O GRUPO PROFINITO DE UMA SUBSTITUIÇÃO PRIMITIVA

JORGE ALMEIDA

Resumo. Para um palavra bi-infinita, o fecho topológico da linguagem dos seus factores finitos no semigrupo profinito livre reflecte propriedades combinatórias e dinâmicas da palavra bi-infinita. Por exemplo, a palavra bi-infinita é uniformemente recorrente se e só se os elementos infinitos do referido fecho são regulares, $\mathcal{J}$-equivalentes e entre eles encontram-se todos os seus factores infinitos. Em particular, há um grupo profinito de estrutura associado à correspondente $\mathcal{J}$-classe, o qual é na realidade um invariante por conjugação do sistema dinâmico simbólico gerado pela palavra bi-infinita.

Um método simples para produzir palavras bi-infinitas consiste na iteração infinita de substituições primitivas. O objectivo último da investigação aqui relatada é o cálculo de grupos profinitos de estrutura associados a palavras bi-infinitas geradas por tais meios. Vários exemplos naturais, como as palavras bi-infinitas de Fibonacci, conduzem a grupos profinitos livres, mas nem sempre assim acontece. No entanto, sob condições bastante gerais, nomeadamente se a substituição induz um automorfismo do grupo livre, o grupo em causa é de facto um grupo profinito livre.

1. Introdução

Em dinâmica simbólica, considera-se sistemas que, em cada instante (sendo o tempo considerado discreto), se encontra em algum de um certo conjunto finito de estados possíveis. Um *historial* do sistema é uma sequência bi-infinita

$$\cdots x_{-n}x_{-n+1}\cdots x_{-1}x_0x_1\cdots x_{n-1}x_n\cdots$$

onde x_i representa o estado no instante i. Por translação da origem do tempo, obtemos uma acção do grupo aditivo dos inteiros $\mathbb{Z}$ no espaço $S^{\mathbb{Z}}$ de todos os historiais do sistema, visto como potência topológica do espaço discreto S, sendo a acção realizada por transformações contínuas.

Um *sistema dinâmico simbólico* é um subconjunto fechado de $S^{\mathbb{Z}}$ que seja estável para a translação da origem do tempo. A topologia de $S^{\mathbb{Z}}$ é determinada pela base formada pelos abertos que consistem em prescrever uma secção do historial num intervalo de tempo específico. Pela estabilidade para a acção do grupo $\mathbb{Z}$, é irrelevante onde se situe a origem, ou seja as condições topológicas traduzem-se combinatoriamente pela prescrição da presença de segmentos finitos nos nossos historiais. Em termos mais formais, mostra-se que um sistema dinâmico simbólico é completamente determinado pelo conjunto dos segmentos finitos dos seus historiais, ou seja por uma *linguagem* de palavras finitas. As linguagens que podem ocorrer deste modo são fáceis de identificar: são aquelas que (a) são fechadas para tomar factores e tais que (b) cada palavra na linguagem pode ser estendida à esquerda e à direita

a outras palavras na linguagem acrescentando letras. Ver [15, 9] para obras de introdução à dinâmica simbólica e [10] para um trabalho mais avançado versando especificamente sistemas dinâmicos simbólicos gerados por iteração de substituições.

A dinâmica simbólica pode portanto ser vista como um capítulo da teoria de linguagens sobre alfabetos finitos, ou seja do estudo combinatório dos subconjuntos do monóide livre A^* sobre um alfabeto finito A. No entanto, a estrutura algébrica disponível no monóide livre para a investigação de problemas combinatórios é muito pobre. Uma ideia que surgiu na teoria de semigrupos finitos consiste em considerar uma métrica natural sobre A^* e passar a trabalhar com o completado $\widehat{A^*}$. A aplicação desta ideia na relação com a dinâmica simbólica surgiu como subproduto de trabalhos do autor, em parte em colaboração com M. V. Volkov, procurando esclarecer aspectos estruturais do monóide profinito livre $\widehat{A^*}$ ou para obter certos resultados da teoria de semigrupos finitos [2, 1, 4, 5, 8].

Este trabalho é o texto desenvolvido, mas sem demonstração detalhada da maior parte dos resultados, correspondente a uma palestra realizada no âmbito do Encontro de Algebristas Portugueses realizado em Vila Real em Setembro de 2004. O leitor interessado poderá consultar as referências bibliográficas para as demonstrações dos resultados apresentados. Em geral, as provas dos resultados para os quais não são apresentadas referências podem ser encontradas no artigo [6], onde o tema deste texto é tratado em detalhe.

Este trabalho pretende ser uma breve introdução ao estudo das $\mathcal{J}$-classes maximais dos semigrupos profinitos livres e das suas relações com os sistemas dinâmicos simbólicos. Concentramo-nos especificamente na estrutura dos subgrupos maximais de tais $\mathcal{J}$-classes. Esboçamos uma demonstração de que, se a $\mathcal{J}$-classe contém a imagem de uma letra por uma substituição primitiva que induz um automorfismo do grupo livre, então os seus subgrupos maximais são grupos profinitos livres finitamente gerados.

