

Ana Isabel Pereira de Moura

Equações no monóide livre e no grupo livre



Departamento de Matemática Pura
Faculdade de Ciências da Universidade do Porto
Junho / 2003

Ana Isabel Pereira de Moura

Equações no monóide livre e no grupo livre



*Tese submetida à Faculdade de Ciências da Universidade do Porto
para obtenção do grau de Mestre em Matemática - Fundamentos e Aplicações*

Departamento de Matemática Pura
Faculdade de Ciências da Universidade do Porto
Junho / 2003

Resumo

Dado um sistema de equações envolvendo somente operações de monóide, pretende-se determinar se ele possui alguma solução num dado monóide livre finitamente gerado. O mesmo problema é colocado para grupos livres finitamente gerados.

A decidibilidade dos sistemas de equações no monóide livre é aqui demonstrada com a descrição da generalização de Schulz do famoso Algoritmo de Makanin, que intervém com restrições racionais nas variáveis do sistema.

Quanto ao problema de decidibilidade de sistemas de equações no grupo livre, apresentamos alguns exemplos para os quais foi possível obter conclusões por métodos elementares de combinatória e/ou Teoria de Grupos. Abordamos ainda uma proposta de solução, alternativa ao Algoritmo de Makanin para equações no grupo livre, obtida por Sabbagh, mas que não funciona em geral. Refutamos esta proposta apresentando um exemplo de equações para as quais a proposta não funciona.

Abstract

Given an equation system involving only monoid operations, one seeks to determine if it has any solution in a given finitely generated free monoid. The analogous problem is also considered for finitely generated free groups.

The decidability of the equation systems in a free monoid is established here with the description of Schulz's generalization of the famous algorithm due to Makanin, which further takes into account rational constraints in the variables of the system.

Concerning the decidability problem for equation systems in a free group, we include some examples for which it was possible to find some conclusions which have been solved by elementary combinatorial and/or group theory methods. We also present a proposal of an alternative to Makanin's Algorithm for equations in a free group, due to Sabbagh, but which does not work in general. We refute this proposal by means of an example of equations for which the proposal fails.

Résumé

Etant donné un système d'équations qui se rapporte seulement à des opérations de monoïde, on cherche à déterminer s'il admet une solution dans un certain monoïde libre finiment engendré. On pose le même problème pour les groupes libres finiment engendrés.

La décidabilité des systèmes d'équations dans le monoïde libre est prouvée dans ce travail avec la description de la généralisation de Schulz du fameux Algorithme de Makanin, qui en plus fait intervenir des contraintes sur les variables du système.

En ce qui concerne la décidabilité des systèmes d'équations dans le groupe libre, nous présentons quelques exemples qu'on sait résoudre par des méthodes élémentaires, soit combinatoires et/ou de théorie des groupes. Nous faisons encore référence à une proposition de solution, en alternative à l'Algorithme de Makanin pour des équations dans le groupe libre, suggérée par Sabbagh, mais qui en général ne fonctionne pas. Nous réfutons cette proposition en présentant un exemple d'équation pour laquelle la méthode de Sabbagh ne réussit pas.

Aos meus pais

Agradecimentos

Agradeço, de uma forma muito especial, ao Professor Jorge Almeida pela motivação, pelo incentivo, pela inteira disponibilidade, pelas sugestões e por tudo o que me ensinou.

Agradeço à Engenheira Maria Alzira Teixeira, colega e amiga, pelo apoio dado no desempenho da minha actividade profissional, no ISEP.

Agradeço a Alfredo Costa e a Marco Ferreira, sobretudo, pelo convívio e pelo companheirismo demonstrados ao longo destes anos.

E à minha família e aos meus amigos, muito obrigada.

Índice

Resumo	3
Abstract	5
Résumé	7
Agradecimentos	11
Introdução	15
1 Preliminares	17
1.1 Semigrupos, monóides e grupos	17
1.2 Palavras, linguagens e equações	18
1.3 Propriedades combinatórias no monóide livre	21
1.4 O grupo livre e a sua representação no monóide livre	23
1.5 Alguns resultados na Teoria de Grupos	27
2 Equações no grupo livre	31
2.1 A equação $x^\alpha = y^\beta z^\gamma$	31
2.1.1 A redução do problema	32
2.1.2 A equação no monóide livre	34
2.1.2.1 Caso I: u é uma palavra ciclicamente reduzida	34
2.1.2.2 Caso II: w é uma palavra ciclicamente reduzida	37
2.2 A equação $x^{-1}y^{-1}xy = z^n$	40

2.3	A generalização de Baumslag	44
3	O Algoritmo de Makanin para equações no monóide livre	47
3.1	Sistemas quadráticos: um algoritmo de decisão	48
3.2	A teoria existencial da concatenação	50
3.3	O Algoritmo: noções e estratégias	55
3.3.1	Torres dominó	55
3.3.2	Formas normais estáveis	57
3.3.3	Uma única variável	58
3.3.4	Restrições num semigrupo	62
3.4	O expoente de periodicidade	64
3.5	Equações fronteira	71
3.5.1	Ordens lineares num semigrupo	71
3.5.2	Das equações de palavras às equações fronteira	74
3.6	O teorema basilar	78
3.7	A condição da cadeia convexa	79
3.8	As regras de transformação	87
3.9	A prova do teorema basilar	95
3.10	Conclusão	98
4	Equações em grupos livres que não são finitamente aproximáveis	101
	Epílogo	105
	Bibliografia	107
	Índice remissivo	111
	Índice de símbolos	113

Introdução

Dado um sistema de equações envolvendo somente as operações de uma estrutura algébrica, pretende-se determinar se ele possui alguma solução numa dada estrutura E livre finitamente gerada. Este problema motivou a realização desta monografia. As estruturas algébricas aqui estudadas são monóides livres finitamente gerados e grupos livres finitamente gerados.

O estudo de equações em monóides livres foi iniciado na escola Russa por Markov no final da década de 1950, mas foi Makanin [21] quem, em 1977, resolveu o problema de decidibilidade. Com um conhecimento profundo da combinatória de palavras construiu um algoritmo que soluciona o problema. Uma consequência do resultado de Makanin foi a decidibilidade da teoria existencial da concatenação. Schulz [32] generalizou o Algoritmo de Makanin envolvendo no problema restrições racionais para as variáveis do sistema.

O estudo das equações no monóide livre como o esqueleto da teoria combinatória em grupos foi introduzido por Lyndon [18]. Lyndon iniciou o estudo das relações entre elementos de um grupo livre com a equação

$$x^2 = y^2 z^2,$$

concluindo que as soluções da equação geram um grupo cíclico, ao qual se seguiram algumas generalizações obtidas por Schenkman [31] com o estudo da equação

$$x^n = y^n z^n \text{ para } n > 1$$

e Schützenberger [30] com o estudo da equação

$$x^\alpha = y^\beta z^\gamma \text{ para } \alpha, \beta, \gamma > 1.$$

Este último estudou ainda a equação

$$x^{-1}y^{-1}xy = z^n \text{ com } n > 1$$

obtendo o mesmo resultado. Baumslag [5] obteve a mesma conclusão usando resultados da Teoria de Grupos. O seu estudo levou-o a uma generalização de todos estes resultados [6] usando novamente a Teoria de Grupos. Também aqui Makanin teve um papel preponderante. O problema da solubilidade de sistemas de equações no grupo

livre foi resolvido por Makanin em [22, 23]. O seu método para a decidibilidade de uma equação no grupo livre é muito mais complicado que o apresentado para monóides livres e envolve muitos conceitos e estratégias. Na tentativa de evitar este método pesado, Sabbagh propôs a consideração da seguinte propriedade para equações no grupo livre: equações que têm solução num grupo livre finitamente gerado se e só se tiverem solução em todo o quociente finito desse grupo. Para este tipo de equações, Sabbagh descreveu um algoritmo que permite responder à questão de decidibilidade. Mas, enquanto se conhecem vários sistemas para os quais a propriedade é válida [6, 4, 27, 28, 2, 3, 14], Coulbois e Khelif [8] mostraram que nem sempre assim se passa.

Dividimos esta monografia em quatro capítulos e um epílogo.

No primeiro capítulo introduzimos a linguagem com que vamos trabalhar: alguns conceitos da Álgebra Universal bem como algumas propriedades combinatórias no monóide livre e alguns resultados na Teoria de Grupos.

No segundo capítulo fazemos o estudo dos dois resultados obtidos por Schützenberger já enunciados. A primeira prova é baseada na combinatória de palavras usada por Lyndon e Schützenberger [19] e a segunda demonstração é uma prova alternativa de Baumslag [5] que usa resultados da Teoria de Grupos. Fazemos ainda uma abordagem à generalização de Baumslag que não é demonstrada neste trabalho.

No terceiro capítulo descrevemos pormenorizadamente a generalização de Schulz [32] do Algoritmo de Makanin para a solubilidade das equações no monóide livre. Fazemos também uma breve descrição de um algoritmo mais simples para a decidibilidade de sistemas onde cada variável ocorre no máximo duas vezes. É também neste capítulo que resolvemos o problema da teoria existencial da concatenação.

No quarto capítulo explicamos o algoritmo de Sabbagh como alternativa ao Algoritmo de Makanin para equações no grupo livre, que funciona para as equações que satisfazem a propriedade enunciada anteriormente. Mostramos ainda a existência de equações onde esta proposta não funciona.

Em cada um dos capítulos procura-se explicitar todo o seu conteúdo, quer nas estratégias, quer nos resultados demonstrados. As referências bibliográficas serão citadas sempre que for conveniente.

Capítulo 1

Preliminares

No trabalho a que nos propomos usamos como ferramentas algumas estruturas algébricas nomeadamente semigrupos, monóides e grupos livres finitamente gerados. Com uma análise combinatória por vezes exaustiva responderemos a algumas questões relativamente às equações que pretendemos estudar. O objectivo deste capítulo é relembrar alguns conceitos básicos da Álgebra Universal e introduzir algumas propriedades combinatórias que nos ajudarão na procura das nossas respostas. As definições e os resultados que aqui apresentamos podem ser encontrados em [1, 16, 19].

1.1 Semigrupos, monóides e grupos

Por *semigrupo* entendemos um conjunto equipado com uma operação binária associativa. Um subconjunto fechado para a operação denominamos de *subsemigrupo*. Um *morfismo de semigrupos*, mais precisamente do semigrupo S no semigrupo T , é uma aplicação $\varphi : S \rightarrow T$ tal que $\varphi(xy) = \varphi(x)\varphi(y)$ para todos os $x, y \in S$.

Definimos *monóide* como um semigrupo com elemento neutro, ou seja, um elemento ϵ tal que $m\epsilon = m = \epsilon m$ para todo o elemento m pertencente ao monóide. Um *submonóide* é um subconjunto fechado para a operação e contendo o elemento neutro e um *morfismo de monóides* é um morfismo de semigrupos que envia o elemento neutro de um semigrupo no elemento neutro do outro.

Dado um conjunto $X \subset S$ representamos por X^+ o *subsemigrupo gerado por X* , ou seja,

$$X^+ = \{x_1 \cdots x_n \mid n \geq 1, x_i \in X\}.$$

Se S for um monóide também definimos o *submonóide gerado por X* ,

$$X^* = X^+ \cup \{\epsilon\}.$$

As operações $X \mapsto X^+$ e $X \mapsto X^*$ são chamadas, respectivamente, de *operação $+$* e *operação $*$* .

Um subconjunto X de um semigrupo S diz-se *racional* se puder obter-se usando um número finito de vezes as operações união ($\cup$), produto ($\cdot$) e $+$ a partir de subconjuntos finitos de S (onde o produto de X por Y é dado por $X \cdot Y = \{xy \mid x \in X, y \in Y\}$).

Um *grupo* é um semigrupo G que possui um elemento ϵ tal que:

1. $\epsilon * x = x = x * \epsilon$ para todo o $x \in G$,
2. para todo o $x \in G$, existe um elemento $y \in G$ tal que $x * y = \epsilon = y * x$

onde $*$ é a operação binária associativa em G . Para todo o $x \in G$ dizemos que y é o *inverso* de x e usamos a notação x^{-1} .

1.2 Palavras, linguagens e equações

Sejam A um conjunto finito e A^+ o conjunto de todas as seqüências finitas $\langle a_1, \dots, a_n \rangle$ de elementos de A . Em A^+ definimos uma operação pela simples concatenação de seqüências:

$$\langle a_1, \dots, a_m \rangle \langle b_1, \dots, b_n \rangle = \langle a_1, \dots, a_m, b_1, \dots, b_n \rangle.$$

Esta operação é claramente associativa definindo em A^+ uma estrutura de semigrupo, o semigrupo gerado por A . O semigrupo A^+ diz-se *livre* em A no seguinte sentido: para todo o semigrupo S e toda a função $\varphi : A \rightarrow S$ existe um e um só homomorfismo $\bar{\varphi} : A^+ \rightarrow S$ tal que o diagrama

$$\begin{array}{ccc} A & \hookrightarrow & A^+ \\ & \searrow \varphi & \downarrow \exists! \bar{\varphi} \\ & & S \end{array} \quad (1.1)$$

comuta, onde $A \hookrightarrow A^+$ é a inclusão natural. O homomorfismo $\bar{\varphi}$ é definido por $\bar{\varphi}(a_1 \cdots a_n) = \varphi(a_1) \cdots \varphi(a_n)$ e chama-se a *extensão natural* de φ a A^+ .

Identificando cada seqüência da forma $\langle a \rangle$ com $a \in A$ temos

$$\langle a_1, \dots, a_n \rangle = a_1 \cdots a_n.$$

Adicionando a A^+ a seqüência vazia, $\langle \rangle$, representada por ϵ obtemos o monóide A^* , o monóide livre gerado por A .

Dizemos que A é o *alfabeto* das constantes, os seus elementos são as *letras*, os elementos de A^* as *palavras* (onde ϵ é a *palavra vazia*) e os subconjuntos de A^* as *linguagens* em A .

Uma linguagem $L \subseteq A^+$ é *reconhecida por um semigrupo* S se existir um homomorfismo $\varphi : A^+ \rightarrow S$ e $K \subseteq S$ tal que $L = \varphi^{-1}(K)$.

Proposição 1.1. *Uma linguagem é reconhecida por um autômato com um número finito de estados se e só se é reconhecida por um semigrupo finito.*

Dizemos que estas linguagens são *linguagens reconhecíveis*. Por outras palavras, $L \subseteq A^+$ é uma linguagem reconhecível se existir uma congruência em A^+ de índice finito para a qual L é uma união de classes, isto é, uma congruência que *satura* L . Notemos que, se σ é uma congruência em A^+ que satura L , então $u\sigma v$ e $xuy \in L$ implica que $xvy \in L$.

Para a linguagem $L \subseteq A^+$, definimos a relação σ_L por

$$u\sigma_L v \text{ se, para quaisquer } x, y \in A^*, xuy \in L \Leftrightarrow xvy \in L.$$

Então σ_L é a maior congruência (com respeito à inclusão) em A^+ que satura L e é chamada de *congruência sintáctica de L* . O quociente A^+/σ_L é denominado de *semigrupo sintáctico de L* e é representado por $SintL$. Seja φ_L o homomorfismo canónico de $A^+ \rightarrow SintL$. Assim, a condição maximal de σ_L diz-nos que um homomorfismo sobrejectivo $\psi : A^+ \rightarrow S$ reconhece L se e só se existe um homomorfismo $\mu : S \rightarrow SintL$ tal que $\mu \circ \psi = \varphi_L$ como podemos ver no seguinte diagrama comutativo:

$$\begin{array}{ccc} A^+ & \xrightarrow{\varphi_L} & SintL \\ & \searrow \psi & \uparrow \mu \\ & & S \end{array} \quad (1.2)$$

Dizemos que o semigrupo S *divide* o semigrupo T e escrevemos $S \prec T$ se S for a imagem homomorfa de um subsemigrupo de T . Temos então a seguinte proposição:

Proposição 1.2. *Seja $L \subseteq A^+$ uma linguagem.*

1. *Um semigrupo S reconhece L se e só se $SintL \prec S$;*
2. *Uma linguagem L é reconhecível se e só se $SintL$ é finito.*

A importância do estudo de semigrupos finitos deve-se ao teorema seguinte:

Teorema 1.3 (Kleene). *Sejam A um alfabeto finito e $L \subseteq A^*$. Então L é uma linguagem racional se e só se L é uma linguagem reconhecível.*

O *comprimento* da palavra $w = a_1a_2 \cdots a_n$ com $a_i \in A$ é o número n de letras cujo produto é w , o qual representamos por $|w|$. Assim sendo, $|\epsilon| = 0$.

