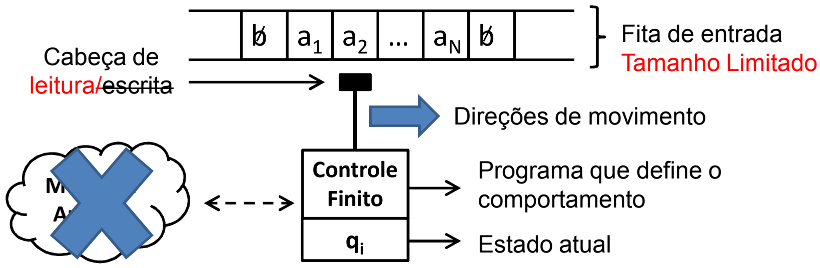
Linguagem aceita por um reconhecedor ***R***:

$$L(R) = \{w \in \Sigma^* \mid R \text{ aceita } w\}$$

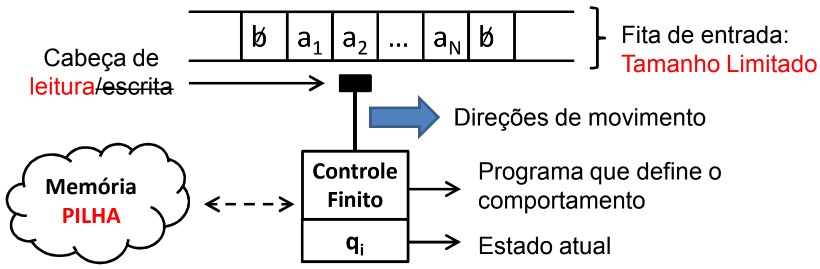
Hierarquia de Chomsky e Reconhecedores



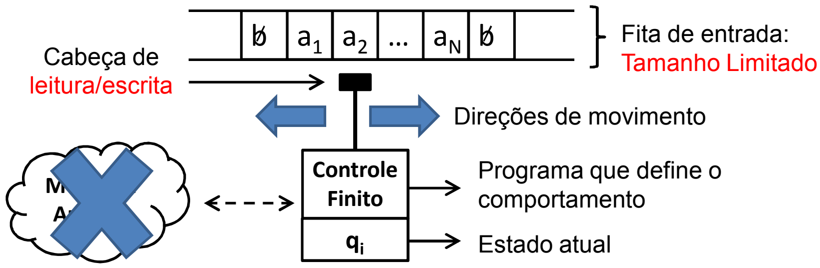
Autômato Finito (Ling. Tipo 3):



Autômato de Pilha (Ling. Tipo 2):



Máquina de Turing com Fita Limitada (Ling. Tipo 1):



Máquina de Turing (Ling. Tipo 0):