CT-200 Fundamentos de Linguagens Formais e Automata Aula 01 - Introdução

Segunda Aula

(updated just now by *YourName*)

Propriedades de Relações

Partições

Seja A={1,2,3,...,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:

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

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

$B_i \cap B_j = \emptyset$

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

$\mathcal{B}$ é então uma partição de A e cada B_i é um bloco de A.

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: $\forall\ x,\ y \in X,\ xRy \rightarrow yRx$
3 - Transitiva: $\forall\ x,\ y,\ z \in X,\ xRy \text{ e } yRz \rightarrow xRz$

Se R é uma relação de equivalência, a classe de equivalência contendo x é:
$R[x] = \{y | y \in X \text{ e } xRy\}$

Uma relação de equivalência em X particiona X em classes de equivalência disjuntas.
1 - Suponha que $x \in R[y]$ e $x \in R[z]$.

2 - Isso implica que yRx e que zRx.

3 - Pela propriedade simétrica de R, temos que xRz.

4 - Pela propriedade transitiva de R, temos que $yRx,\ xRz \rightarrow yRz \Rightarrow y \in R[z]$.

5 - Assim $R[y] \subset R[z]$.

6 - De forma análoga, obtemos que $R[z] \subset R[y]$.

7 - A partir de (5) e (6) conclui-se que $R[y] = R[z]$

8 - Pela propriedade reflexiva, $\forall\ x,\ x \in R[x]$, ou seja, a partição cobre todo o conjunto X.

O ranque de R é o número de classes de equivalência.

Composição de relações

$R_1 \subset X{\times}Z,\ R_2 \subset Z{\times}Y$

$x(R_1 R_2)y \Leftrightarrow \exists\ z \in Z,\ xR_1 z\ \text{ e }\ zR_2 y$

Fechamento da composição de relações no caso de funções

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

f é função $A \to B$
g é função $B \to C$

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

Equivale provar que
$(x,\ y) \in h$ e $(x,\ z) \in h \to y = z$

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

$(x,\ l) \in f\ \text{ e }\ (x,\ k) \in f\ \text{ e f é função }\ \to l = k$
$(k,\ y) \in g\ \text{ e }\ (l,\ z) = (k,\ z) \in g\ \text{ e g é função }\ \to y = z$

Propriedades em potencial de relações

Para relações podem ou não ocorrer as seguintes propriedades:

1. reflexiva: $\forall\ x \in S,\ xRx$
2. antissimétrica: $\forall\ x,\ y \in S,\ xRy \wedge yRx \Rightarrow x = y$
3. transitiva: $\forall\ x,\ y,\ z \in S,\ xRy \wedge yRz \Rightarrow xRz$
4. comparabilidade: $\forall\ x,\ y \in S,\ xRy \vee yRx$
5. simétrica:$\forall\ x,\ y \in S,\ xRy \Rightarrow yRx$

Para operações, as seguintes propriedades podem ou não ocorrer:

1. associativa: $\forall\ x,\ y,\ z,\ \in S,\ x \circ (y \circ z) = (x \circ y) \circ z$
2. elemento neutro ou identidade: $\exists\ |e \in S,\ \forall\ x \in S,\ x \circ e = e \circ x = x$
3. existência do inverso:$\forall\ x \in S,\ \exists\ y \in S,\ x \circ y = y \circ x = e$
4. comutativa: $\forall\ x,\ y \in S,\ x \circ y = y \circ x$
5. distributiva à esquerda: $\forall\ x,\ y,\ z \in S x \circ (y \otimes z) = (x \circ y) \otimes (x \circ z)$
6. distributiva à direita: $\forall\ x,\ y,\ z \in S (y \otimes z) \circ x = (y \circ x) \otimes (z \circ x)$

> Exercício: mostrar que o elemento neutro, se existe, é único.
>
> Exercício: qual o inverso do elemento neutro?

Ordenação

Um sistema $< P, \leq >$ 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:
$< 2^{\{1,2,3\}}, \subset >$ - ordem parcial
$< \mathbb{Z}, \leq >$ - ordem total

Fechos de Relações

Seja $R \subset S \times S$.
Fecho transitivo de R é R^+, definido por
1) $aRb \to aR^+b$
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 $R^\star$ de R:
$R^+ \cup \{(a, a) | a \in S\}$

Exemplo R={(1,2),(2,2),(2,3)} e S={1,2,3}
$R^+ = \{(1, 2), (2, 2), (2, 3), (1, 3)\}$
$R^\star = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$

Cardinalidade de Conjuntos Infinitos

Cardinalidade (geral)

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

Pode-se dizer que os dois conjuntos são equivalentes (cardinalidades iguais definem classes de equivalências entre 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 pra o qual existe uma correspondência com o conjunto dos números naturais
$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Dize-se que sua cardinalidade é $\aleph_0$

Exemplo

Seja $\mathbb{N}^\star = \{1, 2, 3, \ ...\}$ o conjunto dos naturais positivos e E o conjunto dos naturais positivos pares.
Mostre que ambos possuem o mesmo tamanho.