2. Ingredientes básicos

Consideremos no monóide livre A^*, cujos membros são as palavras finitas sobre o alfabeto finito A, e cuja operação é simplesmente a concatenação de palavras, a métrica dada por

$$d(u,v) = \begin{cases} 2^{-r(u,v)} & \text{se } u \neq v \\ 0 & \text{caso contrário} \end{cases} \tag{1}$$

onde $r(u,v)$ é o menor cardinal $|M|$ de um monóide finito M para o qual existe algum homomorfismo $\varphi : A^* \to M$ tal que $\varphi(u) \neq \varphi(v)$. Trata-se de facto de uma *ultra-métrica* no sentido que, em relação às propriedades requeridas para uma métrica, a desigualdade triangular é reforçada na seguinte desigualdade:

$$d(u,w) \leq \max\{d(u,v), d(v,w)\}.$$

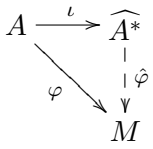
Além disso, a operação de concatenação é contractiva:

$$d(u_1v_1, u_2v_2) \leq \max\{d(u_1,u_2), d(v_1,v_2)\}$$

pelo que a operação de concatenação se estende de forma única a uma operação contínua no completado $\widehat{A^*}$ de A^* em relação à métrica d. Logo $\widehat{A^*}$

é um monóide topológico. Como há, a menos de isomorfismo, somente um número finito de monóides com um dado número N de elementos, existe algum homomorfismo uniformemente contínuo $\varphi_N : \widehat{A^*} \to S_N$ num monóide finito tal que $d(u,v) \leq 2^{-N}$ se e só se $\varphi_N(u) = \varphi_N(v)$. Assim, por um argumento de extracção sucessiva, podemos extrair de uma qualquer sucessão $(w_n)_n$ de $\widehat{A^*}$ uma subsucessão convergente.[1] Por outras palavras, o monóide $\widehat{A^*}$ é compacto. Ele também é zero-dimensional no sentido de admitir uma base da sua topologia formada por abertos fechados, nomeadamente os conjuntos da forma $\varphi_N^{-1}(s)$ com $s \in S_N$ e $N \geq 1$. Por outro lado, como as imagens recíprocas de subconjuntos de monóides finitos M por homomorfismos $\varphi : A^* \to M$ são precisamente as linguagens racionais, e todo o aberto fechado de um semigrupo profinito é união de classes abertas fechadas de um congruência de índice finito (Lema de Hunter [13]), concluímos que os abertos fechados de $\widehat{A^*}$ são precisamente os fechos topológicos das linguagens racionais de A^*.

Um monóide compacto zero-dimensional também se diz um *monóide profinito*. De forma equivalente, trata-se de um monóide compacto residualmente finito, ou ainda de um limite projectivo de monóides finitos [3]. O monóide $\widehat{A^*}$ diz-se o *monóide profinito livre sobre* A porque tem a seguinte propriedade universal para a função de inclusão $\iota : A \to \widehat{A^*}$: para toda a função $\varphi : A \to M$ num monóide profinito, existe um único homomorfismo contínuo $\hat{\varphi} : \widehat{A^*} \to M$ tal que o diagrama seguinte comuta



Esta propriedade decorre imediatamente da definição de $\widehat{A^*}$ no caso de M ser um monóide finito e daí segue para qualquer monóide profinito M pela propriedade deste de ser residualmente finito.

Num monóide finito, dado um elemento m, a sucessão $(m^{n!})_n$ converge (na topologia discreta) para o único idempotente que é uma potência de expoente positivo de m. Esse idempotente representa-se por m^ω. Logo, também em qualquer monóide profinito, dado um elemento m, a sucessão $(m^{n!})_n$ converge para um idempotente, o único que é limite de uma sucessão de potências de expoente positivo de m, e o qual novamente se representa por m^ω. Para um monóide profinito M, representamos por $\operatorname{End} M$ o monóide de endomorfismos contínuos de M.

Teorema 2.1 ([3])**.** *Se M é um monóide profinito finitamente gerado, então* $\operatorname{End} M$ *é ainda um monóide profinito para a topologia da convergência pontual, i.e., como subespaço de M^M. Além disso, a função de avaliação* $(\operatorname{End} M) \times M \to M$ *dada por* $(\varphi, m) \mapsto \varphi(m)$ *é contínua.*

[1] Digamos, começando na posição $n_1 = 1$ e, em cada passo N, retendo o elemento na posição actual e escolhendo uma subsucessão dos elementos que se lhe seguem que tenha valor constante sob φ_N, avançando para a posição n_{N+1} dada pelo índice do primeiro termo dessa subsucessão.

Em particular, dado $\varphi \in \operatorname{End} \widehat{A^*}$, podemos considerar o seu único *iterado infinito idempotente* $\varphi^\omega = \lim_{n\to\infty} \varphi^{n!}$. Sendo $\widehat{A^*}$ um monóide profinito livre sobre A, cada elemento φ de $\operatorname{End} \widehat{A^*}$ é completamente determinado pela sua restrição $\varphi|_A$ a A. Informalmente, $\varphi(w)$ obtém-se substituindo cada letra $a \in A$ por $\varphi(a)$ e "fazendo as contas" em $\widehat{A^*}$. Por isso diz-se simplesmente que φ é uma *substituição*. Uma substituição φ diz-se *finita* se $\varphi(A) \subseteq A^*$. Só consideraremos substituições finitas embora substituições mais gerais também desempenhem um papel importante na teoria [2, 1]. Seguindo a notação adoptada em [8], para simplificar a descrição de φ poderemos escrever $\varphi = [w_1, \ldots, w_n]$, no caso de $A = \{a_1, \ldots, a_n\}$ com uma ordem fixada para as letras, onde $w_i = \varphi(a_i)$ para $i = 1, \ldots, n$.

