Aspectos Formais da Computação

Prof. Sergio D. Zorzo
Departamento de Computação - UFSCar
1º semestre / 2017
Aula 02

Linguagens Formais e Autômatos

Introdução e Conceitos Básicos

- Conjuntos, Relações e Funções
- Lógica
- Técnicas de Demonstração
  - Indução

Introdução

Teoria das Linguagens Formais

Originária da década de 1950 - desenvolver teorias relacionadas com as linguagens naturais

Hoje - importante para o estudo de linguagens artificiais em especial, para as linguagens da Ciência da Computação

Aspectos considerados:

Léxicos **Sintáticos** **Semânticos**

em linguagens de programação

em modelos de sistemas biológicos

em desenho de hardware

relacionamentos com linguagens naturais

Sintaxe e Semântica

Historicamente

- o problema sintático foi reconhecido antes do problema semântico
- foi o primeiro a receber um tratamento adequado
- são de tratamento mais simples que os semânticos

Conseqüência

- grande ênfase à sintaxe
- ao ponto de levar à idéia de que questões das linguagens de programação resumiam-se às questões da sintaxe

Atualmente

- teoria da sintaxe possui construções matemáticas bem definidas e universalmente reconhecidas como as Gramáticas de Chomsky.

Sintaxe e Semântica

Linguagem de Programação (ou qq modelo matemático)
pode ser vista livremente sem qualquer significado associado juntamente com uma interpretação do seu significado

Sintaxe

- trata das propriedades livres da linguagem ("forma“)

exemplo: verificação gramatical de programas

Semântica

- fornece uma interpretação para a linguagem

exemplo: um significado ou valor para um determinado programa

Consequências

- sintaxe basicamente manipula símbolos

não considera os correspondentes significados mas, para resolver qualquer problema real é necessário dar uma interpretação semântica aos símbolos

exemplo: "estes símbolos representam os inteiros"

Sintaticamente "errado"

não existe uma noção de programa "errado“. neste caso, simplesmente não é um programa

Sintaticamente "Correto"

pode não ser o programa que o programador esperava escrever

Programa "Correto" ou "Errado"

deve considerar se modela adequadamente o comportamento desejado

Consequências

Limites entre Sintaxe e Semântica

nem sempre são claros

exemplo: ocorrência de um nome em um programa pode ser tratado como um problema sintático ou semântico

entretanto, para a maioria dos problemas relevantes a distinção entre sintaxe e semântica em linguagens artificiais é, em geral, óbvia

exemplo: um significado ou valor para um determinado programa

Abordagem
Operacional, Axiomático ou 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

Denotacional

Domínio (sintático)

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) os elementos da* linguagem

Denominado como um Formalismo Gerador

Linguagens Formais e Autômatos

Linguagens Regulares

Origens: Formalismos Autômato Finito e Expressões Regulares

- estudos biológicos de redes de neurônios
- circuitos de chaveamentos

Mais recentemente

- analisadores léxicos (parte de um compilador / identifica e codifica as unidades básicas de uma linguagens como variáveis, números, etc)
- editores de textos
- sistemas de pesquisa e atualização em arquivos
- linguagens de comunicação homem-máquina (como protocolos de comunicação)

Linguagens Formais e Autômatos

Linguagens Livre do Contexto

Formalismos

Gramáticas Livre do Contexto

Autômato com Pilha

Ênfase do estudo - analisadores sintáticos

historicamente desenvolvimento de analisadores sintáticos era um problema complexo, de difícil depuração e com eficiência relativamente baixa

- hoje, considerando o conhecimento já adquirido relativo às Linguagens Livre do Contexto desenvolvimento de um analisador sintático é simples (assim como a sua depuração) - somente uma pequena percentagem do tempo de processamento de um compilador é gasto em tal atividade.

