INTRODUÇÃO À TEORIA COMBINATÓRIA DE SEMIGRUPOS INVERSOS

Pedro V. Silva*

Departamento de Matemática Pura, Faculdade de Ciências,
Universidade do Porto, 4000 Porto, Portugal

A teoria combinatória de semigrupos inversos tem como objectivo o estudo dos semigrupos (monoides) inversos livres e respectivas apresentações. A generalidade dos resultados relativos a semigrupos inversos livres pode ser facilmente deduzida a partir de resultados análogos para monoides inversos livres, pelo que adoptaremos invariavelmente a "versão monoide".

O conceito de semigrupo inverso livre remonta a 1961, quando foi introduzido por Vagner [28]. Contudo, para além de alguns resultados esporádicos, a teoria não produziria grandes desenvolvimentos até 1973, quando o problema da palavra para o semigrupo inverso livre foi resolvido (independentemente) por Scheiblich [19] e Munn [16]. A solução de Scheiblich, de natureza essencialmente algébrica, tinha como base o grupo livre, enquanto a solução de Munn era de natureza combinatória e pode ser vista hoje à luz da teoria de linguagens e autómatos.

O estudo consistente e sistemático de apresentações de monoides inversos teve como ponto de partida o desenvolvimento de uma teoria combinatória por parte de Stephen em 1987 [26], que constituiu uma generalização do trabalho efectuado por Munn para os monoides inversos livres. Usando as construções de Stephen, foram obtidos nos últimos anos vários resultados que põem em relevo ligações importantes à teoria combinatória de semigrupos, teoria de semigrupos finitos, teoria combinatória de grupos e teoria de linguagens, o que mostra a vitalidade da teoria. Entre outros autores, podemos citar Margolis, Meakin, Sapir e Silva [10] [11] [13] [14] [24]. No que se refere a resultados de decidibilidade propriamente ditos, têm-se registado alguns sucessos mas permanecem em aberto vários problemas fundamentais, em particular o problema da palavra para apresentações com uma única relação. Entre outros, podemos citar Birget, Margolis, Meakin, Silva, Stephen [4] [12] [21] [22] [23] [25] [27].

Foi nossa opção neste curso privilegiar os fundamentos da teoria e a resolução de problemas de decidibilidade, de modo a manter os pré-requisitos de teoria de grupos e teoria de linguagens a níveis aceitáveis. Apesar disso, a grande importância de que se revestem alguns conceitos oriundos destas áreas obriga-nos a dedicar-lhes

*Este trabalho foi realizado com o apoio da JNICT - Projecto SAL (PBIC/C/CEN/1021/92) e do ESPRIT-BRA Working Group 6317 "ASMICS".

algumas secções específicas. Resulta assim que nada menos do que cinco secções num total de doze são dedicadas à introdução de conceitos fundamentais em áreas exteriores à teoria combinatória de semigrupos inversos. As secções 4 e 7 são dedicadas ao monoide inverso livre, as secções 8 e 9 abordam as construções de Stephen para apresentações de monoides inversos, e as secções 10 e 11 mostram algumas aplicações desta teoria a problemas de decidibilidade para apresentações concretas. Na última secção, é evidenciada a importância da resolução do problema da palavra para apresentações de monoides inversos com uma única relação, e são apresentados (sem demonstração) alguns outros resultados de decidibilidade.

Finalmente, gostaria agradecer ao Centro Internacional de Matemática a oportunidade que me concedeu de elaborar um curso com estas características.

1 Semigrupos e monoides

Nesta secção vamos apresentar de forma resumida alguns conceitos e resultados básicos relativos a semigrupos e monoides em geral. Os conceitos são todos definidos em termos de monoides, sendo as versões para semigrupos inteiramente análogas. Aconselhamos ao leitor interessado em mais detalhes a consulta de [6].

Um *semigrupo* é uma estrutura algébrica da forma $(S, *)$, onde S é um conjunto não vazio e $*$ designa uma operação binária associativa em S. Se a operação estiver subentendida, é habitual designar um tal semigrupo por S e escrever ab em vez de $a * b$ para todos $a, b \in S$. Dizemos que e é *elemento neutro* de S se

$$\forall a \in S,\ ae = ea = a.$$

Um semigrupo com elemento neutro diz-se um *monoide*. É imediato que o elemento neutro de um monoide é único, e é habitualmente designado pelo símbolo 1. Um elemento $e \in M$ diz-se *idempotente* se $e^2 = e$. Todo o monoide tem pelo menos um elemento idempotente, o elemento 1. O conjunto dos elementos idempotentes de M é designado por $E(M)$.

Seja M um monoide. Dizemos que $N \subseteq M$ é um *submonoide* de M se $1 \in N$ e $ab \in N$ para todos $a, b \in N$. Dado um subconjunto $A \subseteq M$ qualquer, existe um submonoide A^* de M que contém A e é o menor submonoide de M contendo A, a saber,

$$A^* = \{1\} \cup \{a_1 ... a_n;\ n \geq 1,\ a_i \in A\}.$$

Dizemos que A^* é o submonoide de M *gerado* por A. Se $A^* = M$, dizemos que A é um conjunto de geradores de M.

Uma *relação* em M é um subconjunto $R \subseteq M \times M$. Dada uma relação finita

$$R = \{(a_1, b_1), ..., (a_n, b_n)\},$$

é habitual enunciar os elementos de R na forma

$$a_1 = b_1, ..., a_n = b_n.$$

Por abuso de linguagem, os elementos de R são também designados por relações. Se R é uma relação em M, designamos por R^{-1} a relação $\{(a,b);\ (b,a) \in \mathrm{R}\}$. A relação R diz-se uma *congruência* se for uma relação de equivalência e satisfizer

$$(a,b) \in R \ \Rightarrow (ac,bc),(ca,cb) \in R$$

para todos $a,b,c \in M$. Dada uma relação R qualquer em M, existe uma congruência em M que é a menor congruência em M contendo R, e que se diz a congruência em M *gerada* por R. Esta congruência é designada por $R^\sharp$ e pode ser descrita do seguinte modo. Dados $a,b \in M$, temos $(a,b) \in R^\sharp$ se existirem $w_0,...,w_n \in M$ $(n \geq 0)$, tais que:

$a = w_0$,

$b = w_n$,

para todo $i \in \{1,...,n\}$, existem $x_i, y_i \in M$ e $(r_i, s_i) \in R \cup R^{-1}$ tais que

$$w_{i-1} = x_i r_i y_i, \qquad w_i = x_i s_i y_i.$$

Seja τ uma congruência no monoide M e seja $a \in M$. Designamos a classe de congruência de a por $a\tau$ e escrevemos

$$M/\tau = \{a\tau;\ a \in M\}.$$

Definimos uma estrutura natural de monoide em M/τ por

$$(a\tau)(b\tau) = (ab)\tau \qquad (a,b \in M)$$

sendo 1τ o elemento neutro. O facto de τ ser uma congruência garante que esta operação está bem definida e M/τ diz-se o monoide *quociente* de M por τ.

Sejam M,N monoides. Uma função $\varphi\colon M \to N$ diz-se um *homomorfismo* (de monoides) se $1\varphi = 1$ e $(ab)\varphi = (a\varphi)(b\varphi)$ para todos $a,b \in M$. Um homomorfismo bijectivo diz-se um *isomorfismo*, e é imediato que a função inversa de um isomorfismo é também um isomorfismo. Se existir um isomorfismo entre dois monoides M e N, dizemos que estes são *isomorfos* e escrevemos $M \simeq N$. O resultado seguinte mostra-nos que os conceitos de congruência e homomorfismo estão intimamente ligados.

Teorema 1.1 *Seja $\varphi\colon M \to N$ um homomorfismo de monoides e seja τ uma congruência em M.*

(i) A projecção

$$\begin{aligned} \pi\colon M &\to M/\tau \\ a &\mapsto a\tau \end{aligned}$$

é um homomorfismo sobrejectivo de monoides.

(ii) *Se* $\tau \subseteq \mathrm{Ker}\varphi$, *então*

$$\begin{aligned}\Phi\colon M/\tau &\to N\\ a\tau &\mapsto a\varphi\end{aligned}$$

é um homomorfismo de monoides, e o diagrama

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\pi"'] & N \\ M/\tau \arrow[ur, "\Phi"'] & \end{tikzcd}$$

comuta.

(iii) *A relação*

$$\mathrm{Ker}\varphi = \{(a,b) \in M \times M : a\varphi = b\varphi\}$$

é uma congruência em M, $M\varphi$ *é um submonoide de* N *e* $M\varphi \simeq M/\mathrm{Ker}\varphi$.

Dem. Exercício. $\square$

Teorema 1.2 *Sejam* τ *e* σ *congruências num monoide* M *tais que* $\tau \subseteq \sigma$.

(i) *A relação* $\sigma/\tau = \{(a\tau, b\tau) : (a,b) \in \sigma\}$ *é uma congruência em* M/τ.

(ii) $(M/\tau)/(\sigma/\tau) \simeq M/\sigma$.

Dem. Exercício. $\square$

Exemplo 1.3 *Consideremos o monoide* $(\mathbf{N}_0, +)$. *Para todo* $p \in \mathbf{N}_0$, *temos*

$$p^* = \{kp;\ k \in \mathbf{N}_0\},$$

$$\{p, p+1\}^* = \{kp + j;\ k \in \mathbf{N}_0,\ 0 \leq j \leq k\}.$$

Se $p > 1$, *o maior inteiro não pertencente a* $\{p, p+1\}^*$ *é*

$$(p-2)p + (p-1) = p^2 - p - 1.$$

Dados $m \in \mathbf{N}_0$ *e* $p \in \mathbf{N}$, *seja* $\tau_{m,p}$ *a congruência em* $\mathbf{N}_0$ *gerada pela relação* $m = m + p$. *É fácil de ver que* $u\tau_{m,p} = v\tau_{m,p}$ *se e só se* $u = v$ *ou*

$$u, v \geq m \qquad \text{e} \qquad p \mid u - v.$$

É imediato que

$$\mathbf{N}_0/\tau_{m,p} = \{0\tau_{m,p}, ..., (m+p-1)\tau_{m,p}\},$$

e todos estes elementos são distintos. Vamos determinar quantos idempotentes existem. Seja $u \in \{0, ..., m+p-1\}$. *Então* $u\tau_{m,p} = (u+u)\tau_{m,p}$ *se e só se* $u = 0$ *ou* $u \geq m$ *com* $p \mid u$. *Como existe exactamente um inteiro* $u \in \{m, ..., m+p-1\}$ *tal que* $p \mid u$, *resulta que, se* $m > 0$, $\mathbf{N}_0/\tau_{m,p}$ *tem dois idempotentes; se* $m = 0$, $0\tau_{m,p}$ *é o único idempotente de* $\mathbf{N}_0/\tau_{m,p}$. $\square$

Seja agora X um conjunto (não vazio). Uma *transformação parcial* de X é uma função da forma $f : Y \to X$, com $Y \subseteq X$. Dizemos que Y é o *domínio* de f, com notação dom$f$, e que Yf é a *imagem* de f, com notação im$f$. Seja $PT(X)$ o conjunto de todas as transformações parciais de X. Definimos uma operação de composição em $PT(X)$ do seguinte modo: se $f, g \in PT(X)$, fg é definida por $\mathrm{dom}(fg) = (\mathrm{im}f \cap \mathrm{dom}g)f^{-1}$ e $x(fg) = (xf)g$ para todo $x \in \mathrm{dom}(fg)$.

Exercício 1.4 *Mostre que $PT(X)$, munido desta operação de composição, constitui um monoide.* $\square$

Seja $T(X)$ o submonoide de $PT(X)$ constituído pelas transformações de domínio X. Vejamos que todo o monoide pode ser visto como um submonoide de $T(X)$ para algum X.

Teorema 1.5 *Seja M um monoide. Então M é isomorfo a um submonoide de $T(X)$ para algum conjunto X.*

Dem. Seja $X = M$ enquanto conjunto, e consideremos a função

$$\begin{aligned} \varphi \colon M &\to T(X) \\ a &\mapsto \varphi_a \end{aligned}$$

onde $\varphi_a \colon X \to X$ é definida por $x\varphi_a = xa$. Dados $a, b, x \in M$, temos

$$x\varphi_{ab} = x(ab) = (xa)b = x\varphi_a\varphi_b$$

e logo $\varphi_{ab} = \varphi_a\varphi_b$. Por outro lado, $\varphi_1 = 1$, logo φ é um homomorfismo. Se $\varphi_a = \varphi_b$, então $a = 1\varphi_a = 1\varphi_b = b$, pelo que φ é injectivo e M é isomorfo ao submonoide $\{\varphi_a; a \in M\}$ de $T(X)$. $\square$

Dado um conjunto X, uma *palavra* em X é uma sequência finita de elementos de X, que representamos na forma

$$x_1 ... x_n \qquad (n \geq 1,\ x_i \in X)$$

se for não vazia, ou pelo símbolo 1 se for vazia. Definimos o *comprimento* da palavra $u = x_1 ... x_n$ como sendo $|\, u \,| = n$, definindo também $|\, 1 \,| = 0$. Designamos por X^* o conjunto de todas as palavras em X, e identificamos os elementos de X (apelidados de *letras*) com as palavras de comprimento 1 correspondentes. Neste contexto, é habitual referirmo-nos a X como um *alfabeto*. Se X é um alfabeto, assumimos sempre que 1 não designa nenhum elemento de X.

Definimos em X^* uma operação binária dita de *concatenação*, definida por

$$(x_1 ... x_n) \cdot (x'_1 ... x'_m) = x_1 ... x_n x'_1 ... x'_m$$

$$u \cdot 1 = 1 \cdot u = u$$

para todos $x_i, x'_j \in X$ e $u \in X^*$. É imediato que X^*, munido da operação de concatenação , constitui um monoide em que a palavra vazia 1 é o elemento neutro. Dizemos que X^* é o *monoide livre* sobre o conjunto X, pois X^* satisfaz a seguinte propriedade (propriedade universal):

Teorema 1.6 *Seja X um conjunto, seja M um monoide e seja $\varphi : X \to M$ uma função qualquer. Então existe um e um só homomorfismo $\Phi : X^* \to M$ tal que o diagrama*

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[d, hook] & M \\ X^* \arrow[ur, "\Phi"'] & \end{tikzcd}$$

comuta.

Dem. Definimos o homomorfismo Φ por

$$(x_1...x_n)\Phi = (x_1)\varphi...(x_n)\varphi$$

para toda a palavra não vazia $x_1...x_n$ ($x_i \in X$), e $1\Phi = 1$. É imediato que Φ satisfaz as condições do enunciado, e a unicidade resulta do facto de X ser um conjunto de geradores de X^*. $\Box$

Exercício 1.7 *Mostre que, dado um conjunto X, a propriedade universal caracteriza o monoide livre sobre X a menos de isomorfismo.* $\Box$

A propriedade universal permite-nos mostrar facilmente que todo o monoide M é isomorfo a um quociente de algum monoide livre. Com efeito, seja X um conjunto de geradores de M (por exemplo, o próprio M), e seja φ a inclusão. Então $\Phi : X^* \to M$ é um homomorfismo sobrejectivo e logo $M \simeq X^*/\mathrm{Ker}\Phi$ pelo Teorema 1.1(iii).

Uma expressão formal do tipo $Mon < X; R >$, em que X é um conjunto e R é uma relação em X^*, diz-se uma *apresentação* de monoides. O monoide definido por esta apresentação é o quociente $X^*/R^\sharp$. Se $|R| = 1$, dizemos que a apresentação tem uma única relação. Resulta do comentário anterior que todo o monoide pode ser definido, a menos de isomorfismo, por uma apresentação.

A teoria combinatória de semigrupos tem como principais objectivos o estudo dos monoides (semigrupos) livres e apresentações correspondentes, com especial destaque para os problemas algorítmicos que estas últimas suscitam. Para que uma apresentação represente eficazmente um monoide, é necessário que disponhamos de meios para extrair da apresentação toda a informação básica julgada essencial para a compreensão do monoide considerado. Em particular, o *problema da palavra* para uma apresentação $Mon < X; R >$ assume importância fundamental:

- Dados $u, v \in X^*$, é decidível se $uR^\sharp = vR^\sharp$?

Mesmo que nos limitemos a apresentações finitas (X e R finitos), a generalidade dos problemas da palavra revela-se indecidível. Os primeiros exemplos de indecidibilidade para apresentações finitas foram produzidos por Markov [15] e Post [18] em 1947.

2 Monoides inversos

Vamos agora introduzir conceitos e resultados básicos envolvendo monoides inversos. Para mais detalhes, aconselha-se a consulta de [17].

Seja M um monoide. Dizemos que M é *regular* se

$$\forall a \in M \, \exists b \in M : aba = a.$$

Um elemento $x \in M$ diz-se um *inverso* de $a \in M$ se $axa = a$ e $xax = x$. Se M é regular, todo $a \in M$ tem um inverso: se $aba = a$, então bab é um inverso de a. Dizemos que M é *inverso* se cada $a \in M$ tem exactamente um inverso, que denotamos por a^{-1}. É imediato que se M é inverso e $a \in M$, então $(a^{-1})^{-1} = a$.

Teorema 2.1 *Um monoide M é inverso se e só se é regular e os seus idempotentes comutam.*

Dem. Suponhamos que M é inverso. Então M é trivialmente regular. Sejam $e, f \in E(M)$. Tomando $x = (ef)^{-1}$, temos

$$efxef = ef \qquad \text{e} \qquad xefx = x.$$

Daqui resulta que

$$ef(fxe)ef = ef \qquad \text{e} \qquad (fxe)ef(fxe) = fxe,$$

logo $fxe = x$ por unicidade do inverso de ef. Mas então

$$x^2 = fxefxe = fxe = x,$$

logo x é inverso de x e $x = ef$ por unicidade do inverso de x. Acabámos assim de demonstrar que o produto de idempotentes de M é ainda um idempotente. Logo

$$ef = efef = ef(fe)ef \qquad \text{e} \qquad fe = fefe = fe(ef)fe,$$

donde resulta que $ef = fe$ por unicidade do inverso de ef.

Reciprocamente, suponhamos que M é regular e que os idempotentes de M comutam. Seja $a \in M$ e sejam $x, y \in M$ inversos de a. Como $ax, xa, ay, ya \in E(M)$, resulta que

$$x = xax = xayax = yaxax = yayax = yaxay = yay = y,$$

logo M é um monoide inverso. $\square$

Resulta do teorema que se M é inverso e $a, b \in M$, então

$$ab(b^{-1}a^{-1})ab = aa^{-1}abb^{-1}b = ab,$$

$$b^{-1}a^{-1}(ab)b^{-1}a^{-1} = b^{-1}bb^{-1}a^{-1}aa^{-1} = b^{-1}a^{-1},$$

logo $(ab)^{-1} = b^{-1}a^{-1}$.

Casos particulares importantes de monoides inversos são os *grupos* e os *semi--reticulados*, que passamos a definir. Dizemos que um monoide G é um grupo se

$$\forall a \in G\, \exists b \in G : ab = ba = 1.$$

Obviamente, G é regular, e é fácil de ver que 1 é o único idempotente de G; logo G é um monoide inverso.

Podemos definir um semi-reticulado como sendo um monoide comutativo em que todos os elementos são idempotentes. Pelo teorema anterior, é imediato que todo o semi-reticulado E é um monoide inverso. O uso do termo semi-reticulado deve-se ao seguinte facto: se definirmos uma relação de ordem parcial em E por

$$e \leq f \qquad \text{se} \qquad ef = e,$$

então quaisquer dois elementos $e, f \in E$ têm ínfimo em $(E, \leq)$, a saber, $e \wedge f = ef$. Reciprocamente, se $(E, \leq)$ é um conjunto parcialmente ordenado em que quaisquer dois elementos e, f têm ínfimo $e \wedge f$, então $(E, \wedge)$ constitui um semigrupo comutativo em que todos os elementos são idempotentes (para que $(E, \wedge)$ constitua um monoide, é necessário que $(E, \leq)$ tenha um máximo).

Em particular, dado um monoide inverso M qualquer, $E(M)$ é um submonoide de M que constitui um semi-reticulado. É habitual designar $E(M)$ como o *semi--reticulado dos idempotentes* de M. A relação de ordem parcial do semi-reticulado $E(M)$ pode ser estendida a uma relação de ordem parcial em M, designada por *ordem parcial natural*: dados $a, b \in M$, escrevemos

$$a \leq b \qquad \text{se} \qquad a = eb \text{ para algum } e \in E(M).$$

Obviamente, $\leq$ é reflexiva, pois $a = (aa^{-1})a$ para todo $a \in M$. Se $a = eb$ e $b = fc$ com $e, f \in E(M)$, então $a = (ef)c$, logo $\leq$ é transitiva. Finalmente, se $a = eb$ e $b = fa$, com $e, f \in E(M)$, então $a = eb = e^2b = ea$ e logo

$$b = fa = fea = efa = eb = a,$$

pelo que $\leq$ é de facto uma relação de ordem parcial em M. Note-se ainda que

(i) $a \leq b \Rightarrow (ac \leq bc \;\wedge\; ca \leq cb)$;

(ii) $a \leq b \Rightarrow a^{-1} \leq b^{-1}$.

Com efeito, se $a = eb$ com $e \in E(M)$, então $ac = e(bc)$, $ca = ceb = (cec^{-1})(cb)$, e $a^{-1} = b^{-1}e = (b^{-1}eb)b^{-1}$.

Outra relação de grande importância para um monoide inverso M é a relação $\mathcal{R}$ definida por

$$(a, b) \in \mathcal{R} \qquad \text{se} \qquad aa^{-1} = bb^{-1}.$$

É imediato que $\mathcal{R}$ é uma relação de equivalência em M, e é usual representar a $\mathcal{R}$-classe de equivalência de a por $\mathcal{R}_a$. Analogamente, definimos a relação dual $\mathcal{L}$ por

$$(a,b) \in \mathcal{L} \qquad \text{se} \qquad a^{-1}a = b^{-1}b.$$

A composição $\mathcal{D} = \mathcal{R} \circ \mathcal{L}$ é definida por

$$(a,b) \in \mathcal{D} \qquad \text{se} \qquad \text{existe } c \in M \text{ tal que } (a,c) \in \mathcal{R} \text{ e } (c,b) \in \mathcal{L}.$$

Dizemos que as relações $\mathcal{R}$, $\mathcal{L}$ e $\mathcal{D}$ são *relações de Green.*

Exercício 2.2 *Seja M um monoide inverso e sejam $a, b \in M$. Mostre que:*

(i) $a\mathcal{R}b$ se e só se $aM = bM$;

(ii) $a\mathcal{L}b$ se e só se $Ma = Mb$;

(iii) $\mathcal{D} = \mathcal{L} \circ \mathcal{R}$;

(iv) $\mathcal{D}$ é uma relação de equivalência em M. □

Seja M um monoide inverso. Dado $A \subseteq M$, escrevemos

$$A^{-1} = \{a^{-1};\ a \in M\}.$$

Um *submonoide inverso* de M é um submonoide N de M tal que $N^{-1} = N$. É imediato que N com a operação binária induzida de M constitui também um monoide inverso. Dado um subconjunto $A \subseteq M$ qualquer, o submonoide inverso de M gerado por A é $(A \cup A^{-1})^*$. Relativamente a congruências, temos que:

Teorema 2.3 *Seja M um monoide inverso e seja τ uma congruência em M. Então M/τ é um monoide inverso.*

Dem. É imediato que M/τ é regular. Sejam $a\tau, b\tau \in E(M/\tau)$. É fácil de ver que

$$\begin{aligned} a\tau &= (a\tau)^2 = [a(a^{-1}a)(aa^{-1})a]\tau = [(aa)a^{-1}a^{-1}(aa)]\tau \\ &= [(aa^{-1})(a^{-1}a)]\tau = [(aa^{-1})(a^{-1}a)(aa^{-1})]\tau = (aaa^{-1})\tau \\ &= (aa^{-1})\tau. \end{aligned}$$

Analogamente, $b\tau = (bb^{-1})\tau$, logo

$$(a\tau)(b\tau) = (aa^{-1}bb^{-1})\tau = (bb^{-1}aa^{-1})\tau = (b\tau)(a\tau)$$

e M/τ é inverso pelo Teorema 2.1. □

Resulta facilmente dos Teoremas 1.1(iii) e 2.3 que toda a imagem homomorfa de um monoide inverso é ainda um monoide inverso.