> Determinar f(n)=2n
>
> Mostrar que f é injetora e sobrejetora (de $\mathbb{N}$ em E)
> f(a)=2a
> f(b)=2b
>
> Se $a \neq b \Rightarrow 2a \neq 2b \Rightarrow f(a) \neq f(b)$
>
> Seja x elemento de E, $\frac{x}{2}$ é um natural positivo, então $f\left(\frac{x}{2}\right) = x$.

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

Exemplo - números racionais

$\mathbb{Q}^+$ são os racionais positivos
$\mathbb{Q}^+ = \left\{\frac{m}{n} | m, \ n \in \mathbb{N}^+\right\}$

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

> Encontre uma função (enumeração) que associe a cada elemento de $\mathbb{Q}$, um de $\mathbb{N}$.

Construir uma matriz com $\frac{i}{j}$, onde i é a linha e j é a coluna

$$\begin{pmatrix} \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \ldots \\ \frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \ldots \\ \frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \ldots \\ \frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \ldots \\ \frac{5}{1} & \ldots & & & & \end{pmatrix}$$

Escrever os elementos da matriz na forma de lista, percorrendo na diagonal, pulando elementos repetidos.

$$\left(\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{1}{3}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{5}{1}, \frac{1}{5}, \ \ldots\right)$$

Exemplo - números reais

Mostrar que $\mathbb{R}$ é incontável.

Prova por contradição.

Supor $f : \mathbb{N} \rightarrow \mathbb{R}$ uma correspondência. (condição necessária e suficiente para $\mathbb{R}$ ser contável)

Encontrar $x \in \mathbb{R},\ x \neq n,\ \forall\ n \in \mathbb{N}$, considerar caso $0 < x < 1$, assim podemos escrever x na forma

0,DDDDDD.... onde D é um dígito de 0 a 9

Por exemplo, o início de uma enumeração poderia ser
f(1)=0,100100100... (dízima periódica)
f(2)=0,31415926 ... (pi dividido por 10)
f(3)=0,44444444.... (dízima periódica)
f(4)=0,000500000 ... (racional)
...

Vamos construir o número real x de forma que o j-ésimo dígito de x é diferente do j-ésimo dígito de f(j), assim garantimos que x é diferente de todos os demais números.

Assim, x é construído diferente de f(1), f(2), f(3), f(4) porque o dígito j o faz diferente de f(j).
Escolhemos arbitrariamente os dígitos de 1 a 4 desde que respeitem a regra dada e sejam diferentes de 0 e 9.
0,4256...

Como x é um número real, então, por hipótese, deve haver uma enumeração f(n)=x pra ele.
Entretanto, por construção, o n-ésimo dígito de x deve ser diferente do n-ésimo dígito de f(n) e portanto $x \neq f(n)$, o que nos leva a uma contradição.

Assim, a hipótese de que os números reais são enumeráveis é absurda.

Noção da cardinalidade de $\mathbb{R}$

Vamos encontrar uma bijeção entre o intervalo $[0,\ 1]$ e o conjunto $2^{\mathbb{N}}$.

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

$r = 0,\ d_1 d_2 d_3 d_4 \ldots$

São infinitos dígitos d_i com valor 0 ou 1.

Cada dígito corresponde a um número natural.

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

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

> Exercício:
>
> O conjunto $\mathbb{N} \times \mathbb{N}$ é enumerável.
>
> O conjunto $2^{\mathbb{N}}$ não é conjunto enumerável.
>
> A cardinalidade do intervalo [0,1] é igual à cardinalidade de $\mathbb{R}$.

Estruturas de dados

Seqüências

(7,21,57) - tupla (no caso uma 3-tupla ou tripla), seqüência finita.

(2,4,6,8,10,...) - seqüência infinita.