Linguagens Formais e Autômatos

Linguagens Enumeráveis Recursivamente e Sensíveis ao Contexto

Formalismos

- Máquina de Turing e variações/restrições
- Gramáticas Irrestritas e Sensíveis ao Contexto

Exploram

limites da capacidade de desenvolvimento de reconhecedores ou geradores de linguagens

ou seja

estuda a solucionabilidade do problema da existência de algum reconhecedor ou gerador para determinada linguagem.

Linguagens Formais e Autômatos

Hierarquia de Classes de Linguagens

Hierarquia de Chomsky

classifica as diversas classes de linguagens em uma ordem hierárquica (inclusão própria)

Conjuntos, Relações e Funções

Conjuntos

Conjunto é uma coleção de zero ou mais objetos distintos, denominados *Elementos do conjunto.*

Notações

$a \in A$, $a \notin A$

$A \subseteq B$ 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 $B \subseteq A$

Conjuntos

número de elementos

- finito
- infinito

conjunto finito

- pode ser denotado por extensão. Ex: {a, b, c}

conjunto vazio

- sem elementos (ou seja, com zero elementos) { } ou $\varnothing$

conjunto (finito ou infinito) denotado por compreensão

- { a | a $\in$ A e p(a) } ou
- { a $\in$ A | p(a) } ou
- { a | p(a) }

Exemplos

$a \in \{b, a\}$ 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

N conjuntos dos números naturais

Z conjuntos dos números inteiros

Q conjuntos dos números racionais

I conjuntos dos números irracionais

R conjuntos dos números reais

$\{1, 2, 3\} = \{ x \in N \mid x > 0 \text{ e } x < 4\}$

$N = \{ x \in Z \mid x \geq 0 \}$;

conjunto dos números pares

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

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 U denominado *universo*

$A' = \{x \mid x \in U \text{ e } x \notin A\}$

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)

Operações sobre Conjuntos

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 (n componentes)

Exemplo : universo N, A = {0, 1, 2} e B = {2, 3}

$A \cup B = \{0, 1, 2, 3\}$

$A \cap B = \{2\}$

$A - B = \{0, 1\}$

$A' = \{ x \in N \mid x > 2 \}$

$2^B = \{\varnothing, \{2\}, \{3\}, \{2, 3\} \}$

$A \times B = \{(0, 2), (0, 3), (1, 2), (1, 3), (2, 2), (2, 3)\}$

Algumas Propriedades

Suponha universo 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*

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

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

Algumas Propriedades

Suponha universo U e conjuntos A, B e C

- relativamente ao *complemento*

  $(A')' = A$

  $A \cup A' = U$

  $A \cap A' = \varnothing$

- *leis de Morgan*

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

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

Relações

Relação

subconjunto de um produto cartesiano

$R \subseteq A \times B$

Notações

A é denominado *domínio*

B é denominado *contra-domínio ou codomínio*

aRb 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

Considere A um conjunto e R uma relação em A

Reflexiva

se, para todo a $\in$ A, aRa

Simétrica

se aRb, então bRa

Antissimétrica

se aRb e bRa, então a=b

Transitiva

se aRb e bRc, então aRc

Importante :

uma relação pode *não ser simétrica nem* antissimétrica: não são noções complementares

uma relação pode *ser simultaneamente simétrica e* antissimétrica

Propriedades das Relações

Exemplo - conjunto não vazio A

$(N, \leq)$ e $(2^A, \subseteq)$

- reflexivas
- antissimétricas
- transitivas

$(Z, <)$ e $(2^A, \subset)$

- transitivas

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

- não é reflexiva
- não é simétrica
- não é antissimétrica
- não é 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 aRb ou bRa

Exemplo: considere um conjunto não vazio A

- relação de ordem (N, ≤), (2^A, $\subseteq$), (Z, <), (2^A, $\subset$)
- relação de ordem parcial (N, ≤), (2^A, $\subseteq$)
- relação de ordem total (N, ≤)