Vamos agora ver que os monoides inversos podem ser representados por monoides de transformações parciais injectivas. Dado um conjunto X, designamos por $PI(X)$ o submonoide de $PT(X)$ constituído pelas transformações parciais injectivas de X. É imediato que se $f\colon Y \to Z$ é uma bijecção com $Y, Z \subseteq X$, então a função inversa $f^{-1}\colon Z \to Y$ satisfaz $ff^{-1}f = f$ e $f^{-1}ff^{-1} = f^{-1}$. Além disso. os idempotentes de $PI(X)$ são precisamente as restrições 1_Y $(Y \subseteq X)$ da função identidade $1\colon X \to X$; como $1_Y 1_Z = 1_{Y\cap Z} = 1_Z 1_Y$ para todos $Y, Z \subseteq X$, resulta que os idempotentes de $PI(X)$ comutam e $PI(X)$ é um monoide inverso.

Teorema 2.4 *Um monoide M é inverso se e só se, para algum conjunto X, M é isomorfo a algum submonoide de $PI(X)$ fechado para funções inversas.*

Dem. A implicação recíproca resulta facilmente dos comentários anteriores.

Suponhamos agora que M é inverso e seja $X = M$ enquanto conjunto. Para cada $a \in M$, definimos a função
$$\begin{aligned}\theta_a\colon Ma^{-1} &\to M\\ x &\mapsto xa.\end{aligned}$$
Dados $x, y \in Ma^{-1}$, temos
$$x\theta_a = y\theta_a \Rightarrow xa = ya \Rightarrow xaa^{-1} = yaa^{-1} \Rightarrow x = y,$$
logo $\theta_a \in PI(X)$. Seja $N = \{\theta_a; a \in M\}$.

Dados $a, b \in M$, temos
$$\mathrm{dom}(\theta_a\theta_b) = (\mathrm{im}\theta_a \cap \mathrm{dom}\theta_b)\theta_a^{-1} = (Ma^{-1}a \cap Mb^{-1})\theta_a^{-1}.$$
Vejamos que $\mathrm{dom}(\theta_a\theta_b) = Mb^{-1}a^{-1} = \mathrm{dom}\theta_{ab}$.

Se $x \in \mathrm{dom}(\theta_a\theta_b)$, então $x \in Ma^{-1}$, logo $x = xaa^{-1}$ e $xa = x\theta_a \in Mb^{-1}$ implica $x = xaa^{-1} \in Mb^{-1}a^{-1}$. Reciprocamente, suponhamos que $x = yb^{-1}a^{-1}$, com $y \in M$. Então $xa = yb^{-1}a^{-1}a = yb^{-1}a^{-1}abb^{-1}$, logo $x\theta_a = xa \in Ma^{-1}a \cap Mb^{-1}$. Logo $x \in \mathrm{dom}(\theta_a\theta_b)$ e $\mathrm{dom}(\theta_a\theta_b) = \mathrm{dom}\theta_{ab}$, donde resulta imediatamente que $\theta_a\theta_b = \theta_{ab}$. Como $\theta_1 = 1$, conclui-se que N é um submonoide de $PI(X)$.

Por outro lado, temos
$$\mathrm{dom}\theta_a = Ma^{-1} = Maa^{-1} = M(a^{-1})^{-1}a^{-1} = \mathrm{im}\theta_{a^{-1}},$$
$$\mathrm{im}\theta_a = Ma^{-1}a = Ma = M(a^{-1})^{-1} = \mathrm{dom}\theta_{a^{-1}};$$
além disso, para todo $y \in Ma$, temos $y\theta_{a^{-1}}\theta_a = ya^{-1}a = y$, logo $\theta_a^{-1} = \theta_{a^{-1}}$ e N é fechado para funções inversas.

Consideremos agora
$$\begin{aligned}\theta\colon M &\to N\\ a &\mapsto \theta_a.\end{aligned}$$

Resulta do que vimos anteriormente que θ é um homomorfismo sobrejectivo de monoides. Por outro lado, sejam $a, b \in M$ tais que $\theta_a = \theta_b$. Então $aa^{-1} \in Ma^{-1} = \mathrm{dom}\theta_a = \mathrm{dom}\theta_b$ e logo

$$a = (aa^{-1})\theta_a = (aa^{-1})\theta_b = (aa^{-1})b,$$

donde resulta que $a \leq b$. Reciprocamente, obtemos $b \leq a$, logo $a = b$ e θ é um isomorfismo. □

Exercício 2.5 *Dado um conjunto X, designamos por $S(X)$ o submonoide de $T(X)$ constituído pelas permutações de X. Mostre que:*

(i) *$S(X)$ é um grupo;*

(ii) *dado um grupo G, existe um conjunto X tal que G é isomorfo a um subgrupo de $S(X)$ (Teorema de Cayley).* □

3 Grupos livres

Vamos agora demonstrar a existência, para qualquer conjunto X, de um grupo $FG(X)$, dito o *grupo livre* sobre X, que satisfaz a propriedade universal relativamente à classe de todos os grupos. O conhecimento da estrutura do grupo livre é essencial para compreender o monoide inverso livre. Em termos de teoria combinatória de grupos, [9] constitui uma boa referência.

Seja X um conjunto. Definimos um conjunto $X^{-1} = \{x^{-1}; x \in X\}$ de inversos formais dos elementos de X, isto é, um conjunto X^{-1} disjunto de X tal que

$$\begin{aligned} {}^{-1} : X &\to X^{-1} \\ x &\mapsto x^{-1} \end{aligned}$$

é uma bijecção. Vamos fixar a notação

$$\overline{X} = X \cup X^{-1}.$$

Estendemos a função ${}^{-1}$ a uma involução do monoide livre $\overline{X}^*$ através de

$$(x^{-1})^{-1} = x \qquad (x \in X),$$

$$(x_1 ... x_n)^{-1} = x_n^{-1} ... x_1^{-1} \qquad (x_i \in \overline{X}),$$

$$1^{-1} = 1.$$

Seja π a congruência em $\overline{X}^*$ gerada pela relação

$$\{(uu^{-1}, 1);\ u \in \overline{X}^*\}$$

e seja $FG(X) = \overline{X}^*/\pi$.

Teorema 3.1 *(i) $FG(X)$ é um grupo;*

(ii) se G é um grupo e $\varphi\colon X \to G$ é uma função qualquer, então existe um e um só homomorfismo $\Phi\colon FG(X) \to G$ tal que o diagrama

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[d, "\epsilon"'] & G \\ FG(X) \arrow[ur, "\Phi"'] & \end{tikzcd}$$

comuta, onde $\epsilon\colon X \to FG(X)$ é definida por $x\epsilon = x\pi$.

Dem. (i) Para todo $u \in \overline{X}^*$, temos

$$(u\pi)(u^{-1}\pi) = (uu^{-1})\pi = 1\pi = (u^{-1}u)\pi = (u^{-1}\pi)(u\pi),$$

logo $FG(X)$ é um grupo.

(ii) Seja $\varphi\colon X \to G$ uma função de X num grupo G. Podemos estender φ a uma função $\varphi_1 : \overline{X} \to G$ fazendo $x^{-1}\varphi = (x\varphi)^{-1}$ para todo $x \in X$. Pelo Teorema 1.6, existe um e um só homomorfismo $\Phi_1\colon \overline{X}^* \to G$ tal que o diagrama

$$\begin{tikzcd} \overline{X} \arrow[r, "\varphi_1"] \arrow[d, hook] & G \\ \overline{X}^* \arrow[ur, "\Phi_1"'] & \end{tikzcd}$$

comuta. Além disso, para quaisquer $x_i \in \overline{X}$, temos

$$\begin{aligned} (x_1...x_n)^{-1}\Phi_1 &= (x_n^{-1}...x_1^{-1})\Phi_1 = (x_n^{-1}\varphi_1)...(x_1^{-1}\varphi_1) \\ &= (x_n\varphi_1)^{-1}...(x_1\varphi_1)^{-1} = [(x_1\varphi_1)...(x_n\varphi_1)]^{-1} \\ &= [(x_1...x_n)\Phi_1]^{-1}, \end{aligned}$$

logo $u^{-1}\Phi_1 = (u\Phi_1)^{-1}$ para todo $u \in \overline{X}^*$. Como G é um grupo, resulta que $\pi \subseteq \mathrm{Ker}\Phi_1$; pelo Teorema 1.1(ii), podemos definir um homomorfismo $\Phi\colon FG(X) \to G$ por $(u\pi)\Phi = u\Phi_1$. Para todo $x \in X$, temos

$$x\epsilon\Phi = (x\pi)\Phi = x\Phi_1 = x\varphi_1 = x\varphi,$$

logo Φ satisfaz as condições do enunciado.

A unicidade de Φ resulta do facto de $FG(X)$ ser gerado, enquanto grupo, pelos elementos $x\pi$ ($x \in X$). $\square$

Para resolver o problema da palavra para a congruência π, precisamos de introduzir alguns conceitos. Dadas palavras $u, v \in X^*$, dizemos que v é um *factor* de u se $u = avb$ para algumas palavras $a, b \in X^*$. Uma palavra $u \in \overline{X}^*$ diz-se *reduzida* se não tiver factores da forma xx^{-1}, com $x \in \overline{X}$. Designamos o subconjunto das palavras reduzidas de $\overline{X}^*$ por R_X.

Sejam $u, v \in \overline{X}^*$. Dizemos que v se obtém a partir de u por *redução simples* e escrevemos $u \vdash v$ se existirem $a, b \in \overline{X}^*$ e $x \in \overline{X}$ tais que $u = axx^{-1}b$ e $v = ab$. Dizemos que v se obtém a partir de u por *redução* e escrevemos $u \overset{*}{\vdash} v$ se $v = u$ ou v resulta de u por um número finito de reduções simples. No resultado seguinte provamos a chamada *confluência* do processo de redução.

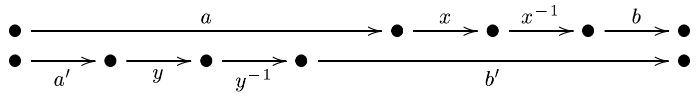
Lema 3.2 *Sejam $u, v, w \in \overline{X}^*$.*

(i) Se $u \vdash v$ e $u \vdash w$, então $v = w$ ou existe $z \in \overline{X}^*$ tal que $v \vdash z$ e $w \vdash z$.

(ii) Se $u \overset{*}{\vdash} v$ e $u \overset{*}{\vdash} w$, então existe $t \in \overline{X}^*$ tal que $v \overset{*}{\vdash} t$ e $w \overset{*}{\vdash} t$.

(iii) Existe uma e uma só palavra $s \in R_X$ tal que $u \overset{*}{\vdash} s$.

Dem. (i) Sejam $a, b, a', b' \in \overline{X}^*$ e $x, y \in \overline{X}$ tais que $u = axx^{-1}b = a'yy^{-1}b'$, $v = ab$ e $w = a'b'$. Se $-1 \leq |\,a\,| - |\,a'\,| \leq 1$, é fácil de ver que $v = w$. Caso contrário, podemos assumir que $|\,a\,| \geq |\,a'\,| + 2$ e podemos escrever $a = a'yy^{-1}p$ e $b' = pxx^{-1}b$ para algum $p \in \overline{X}^*$.



Fazendo $z = a'pb$, é imediato que $v \vdash z$ e $w \vdash z$.

(ii) Resulta imediatamente de (i), considerando um diagrama do tipo

$$
\begin{array}{ccccccccc}
u & = & u_{11} & \longrightarrow & u_{12} & \longrightarrow \; \cdots\cdots \; \longrightarrow & u_{1n} & = & v \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & u_{21} & \longrightarrow & u_{22} & \longrightarrow \; \cdots\cdots \; \longrightarrow & u_{2n} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
w & = & u_{m1} & \longrightarrow & u_{m2} & \longrightarrow \; \cdots\cdots \; \longrightarrow & u_{mn} & = & t
\end{array}
$$

onde $a \to b$ representa $a = b$ ou $a \vdash b$.

(iii) Como $a \vdash b$ implica $\mid b \mid < \mid a \mid$ para todos $a, b \in \overline{X}^*$, qualquer cadeia de reduções é finita e existe necessariamente uma palavra $s \in R_X$ obtida a partir de u por redução. A unicidade resulta de (ii), pois uma palavra reduzida não admite reduções simples. $\square$

Designamos por $\iota\colon \overline{X}^* \to R_X$ a função que associa a cada palavra $u \in \overline{X}^*$ a única palavra $s \in R_X$ tal que $u \overset{*}{\vdash} s$.

Exemplo 3.3 *Seja $X = \{x, y, z\}$. Então*

$$\begin{aligned}(yxyy^{-1}x^{-1}z^{-1}zy^{-1})\iota &= 1,\\ (xyx^{-1})\iota &= xyx^{-1},\\ 1\iota &= 1. \ \square\end{aligned}$$

Teorema 3.4 *(i) Para todos $u, v \in \overline{X}^*$,*

$$u\pi = v\pi \Leftrightarrow u\iota = v\iota.$$

(ii) O problema da palavra para $Mon < X; \pi >$ é decidível.

Dem. (i) Para mostrar a implicação directa, basta observar que $(aww^{-1}b)\iota = (ab)\iota$ para todos $a, b, w \in \overline{X}^*$. Reciprocamente, sejam $u, v \in \overline{X}^*$ tais que $u\iota = v\iota$. Resulta das definições que $u\pi = (u\iota)\pi = (v\iota)\pi = v\pi$.

(ii) Dados $u, v \in \overline{X}^*$, podemos construir efectivamente $u\iota$ e $v\iota$ e determinar se são ou não iguais. $\square$

Seja $\circ$ a operação binária em R_X definida por $u \circ v = (uv)\iota$. Como a redução é confluente, $\circ$ é associativa, e resulta imediatamente que $(R_X, \circ)$ constitui um grupo. Pelo teorema anterior,

$$\begin{aligned}FG(X) &\to (R_X, \circ)\\ u\pi &\mapsto u\iota\end{aligned}$$

é um isomorfismo, logo $(R_X, \circ)$ pode ser visto como o grupo livre sobre X. Embora não referido explicitamente, este facto estará subjacente em muitos resultados posteriores.

Exercício 3.5 *Seja $g \in FG(X)$ e seja $n \geq 1$. Mostre que*

$$g^n = 1 \Rightarrow g = 1. \ \square$$

Uma apresentação de grupos é uma expressão formal do tipo $Gp < X; R >$, onde X designa um conjunto e R uma relação em $\overline{X}^*$. O grupo definido por esta apresentação é o quociente $G = \overline{X}^*/(\pi \cup R)^\sharp$.

4 Monoides inversos livres

Nesta secção demonstraremos a existência, para qualquer conjunto X, de um monoide inverso $FIM(X)$, dito o *monoide inverso livre* sobre X, que satisfaz a propriedade universal relativamente à classe de todos os monoides inversos.

Seja X um conjunto. Tal como no caso do grupo livre, consideramos de novo o monoide livre $\overline{X}^*$ e a involução

$$\begin{aligned} \overline{X}^* &\to \overline{X}^* \\ u &\mapsto u^{-1}. \end{aligned}$$

Seja ρ a congruência em $\overline{X}^*$ gerada pela relação

$$\{(uu^{-1}u, u); u \in \overline{X}^*\} \cup \{(uu^{-1}vv^{-1}, vv^{-1}uu^{-1}); u, v \in \overline{X}^*\}.$$

Dizemos que ρ é a *congruência de Vagner* em $\overline{X}^*$ e definimos $FIM(X) = \overline{X}^*/\rho$.

Teorema 4.1 *(i) $FIM(X)$ é um monoide inverso;*

(ii) se M é um monoide inverso e $\varphi\colon X \to M$ é uma função qualquer, então existe um e um só homomorfismo $\Phi\colon FIM(X) \to M$ tal que o diagrama

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[d, "\epsilon"'] & M \\ FIM(X) \arrow[ur, "\Phi"'] & \end{tikzcd}$$

comuta, onde $\epsilon\colon X \to FIM(X)$ é definida por $x\epsilon = x\rho$.

Dem. (i) Para todo $u \in \overline{X}^*$, temos $u\rho = (uu^{-1}u)\rho = (u\rho)(u^{-1}\rho)(u\rho)$, logo $FIM(X)$ é regular.

Suponhamos agora que $e\rho \in E[FIM(X)]$. Então

$$\begin{aligned} e\rho = e^2\rho &= [e(e^{-1}e)(ee^{-1})e]\rho \\ &= [e(ee^{-1})(e^{-1}e)e]\rho \\ &= (ee^{-1})\rho(e^{-1}e)\rho. \end{aligned}$$

Dados $e\rho, f\rho \in E[FIM(X)]$, resulta que

$$\begin{aligned} (e\rho)(f\rho) &= (ee^{-1})\rho(e^{-1}e)\rho(ff^{-1})\rho(f^{-1}f)\rho \\ &= (ff^{-1})\rho(f^{-1}f)\rho(ee^{-1})\rho(e^{-1}e)\rho \\ &= (f\rho)(e\rho) \end{aligned}$$

e $FIM(X)$ é um monoide inverso pelo Teorema 2.1. Note-se ainda que $(u\rho)^{-1} = u^{-1}\rho$ para todo $u \in \overline{X}^*$.

(ii) Seja $\varphi\colon X \to M$ uma função de X num monoide inverso M. Analogamente ao Teorema 3.1, podemos estender φ a uma função $\varphi_1\colon \overline{X} \to M$ fazendo $x^{-1}\varphi = (x\varphi)^{-1}$

para todo $x \in X$. Pelo Teorema 1.6, existe um e um só homomorfismo $\Phi_1 \colon \overline{X}^* \to M$ tal que o diagrama

$$\begin{tikzcd} \overline{X} \arrow[r, "\varphi_1"] \arrow[d, hook] & M \\ \overline{X}^* \arrow[ur, "\Phi_1"'] & \end{tikzcd}$$

comuta. Além disso, para quaisquer $x_i \in \overline{X}$, temos também

$$\begin{aligned}(x_1 ... x_n)^{-1}\Phi_1 &= (x_n^{-1} ... x_1^{-1})\Phi_1 = (x_n^{-1}\varphi_1)...(x_1^{-1}\varphi_1)\\ &= (x_n\varphi_1)^{-1}...(x_1\varphi_1)^{-1} = [(x_1\varphi_1)...(x_n\varphi_1)]^{-1}\\ &= [(x_1 ... x_n)\Phi_1]^{-1},\end{aligned}$$

logo $u^{-1}\Phi_1 = (u\Phi_1)^{-1}$ para todo $u \in \overline{X}^*$. Como M é inverso, resulta que $\rho \subseteq \mathrm{Ker}\Phi_1$ e, pelo Teorema 1.1(ii), podemos definir um homomorfismo $\Phi \colon FIM(X) \to M$ por $(u\rho)\Phi = u\Phi_1$. Para todo $x \in X$, temos $x\epsilon\Phi = (x\rho)\Phi = x\Phi_1 = x\varphi_1 = x\varphi$, logo Φ satisfaz as condições do enunciado.

A unicidade de Φ resulta do facto de $FIM(X)$ ser gerado, enquanto monoide inverso, pelos elementos $x\rho$ $(x \in X)$. $\square$

A existência do monoide inverso livre foi demonstrada em 1961 por V. V. Vagner [28]. Naturalmente, qualquer progresso significativo na compreensão da estrutura de $FIM(X)$ dependia da resolução do problema da palavra para a congruência de Vagner ρ. Só 12 anos mais tarde é que este problema seria resolvido. Para apresentar a solução, vamos necessitar de algumas noções de teoria de linguagens e autómatos.

Exercício 4.2 *Seja X um conjunto não vazio e seja $x \in X$. Seja R um subconjunto finito de*

$$\{(uu^{-1}u, u); u \in \overline{X}^*\} \cup \{(uu^{-1}vv^{-1}, vv^{-1}uu^{-1}); u, v \in \overline{X}^*\},$$

e seja $n \in \mathbf{N}$ tal que $|\,a\,|, |\,b\,| > n$ para todo $(a, b) \in R$. Dada $u \in \overline{X}^*$, escrevemos $u \models Y$ se existir um factor v de u tal que $v\iota = x^n$.

Mostre que

$$u \models Y \text{ e } uR^\sharp = u'R^\sharp \ \Rightarrow \ u' \models Y. \ \square$$

O exercício anterior pode ser usado para obter o resultado seguinte, provado originalmente por B. Schein em [20].

Exercício 4.3 *Mostre que se X é um conjunto não vazio, a congruência de Vagner ρ em $\overline{X}^*$ não é finitamente gerada.* $\square$

5 Autómatos

Vamos agora introduzir algumas noções básicas sobre autómatos. Para uma abordagem geral desta matéria, ver [5] ou [7].

