Autómatos e Linguagens Formais

M. Lurdes Teixeira
Dep. Matemática
Univ. Minho

2º semestre de 2020/2021

Definições elementares

- Chama-se alfabeto a um conjunto finito e não vazio.
- Os elementos do alfabeto designam-se letras.
- Uma palavra sobre um alfabeto A é uma sequência finita, possivelmente vazia, de letras.
- A sequência vazia designa-se palavra vazia e representa-se por ε.

EXEMPLO 1

- Se o alfabeto é $A = \{a, b, c\}$, então a , b e c são letras e ε, a, b, ba, aa, $aabcaa$ são exemplos de palavras sobre A.

- Se o alfabeto é $A = \{0, 1\}$, então 0 e 1 são letras e ε, 1, 0, 11, 0101, 0001 são exemplos de palavras sobre A.

Nota: duas palavras sobre um alfabeto A são iguais se as sequências de letras são iguais.

Chama-se definição indutiva de um conjunto X a uma colecção de regras que permite descrever X, indicando um processo de construir os seus elementos. As regras podem ser de vários tipos:

- regras básicas, que indicam que certos objectos pertencem ao conjunto;
- regras indutivas, que permitem construir elementos de X a partir de outros elementos de X já conhecidos;
- regra de fecho, regra única em cada definição, que estabelece que os elementos de X são os construídos a partir da utilização das regras básicas e das indutivas um número finito de vezes.

regra básica $\longmapsto$ $\underbrace{s \in X}_{\text{conclusão}}$

regra indutiva $\longmapsto$ se $\underbrace{s_1, \ldots, s_n \in X}_{\text{condição}}$ então $\underbrace{s \in X}_{\text{conclusão}}$

O conjunto de todas as palavras sobre A representa-se por A^* e o conjunto de todas as palavras não vazias é $A^+ (= A^* \setminus \{\varepsilon\})$.

Definição indutiva de A^*

Dado um alfabeto A,

1. $\varepsilon \in A^*$,
2. se $u \in A^*$ e $a \in A$, então $ua \in A^*$.

Definição indutiva de A^+

Dado um alfabeto A,

1. para cada $a \in A$, $a \in A^+$,
2. se $u \in A^+$ e $a \in A$, então $ua \in A^+$.

Definição

Seja A um alfabeto. Em A^* (A^+) define-se a operação concatenação como sendo a operação $\cdot$ que a palavras $u = a_1 \ldots a_m$ e $v = b_1 \ldots b_n$, com $m, n \in \mathbb{N}_0$, associa a palavra $u \cdot v = a_1 \ldots a_m b_1 \ldots b_n$.

Nota: Entende-se que se $m = 0$ ($n = 0$), então $u = \varepsilon$ e $u \cdot v = v$ ($v = \varepsilon$ e $u \cdot v = u$, resp.).

Proposição

Se A é um alfabeto, então a concatenação em A^* goza das seguintes propriedades:

- é associativa: $u \cdot (v \cdot w) = (u \cdot v) \cdot w,$ para $u,\ v,\ w \in A^*$;
- admite elemento neutro que é ε:
  $u \cdot \varepsilon = \varepsilon \cdot u = u,$ para qualquer $u \in A^*$;
- é válida a lei do corte à direita e à esquerda: dadas palavras $u, v, w \in A^*$,

$$\begin{array}{ll} u \cdot v = u \cdot w \Rightarrow v = w & \text{(lei do corte à esquerda)} \\ v \cdot u = w \cdot u \Rightarrow v = w & \text{(lei do corte à direita).} \end{array}$$

NOTAS:

- A operação de concatenação de palavras é também designada por produto e representada por $\cdot$, que vulgarmente se omite.

- Como a operação concatenação é associativa, a estrutura algébrica $(A^+, \cdot)$ é um semigrupo, nomeadamente, é o semigrupo livre gerado por A.

- Como a palavra vazia ε é um elemento neutro em A^*, conclui-se que a estrutura $(A^*, \cdot)$ é um monóide, nomeadamente, é o monóide livre gerado por A.