Uma palavra u diz-se um *factor* de w se existirem palavras x e y tais que $w = xuy$. Dizemos também que u é um *prefixo* de w (respectivamente, *sufixo*) se $x = \epsilon$ (respect., $y = \epsilon$). Dizemos ainda que o factor (respect. prefixo, sufixo) é *próprio* se tivermos $u \neq w$.

A relação prefixo nas palavras é representada por $u \leq w$ sendo $u < w$ a relação prefixo próprio.

Seja Ω um conjunto para o qual assumimos que $A \cap \Omega = \emptyset$. Dizemos que Ω é o conjunto das variáveis.

Usaremos o mesmo símbolo σ para nos referirmos a uma aplicação $\sigma : \Omega \rightarrow A^*$ e à sua extensão canónica, o homomorfismo $\sigma : (A \cup \Omega)^* \rightarrow A^*$ que deixa as letras de A invariantes.

Definimos:

- Uma *equação* é um par $(E, D) \in (A \cup \Omega)^* \times (A \cup \Omega)^*$ e escreve-se como $E = D$.
- Um *sistema de equações* é um conjunto de equações $\{E_1 = D_1, \dots, E_k = D_k\}$.
- Um sistema onde cada variável ocorre no máximo duas vezes é chamado *sistema quadrático*.
- Uma *solução* é um homomorfismo $\sigma : (A \cup \Omega)^* \rightarrow A^*$ que deixa as letras de A invariantes e tal que $\sigma(E_i) = \sigma(D_i)$ para todo o $1 \leq i \leq k$. A solução é *não-singular* se $\sigma(x) \neq \epsilon$ para todo o $x \in \Omega$. Caso contrário, diz-se *singular*.

Exemplo 1.4. Sejam $A = \{a, b\}$ e $\Omega = \{x, y, z, u\}$. Consideremos a equação

$$xauzau = yzbraaby.$$

Trata-se de uma equação quadrática solúvel. Da equação vem que $|x| + |z| + 2|u| + 2 = |x| + |z| + 2|y| + 4$ e portanto $|u| = |y| + 1$. Assim, podemos, sem recorrer a uma procura exaustiva, encontrar soluções singulares e não-singulares.

Como exemplo de solução singular temos

$$\sigma(x) = \epsilon, \quad \sigma(y) = ab, \quad \sigma(u) = bab \quad \text{e} \quad \sigma(z) = aba$$

ficando $abababaabab = \sigma(xauzau) = \sigma(yzbraaby)$.

Uma solução não-singular será

$$\sigma(x) = ab, \quad \sigma(u) = baba, \quad \sigma(z) = ba \quad \text{e} \quad \sigma(y) = aba$$

ficando $ababababaababa = \sigma(xauzau) = \sigma(yzbraaby)$.

Exemplo 1.5. Consideremos agora a equação $abxcy = ycxba$ em que $A = \{a, b, c\}$ e $\Omega = \{x, y\}$. Estamos novamente em presença de uma equação quadrática solúvel em que

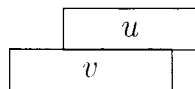
$$\sigma(x) = a \quad \text{e} \quad \sigma(y) = aba$$

é uma solução não-singular.

Note-se que, fazendo $y = \epsilon$ a equação fica reduzida a $abxc = cxba$ que não tem solução. Fazendo agora $x = \epsilon$ ficamos com $abcy = ycba$ que facilmente se verifica que também não tem solução.

1.3 Propriedades combinatórias no monóide livre

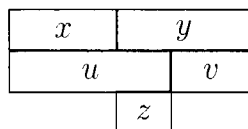
Uma *sobreposição* de duas palavras u e v é descrita pela figura:



Diz-se que a parte comum é um *factor comum*, isto é, tem-se $u = xy$ e $v = zx$ para algum $x \in A^+$.

Lema 1.6. Sejam $x, y, u, v \in A^*$. Se $xy = uv$ e $|x| \leq |u|$, então existe $z \in A^*$ tal que $u = xz$ e $y = zv$.

Demonstração. Imediata como podemos ver pela figura:



Sendo z o sufixo de u de comprimento $|u| - |x|$ obtemos o resultado. $\square$

Duas palavras $y, z \in A^*$ dizem-se *conjugadas* se $xy = zx$ para algum $x \in A^*$.

Lema 1.7. Sejam $x, y, z \in A^*$ com $y, z \neq \epsilon$. Então y e z são palavras conjugadas com $xy = zx$ se e só se existem palavras $r, s \in A^*$ tais que $y = sr$, $z = rs$ e $x \in (rs)^*r$.

Demonstração. A implicação recíproca é trivial. Vejamos a implicação directa. Se $xy = zx$ para $y, z \in A^+$ e $x \in A^*$, então temos, para todo o $n \geq 1$, $xy^n = (xy)y^{n-1} = zxy^{n-1} = z(xy)y^{n-2} = z^2xy^{n-2} = \dots = z^nx$, ou seja,

$$xy^n = z^nx \quad \forall n \geq 1. \quad (1.3)$$

Seja n tal que $n|z| > |x| \geq (n-1)|z|$. Então, deduzimos de (1.3) que, para alguns $r, s \in A^*$, temos

$$x = z^{n-1}r, \quad z = rs \quad \text{e} \quad sx = y^n.$$

Finalmente, $y^n = sx = sz^{n-1}r = (sr)^n$ obtendo assim $y = sr$ e provando o resultado. $\square$

O lema anterior mostra que em monóides livres as palavras conjugadas são obtidas por transposição de factores. Obtemos assim uma outra definição para palavras conjugadas.

Lema 1.8. Sejam $x, y \in A^*$. Se $xy = yx$, então x e y são potências da mesma palavra, isto é, existe $z \in A^*$ tal que $x, y \in z^*$.

Demonstração. Se $x = \epsilon$, então a conclusão é imediata: basta fazer $x = y^0$ e $y = y^1$. Suponhamos que $x \neq \epsilon$. Pelo Lema 1.7 e vendo x como palavra conjugada dela própria, então existem $r, s \in A^*$ tais que $x = rs = sr$ e $y \in (rs)^*r$. Se $r = \epsilon$ ou $s = \epsilon$, então o resultado segue de imediato. Caso contrário, concluímos, por indução sobre $\max\{|x|, |y|\}$, que r e s são potências do mesmo elemento. Logo, x e y são potências do mesmo elemento. $\square$

A palavra $p \in A^*$ diz-se *primitiva* se não for uma potência de outra palavra, isto é, se $p \neq \epsilon$ e $p \in r^*$ para algum $r \in A^*$, então $p = r$ (ou, de outro modo, se não puder ser escrita na forma $p = r^\alpha$ com $r \in A^*$ e $\alpha \neq 1$). Em particular, p é não vazia.

Lema 1.9. Sejam $p \in A^*$ uma palavra primitiva e $p^2 = xpy$ para alguns $x, y \in A^*$. Então tem-se $x = \epsilon$ ou $y = \epsilon$ (mas não ambos, como é óbvio).

Demonstração. Suponhamos que x e y são palavras não vazias. Então temos

p		p	
x	p	y	
	r	s	

$$p = xr, \quad p = sy \quad \text{e} \quad p = rs$$

e portanto $rs = xr$ e $rs = sy$. Logo, x e s são palavras conjugadas bem como y e r . Pelo Lema 1.7 temos

$$\begin{aligned} \exists a, b \in A^*, \alpha \geq 0 : \quad & x = ab, \quad s = ba \quad \text{e} \quad r = (ab)^\alpha a, \\ \exists c, d \in A^*, \beta \geq 0 : \quad & r = cd, \quad y = dc \quad \text{e} \quad s = (cd)^\beta c, \end{aligned}$$

com $a, b, c, d \neq \epsilon$ (senão p não seria uma palavra primitiva). Sendo assim,

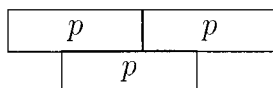
1. $p = (ab)^{\alpha+1}a$,
2. $p = (cd)^{\beta+1}c$,
3. $p = cdba$,

de onde vem

$$\begin{aligned} p^2 &= cdbacdba \\ &= (cd)^{\beta+1}c(ab)^{\alpha+1}a. \end{aligned}$$

Resulta que $bacd = (cd)^\beta c(ab)^\alpha a$ e portanto $\beta = 0$ ou $\alpha = 0$ (mas não ambos). Suponhamos, sem perda de generalidade, que $\beta = 0$ (e portanto $\alpha > 0$). Então temos $bacd = c(ab)^\alpha a$. Como $|bac| = |cab|$ obtemos $d = (ab)^{\alpha-1}a$ e, por 2, vem $p = cdc = c(ab)^{\alpha-1}ac$ que, por 1, é igual a $(ab)^{\alpha+1}a$. Logo, $c = ab = ba$. Pelo Lema 1.8, a e b são potências da mesma palavra e portanto p não seria uma palavra primitiva, contrariando a hipótese. $\square$

Pelo lema anterior é impossível obter a seguinte figura para uma palavra primitiva:



Lema 1.10. Se $x, y \in A^*$ têm potências x^m e y^n com prefixo comum de comprimento $|x| + |y|$, então x e y são potências da mesma palavra.

Demonstração. Tem-se que yx^m e y^{n+1} têm prefixo comum de comprimento $|x| + 2|y|$, logo yx^m e y^n têm prefixo comum de comprimento $|x| + |y|$. Analogamente, xy^n e x^m têm prefixo comum de comprimento $|x| + |y|$. Resulta que xy^n e yx^m têm prefixo comum de comprimento $|x| + |y|$ e portanto $xy = yx$. A conclusão segue pelo Lema 1.8. $\square$

Corolário 1.11. Se $x^m = y^n$ com $x, y \in A^*$ e $n, m \geq 1$, então x e y são potências da mesma palavra.

Demonstração. Se $m = 1$ ou $n = 1$, então a conclusão é imediata. Caso contrário, temos $|x^m| = |y^n| \geq |x| + |y|$ e a conclusão segue do Lema 1.10. $\square$

Corolário 1.12. Se $x \neq \epsilon$, então existem uma única palavra primitiva p e um único inteiro $\alpha \geq 1$ tais que $x = p^\alpha$.

Demonstração. Segue imediatamente do Corolário 1.11. $\square$

Corolário 1.13. Se p e q são palavras primitivas e têm potências p^m e q^n com prefixo comum de comprimento $|p| + |q|$, então $p = q$.

Demonstração. Segue imediatamente do Lema 1.10 e do Corolário 1.12. $\square$

Lema 1.14. A palavra conjugada $q = sr$ da palavra primitiva $p = rs$ é também primitiva.

Demonstração. Sejam $x \in A^+$ e $\alpha > 1$ tais que $q = x^\alpha$. Então existem $u, v \in A^*$ tais que $x = uv$, $s = (uv)^\beta u$ e $r = v(uv)^{\alpha-\beta-1}$. Assim, $p = rs = v(uv)^{\alpha-1}u = (vu)^\alpha$ contrariando a hipótese de p ser primitiva. $\square$

1.4 O grupo livre e a sua representação no monóide livre

Seja X um subconjunto de um grupo G . Dizemos que G é um *grupo livre de base X* se, para todo o grupo F e toda a função $f : X \rightarrow F$, existe um único homomorfismo

$\varphi : G \rightarrow F$ que estende f :

$$\begin{array}{ccc} X & \hookrightarrow & G \\ & \searrow f & \downarrow \exists! \varphi \\ & & F \end{array} \quad (1.4)$$

Dado um alfabeto A seja $\bar{A}$ um conjunto para o qual assumimos que $A \cap \bar{A} = \emptyset$ e existe uma bijecção de A em $\bar{A}$ que a cada elemento $a \in A$ associa um elemento $\bar{a} \in \bar{A}$. Temos $a \neq \bar{a}$ e assumimos que $\bar{\bar{a}} = a$ para todo o $a \in A \cup \bar{A}$. Seja M o monóide livre gerado pelo conjunto $A \cup \bar{A}$ equipado com a operação de concatenação de elementos.

O *inverso formal* $\bar{u}$ de uma palavra $u \in M$ é a imagem pelo automorfismo

$$\begin{aligned} \iota : \quad M & \rightarrow M \\ u = a_1 \cdots a_n & \mapsto \bar{u} = \bar{a}_n \cdots \bar{a}_1 \end{aligned}$$

com $a_i \in A \cup \bar{A}$ para todo o $1 \leq i \leq n$.

Uma palavra diz-se *reduzida* se não tiver factores da forma $a\bar{a}$ com $a \in A \cup \bar{A}$. A palavra vazia e o inverso formal de uma palavra reduzida são palavras reduzidas. Resulta, da definição de palavra reduzida, que uma palavra é reduzida se não tiver factores da forma $u\bar{u}$ com $u \in M \setminus \{\epsilon\}$.

Seja $Red(A)$ o conjunto de todas as palavras reduzidas do monóide M . A concatenação de palavras não define uma operação interna em $Red(A)$ pois a concatenação de duas palavras reduzidas poderá não ser uma palavra reduzida. Definimos em $Red(A)$ uma operação de palavras reduzidas u e v , à qual denominamos de *multiplicação*, como a palavra que é obtida de uv após todos os sucessivos cancelamentos de factores da forma $a\bar{a}$ com $a \in A \cup \bar{A}$. Por outras palavras, se $u = u'w$ e $v = \bar{w}v'$ com $u'v'$ palavra reduzida, então

$$u \cdot v = u'v'.$$

É fácil ver que a multiplicação em $Red(A)$ está bem definida e é associativa. A palavra vazia actua como elemento neutro e o inverso formal $\bar{u}$ da palavra reduzida u é tal que $u \cdot \bar{u} = \bar{u} \cdot u = \epsilon$. Assim, $Red(A)$ equipado com a operação de multiplicação é um grupo. A partir daqui usamos as notações G e u^{-1} para nos referirmos, respectivamente, ao grupo $Red(A)$ e ao inverso $\bar{u}$ de todo o elemento $u \in G$.

Definimos o homomorfismo $\phi : M \rightarrow G$ do seguinte modo:

$$\begin{aligned} \phi : \quad M & \rightarrow G \\ a & \mapsto a \\ \bar{a} & \mapsto a^{-1} \end{aligned}$$

Assim, uma palavra $u \in M$ representa o elemento $\phi(u) \in G$. Note-se que, se $u = a_1 \cdots a_n$ com $a_i \in A \cup \bar{A}$ para todo o $1 \leq i \leq n$, então $\phi(\bar{u}) = \phi(\bar{a}_n \cdots \bar{a}_1) = a_n^{-1} \cdots a_1^{-1} = (a_1 \cdots a_n)^{-1} = (\phi(u))^{-1}$. Temos ainda que cada elemento de G é representado por uma única palavra reduzida.

