Semigrupos automáticos e produtos em coroa

L. Descalço
Departamento de Matemática, Universidade de Aveiro
3830-220 Aveiro, Portugal
Telefax: +351 234 382014
E-mail: luisd@mat.ua.pt

23 de Dezembro de 2004

Resumo

Fazemos uma introdução à classe dos semigrupos automáticos e referimos diversos resultados conhecidos sobre semigrupos automáticos e construções standard da teoria dos semigrupos. Além disso mostramos que, em determinadas condições, a automaticidade é uma propriedade preservada por produtos em coroa.

1 Introdução

A noção de grupo automático foi recentemente generalizada para semigrupos e as propriedades elementares desta nova classe de semigrupos foram estabelecidas em [3]. A noção de semigrupo automático não corresponde a uma propriedade geométrica no diagrama de Cayley como no caso dos grupos onde ser automático é equivalente a ter a propriedade dos companheiros viajantes (ver [1, 5]). No entanto, constitui uma classe de semigrupos natural que contém muitos semigrupos conhecidos, e onde algumas propriedade dos grupos automáticos são satisfeitas naturalmente e outras ou requerem demonstrações diferentes ou não se verificam. A ideia de definir uma classe de semigrupos utilizando linguagens regulares, além de natural, estabelece relações interessantes entre semigrupos e linguagens formais permitindo-nos em particular utilizar ferramentas das linguagens formais para obter resultados sobre semigrupos. Além disso temos interessantes propriedades computacionais, por exemplo, o problema da palavra é solúvel em tempo quadrático (ver [3]), e vários resultados sobre semigrupos automáticos têm sido estabelecidos (ver, por exemplo, [4, 6, 8, 9, 13]).

2 Linguagens regulares e autómatos

Vamos referir algumas definições e resultados sobre linguagens regulares e autómatos que vamos precisar.

Seja A um conjunto finito. Definimos

$$A^+ = \{a_1 \dots a_n : a_1, \dots, a_n \in A, n \in \mathbb{N}\},$$

onde $\mathbb{N}$ é o conjunto dos inteiros positivos, como o conjunto de todas as sucessões finitas de elementos de A (com pelo menos um elemento). Dizemos que A é um *alfabeto* e aos elementos de A^+ chamamos *palavras*. Dado $w \in A^+$ denotamos por $|w|$ o *comprimento* de w, o qual consiste no número de elementos de A que formam a palavra w. Definimos $A^* = A^+ \cup \{\epsilon\}$, onde ϵ não é um elemento de A^+, e chamamos *linguagem* a um subconjunto de A^*. Definimos a operação *concatenação* em A^* por

$$\begin{aligned} \cdot : \quad & A^* \times A^* \to A^*; \\ & a_1 \dots a_n \cdot b_1 \dots b_m = a_1 \dots a_n b_1 \dots b_m \ (n, m \in \mathbb{N}), \\ & a_1 \dots a_n \cdot \epsilon = \epsilon \cdot a_1 \dots a_n = a_1 \dots a_n \ (n \in \mathbb{N}), \\ & \epsilon \cdot \epsilon = \epsilon, \end{aligned}$$

e escrevemos $w_1 w_2$ em vez de $w_1 \cdot w_2$ para $w_1, w_2 \in A^*$. É conveniente pensar em ϵ como uma sucessão sem elements e por isso chamamos a ϵ *palavra vazia* e temos $|\epsilon| = 0$, por convenção. Portanto podemos escrever

$$A^* = \{a_1 \dots a_n : a_1, \dots, a_n \in A, n \in \mathbb{N}_0\}.$$

Para $w \in A^*$ definimos $w^0 = \epsilon$ e $w^{n+1} = w \cdot w^n$ $(n \in \mathbb{N}_0)$. Observe-se que a operação $\cdot$ é *associativa*, i.e. temos $(w_1 \cdot w_2) \cdot w_3 = w_1 \cdot (w_2 \cdot w_3)$ para $w_1, w_2, w_3 \in A^*$.

Dadas duas linguagens $L, K \subseteq A^*$ definimos a concatenação $L \cdot K$ por

$$L \cdot K = \{w_1 \cdot w_2 : w_1 \in L, w_2 \in K\}$$

e escrevemos LK em vez de $L \cdot K$. Dada uma linguagem L definimos

$$\begin{aligned} & L^0 = \{\epsilon\}, \\ & L^{n+1} = L \cdot L^n \ (n \in \mathbb{N}_0), \\ & L^* = \bigcup_{n=0}^{\infty} L^n = \{w_1 \cdot w_2 \cdot \ldots \cdot w_n : w_1, w_2, \dots, w_n \in L, n \in \mathbb{N}_0\} \end{aligned}$$

e chamamos a $*$ a *operação fecho de Kleene.*

Dizemos que uma linguagem é *regular* se pode ser obtida a partir de subconjuntos finitos de A^* aplicando as operações $\cup$ (união), $\cdot$ (concatenação) e $*$ (operação fecho de Kleene) um número finito de vezes. Por exemplo, se definirmos $A = \{b, c\}$, então a linguagem $M = \{c^n b^m : n, m \in \mathbb{N}_0\}$ é regular pois $M = \{c\}^* \cdot \{b\}^*$.

Um *autómato finito* (ou simplesmente um *autómato*) é um quíntuplo

$$\mathcal{A} = (Q, A, \mu, q_0, T)$$

onde Q é um conjunto finito chamado o conjunto de *estados*, A é um alfabeto chamado o *alfabeto de entrada*, μ é uma função $\mu : Q \times A \to \mathcal{P}(Q)$ chamada a *transição* (denotamos por $\mathcal{P}(Q)$ o conjunto de todos os subconjuntos de Q), $q_0 \in Q$ é chamado o *estado inicial* e $T \subseteq Q$ é o conjunto de *estados terminais*. A situação $q' \in (q, a)\mu$, para $q, q' \in Q$, $a \in A$, pode ser entendida intuitivamente do modo seguinte: se $\mathcal{A}$ está no estado q e lê a entrada a então pode transitar para o estado q'.