- Notar que a concatenação não é comutativa:

$$\text{se } A = \{a, b\},\ u = aa \text{ e } v = bb, \text{ então } uv \neq vu.$$

Teorema da Recursão Estrutural

Considere-se uma definição indutiva determinista de um conjunto X. Então existe e é única a função $f : X \to Y$ tal que:

1. para cada regra básica da forma '$s \in X$', existe um valor $y_s \in Y$ e $f(s) = y_s$;
2. para cada regra indutiva da forma 'se $s_1, \ldots s_n \in X$, então $s \in X$', existe um valor $y_s \in Y$, calculado de forma explícita a partir dos valores $f(s_1), \ldots, f(s_n)$, e $f(s) = y_s$.

A definição de uma função por aplicação do teorema anterior diz-se uma definição recursiva da função.

Falaremos do comprimento de uma palavra u de A^* como sendo o comprimento da sequência de letras u. Tal número representa-se por $|u|$.

Definição recursiva do comprimento de uma palavra

O comprimento de uma palavra $u \in A^*$ é a imagem de u pela função $|\_| : A^* \to \mathbb{N}_0$ definida por:

1. $|\varepsilon| = 0$;
2. $|wa| = |w| + 1$, para quaisquer $w \in A^*$ e $a \in A$.

Falaremos também do número de ocorrências de uma letra a numa palavra u de A^*, valor que se representa por $|u|_a$.

Definição recursiva do número de ocorrências de uma letra

Se A é um alfabeto e $a \in A$, o número de ocorrências de a em $u \in A^*$ é a imagem de u pela função $|\_|_a : A^* \to \mathbb{N}_0$ definida por:

1. $|\varepsilon|_a = 0$;
2. $|wx|_a = \begin{cases} |w|_a + 1 & \text{se } x = a \\ |w|_a & \text{se } x \neq a \end{cases}$, para quaisquer $w \in A^*$ e $x \in A$.

EXEMPLO 2

Sejam $A = \{0, 1\}$ e $u = 001110101011$.

- $|u| = |00111010101| + 1 = |0011101010| + 1 + 1 = \ldots = 12.$
- $|u|_0 = |00111010101|_0 = |0011101010|_0 = |001110101|_0 + 1 = \ldots = 5.$
- $|u|_1 = |00111010101|_1 + 1 = |0011101010|_1 + 1 + 1 = |001110101|_1 + 1 + 1 = \ldots = 7.$

Proposição

Sejam A um alfabeto e $u, v \in A^*$. Então,

- $|uv| = |u| + |v|$,
- $|uv|_a = |u|_a + |v|_a$, para qualquer $a \in A$,
- $|u| = \sum_{a \in A} |u|_a$.

Definição

Sejam A um alfabeto e u, $v \in A^*$. Então diz-se que:

- u é um fator de v se existem $x, y \in A^*$ tais que $v = xuy$;
- u é um prefixo de v se existe $y \in A^*$ tais que $v = uy$;
- u é um sufixo de v se existe $x \in A^*$ tais que $v = xu$;
- u é um fator próprio de v se u é um fator de v e $u \neq v$.

EXEMPLO 3

Sejam $A = \{0, 1\}$ e $u = 001110101011$.

- 0011, 0111010 e 101011 são fatores (próprios) de u.
- 1010 é um fator de u que tem várias ocorrências identificadas a vermelho:
  0011**1010**1011, 0011101**010**11.
- 0011, 00 e 00111 são prefixos de u e 011, 11 e 1 são sufixos de u.

Quantos prefixos se podem identificar em u? E quantos sufixos?

Definição

Seja $u \in A^*$. A palavra inversa de u, que se representa por u^{I}, é a sequência das letras que ocorrem em u por ordem inversa e que se define recursivamente por:

1. $\varepsilon^{\mathrm{I}} = \varepsilon$;
2. $(wa)^{\mathrm{I}} = aw^{\mathrm{I}}$, para quaisquer $w \in A^*$ e $a \in A$.