Seja F um grupo e $f : A \rightarrow F$ uma função. Definimos a função $\tilde{f}$ do seguinte modo:

$$\begin{aligned}\tilde{f} : A \cup \bar{A} &\rightarrow F \\ a \in A &\mapsto f(a) \\ \bar{a} \in \bar{A} &\mapsto (f(a))^{-1}.\end{aligned}$$

Como M é o monóide livre sobre $A \cup \bar{A}$ e F é um monóide, resulta que existe uma aplicação $\tilde{\varphi}$ tal que o diagrama seguinte comuta:

$$\begin{array}{ccc} A \cup \bar{A} & \xrightarrow{\quad} & M \\ & \searrow \tilde{f} & \downarrow \exists! \tilde{\varphi} \\ & & F \end{array} \quad (1.5)$$

Resulta que o homomorfismo

$$\begin{aligned}\varphi : \quad G &\rightarrow F \\ a \in A &\mapsto \tilde{\varphi}(a)\end{aligned}$$

estende f :

$$\begin{array}{ccc} A & \xrightarrow{\quad} & G \\ & \searrow f & \downarrow \varphi \\ & & F \end{array} \quad (1.6)$$

A unicidade é imediata. Logo, G é o grupo livre de base A .

Lema 1.15. Seja $u \in M$ uma palavra não vazia. Se u é uma palavra reduzida, então $u \neq \bar{u}$.

Demonstração. Suponhamos que $u = \bar{u}$. Seja $u = a_1 \cdots a_n$ com $a_i \in A \cup \bar{A}$ para todo o $1 \leq i \leq n$. Então $u = a_1 \cdots a_n = \bar{a}_n \cdots \bar{a}_1 = \bar{u}$. Resulta que $|u|$ é par senão teríamos que $a_{\frac{n+1}{2}} = \bar{a}_{\frac{n+1}{2}}$ contrariando o facto de $A \cap \bar{A} = \emptyset$. Resulta também que $a_i = \bar{a}_{n-i+1}$ para todo o $1 \leq i \leq n$. Mas então temos que $u = a_1 \cdots a_n = a_1 \cdots a_{\frac{n}{2}} \bar{a}_{\frac{n}{2}} \cdots \bar{a}_1$ que não é uma palavra reduzida. $\square$

Uma palavra u é *ciclicamente reduzida* se for reduzida e não for da forma $vu'\bar{v}$ onde v é uma palavra não-vazia.

Lema 1.16. Toda a palavra reduzida $u \in M$ tem uma única representação da forma $vu'\bar{v}$ onde u' é uma palavra ciclicamente reduzida.

Demonstração. Sejam $v_1 u'_1 \bar{v}_1 = u = v_2 u'_2 \bar{v}_2$ com u'_1 e u'_2 palavras ciclicamente reduzidas. Se $|u'_1| = |u'_2|$, então resulta que $v_1 = v_2$ e $u'_1 = u'_2$. Suponhamos, sem perda de generalidade, que $|u'_1| < |u'_2|$:

v_1	u'_1	$\bar{v}_1$
v_2	u'_2	$\bar{v}_2$
	w_1	w_2

Então $u'_2 = w_1 u'_1 w_2$, $v_1 = v_2 w_1$ e $\bar{v}_1 = w_2 \bar{v}_2$ com $w_1, w_2 \in M$. Resulta que $v_1 = v_2 w_1 = \overline{w_2 \bar{v}_2} = \overline{v_2 \bar{w}_2}$ e portanto $w_1 = \bar{w}_2$. Mas então $u'_2 = w_1 u'_1 w_2 = w_1 u'_1 \bar{w}_1$ não é uma palavra ciclicamente reduzida, contrariando a hipótese. $\square$

Lema 1.17. Sejam $u, v \in M$ palavras conjugadas. Se u é uma palavra ciclicamente reduzida, então v também é.

Demonstração. Pelo Lema 1.7, duas palavras conjugadas são obtidas por transposição, ou seja, existem $r, s \in M$ tais que $u = rs$ e $v = sr$. Suponhamos que v não é uma palavra ciclicamente reduzida. Então $v = av'\bar{a}$ ou $v = v_1 a \bar{a} v_2$ para alguns $v', v_1, v_2 \in M$ e $a \in A \cup \bar{A}$. No primeiro caso temos a como prefixo de s e $\bar{a}$ como sufixo de r e portanto $u = rs$ tem como factor $\bar{a}a$, contrariando a hipótese de u ser uma palavra reduzida. No segundo caso temos: ou $a\bar{a}$ é factor de s ou $a\bar{a}$ é factor de r e portanto $u = rs$ tem factor $a\bar{a}$, ou s tem sufixo a e r tem prefixo $\bar{a}$ e portanto $u = rs = \bar{a}u'a$ para algum $u' \in M$. Em qualquer um dos casos resulta que u não é uma palavra ciclicamente reduzida, contrariando a hipótese. $\square$

Lema 1.18. Sejam $u, v \in M$. Se u é uma palavra reduzida e $\bar{u}$ é um factor de uv , então $\bar{u}$ é factor de v .

Demonstração. Sejam $r, s \in M$ tais que $uv = r\bar{u}s$. Suponhamos que $\bar{u}$ não é factor de v . Então $|v| < |\bar{u}s|$ como podemos ver na figura seguinte:

u		v	
r		$\bar{u}$	s
	t		

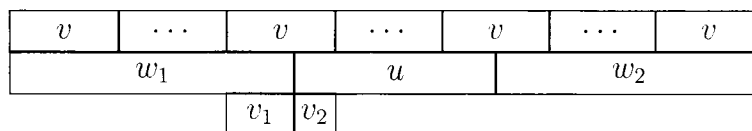
Assim, temos que $|r| < |u|$ e existe $t \in M$ com $t \neq \epsilon$ tal que $u = rt$ e $tv = \bar{u}s$. Obtemos $tv = \bar{u}s = \bar{t}rs$ e portanto, como $|t| = |\bar{t}|$, resulta que $t = \bar{t}$. Logo, pelo Lema 1.15, t não é uma palavra reduzida e, consequentemente, u não é uma palavra reduzida. $\square$

Corolário 1.19. Se u é uma palavra reduzida e $\bar{u}$ é factor de uma potência de $u^m v$ com $m \geq 1$, então $\bar{u}$ é factor de v .

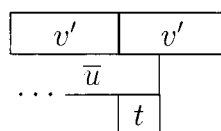
Corolário 1.20. Se u é uma palavra reduzida e $\bar{u}$ é factor de uma potência de u , então $u = \epsilon$.

Lema 1.21. Se u é uma palavra reduzida não-vazia e ambas as palavras u e $\bar{u}$ são factores de uma potência de uma palavra ciclicamente reduzida v , então existem palavras $r, s \in M$ tais que v e $ur\bar{u}s$ são palavras conjugadas.

Demonstração. Sejam $\alpha \geq 1$ e v uma palavra ciclicamente reduzida tais que u e $\bar{u}$ são factores de v^α . Note-se que, se v é uma palavra ciclicamente reduzida, então v^α também é uma palavra ciclicamente reduzida. Consideremos a figura:



Sejam $w_1, w_2 \in M$ tais que $v^\alpha = w_1 u w_2$. Então $u w_2 w_1$ e v^α são palavras conjugadas e $u < u w_2 w_1$. Mais ainda, existem $v_1, v_2 \in M$ tais que $v = v_1 v_2$ e $w_1 = (v_1 v_2)^\beta v_1$ para algum $0 \leq \beta < \alpha$. Obtemos $u w_2 w_1 = v_2 (v_1 v_2)^{\alpha-1} v_1 = (v_2 v_1)^\alpha$ e portanto u é prefixo de uma potência de uma palavra conjugada de v , $v' = v_2 v_1$. Assim, $u = (v')^\gamma v'_1$ com $v' = v'_1 v'_2$, $v'_1 \neq \epsilon$ e $0 \leq \gamma < \alpha$. Como $\bar{u}$ é factor de v^α , então $\bar{u}$ é factor de alguma potência de v' . Seja t o maior sufixo de $\bar{u}$ que é prefixo de v' . Como $|u| = |\bar{u}|$ e u é prefixo de uma potência de v' , temos que $t \leq u$, ou seja, $u = t \dots$. Obtemos $\bar{u} = \dots t = \dots \bar{t}$ e portanto $t = \bar{t}$. Pelo Lema 1.15 resulta que $t = \epsilon$. Logo, não podemos ter a figura seguinte:



resultando que $\bar{u}$ é factor de v' . Ainda pela mesma razão, $\bar{u}$ é factor próprio de v' . Como $|u| = |\bar{u}| \leq |v'|$ e $u = (v')^\gamma v'_1$ com $v'_1 \neq \epsilon$ resulta que $\gamma = 0$ e $u = v'_1$. Como $\bar{u}$ é factor de $v' = u v'_2$, temos, pelo Lema 1.18 que $\bar{u}$ é factor de v'_2 . Logo $v'_2 = r \bar{u} s$ para alguns $r, s \in M$. Resulta que $v' = v'_1 v'_2 = u r \bar{u} s$ e v são palavras conjugadas. $\square$

1.5 Alguns resultados na Teoria de Grupos

Apresentamos em seguida algumas definições e resultados sobre grupos livres que serão necessários na Secção 2.2. Estes resultados são facilmente encontrados em qualquer livro da especialidade. Citamos, em particular, [13, 29].

Lema 1.22. Se F é um grupo livre de base X , então F/F' é um grupo livre Abeliano de base $X_\# = \{x F' \mid x \in X\}$.

Demonstração. Seja A um grupo Abeliano e $f : X_\# \rightarrow A$ uma função. Definimos

$$\begin{aligned} f_\# : X &\rightarrow A \\ x &\mapsto f(x F') \end{aligned}$$

Como F é livre de base X , existe um homomorfismo $\varphi : F \rightarrow A$ que estende $f_\#$:

$$\begin{array}{ccc} X & \hookrightarrow & F \\ & \searrow f_\# & \downarrow \exists^1 \varphi \\ & & A \end{array} \tag{1.7}$$

Notemos que, se $x \in F'$, então $\varphi(x) = 1$ pois A é Abeliano. Logo, $F' \leq \text{Ker } \varphi$ e portanto existe um homomorfismo

$$\begin{aligned} \tilde{\varphi}: F/F' &\rightarrow A \\ wF' &\mapsto \varphi(w) \end{aligned}$$

que estende f :

$$\begin{array}{ccc} X & \hookrightarrow & F \\ \downarrow & & \downarrow \\ X_{\#} & \hookrightarrow & F/F' \\ & \searrow f & \downarrow \exists \tilde{\varphi} \\ & & A \end{array} \quad (1.8)$$

Mostremos a sua unicidade. Suponhamos que existe $\theta : F/F' \rightarrow A$ tal que $\theta(xF') = f(xF')$ para todo o $x \in X$. Seja $\nu : F \rightarrow F/F'$ o homomorfismo natural. Então $\theta \circ \nu : F \rightarrow A$ é um homomorfismo tal que $\theta \circ \nu(x) = \theta(xF') = f(xF') = f_{\#}(x) = \varphi(x)$ para todo o $x \in X$. Como X é uma base de F , temos $\theta \circ \nu = \varphi = \tilde{\varphi} \circ \nu$. Como ν é sobrejectiva, resulta que $\theta = \tilde{\varphi}$. Logo F/F' é um grupo Abeliano livre de base $X_{\#}$. $\square$

Teorema 1.23 (Nielsen-Schreier). Todo o subgrupo de um grupo livre é livre.

Teorema 1.24. Dois grupos livres são isomorfos se e só se têm o mesmo número de geradores livres. Um grupo livre F_r com um número finito r de geradores livres é livremente gerado por qualquer conjunto de r geradores.

Dizemos que um grupo infinito G tem *localmente a propriedade $\mathcal{P}$* se ela se verificar para todo o subgrupo finitamente gerado de G .

Seja G um grupo. Definimos o *comutador* $[x, y]$ com $x, y \in G$ por:

$$[x, y] = x^{-1}y^{-1}xy. \quad (1.9)$$

Lema 1.25. Sejam x, y e z elementos de um grupo. Então temos

1. $[x, y] = [y, x]^{-1}$;
2. $[xy, z] = [x, z]^y[y, z]$;
3. $[x, yz] = [x, z][x, y]^z$.

onde $x^y = y^{-1}xy$ para quaisquer elementos x, y do grupo.

Demonstração. Temos

$$\begin{aligned}[x, y] &= x^{-1}y^{-1}xy \\ &= (y^{-1}x^{-1}yx)^{-1} \\ &= [y, x]^{-1}\end{aligned}$$

e

$$\begin{aligned}[xy, z] &= y^{-1}x^{-1}z^{-1}xyz \\ &= y^{-1}x^{-1}z^{-1}x(zyy^{-1}z^{-1})yz \\ &= y^{-1}(x^{-1}z^{-1}xz)y(y^{-1}z^{-1}yz) \\ &= [x, z]^y[y, z].\end{aligned}$$

De modo análogo obtemos a terceira igualdade. □

Capítulo 2

Equações no grupo livre

Em 1958, R. C. Lyndon [18] inicia o estudo de relações em grupos livres provando que as soluções da equação

$$x^2 = y^2 z^2$$

são elementos de um grupo cíclico. Desde então uma série de generalizações foram feitas. Em 1959, E. Schenkman [31] obtém a mesma conclusão para a equação

$$x^n = y^n z^n$$

com $n > 1$. Na mesma altura M. P. Schützenberger [30] mostra que a equação

$$x^\alpha = y^\beta z^\gamma$$

com $\alpha, \beta, \gamma > 1$ tem também como únicas soluções elementos de um grupo cíclico. Nesse mesmo artigo obtém o mesmo resultado para a equação

$$x^{-1} y^{-1} x y = z^n$$

com $n > 1$. Neste capítulo estudaremos os dois resultados de Schützenberger e na última secção referimos uma generalização de todos estes resultados obtida por G. Baumslag [6].

2.1 A equação $x^\alpha = y^\beta z^\gamma$

Nesta secção procuramos soluções da equação $x^\alpha = y^\beta z^\gamma$ num grupo livre G onde α, β e γ são inteiros não-negativos. Temos a solução óbvia em que $\sigma(x), \sigma(y)$ e $\sigma(z)$, onde $\sigma : \Omega \rightarrow G$, são potências de um mesmo elemento e portanto são elementos de um grupo cíclico. O nosso objectivo é mostrar que estas são as únicas soluções.

Marcel Paul Schützenberger [30] estuda a equação para $\alpha, \beta, \gamma \geq 2$. De facto, o problema só tem interesse se nenhum dos expoentes for 0 ou 1. No que se segue

baseamo-nos no trabalho de R. C. Lyndon e M. P. Schützenberger [19] cuja prova usa somente propriedades combinatórias.

Na Subsecção 2.1.1 reduzimos o problema de encontrar todas as soluções da equação no grupo livre G ao problema de encontrar todas as soluções em duas equações num monóide livre M cujas palavras representam elementos do grupo livre G . Na Subsecção 2.1.2 estudamos as duas equações no monóide M e mostramos que têm somente as soluções triviais.

2.1.1 A redução do problema

Suponhamos que $\phi(u)$, $\phi(v)$ e $\phi(w)$ são elementos do grupo livre G que satisfazem a equação

$$x^\alpha = y^\beta z^\gamma \quad (2.1)$$

onde $\alpha, \beta, \gamma \geq 2$. Queremos mostrar que $\phi(u)$, $\phi(v)$ e $\phi(w)$ são elementos de um grupo cíclico, ou seja, são potências de um elemento de G . O nosso objectivo nesta secção é reduzir o problema inicial a outro no monóide M .

Como a cada elemento de G corresponde uma única palavra reduzida em M podemos assumir que u, v e w são palavras reduzidas. Assumimos também que são palavras primitivas. Se assim não for, escrevemos u, v e w na forma

$$u = (u')^{\alpha'}, v = (v')^{\beta'} \text{ e } w = (w')^{\gamma'}$$

onde u', v' e w' são palavras primitivas. Reduzimos o problema à resolução da equação

$$x^{\alpha'\alpha} = y^{\beta'\beta} z^{\gamma'\gamma}$$

onde consideramos somente soluções que são palavras primitivas. Queremos então mostrar que u, v e w são iguais ou inversos formais das outras.