Podemos ver um autómato como um grafo dirigido com vértices Q e uma aresta (q, a, q') para $q, q' \in Q$, $a \in A$ tais que $q' \in (q, a)\mu$. Representamos uma aresta (q, a, q') por $q \xrightarrow{a} q'$. Um *caminho* π no autómato é uma sucessão de arestas

$$(q_1, a_1, q_2), (q_2, a_2, q_3), \ldots, (q_n, a_n, q_{n+1}),$$

onde $q_1, \ldots, q_{n+1} \in Q$, $a_1, \ldots, a_n \in A$, que representamos por

$$\pi : q_1 \xrightarrow{a_1} q_2 \xrightarrow{a_2} \ldots \xrightarrow{a_n} q_{n+1}, \tag{1}$$

ou apenas um terno (q, ϵ, q), com $q \in Q$, que representamos por

$$\pi : q \xrightarrow{\epsilon} q.$$

Dizemos que um caminho é *bem sucedido* se tiver início no estado inicial e terminar num estado terminal. Dizemos que o caminho π acima é *etiquetado* por $a_1 \ldots a_n$ (ou por ϵ). Escrevemos simplesmente

$$\pi : q \xrightarrow{w} q',$$

com $w \in A^*$, para dizer que π é um caminho em $\mathcal{A}$ do estado q para o estado q' etiquetado por w.

Dizemos que uma palavra $w \in A^*$ é *reconhecida* pelo autómato $\mathcal{A}$ se existir um caminho bem sucedido π em $\mathcal{A}$ etiquetado por w; observe-se que a palavra vazia ϵ é reconhecida se e só se o estado inicial for um estado terminal. A *linguagem reconhecida* pelo autómato $\mathcal{A}$ é o conjunto das palavras reconhecidas por $\mathcal{A}$; denotamos este conjunto por $\mathcal{L}(\mathcal{A})$. Uma linguagem diz-se *reconhecível* se existir um autómato que a reconhece. Por exemplo, a linguagem M definida acima, é reconhecida pelo autómato dado pela Figura 1; a figura também ilustra como um autómato se pode definir por uma figura: uma seta aponta o estado inicial q_0 e saem setas dos estados terminais q_0 e q_1. É sabido que a classe das linguagens regulares e a classe das linguagens reconhecíveis coincidem (ver por exemplo [12]) e usamos os dois termos como sinónimos.

Dizemos que um autómato é *determinístico* se o conjunto $(q, a)\mu$ tem no máximo um elemento para cada $q \in Q, a \in A$, e não determinístico e não determinístico caso contrário. Para autómatos determinísticos escrevemos $q' = qw$, se existir um caminho do estado q para o estado q' etiquetado pela palavra w. Dizemos que um autómato é *completo* se para cada $q \in Q$, $a \in A$ o conjunto $(q, a)\mu$ tem pelo menos um elemento. Se um autómato for determinístico e completo a transição μ pode ser vista como uma função de $Q \times A$ para Q. É sabido que, se uma linguagem é regular, então existe um

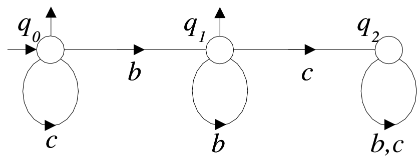

Figura 1: Um autómato que reconhece $\{c^n b^m : n, m \in \mathbb{N}_0\}$

autómato determinístico e completo que a reconhece; ver [12]. A Figura 1 é um exemplo de um autómato determinístico e completo; removendo o estado q_2 e as setas que a ele chegam obtemos um exemplo de um autómato não determinístico que reconhece a mesma linguagem.

Vamos precisar do seguinte resultado, cuja demonstração pode ser encontrada em [10], por exemplo:

Proposição 2.1 *Seja A uma alfabeto. Então temos:*

(i) $\emptyset, A^+$ *e* A^* *são regulares;*

(ii) *Qualquer subconjunto finito de* A^* *é regular;*

(iii) *Se* $L, K \subseteq A^*$ *são regulares, então* $L \cup K$, $L \cap K$, $L - K$, LK, L^* *e* $\mathrm{Pref}(L) = \{u \in A^* : uw \in L,\ \textit{para algum } w \in A^*\}$ *são regulares.*

Vamos utilizar esta proposição sem a referir explicitamente, e dizemos que uma linguagem é regular assim que a consigamos escrever, por exemplo, como uma reunião finita de linguagens regulares.

3 Semigrupos

A referencia [11] é um boa introdução à teoria de semigrupos. Vamos apenas mencionar algumas noções elementares e estabelecer a notação que vamos usar.

Seja S um conjunto e $\cdot : S \times S \to S$ uma operação em S. Dizemos que $(S, \cdot)$ é um *semigrupo* se a operação for associativa. Escrevemos $s_1 s_2$ em vez de $s_1 \cdot s_2$ para $s_1, s_2 \in S$ e dizemos que S é um semigrupo. Por exemplo, A^+ é um semigrupo com a operação concatenação.

Sejam S, T semigrupos. Uma função $\psi : S \to T$ é um *homomorfismo* (*de semigrupos*) se satisfaz $(s_1 s_2)\psi = (s_1\psi)(s_2\psi)$ para quaisquer $s_1, s_2 \in S$.

Dizemos que um semigrupo F é *livre* num conjunto finito A se: *(i)* existe uma função $\alpha : A \to F$; *(ii)* para qualquer semigrupo S e qualquer função $\phi : A \to S$ existe um único homomorfismo $\psi : F \to S$ tal que $\alpha\psi = \phi$ (observe-se que é usual colocar os símbolos das funções do lado direito e $\alpha\psi$ denota a função $\alpha\psi : A \to S; a \mapsto (a\alpha)\psi$). O semigrupo A^+ satisfaz esta definição (sendo α a identidade $A \to A^+;\ a \mapsto a$) e por isso é usual dizer que A^+ é o semigrupo livre em A.

Sejam S um semigrupo, A um conjunto finito e $\theta : A \to S$ uma função. Se a única extensão de θ a um homomorfismo $\psi : A^+ \to S$ for uma função sobrejectiva, dizemos que A é um *conjunto gerador* para S (*relativamente a* ψ).