Seja X um alfabeto. Um subconjunto $L \subseteq X^*$ diz-se uma X-*linguagem*. Um X-1-*grafo* é um par ordenado $\Gamma = (V, E)$, onde V é um conjunto e

$$E \subseteq V \times (X \cup \{1\}) \times V.$$

Escrevemos $V(\Gamma) = V$ e $E(\Gamma) = E$, e designamos os seus elementos por *vértices* e *arestas* de Γ, respectivamente. Dizemos que Γ é *finito* se V e E forem finitos. Se $E \subseteq V \times X \times V$, dizemos que Γ é um X-*grafo*. Por vezes, será conveniente usar a notação

$$E^1(\Gamma) = E(\Gamma) \cup \{(q, 1, q);\ q \in V(\Gamma)\}.$$

Seja Γ um X-1-grafo. Um *caminho* em Γ é uma sequência do tipo

$$q_0 \xrightarrow{x_1} q_1 \xrightarrow{x_2} \ldots \xrightarrow{x_n} q_n$$

onde $n \geq 0$ e $(q_{j-1}, x_j, q_j) \in V(\Gamma)$ para todo $j \in \{1, ..., n\}$. A palavra $x_1...x_n$ diz-se o *rótulo* do caminho (assumimos que 1 é a palavra vazia em X). Se $n \geq 1$, o caminho diz-se *não-trivial*, e se $q_n = q_0$, o caminho diz-se *fechado*. Dizemos que Γ é *conexo* se, para todos $p, q \in V(\Gamma)$, existir um caminho em Γ da forma $p \to q$. Dizemos que Γ é *determinístico* se for um X-grafo e

$$(p, x, q), (p, x, q') \in E(\Gamma) \Rightarrow q = q'$$

para todos $p, q, q' \in V(\Gamma)$ e $x \in X$. Dizemos que Γ é *injectivo* se satisfizer a condição dual

$$(p, x, q), (p', x, q) \in E(\Gamma) \Rightarrow p = p'$$

para todos $p, p', q \in V(\Gamma)$ e $x \in X$.

Dado um conjunto X, definimos um X-1-*autómato* como sendo uma estrutura da forma $\mathcal{A} = (I, \Gamma, F)$, onde Γ é um X-1-grafo e $I, F \subseteq V(\Gamma)$. Dizemos que I, F e Γ são, respectivamente, o conjunto dos *vértices iniciais*, conjunto dos *vértices finais* e *grafo* de $\mathcal{A}$. Se Γ for um X-grafo, dizemos que $\mathcal{A}$ é um X-*autómato*. Podemos denotar por $V(\mathcal{A})$ o conjunto dos vértices do grafo de $\mathcal{A}$ e por $E(\mathcal{A})$ o conjunto das arestas do grafo de $\mathcal{A}$. Na descrição gráfica de um autómato, um vértice inicial i e um vértice final f são identificados respectivamente pelos símbolos

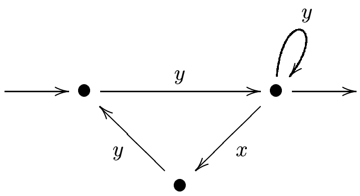
$$\to i \qquad \text{e} \qquad f \to$$

Um *caminho* em $\mathcal{A}$ é um caminho

$$q_0 \xrightarrow{x_1} q_1 \xrightarrow{x_2} \ldots \xrightarrow{x_n} q_n$$

no grafo de $\mathcal{A}$. Se $q_0 \in I$ e $q_n \in F$, o caminho diz-se *bem-sucedido*. A linguagem *reconhecida* por $\mathcal{A}$ é a linguagem $L(\mathcal{A})$ constituída pelos rótulos dos caminhos bem-sucedidos de $\mathcal{A}$. Um X-1-autómato diz-se finito (determinístico, conexo) se o seu grafo for finito (determinístico, conexo). É ainda habitual exigir que um autómato determinístico tenha um único vértice inicial. Convenções semelhantes serão usadas para outros conceitos.

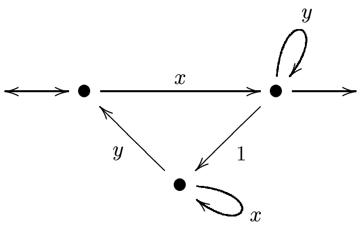
Exemplo 5.1 *Seja $X = \{x, y\}$ e seja $\mathcal{A}$ o X-autómato finito descrito por*



O autómato $\mathcal{A}$ é determinístico, injectivo e conexo, e

$$L(\mathcal{A}) = (yy^*xy)^*yy^*. \ \square$$

Exemplo 5.2 *Seja $X = \{x, y\}$ e seja $\mathcal{B}$ o X-1-autómato finito descrito por*



Então $L(\mathcal{B}) = (xy^*x^*y)^*(1 \cup xy^*)$. $\square$

Uma X-linguagem L diz-se *reconhecível* se $L = L(\mathcal{A})$ para algum X-autómato finito $\mathcal{A}$. Designamos o conjunto das X-linguagens reconhecíveis por Rec$X$.

É fácil de ver que toda a linguagem reconhecível é *recursiva*, no seguinte sentido: dado um X-autómato finito $\mathcal{A}$ e $u \in X^*$, é possível determinar efectivamente se $u \in L(\mathcal{A})$ ou não. Com efeito, o número de caminhos de rótulo u em $\mathcal{A}$ é finito; basta verificar se algum desses caminhos é bem-sucedido.

Vamos agora mostrar que a classe das linguagens reconhecidas por X-1-autómatos finitos é ainda Rec$X$.

Teorema 5.3 *Seja $\mathcal{A} = (I, \Gamma, F)$ um X-1-autómato finito. Então podemos construir efectivamente um X-autómato finito $\mathcal{A}' = (I', \Gamma', F')$ tal que $L(\mathcal{A}') = L(\mathcal{A})$ e $V(\Gamma') = V(\Gamma)$.*

Dem. Seja

$$U = \{(p, q) \in V(\Gamma) \times V(\Gamma) : \text{ existe um caminho } p \xrightarrow{1} q \text{ em } \mathcal{A}\}.$$

Obviamente, se existir um caminho $\omega : p \xrightarrow{1} q$ em $\mathcal{A}$, então podemos assumir que $|\,\omega\,| \leq |\,V(\Gamma)\,|$; resulta assim que é decidível se um tal caminho existe e logo U é efectivamente construível.

Seja $E_0 = \{(p, x, q) \in E(\Gamma) : x \in X\}$. Definimos um X-grafo Γ' por:

- $V(\Gamma') = V(\Gamma)$,
- $E(\Gamma') = \{(p, x, r);\ (p, x, q) \in E_0 \quad \text{e} \quad (q, r) \in U\}$,

e um X-autómato finito $\mathcal{A}' = (I', \Gamma', F)$, onde

$$I' = \{q \in V(\Gamma) : (i, q) \in U \text{ para algum } i \in I\}.$$

Suponhamos que $u \in L(\mathcal{A})$. Então existe um caminho em $\mathcal{A}$ da forma

$$\to q_0 \xrightarrow{1} p_1 \xrightarrow{u_1} q_1 \xrightarrow{1} p_2 \xrightarrow{u_2} \dots \xrightarrow{u_m} q_m \xrightarrow{1} p_{m+1} \to$$

com $u = u_1 \dots u_m$ ($m \geq 0$), tal que todas as arestas nos caminhos $p_j \xrightarrow{u_j} q_j$ estão em E_0. Além disso, podemos factorizar o caminho $p_j \xrightarrow{u_j} q_j$ na forma

$$p_j \xrightarrow{v_j} r_j \xrightarrow{x_j} q_j,$$

onde $x_j \in X$ e $v_j \in X^*$. Resulta das definições que $p_1 \in I'$ e $(r_j, x_j, p_{j+1}) \in E(\Gamma')$ para todo $j = 1, \dots, m$. Logo temos em $\mathcal{A}'$ um caminho da forma

$$\to p_1 \xrightarrow{v_1} r_1 \xrightarrow{x_1} p_2 \xrightarrow{v_2} r_2 \xrightarrow{x_2} \dots \xrightarrow{v_m} r_m \xrightarrow{x_m} p_{m+1} \to$$

e $u = v_1 x_1 v_2 x_2 \dots v_m x_m \in L(\mathcal{A}')$.

Reciprocamente, suponhamos que $u \in L(\mathcal{A}')$. Então existe em $\mathcal{A}'$ um caminho da forma

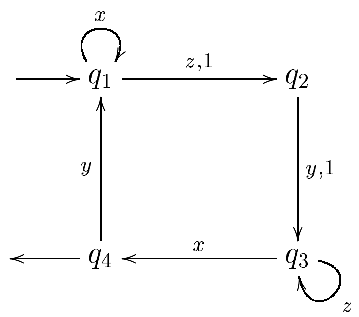
$$\to q_0 \xrightarrow{x_1} q_1 \xrightarrow{x_2} \dots \xrightarrow{x_n} q_n \to$$

com $u = x_1 \dots x_n$ e $x_j \in X$. Resulta da definição de $E(\Gamma')$ que, para todo $j \in \{1, \dots, n\}$, existe $(q_{j-1}, x_j, p_j) \in E_0$ tal que $(p_j, q_j) \in U$. Por outro lado, $(i, q_0) \in U$ para algum $i \in I$, logo existe em $\mathcal{A}$ um caminho da forma

$$\to i \xrightarrow{1} q_0 \xrightarrow{x_1} p_1 \xrightarrow{1} q_1 \xrightarrow{x_2} \dots \xrightarrow{x_n} p_n \xrightarrow{1} q_n \to$$

e logo $u = x_1 \dots x_n \in L(\mathcal{A}')$. Logo $L(\mathcal{A}) = L(\mathcal{A}')$. $\square$

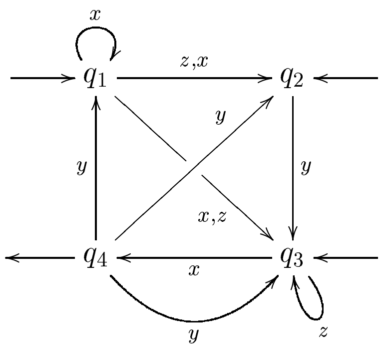
Exemplo 5.4 *Seja $X = \{x, y, z\}$ e seja $\mathcal{A}$ o X-1-autómato descrito por*



Temos

$$U = \{(q_j, q_j);\ j \in \{1, 2, 3, 4\}\} \cup \{(q_1, q_2), (q_1, q_3), (q_2, q_3)\},$$

logo o X-autómato $\mathcal{A}'$ descrito por



reconhece $L(\mathcal{A})$. $\square$

A família Rec$X$ é fechada para diversos operadores Booleanos e algébricos. O resultado seguinte evidencia algumas dessas propriedades de fecho, que se revelarão úteis posteriormente.

Teorema 5.5 *Sejam* $\mathcal{A}$ *e* $\mathcal{A}'$ X*-autómatos finitos. Então podemos construir efectivamente* X*-autómatos finitos* $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ *e* $\mathcal{A}_4$ *tais que:*

(i) $L(\mathcal{A}_1) = L(\mathcal{A}) \cup L(\mathcal{A}')$;

(ii) $L(\mathcal{A}_2) = L(\mathcal{A}) \cap L(\mathcal{A}')$;

(iii) $L(\mathcal{A}_3) = L(\mathcal{A}) \cdot L(\mathcal{A}')$;

(iv) $L(\mathcal{A}_4) = [L(\mathcal{A})]^*$.

Dem. Suponhamos que $\mathcal{A} = (I, \Gamma, F)$ e $\mathcal{A}' = (I', \Gamma', F')$. Sem perda de generalidade, podemos assumir que $V(\Gamma) \cap V(\Gamma') = \emptyset$.

(i) Seja Γ_1 o X-grafo definido por

- $V(\Gamma_1) = V(\Gamma) \cup V(\Gamma')$,
- $E(\Gamma_1) = E(\Gamma) \cup E(\Gamma')$.

e seja $\mathcal{A}_1 = (I \cup I', \Gamma_1, F \cup F')$. É imediato que $L(\mathcal{A}_1) = L(\mathcal{A}) \cup L(\mathcal{A}')$.

(ii) Seja Γ_2 o X-grafo definido por

- $V(\Gamma_2) = V(\Gamma) \times V(\Gamma')$,
- $E(\Gamma_2) = \{((p,p'), x, (q,q'));\ (p,x,q) \in E(\Gamma),\ (p',x,q') \in E(\Gamma')\}$.

e seja $\mathcal{A}_2 = (I \times I', \Gamma_2, F \times F')$. Por definição,

$$\rightarrow (q_0, q_0') \xrightarrow{x_1} (q_1, q_1') \xrightarrow{x_2} \ldots \xrightarrow{x_n} (q_n, q_n') \rightarrow$$

é um caminho em $\mathcal{A}_2$ se e só se

$$\rightarrow q_0 \xrightarrow{x_1} q_1 \xrightarrow{x_2} \ldots \xrightarrow{x_n} q_n \rightarrow$$

é um caminho em $\mathcal{A}$ e

$$\to q_0' \xrightarrow{x_1} q_1' \xrightarrow{x_2} \dots \xrightarrow{x_n} q_n' \to$$

é um caminho em $\mathcal{A}'$. Logo $L(\mathcal{A}_2) = L(\mathcal{A}) \cap L(\mathcal{A}')$.

(iii) Seja Γ_3 o X-1-grafo definido por

- $V(\Gamma_3) = V(\Gamma) \cup V(\Gamma')$,
- $E(\Gamma_3) = E(\Gamma) \cup E(\Gamma') \cup \{(f, 1, i'); f \in F, i' \in I'\}$.

e seja $\mathcal{A}_3' = (I, \Gamma_3, F')$. É imediato que $L(\mathcal{A}_3') = L(\mathcal{A}) \cdot L(\mathcal{A}')$. Pelo teorema anterior, podemos construir efectivamente um X-autómato finito $\mathcal{A}_3$ tal que $L(\mathcal{A}_3) = L(\mathcal{A}_3')$.

(iv) Seja Γ_4 o X-1-grafo definido por

- $V(\Gamma_4) = V(\Gamma)$,
- $E(\Gamma_4) = E(\Gamma) \cup \{(f, 1, i); f \in F, i \in I\}$.

e seja $\mathcal{A}_4' = (I, \Gamma_4, F)$. É imediato que $[L(\mathcal{A})]^* = L(\mathcal{A}_4') \cup \{1\}$. Pelo teorema anterior, podemos construir efectivamente um X-autómato finito $\mathcal{A}_4''$ tal que $L(\mathcal{A}_4'') = L(\mathcal{A}_4')$. Considerando o X-autómato $\to i \to$, que reconhece $\{1\}$, resulta de (i) que podemos construir efectivamente um X-autómato finito $\mathcal{A}_4$ tal que $L(\mathcal{A}_4) = [L(\mathcal{A})]^*$. $\square$

Exercício 5.6 *Seja $\mathcal{A} = (i, \Gamma, F)$ um X-autómato finito determinístico. Construa um X-autómato finito determinístico $\mathcal{A}'$ tal que $L(\mathcal{A}') = X^* - L(\mathcal{A})$.* $\square$

Usando o teorema anterior, vamos mostrar que toda a X-linguagem finita é reconhecível. A linguagem vazia é reconhecida por qualquer autómato sem estados iniciais. Por (i), basta-nos mostrar que toda a X-linguagem com um único elemento é reconhecível. Como já foi visto que 1 é reconhecível, basta-nos mostrar, por (iii), que $\{x\}$ é reconhecível para todo $x \in X$. Obviamente, o X-autómato $\to i \xrightarrow{x} f \to$ reconhece $\{x\}$, logo todas as X-linguagens finitas são reconhecíveis.

Exercício 5.7 *Mostre que é decidível se, dado um X-autómato finito $\mathcal{A}$,*

(i) $L(\mathcal{A})$ é vazia;

(ii) $L(\mathcal{A})$ é finita. $\square$

6 Autómatos duais e inversos

Vamos agora considerar grafos sobre um alfabeto da forma $\overline{X}$. Seja Γ um $\overline{X}$-1-grafo. Dizemos que Γ é *dual* se for conexo e

$$(p, x, q) \in E(\Gamma) \Leftrightarrow (q, x^{-1}, p) \in E(\Gamma)$$

para todos $p, q \in V(\Gamma)$ e $x \in X \cup 1$. Arestas da forma (p, x, q) e (q, x^{-1}, p) dizem-se duais. É habitual, ao descrever um grafo dual, representar uma única aresta de cada par de arestas duais. Dizemos que Γ é *inverso* se for dual e determinístico.

Note-se que um $\overline{X}$-grafo inverso é necessariamente injectivo.

Um $\overline{X}$-1-autómato da forma $\mathcal{A} = (i, \Gamma, f)$, onde Γ é um $\overline{X}$-1-grafo dual e $i, f \in V(\Gamma)$, diz-se um $\overline{X}$-1-autómato *dual*. Se Γ for inverso, dizemos que $\mathcal{A}$ é *inverso*.

Exemplo 6.1 *Seja $X = \{x\}$ e seja $\mathcal{A}$ o $\overline{X}$-autómato dual descrito por*

$$\to i \xrightarrow{x} q \xrightarrow{x} f \to$$

Então $\mathcal{A}$ é inverso e $L(\mathcal{A}) = x(x^{-1}x \cup xx^{-1})^*x$. $\square$

Dados dois X-autómatos da forma $\mathcal{A} = (i, \Gamma, f)$ e $\mathcal{A}' = (i', \Gamma', f')$, dizemos que $\mathcal{A}$ e $\mathcal{A}'$ são *isomorfos* e escrevemos $\mathcal{A} \simeq \mathcal{A}'$ se existir uma bijecção

$$\varphi \colon V(\Gamma) \to V(\Gamma')$$

tal que:

(i) $i\varphi = i'$;

(ii) $f\varphi = f'$;

(iii) $\forall p, q \in V(\Gamma)\ \forall x \in X,\ (p, x, q) \in E(\Gamma) \Leftrightarrow (p\varphi, x, q\varphi) \in E(\Gamma')$.

Por outras palavras, dois X-autómatos são isomorfos se diferem apenas na designação dos vértices, coincidindo em tudo o mais. No que nos diz respeito, consideraremos autómatos isomorfos como sendo essencialmente o mesmo autómato.

Teorema 6.2 *Sejam $\mathcal{A} = (i, \Gamma, f)$ e $\mathcal{A}' = (i', \Gamma', f')$ dois $\overline{X}$-autómatos inversos. Então $\mathcal{A} \simeq \mathcal{A}'$ se e só se $L(\mathcal{A}) = L(\mathcal{A}')$.*

Dem. Suponhamos que $\mathcal{A} \simeq \mathcal{A}'$ e que $\varphi \colon V(\Gamma) \to V(\Gamma')$ é um isomorfismo. Então, para todos $q_j \in V(\Gamma)$ e $x_j \in \overline{X}$,

$$i = q_0 \xrightarrow{x_1} q_1 \xrightarrow{x_2} \ldots \xrightarrow{x_n} q_n = f$$

é um caminho em $\mathcal{A}$ se e só se

$$i' = q_0\varphi \xrightarrow{x_1} q_1\varphi \xrightarrow{x_2} \ldots \xrightarrow{x_n} q_n\varphi = f'$$

for um caminho em $\mathcal{A}'$. Logo $L(\mathcal{A}) = L(\mathcal{A}')$.

Reciprocamente, suponhamos que $L(\mathcal{A}) = L(\mathcal{A}')$. Seja $q \in V(\Gamma)$. Como Γ é conexo, existe em $\mathcal{A}$ um caminho da forma

$$i \xrightarrow{u} q \xrightarrow{v} f.$$

Como $uv \in L(\mathcal{A}) = L(\mathcal{A}')$, existe em $\mathcal{A}'$ um caminho da forma

$$i' \xrightarrow{u} q' \xrightarrow{v} f'.$$

Definimos $q\varphi = q'$. Para ver que φ está bem definida, suponhamos que

$$i \xrightarrow{u_1} q \xrightarrow{v_1} f, \qquad\qquad i' \xrightarrow{u_1} q_1' \xrightarrow{v_1} f'$$

são caminhos em $\mathcal{A}$ e $\mathcal{A}'$, respectivamente. Então $u_1v \in L(\mathcal{A}) = L(\mathcal{A}')$. Como $uv, u_1v \in L(\mathcal{A}')$ e $\mathcal{A}'$ é injectivo, resulta que $\mathcal{A}'$ tem um caminho da forma

$$i' \xrightarrow{u_1} q' \xrightarrow{v} f'.$$

Como $\mathcal{A}'$ é determinístico, resulta que $q_1' = q'$ e φ está bem definida.

Analogamente, podemos definir uma função $\psi \colon V(\Gamma') \to V(\Gamma)$ inversa da função φ, logo φ é bijectiva.

Considerando $q = i$ e $u = 1$, mostramos que $i\varphi = i'$; considerando $q = f$ e $v = 1$, mostramos que $f\varphi = f'$. Finalmente, suponhamos que $(p, x, q) \in E(\Gamma)$ e consideremos um caminho

$$i \xrightarrow{u} p \xrightarrow{x} q \xrightarrow{v} f$$

em $\mathcal{A}$. Então temos em $\mathcal{A}'$ um caminho

$$i' \xrightarrow{u} p' \xrightarrow{x} q' \xrightarrow{v} f'$$

e, por definição de φ, resulta que $p' = p\varphi$ e $q' = q\varphi$. Logo $(p\varphi, x, q\varphi) \in E(\Gamma')$. A implicação recíproca é análoga, logo $\mathcal{A} \simeq \mathcal{A}'$. $\square$

Seja $\mathcal{A} = (i, \Gamma, f)$ um $\overline{X}$-autómato inverso. Um caminho $i \xrightarrow{u} q$ diz-se uma *geodésica* de $\mathcal{A}$ se $\mid u \mid$ for mínimo entre os rótulos dos caminhos de i a q. Uma vez que $\mathcal{A}$ é determinístico, um caminho em $\mathcal{A}$ é determinado pelo seu rótulo; assim, dizemos também que u é uma geodésica.

Lema 6.3 *Seja $\mathcal{A}$ um $\overline{X}$-autómato inverso. Sejam $p, q \in V(\mathcal{A})$ e $u, v \in \overline{X}^*$ tais que u é rótulo de um caminho entre p e q, e $u \overset{*}{\vdash} v$. Então existe um caminho entre p e q de rótulo v.*

Dem. Exercício. $\square$

Resulta do lema anterior que se u é uma geodésica de $\mathcal{A}$ então $u \in R_X$. Dizemos que $\mathcal{A}$ é uma *árvore* se, para todos $p, q \in V(\mathcal{A})$, existe um só caminho entre p e q com rótulo em R_X (pelo Lema 6.3, há pelo menos um tal caminho, já que $\mathcal{A}$ é conexo).

Suponhamos agora que $\mathcal{A} = (i, \Gamma, f)$ é uma árvore, e seja $q \in V(\Gamma)$. Então existe um único caminho de rótulo reduzido entre i e q, que é também o único caminho de comprimento mínimo entre i e q, isto é, uma geodésica; seja g_q o rótulo desse caminho; como $\mathcal{A}$ é determinístico, q é completamente determinado por g_q, e podemos identificar $V(\Gamma)$ com o conjunto $G(\mathcal{A}) = \{g_q;\, q \in V(\Gamma)\}$. A geodésica g_f diz-se a *geodésica principal* de $\mathcal{A}$, sendo designada por $G_p(\mathcal{A})$.

Dadas palavras a e b num alfabeto Y, dizemos que b é *prefixo* de a e escrevemos $b \leq_p a$ se $a = bc$ para algum $c \in Y^*$.

Teorema 6.4 *Seja $\mathcal{A} = (i, \Gamma, f)$ um $\overline{X}$-autómato inverso e seja $v \in \overline{X}^*$. Se $\mathcal{A}$ é uma árvore, então $v \in L(\mathcal{A})$ se e só se*

$$w\iota \in G(\mathcal{A}) \text{ para todo } w \leq_p v$$

e $v\iota = G_p(\mathcal{A})$.