Também é claro que se $\phi(u)$, $\phi(v)$ e $\phi(w)$ são soluções da equação, então podemos substituir estas palavras pela conjugação por um elemento de G e u, v e w pelas correspondentes palavras primitivas reduzidas u', v' e w' e continuamos a obter uma solução da equação. Se $v = rv'\bar{r}$ onde v' é uma palavra ciclicamente reduzida, então a conjugação de $\phi(v)$ por $\phi(r)$ substitui v por v' e portanto podemos assumir que

$$v \text{ é uma palavra ciclicamente reduzida.} \quad (2.2)$$

Podemos assumir também que

$$vw \text{ é uma palavra reduzida} \quad (2.3)$$

como se mostra: se $v = \bar{w}$, então a conclusão de que as componentes da solução são iguais ou inversos formais segue de imediato. Suponhamos que $v \neq \bar{w}$. Pelo Corolário 1.13, $|v| + |w|$ é majorante do comprimento do prefixo comum de potências

de $\bar{v}$ e w . Sejam $m, n \geq 1$ os menores inteiros tais que $\bar{v}^m$ e w^n não são prefixos do outro. Existem factorizações $v = v_1 v_2$ e $w = w_1 w_2$ com $v_1 \neq \epsilon$ e $w_2 \neq \epsilon$ tais que

$$\begin{aligned}\bar{v}^m &= \bar{v}^{m-1} \bar{v}_2 \bar{v}_1 && \text{com } \bar{v}^{m-1} \bar{v}_2 \text{ prefixo máximo de } w^*, \\ w^n &= w^{n-1} w_1 w_2 && \text{com } w^{n-1} w_1 \text{ prefixo máximo de } \bar{v}^*.\end{aligned}$$

Suponhamos, sem perda de generalidade, que $|\bar{v}^{m-1} \bar{v}_2| \leq |w^{n-1} w_1|$. Então obtemos a figura seguinte:

$\bar{v}^{m-1}$	$\bar{v}_2$	$\bar{v}_1$	$\bar{v}$
$w^{n-1} w_1$			

de onde se conclui que, se $|\bar{v}^{m-1} \bar{v}_2| < |w^{n-1} w_1|$, então contrariamos o facto de $\bar{v}^{m-1} \bar{v}_2$ ser prefixo máximo de w^* . Logo, $\bar{v}^{m-1} \bar{v}_2 = w^{n-1} w_1$ e portanto $v_2 v^{m-1}$ e $w^{n-1} w_1$ são inversos formais. Resulta ainda que as primeiras letras de $\bar{v}_1$ e w_2 são diferentes e portanto $v_1 w_2$ é uma palavra reduzida. Da conjugação de $\phi(v)$ e $\phi(w)$ por $\phi(w^{n-1} w_1) = \phi(\bar{v}^{m-1} \bar{v}_2)$ obtemos

$$\begin{aligned}\phi(\bar{v}^{m-1} \bar{v}_2)^{-1} \phi(v) \phi(\bar{v}^{m-1} \bar{v}_2) &= \phi(v_2 v^{m-1}) \phi(v) \phi(\bar{v}^{m-1} \bar{v}_2) \\ &= \phi(v_2 v^{m-1} v \bar{v}^{m-1} \bar{v}_2) \\ &= \phi(v_2 v \bar{v}_2) \\ &= \phi(v_2 v_1)\end{aligned}$$

e

$$\begin{aligned}\phi(w^{n-1} w_1)^{-1} \phi(w) \phi(w^{n-1} w_1) &= \phi(\bar{w}_1 \bar{w}^{n-1}) \phi(w) \phi(w^{n-1} w_1) \\ &= \phi(\bar{w}_1 \bar{w}^{n-1} w w^{n-1} w_1) \\ &= \phi(\bar{w}_1 w w_1) \\ &= \phi(w_2 w_1)\end{aligned}$$

ou seja, temos a substituição de v por $v' = v_2 v_1$ e w por $w' = w_2 w_1$. Como v é uma palavra ciclicamente reduzida, então v' é uma palavra ciclicamente reduzida. Além disso, como $v_1 w_2$ é uma palavra reduzida e $v_1, w_2 \neq \epsilon$, resulta que $v' w'$ é uma palavra reduzida.

Mostramos ainda que podemos assumir uma das duas condições:

Caso I: u é uma palavra ciclicamente reduzida

Caso II: w é uma palavra ciclicamente reduzida

Usamos indução sobre $|u|$. Se $|u| = 1$, então u é uma palavra ciclicamente reduzida. Suponhamos que (2.2) e (2.3) são satisfeitas mas que u e w não são palavras ciclicamente reduzidas. Então $u = a u' \bar{a}$ com $a \in A \cup \bar{A}$ e portanto a palavra reduzida

$a(u')^\alpha \bar{a}$ que representa $(\phi(u))^\alpha$ tem prefixo a e sufixo $\bar{a}$. Como vw é uma palavra reduzida, temos que a palavra reduzida que representa $\phi(v)^\beta \phi(w)^\gamma$ começa com a mesma letra de v e termina com a mesma letra de w . De modo a que a equação (2.1) seja satisfeita resulta que v começa com a letra a e w termina com a letra $\bar{a}$. Assim, $v = av_0$ e $w = aw'\bar{a}$ pois w não é uma palavra ciclicamente reduzida. Conjugando $\phi(u), \phi(v)$ e $\phi(w)$ por $\phi(a)$ substituímos u, v e w por $u', v' = v_0a$ e w' . Como v é uma palavra ciclicamente reduzida, então v' também é. Temos ainda que $v'w'$ é uma palavra ciclicamente reduzida pois $v' = v_0a$ com $a \neq \epsilon$ e, como $w = aw'\bar{a}$ é uma palavra reduzida, então aw' é uma palavra reduzida. Portanto $v'w' = v_0aw'$ é uma palavra reduzida. Assim sendo, as condições (2.2) e (2.3) são satisfeitas quando u é substituído por u' onde $|u'| = |u| - 2$. A conclusão segue por indução.

2.1.2 A equação no monóide livre

Nesta subsecção resolveremos a equação no monóide livre considerando os Casos I e II da secção anterior. Notemos que os dois casos não são disjuntos. De facto, quando estudarmos o Caso II reduzi-lo-emos à sua intersecção com o Caso I. Para esta intersecção, isto é, quando u e w são palavras ciclicamente reduzidas, o argumento do Caso I pode ser simplificado.

2.1.2.1 Caso I: u é uma palavra ciclicamente reduzida

Escrevemos w na forma $\bar{r}w'r$ onde w' é uma palavra ciclicamente reduzida e r poderá ser a palavra vazia. Como u e v são palavras ciclicamente reduzidas e vw é uma palavra reduzida, obtemos a igualdade

$$u^\alpha = v^\beta \bar{r}(w')^\gamma r \quad (2.4)$$

que supomos ser válida em G . Como ambos os membros são palavras reduzidas eles são iguais em M . Vamos mostrar que $r = \epsilon$ e $u = v = w'$. Usamos indução sobre $|u|$. O caso $|u| = 1$ é óbvio: u é uma letra e portanto u^α é potência de uma letra. Logo, $u = v = w'$ e $r = \epsilon$ visto vw ser uma palavra reduzida.

A igualdade (2.4) leva à igualdade

$$(u')^\alpha = (\bar{w}')^\gamma r \bar{v}^\beta \bar{r} \quad (2.5)$$

onde u' é um conjugado de $\bar{u}$.

Se $|v^\beta| \geq |u| + |v|$, então u^α e v^β têm um prefixo comum de comprimento $|u| + |v|$ e portanto, pelo Lema 1.10, temos $u = v$. Suponhamos que

$$|v^{\beta-1}| < |u|$$

e, por simetria, usando (2.5), que

$$|(w')^{\gamma-1}| < |u|.$$

Pelo Lema 1.21, como r e $\bar{r}$ são factores de u^α , existem $s, t \in M$ tais que $u = s\bar{r}tr$ e

$$v^\beta \bar{r} = u^{\alpha_1} s \bar{r} \quad \text{e} \quad (w')^\gamma r = tr u^{\alpha_2}$$

com $\alpha_1 + \alpha_2 + 1 = \alpha$. Logo, $|u^{\alpha_1}| < |v^\beta|$. Como $|v^{\beta-1}| < |u|$, então $|v^\beta| < |u^2|$ e portanto $\alpha_1 \leq 1$. De modo análogo, concluímos que $\alpha_2 \leq 1$ e portanto $\alpha \leq 3$. Como $\alpha \geq 2$, temos $\alpha = 2$ ou $\alpha = 3$.

Suponhamos que $\alpha = 2$. Por simetria, assumimos que $\alpha_1 = 1$ e $\alpha_2 = 0$. Obtemos $v^\beta = us = s\bar{r}trs$ e $(w')^\gamma = t$. Logo, $v^\beta = s\bar{r}(w')^\gamma rs$. Assim, existe uma palavra conjugada v' de v tal que

$$(v')^\beta = s^2 \bar{r} (w')^\gamma r \quad (2.6)$$

que é uma igualdade da forma inicial: v' é uma palavra ciclicamente reduzida visto v e v' serem palavras conjugadas e v ser uma palavra ciclicamente reduzida e s é uma palavra ciclicamente reduzida pois, caso contrário, $v^\beta = s\bar{r}trs$ não seria ciclicamente reduzida. Como

$$|v'| = |v| \leq |v^{\beta-1}| < |u|$$

concluimos, por indução, que $r = \epsilon$ e $v' = s = w'$ e portanto, como $v^\beta = s\bar{r}(w')^\gamma rs$, resulta que $v = v' = w'$. Obtemos de (2.4) a igualdade $u^\alpha = v^{\beta+\gamma}$. Logo, pelo Corolário 1.13, como u e v são palavras primitivas, temos $u = v = w'$.

Se $\alpha = 3$, então $\alpha_1 = \alpha_2 = 1$ visto termos $\alpha_1, \alpha_2 \leq 1$. Obtemos

$$v^\beta = us = s\bar{r}trs \quad \text{e} \quad (w')^\gamma = trs\bar{r}t.$$

Por simetria podemos supor que $|(w')^\gamma| \leq |v^\beta|$ e portanto $|t| \leq |s|$. Como $|v^{\beta-1}| < |u|$ e $v^\beta = us$, temos $|s| < |v|$. Segue de $v^\beta = s\bar{r}trs$ que v tem s como prefixo e sufixo. Pelo Lema 1.7, como $v = s \cdots = \cdots s$, temos $s = (pq)^k p$ e $v = (pq)^{k+1} p$ com p, q palavras reduzidas tais que $p, q \neq \epsilon$ pois v é uma palavra primitiva. Assim, $v = sqp = pqs$ e portanto, como $v^\beta = s\bar{r}trs$, obtemos

$$\bar{r}tr = qp v^{\beta-2} pq.$$

Se $|q| \leq |r|$, então r tem q e $\bar{q}$ como sufixo o que, pelo Lema 1.15, é impossível pois $q \neq \epsilon$ é uma palavra reduzida. Logo, $|r| < |q|$ e $\bar{r}$ é prefixo de q e r é sufixo de q . Se houver sobreposição de $\bar{r}$ e r como na figura

$\bar{r}$		
q_1	q_2	q_3
	r	

com q_1, q_2 e q_3 palavras reduzidas, obtemos $\bar{r} = q_1 q_2$ e $r = q_2 q_3$ e, consequentemente, $\bar{r} = q_1 q_2 = \bar{q}_3 \bar{q}_2$. Logo, $q_2 = \bar{q}_2$ o que é impossível pois q_2 é uma palavra reduzida. Assim, $q = \bar{r} q' r$ com q' palavra reduzida e $q' \neq \epsilon$ (senão q não seria palavra reduzida) e

$$t = q' r p v^{\beta-2} p \bar{r} q'.$$

Como $|t| \leq |s| < |v|$, obtemos $\beta = 2$ e $t = q'rp^2\bar{r}q'$. Temos

$$2|p| + |q| < |t| \leq |s| = (k+1)|p| + k|q|$$

e portanto $k \geq 2$.

A relação

$$\begin{aligned} (w')^\gamma &= trs\bar{r}t \\ &= q'rp^2\bar{r}q'r(pq)^k p\bar{r}q'rp^2\bar{r}q' \\ &= q'rp(pq)^{k+2}p^2\bar{r}q', \end{aligned}$$

pois $q = \bar{r}q'r$, implica que

$$(w'')^\gamma = (pq)^{k+2}p^2\bar{r}(q')^2rp$$

onde w'' é uma palavra conjugada de w' . Como $k \geq 2$ obtemos

$$|qp^2\bar{r}(q')^2rp| < 4|p| + 3|q| \leq |(pq)^{k+1}p|.$$

Assim

$$|(w'')^\gamma| = |(pq)^{k+1}p| + |qp^2\bar{r}(q')^2rp| < 2|(pq)^{k+1}p|$$

e, como $\gamma \geq 2$, temos $|w''| < |(pq)^{k+1}p|$. Portanto, $(w'')^\gamma$ e $(pq)^{k+3}$ têm prefixo comum de comprimento superior a $|w''| + |pq|$. Pelo Lema 1.10 e pelo Corolário 1.12, como w'' é primitiva, então pq é uma potência de w'' . Como $(pq)^{k+2}$ e $(pq)^{k+2}p^2\bar{r}(q')^2rp$ são potências de w'' , resulta que $p^2\bar{r}(q')^2rp$ é uma potência de w'' . Logo, $p^3\bar{r}(q')^2r$ é uma potência de uma palavra w''' conjugada de w'' . Da relação

$$|w'''| = |w''| \leq |pq| < |p^3\bar{r}(q')^2r|,$$

pois pq é potência de w'' , obtemos

$$(w''')^\delta = p^3\bar{r}(q')^2r \tag{2.7}$$

para algum $\delta \geq 2$ que é novamente uma igualdade da forma (2.4). Notemos que p é uma palavra ciclicamente reduzida pois é prefixo e sufixo de v e v é uma palavra ciclicamente reduzida. De modo análogo, como w' é uma palavra ciclicamente reduzida e tem como prefixo e sufixo a palavra t e portanto a palavra q' , temos que q' também é uma palavra ciclicamente reduzida. Finalmente, w''' é uma palavra ciclicamente reduzida pois w' e w''' são palavras conjugadas e w' é uma palavra ciclicamente reduzida. Como $|w'''| = |w'| \leq |(w')^{\gamma-1}| < |u|$, concluímos, por indução, que $r = \epsilon$ e $p = q' = q$ são potências de um mesmo elemento, que contradiz a hipótese de $v = (pq)^{k+1}p$ ser palavra primitiva. Logo, o caso $\alpha = 3$ é impossível.

2.1.2.2 Caso II: w é uma palavra ciclicamente reduzida

Escrevemos u na forma $u = \bar{r}u'r$ onde u' é uma palavra ciclicamente reduzida e r poderá ser a palavra vazia. A igualdade em G é representada em M pela igualdade

$$\bar{r}(u')^\alpha r = v^\beta w^\gamma \quad (2.8)$$

onde as palavras de ambos os membros são palavras reduzidas e u', v e w são palavras primitivas. Vamos mostrar que $r = \epsilon$ e $u' = v = w$. Para reduzirmos ao Caso I basta mostrar que $r = \epsilon$.