Observe-se que, uma vez que vamos considerar linguagens em A^*, não é conveniente ver o conjunto A como um subconjunto de S. De facto, nem é requerido que a função $\theta : A \to S$ seja injectiva. No entanto, sempre que possível, não se faz uso explícito dos homomorfismos associados aos conjuntos geradores, para não complicar a notação. Para duas palavras $w_1, w_2 \in A^*$ escrevemos $w_1 = w_2$ em vez de $w_1\psi = w_2\psi$ e escrevemos $w_1 \equiv w_2$ quando queremos dizer que w_1 e w_2 são iguais enquanto palavras em A^*. Também escrevemos $w = s$ e $s = w$ com $w \in A^*$ e $s \in S$ em vez de $w\psi = s$. Finalmente, um produto da forma $x_1 \dots x_n$ onde $x_i \in A \cup S$ $(i = 1, \dots, n)$ é considerado como um produto em A^* se todos os factores pertencem a A e como um produto em S caso contrário.

Dado um semigrupo S e um conjunto gerador A para S relativamente ao homomorfismo $\psi : A^+ \to S$ dizemos que $L \subseteq A^+$ é um *conjunto de formas normais* para S se $L\psi = S$. Se a restrição $\psi \restriction_L$ for injectiva dizemos que L é um *conjunto de formas normais com unicidade* para S. Observe-se que a multiplicação no semigrupo está definida se soubermos como multiplicam as formas normais.

4 Semigrupos automáticos

Vamos agora introduzir a noção de semigrupo automático e mostrar alguns exemplos. Referimos ainda alguns resultados de maior interesse sobre semigrupos automáticos bem como alguns resultados mais técnicos que vamos utilizar.

De modo a trabalhar com autómatos que aceitam pares de palavras e para poder definir semigrupo automático, dado um conjunto A, precisamos de definir o conjunto

$$A(2, \$) = ((A \cup \{\$\}) \times (A \cup \{\$\})) \backslash \{(\$, \$)\}$$

onde \$ é um símbolo que não pertence a A e a função $\delta_A : A^* \times A^* \to A(2, \$)^*$ é definida por

$$(a_1 \dots a_m, b_1 \dots b_n)\delta_A = \begin{cases} \epsilon & \text{se } 0 = m = n \\ (a_1, b_1) \dots (a_m, b_m) & \text{se } 0 < m = n \\ (a_1, b_1) \dots (a_m, b_m)(\$, b_{m+1}) \dots (\$, b_n) & \text{se } 0 \leq m < n \\ (a_1, b_1) \dots (a_n, b_n)(a_{n+1}, \$) \dots (a_m, \$) & \text{se } m > n \geq 0. \end{cases}$$

Normalmente omite-se o índice A e escreve-se δ em vez de δ_A.

Definição 4.1 Seja S um semigrupo e A um conjunto gerador finito para S relativamente ao homomorfismo $\psi : A^+ \to S$. O par (A, L) é uma *estrutura automática para* S *(relativamente a* ψ*)* se:

(i) L é uma linguagem regular em A^+ e $L\psi = S$;

(ii) $L_= = \{(\alpha, \beta)\delta_A : \alpha, \beta \in L, \alpha = \beta\}$ é uma linguagem regular em $A(2, \$)^+$;

(iii) Para cada $a \in A$, a linguagem $L_a = \{(\alpha, \beta)\delta_A : \alpha, \beta \in L, \alpha a = \beta\}$ é regular em $A(2, \$)^+$.

Se existirem conjuntos A e L tais que (A, L) é uma estrutura automática para S dizemos que S é *automatico*.

Mostrou-se em [8] que, com esta definição, um monóide (um semigrupo com elemento neutro) automático tem uma estrutura automática (A, L) para qualquer conjunto de geradores A. Portanto a existência de uma estrutura automática não depende do conjunto geradores considerado, tal como acontece com os grupos automáticos; ver [1]. No entanto, um semigrupo pode ser automático e não admitir uma estrutura automática para um dado conjunto de geradores; ver [3].

Exemplo 4.2 Seja A um alfabeto. Então A^+, o semigrupo livre em A, é automático. Podemos considerar a linguagem regular $L = A^+$ que o par (A, L) é uma estrutura automática para o semigrupo A^+. De facto, temos

$$L_= = \{(a_1, a_1) \dots (a_k, a_k) : k \in \mathbb{N}, a_1, \dots, a_k \in A\}$$

e portanto $L_=$ é uma linguagem regular. Para cada gerador $a \in A$, temos

$$L_a = \{(a_1, a_1) \dots (a_k, a_k)(\$, a) : k \in \mathbb{N}, a_1 \dots, a_k \in A\}$$

e portanto L_a é uma linguagem regular.

O nosso próximo exemplo é o *monóide bicíclico* $\mathbf{B}$, o qual se pode definir pela apresentação (de monóides) $\langle b, c \mid bc = 1\rangle$; ver [11]. Um conjunto de formas normais com unicidade para $\mathbf{B}$ é $\{c^i b^j : i, j \geq 0\}$ e podemos identificar $\mathbf{B}$ com este conjunto. As formas normais multiplicam de acordo com a regra seguinte:

$$c^i b^j c^k b^l = \begin{cases} c^{i-j+k} b^l & \text{se } j \leq k \\ c^i b^{j-k+l} & \text{se } j > k. \end{cases}$$

Exemplo 4.3 Seja $A = \{b, c\}$ e $L = \{c^i b^j : i, j \geq 0\}$. Uma vez que a linguagem regular $L = \{c\}^*\{b\}^*$ é um conjunto de formas normais com unicidade para $\mathbf{B}$, temos

$$L_= = \{(w, w)\delta_A : w \in L\},$$

o qual é uma linguagem regular, pela Proposição 4.4, que se segue. Uma vez que

$$L_b = \{(c, c)\}^*\{(b, b)\}^*\{(\$, b)\}$$

e

$$L_c = \{(c, c)\}^*\{(b, b)\}^*\{(b, \$)\} \cup \{(c, c)\}^*\{(\$, c)\},$$

as linguagens L_b e L_c são regulares e portanto (A, L) é uma estrutura automática para $\mathbf{B}$.