Dem. Suponhamos que $\mathcal{A}$ é uma árvore. Suponhamos que $v \in L(\mathcal{A})$ e seja $w \leq_p v$. Então existe um caminho da forma $i \xrightarrow{w} q$ em $\mathcal{A}$. Pelo Lema 6.3, existe um caminho $i \xrightarrow{w\iota} q$ em $\mathcal{A}$. Como $w\iota \in R_X$, resulta que $w\iota$ é uma geodésica de $\mathcal{A}$. Se $w = v$, então $q = f$, logo $v\iota$ é a geodésica principal de $\mathcal{A}$.

Vamos agora mostrar que se $w\iota \in G(\mathcal{A})$ para todo $w \leq_p v$, então existe um caminho da forma $i \xrightarrow{v} q$ em $\mathcal{A}$, usando indução sobre $|v|$.

A implicação é trivialmente verificada para $|v| = 0$. Suponhamos que é válida para $|v| = k$ ($k \geq 0$), e seja $u \in \overline{X}^*$ tal que $w\iota \in G(\mathcal{A})$ para todo $w \leq_p u$ e $|u| = k+1$. Seja $u = vx$, com $v \in \overline{X}^*$ e $x \in X$. Por hipótese de indução , existe um caminho da forma $i \xrightarrow{v} q$ em $\mathcal{A}$, e consequentemente um caminho $i \xrightarrow{v\iota} q$.

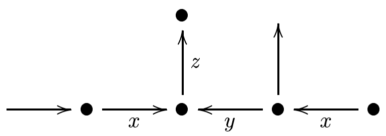
Suponhamos primeiro que $v\iota = zx^{-1}$, com $z \in R_X$. Então temos em $\mathcal{A}$ um caminho $i \xrightarrow{z} p \xrightarrow{x^{-1}} q$ e logo um caminho $i \xrightarrow{v} q \xrightarrow{x} p$ de rótulo u.

Suponhamos agora que $v\iota$ não é da forma zx^{-1}. Então $(v\iota)x = u\iota \in G(\mathcal{A})$, logo $(q, x, r) \in E(\Gamma)$ para algum $r \in V(\Gamma)$ e $i \xrightarrow{v} q \xrightarrow{x} r$ é um caminho em $\mathcal{A}$ de rótulo u. Logo a implicação é válida.

Suponhamos agora que $w\iota \in G(\mathcal{A})$ para todo $w \leq_p v$ e $v\iota = G_p(\mathcal{A})$. Pela implicação que acabámos de demonstrar, existe um caminho $i \xrightarrow{v} q$ em $\mathcal{A}$, e logo um caminho $i \xrightarrow{v\iota} q$. Como $v\iota = G_p(\mathcal{A})$ e $\mathcal{A}$ é determinístico, resulta que $q = f$ e logo $v \in L(\mathcal{A})$. $\square$

Em particular, resulta dos Teoremas 6.2 e 6.4 que se um $\overline{X}$-autómato inverso $\mathcal{A}$ é uma árvore, então $\mathcal{A}$ é completamente determinado pelo seu conjunto de geodésicas e pela sua geodésica principal.

Exemplo 6.5 *Seja $X = \{x, y, z\}$ e seja $\mathcal{A}$ o $\overline{X}$-autómato inverso descrito por*



Então $\mathcal{A}$ é uma árvore, $G(\mathcal{A}) = \{1, x, xz, xy^{-1}, xy^{-1}x^{-1}\}$ e $G_p(\mathcal{A}) = xy^{-1}$. $\square$

Exercício 6.6 *Seja $\mathcal{A} = (i, \Gamma, f)$ um $\overline{X}$-autómato inverso. Mostre que as condições seguintes são equivalentes:*

(i) $\mathcal{A}$ é uma árvore;

(ii) não existe em $\mathcal{A}$ nenhum caminho $i \xrightarrow{u} i$ com $u \in R_X - \{1\}$. $\square$

Seja $\mathcal{A} = (i, \Gamma, f)$ um $\overline{X}$-1-autómato dual. Estabelecemos uma relação $\sim$ em $V(\Gamma)$ do seguinte modo: dados $p, q \in V(\Gamma)$, escrevemos $p \sim q$ se

$$(r, x, p), (r, x, q) \in E^1(\Gamma) \text{ para alguns } r \in V(\Gamma) \text{ e } x \in \overline{X} \cup 1.$$

Suponhamos que $p \sim q$. Adaptando a notação típica das congruências, definimos uma relação de equivalência α em $V(\Gamma)$ do seguinte modo: dado $s \in V(\Gamma)$, escrevemos

$$s\alpha = \begin{cases} \{s\} & \text{se } s \neq p, q \\ \{p, q\} & \text{se } s = p \text{ ou } s = q \end{cases}$$

Definimos o $\overline{X}$-1-grafo Γ/α por

- $V(\Gamma/\alpha) = \{s\alpha;\ s \in V(\Gamma)\}$;
- $E(\Gamma/\alpha) = \{(s\alpha, y, t\alpha);\ (s, y, t) \in E(\Gamma)\}$.

e o $\overline{X}$-1-autómato

$$\mathcal{A}/\alpha = (i\alpha, \Gamma/\alpha, f\alpha).$$

Dizemos que $\mathcal{A}/\alpha$ é o $\overline{X}$-1-autómato obtido a partir de $\mathcal{A}$ por *identificação* dos vértices p e q. Obviamente, $\mathcal{A}/\alpha$ é ainda um $\overline{X}$-1-autómato dual. Se $p \neq q$ e $\mathcal{A}'$ é isomorfo a $\mathcal{A}/\alpha$, escrevemos $\mathcal{A} \vdash \mathcal{A}'$ e dizemos que $\mathcal{A}'$ resulta de $\mathcal{A}$ por uma *redução simples.*

Se $\mathcal{A}' = \mathcal{A}$ ou $\mathcal{A}'$ resulta de $\mathcal{A}$ por um número finito de reduções simples, escrevemos $\mathcal{A} \overset{*}{\vdash} \mathcal{A}'$ e dizemos que $\mathcal{A}'$ resulta de $\mathcal{A}$ por *redução* .

É fácil de ver que um $\overline{X} - 1$-autómato dual é determinístico se e só se não admite reduções simples. Se $\mathcal{A} \overset{*}{\vdash} \mathcal{A}'$ e $\mathcal{A}'$ é determinístico, dizemos que $\mathcal{A}'$ resulta de $\mathcal{A}$ por *redução total.*

Teorema 6.7 *Sejam $\mathcal{A}$, $\mathcal{A}_1$ e $\mathcal{A}_2$ $\overline{X}$-1-autómatos duais.*

(i) Se $\mathcal{A} \vdash \mathcal{A}_1$ e $\mathcal{A} \vdash \mathcal{A}_2$, então $\mathcal{A}_1 = \mathcal{A}_2$ ou existe um $\overline{X}$-1-autómato dual $\mathcal{A}_3$ tal que $\mathcal{A}_1 \vdash \mathcal{A}_3$ e $\mathcal{A}_2 \vdash \mathcal{A}_3$.

(ii) Se $\mathcal{A} \overset{*}{\vdash} \mathcal{A}_1$ e $\mathcal{A} \overset{*}{\vdash} \mathcal{A}_2$, então existe um $\overline{X}$-1-autómato dual $\mathcal{A}_3$ tal que $\mathcal{A}_1 \overset{*}{\vdash} \mathcal{A}_3$ e $\mathcal{A}_2 \overset{*}{\vdash} \mathcal{A}_3$.

(iii) Se $\mathcal{A}$ é finito, então existe um e um só $\overline{X}$-autómato inverso $\mathcal{A}'$ (a menos de isomorfismo) tal que $\mathcal{A} \overset{*}{\vdash} \mathcal{A}'$.

(iv) Se $\mathcal{A} \overset{*}{\vdash} \mathcal{A}_1$, então $L(\mathcal{A}) \subseteq L(\mathcal{A}_1)$.

Dem. (i) Seja $\mathcal{A} = (i, \Gamma, f)$. Sem perda de generalidade, podemos assumir que, para $j = 1, 2$, se tem

$$\mathcal{A}_j = (i\alpha_j, \Gamma/\alpha_j, f\alpha_j),$$

onde α_j designa a relação de equivalência em $V(\Gamma)$ induzida pela identificação dos vértices p_j e q_j, com $p_j \sim q_j$ e $p_j \neq q_j$. Se $\{p_1, q_1\} = \{p_2, q_2\}$, temos $\mathcal{A}_1 = \mathcal{A}_2$, logo podemos assumir que $\{p_1, q_1\} \neq \{p_2, q_2\}$.

Resulta facilmente das definições que $p_2\alpha_1 \sim q_2\alpha_1$ em $V(\Gamma/\alpha_1)$. Seja $\overline{\alpha_2}$ a relação de equivalência em $V(\Gamma/\alpha_1)$ induzida pela identificação dos vértices $p_2\alpha_1$ e $q_2\alpha_1$. Como $\{p_1, q_1\} \neq \{p_2, q_2\}$, temos $p_2\alpha_1 \neq q_2\alpha_1$ e $\mathcal{A}_1 \vdash \mathcal{A}_1/\overline{\alpha_2}$. Analogamente, temos $\mathcal{A}_2 \vdash \mathcal{A}_2/\overline{\alpha_1}$, onde $\overline{\alpha_1}$ designa a relação de equivalência em $V(\Gamma/\alpha_2)$ induzida pela identificação dos vértices $p_1\alpha_2$ e $q_1\alpha_2$. Basta-nos mostrar que $\mathcal{A}_1/\overline{\alpha_2}$ e $\mathcal{A}_2/\overline{\alpha_1}$ são isomorfos.

Consideremos a função

$$\begin{aligned} \varphi\colon V((\Gamma/\alpha_1)/\overline{\alpha_2}) &\to V((\Gamma/\alpha_2)/\overline{\alpha_1}) \\ (p\alpha_1)\overline{\alpha_2} &\mapsto (p\alpha_2)\overline{\alpha_1} \end{aligned}$$

e vejamos que φ está bem definida.

Suponhamos que $(p\alpha_1)\overline{\alpha_2} = (q\alpha_1)\overline{\alpha_2}$. Então $p\alpha_1 = q\alpha_1$ ou $\{p\alpha_1, q\alpha_1\} = \{p_2\alpha_1, q_2\alpha_1\}$.

Se $p\alpha_1 = q\alpha_1$, então $p = q$ ou $\{p, q\} = \{p_1, q_1\}$, o que em qualquer dos casos garante imediatamente $(p\alpha_2)\overline{\alpha_1} = (q\alpha_2)\overline{\alpha_1}$, logo vamos assumir, sem perda de generalidade, que $p\alpha_1 = p_2\alpha_1$ e $q\alpha_1 = q_2\alpha_1$. Então temos

(1) $p = p_2$ ou $\{p, p_2\} = \{p_1, q_1\}$,

(2) $q = q_2$ ou $\{q, q_2\} = \{p_1, q_1\}$,

e logo

(3) $p\alpha_2 = p_2\alpha_2$ ou $\{p\alpha_2, p_2\alpha_2\} = \{p_1\alpha_2, q_1\alpha_2\}$,

(4) $q\alpha_2 = q_2\alpha_2$ ou $\{q\alpha_2, q_2\alpha_2\} = \{p_1\alpha_2, q_1\alpha_2\}$.

Em qualquer dos casos, resulta que $(p\alpha_2)\overline{\alpha_1} = (p_2\alpha_2)\overline{\alpha_1}$ e $(q\alpha_2)\overline{\alpha_1} = (q_2\alpha_2)\overline{\alpha_1}$. Logo $(p\alpha_2)\overline{\alpha_1} = (q\alpha_2)\overline{\alpha_1}$ e φ está bem definida.

Analogamente, definimos a função

$$\begin{aligned} \psi\colon V((\Gamma/\alpha_2)/\overline{\alpha_1}) &\to V((\Gamma/\alpha_1)/\overline{\alpha_2}) \\ (p\alpha_2)\overline{\alpha_1} &\mapsto (p\alpha_1)\overline{\alpha_2} \end{aligned}$$

que é inversa de φ, logo φ é bijectiva. É também imediato que φ preserva os vértices inicial e final.

Finalmente, suponhamos que

$$((p\alpha_1)\overline{\alpha_2}, x, (q\alpha_1)\overline{\alpha_2}) \in E((\Gamma/\alpha_1)/\overline{\alpha_2}),$$

com $x \in \overline{X} \cup 1$. É fácil de ver que existem $p', q' \in V(\Gamma)$ tais que:

$(p'\alpha_1, x, q'\alpha_1) \in E(\Gamma/\alpha_1)$,

$(p'\alpha_1)\overline{\alpha_2} = (p\alpha_1)\overline{\alpha_2}$

$(q'\alpha_1)\overline{\alpha_2} = (q\alpha_1)\overline{\alpha_2}$.

Além disso, existem $p'', q'' \in V(\Gamma)$ tais que:

$(p'', x, q'') \in E(\Gamma)$,

$p''\alpha_1 = p'\alpha_1$,

$q''\alpha_1 = q'\alpha_1$.

Resulta das definições que

$$((p''\alpha_2)\overline{\alpha_1}, x, (q''\alpha_2)\overline{\alpha_1}) \in E((\Gamma/\alpha_2)/\overline{\alpha_1}).$$

Como $(p''\alpha_1)\overline{\alpha_2} = (p\alpha_1)\overline{\alpha_2}$ e φ é bijectiva, resulta que $(p''\alpha_2)\overline{\alpha_1} = (p\alpha_2)\overline{\alpha_1}$. Analogamente, $(q''\alpha_2)\overline{\alpha_1} = (q\alpha_2)\overline{\alpha_1}$. Logo

$$((p\alpha_2)\overline{\alpha_1}, x, (q\alpha_2)\overline{\alpha_1}) \in E((\Gamma/\alpha_2)/\overline{\alpha_1}).$$

A implicação recíproca é análoga, logo φ é um isomorfismo de $\overline{X}$-1-autómatos.

(ii) e (iii) resultam de (i) por um argumento análogo ao da demonstração do Lema 3.2.

(iv) Basta considerar o caso $\mathcal{A} \vdash \mathcal{A}_1$, em que $\mathcal{A}_1 = \mathcal{A}/\alpha$. Se

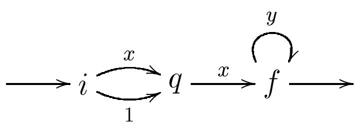
$$i = q_0 \xrightarrow{x_1} q_1 \xrightarrow{x_2} \dots \xrightarrow{x_n} q_n = f$$

é um caminho em $\mathcal{A}$, então

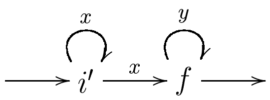
$$i\alpha = q_0\alpha \xrightarrow{x_1} q_1\alpha \xrightarrow{x_2} \dots \xrightarrow{x_n} q_n\alpha = f\alpha$$

é um caminho em $\mathcal{A}_1$, logo $L(\mathcal{A}) \subseteq L(\mathcal{A}_1)$. $\square$

Exemplo 6.8 *Seja $X = \{x, y\}$ e seja $\mathcal{A}$ o $\overline{X}$-1-autómato dual descrito por*



Temos $i \sim q$, logo podemos reduzir $\mathcal{A}$ identificando os vértices i e q, obtendo o $\overline{X}$-autómato dual $\mathcal{A}_1$ descrito por



Como $i' \sim f$, temos $\mathcal{A}_1 \vdash \mathcal{A}_2$, onde $\mathcal{A}_2$ é o $\overline{X}$-autómato dual descrito por

$$\begin{tikzcd} {} \arrow[r] & i'' \arrow[loop above, "x"] \arrow[loop below, "y"] \arrow[r] & {} \end{tikzcd}$$

Como $\mathcal{A}_2$ é inverso, $\mathcal{A}_2$ é o (único) $\overline{X}$-autómato obtido a partir de $\mathcal{A}$ por redução total.

$\square$

Exercício 6.9 *Seja $\mathcal{A}$ um $\overline{X}$-1-autómato dual e suponhamos que $\mathcal{A}'$ resulta de $\mathcal{A}$ por redução total. Dado $p \in V(\mathcal{A})$, seja p' o vértice de $\mathcal{A}'$ resultante de p. Mostre que, para todos $p, q \in V(\mathcal{A})$, $p' = q'$ se e só se existe um caminho $p \xrightarrow{e} q$ em $\mathcal{A}$ com $e\iota = 1$.*

$\square$

7 Árvores de Munn

Vamos agora apresentar o algoritmo descoberto por W. D. Munn [16] em 1974 que resolve o problema da palavra para $Mon < \overline{X}; \rho >$.

Dada uma palavra $u \in \overline{X}^*$, definimos

$$L(u) = \{v \in \overline{X} : v\rho \geq u\rho\},$$

onde $\leq$ designa a ordem parcial natural de $FIM(X)$. Definimos também um $\overline{X}$-autómato dual $Lin(u)$, dito o *autómato linear* de u, do seguinte modo. Se $u = 1$, $Lin(u)$ é o autómato

$$\to q_0 \to$$

Se $u = x_1 ... x_n$, com $x_j \in \overline{X}$, $Lin(u)$ é o autómato dual descrito por

$$\to q_0 \xrightarrow{x_1} q_1 \xrightarrow{x_2} \ldots \xrightarrow{x_n} q_n \to$$

Lema 7.1 *Para todo $u \in \overline{X}^*$, $L(Lin(u)) \subseteq L(u)$.*

Dem. Como $L(Lin(1)) = \{1\} \subseteq L(1)$ trivialmente, vamos assumir que $u = x_1 ... x_n$ ($x_j \in \overline{X}$) e vamos usar indução sobre o comprimento das palavras de $L(Lin(u))$. Como $\{v \in L(Lin(u)) : |v| \leq n\} = \{u\}$, a implicação

$$v \in L(Lin(u)) \Rightarrow v \in L(u)$$

verifica-se sempre que $|v| \leq n$. Suponhamos agora que a implicação é válida sempre que $|v| \leq k$ $(k \geq n)$, e suponhamos que $w \in L(Lin(u))$ é tal que $|w| = k + 1$. Por hipótese, w é rótulo de um caminho bem-sucedido em $Lin(u)$ em que há pelo menos duas inflexões de sentido (pois $|w| > n$). Considerando as duas últimas inflexões de sentido nesse caminho, concluimos facilmente que

$$w = ax_j x_j^{-1} bb^{-1} x_j c$$

para alguns $a, b, c \in \overline{X}$, $j \in \{1, ..., n\}$ e $t \in \{0, ..., j-1\}$ tais que:

- a é rótulo de um caminho de q_0 a q_{j-1};

- b é rótulo de um caminho de q_{j-1} a q_t;

- c é rótulo de um caminho de q_j a q_n.

Mas então

$$w\rho = (ax_jx_j^{-1}bb^{-1}x_jc)\rho = (abb^{-1}x_jx_j^{-1}x_jc)\rho = (abb^{-1}x_jc)\rho.$$

Além disso,

$$abb^{-1}x_jc \in L(Lin(u)) \qquad \text{e} \qquad |abb^{-1}x_jc| = k-1,$$

logo $abb^{-1}x_jc \in L(u)$ por hipótese de indução . Logo $w\rho = (abb^{-1}x_jc)\rho \geq u\rho$ e $w \in L(u)$. Logo $L(Lin(u)) \subseteq L(u)$. $\square$

Lema 7.2 *Seja $u \in \overline{X}^*$ e seja τ uma congruência em $\overline{X}^*$ tal que $\rho \subseteq \tau$. Sejam $\mathcal{A}$ e $\mathcal{A}'$ $\overline{X}$-1-autómatos duais tais que $\mathcal{A} \overset{*}{\vdash} \mathcal{A}'$ e $L(\mathcal{A}) \subseteq \{v \in \overline{X}^* : v\tau \geq u\tau\}$. Então $L(\mathcal{A}') \subseteq \{v \in \overline{X}^* : v\tau \geq u\tau\}$.*

Dem. Seja $\mathcal{A} = (i, \Gamma, f)$. Basta-nos considerar o caso $\mathcal{A} \vdash \mathcal{A}'$, logo podemos assumir que $\mathcal{A}' = \mathcal{A}/\alpha$, onde α designa a equivalência em $V(\Gamma)$ induzida pela identificação dos vértices (distintos) p e q. Além disso, temos $(r, x, p), (r, x, q) \in E^1(\Gamma)$ para alguns $r \in V(\Gamma)$ e $x \in \overline{X} \cup 1$. Seja $e = x^{-1}x$. Então existem caminhos em $\mathcal{A}$ da forma

$$p \xrightarrow{e} p, \qquad p \xrightarrow{e} q, \qquad q \xrightarrow{e} p, \qquad q \xrightarrow{e} q.$$

Seja

$$i\alpha = s_0\alpha \xrightarrow{y_1} s_1\alpha \xrightarrow{y_2} \ldots \xrightarrow{y_n} s_n\alpha = f\alpha$$

um caminho em $\mathcal{A}'$. Se $s_j \notin \{p, q\}$ para todo j, é imediato que

$$i = s_0 \xrightarrow{y_1} s_1 \xrightarrow{y_2} \ldots \xrightarrow{y_n} s_n = f$$

é um caminho em $\mathcal{A}$, logo $y_1 \ldots y_n \in L(\mathcal{A}) \subseteq L(u)$. Caso contrário, sejam $k_1 < \ldots < k_m$ os índices j tais que $s_j\alpha = p\alpha = q\alpha$. Resulta da definição de Γ/α que existem caminhos em $\mathcal{A}$ da forma

$$s_0 \xrightarrow{y_1} s_1 \xrightarrow{y_2} \ldots \xrightarrow{y_{k_1}} s''_{k_1}$$

$$s'_{k_j} \xrightarrow{y_{k_j+1}} s_{k_j+1} \xrightarrow{y_{k_j+2}} \ldots \xrightarrow{y_{k_{j+1}-1}} s_{k_{j+1}-1} \xrightarrow{y_{k_{j+1}}} s''_{k_{j+1}} \qquad (j = 1, \ldots, m-1)$$

$$s''_{k_m} \xrightarrow{y_{k_m+1}} s_{k_m+1} \xrightarrow{y_{k_m+2}} \ldots \xrightarrow{y_n} s_n$$

com $s'_l, s''_l \in \{p, q\}$ para todo l. Considerando os caminhos em $\mathcal{A}$ da forma

$$p \xrightarrow{e} p, \qquad p \xrightarrow{e} q, \qquad q \xrightarrow{e} p, \qquad q \xrightarrow{e} q$$

resulta que existe um caminho bem-sucedido em $\mathcal{A}$ de rótulo

$$v = y_1 \dots y_{k_1} e y_{k_1+1} \dots y_{k_2} e \dots e y_{k_m+1} \dots y_n.$$

Por hipótese de indução , temos $v\tau \geq u\tau$. Para mostrar que $(y_1 ... y_n)\tau \geq u\tau$, basta-nos pois provar que

$$(ab)\tau \geq (ax^{-1}xb)\tau$$

para todos $a, b \in \overline{X}^*$ e $x \in \overline{X}$. Da aplicação sucessiva deste facto resulta que $(y_1 ... y_n)\tau \geq v\tau$ e logo $(y_1 ... y_n)\tau \geq u\tau$ e $L(\mathcal{A}') \subseteq \{v \in \overline{X}^* : v\tau \geq u\tau\}$.