Proposição

Sejam A um alfabeto e $u,\ v \in A^*$. Então,

- $(uv)^{\mathrm{I}} = v^{\mathrm{I}}u^{\mathrm{I}}$,
- $(u^{\mathrm{I}})^{\mathrm{I}} = u$.

EXEMPLO 4

Sejam $A = \{0, 1\}$ e $u = 001110101011$ $(= 001110 \cdot 1010 \cdot 11)$. Então,

- $u^{\mathrm{I}} = 110101011100$.
- $u^{\mathrm{I}} = (11)^{\mathrm{I}} \cdot (1010)^{\mathrm{I}} \cdot (001110)^{\mathrm{I}} = (11) \cdot (0101) \cdot (011100) = 110101011100$.

Sejam $u \in A^*$ e $n \in \mathbb{N}$. Representa-se por u^n a concatenação de n cópias de u. A expressão u^0 representa a palavra vazia.

Definição recursiva de potência de uma palavra

Sejam A é um alfabeto, $u \in A^*$ e $n \in \mathbb{N}_0$. Define- se a potência de ordem n de u como sendo a palavra de A^*, representada por u^n, que se define recursivamente por:

1. $u^0 = \varepsilon$;
2. $u^n = u^{n-1}u$.

Proposição

Sejam A é um alfabeto, $a \in A$, $u \in A^*$ e $m, n \in \mathbb{N}_0$. Então,

- $u^{m+n} = u^m u^n$,
- $(u^n)^m = u^{nm}$,
- $|u^n| = n \times |u|$,
- $|u^n|_a = n \times |u|_a$.

Definição

Seja A um alfabeto. Um qualquer subconjunto de A^* designa-se linguagem.

Designa-se linguagem finita uma linguagem que é um conjunto finito.

EXEMPLOS 5

- $\varnothing$, A e $\{u \mid |u| = n \in \mathbb{N}\}$ são linguagens finitas;
- A^+ e A^* são linguagens numeráveis;
- $L = \{a^n b^n \mid n \in \mathbb{N}\}$ é uma linguagem numerável, sendo que $\{a, b\} \subseteq A$;
- $L = \{u \in A^* \mid 001 \text{ não é fator de } u\}$, sendo $A = \{0, 1\}$, é uma linguagem numerável.

O conjunto de todas as linguagens é $\mathcal{P}(A^*)$, que vulgarmente se representa por $L(A)$, e que é um conjunto infinito não numerável.

Definição

As operações booleanas sobre linguagens são:

- a união: $L_1 \cup L_2 = \{u \mid u \in L_1 \vee u \in L_2\}$,
- a interseção: $L_1 \cap L_2 = \{u \mid u \in L_1 \wedge u \in L_2\}$,
- o complementar: $L_1 \setminus L_2 = \{u \mid u \in L_1 \wedge u \notin L_2\}$,

para quaisquer linguagens L_1 e L_2 sobre um alfabeto A.

Sendo $L \subseteq A^*$, define-se $\overline{L} = A^* \setminus L$ que se designa apenas complementar de L.

Definição

Define-se produto das linguagens L_1 e L_2 sobre um alfabeto A por:

$$L_1 L_2 = \{uv \mid u \in L_1 \wedge v \in L_2\}$$

Para L uma linguagem e $u \in A^*$, por simplicidade escreve-se:

$$uL = \{u\}L = \{uv \mid v \in L\} \quad \text{e} \quad Lu = L\{u\} = \{vu \mid v \in L\}.$$