Vamos precisar também do seguinte resultado sobre linguagens regulares:

Proposição 4.4 *Sejam A e B dois alfabetos. Então temos:*

(i) *Se $L \subseteq A^*$ e $K \subseteq B^*$ são linguagens regulares e $\psi : A^* \to B^*$ é um homomorfismo de monóides, então $L\psi$ e $K\psi^{-1}$ são linguagens regulares;*

(ii) *Se $L, K \subseteq A^*$ são linguagens regulares, então $(L \times K)\delta_A$ é uma linguagem regular;*

(iii) *Se L é uma linguagem regular em A^*, então $\{(w, w)\delta_A : w \in L\}$ é uma linguagem regular.*

Dem. Ver por exemplo [10] e [1]. □

Dizemos que (A, L) é uma *estrutura automática com unicidade* para um semigrupo S se (A, L) é for uma estrutura automática para S e L um conjunto de formas normais com unicidade.

Em [3] foi provado o seguinte:

Proposição 4.5 *Se (A, L) é uma estrutura automática para o semigrupo S então existe uma estrutura automática (A, K) com unicidade para S.*

Vamos precisar do seguinte resultado, provado em [7]:

Proposição 4.6 *Seja S um semigrupo automático tal que $S^2 = S$. Então S tem uma estrutura automática com unicidade (A, K) tal que $K \cap A = \emptyset$.*

Vamos agora apresentar a generalização para semigrupos, considerada em [3], dos conceitos da teoria de grupos, de diagrama de Cayley e da propriedade dos companheiros viajantes. Seja S um semigrupo gerado por um conjunto finito A. O *diagrama de Cayley* (direito) Γ de S relativamente a A é o grafo dirigido com conjunto de vértices S e com uma aresta etiquetada por a de s para sa para cada vértice $s \in S$ e cada $a \in A$. Se s e t são vértices de Γ, então um *caminho (não dirigido)* de s para t é apenas uma sequência de arestas de s até t (sem ter em conta as direcções das arestas), e o *comprimento* do caminho é o número de arestas que contém. Definimos a *distância* $d(s, t)$ de s para t como o comprimento do caminho mais curto de s para t se tal caminho existir, e igual a infinito caso contrário. Seja $L \subseteq A^+$ um conjunto regular de formas normais para S, então dizemos que Γ tem a *propriedade dos companheiros viajantes* relativamente a L se existir uma constante K tal que, sempre que $\alpha, \beta \in L$ com $d(\alpha, \beta) \leq 1$, temos $d(\alpha(t), \beta(t)) \leq K$ para cada $t \geq 1$. A propriedade dos companheiros viajantes caracteriza os grupos automáticos (ver [1]) e para semigrupos ainda temos o seguinte:

Proposição 4.7 *Se S é um semigrupo com uma estrutura automática (A, L) e se Γ é o diagrama de Cayley de S relativamente a A, então Γ tem a propriedade dos companheiros viajantes relativamente a L.*

Dem. Ver [3]. $\square$

Como observado em [3], qualquer semigrupo não automático com um zero, por exemplo, tem a propriedade dos companheiros viajantes e portanto a reciproca desta proposição não é verdadeira.

5 Máquinas sequenciais generalizadas

Uma vez que a propriedade dos companheiros viajantes não caracteriza os semigrupos automáticos, é preciso trabalhar directamente com linguagens regulares em vez do diagrama de Cayley como acontece para os grupos, para provar que um semigrupo é automático. Quando se consideram construções de semigrupos, é usual ter que construir estruturas automáticas a partir de estruturas automáticas conhecidas. Para esse efeito, o conceito de máquina sequencial generalizada, mostra-se particularmente útil.

Uma *máquina sequencial generalizada* (usualmente designada *gsm*) é um sextuplo

$$\mathcal{A} = (Q, A, B, \mu, q_0, T)$$

onde Q, A são B conjuntos finitos (chamados *conjunto dos estados*, *alfabeto de entrada* e *alfabeto de saída* respectivamente), μ é uma função (parcial) de $Q \times A$ para subconjuntos finitos de $Q \times B^*$, $q_0 \in Q$ é o *estado inicial* e $T \subseteq Q$ é o *conjunto dos estados terminais.* A inclusão $(q', u) \in (q, a)\mu$ corresponde à seguinte situação: se $\mathcal{A}$ está no estado q e lê a entrada a, então pode mover-se para o estado q' e produzir a saída u.

Podemos ver $\mathcal{A}$ como um grafo dirigido onde Q é o conjunto dos vértices, e com uma aresta $q \xrightarrow{(a,u)} q'$ para cada par $(q', u) \in (q, a)\mu$. Para um caminho

$$\pi \ : \ q_1 \xrightarrow{(a_1,u_1)} q_2 \xrightarrow{(a_2,u_2)} q_3 \dots \xrightarrow{(a_n,u_n)} q_{n+1}$$

definimos

$$\Phi(\pi) = a_1 a_2 \dots a_n, \ \Sigma(\pi) = u_1 u_2 \dots u_n.$$

Para $q, q' \in Q$, $u \in A^+$ e $v \in B^+$ escrevemos $q \xrightarrow{(u,v)}_+ q'$ para dizer que existe um caminho π de q para q' tal que $\Phi(\pi) \equiv u$ e $\Sigma(\pi) \equiv v$, e dizemos que (u, v) é a *etiqueta* do caminho. Dizemos que um caminho é *bem sucedido* se for da forma $q_0 \xrightarrow{(u,v)}_+ t$ com $t \in T$.