Uma substituição φ diz-se *primitiva* se existir n tal que, para qualquer par de letras $a, b \in A$, a ocorre em $\varphi^n(b)$. Uma substituição primitiva φ determina um sistema dinâmico simbólico $\mathcal{S}_\varphi$, cuja linguagem L de segmentos finitos consiste dos factores das palavras $\varphi^n(a)$ para n suficientemente grande e $a \in A$. Como, para n suficientemente grande, $\varphi^n(a)$ é factor de $\varphi^{n+1}(b)$ para quaisquer $a, b \in A$, e $\varphi^\omega(a) = \lim_{n\to\infty} \varphi^{n!}(a)$, o fecho da linguagem L em $\widehat{A^*}$ consiste precisamente dos factores (finitos ou *infinitos*) de $\varphi^\omega(a)$ para qualquer $a \in A$.

O resultado seguinte é essencialmente bem conhecido [20]. Uma demonstração na linguagem deste trabalho de um resultado mais geral pode ser encontrada em [6].

Proposição 2.2. *Para qualquer substituição primitiva φ, o sistema dinâmico simbólico associado $\mathcal{S}_\varphi$ é minimal, i.e., não contém estritamente nenhum outro sistema.*

Eis alguns exemplos clássicos sobre o alfabeto $A = \{a, b\}$.

Exemplo 2.3. Seja $\varphi = [ab, ba]$. O sistema dinâmico simbólico $\mathcal{S}_\varphi$ foi introduzido por Hedlund e Morse em 1938 [12] como forma de descrever uma geodésica *recorrente* não periódica numa superfície simplesmente conexa de curvatura constante negativa.[2] A forma de descrever uma tal geodésica consistiu na sua codificação através da sequência de intersecções com determinadas curvas. Este trabalho constituiu a fundação da dinâmica simbólica, sendo precisamente esse o seu título. A sequência

$$abbabaabbaababbabaababbaabbabaabbaababbaabbabaababbabaabbaab\ldots,$$

cujos prefixos são os de $\varphi^n(a)$ para n suficientemente grande, tinha já anteriormente sido considerada por Prouhet [19] e Thue [23] em trabalhos de natureza combinatória. Uma sua propriedade importante é que não possui segmentos da forma u^3, o que permite, por codificação, obter um sistema em três letras que não possui segmentos da forma u^2. Daqui segue que o semigrupo de Burnside em pelo menos três geradores definido pela lei $x^3 = x^2$ é infinito. Ver [16] para mais detalhes.

[2] A recorrência de uma geodésica g significa que, para todo o $\epsilon > 0$, existe $\ell \in \mathbb{R}$ tal que, para todo o segmento s de g de comprimento pelo menos ℓ, qualquer ponto de g está a distância no máximo ϵ de algum ponto de s.

Exemplo 2.4. Seja $\varphi = [ab, a]$. A sucessão dos comprimentos das palavras $\varphi^n(b)$ $(n \geq 0)$

$$b, a, ab, aba, abaab, abaababa, abaababaabaab, abaababaabaababaababa, \ldots$$

é precisamente a sucessão de (números de) Fibonacci, pelo que $\mathcal{S}_\varphi$ se diz o *sistema de Fibonacci*. Trata-se do exemplo mais simples de um sistema dinâmico simbólico não periódico gerado por substituições. Possui várias propriedades notáveis. Por exemplo, entre dois quaisquer factores do mesmo comprimento, a diferença dos números de ocorrências de uma letra não excede 1 e, para cada comprimento, há precisamente um factor u desse comprimento tal que ua e ub também são factores. Daqui decorre que o número de factores de comprimento n é $q(n) = n+1$, precisamente o número mínimo para que o sistema não seja periódico [12]. Sistemas dinâmicos simbólicos cuja *função de complexidade* $q(n)$ possui esta propriedade dizem-se *Sturmianos* e têm sido objecto de numerosos estudos, cf. [17, Capítulo 2], [10, Capítulo 6]. Eles também são conhecidos como "rectas discretizadas" pois, grosso modo, descrevem as instersecções com a quadrícula $\mathbb{Z} \times \mathbb{R} \cup \mathbb{R} \times \mathbb{Z}$ de rectas ℓ no plano Euclidiano $\mathbb{R}^2$ de declive irracional, onde a e b codificam respectivamente intersecções com rectas horizontais ou verticais, rectas estas ℓ que podem ser vistas como geodésicas não periódicas no toro $\mathbb{R}^2/\mathbb{Z}^2$.

Um sistema dinâmico simbólico minimal é, como consequência imediata da definição, o fecho da órbita de qualquer dos seus pontos para a acção de $\mathbb{Z}$ por translações, uma vez que esse fecho é ele próprio um sistema dinâmico simbólico. Uma caracterização alternativa é dada pela *recorrência uniforme*, que se exprime em termos da linguagem dos segmentos finitos como segue: todo o segmento finito ocorre como segmento de todo o segmento finito suficientemente longo. Analogamente, diremos que um elemento de $\widehat{A^*}$ é *uniformemente recorrente* se todo o seu factor finito for factor de todo o seu factor finito suficientemente longo. O seguinte resultado é essencialmente uma reformulação da Proposição 2.2.