EXEMPLO 6

Seja $A = \{x, y, z\}$. Então,

- $A^* \setminus A^*yx$ é o conjunto das palavras que não têm sufixo yx;
- xzA^*xy é o conjunto das palavras que têm como prefixo xz e como sufixo xy e $xzA^*xy = xzA^* \cap A^*xy$;
- $xyA^* \cup A^*yx$ é o conjunto das palavras que têm como prefixo xy ou como sufixo yx;
- $xyA^*yx \neq xyA^* \cap A^*yx$, porque, $xyx \in xyA^* \cap A^*yx$ mas $xyx \notin xyA^*yx$;
- A^*xyA^* é o conjunto das palavras que têm como fator xy;
- $xy(A^*y \cup A^*yyA^*) = xyA^*y \cup xyA^*yyA^*$ é o conjunto das palavras que têm prefixo xy e,
  - de comprimento maior ou igual a 3 e sufixo y ou
  - comprimento maior ou igual a 4 e pelo menos um fator yy mas xy e yy não se sobrepõem;
- $\varnothing A^*xyA^* = \{uv \mid u \in \varnothing \wedge v \in A^*xyA^*\} = \varnothing$.

Propriedades das operações

- A união de linguagens é associativa e comutativa.
- A interseção de linguagens é associativa e comutativa.
- O produto de linguagens é associativo.
- O produto de linguagens é distributivo em relação à união.
- O elemento neutro do produto é a linguagem $\{\varepsilon\}$.
- O elemento absorvente do produto é a linguagem $\emptyset$.

Notar que o produto de linguagens não é comutativo.

EXEMPLO 7

Seja $A = \{x, y, z\}$. Se $L_1 = yA^*$ e $L_2 = A^*y$, então

- $L_1L_2 = yA^*y$ é a linguagem das palavras de comprimento maior ou igual a 2 em que y é um prefixo e um sufixo;
- $L_2L_1 = A^*yyA^*$ é a linguagem das palavras de comprimento maior ou igual a 2 em que yy é um fator.

Em particular, $xyyx \in L_2L_1$ mas $xyyx \notin L_1L_2$, e $yxzxy \in L_1L_2$ mas $yxzxy \notin L_2L_1$.

Definição

Sejam K e L linguagens sobre um alfabeto A. Definem-se as operações:

- Potência de ordem n ($n \in \mathbb{N}_0$) da linguagem L:

  (i) $L^0 = \{\varepsilon\}$,
  (ii) $L^n = L^{n-1}L$, para qualquer $n \geq 1$.

- Fecho de Kleen da linguagem L:
  $$L^* = \bigcup_{n\in N_0} L^n = \{u_1 \cdots u_n \mid n \in \mathbb{N}_0,\ u_1, \ldots, u_n \in L\}.$$

- Fecho positivo da linguagem L:
  $$L^+ = \bigcup_{n\in N} L^n = \{u_1 \cdots u_n \mid n \in \mathbb{N},\ u_1, \ldots, u_n \in L\}.$$

- Resíduo à esquerda de L por K:
  $$K^{-1}L = \{u \in A^* \mid Ku \cap L \neq \varnothing\}.$$

- Resíduo à direita de L por K:
  $$LK^{-1} = \{u \in A^* \mid uK \cap L \neq \varnothing\}.$$

Proposição

Seja L uma linguagem. Então, as operações de fecho positivo e de fecho de Kleene gozam das seguintes propriedades:

- $\emptyset^* = \{\varepsilon\}$, $\emptyset^+ = \emptyset$, $\{\varepsilon\}^* = \{\varepsilon\} = \{\varepsilon\}^+$;
- $L = L^1 \subseteq L^+ \subseteq L^*$;
- $\varepsilon \in L^+$ se e só se $\varepsilon \in L$;
- $L^+ = LL^* = L^*L$.

Proposição

Sejam L, L_1 e L_2 linguagens sobre um alfabeto A, $a \in A$ e $u, v \in A^*$. Então,

1. $u^{-1}(L_1 \cup L_2) = u^{-1}L_1 \cup u^{-1}L_2$;
2. $u^{-1}(L_1 \cap L_2) = u^{-1}L_1 \cap u^{-1}L_2$;
3. $u^{-1}(L_1 \setminus L_2) = u^{-1}L_1 \setminus u^{-1}L_2$;
4. $a^{-1}(L_1L_2) = \begin{cases} (a^{-1}L_1)L_2 & \text{se } \varepsilon \notin L_1 \\ (a^{-1}L_1)L_2 \cup a^{-1}L_2 & \text{se } \varepsilon \in L_1 \end{cases}$;
5. $a^{-1}L^* = (a^{-1}L)L^*$;
6. $(uv)^{-1}L = v^{-1}(u^{-1}L)$.