Ora

$$[(ax^{-1}xa^{-1})(ax^{-1}xa^{-1})]\tau = (ax^{-1}xx^{-1}xa^{-1}aa^{-1})\tau = (ax^{-1}xa^{-1})\tau,$$

logo $(ax^{-1}xa^{-1})\tau \in E(FIM(X))$. Como

$$(ax^{-1}xb)\tau = (aa^{-1}ax^{-1}xb)\tau = (ax^{-1}xa^{-1}ab)\tau = (ax^{-1}xa^{-1})\rho(ab)\tau,$$

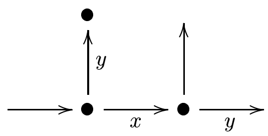
resulta que $(ab)\tau \geq (ax^{-1}xb)\tau$ e o lema está demonstrado. $\square$

Para todo $u \in \overline{X}^*$, designamos por $MT(u)$ o $\overline{X}$-autómato inverso obtido por redução completa de $Lin(u)$. Pelo Teorema 6.7(iii), $MT(u)$ está bem definido (a menos de isomorfismo).

Exemplo 7.3 *Seja $u = xyy^{-1}x^{-1}yy^{-1}x$. Então $Lin(u)$ é o autómato*

$$\longrightarrow \bullet \xrightarrow{x} \bullet \xrightarrow{y} \bullet \xleftarrow{y} \bullet \xleftarrow{x} \bullet \xrightarrow{y} \bullet \xleftarrow{y} \bullet \xrightarrow{x} \bullet \longrightarrow$$

e $MT(u)$ é o autómato



Dado um $\overline{X}$-autómato dual $\mathcal{A} = (i, \Gamma, f)$, dizemos que $\mathcal{A}$ satisfaz $\mathbf{P}$ e escrevemos $\mathcal{A} \models \mathbf{P}$ se não existir em Γ nenhum caminho da forma $i \xrightarrow{u} i$, com $u\iota \neq 1$.

Lema 7.4 *(i) Seja $\mathcal{A}$ um $\overline{X}$-autómato inverso. Então $\mathcal{A} \models \mathbf{P}$ se e só se for uma árvore.*

(ii) Sejam $\mathcal{A}$ e $\mathcal{A}'$ $\overline{X}$-autómatos duais. Se $\mathcal{A} \vdash \mathcal{A}'$ e $\mathcal{A} \models \mathbf{P}$, então $\mathcal{A}' \models \mathbf{P}$.

Dem. (i) Resulta do Exercício 6.6 e do Lema 6.3.

(ii) Suponhamos que $\mathcal{A}'$ resulta de $\mathcal{A} = (i, \Gamma, f)$ por identificação α dos vértices p e q, e que $(r, x, p), (r, x, q) \in E(\mathcal{A})$ $(x \in \overline{X})$. Seja $i\alpha \xrightarrow{v} i\alpha$ um caminho em $\mathcal{A}'$. É fácil de ver que v admite uma factorização $v = v_1 ... v_n$ tal que

$$i \xrightarrow{v_1} p_1 \xrightarrow{x^{-1}x} q_1 \xrightarrow{v_2} \dots \xrightarrow{x^{-1}x} q_{n-1} \xrightarrow{v_n} i$$

é um caminho em $\mathcal{A}$. Mas então $v\iota = (v_1 ... v_n)\iota = (v_1 x^{-1}xv_2 ... x^{-1}xv_n)\iota = 1$, pois $\mathcal{A} \models \mathbf{P}$. Logo $\mathcal{A}' \models \mathbf{P}$. $\square$

Teorema 7.5 *Seja* $u \in \overline{X}^*$. *Então:*

(i) $MT(u)$ *é uma árvore;*

(ii) o conjunto das geodésicas de $MT(u)$ *é* $\{v\iota;\ v \leq_p u\}$*;*

(iii) a geodésica principal de $MT(u)$ *é* $u\iota$.

Dem. (i) Pelo lema anterior, basta-nos mostrar que $Lin(u) \models \mathbf{P}$. Vamos usar indução sobre $\mid u \mid$. O caso $\mid u \mid = 0$ é trivial. Suponhamos que $Lin(v) \models \mathbf{P}$ sempre que $\mid v \mid = k$ $(k \geq 0)$. Seja $u \in \overline{X}^*$ com $\mid u \mid = k+1$. Então podemos escrever $u = vx$ para alguns $v \in \overline{X}^*$ e $x \in \overline{X}$. Seja $\rightarrow i \xrightarrow{w} i$ um caminho em $Lin(u)$. É fácil de ver que existe uma factorização

$$w = w_0 x x^{-1} w_1 ... w_{n-1} x x^{-1} w_n \qquad (n \geq 0)$$

tal que

$$\rightarrow i \xrightarrow{w_0 w_1 ... w_n} i$$

é um caminho em $Lin(v)$. Como $Lin(v) \models \mathbf{P}$ por hipótese de indução, resulta que $w\iota = (w_0 w_1 ... w_n)\iota = 1$. Logo $Lin(u) \models \mathbf{P}$ para todo $u \in \overline{X}^*$.

(ii) Dado um vértice q de $Lin(u)$, designamos por q' o vértice de $MT(u)$ resultante de q. Resulta da definição de redução simples que, se $\mathcal{A} \vdash \mathcal{A}/\alpha$ e $p \xrightarrow{z} q$ é um caminho em $\mathcal{A}$, então $p\alpha \xrightarrow{z} q\alpha$ é um caminho em $\mathcal{A}/\alpha$. Daqui resulta que se $i \xrightarrow{z} q$ é um caminho em $Lin(u)$, então $i' \xrightarrow{z} q'$ é um caminho em $MT(u)$.

Seja v um prefixo de u. Então existe em $Lin(u)$ um caminho da forma $i \xrightarrow{v} q$. Pelo comentário anterior, existe um caminho $i' \xrightarrow{v} q'$ em $MT(u)$. Pelo Lema 6.3, existe um caminho $i' \xrightarrow{v\iota} q'$ em $MT(u)$, e $v\iota$ é necessariamente uma geodésica de $MT(u)$.

Reciprocamente, suponhamos que $i' \xrightarrow{z} q'$ é uma geodésica de $MT(u)$. Então existe um caminho $i \xrightarrow{v} q$ em $Lin(u)$ com v prefixo de u. Pelo argumento anterior, existe um caminho $i' \xrightarrow{v\iota} q'$ em $MT(u)$ e $v\iota$ é uma geodésica. Por unicidade, resulta que $z = v\iota$ e logo o conjunto das geodésicas de $MT(u)$ é $\{v\iota;\ v \leq_p u\}$.

(iii) Como vimos em (ii), o facto de haver um caminho $i \xrightarrow{u} f$ em $Lin(u)$ implica que existe um caminho $i' \xrightarrow{u\iota} f'$ em $MT(u)$ e que $u\iota$ é uma geodésica. Logo $u\iota$ é a geodésica principal de $MT(u)$. $\square$

Dizemos que $MT(u)$ é a *árvore de Munn* de u e designamos o conjunto das geodésicas (palavras) de $MT(u)$ por $G(u)$.

Finalmente, estamos em condições de apresentar a solução do problema da palavra para ρ.

Teorema 7.6 *Sejam* $u, v \in \overline{X}^*$. *Então:*

(i) $u\rho = v\rho \Leftrightarrow MT(u) \simeq MT(v)$*;*

(ii) $L(MT(u)) = L(u)$.

Dem. (i) Para mostrar a implicação directa, basta observar que

$$MT(cwd) \simeq MT(cww^{-1}wd)$$

e

$$MT(cww^{-1}zz^{-1}d) \simeq MT(czz^{-1}ww^{-1}d)$$

para todos $c, d, w, z \in \overline{X}^*$, o que é imediato.

Reciprocamente, suponhamos que $MT(u) \simeq MT(v)$. Então $L(MT(u)) = L(MT(v))$. Pelos Lemas 7.1 e 7.2, temos $L(MT(u)) \subseteq L(u)$, logo

$$v \in L(MT(v)) = L(MT(u)) \subseteq L(u)$$

e $v\rho \geq u\rho$. Analogamente, $u\rho \geq v\rho$, logo $u\rho = v\rho$.

(ii) Já observámos na demonstração de (i) que $L(MT(u)) \subseteq L(u)$. Reciprocamente, suponhamos que $w\rho \geq u\rho$. Então $u\rho = (e\rho)(w\rho)$ para algum idempotente $e\rho$ e logo $u\rho = (ee^{-1}w)\rho$. Por (i), resulta que $MT(u) \simeq MT(ee^{-1}w)$, e logo $ee^{-1}w \in L(MT(u))$. Como ee^{-1} é necessariamente rótulo de um caminho fechado, resulta que $w \in L(MT(u))$ e logo $L(u) \subseteq L(MT(u))$. Logo $L(MT(u)) = L(u)$. $\square$

Corolário 7.7 *O problema da palavra para* $Mon < \overline{X}; \rho >$ *é decidível.*

Dem. Dados $u, v \in \overline{X}^*$, podemos construir efectivamente os autómatos $MT(u)$ e $MT(v)$. Como $MT(u)$ e $MT(v)$ são finitos, podemos decidir se são ou não isomorfos. $\square$

As árvores de Munn proporcionam uma excelente caracterização dos idempotentes de $FIM(X)$.

Teorema 7.8 *Para todo* $u \in \overline{X}^*$, *as condições seguintes são equivalentes:*

(i) $u\rho \in E(FIM(X))$;

(ii) os vértices inicial e final de $MT(u)$ *coincidem;*

(iii) $u\iota = 1$.

Dem. (i) $\Rightarrow$ (ii). Se $u\rho \in E(FIM(X))$, então $u\rho = (uu^{-1})\rho$, logo $MT(u) \simeq MT(uu^{-1})$. É imediato que os vértices inicial e final de $MT(uu^{-1})$ coincidem, logo o mesmo acontece com $MT(u)$.

(ii) $\Rightarrow$ (i). Se os vértices inicial e final de $MT(u)$ coincidem, é imediato que $MT(u) \simeq MT(u^2)$, logo $u\rho = u^2\rho$ e $u\rho \in E(FIM(X))$.

(ii) $\Leftrightarrow$ (iii). Resulta do Teorema 7.5(iii). $\square$

Uma palavra $e \in \overline{X}^*$ tal que $e\iota = 1$ diz-se uma *palavra de Dyck*. Designamos o conjunto das palavras de Dyck no alfabeto $\overline{X}$ por D_X.

Exercício 7.9 *Caracterize as relações de Green $\mathcal{R}$, $\mathcal{L}$ e $\mathcal{D}$ em $FIM(X)$.* $\square$

Exercício 7.10 *Mostre que $FIM(X) \simeq FIM(Y)$ se e só se $|X| = |Y|$.* $\square$

Exercício 7.11 *Mostre que $FIM(X)$ é* residualmente finito*: dados $u, v \in FIM(X)$ distintos, existe uma congruência τ em $FIM(X)$ tal que $FIM(X)/\tau$ é finito e $u\tau \neq v\tau$.* $\square$

Vamos agora derivar uma descrição alternativa de $FIM(X)$ a partir das árvores de Munn, que corresponde na realidade à descrição de Scheiblich [19], que precedeu em alguns meses a descrição de Munn.

Um subconjunto de R_X diz-se *fechado para prefixos* se contiver os prefixos de todos os seus elementos. Definimos

$$S(X) = \{(A, u) : A \subseteq R_X,\ A \text{ finito e fechado para prefixos}, u \in A\}.$$

Exercício 7.12 *Mostre que $S(X)$, munido do produto*

$$(A, u)(B, v) = (A \cup (uB)\iota, (uv)\iota),$$

constitui um monoide.

Teorema 7.13 *A função*

$$\begin{aligned} \theta \colon FIM(X) &\to S(X) \\ u\rho &\mapsto (G(u), u\iota) \end{aligned}$$

é um isomorfismo.

Dem. Pelos Teoremas 7.5 e 7.6, a função θ está bem definida. Tal como vimos anteriormente, o facto de $MT(u)$ ser uma árvore faz com que $MT(u)$ seja completamente determinada pelo seu conjunto de geodésicas e pela sua geodésica principal; logo $(u\rho)\theta = (v\rho)\theta$ implica $MT(u) \simeq MT(v)$ que implica $u\rho = v\rho$ pelo Teorema 7.6. Logo θ é injectiva.

Por outro lado, seja $P \subseteq R_X$ finito e fechado para prefixos, e seja $r \in P$. Seja $u = (\Pi_{z \in P} zz^{-1})r$. É fácil de ver que $(P, r) = (u\rho)\theta$, logo θ é uma bijecção.

Sejam agora $u, v \in \overline{X}^*$. É imediato que

$$\{w\iota : w \leq_p uv\} = \{z\iota : z \leq_p u\} \cup \{(ut)\iota : t \leq_p v\},$$

logo

$$G(uv) = G(u) \cup [uG(v)]\iota$$

pelo Teorema 7.5(ii). Como $(uv)\iota = ((u\iota)(v\iota))\iota$, resulta que

$$(G(uv), (uv)\iota) = (G(u) \cup [uG(v)]\iota, ((u\iota)(v\iota))\iota),$$

logo θ é um isomorfismo. $\square$

8 Apresentações de monoides inversos

Uma apresentação de monoides inversos é uma expressão formal do tipo $Inv < X; R >$, onde X designa um conjunto e R uma relação em $\overline{X}^*$. A apresentação diz-se finita se X e R forem finitos. O monoide inverso definido pela apresentação $Inv < X; R >$ é o quociente $M = \overline{X}^*/(\rho \cup R)^\sharp$. Pelo Teorema 1.2(ii), temos

$$\overline{X}^*/(\rho \cup R)^\sharp \simeq FIM(X)/[(\rho \cup R)^\sharp/\rho],$$

logo M é um monoide inverso pelo Teorema 2.3. Reciprocamente, é fácil de ver que todo o monoide inverso pode ser definido por uma apresentação.

Identificamos a apresentação de monoides inversos $Inv < X; R >$ com a apresentação de monoides $Mon < \overline{X}; \rho \cup R >$. Em particular, o problema da palavra para $Inv < X; R >$ é o problema da palavra para $Mon < \overline{X}; \rho \cup R >$.

Até ao fim desta secção, vamos fixar uma apresentação $Inv < X; R >$ e vamos escrever $\tau = (\rho \cup R)^\sharp$ e $M = \overline{X}^*/\tau$. Seja $u \in \overline{X}^*$. O *grafo de Schützenberger* de u relativamente a esta apresentação é o $\overline{X}$-grafo $\Gamma(u)$ definido por

- $V(\Gamma(u)) = \mathcal{R}_{u\tau}$,
- $E(\Gamma(u)) = \{(v\tau, x, w\tau) \in \mathcal{R}_{u\tau} \times \overline{X} \times \mathcal{R}_{u\tau} : w\tau = (vx)\tau\}$,

onde $\mathcal{R}_{u\tau}$ designa a $\mathcal{R}$-classe de $u\tau$ em M.

Designamos por *autómato de Schützenberger* de u (relativamente à apresentação $Inv < X; R >$) o $\overline{X}$-autómato

$$\mathcal{S}(u) = ((uu^{-1})\tau, \Gamma(u), u\tau).$$

Note-se que $(uu^{-1})\tau \, \mathcal{R} \, u\tau$, logo $\mathcal{S}(u)$ está bem definido.

No caso particular de M ser um grupo, $\mathcal{R}$ é a relação universal e $\Gamma(u)$ é o *grafo de Cayley* de M relativamente ao conjunto de geradores X.

Teorema 8.1 *(i) $\mathcal{S}(u)$ é um $\overline{X}$-autómato inverso;*

(ii) $L(\mathcal{S}(u)) = \{v \in \overline{X}^* : v\tau \geq u\tau\}$.

Dem. (i) Suponhamos que $(v\tau, x, w\tau) \in E(\Gamma(u))$. Então $w\tau = (vx)\tau$ e $(vv^{-1})\tau = (uu^{-1})\tau = (ww^{-1})\tau$. Logo

$$\begin{aligned}(wx^{-1})\tau &= (vxx^{-1})\tau = (vv^{-1}vxx^{-1})\tau = (vxx^{-1}v^{-1}v)\tau \\ &= (ww^{-1}v)\tau = (vv^{-1}v)\tau = v\tau\end{aligned}$$

e $(w\tau, x^{-1}, v\tau) \in E(\Gamma(u))$.

Por outro lado, sejam $v\tau, w\tau \in \mathcal{R}_{u\tau}$. Então $w\tau = (ww^{-1}w)\tau = (vv^{-1}w)\tau$. Suponhamos que $v^{-1}w = x_1 ... x_n$, com $n \geq 0$ e $x_j \in \overline{X}$. Para mostrar que $\mathcal{S}(u)$ é conexo, basta-nos provar que $(vx_1...x_j)\tau \in \mathcal{R}_{u\tau}$ para todo $j = 0, ..., n$. Ora

$$\begin{aligned}(vx_1...x_jx_j^{-1}...x_1^{-1}v^{-1})\tau &= (vv^{-1}vx_1...x_jx_j^{-1}...x_1^{-1}v^{-1})\tau \\ &= (ww^{-1}vx_1...x_jx_j^{-1}...x_1^{-1}v^{-1})\tau \\ &= (wx_n^{-1}...x_1^{-1}x_1...x_jx_j^{-1}...x_1^{-1}v^{-1})\tau \\ &= (wx_n^{-1}...x_1^{-1}v^{-1})\tau = (ww^{-1}vv^{-1})\tau = (uu^{-1})\tau,\end{aligned}$$

logo $(vx_1...x_j)\tau \in \mathcal{R}_{u\tau}$ e $\mathcal{S}(u)$ é conexo. Logo $\mathcal{S}(u)$ é dual.

É imediato que $\mathcal{S}(u)$ é determinístico, logo $\mathcal{S}(u)$ é inverso.

(ii) Seja $v \in L(\mathcal{S}(u))$, digamos $v = x_1...x_n$, com $x_j \in \overline{X}$. Então existe em $\mathcal{S}(u)$ um caminho da forma

$$(uu^{-1})\tau = q_0\tau \xrightarrow{x_1} q_1\tau \xrightarrow{x_2} ... \xrightarrow{x_n} q_n\tau = u\tau.$$

Logo, para $j = 1, ..., n$ temos $q_j\tau = (q_{j-1}x_j)\tau$, donde resulta que

$$u\tau = q_n\tau = (q_0x_1...x_n)\tau = (uu^{-1}v)\tau.$$

Logo $v\tau \geq u\tau$.

Reciprocamente, seja $v \in \overline{X}^*$ tal que $v\tau \geq u\tau$, digamos $v = x_1...x_n$, com $x_j \in \overline{X}$. Temos $u\tau = (e\tau)(v\tau)$ para algum idempotente $e\tau$, logo

$$(uu^{-1}v)\tau = (evv^{-1}ev)\tau = (evv^{-1}v)\tau = (ev)\tau = u\tau$$

e

$$\begin{aligned}(uu^{-1}vv^{-1})\tau &= (vv^{-1}uu^{-1})\tau = (vv^{-1}uu^{-1}vu^{-1})\tau \\ &= (uu^{-1}vu^{-1})\tau = (uu^{-1})\tau.\end{aligned}$$

Para todo $j = 0, ..., n$, temos então

$$\begin{aligned}(uu^{-1}x_1...x_jx_j^{-1}...x_1^{-1}uu^{-1})\tau &= (uu^{-1}vv^{-1}x_1...x_jx_j^{-1}...x_1^{-1}uu^{-1})\tau \\ &= (uu^{-1}vv^{-1}uu^{-1})\tau = (uu^{-1})\tau,\end{aligned}$$

logo

$$((uu^{-1}x_1...x_{j-1})\tau, x_j, (uu^{-1}x_1...x_j)\tau) \in E(\mathcal{S}(u))$$

para todo j e $v = x_1...x_n$ é rótulo de um caminho entre $(uu^{-1})\tau$ e $(uu^{-1}v)\tau = u\tau$. Logo $v \in L(\mathcal{S}(u))$. $\square$

Corolário 8.2 *Dados $u, v \in \overline{X}^*$, as condições seguintes são equivalentes:*

(i) $u\tau = v\tau$;

(ii) $v \in L(\mathcal{S}(u))$ *e* $u \in L(\mathcal{S}(v))$;

(iii) $\mathcal{S}(u) \simeq \mathcal{S}(v)$.

Dem. (i) $\Rightarrow$ (ii). Resulta imediatamente do teorema anterior.

(ii) $\Rightarrow$ (iii). Suponhamos que $v \in L(\mathcal{S}(u))$ e $u \in L(\mathcal{S}(v))$. Seja $w \in L(\mathcal{S}(v))$. Então $w\tau \geq v\tau$. Como $v \in L(\mathcal{S}(u))$, temos também $v\tau \geq u\tau$ e logo $w\tau \geq u\tau$. Resulta que $w \in L(\mathcal{S}(u))$ e logo $L(\mathcal{S}(v)) \subseteq L(\mathcal{S}(u))$. Por simetria, $L(\mathcal{S}(u)) = L(\mathcal{S}(v))$, e logo, pelo Teorema 6.2, $\mathcal{S}(u) \simeq \mathcal{S}(v)$.

(iii) $\Rightarrow$ (i). Suponhamos que $\mathcal{S}(u) \simeq \mathcal{S}(v)$. Pelo Teorema 6.2, temos $L(\mathcal{S}(u)) = L(\mathcal{S}(v))$, logo $u \in L(\mathcal{S}(u)) = L(\mathcal{S}(v))$ e $u\tau \geq v\tau$. Por simetria, $u\tau = v\tau$. $\square$

Resulta do corolário anterior que o problema da palavra para $Inv < X; R >$ está intimamente relacionado com os autómatos de Schützenberger $\mathcal{S}(u)$. O problema da palavra para $Inv < X; R >$ será decidível se e só se $L(\mathcal{S}(u))$ for *recursiva* para todo $u \in \overline{X}^*$ (isto é, se for decidível, para todos $v, u \in \overline{X}^*$, se $v \in L(\mathcal{S}(u))$).