A gsm $\mathcal{A}$ induz uma função $\eta_{\mathcal{A}} \ : \ \mathcal{P}(A^+) \longrightarrow \mathcal{P}(B^+)$ de subconjuntos de A^+ para subconjuntos de B^+ definida por

$$X\eta_{\mathcal{A}} = \{v \in B^+ \ : \ (\exists u \in X)(\exists t \in T)(q_0 \xrightarrow{(u,v)}_+ t)\}.$$

Sabe-se que se X é regular então $X\eta_{\mathcal{A}}$ também é; ver [10, Teorema 11.1 e Exemplo 11.1]. Analogamente, $\mathcal{A}$ induz uma função $\zeta_{\mathcal{A}} \ : \ \mathcal{P}(A^+ \times A^+) \longrightarrow \mathcal{P}(B^+ \times B^+)$ definida por

$$Y\zeta_{\mathcal{A}} = \{(w, z) \in B^+ \times B^+ \ : \ (\exists (u, v) \in Y)(w \in u\eta_{\mathcal{A}} \ \& \ z \in v\eta_{\mathcal{A}})\}.$$

Foi provado em [6] que, em certas condições, também a função $\zeta_{\mathcal{A}}$ preserva a regularidade:

Teorema 5.1 *Seja* $\mathcal{A} = (Q, A, B, \mu, q_0, T)$ *uma gsm, e seja* $\pi_A : (A^* \times A^*)\delta_A \longrightarrow A^* \times A^*$ *a função inversa de* δ_A*. Suponhamos que existe uma constante* C *tal que, para quaisquer dois caminhos* α_1, α_2 *in* $\mathcal{A}$*, temos*

$$|\Phi(\alpha_1)| = |\Phi(\alpha_2)| \Longrightarrow ||\Sigma(\alpha_1)| - |\Sigma(\alpha_2)|| \leq C. \tag{2}$$

Se $M \subseteq (A^+ \times A^+)\delta_A$ *é uma linguagem regular em* $A(2, \$)^+$ *então* $N = M\pi_A\zeta_{\mathcal{A}}\delta_B$ *é uma linguagem regular em* $B(2, \$)^+$*.*

6 Construções

Foram estudadas algumas diversas standard de semigrupos e provou-se que algumas preservam a automaticidade. Apresentamos de seguida alguns resultados mais relevantes sobre semigrupos automáticos e construções de semigrupos (para uma introdução às construções referidas ver [11]).

O produto livre de semigrupos foi estudado em [3] e provou-se o seguinte:

Proposição 6.1 *Sejam* S *e* T *semigrupos. O produto livre de semigrupos* $S * T$ *é automático se e só se ambos os factores forem automáticos.*

Em [4] foi estudado o produto directo de semigrupos e provou-se o seguinte:

Proposição 6.2 *Sejam* S *e* T *semigrupos automáticos.*

(i) *Se* S *e* T *são infinitos, então* $S \times T$ *é automático se e só se* $S^2 = S$ *e* $T^2 = T$*.*

(ii) *Se* S *é finito e* T *é infinito, então* $S \times T$ *é automático se e só se* $S^2 = S$*.*

Em [15], os autores estabeleceram condições necessárias e suficientes para que o produto directo de semigrupos seja finitamente gerado:

Proposição 6.3 *Sejam* S *e* T *semigrupos. Se* S *e* T *são infinitos então* $S \times T$ *é finitamente gerado se e só se* S *e* T *são finitamente gerados,* $S^2 = S$ *e* $T^2 = T$*. Se* S *é finito e* T *é infinito então* $S \times T$ *é finitamente gerado se e só se* $S^2 = S$ *e* T *é finitamente gerado.*

Usando esta proposição, a Proposição 6.2 pode-se escrever do seguinte modo:

Proposição 6.4 *O produto directo de semigrupos é automático se e só se for finitamente gerado.*

A resposta para a questão reciproca não é conhecida nem para grupos: Se o produto directo $G_1 \times G_2$ é automático serão os factores G_1 e G_2 necessariamente automáticos?

Os semigrupos de matriz de Rees foram considerados em [6] onde se obtiveram os seguintes resultados:

Proposição 6.5 *Seja $S = \mathcal{M}[U; I, J; P]$ um semigrupo de matrix de Rees. Se U é um semigrupo automático e S é finitamente gerado então S é automático.*

Como consequência deste resultado temos o seguinte:

Corolario 6.6 *Se U é um semigrupo automático e simples então qualquer semigrupo de matriz de Rees $\mathcal{M}[U; I, J; P]$ (I e J finitos) é automático.*

A implicação reciproca não foi resolvida no caso geral, mas foi provado o seguinte:

Proposição 6.7 *Seja $S = \mathcal{M}[U; I, J; P]$ um semigrupo, e suponhamos que existe uma entrada p na matriz P tal que $pU^1 = U$. Se S é automático então U é automático.*

Foi ainda obtido outro resultado para este sentido da implicação que requer uma noção introduzida em [18]. Dizemos que um semigrupo é *prefixo-automatico* or *p-automatico* se admite uma estrutura automática (A, L) tal que o conjunto

$$L'_= = \{(w_1, w_2)\delta_A : w_1 \in L, w_2 \in \mathrm{Pref}(L), w_1 = w_2\}$$

também é regular, onde

$$\mathrm{Pref}(L) = \{w \in A^+ : ww' \in L \text{ para algum } w' \in A^*\}.$$

Provou-se o seguinte:

Proposição 6.8 *Seja $S = \mathcal{M}[U; I, J; P]$ um semigrupo de matriz de Rees. Se S é p-automatico então U é p-automatico.*

Observe-se as noções de "automático"e "p-automático"coincidem para grupos mas não se sabe se coincidem para semigrupos.

7 Produtos em coroa

Vamos considerar a automaticidade de produtos em coroa de semigrupos, $S \,\mathrm{wr}\, T$, no caso em que T é um semigrupo finito. Vamos começar por referir as condições necessárias e suficientes, obtidas em [14], para o produto em coroa neste caso ser finitamente gerado.

A propriedade "ser finitamente gerado"para produtos em coroa está relacionada com a mesma propriedade para S-actos diagonais. Vamos usar as condições obtidas para o caso em que o S-acto diagonal não é finitamente gerado para provar que, neste caso, o produto em coroa $S \,\mathrm{wr}\, T$ é automático se for finitamente gerado e S for um semigrupo automático.

Vamos começar por introduzir algumas definições que vão ser precisas. Se S é um semigrupo e X é um conjunto, então o conjunto S^X de todas as funções $X \to S$ é um semigrupo com a seguinte multiplicação: for $f, g \in S^X$, $fg : X \to S$; $x \mapsto (xf)(xg)$; este semigrupo é chamado a *potência cartesiana* de S por X. Se S tem um idempotente e, então o *suporte* de $f \in S^X$ relativamente a e é definido por

$$\operatorname{supp}_e(f) = \{x \in X : xf \neq e\}.$$

O conjunto

$$S^{(X)_e} = \{f \in S^X : |\operatorname{supp}_e(f)| < \infty\}$$

é um subsemigrupo de S^X; é chamado a *potência directa* de S em relação a e. Quando não existe perigo de confusão o índice e é normalmente omitido. Se X é finito com n elementos então S^X e $S^{(X)_e}$ coincidem, e são isomorfos ao semigrupo $S^{(n)}$ que é formado por n-uplos de elementos de S com a multiplicação componente a componente. Neste contexto escreve-se $S^{(X)_e}$ mesmo se S não tem idempotentes; podemos pensar em suportes relativamente a uma identidade previamente adicionada a S.