Se $|w^\gamma| \leq |r|$, então $r = sw^\gamma$ para algum s . Após cancelarmos o factor w^γ de cada membro, obtemos $\bar{w}^\gamma \bar{s}(u')^\alpha s = v^\beta$. Esta igualdade reduz-se ao Caso I e é verdadeira se e só se $\bar{w} = v$, o que contradiz a hipótese de $v^\beta w^\gamma$ ser uma palavra reduzida. Logo, podemos assumir que $|r| < |w^\gamma|$ e, por simetria, que $|r| < |v^\beta|$. Segue, pelo Lema 1.6, que

$$\begin{aligned} r &= \overline{v^{\beta_1} v_1} = w_2 w^{\gamma_2}, \\ (u')^{\alpha_1} u_1 &= v_2 v^{\beta_2}, \\ w^{\gamma_1} w_1 &= u_2 (u')^{\alpha_2} \end{aligned} \quad (2.9)$$

com $u' = u_1 u_2$, $v = v_1 v_2$, $w = w_1 w_2$, $\alpha_1 + \alpha_2 + 1 = \alpha$, $\beta_1 + \beta_2 + 1 = \beta$ e $\gamma_1 + \gamma_2 + 1 = \gamma$. Deste sistema podemos obter os dois seguintes:

$$\begin{aligned} r' &= \overline{(u')^{\alpha_1} u_1} = \overline{v_2} (\overline{v_1} \overline{v_2})^{\beta_2}, \\ w^{\gamma_1} w_1 &= u_2 (u')^{\alpha_2}, \\ (\overline{v_1} \overline{v_2})^{\beta_1} \overline{v_1} &= w_2 w^{\gamma_2} \end{aligned} \quad (2.10)$$

e

$$\begin{aligned} r'' &= \overline{\overline{w}^{\gamma_2} \overline{w_2}} = \overline{v_1} \overline{v}^{\beta_1}, \\ (\overline{u'})^{\alpha_2} \overline{u_2} &= \overline{w_1} \overline{w}^{\gamma_1}, \\ \overline{v}^{\beta_2} \overline{v_2} &= \overline{u_1} (\overline{u'})^{\alpha_1}. \end{aligned} \quad (2.11)$$

Portanto, a hipótese nos seis expoentes de que existem um elemento r e factorizações das palavras primitivas u', v e w que satisfazem o sistema (2.9) é simétrica à permutação cíclica dos pares (α_1, α_2) , (β_1, β_2) e (γ_1, γ_2) que nos conduz ao sistema (2.10) e também à troca do par (β_1, β_2) com (γ_1, γ_2) seguida da inversão dos três pares que nos conduz ao sistema (2.11).

Usando esta simetria reduzimos a discussão de (2.9) aos três casos:

Caso A: Uma das equações tem os expoentes nulos;

Caso B: $\alpha_1, \beta_1, \gamma_1 > 0$ ou $\alpha_2, \beta_2, \gamma_2 > 0$;

Caso C: Aqui tratamos o caso que resta. Evitando o Caso B, assumimos que $\beta_1 = 0$. Como $\beta_1 + \beta_2 + 1 \geq 2$, temos $\beta_2 \neq 0$. Para evitarmos o Caso A, assumimos que $\gamma_2 \neq 0$. Podemos assumir que $\alpha_2 = 0$ para excluirmos o Caso B e, como $\alpha_1 + \alpha_2 + 1 \geq 2$, temos $\alpha_1 \neq 0$. Finalmente fazemos $\gamma_1 \neq 0$ para evitar o Caso A. Obtemos $\beta_1 = \alpha_2 = 0$ e $\alpha_1, \beta_2, \gamma_1, \gamma_2 > 0$.

Estudemos então estes três casos:

Caso A: Suponhamos que os dois expoentes da primeira equação do sistema (2.9) são nulos. Obtemos a equação $r = \bar{v}_1 = w_2$. Então temos $v = \bar{r}v_2$ e $w = w_1r$ e substituindo na equação (2.8) e cancelando o primeiro $\bar{r}$ e o último r obtemos a equação

$$(u')^\alpha = (v_2\bar{r})^{\beta-1}v_2w_1(rw_1)^{\gamma-1}. \quad (2.12)$$

Se $|(v_2\bar{r})^{\beta-1}v_2| \geq |v_2\bar{r}| + |u'|$, segue do Corolário 1.13 que $u' = v_2\bar{r}$ visto que u' e $v_2\bar{r}$, que é uma palavra conjugada de v , são palavras primitivas. Como $\bar{r}u'r$ é uma palavra reduzida, então $r = \epsilon$.

Assumimos agora que

$$|(v_2\bar{r})^{\beta-2}v_2| < |u'|.$$

Se $|(v_2\bar{r})^{\beta-1}| = |u'|$, então temos $u' = (v_2\bar{r})^{\beta-1}$ e, como $\bar{r}u'r$ é uma palavra reduzida, $r = \epsilon$. Assumimos então que $u' \neq (v_2\bar{r})^{\beta-1}$. Vamos mostrar que a desigualdade $|u'| < |(v_2\bar{r})^{\beta-1}|$ é impossível. Esta desigualdade faz com que o primeiro factor u' de (2.12) tenha prefixo v_2 e o segundo tenha prefixo r_2v_2 para alguma factorização $\bar{r} = r_1r_2$ com $r_1, r_2 \neq \epsilon$ pois $|(v_2\bar{r})^{\beta-2}v_2| < |u'| < |(v_2\bar{r})^{\beta-1}|$. Pelo Lema 1.7, como $v_2 \cdots = r_2v_2$, temos $v_2 = (pq)^k p$ como factor de uma potência de $r_2 = pq$. Assim, existe um conjugado u'' de u' tal que

$$(u'')^\alpha = (\bar{r}v_2)^{\beta-1}w_1(rw_1)^{\gamma-1}v_2.$$

Pelo Lema 1.21 resulta que existem $s, t \in M$ tais que $u'' = \bar{r}srt$ e, como

$$|u''| = |u'| < |(v_2\bar{r})^{\beta-1}| = |(\bar{r}v_2)^{\beta-1}|,$$

concluimos, pelo Lema 1.18, que r é factor de v_2 . Mais ainda, como $\bar{r}_2$ é factor de $r = \bar{r}_2 \bar{r}_1$, r é factor de v_2 e v_2 é factor de uma potência de r_2 , temos que $\bar{r}_2$ é factor de uma potência de r_2 que, pelo Corolário 1.20, contradiz a hipótese de $r_2 \neq \epsilon$. Assim, podemos, por simetria, assumir que

$$|(v_2\bar{r})^{\beta-1}| < |u'| \text{ e } |(rw_1)^{\gamma-1}| < |u'|. \quad (2.13)$$

Resulta que $(u')^{\alpha-2}$ é factor de v_2w_1 . Por (2.13) temos que $|v_2|, |w_1| < |u'|$ e portanto $|v_2w_1| < 2|u'|$. Segue que $\alpha - 2 < 2$, ou seja, $\alpha = 2$ ou $\alpha = 3$.

Se $\alpha = 2$, supomos, por simetria, que

$$|(v_2\bar{r})^{\beta-1}v_2| \geq |w_1(rw_1)^{\gamma-1}|.$$

Resulta que $(v_2\bar{r})^{\beta-1}v_2 = u_1u_2u_1$ e $u_2 = w_1(rw_1)^{\gamma-1}$ com $u' = u_1u_2$. Logo, $(v_2\bar{r})^\beta = u_1w_1(rw_1)^{\gamma-1}u_1\bar{r}$ e $(v')^\beta = (u_1\bar{r})^1u_1w_1(rw_1)^{\gamma-1}$ onde v' é uma palavra conjugada de v (visto que v e $v_2\bar{r}$ são palavras conjugadas). Como esta equação é da forma (2.12) com $|v'| = |v_2r| < |u'|$, concluímos, por indução sobre $|u'|$, que $r = \epsilon$.

Se $\alpha = 3$, então β e γ não podem ser ambos superiores a 2 senão, por (2.13), teríamos $2|v_2|, 2|w_1| < |u'|$ e, como $(u')^{\alpha-2} = u'$ é factor de v_2w_1 , obteríamos

$$|v_2| + |w_1| < |u'| \leq |v_2w_1|.$$

Por simetria, suponhamos que $\beta = 2$. De (2.12) obtemos

$$(u')^3 = v_2\bar{r}v_2w_1(rw_1)^{\gamma-1}.$$

Resulta que existem factorizações $v_2 = v_3v_4$ e $w_1 = w_3w_4$ com $v_3, w_4 \neq \epsilon$ tais que

$$u' = v_2\bar{r}v_3 = v_4w_3 = w_4(rw_1)^{\gamma-1}.$$

Como $v_2 = v_3v_4$ e v_4 são prefixos de u' , segue do Lema 1.7 que $v_3 = pq$ e $v_4 = (pq)^k p$ para alguns $p, q \in M$ e $k \geq 0$. Assim, $v_2\bar{r}v_3 = v_3v_4\bar{r}v_3 = v_4w_3$ implica que $w_3 = qp\bar{r}pq$ e $v_4w_3 = w_4(rw_1)^{\gamma-1}$ implica que $w_3v_4w_3 = w_1(rw_1)^{\gamma-1}$ e portanto

$$w_1(rw_1)^{\gamma-1} = qp\bar{r}(pq)^{k+2}p\bar{r}pq.$$

Como $|w_1| > |w_3| = |qp\bar{r}pq|$, existe $h \geq 1$ e uma factorização $pq = t_1t_2$ com $t_1 \neq \epsilon$ tais que a primeira ocorrência de w_1 na expressão $w_1(rw_1)^{\gamma-1}$ tem a forma $w_1 = qp\bar{r}(pq)^h t_1$. Assim, $t_1t_2t_1$ e $\bar{r}pq$ são sufixos de w_1 . Como $|t_2t_1| = |pq|$, resulta que, se $r \neq \epsilon$, $\bar{r}$ termina com a mesma letra que t_1 e, consequentemente, com a mesma letra que w_1 , contradizendo a hipótese de w_1r ser uma palavra reduzida. Logo, $r = \epsilon$.

Caso B: Assumimos que $\alpha_1, \beta_1, \gamma_1 \neq 0$ e, permutando ciclicamente os elementos do sistema, assumimos também que $|w| \leq |u'|$. Da igualdade

$$w^{\gamma_1}w_1 = u_2(u')^{\alpha_2} \quad \text{com } \gamma_1 \neq 0$$

concluimos que w é prefixo de $(u_2u_1)^{\alpha_2+1}$ e, como $|w| \leq |u'| = |u_2u_1|$, w é prefixo de u_2u_1 . Da igualdade

$$(u')^{\alpha_1}u_1 = v_2v^{\beta_2} \quad \text{com } \alpha_1 \neq 0$$

concluimos que u_2u_1 é sufixo de v^{β_2+1} e portanto w é factor de v^{β_2+1} . Da igualdade

$$v^{\beta_1}v_1 = \bar{w}^{\gamma_2}\bar{w}_2 \quad \text{com } \beta_1 \neq 0$$

resulta que v é prefixo de $\bar{w}^{\gamma_2+1}$, ou seja, existe uma factorização $\bar{w} = t_1t_2$ tal que $v = (t_1t_2)^\delta t_1$ com $t_1 \neq \epsilon$ e $0 \leq \delta \leq \gamma_2$. Assim, o factor w de v^{β_2+1} tem como sufixo um prefixo $s_1 \neq \epsilon$ de $\bar{w}$, ou seja, $w = s_3s_1$ e $\bar{w} = s_1s_2$ para alguns s_2 e s_3 . Resulta que $w = s_3s_1 = \bar{s}_2\bar{s}_1$ e portanto $s_1 = \bar{s}_1$ o que é impossível pelo Lema 1.15 pois $s_1 \neq \epsilon$ e s_1 é uma palavra reduzida visto $\bar{w}$ ser uma palavra reduzida. Logo, o Caso B é impossível.

Caso C: Temos $\alpha_2 = \beta_1 = 0$ e $\alpha_1, \beta_2, \gamma_1, \gamma_2 > 0$. O sistema (2.9) tem a forma

$$\begin{aligned} v_1 &= \overline{w}^{\gamma_2} \overline{w}_2, \\ (u')^{\alpha_1} u_1 &= v_2 v^{\beta_2}, \\ u_2 &= w^{\gamma_1} w_1. \end{aligned} \quad (2.14)$$

Se u_2 é factor de v_1 , então w , que é factor de u_2 , é também factor de v_1 . Logo, pela primeira igualdade, w é factor de uma potência de $\overline{w}$. Pelo Corolário 1.20 temos $w = \epsilon$. Concluimos, por simetria, que nem u_2 nem v_1 são factores um do outro. Se tivermos $|(u')^{\alpha_1} u_1| = |v_2 v^{\beta_2}| \geq |u'| + |v|$, então, pelo Corolário 1.13, resulta que $u_1 u_2 = v_2 v_1$ e portanto ou u_2 ou v_1 é factor do outro. Logo, $|(u')^{\alpha_1} u_1| = |v_2 v^{\beta_2}| < |u'| + |v|$. Por simetria, assumimos que $|v| \leq |u'|$. Logo, $|(u')^{\alpha_1} u_1| < 2|u'|$ e portanto $\alpha_1 = 1$. Obtemos $|u_1 u_2 u_1| < |u'| + |v|$ e portanto $|u_1| < |v|$. Se $\beta_2 = 1$, então segue da igualdade $u_1 u_2 u_1 = v_2 v_1 v_2$ que u_2 é factor de v_1 ou v_1 é factor de u_2 . Se $\beta_2 > 2$, então da igualdade $u_1 u_2 u_1 = v_2 v^{\beta_2} = v_2 v_1 v_2 v^{\beta_2-2} v_1 v_2$ e como $|u_1| < |v|$, resulta que $(v_2 v_1)^{\beta_2-2} v_2$ é factor de u_2 e portanto v_1 é factor de u_2 . Concluimos que $\beta_2 = 2$ e portanto temos a igualdade

$$u_1 u_2 u_1 = v_2 v_1 v_2 v_1 v_2. \quad (2.15)$$

Como $|u_1| < |v| = |v_2 v_1|$, resulta que $|u_2| > |v_2|$ e ainda que $u_2 = s_1 v_2 s_2$ com $|s_1| = |s_2|$. Obtemos de (2.15) que $u_1 s_1 = v_2 v_1$ e $s_2 u_1 = v_1 v_2$. Como v_1 não é factor de $u_2 = s_1 v_2 s_2$, então v_1 não é factor de s_1 e, como $u_1 s_1 = v_2 v_1$, temos $|s_1| < |v_1|$. Como $|s_2| = |s_1| < |v_1|$ e $s_2 u_1 = v_1 v_2$, resulta que s_2 é prefixo de $v_1 = \overline{w}^{\gamma_2} \overline{w}_2$. Se $|w| \leq |s_2|$, então $\overline{w}$ é prefixo de s_2 que, como s_2 é factor de $u_2 = w^{\gamma_1} w_1$, contradiz o Corolário 1.20. Concluimos que $|s_1| = |s_2| < |w|$. Assim sendo, como $u_2 = s_1 v_2 s_2 = w^{\gamma_1} w_1$ e $s_1 v_2 s_2 < s_1 v_2 v_1$, temos w como prefixo de $s_1 v_2 v_1$ pois $\gamma_1 > 0$. Por outro lado, $s_2 v_2 v_1 = s_2 u_1 s_1 = v_1 v_2 s_1$ tem prefixo $\overline{w}$ pois $\gamma_2 > 0$. Como $|s_1| = |s_2| < |w|$, existe um prefixo s de $v_2 v_1$, com $s \neq \epsilon$, tal que $w = s_1 s$ e $\overline{w} = s_2 s$. Isto implica que $w = s_1 s = \overline{s} \overline{s}_2$ que contradiz a hipótese de w ser uma palavra ciclicamente reduzida.

2.2 A equação $x^{-1}y^{-1}xy = z^n$

Schützenberger [30] mostra também que a equação

$$x^{-1}y^{-1}xy = z^n \quad (2.16)$$

tem como únicas soluções as soluções triviais, ou seja, soluções que geram um grupo cíclico. Nesta secção apresentamos a prova do mesmo resultado obtida por Baumslag [5]:

Seja $n > 1$. Então um comutador num grupo livre é uma potência de ordem n se e só se é a identidade.

Seja F um grupo livre não-Abeliano e suponhamos que existe um elemento não-trivial $f \in F$ tal que

$$f^n = [g, h],$$

com $g, h \in F$.

Notemos que $f = f_1 f_2 \overline{f_1}$, onde f_1, f_2 são palavras e f_2 é uma palavra ciclicamente reduzida não-trivial, representa o elemento do grupo. Assim, $f^n \equiv f_1 f_2^n \overline{f_1}$, onde $\equiv$ representa a igualdade no grupo F , é não-trivial para todo o $n \neq 0$ visto que f_2^n é uma palavra ciclicamente reduzida não-trivial. Isto mostra que $f^n \neq 1$ e F é localmente infinito. Resulta que g e h não comutam.