Definição indutiva de expressão regular

Se A é um alfabeto, uma expressão regular sobre A é uma palavra da linguagem $ER(A)$ sobre o alfabeto $A \cup \{\varnothing, \varepsilon, (,), +, \cdot, ^*\}$ definida por:

1. os símbolos $\varnothing$ e ε são elementos de $ER(A)$;
2. para qualquer $a \in A$, $a \in ER(A)$;
3. se $e_1, e_2 \in ER(A)$, então $(e_1 + e_2) \in ER(A)$;
4. se $e_1, e_2 \in ER(A)$, então $(e_1 \cdot e_2) \in ER(A)$;
5. se $e \in ER(A)$, então $(e^*) \in ER(A)$.

Notas:

- o símbolo $+$ pode ser substituído pelo símbolo $\cup$;
- o símbolo $\cdot$ é usualmente omitido;
- por vezes omitem-se os parêntesis, considerando que na construção da expressão a introdução de * tem prioridade em relação a $\cdot$, que por sua vez tem prioridade em relação a $+$, por exemplo, $e_1 e_2^* + e_3 = ((e_1 \cdot (e_2^*)) + e_3)$.

A cada expressão regular sobre $A \cup \{\emptyset, \varepsilon, (,), +, \cdot, ^*\}$ associa-se uma linguagem sobre A:

$$\begin{array}{rcll}
\mathcal{L} : ER(A) & \longrightarrow & L(A) & \\
\emptyset & \longmapsto & \emptyset & \\
\varepsilon & \longmapsto & \{\varepsilon\} & \\
a & \longmapsto & \{a\} & \text{para qualquer } a \in A \\
(e_1 + e_2) & \longmapsto & \mathcal{L}(e_1) \cup \mathcal{L}(e_2) & \text{para quaisquer } e_1, e_2 \in ER(A) \\
(e_1 \cdot e_2) & \longmapsto & \mathcal{L}(e_1)\mathcal{L}(e_2) & \text{para quaisquer } e_1, e_2 \in ER(A) \\
(e^*) & \longmapsto & \mathcal{L}(e)^* & \text{para qualquer } e \in ER(A)
\end{array}$$

Definição

Uma linguagem sobre um alfabeto A diz-se uma linguagem regular se ela pertence à imagem da função $\mathcal{L}$.

O conjunto das linguagens regulares sobre A representa-se por $\mathcal{R}eg(A)$

EXEMPLOS 8

Seja $A = \{a, b, c, d\}$ um alfabeto.

- $(((a^*) \cdot a) \cdot (b \cdot b \cdot c))$ é uma expressão regular que, abreviadamente, se pode representar por $a^* ab^2 c$ ou por $a^+ b^2 c$.
- $((((a \cdot b)^* \cdot c) + (\varnothing^*)) \cdot ((b \cdot b)^*))$ é uma expressão regular que, abreviadamente, se pode representar por $((ab)^* c + \varnothing^*)(b^2)^*$.
- A linguagem associada à expressão $a^+ b^2 c$ é
$$\mathcal{L}(a^+ b^2 c) = \mathcal{L}(a^+)\mathcal{L}(b^2)\mathcal{L}(c) = \{a^k \mid k \in \mathbb{N}\}\{b^2\}\{c\} = \{a^k b^2 c \mid k \in \mathbb{N}\}.$$
- A linguagem associada à expressão $((ab)^* c + \varnothing^*)(bb)^*$ é