Relação de Equivalência

se for reflexiva, simétrica e transitiva

Importante:

cada relação de equivalência induz um particionamento em *classes de equivalência (* particionamento do conjunto em subconjuntos disjuntos e não vazios)

Exemplo

$R = \{ (a, b) \in N^2 \mid a \text{ MOD } 2 = b \text{ MOD } 2\}$

(MOD: resto da divisão inteira)

R induz um particionamento de N

subconjuntos dos pares (resto zero)

subconjuntos dos ímpares (resto um)

Fecho de uma Relação R em relação a um propriedade P

denotado por FECHO-P(R)

menor relação que contém R e que satisfaz às propriedades em P

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:

$R^* = R^+ \cup \{ (a, a) \mid a \in A \}$

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 contradomínio

notação $f: A \rightarrow B$

$f(a) = b$ denota $(a, b) \in f$

f está definida para a

b é *imagem de a*

$\{ b \in B \mid$ existe $a \in A$ tal que $f(a) = b \}$

conjunto imagem de f

denotado por f(A) ou Img(f)

Funções

Função (Total) ou Aplicação

função parcial f: A $\rightarrow$ B onde

para todo a $\in$ A existe b $\in$ B tal que f(a) = b

ou seja, é uma função parcial, definida para todos os elementos do domínio

Exemplos

Adição nos naturais

ad: N×N $\rightarrow$ N tq ad(a, b) = a + b

ad é uma função (total)

Divisão nos inteiros

div: Z×Z $\rightarrow$ Z tq div(a, b) = a/b

div é uma função parcial (não é definida para (a, 0) $\in$ Z×Z)

Funções

Composição de Funções

Sejam $f: A \rightarrow B$ e $g: B \rightarrow C$ funções

$g \bullet f: A \rightarrow C$ tal que

$(g \bullet f)(a) = g(f(a))$

aplicação da função f ao elemento a e, na seqüência, da função g à imagem f(a)

Exemplo

$ad: N \times N \rightarrow N$

$quadrado: N \rightarrow N$ tq $quadrado(a) = a^2$

$quadrado \bullet ad: N^2 \rightarrow N$

$(quadrado \bullet ad)(3, 1) = quadrado(ad(3, 1)) = quadrado(4) = 16$

Tipos de Funções **função f: A → B é**

Injetora

se, para todo b ∈ B, existe no máximo um a ∈ 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 ∈ B, existe pelo menos um a ∈ 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

Tipos de Funções **função f: A → B é**

Injetora

Ex: inclusão: N → Z tq inclusão(a) = a é injetora

Sobrejetora

Ex: módulo: Z → N tq módulo(a) = |a| é sobrejetora

Bijetora

Ex: Z → N tq

f(a) = 2a se a ≥ 0

f(a) = |2a|-1 se a < 0 é bijetora

Cardinalidade de Conjuntos

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}, $n \in N$

#A = n

Cardinalidade Infinita

se existe uma bijeção entre A com um subconjunto próprio de A

Ex: f: $Z \rightarrow N$ tal que

f(a) = 2a se $a \geq 0$ e f(a) = |2a|-1 se $a < 0$ é bijetora

N é subconjunto próprio de Z então Z é infinito

Nem todos os conjuntos infinitos possuem a mesma cardinalidade

Cardinalidade do conjunto dos números naturais N é denotado por $\aleph_0$ - $\aleph_0$ ("alef" zero)

Conjunto Contável ou Infinatamente Contável

se existe uma bijeção com um subconjunto infinito de N
denominada *Enumeração de A*

Conjunto é contável

pode-se enumerar seus elementos

como uma seqüência na forma a0, a1, a2, ...

cardinalidade de qualquer conjunto contável é $\aleph_0$

Conjunto (Infinito) Não-Contável

caso contrário

Exemplos

Z é um conjunto contável

R é não-contável - cardinalidade $2^{\aleph_0}$

Lógica - Lógica Booleana

o estudo dos princípios e métodos usados para distinguir sentenças verdadeiras de falsas