O *produto em coroa não restrito* $S \operatorname{Wr} T$ de dois semigrupos S e T é o conjunto $S^T \times T$ com a multiplicação

$$(f, t)(g, u) = (f\, {}^t g, tu),$$

onde ${}^t g \in S^T$ é definido por

$$(x)\, {}^t g = (xt)g.$$

Seja $e \in S$ um idempotente. O *produto em coroa (restrito)* $S_e \operatorname{wr} T$ (relativamente a e) é o subsemigrupo de $S \operatorname{Wr} T$ gerado pelo conjunto $\{(f, t) \in S \operatorname{Wr} T : |\operatorname{supp}_e(f)| < \infty\}$. Novamente, é usual omitir o índice e.

O produto em coroa $S \operatorname{wr} T$ coincide com o produto em coroa não restrito $S \operatorname{Wr} T$ no caso em que T é finito, como observado em [19, Capítulo 3].

Uma *acção* de um semigrupo S num conjunto X é uma função $X \times S \to X$, $(x, s) \mapsto xs$, que satisfaz $(xs_1)s_2 = x(s_1 s_2)$. Ao conjunto X, juntamente com a acção, chama-se uma *S-acção.* Diz-se gerada pelo conjunto $U \subseteq X$ se $US^1 = X$, e *finitamente gerada* se existir um conjunto finito U que a gera.

O *acto diagonal* de um semigrupo S é o conjunto $S \times S$ com a acção $(s_1, s_2)s = (s_1 s, s_2 s)$. Por exemplo, os actos diagonais de grupos infinitos, semigrupos livres, semigrupos comutativos livres e semigrupos completamente simples não são finitamente gerados. O acto diagonal do monoide total de transformações $T_{\mathbb{N}}$ no conjunto dos inteiros positivos pode ser gerado por um único elemento; ver [2]. Em [16] os autores mostram um exemplo de um monóide finitamente apresentado infinito com um acto diagonal finitamente gerado.

Vamos apenas referir as condições obtidas em [14] para o caso em que T é finito e S é infinito.

Proposição 7.1 *Seja S um semigrupo infinito e T um semigrupo finito não trivial. Se o S-acto diagonal é finitamente gerado então $S \operatorname{wr} T$ é finitamente gerado se e só se as seguintes condições são satisfeitas:*

(i) $S^2 = S$ *e* $T^2 = T$*;*

(ii) S *é finitamente gerado.*

Se o S*-acto diagonal não é finitamente gerado então* $S \operatorname{wr} T$ *é finitamente gerado se e só se as seguintes condições são satisfeitas:*

(i) $S^2 = S$*;*

(ii) S *é finitamente gerado;*

(iii) *cada elemento de* T *está contido no ideal principal direito gerado por uma identidade direita.*

Vamos agora considerar a automaticidade do produto em coroa $S \operatorname{wr} T$ no caso em que T é finito. Note-se que no caso em que S também é finito, $S \operatorname{wr} T$ é finito e portanto é automático. Vamos considerar o caso em que S é infinito e o S-acto diagonal não é finitamente gerado.

Teorema 7.2 *Sejam* S *e* T *semigrupos que satisfazem as seguintes condições:*

(i) T *é finito;*

(ii) S *é automático;*

(iii) *o* S*-acto diagonal não é finitamente gerado;*

(iv) *o produto em coroa* $S \operatorname{wr} T$ *é finitamente gerado;*

então $S \operatorname{wr} T$ *é automático.*

Dem. Assumimos que T não é trivial e escrevemos $T = \{t_1, \ldots, t_m\}$ com $m > 1$. Utilizando a Proposição 7.1 sabemos que S é finitamente gerado e que $S^2 = S$. Assim, pela Proposição 6.2, concluímos que o produto directo $S^{|T|}$ é automático. Seja (F, K) uma estrutura automática com unicidade para $S^{|T|}$ com $F = \{f_1, \ldots, f_k\}$. Uma vez que $S^2 = S$, podemos utilizar o Teorema 4.6, e assumir que K não tem palavras de comprimento 1. Dado $t \in T$, usando novamente a Proposição 7.1, existe uma identidade direita $e \in T$ tal que $t = eq$ para algum $q \in T$. Assim podemos definir o conjunto gerador

$$Y = \{e_1, \ldots, e_m\} \cup \{q_1, \ldots, q_m\}$$

para T com $t_i = e_i q_i$ $(i = 1, \ldots, m)$ onde $e_1, \ldots, e_m$ representam identidades direitas em T (não necessariamente distintas). Definimos um novo alfabeto A por

$$A = \{(f, e_i) : f \in F, i = 1, \ldots, m\} \cup \{(f, q_i) : f \in F, i = 1, \ldots, m\}$$

e a linguagem L em A por

$$L = \bigcup_{i=1,\ldots,m} \{(f_{\alpha_1}, e_i) \ldots (f_{\alpha_{n-1}}, e_i)(f_{\alpha_n}, q_i) : f_{\alpha_1} \ldots f_{\alpha_n} \in K\}.$$