$$\begin{aligned}
\mathcal{L}(((ab)^* c + \varnothing^*)(bb)^*) &= \mathcal{L}(((ab)^* c + \varnothing^*))\ \mathcal{L}((bb)^*) \\
&= \big(\mathcal{L}((ab)^* c) \cup \mathcal{L}(\varnothing^*)\big)\ \mathcal{L}((bb)^*) \\
&= \big(\{ab\}^* \{c\} \cup \varnothing^*\big)\ \{b^2\}^* \\
&= \big(\{(ab)^k \mid k \in \mathbb{N}_0\}\{c\} \cup \{\varepsilon\}\big)\ \{b^{2k} \mid k \in \mathbb{N}_0\} \\
&= \big(\{(ab)^k c \mid k \in \mathbb{N}_0\} \cup \{\varepsilon\}\big)\ \{b^{2k} \mid k \in \mathbb{N}_0\} \\
&= \{(ab)^{k'} c b^{2k} \mid k, k' \in \mathbb{N}_0\} \cup \{b^{2k} \mid k \in \mathbb{N}_0\}.
\end{aligned}$$

Alternativamente, pode definir-se $\mathcal{R}eg(A)$ indutivamente por:

1. $\emptyset, \{\varepsilon\} \in \mathcal{R}eg(A)$;
2. para qualquer $a \in A$, $\{a\} \in \mathcal{R}eg(A)$;
3. se $L_1, L_2 \in \mathcal{R}eg(A)$, então $L_1 \cup L_2 \in \mathcal{R}eg(A)$;
4. se $L_1, L_2 \in \mathcal{R}eg(A)$, então $L_1 L_2 \in \mathcal{R}eg(A)$;
5. se $L \in \mathcal{R}eg(A)$, então $L^* \in \mathcal{R}eg(A)$.

Definição

Sejam $e_1, e_2 \in ER(A)$. Diz-se que:

- $e_1 = e_2$ se $\mathcal{L}(e_1) = \mathcal{L}(e_2)$;
- $e_1 \leq e_2$ se $\mathcal{L}(e_1) \subseteq \mathcal{L}(e_2)$.

Destas definições resulta um lista de igualdades válidas entre expressões regulares.

Proposição

Sejam A um alfabeto e $r, s, t \in \mathcal{R}eg(A)$. Então,

1. $(r+s)+t = r+(s+t)$;
2. $r+\varnothing = \varnothing+r = r$;
3. $r+s = s+r$;
4. $r+r = r$;
5. $r\varnothing = \varnothing r = \varnothing$;
6. $r\varepsilon = \varepsilon r = r$;
7. $(rs)t = r(st)$;
8. $r(s+t) = rs+rt$;
9. $(r+s)t = rt+st$;
10. $\varnothing^* = \varepsilon^* = \varepsilon$;
11. $r^* = r^*r^* = (r^*)^* = (\varepsilon+r)^* = rr^*+\varepsilon$;
12. $rr^* = r^*r$;
13. $(r+s)^* = (r^*+s^*)^* = (r^*s^*)^* = (r^*s)^*r^*$;
14. $r(sr)^* = (rs)^*r$;
15. $(r^*s)^* = (r+s)^*s+\varepsilon$;
16. $(rs^*)^* = r(r+s)^*+\varepsilon$.

Notas:

- podem omitir-se os parêntesis usando as propriedades 1. e 7.;
- para $e \in ER(A)$, $n \in \mathbb{N}$, $e^0 = \varepsilon$ e $e^n = ee^{n-1}$;
- para $e \in ER(A)$, $e^+ = ee^* = e^*e$.

EXEMPLOS 8

Seja $A = \{a_1, \ldots, a_n\}$ um alfabeto.

- A linguagem A é regular, porque

$$A = \{a_1\} \cup \cdots \cup \{a_n\} = \mathcal{L}(a_1) \cup \cdots \cup \mathcal{L}(a_n) = \mathcal{L}(a_1 + \cdots + a_n).$$

- A linguagem A^* é regular, porque

$$A^* = (\{a_1\} \cup \cdots \cup \{a_n\})^* = (\mathcal{L}(a_1) \cup \cdots \cup \mathcal{L}(a_n))^* = \mathcal{L}(a_1 + \cdots + a_n)^* = \mathcal{L}((a_1 + \cdots + a_n)^*).$$