Exemplo 8.3 *Consideremos a apresentação*

$$Inv < x, y; x^2 = x, y^2 = 1, xy = yx > .$$

Temos $x\tau = x^{-1}\tau$ *e* $y\tau = y^{-1}\tau$*; como* $(xy)\tau = (yx)\tau$*, podemos concluir que* $M = \{(x^n y^m)\tau;\ n, m \geq 0\}$*. Como* $x^2\tau = x\tau$ *e* $y^2\tau = 1\tau$*, resulta que*

$$M = \{1\tau, x\tau, y\tau, (xy)\tau\}.$$

Estes quatro elementos são efectivamente distintos, pois

- *se* $u\tau = v\tau$*, então* x *ocorre em* u *se e só se* x *ocorre em* v*;*

- *se* $u\tau = v\tau$*, então a soma dos expoentes de* y *tem a mesma paridade em* u *e em* v*.*

É imediato que $\mathcal{R}_{1\tau} = \{1\tau, y\tau\}$ *e* $\mathcal{R}_{x\tau} = \{x\tau, (xy)\tau\}$*, logo os grafos de Schützenberger de* M *são descritos por*

$$\begin{tikzcd} 1\tau \arrow[r, bend left, "y"] & y\tau \arrow[l, bend left, "y"] \end{tikzcd} \qquad \begin{tikzcd} x\tau \arrow[loop above, "x"] \arrow[r, bend left, "y"] & (xy)\tau \arrow[loop above, "x"] \arrow[l, bend left, "y"] \end{tikzcd}$$

Exercício 8.4 *Dada uma apresentação* $Inv < X; R >$*, mostre que* $\mathcal{S}(u)$ *é uma árvore para todo* $u \in \overline{X}^*$ *se e só se* $R \subseteq \pi$*.* $\square$

9 A sucessão de Stephen

Vamos agora ver como, dadas uma apresentação finita $Inv < X; R >$ e $u \in \overline{X}^*$, é possível construir efectivamente uma sucessão de $\overline{X}$-autómatos inversos finitos $\mathcal{A}_k(u)$ tal que

$$L(\mathcal{S}(u)) = \bigcup_{k \geq 1} L(\mathcal{A}_k(u)).$$

Na realidade, é possível demonstrar que $\mathcal{S}(u)$ é o *limite directo* dos $\overline{X}$-autómatos $\mathcal{A}_k(u)$ na categoria dos $\overline{X}$-autómatos inversos [27]. A sucessão $(\mathcal{A}_k(u))_{k\geq 1}$, dita *sucessão de Stephen*, tem sido usada com êxito em vários casos para solucionar o problema da palavra e outros problemas de decidibilidade envolvendo apresentações de monoides inversos – analisaremos diversas aplicações nas secções posteriores.

Ao longo de toda a secção, fixamos uma apresentação finita $Inv < X; R >$, além da notação $\tau = (\rho \cup R)^\sharp$ e $M = \overline{X}^*/\tau$.

Suponhamos que $\mathcal{A} = (i, \Gamma, f)$ é um $\overline{X}$-1-autómato dual finito, e suponhamos que existem $(r, s) \in R \cup R^{-1}$ e $p, q \in V(\Gamma)$ tais que:

($\dagger$) existe um caminho $p \xrightarrow{r} q$ em $\mathcal{A}$;

($\dagger\dagger$) não existe um caminho $p \xrightarrow{s} q$ em $\mathcal{A}$.

Definimos um $\overline{X}$-1-autómato dual $\mathcal{A}'$ do seguinte modo. Se $s = x_1 ... x_n$, com $n \geq 1$ e $x_j \in \overline{X}$, acrescentamos a $\mathcal{A}$ novos vértices $t_1, ..., t_{n-1}$ e as arestas descritas por

$$p = t_0 \xrightarrow{x_1} t_1 \xrightarrow{x_2} ... \xrightarrow{x_n} t_n = q,$$

bem como as suas duais. Se $s = 1$, juntamos a $\mathcal{A}$ a aresta $p \xrightarrow{1} q$ e a sua dual. Dizemos que $\mathcal{A}'$ resulta de $\mathcal{A}$ por uma *R-expansão simples*, mais especificamente por colagem de um caminho $p \xrightarrow{s} q$. Usaremos a notação $\mathcal{A} \prec_R \mathcal{A}'$.

Consideremos agora simultaneamente todos $(r, s) \in R \cup R^{-1}$ e $p, q \in V(\Gamma)$ tais que ($\dagger$) e ($\dagger\dagger$) são satisfeitas, e colemos um caminho a $\mathcal{A}$ por cada uma dessas situações de acordo com as regras definidas para as expansões simples (assumindo que os novos vértices são todos distintos). Como R e $V(\Gamma)$ são finitos, o $\overline{X}$-1-autómato dual $\mathcal{B}$ assim obtido é também finito. Dizemos que $\mathcal{B}$ resulta de $\mathcal{A}$ por uma *R-expansão completa*.

Lema 9.1 *Sejam $\mathcal{A}$ e $\mathcal{A}'$ $\overline{X}$-1-autómatos duais tais que $\mathcal{A}'$ resulta de $\mathcal{A}$ por uma R-expansão completa. Então:*

(i) $L(\mathcal{A}) \subseteq L(\mathcal{A}')$;

(ii) se $L(\mathcal{A}) \subseteq \{v \in \overline{X}^* : v\tau \geq u\tau\}$, então $L(\mathcal{A}') \subseteq \{v \in \overline{X}^* : v\tau \geq u\tau\}$.

Dem. (i) Imediato, pois qualquer caminho bem-sucedido em $\mathcal{A}$ é ainda um caminho bem-sucedido em $\mathcal{A}'$.

(ii) Sejam $\mathcal{A} = (i, \Gamma, f)$ e $\mathcal{A}' = (i, \Gamma', f)$, e suponhamos que $L(\mathcal{A}) \subseteq \{v \in \overline{X}^* : v\tau \geq u\tau\}$. Suponhamos que $(r, s) \in R \cup R^{-1}$, $p, q \in V(\Gamma)$, existe um caminho $p \xrightarrow{r} q$ em $\mathcal{A}$, não existe um caminho $p \xrightarrow{s} q$ em $\mathcal{A}$ e $\mathcal{A}'$ resulta de $\mathcal{A}$ por colagem do caminho $p \xrightarrow{s} q$. Designamos por Γ'' o $\overline{X}$-1-grafo dual definido pelo novo caminho $p \xrightarrow{s} q$.

Dado um caminho ω em $\mathcal{A}'$, designamos por *índice* de ω e denotamos por $h(\omega)$ o número de vezes que ω passa em arestas de Γ''. Vamos mostrar que

$(*)$ se $\omega\colon i \xrightarrow{v} f$ é um caminho em $\mathcal{A}'$, então $v\tau \geq u\tau$

por indução sobre o índice de ω.

Obviamente, $(*)$ é válido para todos os caminhos de índice 0, pois um caminho bem-sucedido em $\mathcal{A}'$ de índice 0 pode ser visto como um caminho bem-sucedido em $\mathcal{A}$.

Suponhamos agora que $(*)$ é válido para todos os caminhos de índice $\leq k$ $(k \geq 0)$, e que $\omega\colon i \xrightarrow{v} f$ é um caminho em $\mathcal{A}'$ de índice $k+1$. Então podemos factorizar o caminho ω em três caminhos do seguinte modo: existem $v_1, v_2, v_3 \in \overline{X}^*$ e $a, b \in \{p, q\}$ tais que

$\omega_1\colon i \xrightarrow{v_1} a$ é um caminho em $\mathcal{A}'$;

$\omega_2\colon a \xrightarrow{v_2} b$ é um caminho não-trivial em Γ'';

$\omega_3\colon b \xrightarrow{v_3} f$ é um caminho em $\mathcal{A}'$;

$v = v_1v_2v_3$;

$h(\omega_1) + h(\omega_2) + h(\omega_3) = k + 1.$

Como ω_2 é não -trivial, $h(\omega_2) > 0$. Além disso, podemos supor que p e q não ocorrem como vértices intermédios no caminho ω_2. Vejamos que existe um caminho $\omega_2'\colon a \xrightarrow{z} b$ em $\mathcal{A}'$ de índice 0 tal que $v_2\tau \geq z\tau$.

Se $a = p$ e $b = q$, então $v_2 \in L(MT(s))$, logo $v_2\rho \geq s\rho$ pelo Teorema 7.6(ii) e logo $v_2\tau \geq s\tau = r\tau$. Por hipótese, existe um caminho $p \xrightarrow{r} q$ em $\mathcal{A}'$ de índice 0.

Se $a = b = p$, é fácil de ver que $v_2 \in L(MT(ss^{-1}))$ e logo $v_2\tau \geq (ss^{-1})\tau = (rr^{-1})\tau$. Por hipótese, existe um caminho

$$p \xrightarrow{rr^{-1}} p$$

em $\mathcal{A}'$ de índice 0.

Os casos $a = q$, $b = p, q$ são análogos, considerando s^{-1} e $s^{-1}s$, logo podemos afirmar que existe sempre um caminho $\omega_2'\colon a \xrightarrow{z} b$ em $\mathcal{A}'$ de índice 0 tal que $v_2\tau \geq z\tau$. Mas então, compondo os caminhos ω_1, ω_2' e ω_3 em $\mathcal{A}'$ obtemos um caminho

$$\omega'\colon i \xrightarrow{v_1zv_3} f$$

com $h(\omega') \leq k$, logo $(v_1zv_3)\tau \geq u\tau$ por hipótese de indução. Como $v_2\tau \geq z\tau$, resulta que

$$v\tau = (v_1v_2v_3)\tau \geq (v_1zv_3)\tau \geq u\tau,$$

logo $(*)$ é válido para $\omega\colon i \xrightarrow{v} f$ e o lema está demonstrado. $\square$

Seja $u \in \overline{X}^*$. Definimos indutivamente uma sucessão $(\mathcal{A}_k(u))_{k\geq 1}$ de $\overline{X}$-autómatos inversos finitos e uma sucessão $(\mathcal{B}_k(u))_{k\geq 1}$ de $\overline{X}$-1-autómatos duais finitos do seguinte modo:

(i) $\mathcal{A}_1(u) = MT(u)$;

(ii) $\mathcal{B}_k(u)$ resulta de $\mathcal{A}_k(u)$ por uma R-expansão completa;

(iii) $\mathcal{A}_{k+1}(u)$ resulta de $\mathcal{B}_k(u)$ por uma redução completa.

Teorema 9.2 *Seja $u \in \overline{X}^*$.*

(i) $L(\mathcal{A}_k(u)) \subseteq L(\mathcal{A}_{k+1}(u))$ para todo $k \geq 1$;

(ii)

$$L(\mathcal{S}(u)) = \bigcup_{k\geq 1} L(\mathcal{A}_k(u)).$$

Dem. (i) Resulta imediatamente dos Lemas 6.7(iv) e 9.1(i).

(ii) Pelo Teorema 8.1(ii), temos

$$L(\mathcal{S}(u)) = \{v \in \overline{X}^* : v\tau \geq u\tau\}.$$

Como $\mathcal{A}_1(u) = MT(u)$, resulta do Lema 7.6(ii) que $L(\mathcal{A}_1(u)) \subseteq L(\mathcal{S}(u))$. Por outro lado, pelo Lema 9.1(ii), $L(\mathcal{A}_k(u)) \subseteq L(\mathcal{S}(u))$ implica $L(\mathcal{B}_k(u)) \subseteq L(\mathcal{S}(u))$, e o Lema 7.2 garante que $L(\mathcal{B}_k(u)) \subseteq L(\mathcal{S}(u))$ implica $L(\mathcal{A}_{k+1}(u)) \subseteq L(\mathcal{S}(u))$. Logo $L(\mathcal{A}_k(u)) \subseteq L(\mathcal{S}(u))$ para todo $k \geq 1$ e

$$\bigcup_{k\geq 1} L(\mathcal{A}_k(u)) \subseteq L(\mathcal{S}(u)).$$

Reciprocamente, seja $v \in L(\mathcal{S}(u))$. Então $(uu^{-1}v)\tau = u\tau$, logo existem $w_0, ..., w_n \in \overline{X}^*$ $(n \geq 0)$, tais que:

$u = w_0$,

$uu^{-1}v = w_n$,

para todo $j \in \{1, ..., n\}$, existem $a_j, b_j \in \overline{X}^*$ e $(r_j, s_j) \in \rho \cup R \cup R^{-1}$ tais que

$$w_{j-1} = a_j r_j b_j, \qquad w_j = a_j s_j b_j.$$

Vamos mostrar que $w_j \in L(\mathcal{A}_{j+1}(u))$ por indução sobre j.

É imediato que

$$w_0 = u \in L(MT(u)) = L(\mathcal{A}_1(u)).$$

Suponhamos que $w_{j-1} \in L(\mathcal{A}_j(u))$ com $j \in \{1, ..., n\}$. Como $w_{j-1} = a_j r_j b_j$, existe em $\mathcal{A}_j(u)$ um caminho da forma

$$\rightarrow i \xrightarrow{a_j} p \xrightarrow{r_j} q \xrightarrow{b_j} f \rightarrow$$

Se existir em $\mathcal{A}_j(u)$ um caminho da forma $p \xrightarrow{s_j} q$, então

$$w_j = a_j s_j b_j \in L(\mathcal{A}_j(u)) \subseteq L(\mathcal{A}_{j+1}(u))$$

por (i). Caso contrário, existe um caminho da forma $p \xrightarrow{s_j} q$ no $\overline{X}$-1-autómato $\mathcal{B}_j(u)$ resultante da R-expansão completa de $A_j(u)$. Logo $w_j = a_j s_j b_j \in L(\mathcal{B}_j(u))$. Como $L(\mathcal{B}_j(u)) \subseteq L(\mathcal{A}_{j+1}(u))$ pelo Teorema 6.7(iv), resulta que $w_j \in L(\mathcal{A}_{j+1}(u))$.

Em particular, $uu^{-1}v = w_n \in L(\mathcal{A}_{n+1}(u))$. Como $\mathcal{A}_{n+1}(u)$ é inverso, resulta que $v \in L(\mathcal{A}_{n+1}(u))$ e logo

$$L(\mathcal{S}(u)) = \bigcup_{k \geq 1} L(\mathcal{A}_k(u)),$$

provando o teorema. □

Uma análise cuidadosa da demonstração anterior permite-nos observar que se na definição de $\mathcal{A}_1(u)$ substituirmos $MT(u)$ por qualquer $\overline{X}$-autómato inverso $\mathcal{A}'$ tal que $L(MT(u)) \subseteq L(\mathcal{A}') \subseteq L(\mathcal{S}(u))$, a sucessão $(\mathcal{A}_k(u))_{k \geq 1}$ então obtida satisfaz ainda $L(\mathcal{S}(u)) = \cup_{k \geq 1} L(\mathcal{A}_k(u))$. É este o caso, em particular, se $\mathcal{A}'$ for um $\overline{X}$-autómato inverso obtido a partir de $MT(u)$ por uma sequência arbitrária de R-expansões simples e reduções; se $\mathcal{A}'$ não admitir qualquer R-expansão simples, podemos concluir que $L(\mathcal{S}(u)) = L(\mathcal{A}')$ e logo $\mathcal{S}(u) \simeq \mathcal{A}'$.

Em resumo, se ao efectuar uma sequência finita de R-expansões simples/reduções em $MT(u)$ obtivermos um $\overline{X}$-autómato (finito) que não admita quaisquer R-expansões simples/reduções, então esse $\overline{X}$-autómato é $\mathcal{S}(u)$, que é portanto finito e pode ser efectivamente construído.

O resultado seguinte mostra-nos que o recíproco também acontece: se $\mathcal{S}(u)$ é finito, então pode ser efectivamente construído através da sucessão de Stephen.

Teorema 9.3 *Dado $u \in \overline{X}^*$, as condições seguintes são equivalentes:*

(i) $\mathcal{S}(u)$ é finito;

(ii) $\mathcal{R}_{u\tau}$ é finita;

(iii) a sucessão $(\mathcal{A}_k(u))_{k \geq 1}$ é estacionária.

Dem. (i) ⇔ (ii). Por definição de $\mathcal{S}(u)$.

(iii) ⇒ (i). Se $\mathcal{A}_m(u) = \mathcal{A}_{m+l}(u)$ para todo $l \geq 1$, então $\mathcal{S}(u) \simeq \mathcal{A}_m(u)$ é finito.

(i) ⇔ (iii). Suponhamos que $\mathcal{S}(u) = (i, \Gamma, f)$ é finito. Para cada $p \in V(\Gamma)$, seja $i \xrightarrow{g_p} p$ uma geodésica em $\mathcal{S}(u)$. Então $g_p g_p^{-1} g_f \in L(\mathcal{S}(u))$ para todo $p \in V(\Gamma)$. Além disso, para todo $(p,x,q) \in E(\Gamma)$, temos $g_p x g_q^{-1} g_f \in L(\mathcal{S}(u))$. Como Γ é finito e $L(\mathcal{S}(u)) = \cup_{k\geq 1} L(\mathcal{A}_k(u))$, existe $m \geq 1$ tal que

$$\{g_p g_p^{-1} g_f; p \in V(\Gamma)\} \cup \{g_p x g_q^{-1} g_f; (p,x,q) \in E(\Gamma)\} \subseteq L(\mathcal{A}_m(u)).$$

Seja $\mathcal{A}_m(u) = (i_m, \Gamma_m, f_m)$. Como $g_f g_f^{-1} g_f \in L(\mathcal{A}_m(u))$ e $\mathcal{A}_m(u)$ é inverso, temos $g_f \in L(\mathcal{A}_m(u))$ e logo existe um caminho

$$i_m \xrightarrow{g_p x g_q^{-1}} i_m$$

em $\mathcal{A}_m(u)$ para todo $(p,x,q) \in E(\Gamma)$.

Vamos mostrar que $L(\mathcal{S}(u)) \subseteq L(\mathcal{A}_m(u))$. Seja

$$i = q_0 \xrightarrow{x_1} q_1 \xrightarrow{x_2} \dots \xrightarrow{x_n} q_n = f$$

um caminho em $\mathcal{S}(u)$. Então existe em $\mathcal{A}_m(u)$ um caminho da forma

$$i_m \xrightarrow{g_i x_1 g_{q_1}^{-1}} i_m \xrightarrow{g_{q_1} x_2 g_{q_2}^{-1}} \dots \xrightarrow{g_{q_{n-1}} x_n g_f^{-1}} i_m \xrightarrow{g_f} f_m.$$

Como $g_i = 1$, resulta que

$$w = x_1 g_{q_1}^{-1} g_{q_1} x_2 g_{q_2}^{-1} g_{q_2} x_3 \dots x_n g_f^{-1} g_f \in L(\mathcal{A}_m(u)).$$

Como $\mathcal{A}_m(u)$ é inverso, resulta imediatamente que $x_1 \dots x_n \in L(\mathcal{A}_m(u))$. Logo $L(\mathcal{S}(u)) \subseteq L(\mathcal{A}_m(u))$ e $L(\mathcal{A}_m(u)) = L(\mathcal{A}_{m+l}(u))$ para todo $l \geq 1$. Logo a sucessão $(\mathcal{A}_k(u))_{k\geq 1}$ é estacionária. $\square$

Corolário 9.4 *Se $\mathcal{S}(u)$ é finito para todo $u \in \overline{X}^*$, então o problema da palavra para $Inv < X; R >$ é decidível.*

Exemplo 9.5 *Consideremos a apresentação*

$$Inv < x, y; x^2 = x, y^2 = y^3, xy = xy^2 > .$$

Seja $u = x^{-1} y x^{-1}$. Temos

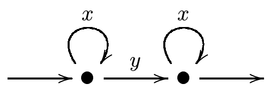
$\mathcal{A}_1(u)$:

$$\begin{tikzcd} {} \arrow[r] & \bullet & \bullet \arrow[l, "x"'] \arrow[r, "y"] & \bullet & \bullet \arrow[l, "x"'] \arrow[r] & {} \end{tikzcd}$$

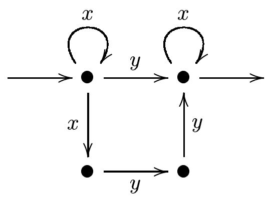
$\mathcal{B}_1(u)$:

$$\begin{tikzcd} {} \arrow[r] & \bullet & \bullet \arrow[l, "x"'] \arrow[r, "y"] \arrow[d, "x"] & \bullet & \bullet \arrow[l, "x"'] \arrow[r] \arrow[d, "x"] & {} \\ & & \bullet \arrow[ul, "x"] & & \bullet \arrow[ul, "x"] & \end{tikzcd}$$

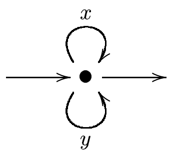
$\mathcal{A}_2(u)$:



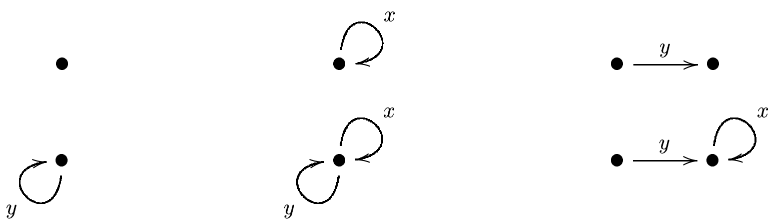
$\mathcal{B}_2(u)$:



$\mathcal{A}_3(u) = \mathcal{S}(u)$:



Não é difícil verificar que os grafos de Schützenberger desta apresentação são



logo o monoide inverso por ela definido tem $1+1+2^2+1+1+2^2 = 12$ *elementos.* $\square$

Exercício 9.6 *Determine os grafos de Schützenberger da apresentação*

$$Inv < x; x^3 = x, y = y^3, xyx = y^{-1} > . \square$$

Exercício 9.7 *Determine os grafos de Schützenberger da apresentação*

$$Inv < x, y; x^2x^{-2} = xx^{-1} >$$

e resolva o problema da palavra. $\square$

10 Apresentações com autómatos de Schützenberger finitos

Vamos ver nesta secção alguns exemplos significativos de apresentações de monoides inversos em que os autómatos de Schützenberger são finitos, e consequentemente, em que a construção da sucessão de Stephen permite a solução efectiva do problema da palavra. Tais exemplos devem-se a Stephen [27]. Obviamente, um caso trivial é a apresentação $Inv < X; \emptyset >$ de $FIM(X)$, em que $\mathcal{S}(u) = \mathcal{A}_1(u) = MT(u)$ para todo $u \in \overline{X}^*$.

Teorema 10.1 *Seja $Inv < X; R >$ uma apresentação finita em que cada elemento de R é da forma $r^{k+l} = r^k$, com $r \in \overline{X}^*$, $0 < l \leq k$. Então:*

(i) $\mathcal{S}(u)$ é finito para todo $u \in \overline{X}^*$;

(ii) o problema da palavra para $Inv < X; R >$ é decidível.