Proposição 2.5. *Se φ é uma substituição primitiva finita, então todo o $\varphi^\omega(a)$ $(a \in A)$ é uniformemente recorrente.*

Um elemento s de um semigrupo S diz-se *regular* se existir algum $t \in S$ tal que $sts = s$.

Para poder dispor da linguagem clássica da teoria de semigrupos, passamos a relembrar as relações de Green. Chamamos *prefixo* de um elemento u de um monóide um seu factor esquerdo, isto é v tal que $u = vw$ para algum w. Um *sufixo* é definido dualmente. Dados dois elementos u e v de um monóide M, escrevemos

- $u \leq_{\mathcal{J}} v$ se v é factor de u;
- $u \leq_{\mathcal{R}} v$ se v é um prefixo de u;
- $u \leq_{\mathcal{L}} v$ se v é um sufixo de u.

Trata-se de três relações de quasi-ordem sobre M. Dois elementos u, v são equivalentes para a relação de equivalência associada a uma quasi-ordem $\leq$ se $u \leq v$ e $v \leq u$. A relação de equivalência associada a uma quasi-ordem de Green $\leq_{\mathcal{K}}$ denota-se por $\mathcal{K}$. Adicionalmente, considera-se a relação de equivalência $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$.

Eis alguns factos sobre as relações de Green. Num monóide compacto,

(1) todos os elementos de uma $\mathcal{J}$-classe J são regulares se e só se J contiver algum idempotente; neste caso, todos os subgrupos maximais contidos em J são grupos compactos isomorfos;
(2) toda a $\mathcal{J}$-classe é união de $\mathcal{R}$-classes e união de $\mathcal{L}$-classes, sendo não vazia a intersecção de cada $\mathcal{R}$-classe com cada $\mathcal{L}$-classe;
(3) as $\mathcal{H}$-classes que contêm idempotentes são os subgrupos maximais;
(4) se $u \mathcal{J} v$ e $u \leq_{\mathcal{R}} v$, então $u \mathcal{R} v$, e analogamente para $\mathcal{L}$.

O leitor interessado poderá encontrar em qualquer livro clássico sobre teoria de semigrupos, por exemplo em [14], a demonstração destes resultados no contexto dos semigrupos discretos. Algumas das propriedades mais restritivas, respeitantes a semigrupos compactos, são válidas mais geralmente nos chamados *semigrupos estáveis*.

Munidos desta linguagem, podemos passar a apresentar alguns resultados básicos sobre as $\mathcal{J}$-classes de palavras profinitas uniformemente recorrentes.

Teorema 2.6. *Seja w uma palavra profinita infinita. Então w é uniformemente recorrente se e só se w é $\leq_{\mathcal{J}}$-maximal como palavra profinita infinita.*

Assim sendo, na ordem $\leq_{\mathcal{J}}$ de $\widehat{A^*}$ encontramos, no topo, uma parte formada por $\mathcal{J}$-classes singulares, constituídas pelos elementos de A^*, pois é fácil mostrar que os factores destes são necessariamente finitos. Imediatamente abaixo situa-se uma "faixa" de $\mathcal{J}$-classes formadas precisamente pelas palavras profinitas uniformemente recorrentes. A não ser no caso especial do alfabeto com uma só letra, para baixo desta faixa ficam ainda muitas $\mathcal{J}$-classes. Delas, pouco se conhece, a não ser daquela que fica no fundo da ordem, a $\mathcal{J}$-classe que coincide com o ideal mínimo de $\widehat{A^*}$ [22, 21, 7].

Eis algumas outras propriedades das $\mathcal{J}$-classes das palavras uniformemente recorrentes.

Proposição 2.7. *(1) A $\mathcal{J}$-classe de uma palavra profinita uniformemente recorrente é completamente determinada pelos seus factores finitos e também pelos seus prefixos finitos, e ainda pelos seus sufixos finitos.*
(2) Toda a palavra profinita uniformemente recorrente w é $\mathcal{H}$-equivalente a algum limite de uma sucessão de factores finitos de w.
(3) A $\mathcal{J}$-classe de uma palavra profinita uniformemente recorrente é regular.

Logo, a uma tal $\mathcal{J}$-classe está associado um grupo profinito, a saber qualquer dos subgrupos maximais dessa $\mathcal{J}$-classe, que já observámos serem todos isomorfos.

O correspondente natural em $\widehat{A^*}$ à linguagem L de um sistema dinâmico simbólico é simplesmente o seu fecho topológico $\overline{L}$. Na passagem a $\overline{L}$ não há perda de informação: u é um factor finito de $v = \lim_{n\to\infty} v_n$, com $v_n \in L$; a linguagem A^*uA^*, das palavras que têm u como factor, é racional, pelo que o seu fecho $\widehat{A^*}\, u\, \widehat{A^*}$, formado pelas palavras profinitas que têm u como factor, é um aberto; logo u é factor de v_n para n suficientemente grande; como L é fechado para tomar factores, resulta que $u \in L$.

Nesta passagem, é agora fácil identificar os sistemas dinâmicos simbólicos minimais através do seguinte resultado.