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

Grafos

Um grafo G=(V,E) é uma tupla onde
V é um conjunto de vértices e
$E \subset V \times V$ é o conjunto de arestas que conectam 2 vértices. (uma relação)

Exemplo
V={1,2,3,4,5}
E={(1,2),(2,3),(3,4),(4,5),(5,1)}

Exemplo (desconexo)
V={1,2,3,4,5}
E={(n,m) | n+m=4 ou n+m=7}

> Desenhar os grafos representando os vértices por círculos e as arestas por cenexões entre círculos.

Definições

sub-grafo: subconjunto de V e de E que também é um grafo.

caminho: seqüência de vértices $v_1, v_2 ... v_k, k \geq 1$ tais que existam as arestas, isto é, $(v_i, v_{i+1}) \in E$ com $1 \leq i < K$. O comprimento do caminho é k-1.

ciclo: caminho com $v_1 = v_k$

árvore: grafo sem ciclos

Conectividade

Um grafo é conexo se existe caminho de um vértice a qualquer outro

> Utilizar o fecho de E para obter a conectividade

Grafos disjuntos: não existe caminho para dois nós escolhidos.

Grafo direcionado (digrafo)

Pares ordenados $v_1 \mapsto v_2$ formam as arestas ou arcos.

Exemplo $G = (\{1, 2, 3, 4\}, \{i \mapsto j | i < j\})$

Exemplo:
$V = \{1, 2, 3, 4, 5, 6\}$
$E = \{(1 \mapsto 2), (1 \mapsto 5), (2 \mapsto 1), (2 \mapsto 4), (5 \mapsto 4), (5 \mapsto 6), (6 \mapsto 1), (6 \mapsto 3)\}$

Grau de um vértice é o número de arestas ligadas ao vértice.
Grau de entrada do nó (fan-in) é o número de arcos destinados ao nó.
Grau de saída do nó (fan-out) é o número de arcos originados no nó.

Árvore com raiz e indução de direções

A escolha de um vértice como raiz na ´rvore induz um direcionamento das arestas, representando a relação "é filho de".

Árvore binária: máximo número de filhos por nó é 2.
Os filhos podem ser ordenados: filho à esquerda e filho à direita.

Tipos de Demonstração

Demonstração por construção

Teorema: para qualquer número par n>2 existe um grafo formado por apenas n vértices de grau 3

Prova: Construa um grafo G=(V,E) da seguinte maneira:
V={0,1,....,n-1}
E={ {i,i+1} para $0 < i \leq n - 1$} $\cup$ { {n-1,0}} $\cup$ { {i,i+n/2} para $0 \leq i \leq \frac{n}{2} - 1$}

> Desenhe o grafo e verifique.

Demonstração por contradição

Teorema: $\sqrt{2}$ é irracional

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

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

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

4 - $m = 2k$ com k inteiro

5 - Substituindo m=2k
$2n^2 = (2k)^2 = 4k^2$
$n^2 = 2k^2$

6 - n é portanto par.

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

8 - $\sqrt{2}$ não pode ser racional.

Demonstração por indução

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

a) demonstro P(0)

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

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 em ambos os lados

$$\sum_{i=0}^{n} i^2 = \frac{2n^3 - 2n^2 - n^2 - n + 6n^2}{6} = \frac{2n^3 + 3n^2 + n}{6} = \frac{n(2n^2 + 3n + 1)}{6} = \frac{n(2n+1)(n+1)}{6}$$

Termos usados

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 de 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
assumir verdadeiro: $n^3 - n + 3 = 3k$

$$(n+1)^3 - (n+1) + 3 = n^3 + 3n^2 + 2n + 3 = n^3 - n + 3 + \left(n^2 + n\right)3 = 3k + 3l = 3(k+l)$$

Linguagens

Cadeias de Símbolos e Linguagens

Strings, cadeias ou fitas: são seqüências finitas de símbolos.

Símbolos são entidades primitivas.

Alfabeto é um conjunto de símbolos
$\Sigma_1 = \{0, 1\}$
$\Sigma_2 = \{a, b, c, d, e, \ldots, z\}$

Uma string de um alfabeto Σ é uma seqüência finita de símbolos do alfabeto Σ.

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

Se w é uma cadeia o comprimento de w é escrito $|w|$ e é o número de símbolos que w contém.

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

Substring z de w se z aparece de forma consecutiva dentro de w.

cad é substring de abracadabra.