Consideremos agora o subgrupo G de F gerado por f, g e h :

$$G = \langle f, g, h \rangle.$$

Pelo Teorema de Nielsen-Schreier temos que G é um grupo livre visto ser um subgrupo do grupo livre F . Pelo Lema 1.22 temos que G/G' é um grupo livre Abelian de característica m , onde m é a característica de G .

Notemos que $G/G' \simeq \mathbb{Z}^m$ e portanto, se $(f_1, \dots, f_m) \in \mathbb{Z}^m$ é tal que $n(f_1, \dots, f_m) = (0, \dots, 0)$, então $(f_1, \dots, f_m) = (0, \dots, 0)$. Como $f^n \in G'$, resulta que

$$(fG')^n = fG' \dots fG' = f^n G' = G'$$

e portanto $fG' = G'$, ou seja, $f \in G'$. Logo, G/G' tem característica 2 e é gerado por gG' e hG' :

$$G/G' = \langle gG', hG' \rangle.$$

Consequentemente, G tem também característica 2. Notemos que G não pode ter característica 1 senão seria cíclico e, consequentemente, Abelian, contradizendo o facto de g e h não comutarem.

Vamos agora mostrar que existem dois elementos g^* e h^* que geram G e tais que $g^*G' = gG'$ e $h^*G' = hG'$. Sejam g_1 e g_2 dois elementos que geram livremente G . Consideremos o homomorfismo natural $G \rightarrow G/G'$ e o automorfismo φ de G/G' que envia g_1G' em gG' e g_2G' em hG' . Queremos mostrar que existe um automorfismo $\tilde{\varphi}$ de G que torna o diagrama seguinte comutativo:

$$\begin{array}{ccc} G & \longrightarrow & G/G' \\ \exists \tilde{\varphi} \downarrow & & \downarrow \varphi \\ G & \longrightarrow & G/G' \end{array} \quad (2.17)$$

Para isso, basta mostrar que o homomorfismo natural de grupos

$$\text{Aut } G \rightarrow \text{Aut } G/G'$$

é sobrejectivo. Note-se que, para todo o grupo H , $\text{Aut } H$ equipado com a operação de composição é um grupo. Como G/G' tem característica 2, temos que $G/G' \simeq \mathbb{Z}^2$.

Notemos que

$$\text{Aut } \mathbb{Z}^2 = \left\langle \psi_x = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \varphi_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \varphi_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} : x \in \mathbb{Z} \right\rangle.$$

A $\varphi_i, \psi_x \in \text{Aut } G/G'$ com $i \in \{1, 2\}$ e $x \in \mathbb{Z}$ correspondem automorfismos $\tilde{\varphi}_i$ e $\tilde{\psi}_x$ de G definidos por:

$$\begin{array}{lll} \tilde{\psi}_x : G \rightarrow G & , & \tilde{\varphi}_1 : G \rightarrow G \quad \text{e} \quad \tilde{\varphi}_2 : G \rightarrow G \\ g_1 \mapsto g_1 & & g_1 \mapsto g_2 \quad \quad \quad g_1 \mapsto g_1^{-1} \\ g_2 \mapsto g_1^x g_2 & & g_2 \mapsto g_1 \quad \quad \quad g_2 \mapsto g_2. \end{array}$$

O automorfismo φ de G/G' é um produto de $\varphi_i, \varphi_i^{-1}, \psi_x$ e ψ_x^{-1} com $i \in \{1, 2\}$ e $x \in \mathbb{Z}$. A este produto corresponde o produto de $\tilde{\varphi}_i, \tilde{\varphi}_i^{-1}, \tilde{\psi}_x$ e $\tilde{\psi}_x^{-1}$ com $i \in \{1, 2\}$ e $x \in \mathbb{Z}$ que define um automorfismo $\tilde{\varphi}$ de G tal que o diagrama (2.17) comuta. Resulta que

$$g^* = gg' \quad \text{e} \quad h^* = hh' \quad \text{com} \quad g', h' \in G'. \quad (2.18)$$

Pelo Teorema 1.24 temos que, se um grupo livre de característica m é gerado por m elementos, então estes m elementos constituem um conjunto de geradores livres. Assim, g^* e h^* constituem um conjunto de geradores livres de G .

Seja agora H o grupo nilpotente de classe 2 definido do seguinte modo:

$$H = \langle a, b \mid a^{n^2} = b^{n^2} = 1, [a, b] = a^n = b^n \rangle.$$

Temos ainda que o centro de H , $Z(H)$, coincide com o seu derivado, H' , e tem ordem n . Vejamos que estas propriedades se verificam.

Pelo Lema 1.25 resulta que, no grupo H ,

$$[a^2, b] = [a, b]^a [a, b] = (a^n)^a a^n = a^{2n}$$

e, por indução sobre k , obtemos

$$[a^k, b] = [a^{k-1}, b]^a [a, b] = (a^{(k-1)n})^a a^n = a^{kn}.$$

Resulta que

$$[a^n, b] = a^{n^2} = 1.$$

Concluimos que a^n comuta com b e, trivialmente, com a . Como estes dois elementos são geradores de H resulta que

$$a^n = [a, b] \in Z(H).$$

Vamos mostrar que, para todos os $u, v \in H$, temos $[u, v] \in \langle a^n \rangle = \langle b^n \rangle$. Procedemos por indução sobre o comprimento mínimo das palavras que representam u e v . A base de indução é óbvia. Se $|u| = |v| = 1$, então $u, v \in \{a, b\}$ (note-se que a^{-1} e b^{-1} podem

ser escritas como potências positivas de a e b , respectivamente, pois $a^{n^2} = b^{n^2} = 1$). Temos

$$[a, a] = 1, \quad [b, b] = 1, \quad [a, b] = a^n \quad \text{e} \quad [b, a] = [a, b]^{-1} = (a^n)^{-1}$$

e portanto $[u, v] \in \langle a^n \rangle$. Por simetria, seja $u = u_1 u_2$ com u_1, u_2 palavras não-triviais. Então temos

$$\begin{aligned} [u, v] &= [u_1 u_2, v] \\ &= [u_1, v]^{u_2} [u_2, v]. \end{aligned}$$

Por hipótese de indução, os comutadores $[u_i, v]$ com $i \in \{1, 2\}$ são potências de $a^n \in Z(H)$. Resulta que a conjugação destes comutadores por qualquer elemento é a identidade e portanto $[u, v] \in \langle a^n \rangle$.

Concluimos que $H' \leq Z(H)$ e portanto H é nilpotente de classe 2. Mais ainda, temos que $H' = \langle a^n \rangle$ tem ordem n . Falta mostrar que $Z(H) \leq H'$. Temos

$$[a, b] = a^n \Leftrightarrow a^{-1} b^{-1} a b = a^n \Leftrightarrow a b = b a^{n+1}.$$

Resulta que todo o elemento de H pode ser escrito na forma $b^i a^j$ para alguns i, j . Suponhamos que $u = b^i a^j \in Z(H)$. Então $[u, a] = [u, b] = 1$. Notemos que

$$\begin{aligned} [b^i a^j, a] &= [b^i a^{j-1}, a]^a [a, a] \\ &= [b^i a^{j-1}, a] \\ &= \dots \\ &= [b^i, a] \\ &= [b^{i-1}, a]^b [b, a] \\ &= \dots \\ &= [b, a]^i \end{aligned}$$

pois os comutadores são elementos centrais. Resulta que

$$[b^i a^j, a] = [b, a]^i = a^{-in} = 1,$$

e, de modo análogo,

$$[b^i a^j, b] = [a, b]^j = a^{jn} = 1$$

e portanto, como a^n tem ordem n , temos que i e j são divisíveis por n . Logo, como $a^n = b^n \in H'$, resulta que u é um produto de comutadores e portanto $u \in H'$.

Seja ψ o homomorfismo de G em H definido por

$$\psi(g^*) = a \quad \text{e} \quad \psi(h^*) = b.$$

Segue de (2.18) e do facto de $H' = Z(H)$ que

$$\begin{aligned}
\psi([g, h]) &= \psi([g^* g'^{-1}, h^* h'^{-1}]) \\
&= [\psi(g^*)\psi(g')^{-1}, \psi(h^*)\psi(h')^{-1}] \\
&= [a\psi(g')^{-1}, b\psi(h')^{-1}] \\
&= \psi(g')a^{-1}\psi(h')b^{-1}a\psi(g')^{-1}b\psi(h')^{-1} \\
&= a^{-1}b^{-1}ab \\
&= [a, b]
\end{aligned}$$

visto que, como ψ é sobrejectiva, $\psi(G') = \psi([G, G]) = [\psi(G), \psi(G)] = [H, H] = H' = Z(H)$.

Como $f^n = [g, h]$ e $\psi(f^n) = \psi([g, h]) = [a, b] \neq 1$, resulta que $\psi(f^n)$ tem ordem n . No entanto, $f \in G'$ e, consequentemente, a sua imagem por ψ está em H' . Mas H' tem ordem n e portanto

$$\psi(f^n) = (\psi(f))^n = 1.$$

Logo, $\psi(f^n)$ é simultaneamente um elemento de ordem n e um elemento de ordem 1, o que é impossível. Portanto, f^n não pode ser um comutador.

2.3 A generalização de Baumslag

Em 1965, G. Baumslag [6] obtém uma generalização de todos estes resultados no seguinte teorema:

Teorema 2.1. Seja $w = w(x_1, x_2, \dots, x_n)$ um elemento de um grupo livre F livremente gerado por $x_1, x_2, \dots, x_n$ que não é uma potência própria nem um elemento básico. Se $g_1, g_2, \dots, g_n, g$ são elementos de um grupo livre ligados pela relação

$$w(g_1, g_2, \dots, g_n) = g^m \quad \text{com } m > 1,$$

então a característica do grupo gerado por $g_1, g_2, \dots, g_n, g$ é menor ou igual a $n - 1$.

Um elemento $f \in F$ diz-se um *elemento básico* se estiver contido em algum conjunto de geradores livres de F . No artigo de Baumslag bem como na linguagem da Teoria de Grupos é usado o termo *primitivo*. Optamos pela designação anterior para que não haja confusão com a definição de *palavra primitiva* que é usada no decorrer desta monografia.

Resulta, em particular, que nas condições do teorema anterior e fazendo $n = 2$, qualquer equação da forma

$$w(x, y) = z^m \quad \text{com } m > 1$$

possui como únicas soluções elementos de um grupo cíclico desde que $w(x, y)$ não seja uma potência própria nem um elemento básico do grupo livre em $\{x, y\}$.

Assim, se mostrarmos que $x_1^\alpha x_2^\beta$ com $\alpha, \beta \geq 2$ e $x_1^{-1} x_2^{-1} x_1 x_2$ não são potências próprias nem elementos básicos, onde x_1 e x_2 são geradores livres de um grupo livre F , então obtemos os resultados das Secções 2.1 e 2.2. É óbvio que não se tratam de potências próprias. Quanto a serem elementos básicos a conclusão não é simples. Magnus, Karrass e Solitar [20, p. 121] afirmam que é extremamente difícil decidir se uma dada palavra é um elemento básico. Num artigo posterior, Cohen, Metzler e Zimmermann [7] respondem à nossa questão provando, entre outros, os lemas seguintes:

Lema 2.2 (Nielsen). Suponhamos que $w = x^{\alpha_1} y^{\beta_1} \dots x^{\alpha_q} y^{\beta_q}$ é um elemento básico do grupo livre em x e y , onde $q \geq 2$ e os expoentes indicados são não-nulos. Então todos os expoentes α_i com $1 \leq i \leq q$ têm o mesmo sinal e todos os expoentes β_i com $1 \leq i \leq q$ têm o mesmo sinal.

Resulta do Lema de Nielsen que $x_1^{-1} x_2^{-1} x_1 x_2$ não é um elemento básico.

Lema 2.3. Suponhamos que $w = x^{\alpha_1} y^{\beta_1} \dots x^{\alpha_q} y^{\beta_q}$ é um elemento básico do grupo livre em x e y , onde $q \geq 1$ e todos os expoentes são não-nulos. Assumimos que $\alpha_1 > 1$ e $\beta_1 > 0$. Então $\beta_1 = \beta_2 = \dots = \beta_q = 1$.

Resulta do lema anterior que $x_1^\alpha x_2^\beta$ com $\alpha, \beta \geq 2$ não é um elemento básico.

Em conclusão, neste capítulo ficamos a conhecer um conjunto de equações no grupo livre para as quais conseguimos identificar o seu conjunto de soluções.

Capítulo 3

O Algoritmo de Makanin para equações no monóide livre

Enunciando a decidibilidade de um sistema de equações de palavras, Makanin [21] apresenta um algoritmo de decisão que, sem perda de generalidade, soluciona o problema para uma única equação.

Neste capítulo basear-nos-emos numa exposição de Volker Diekert [17] acerca do trabalho de Makanin apresentando um algoritmo para a resolução de sistemas de equações no semigrupo livre.

Volker Diekert no seu “*Makanin’s Algorithm*” faz uma exposição com tudo o que é necessário do famoso teorema de Makanin. Inspirado em Schulz [32] mostra o resultado de Makanin de um modo mais generalizado:

Dada uma equação $E = D$ e uma lista de linguagens racionais $L_x \subseteq A^*$ onde $x \in \Omega$ é uma incógnita e A é o alfabeto das constantes, é decidível a existência de uma solução $\sigma : \Omega \rightarrow A^*$ que, além de $\sigma(E) = \sigma(D)$, satisfaz as restrições racionais $\sigma(x) \in L_x$ para todo o $x \in \Omega$.

Usando um ponto de vista algébrico, restrições racionais levam ao trabalho num semigrupo finito mas não será necessário nenhum resultado profundo nesta teoria e a prova do resultado de Makanin não será mais complicada.

Na Secção 3.1 iniciamos o nosso estudo apresentando um algoritmo muito simples para a resolução de um grupo especial de sistemas de equações, onde cada variável ocorre no máximo duas vezes.

A redução do problema numa fórmula proposicional de equações ao problema numa única equação é feita na Secção 3.2. Aqui também é feita a redução do problema numa equação num alfabeto com cardinal arbitrário ao problema numa equação num alfabeto de duas letras.

O resto do capítulo é dedicado à construção do Algoritmo. Na Secção 3.3 introduzimos as noções de torre dominó, expoente de periodicidade, formas normais estáveis e escolhemos um semigrupo e um homomorfismo de semigrupos que nos permitirão solucionar a equação satisfazendo as restrições racionais. Na Subsecção 3.3.3 mostramos ainda que, se houver unicamente uma variável na equação, então uma descrição paramétrica do conjunto de todas as soluções pode ser calculada em tempo polinomial. Na Secção 3.4 calculamos um majorante para o expoente de periodicidade e explicamos que este majorante por si só não soluciona o nosso problema de decidibilidade. É então que passamos à construção de um sistema de equações fronteira (Secção 3.5), definimos as regras de transformação para estes sistemas (Secção 3.8) e construímos o *grafo de procura* do Algoritmo de Makanin. Na Secção 3.7 definimos cadeia convexa e condição da cadeia convexa que, juntamente com o majorante calculado na Secção 3.4, produzirá um majorante que irá garantir a paragem do Algoritmo: ou fornecendo uma solução, ou respondendo *não* à existência desta. Nas Secções 3.6 e 3.9 fundamentamos toda a estratégia da resolução do problema.

O algoritmo que aqui apresentamos pode ser implementado em espaço exponencial. Embora não seja óptimo para a resolução do problema, visto Plandowski (1999) ter mostrado que tal resultado pode ser decidido em espaço polinomial (PSPACE), resultados experimentais indicam que o algoritmo de Makanin é bastante apropriado para aplicações práticas. Um ingrediente importante no trabalho de Plandowski é o uso de dados comprimidos em expressões exponenciais (por exemplo: usa $a(aba)^3ab$ em vez de $aabaabaabaab$). Makanin, não fazendo uso disso, escrevendo todas as equações por extenso torna mais fácil o seguimento de uma estratégia durante a procura de solução.