Proposição 2.8. *Seja $X \subseteq A^{\mathbb{Z}}$ um sistema dinâmico simbólico e seja L a linguagem dos seus segmentos finitos. Então X é minimal se e só se os elementos infinitos de $\overline{L}$ são $\mathcal{J}$-equivalentes (e, portanto, $\leq_{\mathcal{J}}$-maximais como palavras profinitas infinitas).*

Logo todo o sistema dinâmico simbólico minimal X tem um grupo profinito natural associado, nomeadamente "o" grupo da $\mathcal{J}$-classe dos limites infinitos das sucessões dos segmentos finitos de X. Como caso particular de um resultado muito mais geral obtido recentemente por Alfredo Costa, segue que este grupo é um *invariante topológico* do sistema X, ou seja é *invariante por conjugação*. Uma *conjugação* de um sistema dinâmico simbólico $X \subseteq A^{\mathbb{Z}}$ noutro sistema $Y \subseteq B^{\mathbb{Z}}$ é um homeomorfismo $\varphi : X \to Y$ tal que o seguinte diagrama comuta:

$$\begin{array}{ccc} X & \xrightarrow{\sigma_A} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow{\sigma_B} & Y \end{array}$$

onde σ_A e σ_B designam as translações de origem, repectivamente em $A^{\mathbb{Z}}$ e $B^{\mathbb{Z}}$.

3. De volta às substituições

Em particular, a toda a substituição primitiva φ está naturalmente associado um grupo profinito G_φ, o qual é um invariante para conjugação topológica do sistema dinâmico simbólico $\mathcal{S}_\varphi$.

Problema 3.1. Calcular estes grupos.

O objectivo destas notas é apresentar alguns resultados parciais para a resolução deste problema que mostram que há situações relativamente gerais em que estes grupos são grupos profinitos livres. Dizemos que uma substituição finita φ é *grupo-invertível* se φ induz um automorfismo do grupo livre FG_A. O resultado principal é o seguinte.

Teorema 3.2. *Seja φ uma substituição primitiva sobre um alfabeto finito que é grupo-invertível. Então G_φ é um grupo profinito livre finitamente gerado.*

Podemos ser mais precisos quanto ao número de geradores livres de G_φ e podemos mesmo calculá-lo. A descrição deste cálculo segue da apresentação que se segue dos ingredientes essenciais para a demonstração do teorema.

Começamos por ver como a recorrência uniforme se comporta para substituições. Dizemos que uma substituição φ *apaga* uma letra a se $\varphi(a) = 1$.

Teorema 3.3. *Se a substituição φ não apaga todas as letras e w é uniformemente recorrente, então $\varphi(w)$ também o é.*

Seja φ uma substituição finita sobre um alfabeto finito e seja $w \in \widehat{A^*}$. Uma igualdade $x_1 \cdots x_m = y_1 \cdots y_n$ diz-se *redutível* se existirem índices i e j tais que $x_1 \cdots x_i = y_1 \cdots y_j$ e $2 \leq i + j < m + n$. Dizemos que φ tem *atraso*

limitado em relação a w se existir um inteiro N tal que seja redutível toda a igualdade de factores de w de uma das formas

$$uc_1 \cdots c_m v = c'_1 \cdots c'_n$$
$$uc_1 \cdots c_m = c'_1 \cdots c'_n v$$

com os $c_i, c'_j \in \varphi(A)$, $u, v \in A^*$ tais que $A^*u \cap \varphi(A^*) \neq \emptyset$ e $vA^* \cap \varphi(A^*) \neq \emptyset$, e $m + n > N$. Dizemos que φ é uma *codificação* se φ é um endomorfismo injectivo de $\widehat{A^*}$. Sendo φ uma substituição finita, segue de [18] que φ é uma codificação neste sentido se e só se $\varphi|_{A^*}$ for uma codificação no sentido clássico, isto é se $\varphi|_{A^*}$ for injectiva.

Teorema 3.4. *Se $\varphi(w)$ é uniformemente recorrente e φ é uma codificação de atraso limitado em relação a $\varphi(w)$, então w também é uniformemente recorrente.*

Daqui por diante, assumimos que φ é uma substituição finita primitiva sobre A. Notamos que, se ba é um factor de comprimento 2 (dos elementos) de J_φ, então todas as palavras profinitas da forma $\varphi^\omega(u)$, com u um factor finito de J_φ que começa com a letra a e termina com a letra b, são $\mathcal{H}$-equivalentes e pertencem a um subgrupo maximal de $\widehat{A^*}$ contido em J_φ. A razão essencial que justifica esta afirmação reside na observação de que, como φ^ω é um homomorfismo e a imagem de cada letra é uma palavra profinita infinita, os factores finitos de $\varphi^\omega(u)$ são factores de $\varphi^\omega(v)$ para algum factor v de u de comprimento 2. Se tomarmos para a a primeira letra dos elementos de H e para b a última letra desses elementos, chamamos a ba uma *conexão* para φ. As conexões estão em bijecção com os subgrupos maximais de J_φ que contêm elementos da imagem de φ^ω.

Dadas duas letras $a, b \in A$ tais que ba é um factor de J_φ, seja $X_\varphi(a, b)$ o conjunto das palavras finitas u tais que:

- bua é factor de J_φ;
- u começa com a;
- u termina com b;
- u não contém ba como factor.

Uma vez que os elementos de J_φ são uniformemente recorrentes, todo o factor suficientemente longo de $\varphi^\omega(a)$ contém ba como factor e, portanto, $X_\varphi(a, b)$ é um conjunto finito.