$w = w_1 w_2 w_3 \ldots w_n,\ w_i \in \Sigma$

Concatenação de $x = x_1 x_2 \ldots x_n$ e $y = y_1 y_2 \ldots y_m$ é
$xy = x_1 x_2 \ldots x_n y_1 y_2 \ldots y_m$

Concatenação múltipla de x com si próprio
$x^k = xxx \ldots x$ k vezes.

Ordem lexicográfica:
"ordem do dicionário", strings mais curtas precedem strings mais longas
$(\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots)$

Linguagens

Linguagem é o conjunto de strings sobre um alfabeto

$\emptyset$ é uma linguagem

$\{\varepsilon\}$ é uma linguagem

> Qual a diferença entre as duas?

O conjunto dos palíndromos no alfabeto {0,1} é uma linguagem
$\{\varepsilon, 0, 1, 00, 11, 000, 101, 010, 111, \ldots\}$

O conjunto de todas as strings sobre o alfabeto Σ é designada por $\Sigma^\star$.

Para $\Sigma = \{a\}$, $\Sigma^\star = \{\varepsilon, a, aa, aaa, \ldots\}$

Para $\Sigma = \{0, 1\}$, $\Sigma^\star = ?$

Definição

i) $\varepsilon \in \Sigma^\star$
ii) Se $w \in \Sigma^\star$ e $a \in \Sigma$, então $wa \in \Sigma^\star$
iii) $w \in \Sigma^\star$ 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 $\Sigma^\star$.

Concatenação de Strings

Sejam u e $v \in \Sigma^\star$. A concatenação uv é uma operação binária definida em $\Sigma^\star$ da seguinte forma.
i) Se $|v| = 0 \Rightarrow uv = u$
ii) Seja v de comprimento n > 0. $v = wa$, onde w é string de tamnho n-1 e $a \in \Sigma$, e $uv = (uw)a$

Concatenação é associativa, com elemento neutro ε.

Reverso

$u^R = (u_{v\_}(n-1) \dots u_1)$ onde $u = (u_1 u_2 \dots u_n)$

Definição recursiva:
i) Se $|u| = 0 \Rightarrow u^R = \varepsilon$
ii) Se $|u| = n > 0$, então $u = wa$ para alguma string w, $|w| = n-1$ e $a \in \Sigma$ e $u^R = a w^R$.

Propriedade: $(uv)^R = v^R u^R$

> Demonstração:
> Base da Indução
> $|v| = 0 \Rightarrow v = \varepsilon,\ (uv)^R = u^R$
> Analogamente, $v^R u^R = \varepsilon u^R = u^R$
>
> Passo indutivo:
> $|v| = n+1$, provar $(uv)^R = v^R u^R$
> $v = wa,\ |w| = n \text{ e } a \in \Sigma$
> $(uv)^R = (u(wa))^R = ((uw)a)^R = a(uw)^R = a(w^R u^R) = (aw^R)u^R = (wa)^R u^R = v^R u^R$.

Especificações finitas de linguagens

Expressão lógica

$L_1 = \{x \in \Sigma_1^\star \mid x = wa,\ w \in \Sigma_1^\star,\ a \in \{1, 3, 5, 7, 9\}\},\ \Sigma_1 = \{0, 1, 2, 3, \dots, 9\}$

Representação recursiva

$\Sigma_2 = \{a, b\}$ - Strings de comprimento par começando por a.

(i) aa e ab $\in L_2$
(ii) Se $u \in L_2$, então $uaa,\ uab,\ uba$ e $ubb \in L_2$
(iii) $u \in L_2$ apenas se pode ser obtida a partir dos elementos de (i) por um número finito de aplicações de (ii)

Exemplo

$\Sigma_3 = \{a, b\}$ - Cada b é imediatamente precedido por um a.

(i) $\varepsilon \in L_3$
(ii) $u \in L_3 \Rightarrow ua,\ uab \in L_3$
(iii) $u \in L_3$ 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
$XY = \{uv | u \in X \text{ e } v \in Y\}$

A concatenação de X consigo n vexes 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

$$X^\star = \bigcup_{i=0}^{\infty} X^i$$

$$X^+ = \bigcup_{i=1}^{\infty} X^i$$

Notar que $X^+ = XX^\star$

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

X^+ não contém o ε

Reverso da linguagem

$X^R = \{u^R | u \in X\}$

Representação da lingaugem 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 pelo menos um b
{a}{a,b}*{b}{a,b}*{a}

Cadeias sobre {a,b} começando com aa ou terminando com bb
{aa}{a,b}* U {a,b}*{bb}

Cadeias sobre {a,b} de comprimento par.
{aa,bb,ab,ba}*