3.1 Sistemas quadráticos: um algoritmo de decisão

Dizemos que

$$f(n) \in \mathcal{O}(g(n)) \text{ se e só se } \exists c, \exists n_0, \forall n \geq n_0, |f(n)| \leq c|g(n)|.$$

Consideremos uma sucessão $\mathcal{S}_1, \mathcal{S}_2, \dots$ de sistemas quadráticos onde $\mathcal{S}_n = \{E_{n1} = D_{n1}, \dots, E_{nk} = D_{nk}\}$. Seja $\|\mathcal{S}_n\| = \sum_{i=1}^k |E_{ni}D_{ni}|$ o *comprimento notacional* de $\mathcal{S}_n$. Seja $g(n) = \|\mathcal{S}_n\|$. Usando indução sobre $|\Omega|$ descrevemos um algoritmo de decisão não-determinístico que soluciona a questão da existência de solução em espaço $f(n) \in \mathcal{O}(\|\mathcal{S}_n\|)$:

O caso $\Omega = \emptyset$ é trivial.

Seja $\Omega \neq \emptyset$. O primeiro passo consiste em procurar a existência de uma solução singular de $\mathcal{S}$, ou seja, de uma solução $\sigma : \Omega \rightarrow A^*$ tal que $\sigma(x) = \epsilon$ para algum $x \in \Omega$. Para isso, escolhemos, de um modo não-determinístico, algum $\Omega' \subseteq \Omega$ e substituímos todas as ocorrências de $x \in \Omega'$ pela palavra vazia. Obtemos assim um

novo sistema $\mathcal{S}'$ nas variáveis $\Omega \setminus \Omega'$ e, recursivamente, se $\Omega' \neq \emptyset$, decidimos, em espaço linear não-determinístico, se $\mathcal{S}'$ tem solução. Posto isto, procuramos somente as soluções não-singulares de $\mathcal{S}$. Consideremos a primeira equação. Se for da forma $a_1 \cdots = a_2 \cdots$ com $a_1, a_2 \in A$, então teremos um dos seguintes casos: ou $a_1 \neq a_2$ e portanto a equação não terá solução e por conseguinte o sistema não será solúvel, ou $a_1 = a_2$ e então o conjunto de soluções desta equação é igual ao conjunto de soluções da equação que resulta de retirarmos a primeira letra de cada membro da equação. Procedemos deste modo até que a equação tenha uma das formas

$$\begin{aligned} x \cdots &= a \cdots && \text{com } x \in \Omega, a \in A \\ \text{ou } x \cdots &= y \cdots && \text{com } x \in \Omega, y \in \Omega, x \neq y. \end{aligned}$$

Por simetria, podemos escrever $x = az$ ou $x = yz$ onde z é uma nova variável. Substituindo as ocorrências de x por az ou yz e cancelando a ou y respectivamente, obtemos um novo sistema sem a variável x e onde z aparece no máximo duas vezes. Estamos em presença de um novo sistema quadrático $\mathcal{S}'$ onde o número de variáveis se manteve e $\|\mathcal{S}'\| \leq \|\mathcal{S}\|$.

É claro que, se $\mathcal{S}$ tem solução não-singular, então $\mathcal{S}'$ é solúvel podendo ter a solução singular $\sigma(z) = \epsilon$. De qualquer modo, se $\mathcal{S}'$ é solúvel, então $\mathcal{S}$ também é solúvel.

Seja agora $\sigma : \Omega \rightarrow A^*$ uma solução não-singular de $\mathcal{S}$ onde $\sum_{x \in \Omega} |\sigma(x)|$ é mínimo. Procuramos uma solução $\sigma' \in \mathcal{S}'$ com $|\sigma'(z)| < |\sigma(x)|$ visto que $\sigma(y) \neq \epsilon$ pois supusemos que as soluções de $\mathcal{S}$ são não-singulares. Assim sendo, o comprimento de uma solução mínima diminuiu. Usamos os mesmos processos no sistema $\mathcal{S}'$ e sucessivamente nos novos sistemas que são obtidos. O processo pára: ou obtemos uma equação trivial e portanto a solução está determinada, ou chegamos a uma equação impossível, ou ainda entramos num ciclo fechado e, pelo facto dos comprimentos das soluções estarem a diminuir, temos a garantia de, a dada altura, como a solução terá de ser a palavra vazia, obtermos uma equação impossível. Isto mostra que um processo não-determinístico encontrará uma solução, se ela existir.

O espaço requerido para este algoritmo é linear mas a sua complexidade temporal poderá ser exponencial.

Exemplo 3.1. Corremos o algoritmo para o Exemplo 1.5. Nas duas figuras que se seguem vemos duas partes do algoritmo. As arestas são etiquetadas de tal modo que possamos reconstruir uma solução percorrendo um caminho que se inicie na equação inicial e finalize numa equação trivial.

Na Figura 3.1 visualizamos o que acontece no primeiro passo, quando procuramos uma solução singular. Obtemos uma equação impossível, ou entramos num ciclo fechado. Como o comprimento das soluções está a diminuir a dada altura temos de fazer $\sigma(y_i) = \epsilon$ conduzindo a uma equação impossível.

Na Figura 3.2 omitimos todos os vértices e arestas que não levam a nenhuma solução. Assim, correndo este algoritmo, podemos encontrar qualquer solução desta equação.

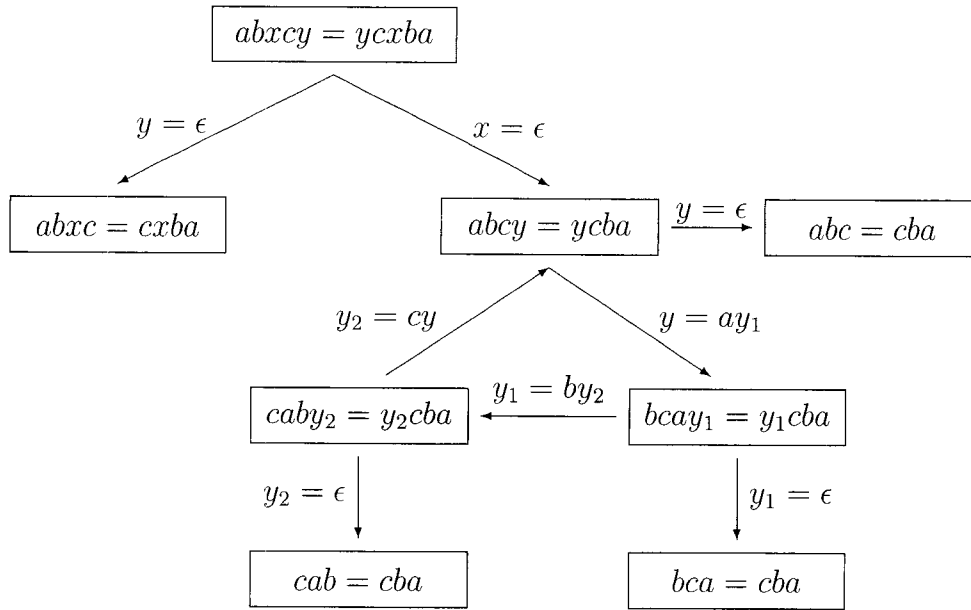


Figura 3.1: A procura de soluções singulares da equação $abxcy = ycxba$

Um dos caminhos tem a etiqueta

$$y = ay_1 \quad y_1 = by_2 \quad x = y_2x_1 \quad x_1 = \epsilon \quad y_2 = ay_3 \quad y_3 = \epsilon$$

que corresponde à solução minimal

$$\sigma(x) = a \quad \sigma(y) = aba.$$

Seguindo um outro caminho

$$y = ay_1 \quad y_1 = by_2 \quad y_2 = xy_3 \quad y_3 = \epsilon \quad x = ax_1 \quad x_1 = \epsilon$$

obtemos a mesma solução (embora haja caminhos que não conduzem a ela).

3.2 A teoria existencial da concatenação

A teoria existencial das equações no monóide livre é decidível, ou seja, a solubilidade de uma dada fórmula proposicional cujos elementos proposicionais elementares são equações (com restrições racionais) é decidível.

Isto pode ser deduzido do algoritmo de Makanin, que soluciona o problema para uma única equação, como se segue. Em primeiro lugar, assumimos que todas as negações de uma dada fórmula são do tipo $E \neq D$. Pela proposição seguinte essas negações podem ser eliminadas.

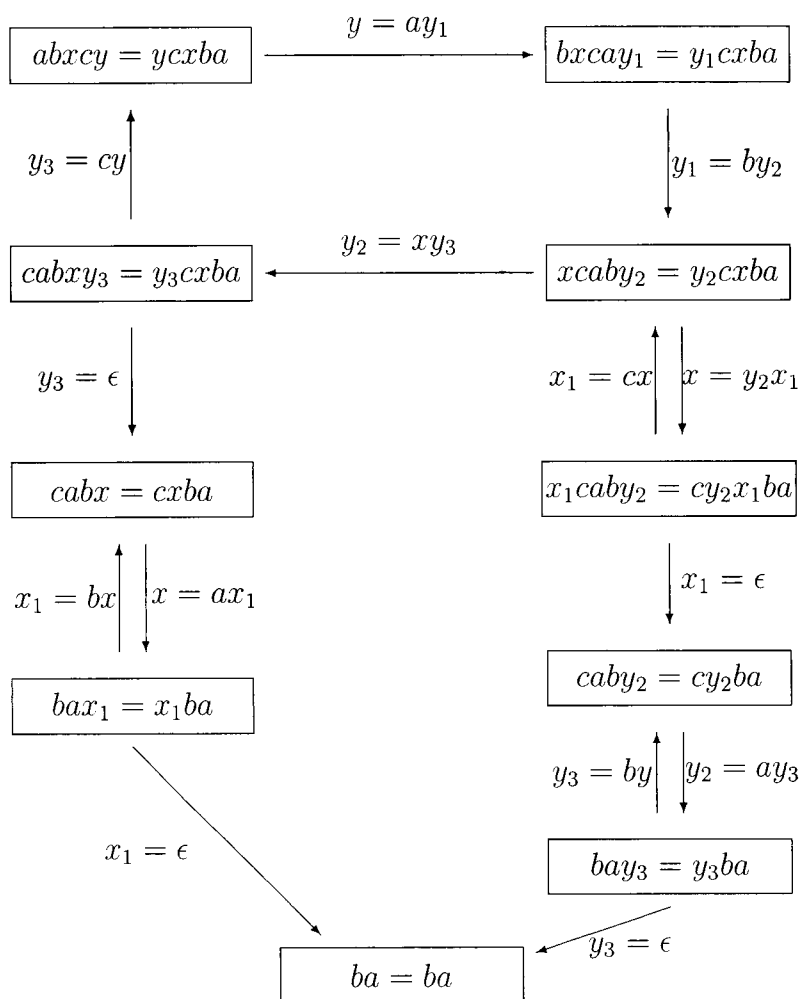


Figura 3.2: Algoritmo que fornece as soluções da equação $abxcy = ycxba$

Proposição 3.2. *Uma desigualdade $E \neq D$ é equivalente à seguinte fórmula existencial:*

$$\exists x \exists y \exists z : \bigvee_{a \in A} (E = Dax \vee D = Eax) \vee \bigvee_{a, b \in A, a \neq b} (E = xay \wedge D = xbz).$$

Demonstração. Na primeira disjunção temos uma das palavras como prefixo da outra. Na segunda disjunção consideram-se todos os restantes casos: quando as palavras E e D têm um prefixo comum ou, fazendo $x = \epsilon$, como $a \neq b$, obtemos E e D sem prefixos comuns. $\square$

Depois de eliminadas as negações temos uma fórmula escrita somente com disjunções e conjunções. Assim sendo, para a sua solubilidade, é suficiente ver se um sistema de equações pode ser transformado numa única equação. O método é dado na proposição seguinte:

Proposição 3.3. *Sejam $a, b \in A$ com $a \neq b$ e $\mathcal{S} = \{E_1 = D_1, \dots, E_k = D_k\}$ um sistema de equações. Então o conjunto de soluções de $\mathcal{S}$ é idêntico ao conjunto de soluções da seguinte equação:*

$$E_1 a \cdots E_k a E_1 b \cdots E_k b = D_1 a \cdots D_k a D_1 b \cdots D_k b.$$

Demonstração. Sejam $u, v \in A^*$ e $a, b \in A$ com $a \neq b$. Se $ua \leq va$ e $ub \leq vb$, então na posição $|u| + 1$ de va temos a letra a e na posição $|u| + 1$ de vb temos a letra b . Como $a \neq b$ resulta que $u = v$.

Temos $E_1 a \cdots E_k a = D_1 a \cdots D_k a$ e $E_1 b \cdots E_k b = D_1 b \cdots D_k b$ visto que $|E_1 a \cdots E_k a| = |E_1 b \cdots E_k b|$ e $|D_1 a \cdots D_k a| = |D_1 b \cdots D_k b|$. Usamos a observação anterior. Supondo, sem perda de generalidade, que $|E_1| \leq |D_1|$ temos $E_1 a \leq D_1 a$ e $E_1 b \leq D_1 b$ e portanto $E_1 = D_1$. Resulta que $E_2 a \cdots E_k a = D_2 a \cdots D_k a$ e $E_2 b \cdots E_k b = D_2 b \cdots D_k b$. Usando o mesmo processo $k - 2$ vezes obtemos o sistema inicial. $\square$

Por vezes torna-se útil fazer o contrário, isto é, dividir uma equação nas palavras num sistema onde todas as equações são da forma $xy = z$ com $x, y, z \in (A \cup \Omega)^*$:

Proposição 3.4. *Sejam $x_1 \cdots x_g = x_{g+1} \cdots x_d$ uma equação com $1 \leq g < d$ e $x_i \in A \cup \Omega$ para $1 \leq i \leq d$. Então o conjunto de soluções está em bijecção canónica com o conjunto de soluções do sistema seguinte:*

$$\begin{array}{ll} x_1 &= y_1, & x_{g+1} &= y_{g+1}, \\ y_1 x_2 &= y_2, & y_{g+1} x_{g+2} &= y_{g+2}, \\ &\vdots & &\vdots \\ y_{g-1} x_g &= y_g, & y_{d-1} x_d &= y_d, \\ & & y_g &= y_d, \end{array}$$

onde $y_1, \dots, y_d$ são novas variáveis.

Também é de notar que uma disjunção de equações pode ser substituída por uma fórmula existencial numa simples equação como se mostra na proposição seguinte:

Proposição 3.5 (Karhumäki, Mignosi, Plandowski, 2000). *Sejam $a, b \in A$ com $a \neq b$. Uma disjunção de duas equações é equivalente a uma equação única com duas variáveis adicionais.*

Demonstração. Considere a disjunção $E_1 = D_1 \vee E_2 = D_2$ onde $E_1, E_2, D_1, D_2 \in (A \cup \Omega)^*$. Isto é equivalente à disjunção

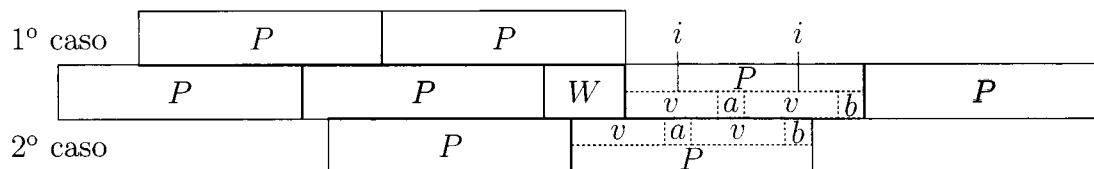
$$E_1 D_2 = D_1 D_2 \vee D_1 E_2 = D_1 D_2.$$

Então, para a construção, podemos começar com uma disjunção onde os membros da direita são iguais: $E_1 = D \vee E_2 = D$. Tem-se que a palavra $P = E_1 E_2 D a E_1 E_2 D b \in (A \cup \Omega)^+$ é primitiva. De facto, necessitamos de uma constatação mais profunda: sejam $Q \in (A \cup \Omega)^+$ uma palavra primitiva e $\alpha \geq 1$ tal que P é prefixo de Q^α . Então temos $|Q| > \frac{1}{2}|P|$. Para vermos isso vamos assumir o contrário, que $|Q| \leq \frac{1}{2}|P|$. Se $|Q| = \frac{1}{2}|P|$, então, como P é prefixo de Q^α , teríamos na última posição de Q as letras a e b , o que é absurdo pois $a \neq b$. Assim, Q é prefixo de $E_1 E_2 D$. Dois casos podem ocorrer:

$$\begin{array}{l} \text{ou} \quad \begin{array}{|c|c|c|c|c|} \hline Q & \cdots & Q & Q & \cdots & Q \\ \hline E_1 E_2 D a & & E_1 E_2 D b & & \\ \hline \end{array} \\ \text{ou} \quad \begin{array}{|c|c|c|c|c|} \hline Q & \cdots & Q & Q & \cdots \\ \hline & & Q & & \\ \hline \end{array} \end{array}$$

No primeiro caso temos novamente $a = b$, que é absurdo. No segundo caso Q é factor interno de QQ que, pelo Lema 1.9 é impossível. Como $|Q| > \frac{1}{2}|P|$, então não existe nenhuma palavra primitiva Q tal que $P = Q^\alpha$ com $\alpha > 1$. Logo, P é uma palavra primitiva.