- Se $u = a_{i_1} \ldots a_{i_k} \in A^*$, então $\{u\}$ é uma linguagem regular, porque, se $k = 0$, $\{\varepsilon\} = \mathcal{L}(\varepsilon)$ e, se $k \geq 1$,

$$\{u\} = \{a_{i_1}\} \cdots \{a_{i_k}\} = \mathcal{L}(a_{i_1}) \cdots \mathcal{L}(a_{i_k}) = \mathcal{L}(a_{i_1} \cdots a_{i_k}).$$

- Qualquer linguagem finita $L = \{u_1, \ldots, u_r\}$ ($r \in \mathbb{N}$) é uma linguagem regular, porque

$$L = \{u_1, \ldots, u_r\} = \{u_1\} \cup \cdots \cup \{u_r\} = \mathcal{L}(u_1) \cup \cdots \cup \mathcal{L}(u_r) = \mathcal{L}(u_1 + \cdots + u_r).$$

Definição

Uma equação linear à direita sobre expressões regulares é uma equação do tipo

$$X = rX + s$$

na qual $r, s \in ER(A)$ são expressões regulares e X é a incógnita.

Diz-se que:

- uma expressão regular $t \in ER(A)$ é uma solução da equação se

$$t = rt + s;$$

- uma expressão regular $t \in ER(A)$ é uma solução mínima da equação se t é uma solução e $t \leq t'$ para toda a solução t' da equação.

Proposição

Sejam $r, s \in ER(A)$ e $X = rX + s$ uma equação linear à direita sobre expressões regulares.

1. $X = rX + s$ admite uma única solução mínima.
2. $r^* s$ é a solução mínima de $X = rX + s$.
3. Se $\varepsilon \notin \mathcal{L}(r)$, então $r^* s$ é a única solução de $X = rX + s$.

DEMONSTRAÇÃO de 1. e 2.

1. Se $t, t' \in ER(A)$ são soluções mínimas de $X = rX + s$, então, $t \leq t'$ e $t' \leq t$. Logo $t = t'$.

2. Verifica-se que $r^* s$ é uma solução de $X = rX + s$, porque

$$r(r^* s) + s = (rr^*)s + s = (rr^* + \varepsilon)s = r^* s.$$

Seja $t \in ER(A)$ outra solução de $X = rX + s$. Então $t = rt + s$, o que significa que

$$\mathcal{L}(t) = \mathcal{L}(r)\mathcal{L}(t) \cup \mathcal{L}(s). \tag{1}$$

Logo $\mathcal{L}(r)\mathcal{L}(t) \subseteq \mathcal{L}(t)$. Consequentemente,

$$\mathcal{L}(r)^2\mathcal{L}(t) = \mathcal{L}(r)\mathcal{L}(r)\mathcal{L}(t) \subseteq \mathcal{L}(r)\mathcal{L}(t) \subseteq \mathcal{L}(t)$$

e, por recorrência, $\mathcal{L}(r)^n\mathcal{L}(t) \subseteq \mathcal{L}(t)$ para todo o $n \in \mathbb{N}_0$. Assim, $\mathcal{L}(r)^*\mathcal{L}(t) = \mathcal{L}(t)$.
Usando a igualdade (1) deduz-se

$$\mathcal{L}(t) = \mathcal{L}(r)^*\mathcal{L}(t) =_{(1)} \mathcal{L}(r)^*(\mathcal{L}(r)\mathcal{L}(t) \cup \mathcal{L}(s)) = \mathcal{L}(r)^*\mathcal{L}(r)\mathcal{L}(t) \cup \mathcal{L}(r)^*\mathcal{L}(s).$$

Conclui-se então que $\mathcal{L}(r)^*\mathcal{L}(s) \subseteq \mathcal{L}(t)$, donde $r^* s \leq t$, como queríamos provar.