Vamos provar que o par (A, L) é uma estrutura automática para $S \operatorname{wr} T$ (com unicidade). Para ver que A gera $S \operatorname{wr} T$ e que L é um conjunto de formas normais com unicidade para $S \operatorname{wr} T$ basta observar que, dado $(f, t_i) \in S \operatorname{wr} T$ existe uma única palavra $f_{\alpha_1} \dots f_{\alpha_n}$ em K tal que $f = f_{\alpha_1} \dots f_{\alpha_n}$. Portanto existe uma só palavra em L que representa (f, t_i), que é a palavra

$$(f_{\alpha_1}, e_i) \dots (f_{\alpha_{n-1}}, e_i)(f_{\alpha_n}, q_i).$$

Para provar que L é uma linguagem regular definimos uma gsm $\mathcal{A}$ tal que $K\eta_{\mathcal{A}} = L$. Seja

$$\mathcal{A} = (Q, F, A, \mu, q_0, \{\chi\})$$

com $Q = \{q_0, \dots, q_m\} \cup \{\chi\}$, onde q_0 é o estado inicial, χ é o único estado terminal e μ é uma função parcial de $Q \times F$ para subconjuntos finitos de $Q \times A^+$ definida por:

$$\begin{aligned}
(q_0, f)\mu &= \{(q_i, (f, e_i))\} \ (i = 1, \dots, m), \\
(q_i, f)\mu &= \{(q_i, (f, e_i)), (\chi, (f, q_i)))\} \ (i = 1, \dots, m).
\end{aligned}$$

Vamos agora provar que $L_{(f,e_r)}$ é uma linguagem regular, para $(f, e_r) \in A$. Se definirmos

$$L^{(i)}_{(f,e_r)} = L_{(f,e_r)} \cap (A^+ \cdot \{(f, q_i) : f \in F\} \times A^+)\delta_A \ (i = 1, \dots, m)$$

podemos escrever

$$L_{(f,e_r)} = \bigcup_{i=1,\dots,m} L^{(i)}_{(f,e_r)}$$

e é suficiente provar que, para cada $i \in \{1, \dots, m\}$, a linguagem $L^{(i)}_{(f,e_r)}$ é regular. Para esse fim, vamos usar o Teorema 5.1, e começamos por mostrar que

$$L^{(i)}_{(f,e_r)} = K_{\bar{w}}\pi_F\zeta_{\mathcal{A}}\delta_A \cap (A^+ \cdot \{(f, q_i) : f \in F\} \times A^+ \cdot \{(f, q_i) : f \in F\})\delta_A$$

onde $\bar{w}$ é a palavra em K que representa ${}^{q_i}f \in S^{|T|}$. Seja

$$(f_{\alpha_1}, e_i) \dots (f_{\alpha_{n-1}}, e_i)(f_{\alpha_n}, q_i), (f_{\beta_1}, e_j) \dots (f_{\beta_{s-1}}, e_j)(f_{\beta_s}, q_j) \in L.$$

Então

$$\begin{aligned}
& ((f_{\alpha_1}, e_i) \dots (f_{\alpha_{n-1}}, e_i)(f_{\alpha_n}, q_i), (f_{\beta_1}, e_j) \dots (f_{\beta_{s-1}}, e_j)(f_{\beta_s}, q_j))\delta_A \in L^{(i)}_{(f,e_r)} \\
\Longleftrightarrow\ & f_{\alpha_1} \dots f_{\alpha_n}\, {}^{q_i}f = f_{\beta_1} \dots f_{\beta_s} \ \&\ e_i q_i e_r = e_j q_j \\
\Longleftrightarrow\ & f_{\alpha_1} \dots f_{\alpha_n}\, {}^{q_i}f = f_{\beta_1} \dots f_{\beta_s} \ \&\ e_i q_i = e_j q_j \\
\Longleftrightarrow\ & f_{\alpha_1} \dots f_{\alpha_n}\, {}^{q_i}f = f_{\beta_1} \dots f_{\beta_s} \ \&\ t_i = t_j \\
\Longleftrightarrow\ & (f_{\alpha_1} \dots f_{\alpha_n}, f_{\beta_1} \dots f_{\beta_s})\delta_F \in K_{\bar{w}} \ \&\ i = j \\
\Longleftrightarrow\ & ((f_{\alpha_1}, e_i) \dots (f_{\alpha_{n-1}}, e_i)(f_{\alpha_n}, q_i), (f_{\beta_1}, e_j) \dots (f_{\beta_{s-1}}, e_j)(f_{\beta_s}, q_j))\delta_A \in \\
& K_{\bar{w}}\pi_F\zeta_{\mathcal{A}}\delta_A \cap (A^+ \cdot \{(f, q_i) : f \in F\} \times A^+ \cdot \{(f, q_i) : f \in F\})\delta_A
\end{aligned}$$

Concluímos, pelo Teorema 5.1, que $L^{(i)}_{(f,e_r)}$ é uma linguagem regular. Para um gerador $(f, q_r) \in A$ vamos provar que $L_{(f,q_r)}$ é regular de modo semelhante. Podemos escrever

$$L_{(f,q_r)} = \bigcup_{i=1,\dots,m} L^{(i)}_{(f,q_r)}$$

onde

$$L^{(i)}_{(f,q_r)} = L_{(f,q_r)} \cap (A^+ \cdot \{(f,q_i) : f \in F\} \times A^+)\delta_A \ (i = 1,\dots,m).$$

Dado $i \in \{1,\dots,m\}$ arbitrário vamos provar que $L^{(i)}_{(f,q_r)}$ é uma linguagem regular. Seja j o único elemento em $\{1,\dots,m\}$ tal que $e_i q_i q_r = e_j q_j$ e seja $\bar{w}$ a palavra em K que representa ${}^{q_i}f \in S^{|T|}$. Sejam

$$(f_{\alpha_1}, e_i)\dots(f_{\alpha_{n-1}}, e_i)(f_{\alpha_n}, q_i), (f_{\beta_1}, e_k)\dots(f_{\beta_{s-1}}, e_k)(f_{\beta_s}, q_k) \in L.$$