Proposição 3.5. *Seja ba uma conexão para φ e seja H o subgrupo maximal que contém $\varphi^\omega(X_\varphi(a, b))$. Então $\varphi^\omega(H)$ é gerado, como subgrupo fechado, pelo conjunto $\varphi^\omega(X_\varphi(a, b))$.*

Mas, o que nos interessa é calcular o subgrupo maximal H. Para começar, note-se que, por construção, como $\varphi^\omega(X_\varphi(a, b)) \subseteq H$, também $\varphi^\omega(H) \subseteq H$. Logo $\varphi^\omega(H)$ é um subgrupo fechado de H, sendo portanto ele próprio também um grupo profinito. Na hipótese de que φ induz um automorfismo do grupo livre, os dois grupos coincidem. Mais geralmente, temos o seguinte resultado cuja demonstração, tecnicamente delicada, consiste em usar a hipótese do atraso limitado para descodificar sucessivamente elementos de uma $\mathcal{H}$-classe que contenha elementos de $\operatorname{Im} \varphi^\omega$.

Proposição 3.6. *Seja φ uma substituição primitiva que é uma codificação de atraso limitado. Se $w \in J_\varphi$ pertence à mesma $\mathcal{H}$-classe que algum elemento de $\operatorname{Im}\varphi^\omega$ então $w \in \operatorname{Im}\varphi^\omega$.*

Por outras palavras, se H é uma $\mathcal{H}$-classe de J_φ tal que $H \cap \varphi^\omega(H) \neq \emptyset$, então $H = \varphi^\omega(H)$. Como corolário, obtemos o seguinte resultado.

Corolário 3.7. *Seja φ uma substituição primitiva que é uma codificação de atraso limitado. Se ba é uma conexão para φ, então $\varphi^\omega(X_\varphi(a,b))$ gera, como grupo profinito, um subgrupo maximal de J_φ.*

Para já, temos identificados geradores de certos subgrupos maximais de J_φ. Mas isso não é suficiente para identificar a estrutura de tais grupos. Para o fazer, começamos por considerar o grupo profinito livre $\widehat{FG_A}$ sobre o conjunto gerador livre A. Ele é obtido por completamento do monóide livre em relação à métrica d definida pela fórmula (1) mas onde agora $r(u,v)$ é definida considerando somente homomorfismos $A^* \to G$ em grupos finitos. Novamente, trata-se de um monóide profinito e efectivamente possui a propriedade universal análoga à de $\widehat{A^*}$, mas agora para grupos profinitos. Sendo bem conhecido que o grupo livre FG_A é residualmente finito, segue que o subgrupo de $\widehat{FG_A}$ gerado por A é efectivamente isomorfo a FG_A, o que justifica a notação.[3]

Enviando o gerador $a \in A$ em si próprio, obtemos uma projecção natural $p : \widehat{A^*} \to \widehat{FG_A}$. A substituição φ induz um endomorfismo de FG_A e um endomorfismo contínuo de $\widehat{FG_A}$ enviando $a \in A$ em $p(\varphi(a))$. Recorde-se que φ é *grupo-invertível* se φ induz um automorfismo de FG_A. De forma equivalente, $\varphi(A)$ gera o grupo FG_A, ou ainda um subgrupo denso do completado $\widehat{FG_A}$, ou ainda φ induz um automorfismo contínuo do grupo profinito livre $\widehat{FG_A}$.

Daqui por diante, seja φ uma substituição primitiva grupo-invertível.

Proposição 3.8. *O endomorfismo de $\widehat{FG_A}$ induzido por φ^ω é a função identidade.*

Dizemos que $X \subseteq A^+$ é um *código circular* se X é um conjunto gerador minimal de X^* e a condição $uv, vu \in X^*$ com $u, v \in A^+$ implica $u, v \in X^*$. Mostra-se que todo o código circular tem atraso finito em relação a qualquer palavra profinita. Assim, a condição de atraso limitado requerida para poder aplicar o processo de descodificação sucessiva da Proposição 3.6 fica garantido pelo resultado seguinte.

Proposição 3.9. *O conjunto $\varphi(A)$ é um código circular.*

Os passos finais para a demonstração do Teorema 3.2 podem agora ser esboçados. Seja ba uma conexão para φ e seja H o subgrupo maximal gerado por $\varphi^\omega(X_\varphi(a,b))$. A Proposição 3.8 implica que a imagem de H pela projecção $p : \widehat{A^*} \to \widehat{FG_A}$ é um subgrupo fechado gerado por $X_\varphi(a,b)$. Ora, $X_\varphi(a,b)$ é um conjunto finito de palavras finitas e, portanto está contido em FG_A. Logo, pelo Teorema de Nielsen-Schreier ele gera um subgrupo livre

[3]Em alternativa, $\widehat{FG_A}$ poderia ser definido directamente por completamento de FG_A em relação à métrica definida pelas mesmas fórmulas.

K de FG_A. Mais precisamente, podemos calcular uma base de H reduzindo sucessivamente $X_\varphi(a,b)$ pela aplicação das seguintes regras:

(1) se o conjunto contiver um par de palavras distintas da forma x, xy, substituir xy por y;
(2) se o conjunto contiver um par de palavras distintas da forma x, yx, substituir yx por y.

Ao cabo de um número finito de etapas, obtemos um conjunto ao qual não é possível aplicar nenhuma destas regras, precisamente o código biprefixo que gera o mais pequeno submonóide de A^* que contém $X_\varphi(a,b)$. É fácil ver que este código gera livremente o subgrupo K.