Definição

Um sistema de equações lineares à direita sobre expressões regulares é um sistema de equações da forma

$$\begin{cases} X_1 = r_{11}X_1 + r_{12}X_2 + \cdots + r_{1n}X_n + s_1 \\ X_2 = r_{21}X_1 + r_{22}X_2 + \cdots + r_{2n}X_n + s_2 \\ \quad \vdots \\ X_n = r_{n1}X_1 + r_{n2}X_2 + \cdots + r_{nn}X_n + s_n \end{cases}$$

onde $r_{ij}, s_i \in ER(A)$ para todos os $i, j \in \{1, \ldots, n\}$ e $X_1, X_2, \ldots, X_n$ são as incógnitas. Diz-se que:

- $(t_1, t_2, \ldots, t_n) \in ER(A)^n$ é uma solução do sistema se, para cada $i \in \{1, \ldots, n\}$,
$$t_i = r_{i1}t_1 + r_{i2}t_2 + \cdots + r_{in}t_n + s_i;$$
- uma solução $(t_1, t_2, \ldots, t_n) \in ER(A)^n$ do sistema é uma solução mínima se, para toda a solução $(t'_1, t'_2, \ldots, t'_n)$ do sistema,
$$t_i \leq t'_i \text{ para todo o } i \in \{1, \ldots, n\}.$$

Proposição

- Um sistema de equações lineares à direita sobre expressões regulares num alfabeto A tem uma única solução mínima.
- Se $\varepsilon \notin \mathcal{L}(r_{ij})$, para cada coeficiente r_{ij} do sistema, então o sistema tem uma única solução.

Para determinar a solução mínima de um sistema pode usar-se:

- o "método de substituição" e
- a solução mínima das equações da forma $X = rX + s$.

EXEMPLO 9

Calcule a solução solução mínima do sistema:

$$\begin{cases} X_1 = bX_1 + aX_2 + \emptyset \\ X_2 = aX_1 + bX_2 + \varepsilon \end{cases}.$$

Pode-se deduzir sucessivamente

$$\begin{aligned} \begin{cases} X_1 = bX_1 + aX_2 + \emptyset \\ X_2 = aX_1 + bX_2 + \varepsilon \end{cases} &\Leftrightarrow \begin{cases} X_1 = b^* aX_2 \\ X_2 = aX_1 + bX_2 + \varepsilon \end{cases} \\ &\Leftrightarrow \begin{cases} X_1 = b^* aX_2 \\ X_2 = ab^* aX_2 + bX_2 + \varepsilon \end{cases} \\ &\Leftrightarrow \begin{cases} X_1 = b^* aX_2 \\ X_2 = (ab^* a + b)X_2 + \varepsilon \end{cases} \\ &\Leftrightarrow \begin{cases} X_1 = b^* a(ab^* a + b)^* \\ X_2 = (ab^* a + b)^* \varepsilon \end{cases}. \end{aligned}$$

Então a solução mínima do sistema é

$$(b^* a(ab^* a + b)^*, (ab^* a + b)^*).$$

Os sistemas de equações lineares podem ser usados para determinar uma expressão regular que represente uma dada linguagem regular.

EXEMPLO 10

Sejam $A = \{a, b\}$, $L_1 = \{w \in A^* \mid |w|_a \text{ é ímpar}\}$ e $L_2 = \{w \in A^* \mid |w|_a \text{ é par}\}$.

Então são válidas as igualdades

$$L_1 = bL_1 \cup aL_2 \quad \text{e} \quad L_2 = aL_1 \cup bL_2 \cup \{\varepsilon\}.$$

Ou seja, (L_1, L_2) é solução do sistema

$$\begin{cases} X_1 = bX_1 \cup aX_2 \cup \varnothing \\ X_2 = aX_1 \cup bX_2 \cup \{\varepsilon\} \end{cases}$$

que convertido em sistema de equações lineares é precisamente o sistema do EXEMPLO 9. Assim, a solução mínima desse sistema

$$t_1 = b^* a(ab^* a + b)^* \quad \text{e} \quad t_2 = (ab^* a + b)^*$$

determina as expressões regulares que representam as linguagens L_1 e L_2, respetivamente.