Dem. (i) Suponhamos que $\mathcal{A}$ e $\mathcal{A}'$ são $\overline{X}$-autómatos inversos finitos tais que $\mathcal{A}'$ resulta de $\mathcal{A}$ por uma R-expansão simples seguida de uma redução completa. Vamos mostrar que

$$|V(\mathcal{A}')| < |V(\mathcal{A})|\,. \tag{1}$$

Com efeito, suponhamos que $(r^{k+l}, r^k) \in R$, existe um caminho em $\mathcal{A}$ da forma

$$p \xrightarrow{r^k} q,$$

mas não existe nenhum caminho em $\mathcal{A}$ da forma

$$p \xrightarrow{r^{k+l}} q.$$

Dividindo k por l, obtemos $k = la + b$, com $a \geq 1$ e $0 \leq b < l$. Se efectuarmos a R-expansão correspondente à colagem do caminho

$$p \xrightarrow{r^{k+l}} q,$$

seguida de redução completa, o $\overline{X}$-autómato $\mathcal{A}$ evolui de acordo com o esquema seguinte:

(a):

$$\begin{tikzcd} p \arrow[r, bend left, "r^k"] \arrow[r, dashed, bend right, "r^{k+l}"'] & q \end{tikzcd}$$

(b):

$$\begin{tikzcd} p \arrow[r, "r^k"] & q \arrow[loop right, "r^l"] \end{tikzcd}$$

(c):

$$p \underset{r^{l-b}}{\overset{r^b}{\rightleftarrows}} q$$

Independentemente de virem a ter lugar mais reduções, o autómato em (c) já tem menos vértices do que $\mathcal{A}$: todos os vértices e arestas em (c) resultam de vértices e arestas já existentes em $\mathcal{A}$, e existe um caminho

$$p \xrightarrow{r^{k+l}} q$$

em (c), logo na passagem de $\mathcal{A}$ para (c) houve necessariamente identificação de vértices distintos. Naturalmente, se o autómato em (c) admitir mais reduções, o número de vértices baixará ainda mais.

O caso dual, em que existe em $\mathcal{A}$ um caminho $p \xrightarrow{r^{k+l}} q$ mas não um caminho $p \xrightarrow{r^k} q$, é inteiramente análogo.

Em qualquer caso, resulta que $|V(\mathcal{A}')| < |V(\mathcal{A})|$.

Seja agora $u \in \overline{X}^*$ e consideremos $MT(u)$. Se aplicarmos sucessivamente o processo R-expansão simples/redução completa a $MT(u)$, o número de vértices vai diminuindo, logo obtemos necessariamente um $\overline{X}$-autómato inverso que não admite R-expansões simples. Pelos comentários feitos na secção anterior, esse autómato é $\mathcal{S}(u)$, que é portanto finito.

(ii) resulta de (i) e do Corolário 9.4. $\square$

Exercício 10.2 *Seja T uma relação finita em $\overline{X}^*$ tal que $(a\rho)\,\mathcal{R}\,(b\rho)$ para todo $(a,b) \in T$. Mostre que o problema da palavra para $Inv < X; T >$ é decidível.*

Seja agora $\sigma : \overline{X}^* \to (\mathbf{Z}, +)$ o homomorfismo definido por

$$x\sigma = 1, \qquad x^{-1}\sigma = -1 \qquad (x \in X).$$

Dado um $\overline{X}$-autómato dual $\mathcal{A} = (i, \Gamma, f)$, definimos

$$\delta(\mathcal{A}) = \sup\{|g| + w\sigma : i \xrightarrow{g} p \xrightarrow{w} q \text{ é um caminho em } \mathcal{A}, \text{ com } g \text{ geodésica}\}.$$

Lema 10.3 *(i) Para todo $u \in \overline{X}^*$, $\delta(MT(u)) < \infty$;*

(ii) Sejam $\mathcal{A}$ e $\mathcal{A}'$ $\overline{X}$-autómatos duais. Se $\mathcal{A} \vdash \mathcal{A}'$, então $\delta(\mathcal{A}') \leq \delta(\mathcal{A})$.

(iii) Seja $n \in \mathbf{N}$. A menos de isomorfismo, o número de $\overline{X}$-autómatos inversos $\mathcal{A}$ tais que $\delta(\mathcal{A}) \leq n$ é finito.

Dem. (i) Como as geodésicas de $MT(u)$ são da forma $v\iota$, com $v \leq_p u$, é imediato que $|\,g\,| \leq |\,u\,|$ para toda a geodésica g de $MT(u)$.

Suponhamos agora que $p \xrightarrow{w} q$ é um caminho em $MT(u)$. Então existe um caminho $p \xrightarrow{w\iota} q$ em $MT(u)$ e $(w\iota)\sigma = w\sigma$. Como $|\,w\iota\,| \leq |\,u\,|$, resulta que

$$\delta(MT(u)) \leq 2\,|\,u\,|\,.$$

(ii) Suponhamos que $\mathcal{A}' = \mathcal{A}/\alpha$, onde α é a relação de equivalência em $V(\mathcal{A})$ induzida pela identificação dos vértices distintos p e q, e que $(r,x,p),(r,x,q) \in E(\mathcal{A})$, com $x \in \overline{X}$. Seja

$$\to i\alpha \xrightarrow{g} s\alpha \xrightarrow{w} t\alpha$$

um caminho em $\mathcal{A}'$, com g geodésica. É fácil de ver que w admite uma factorização $w = w_1 ... w_k$ $(k \geq 1)$, tal que existe um caminho

$$s \xrightarrow{w_1} a_1 \xrightarrow{x^{-1}x} b_1 \xrightarrow{w_2} ... \xrightarrow{w_{k-1}} a_{k-1} \xrightarrow{x^{-1}x} b_{k-1} \xrightarrow{w_k} t$$

em $\mathcal{A}$. Seja $w' = w_1 x^{-1} x w_2 ... x^{-1} x w_k$ e seja $\to i \xrightarrow{c} s$ um caminho em $\mathcal{A}$, com c geodésica. Então há um caminho $\to i\alpha \xrightarrow{c} s\alpha$ em $\mathcal{A}'$ e logo $|\ g\ | \leq |\ c\ |$, pois g é geodésica. Logo

$$|\,g\,| + w\sigma \leq |\,c\,| + w\sigma = |\,c\,| + w'\sigma \leq \delta(\mathcal{A})$$

e $\delta(\mathcal{A}') \leq \delta(\mathcal{A})$.

(iii) Se $\delta(\mathcal{A}) \leq n$, então toda a geodésica de $\mathcal{A}$ tem comprimento $\leq n$ e logo $|\,V(\mathcal{A})\,|$ é majorado por $|\,\{v \in R_X : |\,v\,| \leq n\}\,|$. É imediato que para todo $k \geq 1$, a menos de isomorfismo, há apenas um número finito de $\overline{X}$-autómatos inversos com k vértices. Logo o número de $\overline{X}$-autómatos inversos $\mathcal{A}$ tais que $\delta(\mathcal{A}) \leq n$ é finito (a menos de isomorfismo). $\square$

Teorema 10.4 *Seja $Inv < X; R >$ uma apresentação finita em que cada elemento de R é da forma $r = s$, com $r, s \in X^*$ e $|\,r\,| = |\,s\,|$. Então:*

(i) $\mathcal{S}(u)$ é finito para todo $u \in \overline{X}^*$;

(ii) o problema da palavra para $Inv < X; R >$ é decidível.

Dem. (i) Sejam $\mathcal{A} = (i, \Gamma, f)$ e $\mathcal{A}'$ dois $\overline{X}$-autómatos duais. Vamos mostrar que

$$\mathcal{A} \prec_R \mathcal{A}' \Rightarrow \delta(\mathcal{A}') \leq \delta(\mathcal{A}). \qquad (2)$$

Seja $(r,s) \in R \cup R^{-1}$, com $r = r_1 ... r_m$ e $s = s_1 ... s_m$ $(r_j, s_j \in X)$, e suponhamos que:

- existe um caminho

$$p_0 \xrightarrow{r_1} p_1 \xrightarrow{r_2} ... \xrightarrow{r_m} p_m$$

em Γ;

- não existe um caminho $p_0 \xrightarrow{s} p_m$ em Γ;

- $\mathcal{A}'$ resulta de $\mathcal{A}$ por colagem de um caminho

$$p_0 = p'_0 \xrightarrow{s_1} p'_1 \xrightarrow{s_2} \ldots \xrightarrow{s_m} p'_m = p_m.$$

Seja $\to i \xrightarrow{g} q \xrightarrow{w} t$ um caminho em $\mathcal{A}'$, com g geodésica.

Suponhamos primeiro que $q \in V(\Gamma)$. Seja $i \xrightarrow{c} q$ uma geodésica em $\mathcal{A}$. É imediato que $|\,g\,| \leq |\,c\,|$, pois existe um caminho $i \xrightarrow{c} q$ em $\mathcal{A}'$. Por outro lado, se no caminho $q \xrightarrow{w} t$ substituirmos

- (p'_{j-1}, s_j, p'_j) por (p_{j-1}, r_j, p_j)

- $(p'_j, s_j^{-1}, p'_{j-1})$ por (p_j, r_j^{-1}, p_{j-1})

para todo j, é fácil de ver que obtemos um caminho $q \xrightarrow{w_1} t_1$ em $\mathcal{A}$ com $w_1\sigma = w\sigma$. Logo $|\,g\,| + w\sigma \leq |\,c\,| + w_1\sigma \leq \delta(\mathcal{A})$.

Suponhamos agora que $q = p'_l$, com $l \in \{1, \ldots, m-1\}$. Seja $i \xrightarrow{c} p_0$ um caminho em $\mathcal{A}$ com c geodésica, e seja $z = s_1 \ldots s_l$.

Obviamente, temos um caminho $i \xrightarrow{cz} p'_l$ em $\mathcal{A}'$; como g é geodésica, temos $|\,g\,| \leq |\,cz\,|$. Além disso, se considerarmos o caminho $p_0 \xrightarrow{zw} t$ em $\mathcal{A}'$, resulta do caso anterior que existe em $\mathcal{A}$ um caminho da forma $p_0 \xrightarrow{w_1} t_1$ com $w_1\sigma = (zw)\sigma$. Logo também neste caso obtemos

$$|\,g\,| + w\sigma \leq |\,cz\,| + w\sigma = |\,c\,| + z\sigma + \; w\sigma = |\,c\,| + (zw)\sigma = |c| + w_1\sigma \leq \delta(\mathcal{A}).$$

Logo $\delta(\mathcal{A}') \leq \delta(\mathcal{A})$ e (2) é válido.

Seja agora $u \in \overline{X}^*$. Pelo Lema 10.3(i), $\delta(MT(u)) = n$ para algum $n \in \mathbf{N}$. Por (2) e pelo Lema 10.3(ii), obtemos

$$n = \delta(\mathcal{A}_1(u)) \geq \delta(\mathcal{A}_2(u)) \geq \ldots$$

Pelo Lema 10.3(iii), resulta que a sucessão $(\mathcal{A}_k(u))_{k\geq 1}$ é estacionária, logo $\mathcal{S}(u)$ é finito.

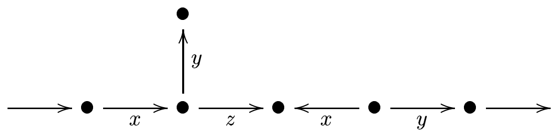
(ii) Imediato a partir de (i) e do Corolário 9.4. $\square$

Corolário 10.5 *Seja X um alfabeto finito e seja $C = \{(xy, yx);\, x, y \in X\}$. Então o problema da palavra para $Inv < X; C >$ é decidível.* $\square$

O quociente $\overline{X}^*/(\rho \cup C)^\sharp$ diz-se o *monoide inverso livre nas variáveis comutativas $x \in X$.*

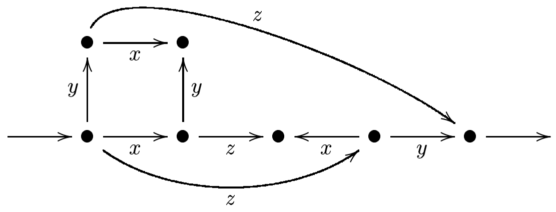
Exemplo 10.6 *Seja $X = \{x, y, z\}$ e consideremos a apresentação $Inv < X; C >$. Para $u = xyy^{-1}zx^{-1}y$, temos*

$MT(u)$:



$\delta(MT(u)) = 4$;

$\mathcal{S}(u)$:



$\delta(\mathcal{S}(u)) = 2.$

Exercício 10.7 *Dados $x \in X$ e $k, l \in \mathbf{Z}$, mostre que o problema da palavra para a apresentação $Inv < X; x^k = x^l >$ é decidível.*

11 Apresentações da forma $Inv < X; e = 1 >$, $e \in D_X$

Vamos agora considerar apresentações do tipo $Inv < X; e = 1 >$, com $e \in D_X$. Veremos que o problema da palavra é decidível para estas apresentações, tal como foi provado por Margolis e Meakin [12] [4], embora os autómatos de Schützenberger sejam infinitos. A decidibilidade resultará do facto das geodésicas de um tal autómato constituirem uma linguagem reconhecível.

Lema 11.1 *$R_X \in \mathrm{Rec}\overline{X}$.*

Dem. Seja Γ o $\overline{X}$-grafo definido por

- $V(\Gamma) = \{i\} \cup \{q_x; x \in \overline{X}\}$,
- $E(\Gamma) = \{(i, x, q_x);\ x \in \overline{X}\} \cup \{(q_y, x, q_x);\ x, y \in \overline{X}, y \neq x^{-1}\}$.

Definimos o $\overline{X}$-autómato $\mathcal{A} = (i, \Gamma, V(\Gamma))$. Temos $1 \in L(\mathcal{A})$ e os caminhos bem-sucedidos não-triviais em $\mathcal{A}$ são da forma

$$i \xrightarrow{x_1} q_{x_1} \xrightarrow{x_2} \dots \xrightarrow{x_n} q_{x_n}$$

com $x_j \in \overline{X}$ e $x_{j+1} \neq x_j^{-1}$; logo $L(\mathcal{A}) = R_X$ e $R_X \in \mathrm{Rec}\overline{X}$. $\square$

O resultado seguinte é habitualmente referido como Teorema de Benois.

Teorema 11.2 *Seja* $L \in \mathrm{Rec}\overline{X}$. *Então* $L\iota \in \mathrm{Rec}\overline{X}$ *e podemos construir efectivamente um* $\overline{X}$*-autómato* $\mathcal{A}'$ *tal que* $L(\mathcal{A}') = L\iota$ *a partir de um* $\overline{X}$*-autómato* $\mathcal{A}$ *tal que* $L(\mathcal{A}) = L$.

Dem. Seja $\mathcal{A} = (I, \Gamma, F)$ um $\overline{X}$-autómato tal que $L(\mathcal{A}) = L$. Vamos definir uma sequência $(\mathcal{A}_k)_{k\geq 1}$ de $\overline{X}$-autómatos indutivamente. Tomamos $\mathcal{A}_1 = \mathcal{A}$. Se $A_k = (I_k, \Gamma_k, F_k)$ está definido, definimos um $\overline{X}$-1-autómato $B_k = (I_k, \Gamma'_k, F_k)$ por

- $V(\Gamma'_k) = V(\Gamma_k)$,
- $E(\Gamma'_k) = E(\Gamma_k) \cup \{(p, 1, q);\ (p, xx^{-1}, q)$ é um caminho em Γ_k, $x \in \overline{X}$, $p \neq q\}$.

Finalmente, definimos $\mathcal{A}_{k+1} = (I_{k+1}, \Gamma_{k+1}, F_{k+1})$ como sendo o $\overline{X}$-autómato obtido a partir de $\mathcal{B}_k$ pelo algoritmo do Teorema 5.3. Para todo $k \geq 1$, temos

$$V(\Gamma_k) = V(\Gamma_{k+1}),$$

$$E(\Gamma_k) \subseteq E(\Gamma_{k+1}),$$

$$I_k \subseteq I_{k+1},$$

$$F_k = F_{k+1},$$

logo $\mathcal{A}_m = \mathcal{A}_{m+1}$ para algum $m \geq 1$. Além disso, $L(\mathcal{A}_k) \subseteq L(\mathcal{A}_{k+1})$ para todo $k \geq 1$, logo $L(\mathcal{A}_m) = \cup_{k\geq 1} L(\mathcal{A}_k)$. Seja

$$\widetilde{L} = \{v \in \overline{X}^* : u \overset{*}{\vdash} v \text{ para algum } u \in L\}.$$

Vamos mostrar que

$$L(\mathcal{A}_k) \subseteq \widetilde{L}$$

por indução sobre k. É imediato que $L(\mathcal{A}_1) = L \subseteq \widetilde{L}$. Suponhamos que $L(\mathcal{A}_k) \subseteq \widetilde{L}$ ($k \geq 1$), e seja $v \in L(\mathcal{A}_{k+1})$. Como $L(\mathcal{A}_{k+1}) = L(\mathcal{B}_k)$, v é rótulo de um caminho em $\mathcal{B}_k$ da forma

$$\to q_0 \xrightarrow{v_0} p_1 \xrightarrow{1} q_1 \xrightarrow{v_1} p_2 \xrightarrow{1} \ldots \xrightarrow{1} q_n \xrightarrow{v_n} p_{n+1} \to$$

onde $n \geq 0$, $q_j \xrightarrow{v_j} p_{j+1}$ é um caminho em $\mathcal{A}_k$, e $(p_j, 1, q_j) \in E(\mathcal{B}_k)$ para todo j. Por definição de $\mathcal{B}_k$, existe em $\mathcal{A}_k$ um caminho da forma

$$p_j \xrightarrow{x_j x_j^{-1}} q_j$$

para todo $j \in \{1, ..., n\}$. Logo $w = v_0 x_1 x_1^{-1} v_1 ... x_n x_n^{-1} v_n \in L(\mathcal{A}_k)$. Por hipótese de indução, $u \overset{*}{\vdash} w$ para algum $u \in L$. Como $w \overset{*}{\vdash} v_1 ... v_n = v$, resulta que $u \overset{*}{\vdash} v$ e logo $L(\mathcal{A}_{k+1}) \subseteq \widetilde{L}$.

Por indução, $L(\mathcal{A}_k) \subseteq \widetilde{L}$ para todo $k \geq 1$; em particular, $L(\mathcal{A}_m) \subseteq \widetilde{L}$ Por outro lado, como $L(\mathcal{A}_{k+1}) = L(\mathcal{B}_k)$, é imediato que

$$u \in L(\mathcal{A}_k), u \vdash v \ \Rightarrow\ v \in L(\mathcal{A}_{k+1})$$

para todo $k \geq 1$. Logo

$$\widetilde{L} \subseteq \bigcup_{k \geq 1} L(\mathcal{A}_k) = L(\mathcal{A}_m),$$

e $\widetilde{L} = L(\mathcal{A}_m)$.

Daqui resulta que

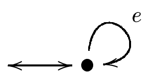
$$L\iota = \widetilde{L} \cap R_X = L(\mathcal{A}_m) \cap R_X.$$

Obviamente, $\mathcal{A}_m$ é efectivamente construível e, pelo Lema 11.1, podemos construir um $\overline{X}$-autómato finito que reconheça R_X. Pelo Teorema 5.5(ii), podemos construir efectivamente um $\overline{X}$-autómato finito $\mathcal{A}'$ tal que $L(\mathcal{A}') = L\iota$. $\square$

Até ao fim desta secção, fixamos uma apresentação $Inv < X; e = 1 >$, com $e \in D_X - \{1\}$, e escrevemos $R = \{(e,1)\}$. Note-se que, se $p \xrightarrow{e} q$ é um caminho num $\overline{X}$-autómato inverso, então $q = p$; assim, na R-expansão completa de um $\overline{X}$-autómato inverso finito, apenas há a considerar colagens de caminhos da forma $p \xrightarrow{e} p$.

Lema 11.3 *Sejam $\mathcal{A}$ e $\mathcal{A}'$ $\overline{X}$-autómatos duais tais que $\mathcal{A} \prec_R \mathcal{A}'$ e $\mathcal{A} \models \mathbf{P}$. Então $\mathcal{A}' \models \mathbf{P}$.*

Dem. Seja $\mathcal{B}$ o $\overline{X}$-autómato dual descrito por



Qualquer caminho $p \xrightarrow{v} p$ em $\mathcal{B}$ induz um caminho $\rightarrow p' \xrightarrow{v} p'$ em $MT(e)$, que satisfaz $\mathbf{P}$. Resulta que $L(\mathcal{B}) \subseteq L(MT(e))$ e logo $L(\mathcal{B}) \subseteq D_X$.

Podemos assumir que $\mathcal{A}'$ resulta de $\mathcal{A} = (i, \Gamma, f)$ por colagem de um caminho $p \xrightarrow{e} p$, $p \in V(\mathcal{A})$, ou seja, por colagem de $\mathcal{B}$. Seja $\omega\colon i \xrightarrow{v} i$ um caminho em $\mathcal{A}'$. Se ω for também um caminho em $\mathcal{A}$, então $v\iota = 1$, pois $\mathcal{A} \models \mathbf{P}$. Caso contrário, ω admite uma factorização do tipo

$$i \xrightarrow{a_0} p \xrightarrow{b_1} p \xrightarrow{a_1} \ldots \xrightarrow{b_n} p \xrightarrow{a_n} i,$$

onde

$n \geq 1$,

$i \xrightarrow{a_0 \ldots a_n} i$ é um caminho em $\mathcal{A}$,

$b_j \in L(\mathcal{B})$ para $j = 1, \ldots, n$.

Como $\mathcal{A} \models \mathbf{P}$ e $L(\mathcal{B}) \subseteq D_X$, resulta que

$$v\iota = (a_0 b_1 a_1 \ldots b_n a_n)\iota = (a_0 \ldots a_n)\iota = 1,$$

logo $\mathcal{A}' \models \mathbf{P}$. $\square$

Lema 11.4 *Para todos* $u \in \overline{X}^*$ *e* $k \geq 1$,

(i) $\mathcal{A}_k(u)$ *é uma árvore,*

(ii) $G(\mathcal{A}_k(u)) = (G(u) \cdot [G(e)]^{k-1})\iota$,

(iii) $G_p(\mathcal{A}_k(u)) = u\iota$.

Dem. (i) Pelo Lema 7.4(i), basta-nos mostrar que $\mathcal{A}_k(u) \models \mathbf{P}$ por indução sobre k. Como $\mathcal{A}_1(u) = MT(u)$ é uma árvore, é imediato que $\mathcal{A}_1(u) \models \mathbf{P}$. Suponhamos que $\mathcal{A}_k(u) \models \mathbf{P}$, com $k \geq 1$. Como $\mathcal{B}_k(u)$ é obtido a partir de $\mathcal{A}_k(u)$ por uma R-expansão completa, resulta da aplicação sucessiva do lema anterior que $\mathcal{B}_k(u) \models \mathbf{P}$. Como $\mathcal{A}_{k+1}(u)$ é obtido a partir de $\mathcal{B}_k(u)$ por redução completa, resulta da aplicação sucessiva do Lema 7.4(ii) que $\mathcal{A}_{k+1}(u) \models \mathbf{P}$. Logo $\mathcal{A}_k(u)$ é uma árvore para todo $k \geq 1$.

(ii) Vamos usar indução sobre k. O caso $k = 1$ é trivial. Suponhamos que

$$G(\mathcal{A}_k(u)) = (G(u) \cdot [G(e)]^{k-1})\iota \qquad (k \geq 1).$$

Seja $\to i \xrightarrow{g} q$ uma geodésica de $\mathcal{A}_{k+1}(u)$. Como $\mathcal{A}_{k+1}(u)$ é obtido a partir de $\mathcal{B}_k(u)$ por redução completa, existe um vértice q' em $\mathcal{B}_k(u)$ que após a sequência de reduções dá origem a q. Seja $\to i' \xrightarrow{v} q'$ uma geodésica em $\mathcal{B}_k(u)$.