Neste ponto, invocamos um resultado recente que garante que o fecho topológico $\overline{K}$ em $\widehat{A^*}$ de um sugrupo K do grupo livre FG_A é um grupo profinito livre sobre os mesmos geradores livres que K [11]. Resta portanto mostrar que a restrição de p a H é injectiva, para o que é suficiente observar que as operações (1) e (2) podem ser realizadas dentro de qualquer grupo H, não alterando o subgrupo gerado pelo conjunto a que são aplicadas.

Finalmente, convém observar que é possível calcular efectivamente o conjunto de geradores livres de H.

Proposição 3.10. *Dada uma substituição φ sobre um alfabeto finito, existem algoritmos para realizar cada uma das seguintes tarefas:*

(1) determinar se a substituição é primitiva;
(2) no caso de φ ser primitiva, determinar as suas conexões;
(3) sendo φ primitiva e ba uma sua conexão, identificar o conjunto $X_\varphi(a,b)$.

4. Casos particulares

Nesta secção, apresentamos alguns casos concretos de aplicação do Teorema 3.2.

Teorema 4.1 ([8])**.** *Seja φ uma substituição primitiva grupo-invertível sobre um alfabeto finito A e suponhamos que existe n tal que a primeira letra de $\varphi^n(a)$ é independente de $a \in A$, e analogamente para a última letra. Então os elementos $\varphi^\omega(a)$ $(a \in A)$ são geradores livres de um subgrupo profinito de J_φ.*

De facto, neste caso os próprios $\varphi^\omega(a)$ $(a \in A)$ geram um subgrupo maximal, pelo que se trata realmente de um caso particular do resultado mais geral.

Um segmento u de um sistema dinâmico simbólico diz-se *especial à direita de grau d* se existirem exactamente d letras distintas a tais que ua ainda é um segmento; a palavra u diz-se um *segmento especial* se for um segmento especial de algum grau $d \geq 2$. Segmentos especiais à esquerda são definidos de forma dual. Um sistema dinâmico simbólico em duas letras possui exactamente um *segmento especial à esquerda* e um *segmento especial à direita*, de cada comprimento finito, ambos de grau 2, se e só se ele for Sturmiano (cf. Exemplo 2.4).

Teorema 4.2. *O grupo profinito associado a um sistema dinâmico simbólico Sturmiano gerado por substituições é um grupo profinito livre em 2 geradores livres.*

Para a demonstração, pode-se mostrar, mais precisamente, que há uma conexão ba tal que, sendo A um alfabeto com duas letras, $X_\varphi(a,b)$ gera o grupo livre FG_A.

Mais geralmente, um sistema dinâmico simbólico em n letras é *de Arnoux-Rauzy* se possuir exactamente um *factor especial à esquerda* e um *factor especial à direita*, de cada comprimento finito, ambos de grau n.

Teorema 4.3. *O grupo profinito associado a um sistema dinâmico simbólico de Arnoux-Rauzy em n letras gerado por substituições é um grupo profinito livre em n geradores livres.*

Aqui, mostra-se que há uma conexão ba tal que $X_\varphi(a,b)$ gera o grupo livre FG_A, onde A é um alfabeto com n letras.

O resultado seguinte foi anunciado em [5], onde também é esboçada uma sua demonstração a qual consiste em reduzir ao caso dos sistemas gerados por substituições aplicando um argumento tipo Ramsey.

Teorema 4.4. *Mais geralmente, os dois teoremas acima valem sem as hipóteses dos sistemas dinâmicos simbólicos serem gerados por substituições.*

Para concluir apresentamos dois exemplos de [6]. No primeiro, calculamos geradores concretos para um subgrupo maximal aplicando o processo descrito para a demonstração do Teorema 3.2. A correcção dos cálculos segue da validade dos algoritmos referidos na Proposição 3.10, que são aplicados em tais cálculos. No segundo exemplo, em que a substituição não é grupo-invertível, o grupo profinito associado não é um grupo profinito livre e mostra como alguns dos resultados da Secção 3 podem ainda ser usados em situações mais gerais.

Exemplo 4.5. Seja $A = \{a,b,c\}$ e seja $\varphi = [bcac, bcacbc, cbcbcac]$. Note-se que φ é uma substituição primitiva grupo-invertível. A palavra cb é uma conexão para φ e $X_\varphi(b,c) = \{bc, bcc, bcac, bcacc\}$. O código biprefixo que gera o mais pequeno submonóide de A^* contendo $X_\varphi(b,c)$ é precisamente A. Logo o subgrupo maximal contendo $\varphi^\omega(bc)$ é um grupo profinito livre gerado pelas seguintes palavras profinitas:

$$\Big\{\varphi^\omega\Big(\big((bc)^\omega c\big)^{\omega-1}\cdot\Big(bc\big((bc)^\omega c\big)^{\omega-1}\Big)^{\omega-1}\cdot bcac\cdot\big((bc)^\omega c\big)^{\omega-1}\Big),$$
$$\varphi^\omega\Big(bc\cdot((bc)^\omega c)^{\omega-1}\Big),\ \varphi^\omega\big((bc)^{\omega-1}\cdot bcc\big)\Big\}.$$