Proposição

sentença declarativa

possui valor lógico (*verdadeiro ou falso)*

usualmente denotados por V e F

Proposição sobre U (conjunto universo U)

proposição cujo valor lógico depende de x $\in$ U

p sobre U

induz uma partição de 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 $x \in U$

Contradição

se p(x) é F para qq $x \in U$

Ex: 3 + 4 > 5 é uma *tautologia*

para a proposição n! < 10 sobre N

{0, 1, 2, 3} é o *conjunto verdade*

$\{n \in N \mid n > 3\}$ é o *conjunto falsidade*

A proposição n + 1 > n sobre N é uma *tautologia*

"2n é ímpar" sobre N é uma *contradição*

Operador em Lógica : função da forma op: $A^n \rightarrow A$

Operador Lógico ou Conetivo

operador sobre o conjunto das proposições 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

Operadores Lógicos

Operador $\neg$ *Negação*

Operador $\wedge$ *E*

Operador $\vee$ *Ou*

Operador $\rightarrow$ *Se-Então*

Operador $\leftrightarrow$ *Se-Somente-Se*

Técnicas de Demonstração

Teorema

proposição p → q prova-se ser uma tautologia

p: hipótese e q: tese (antes de iniciar uma demonstração deve-se identificar claramente quem é a hipótese e quem é a 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

Ex: : ∩ *distribui-se sobre a* ∪*, 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 $p \leftrightarrow q$

$p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$

- demonstra-se "ida" ($\rightarrow$) e "volta" ($\leftarrow$)

Ex:

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

Ex:

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

lembre-se que

$X = Y$ sse $X \subseteq Y$ e $Y \subseteq X$

$X \subseteq Y$ sse todos os elementos de X tb. 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 $x \in A \cap (B \cup C)$

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

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

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

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

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

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

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

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

Ex:

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

pode-se, equivalentemente, demonstrar por contraposição que $n \leq 2 \rightarrow n! \leq n + 1$

prova de que $n \leq 2 \rightarrow n! \leq n + 1$?

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*

Ex: *0 é o único elemento neutro da adição em N*

reescrevendo na forma de $p \rightarrow q$

se 0 é elemento neutro da adição em N,

então 0 é o único elemento neutro da adição em N

Prova por Absurdo

suponha que 0 é o neutro da adição em N

suponha que não é o único

seja e esse elemento neutro da adição em N tq $e \neq 0$

como 0 é neutro

para qualquer $n \in N$ tem-se que $n = 0 + n$

em particular, para $n = e$, tem-se que $e = 0 + e$

como e é elemento

para qualquer $n \in N$, 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 N não é único

Indução

Prova por Indução

é usada com freqüência

é usada em proposições que dependem de N

Princípio da Indução Matemática

seja p(n) uma proposição sobre N

p(0) é V

se, para qualquer $k \in N$, $p(k) \rightarrow p(k + 1)$ então, para qualquer $n \in N$, p(n) é V

Nomenclatura

p(0): *base de indução.*

p(k): *hipótese de indução*

$p(k) \rightarrow p(k + 1)$: *passo de indução*

Prova por 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

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

Base de Indução

Seja n = 0. Então: $(0^2 + 0)/2 = (0 + 0)/2 = 0/2 = 0$

Portanto, $1 + 2 + ... + n = (n^2 + n)/2$ é Verdade para n = 0

Hipótese de Indução

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

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

Passo de Indução.

Prova para $1 + 2 + ... + n + (n + 1)$

$1 + 2 + ... + n + (n + 1) = (1 + 2 + ... + n) + (n + 1) =$

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

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

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

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

Logo, para qq $n \in N$ tq $n \geq 0$, tem-se que $1+2+... +n = (n^2 + n)/2$

Fim