Se $q' \in V(\mathcal{A}_k(u))$ então, por minimalidade de $\mid v \mid$, $\to i' \xrightarrow{v} q'$ é uma geodésica em $\mathcal{A}_k(u)$. Caso contrário, novamente por minimalidade de $\mid v \mid$, existe uma factorização $v = wf$ tal que:

(†) $\to i' \xrightarrow{w} p'$ é uma geodésica em $\mathcal{A}_k(u)$ para algum $p' \in V(\mathcal{A}_k(u))$;

(††) $f \leq_p e$ ou $f \leq_p e^{-1}$.

Em qualquer dos casos, podemos assumir a existência de uma factorização $v = wf$ nas condições (†) e (††). Como $\to i' \xrightarrow{v} q'$ é um caminho em $\mathcal{B}_k(u)$, existe em $\mathcal{A}_{k+1}(u)$ um caminho $\to i \xrightarrow{v} q$, e logo um caminho $\to i \xrightarrow{v\iota} q$. Como $\mathcal{A}_{k+1}(u)$ é uma árvore, resulta que $g = v\iota = (wf)\iota$. Por hipótese de indução, $w \in (G(u) \cdot [G(e)]^{k-1})\iota$. Por outro lado, $f\iota \in G(e) = G(e^{-1})$, logo $g \in (G(u) \cdot [G(e)]^k)\iota$.

Para provar a inclusão recíproca, basta observar que para qualquer palavra $v \in (G(u) \cdot [G(e)]^{k-1})\iota \cdot G(e)$ existe um caminho $\to i \xrightarrow{v\iota} q$ em $\mathcal{A}_{k+1}(u)$, que será necessariamente uma geodésica.

Seja $w \in (G(u) \cdot [G(e)]^{k-1})\iota$ e seja $f \in G(e)$. Por hipótese de indução, existe uma geodésica $\to i' \xrightarrow{w} q'$ em $\mathcal{A}_k(u)$. Além disso, $f = e'\iota$ para algum $e' \leq_p e$. Logo existem caminhos

$\to i' \xrightarrow{we'} p'$ em $\mathcal{B}_k(u)$;

$\to i \xrightarrow{we'} p$ em $\mathcal{A}_{k+1}(u)$;

$\rightarrow i \xrightarrow{(we')\iota} p'$ em $\mathcal{A}_{k+1}(u)$.

Como $(we')\iota = (wf)\iota$, resulta que $G(\mathcal{A}_{k+1}(u)) = (G(u) \cdot [G(e)]^k)\iota$, como queríamos demonstrar.

(iii) Para todo $k \geq 1$, $u\iota \in L(\mathcal{A}_k(u))$ implica que $u\iota$ é a geodésica principal de $\mathcal{A}_k(u)$. $\square$

Teorema 11.5 *Para todo $u \in \overline{X}^*$,*

(i) $\mathcal{A}(u)$ é uma árvore,

(ii) $G(\mathcal{A}(u)) = (G(u) \cdot [G(e)]^*)\iota$,

(iii) $G_p(\mathcal{A}(u)) = u\iota$.

Dem. (i) Suponhamos que $\mathcal{A}(u) = (i, \Gamma, f)$ não é uma árvore. Então existe em $\mathcal{A}(u)$ um caminho da forma $i \xrightarrow{v} i$ com $v\iota \neq 1$. Seja $i \xrightarrow{w} f$ um caminho em $\mathcal{A}(u)$. Então

$$w, vw \in L(\mathcal{A}(u)) = \bigcup_{k \geq 1} L(\mathcal{A}_k(u)),$$

logo $w, vw \in L(\mathcal{A}_m(u))$ para algum $m \geq 1$. Como $\mathcal{A}_m(u)$ é injectivo, resulta que existe um caminho $\rightarrow i' \xrightarrow{v} i'$ em $\mathcal{A}_m(u)$, contradizendo o lema anterior. Logo $\mathcal{A}_m(u)$ é uma árvore.

(ii) Seja $i \xrightarrow{g} q$ uma geodésica de $\mathcal{A}(u)$, e seja $q \xrightarrow{v} f$ um caminho em $\mathcal{A}(u)$. Então $gf \in L(\mathcal{A}(u)) = \cup_{k \geq 1} L(\mathcal{A}_k(u))$ e logo existe um caminho $\rightarrow i' \xrightarrow{g} q'$ em $\mathcal{A}_m(u)$ para algum $m \geq 1$. Como $g \in R_X$ e $\mathcal{A}_m(u)$ é uma árvore, g é uma geodésica de $\mathcal{A}_m(u)$. Pelo lema anterior,

$$g \in (G(u) \cdot [G(e)]^{m-1})\iota \subseteq (G(u) \cdot [G(e)]^*)\iota.$$

Reciprocamente, suponhamos que $g \in (G(u) \cdot [G(e)]^m)\iota$ para algum $m \geq 1$. Pelo lema anterior, existe uma geodésica $i' \xrightarrow{g} p$ em $\mathcal{A}_{m+1}(u)$. Logo

$$gh \in L(\mathcal{A}_{m+1}(u)) \subseteq L(\mathcal{A}(u))$$

para algum $h \in \overline{X}^*$, pelo que existe um caminho $i \xrightarrow{g} q$ em $\mathcal{A}(u)$. Como $g \in R_X$, g é uma geodésica de $\mathcal{A}(u)$.

(iii) Imediato. $\square$

Resulta do teorema anterior que os autómatos $\mathcal{A}(u)$ são sempre infinitos. No entanto, podemos provar que:

Teorema 11.6 *O problema da palavra para $Inv < X; e = 1 >$ é decidível.*

Dem. Pelo Corolário 8.2, basta-nos mostrar que é decidível, para todos $u, v \in \overline{X}^*$, se $v \in L(\mathcal{A}(u))$. Pelos Teoremas 6.4 e 11.5, $v \in L(\mathcal{A}(u))$ se e só se

$$w\iota \in (G(u) \cdot [G(e)]^*)\iota \text{ para todo } w \leq_p v$$

e $v\iota = u\iota$. Logo basta-nos mostrar que é decidível, para todos $u \in \overline{X}^*$ e $w \in R_X$, se $w \in (G(u) \cdot [G(e)]^*)\iota$.

Como $G(u)$ e $G(e)$ são linguagens finitas, são reconhecíveis. Pelo Teorema 5.5, podemos construir efectivamente um $\overline{X}$-autómato finito $\mathcal{B}$ tal que

$$L(\mathcal{B}) = G(u) \cdot [G(e)]^*.$$

Pelo Teorema 11.2, podemos construir efectivamente um $\overline{X}$-autómato finito $\mathcal{B}'$ tal que

$$L(\mathcal{B}') = (G(u) \cdot [G(e)]^*)\iota.$$

Como é decidível, para todo $w \in R_X$, se $w \in L(\mathcal{B}')$, resulta que o problema da palavra para $Inv < X; e = 1 >$ é decidível. □

Exercício 11.7 *Considere a apresentação* $Inv < x, y; x^{-1}xyxx^{-1}y^{-1} = 1 >$.

(i) Construa um autómato que reconheça as geodésicas de $\mathcal{A}(1)$.

(ii) Determine se a palavra $x^{-1}y^2xyx^{-1}xy^{-1}x^{-1}y^{-2}x$ *é congruente com 1 para esta apresentação.* □

12 Alguns resultados, algumas expectativas

A teoria combinatória de semigrupos inversos criou novas expectativas para a resolução de alguns problemas clássicos, nomeadamente ao nível das apresentações com uma única relação. O problema da palavra para apresentações com uma única relação $Gp < X; u = v >$ foi resolvido em 1932 por Magnus [9], no que constitui um dos mais celebrados resultados da teoria combinatória de grupos. O problema correspondente para apresentações de monoides $Mon < X; u = v >$ foi resolvido em dois casos particulares importantes por Adjan:

- o caso $v = 1$ [1];
- o caso em que u e v começam por letras diferentes e acabam por letras diferentes [2].

Posteriormente, o que restava do problema foi reduzido aos casos

$$Mon < x, y; xay = xbx >,$$

$$Mon < x, y; xay = x >,$$

onde $a, b \in \{x, y\}^*$ [3]. Em função disto, vamos mostrar que a resolução do problema da palavra para as apresentações da forma $Inv < x, y; w = 1 >$, $w \in R_{\{a,b\}}$, implica a resolução do problema da palavra para todas as apresentações da forma $Mon < X; u = v >$.

Vamos fixar $X = \{x, y\}$, $u \in xX^*y$ e $v \in xX^*x \cup x$. Seja τ a congruência em X^* gerada pela relação $u = v$ e seja $M = X^*/\tau$.

Lema 12.1 *Para todos $a, b, c \in X^*$,*

$$(ac)\tau = (bc)\tau \Rightarrow a\tau = b\tau.$$

Dem. Dados $p, q \in X^*$, escrevemos $p\,\tau_n\,q$ se $p\,\tau\,q$ e n é o menor inteiro não negativo tal que existem $w_0, ..., w_n \in X^*$ tais que:

$p = w_0,$

$q = w_n,$

para todo $i \in \{1, ..., n\}$, existem $g_i, h_i \in X^*$ tais que

$$\{w_{i-1}, w_i\} = \{g_i u h_i, g_i v h_i\}.$$

Vamos mostrar que

$$(ac)\,\tau_n\,(bc) \Rightarrow a\,\tau_n\,b$$

usando indução sobre n.

O caso $n = 0$ é trivial. Suponhamos que

$$(ac)\,\tau_m\,(bc) \Rightarrow a\,\tau_m\,b$$

para todos $a, b, c \in X^*$ e $m < n$ $(n \geq 1)$. Suponhamos que $(ac)\,\tau_n\,(bc)$. Sem perda de generalidade, podemos assumir que $c \in X$. Mais especificamente, vamos assumir que $c = y$ (o caso $c = x$ é inteiramente análogo). Por hipótese, existem $w_0, ..., w_n \in X^*$ tais que:

$ac = w_0,$

$bc = w_n,$

para todo $i \in \{1, ..., n\}$, existem $g_i, h_i \in X^*$ tais que

$$\{w_{i-1}, w_i\} = \{g_i u h_i, g_i v h_i\}.$$

Suponhamos que $h_i = 1$ para algum $i \in \{1, ..., n\}$. Então a última letra na sucessão $w_0, ..., w_n$ muda pelo menos duas vezes e, por minimalidade de n, as mudanças não são consecutivas. Logo, existem $i, j \in \{1, ..., n-1\}$, com $i < j$, tais que

$$w_{i-1} = g_i u, \qquad w_i = g_i v,$$

$$w_j = g_{j+1}v, \qquad w_{j+1} = g_{j+1}u.$$

Como $w_i\,\tau_{j-i}\,w_j$ e $j-i<n$, resulta da hipótese de indução que $g_i\,\tau_{j-i}\,g_{j+1}$. Logo $w_{i-1}\,\tau_{j-i}\,w_{j+1}$ e $(ac)\,\tau_{n-2}\,(bc)$, absurdo. Logo $h_i \neq 1$ para todo $i \in \{1,...,n\}$. Daqui resulta que podemos escrever $w_i = w_i'c$ para todo $i \in \{1,...,n\}$, e logo $a\,\tau_m\,b$ para algum $m \leq n$. Verifica-se facilmente que o caso $m<n$ conduz a um absurdo, logo $a\,\tau_n\,b$ e o lema está demonstrado. $\square$

Teorema 12.2 *Se o problema da palavra para* $Inv < X; uv^{-1} = 1 >$ *for decidível, então o problema da palavra para* $Mon < X; u = v >$ *é decidível.*

Dem. Seja ν a congruência em $\overline{X}^*$ gerada pela relação $\rho \cup \{(uv^{-1},1)\}$, e seja $N = \overline{X}^*/\nu$. Consideremos o homomorfismo

$$\begin{aligned} \varphi\colon X^* &\to N \\ t &\mapsto t\nu. \end{aligned}$$

Como

$$u\varphi = (vu^{-1}u)\varphi = (vu^{-1}uv^{-1}v)\varphi = v\varphi,$$

resulta do Teorema 1.1(ii) que podemos definir um homomorfismo $\Phi: M \to N$ por $(t\tau)\Phi = t\nu$.

Para cada $z \in X$, definimos uma função

$$\begin{aligned} \gamma_z\colon M &\to M \\ b &\mapsto b(z\tau). \end{aligned}$$

Pelo lema anterior, γ_z é injectiva. Definimos também $\gamma_{z^{-1}} = \gamma_z^{-1}$, $\gamma_1 = 1$ e, dados $z_1, ..., z_n \in \overline{X}$,

$$\gamma_{z_1...z_n} = \gamma_{z_1}...\gamma_{z_n}.$$

É imediato que

$$\begin{aligned} \gamma\colon \overline{X}^* &\to PI(M) \\ w &\mapsto \gamma_w \end{aligned}$$

é um homomorfismo de monoides. Como $\gamma_w^{-1} = \gamma_{w^{-1}}$ para todo $w \in \overline{X}^*$, imγ é um submonoide inverso de $PI(M)$.

Como $\gamma_u = \gamma_v$, podemos definir um homomorfismo

$$\begin{aligned} \Gamma_1\colon M &\to PI(M) \\ t\tau &\mapsto \gamma_t. \end{aligned}$$

Finalmente, como $\rho \subseteq \mathrm{Ker}\gamma$ e

$$\gamma_{uv^{-1}} = \gamma_u\gamma_v^{-1} = \gamma_u\gamma_u^{-1} = \gamma_1,$$

podemos definir um homomorfismo

$$\begin{aligned} \Gamma_2 \colon N &\to PI(M) \\ w\nu &\mapsto \gamma_w. \end{aligned}$$

Obtemos assim um diagrama comutativo

$$\begin{tikzcd} M \arrow[r, "\Phi"] \arrow[d, "\Gamma_1"'] & N \arrow[dl, "\Gamma_2"] \\ PI(M) & \end{tikzcd}$$

Dados $t, t' \in X^*$, temos que $t\Gamma_1 = t'\Gamma_1$ implica

$$t\tau = (1\tau)\gamma_t = (1\tau)\gamma_{t'} = t'\tau,$$

logo Γ_1 é injectivo. Consequentemente, Φ é injectivo e

$$t\nu = t'\nu \Leftrightarrow t\tau = t'\tau$$

para todos $t, t' \in X^*$. Daqui resulta que se o problema da palavra for decidível para $Inv < X; uv^{-1} = 1 >$, então é decidível para $Mon < X; u = v >$. $\square$

Corolário 12.3 *Se o problema da palavra for decidível para as apresentações da forma* $Inv < x, y; w = 1 >$, $w \in R_{\{x,y\}}$, *então é decidível para todas as apresentações da forma* $Mon < X; u = v >$. $\square$

Infelizmente, o problema da palavra para estas apresentações de monoides inversos permanece em aberto.

Vamos agora enumerar alguns resultados positivos obtidos nos últimos anos para tipos particulares de apresentações de monoides inversos.

Teorema 12.4 *[12] [22] Se* R *é uma relação finita em* $\overline{X}^*$ *e* $R \subseteq \pi$, *então o problema da palavra para* $Inv < X; R >$ *é decidível.* $\square$

Note-se que o Teorema 11.7 pode ser visto como um corolário deste resultado. Contudo, os dois algoritmos conhecidos para demonstrar o Teorema 12.4 são de complexidade bastante superior ao algoritmo apresentado na demonstração do Teorema 11.7.

Dados dois elementos a, b de um grupo G, dizemos que a e b são *conjugados* se $b = cac^{-1}$ para algum $c \in G$. O *problema da conjugação* (decidir se dois elementos do quociente definido por uma dada apresentação são ou não conjugados) é em geral bastante mais complexo que o problema da palavra; em particular, o problema da conjugação para apresentações de grupos com uma única relação encontra-se ainda em aberto.

Procurou-se estender o conceito de conjugação aos monoides de forma razoável, surgindo várias alternativas. Assim, dado um monoide M e $a, b \in M$, dizemos que a e b são:

- *conjugados* se existirem $c, d \in M$ tais que

$$ac = cb \qquad \text{e} \qquad bd = da;$$

- *transpostos* se existirem $u, v \in M$ tais que

$$a = uv \qquad \text{e} \qquad b = vu.$$

Para grupos, os dois conceitos coincidem com o conceito clássico de conjugação. No caso dos monoides livres, os dois conceitos são também equivalentes [8].

Dada uma palavra de Dyck $e \in D_X$, dizemos que e é uma palavra de Dyck *restrita* se $f\iota \in X^*$ para todo $f \leq_p e$.

Teorema 12.5 *[25] Seja $e \in D_X$. Então:*

(i) o problema da transposição para $Inv < X; e = 1 >$ é decidível;

(ii) se e é uma palavra de Dyck restrita, o problema da conjugação para $Inv < X; e = 1 >$ é decidível. □

Um monoide inverso M diz-se um *monoide de Clifford* se

$$\forall a \in M \, \forall e \in E(M) \; ae = ea.$$

Seja ξ a congruência em $\overline{X}^*$ gerada pela relação

$$\rho \cup \{(ae, ea); \; a \in \overline{X}^*, \; e \in D_X\}.$$

Então $\overline{X}^*/\xi$ é o *monoide de Clifford livre* sobre o conjunto X. O monoide de Clifford definido por uma apresentação da forma $Clf < X; R >$, com $R \subseteq \overline{X}^* \times \overline{X}^*$, é o quociente $\overline{X}^*/(\xi \cup R)^\sharp$.

Teorema 12.6 *[21] Seja $Clf < X; R >$ uma apresentação finita. Então o problema da palavra para $Clf < X; R >$ é decidível se e só se o problema da palavra para $Gp < X; R' >$ é decidível para todo $R' \in S$, onde S é um conjunto efectivamente construível de subconjuntos de R.* □

Corolário 12.7 *O problema da palavra para a apresentação $Clf < X; u = v >$ é decidível para todos $u, v \in \overline{X}^*$.* □

Designamos por $\overline{X}^* \cup \{0\}$ o monoide obtido a partir de $\overline{X}^*$ acrescentando um elemento absorvente 0, isto é, tal que

$$0a = a0 = 0$$

para todo $a \in \overline{X}^* \cup \{0\}$.

Dado $k \geq 2$, designamos por η_k a congruência em $\overline{X}^* \cup \{0\}$ gerada pela relação

$$\rho \cup \{(a^k, 0); \; a \in \overline{X}^* - D_X\}.$$

O monoide inverso definido por uma apresentação da forma $Nil_k < X; R >$, com $R \subseteq (\overline{X}^* \cup \{0\}) \times (\overline{X}^* \cup \{0\})$, é o quociente

$$(\overline{X}^* \cup \{0\})/(\eta_k \cup R)^\sharp.$$

Teorema 12.8 *[23] O problema da palavra é decidível para toda a apresentação finita* $Nil_k < X; R >$, $k \geq 2$. $\square$

References

[1] S. I. Adjan, On algorithmic problems in effectively complete classes of groups, *Dokl. Akad. Nauk. SSSR* 123 (1958), 13–16 (Russo).

[2] S. I. Adjan, On the embeddability of semigroups in groups (Tradução inglesa), *Soviet Mathematics* 1, Amer. Math. Soc. (1960).

[3] S. I. Adjan and G. S. Makanin, Studies in algorithmic questions of algebra, *Proc. Steklov Inst. of Math.* 168 (1984), Tradução inglesa (1986), 207–226.

[4] J.-C. Birget, S. W. Margolis and J. C. Meakin, The word problem of inverse monoids presented by one idempotent relator, *Theor. Comp. Sci.* 123 (2) (1994), 273–289.

[5] S. Eilenberg, *Automata, languages and machines* (vol.A) (Academic Press 1974).

[6] J. M. Howie, *An introduction to semigroup theory* (Academic Press 1976).

[7] J. M. Howie, *Automata and languages* (Clarendon Press 1991).

[8] A. Lentin and M. P. Schützenberger, A combinatorial problem in the theory of free monoids, *Proc. Univ. North Carolina* (1967), 128-144.

[9] R. C. Lyndon, *Combinatorial group theory* (Springer-Verlag 1977).

[10] S. W. Margolis and J. C. Meakin, E-unitary inverse monoids and the Cayley graph of a group presentation, *J. Pure Appl. Alg.* 58 (1989), 45–76.

[11] S. W. Margolis and J. C. Meakin, Inverse monoids and rational Schreier subsets of the free group, Semigroup Forum 44 (1992), 137–148.

[12] S. W. Margolis and J. C. Meakin, Inverse monoids, trees and context-free languages, *Trans. Amer. Math. Soc.* 335 (1) (1993), 259–276.

[13] S. W. Margolis and J. C. Meakin, Free inverse monoids and graph immersions, *Int. J. Alg. Comp.* 3.1 (1993), 79–100.

[14] S. W. Margolis, J. C. Meakin and M. V. Sapir, Algorithmic problems in groups, semigroups and inverse semigroups, in *Semigroups, formal languages and groups*, J. Fountain (ed.), Kluwer 1995, 147–214.

[15] A. Markov, On the impossibility of certain algorithms in the theory of associative systems, *Dokl. Acad. Sci. URSS* 55 (1947), 583–586.

[16] W. D. Munn, Free inverse semigroups, *Proc. London Math. Soc.* (3) 29 (1974), 385–404.

[17] M. Petrich, *Inverse semigroups* (Wiley 1984).

[18] E. L. Post, Recursive unsolvability of a problem of Thue, *J. Symbolic Logic* 1,12 (1947), 1–11.

[19] H. E. Scheiblich, Free inverse semigroups, *Proc. Amer. Math. Soc.* 38 (1973), 1–7.

[20] B. M. Schein, Free inverse semigroups are not finitely presentable, *Acta. Math. Acad. Sci. Hung.* 26 (1975), 41–52.

[21] P. V. Silva, Clifford monoid presentations, *Math. Proc. Camb. Phil. Soc.* 111 (1992), 445–454.

[22] P. V. Silva, Rational languages and inverse monoid presentations, *Int. J. Alg. Comp.* 2.2 (1992), 187–207.

[23] P. V. Silva, The word problem for nilpotent inverse monoids, *Semigroup Forum* 51 (1995), 285–293.

[24] P. V. Silva, On free inverse monoid languages, *R. A. I. R. O. Theoretical Informatics and Applications* (aguarda publicação).

[25] P. V. Silva, Conjugacy and transposition for inverse monoid presentations (pré-publicação).

[26] J. B. Stephen, *Application of automata theory to presentations of monoids and inverse monoids*, Ph. D. Thesis, University of Nebraska 1987.

[27] J. B. Stephen, Presentations of inverse monoids, *J. Pure Appl. Alg.* 63 (1990), 81–112.

[28] V. V. Vagner, Generalized heaps and generalized groups with a transitive compatibility relation, *Uc. Zap. Saratov Univ. Meh.-Matem.* 70 (1961), 25–39 (Russo).