Exemplo 4.6. Seja $A = \{a,b\}$ e seja $\varphi = [ab, a^3b]$. Aqui φ é uma substituição primitiva mas não é grupo-invertível. Como a imagem de qualquer palavra começa por a e acaba com b, todos os elementos da forma $\varphi^\omega(u)$, com u factor de J_φ, pertencem à mesma $\mathcal{H}$-classe H, a qual é um subgrupo maximal. A única conexão para φ é ba, sendo $X_\varphi(a,b) = \{ab, a^3b\}$. Acontece que φ é uma codificação de atraso limitado. Logo, pelas Proposições 3.6 e 3.5, H é o subgrupo fechado gerado por $S = \{\varphi^\omega(ab), \varphi^\omega(a^3b)\}$. Logo H

também é o subgrupo fechado gerado por $T = \{\varphi^\omega(a), \varphi^\omega(b)\}$. Porque ambas as palavras ab e a^3b têm comprimento par, se H fosse um grupo profinito livre em dois geradores, sê-lo-ia nos dois conjuntos de geradores S e T, o que conduziria ao absurdo de ser possível encontrar um homomorfismo contínuo $H \to \mathbb{Z}/2\mathbb{Z}$, não constante, que envia o elementos de S no elemento neutro. Resta mostrar que H não é um grupo profinito livre num gerador, para o que basta encontrar um homomorfismo contínuo de domínio H, que é facilmente construído como restrição de um homomorfismo contínuo definido em $\widehat{A^*}$, que tenha por imagem um grupo finito não cíclico.

Referências

[1] J. Almeida, *Dynamics of finite semigroups*, in Semigroups, Algorithms, Automata and Languages, G. M. S. Gomes, J.-E. Pin, and P. V. Silva, eds., Singapore, 2002, World Scientific, 269–292.

[2] ————, *Dynamics of implicit operations and tameness of pseudovarieties of groups*, Trans. Amer. Math. Soc. **354** (2002) 387–411.

[3] ————, *Profinite semigroups and applications*, Tech. Rep. CMUP 2003-33, Univ. Porto, 2003. Aguarda publicação nas notas de lições da Escola SMS-NATO ASI 2003 sobre *Théorie structurale des automates, demi-groupes et algèbre universelle*, Montréal, 6 a 17/7.

[4] ————, *Profinite structures and dynamics*, CIM Bulletin **14** (2003) 8–18.

[5] ————, *Symbolic dynamics in free profinite semigroups*, no. 1366 in RIMS Kokyuroku, Kyoto, Japan, April 2004, 1–12.

[6] ————, *Profinite groups associated with weakly primitive substitutions*. Submetido para publicação. Disponível em http://www.fc.up.pt/cmup/jalmeida.

[7] J. Almeida and M. V. Volkov, *Profinite identities for finite semigroups whose subgroups belong to a given pseudovariety*, J. Algebra Appl. **2** (2003) 137–163.

[8] ————, *Subword complexity of profinite words and subgroups of free profinite semigroups*, Int. J. Algebra Comput. (2004). Aguarda publicação.

[9] M.-P. Béal, *Codage Symbolique*, Masson, Paris, 1993.

[10] V. Berthé, S. Ferenczi, C. Mauduit, and A. Siegel (Eds.), *Substitutions in Dynamics, Arithmetics and Combinatorics*, 2001. http://iml.univ-mrs.fr/editions/preprint00/book/prebookdac.html.

[11] T. Coulbois, M. Sapir, and P. Weil, *A note on the continuous extensions of injective morphisms between free groups to relatively free profinite groups*, Pub. Mat. **47** (2003) 477–487.

[12] G. A. Hedlund and M. Morse, *Symbolic dynamics*, Amer. J. Math. **60** (1938) 815–866.

[13] R. P. Hunter, *Certain finitely generated compact zero-dimensional semigroups*, J. Austral. Math. Soc., Ser. A **44** (1988) 265–270.

[14] G. Lallement, *Semigroups and Combinatorial Applications*, Wiley, New York, 1979.

[15] D. Lind and B. Marcus, *An introduction to symbolic dynamics and coding*, Cambridge University Press, Cambridge, 1996.

[16] M. Lothaire, *Combinatorics on Words*, Addison-Wesley, Reading, Mass., 1983.

[17] ————, *Algebraic Combinatorics on Words*, Cambridge University Press, Cambridge, UK, 2002.

[18] S. Margolis, M. Sapir, and P. Weil, *Irreducibility of certain pseudovarieties*, Comm. Algebra **26** (1998) 779–792.

[19] E. Prouhet, *Mémoire sur quelques relations entre les puissances des nombres*, C. R. Acad. Sci. Paris **33** (1851) 31.

[20] M. Queffélec, *Substitution Dynamical Systems—Spectral Analysis*, vol. 1294 of Lect. Notes in Math., Springer-Verlag, Berlin, 1987.

[21] N. R. Reilly and S. Zhang, *Decomposition of the lattice of pseudovarieties of finite semigroups induced by bands*, Algebra Universalis **44** (2000) 217–239.

[22] J. Rhodes and B. Steinberg, *Profinite semigroups, varieties, expansions and the structure of relatively free profinite semigroups*, Int. J. Algebra Comput. **11** (2002) 627–672.

[23] A. Thue, *Über unendlichen Zeichenreihen*, Kra. Vidensk. Selsk. Skrifter, I. Mat. Nat. Kl. (1906) 1–22.

Centro de Matemática, Departamento de Matemática Pura, Faculdade de Ciências, Universidade do Porto, Rua do Campo Alegre, 687, 4169-007 Porto, Portugal.

URL: `http://www.fc.up.pt/cmup/jalmeida`