Então

$$\begin{aligned}
& ((f_{\alpha_1}, e_i)\dots(f_{\alpha_{n-1}}, e_i)(f_{\alpha_n}, q_i), (f_{\beta_1}, e_k)\dots(f_{\beta_{s-1}}, e_k)(f_{\beta_s}, q_k))\delta_A \in L^{(i)}_{(f,q_r)} \\
\iff\ & f_{\alpha_1}\dots f_{\alpha_n}\, {}^{q_i}f = f_{\beta_1}\dots f_{\beta_s} \ \&\ e_i q_i q_r = e_k q_k \\
\iff\ & (f_{\alpha_1}\dots f_{\alpha_n}, f_{\beta_1}\dots f_{\beta_s})\delta_F \in K_{\bar{w}} \ \&\ e_i q_i q_r = e_k q_k \ \&\ k = j \\
\iff\ & ((f_{\alpha_1}, e_i)\dots(f_{\alpha_{n-1}}, e_i)(f_{\alpha_n}, q_i), (f_{\beta_1}, e_k)\dots(f_{\beta_{s-1}}, e_k)(f_{\beta_s}, q_k))\delta_A \in \\
& K_{\bar{w}}\pi_F\zeta_{\mathcal{A}}\delta_A \cap (A^+ \cdot \{(f,q_i) : f \in F\} \times A^+ \cdot \{(f,q_j) : f \in F\})\delta_A
\end{aligned}$$

Podemos então utilizar o Teorema 5.1 e concluir que, para cada i, a linguagem

$$L^{(i)}_{(f,q_r)} = K_{\bar{w}}\pi_F\zeta_{\mathcal{A}}\delta_A \cap (A^+ \cdot \{(f,q_i) : f \in F\} \times A^+ \cdot \{(f,q_j) : f \in F\})\delta_A$$

é regular. $\square$

No caso em que os semigrupos S e T são monóides, as condições necessárias e suficientes para o produto em coroa $S \operatorname{wr} T$ ser finitamente gerado, estabelecidas em [17], são as seguintes:

Proposição 7.3 *Sejam S e T monóides, e seja G o grupo das unidades de T. Então o produto em coroa $S \operatorname{wr} T$ é finitamente gerado se e só se S e T são ambos finitamente gerados, e ou S é trivial, ou $T = VG$ para algum subconjunto finito V de T.*

Utilizando este resultado, o nosso teorema tem a seguinte consequência:

Corolario 7.4 *Seja S um monóide automático e T um monóide finito. Então o produto em coroa $S \operatorname{wr} T$ é automático.*

Dem. Assumimos que S não é trivial. Podemos aplicar a Proposição 7.3, com $V = T$, e portanto $S \operatorname{wr} T$ é finitamente gerado. Além disso, as três condições na Proposição 7.1, para o caso em que o S-acto diagonal não é finitamente gerado, verificam-se trivialmente uma vez que S e T são monóides. A prova do nosso teorema é baseada nestas condições e portanto o produto em coroa $S \operatorname{wr} T$ é automático. $\square$

Continua a ser uma questão em aberto se o produto em coroa $S \operatorname{wr} T$ é automático sempre que é finitamente gerado. Claro que, devido ao resultado acima, falta apenas considerar o caso em que o S-acto diagonal é finitamente gerado. Em [17] e [19] podemos encontrar alguns exemplos de produtos em coroa com S-acto diagonal finitamente gerado os quais, como os autores observam, são de certa forma o caso menos comum. Outro problema interessante é o estudo da automaticidade do produto em coroa no caso em que o semigrupo T também é infinito. Um ponto de partida natural será utilizar a Proposição 7.3 e investigar o caso em que S e T são monóides.

Referências

[1] G. Baumslag, S. M. Gersten, M. Shapiro e H. Short, Automatic Groups and Amalgams, *J. Pure Appl. Algebra* **76** (1991) 229–316.

[2] S. Bulman-Fleming e K. McDowell, Solution: Problem E3311, *Amer. Math. Monthly*, **97** (1990) 617.

[3] C.M. Campbell, E.F. Robertson, N. Ruškuc e R.M. Thomas, Automatic semigroups, *Theoretical Computer Science* **250** (2001) 365–391.

[4] C.M. Campbell, E.F. Robertson, N. Ruškuc e R.M. Thomas, Direct products of automatic semigroups, *J. Austral. Math. Soc. Ser. A* **69** (2000) 19–24.

[5] J. W. Cannon, D. B. A. Epstein, D. F. Holt, S. V. F. Levy, M. S. Paterson e W. P. Thurston, *Word Processing in Groups* Jones and Bartlett Publishers, 1992.

[6] L. Descalço e N. Ruškuc, On automatic Rees matrix semigroups *Comm. Algebra* **30** (2002) 1207–1226.

[7] L. Descalço, *Automatic semigroups: constructions and subsemigroups*, Ph.D. Thesis, University of St Andrews, 2002.

[8] A. J. Duncan, E. F. Robertson e N. Ruškuc, Automatic monoids and change of generators, *Math. Proc. Cambridge Philos. Soc.* **127** (1999) 403–409.

[9] M. Hoffmann, N. Ruškuc e R.M. Thomas, Automatic semigroups with subsemigroups of finite Rees index, *Internat. J. Algebra Comput.* **12** (2002) 463–476.

[10] J.E. Hopcroft e J.D. Ullman, *Formal Languages and Their Relation to Automata*, Addison-Wesley, Reading MA, 1969.

[11] J.M. Howie, *Fundamentals of Semigroup Theory*, Oxford University Press, Oxford, 1991.

[12] J. M. Howie, *Automata and Languages*, Oxford University Press, 1991.

[13] F. Otto, On Dehn functions of finitely presented bi-automatic monoids, *J. Autom. Lang. Comb.* **5** (2000) 405–419.

[14] E. F. Robertson, N. Ruškuc e M. R. Thomson, On finite generation and other finiteness conditions for wreath products of semigroups, *Comm. Algebra* **30** (2002) 3851–3873.

[15] E. F. Robertson, N. Ruškuc e J. Wiegold, Generators and Relations of Direct Products of Semigroups, *Trans. Amer. Math. Soc.* **350** (1998) 2665–2685.

[16] E. F. Robertson, N. Ruškuc e M. R. Thomson, On Diagonal Acts of Monoids, *Bull. Austral. Math. Soc.* **63** (2001) 167–175.

[17] E.F. Robertson, N. Ruškuc e M.R. Thomson, Finite generation and presentability of wreath products of monoids, *J. Algebra* **266** (2003) 382–392.

[18] P. V. Silva e B. Steinberg, A Geometric Characterization of Automatic Monoids, Universidade do Porto, 2000.

[19] R. Thomson, *Finiteness Conditions of Wreath Products of Semigroups and Related Properties of Diagonal Acts*, Ph.D. Thesis, University of St Andrews, 2001.