Como consequência, as únicas ocorrências de P^2 como factor de $P^2 W P^2$ com $|W| \leq \frac{1}{2}|P|$ são como prefixo e sufixo. Vejamos:



No primeiro caso teríamos P como factor interno de P^2 , o que é impossível pois P é uma palavra primitiva. No segundo caso resulta que existe uma posição i em P tal que a posição i tem a letra a e a posição $|v| + i + 1$ de P não é a última posição e tem a letra b . Logo, a posição i da palavra v tem $a = b$, que também é impossível.

Assim sendo, sejam x, y duas novas variáveis. Vamos mostrar que a disjunção

$$E_1 = D \vee E_2 = D$$

é equivalente à fórmula existencial

$$\exists x \exists y : P^2 E_1 P^2 E_2 P^2 = x P^2 D P^2 y. \quad (3.1)$$

Se $E_1 = D \vee E_2 = D$ é solúvel então a fórmula acima é satisfeita.

Reciprocamente, seja σ uma solução da fórmula (3.1). Como $|\sigma(E_i)| \leq \frac{1}{2}|\sigma(P)|$ com $i = 1, 2$, o primeiro P^2 do membro da direita coincide ou com o primeiro ou com o segundo P^2 do membro da esquerda. Se coincidir com o segundo está resolvido: $x = P^2 E_1$, o segundo P^2 do membro da direita é factor de $P^2 E_2 P^2$ logo coincide com o último e portanto $E_2 = D$ e $y = \epsilon$. Suponhamos que o primeiro P^2 do membro da direita coincide com o primeiro P^2 do membro da esquerda ficando $E_1 P^2 E_2 P^2 = D P^2 y$. Assim, o segundo P^2 do membro da direita não pode coincidir com o último pois $|\sigma(D)| < |\sigma(E_1 P^2 E_2)|$ visto que $|\sigma(D)| < |\sigma(P)|$. Logo, ele coincide com o segundo. Portanto, $E_1 = D$ e o resultado segue. $\square$

Olhemos agora para o número de diferentes constantes existentes numa dada equação. Vejamos que o problema da resolução de equações pode ser reduzido ao caso onde aparecem somente duas constantes.

Proposição 3.6. *Seja $E = D$ uma equação num alfabeto A e seja $B = \{a, b\}$ um alfabeto de duas letras. Então podemos construir (em tempo polinomial) uma equação em B que é solúvel se e só se $E = D$ tem solução não-singular.*

Demonstração. Seja $A = \{a_1, \dots, a_k\}$ com $k > 2$. Consideremos o homomorfismo

$$\begin{aligned} \eta : (A \cup \Omega)^* &\longrightarrow (B \cup \Omega)^* \\ a_i &\mapsto ab^i a & 1 \leq i \leq k \\ x &\mapsto axa & x \in \Omega \end{aligned}$$

Obtemos a equação $\eta(E) = \eta(D)$. É claro que, se $E = D$ tem uma solução não-singular $\sigma : \Omega \rightarrow A^+$, então para todo o $x \in \Omega$ podemos escrever $\eta(\sigma(x)) = a\tau(x)a$ e $\tau : \Omega \rightarrow B^+$ é uma solução não-singular de $\eta(E) = \eta(D)$.

Reciprocamente, seja $\tau : \Omega \rightarrow B^*$ uma solução de $\eta(E) = \eta(D)$ (mesmo que esta solução seja singular produziremos uma solução não-singular de $E = D$). Definimos $\sigma'(x) = a\tau(x)a$ para todo o $x \in \Omega$ e modificamos η definindo $\eta'(a_i) = ab^i a$ e $\eta'(x) = x$ para quaisquer $1 \leq i \leq k$ e $x \in \Omega$. Seja $E' = \eta'(E)$ e $D' = \eta'(D)$. Então σ' é uma solução não-singular de $E' = D'$ tal que $\sigma'(x) \in aB^*a$ para todo o $x \in \Omega$. Queremos mostrar que $E = D$ tem solução não-singular. Se $\sigma'(x) \in \eta(A)^+$ para todo o $x \in \Omega$, então poderíamos identificar cada uma destas palavras com uma palavra de A^+ e obteríamos uma solução de $E = D$. Mas, poderá acontecer que $\sigma'(x)$ contenha factores da forma aaa ou ab^+ab^+a que não estão identificados pelo homomorfismo η a palavras de A^+ . No entanto, a um factor deste tipo num dos membros da equação corresponderá outro igual no outro membro que também pertencerá à imagem de uma variável. Formalizando esta ideia, observemos que o conjunto $\{\epsilon\} \cup (aB^* \cap B^*a)$ é um

submonóide livre de B^* . A base (infinita) é $\Sigma = \{a\} \cup aB^*a \setminus B^*aaB^*$. Assim, $\sigma' \circ \eta' : \Omega \rightarrow \Sigma^+$ é uma solução não-singular da equação original $E = D$ se identificarmos $\eta'(A)$ com A . O único problema é que $\sigma'(x)$ poderá ter como factores (em número finito) palavras de $\Sigma \setminus \eta'(A)$. Assim, para um conjunto finito $C \subseteq \Sigma \setminus \eta'(A)$, temos $\sigma'(E'D') \subseteq (\eta'(A) \cup C)^*$. Escolhemos uma aplicação $\rho : C \rightarrow \eta'(A)^+$ e obtemos uma solução não-singular $\sigma = \rho \circ \sigma'$ que pode ser identificada com uma solução não-singular de $E = D$ usando a seguinte composição que deixa as letras de A invariantes:

$$(A \cup \Omega)^+ \xrightarrow{\eta'} (\eta'(A) \cup \Omega)^+ \xrightarrow{\sigma'} (\eta'(A) \cup C)^+ \xrightarrow{\rho} (\eta'(A))^+ \xrightarrow{\eta'^{-1}} A^+.$$

Dada a equação $E = D$ aplicamos η' e obtemos a equação $E' = D'$ onde as letras de A são identificadas com as de $\eta'(A)$ e as variáveis de Ω mantêm-se. Como existe a solução τ de $\eta(E) = \eta(D)$, então existe a solução não-singular σ' de $E' = D'$. Agora, para podermos identificar a palavra $\sigma'(E)$ com uma palavra de A^+ basta identificar os factores de $\sigma'(E)$ que não pertencem a $\eta'(A)^+$ com alguma palavra de $\eta'(A)^+$. Para isso, constrói-se a aplicação ρ . Após esta aplicação, η'^{-1} fornece-nos uma solução de $E = D$ não-singular visto que σ' é não-singular. $\square$

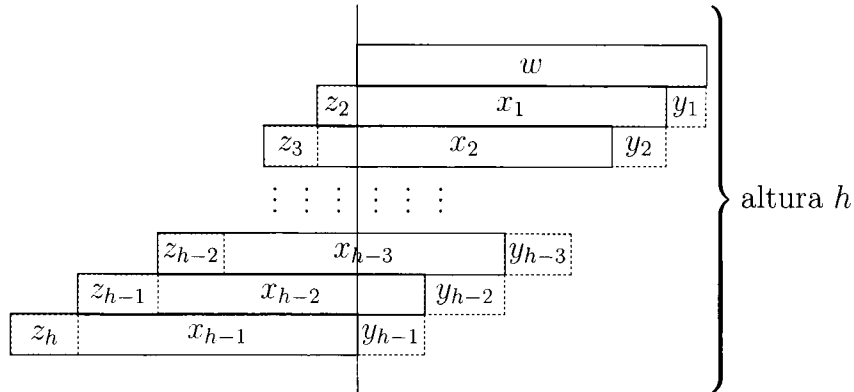
3.3 O Algoritmo: noções e estratégias

3.3.1 Torres dominó

Seja $h \geq 2$. Dizemos que uma palavra não-vazia $w \in A^+$ pode ser arranjada numa *torre dominó de altura h* se existirem palavras $x_1, \dots, x_{h-1} \in A^*$ e palavras não-vazias $y_1, \dots, y_{h-1}, z_2, \dots, z_h \in A^+$ tais que

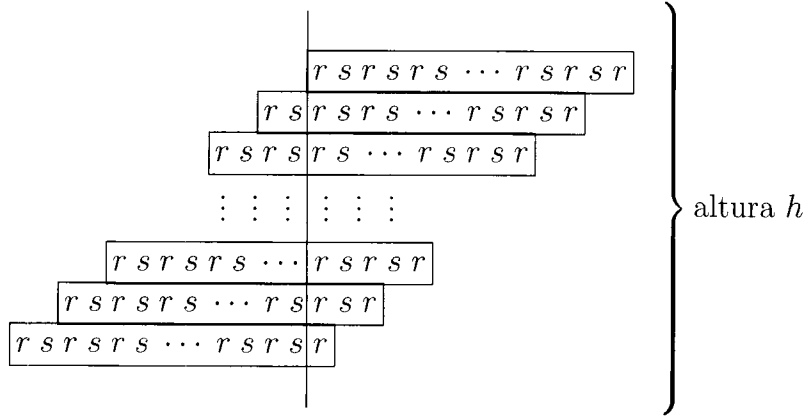
1. $w = x_i y_i = z_{i+1} x_i \ \forall \ 1 \leq i < h$,
2. $|z_2 \cdots z_h| \leq |w|$.

Figurativamente temos



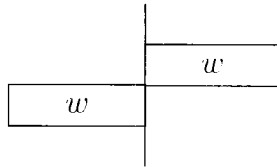
Notemos que a linha vertical permite-nos observar que $|z_2 \cdots z_j| \leq |w|$ para qualquer $2 \leq j \leq h$.

Podemos também optar por uma configuração mais uniforme. Toda a palavra não-vazia $w \in A^+$ pode ser escrita na forma $w = (rs)^{h-1}r$ com $s \neq \epsilon$ e $h \geq 2$ (trivial para $r = \epsilon$ e $h = 2$). Suponhamos que $r \neq \epsilon$. Escrevendo $w = (rs)^{h-1}r$ leva a um arranjo da seguinte forma:



A verificação de que se trata de uma torre dominó resulta de fazermos $x_1 = \cdots = x_{h-1} = (rs)^{h-2}r$, $y_1 = \cdots = y_{h-1} = sr$ e $z_2 = \cdots = z_h = rs$.

Note-se que, uma torre dominó de altura 2 pode degenerar na figura seguinte (com $x_1 = \epsilon$, $y_1 = w$, $z_2 = w$):



Seja $w \in A^*$ uma palavra. O *expoente de periodicidade* de w , $\exp(w)$, é definido por

$$\exp(w) = \max\{\alpha \in \mathbb{N} \mid \exists r, s, p \in A^*, p \neq \epsilon : w = rp^\alpha s\}.$$

Lema 3.7. Sejam $h \geq 2$ e $w \in A^+$ uma palavra não-vazia que pode ser arranjada numa torre dominó de altura h . Então $\exp(w) \geq h - 1$.

Demonstração. Escolhemos uma torre dominó e palavras x_i, y_i, z_i como na definição. Sejam $z = z_i \in \{z_2, \dots, z_h\}$ de comprimento mínimo, $x = x_{i-1}$ e $y = y_{i-1}$. Então $(h-1)|z| \leq |w|$ e temos $xy = zx = w$. Tem-se então que y e z são palavras conjugadas. Pelo Lema 1.7, $z = rs$ e $x = (rs)^\alpha r$ para alguns $\alpha \geq 0$ e $|r| < |z|$. Assim, $w = z^{\alpha+1}r$ e portanto

$$(h-1)|z| \leq |w| < (\alpha+2)|z|.$$

Como $|z| > 0$ temos $h-1 \leq \alpha+1 \leq \exp(w)$. □

3.3.2 Formas normais estáveis

Seja $p \in A^*$ uma palavra primitiva. A *forma normal p -estável* de $w \in A^*$ é uma sequência mínima (k mínimo)

$$(u_0, \alpha_1, u_1, \dots, \alpha_k, u_k)$$

tal que $k \geq 0$, $u_0, u_i \in A^*$, $\alpha_i \geq 0$ para $1 \leq i \leq k$ e satisfazendo as seguintes condições:

1. $w = u_0 p^{\alpha_1} u_1 \dots p^{\alpha_k} u_k$,
2. $k = 0$ se e só se p^2 não é factor de w ,
3. se $k \geq 1$, então:

$$\begin{aligned} u_0 &\in A^*p \setminus A^*p^2A^*, \\ u_i &\in (A^*p \cap pA^*) \setminus A^*p^2A^* \text{ para } 1 \leq i < k, \\ u_k &\in pA^* \setminus A^*p^2A^*. \end{aligned}$$

Exemplo 3.8. Seja $p = bab$ e $w = b(bab)^4ab(bab)ab$. Então, a forma normal p -estável de w é a sequência

$$(bbab, 2, babab, 0, babab).$$

$$\underbrace{bbab}_{u_0} \underbrace{babbab}_{u_1} \underbrace{babab}_{u_2}$$

Proposição 3.9. *Seja $p \in A^*$ uma palavra primitiva. A forma normal p -estável de $w \in A^*$ é única, ou seja, se $(u_0, \alpha_1, u_1, \dots, \alpha_k, u_k)$ e $(v_0, \beta_1, v_1, \dots, \beta_l, v_l)$ são formas normais p -estáveis de $w \in A^*$, então elas são iguais, isto é, temos $k = l$, $u_0 = v_0$, $u_i = v_i$ e $\alpha_i = \beta_i$ para todo o $1 \leq i \leq k$.*

Demonstração. Suponhamos que $(u_0, \alpha_1, u_1, \dots, \alpha_k, u_k)$ e $(v_0, \beta_1, v_1, \dots, \beta_l, v_l)$ são duas formas normais p -estáveis de w . Como são sequências mínimas, os índices k e l são ambos mínimos, logo $k = l$.

Para $k = 0$ temos $w = u_0 = v_0$.

Suponhamos que $k = l \geq 1$. Vejamos primeiro que $u_0 = v_0$. Assumimos, por simetria, que $|u_0| \leq |v_0|$. Como $u_0 p \in A^*p^2$ e $v_0 \in (A^*p \setminus A^*p^2A^*)$ obtemos $u_0 \leq v_0 < u_0 p$.

u_0	p	
v_0	p	
u_0	p	p

Pelo Lema 1.9 tem-se $u_0 = v_0$.

Seja $w' = u_1 p^{\alpha_2} u_2 \dots p^{\alpha_k} u_k$. Como $u_1 \neq p$ e $u_1 \in (A^*p \cap pA^*) \setminus A^*p^2A^*$, concluímos, usando novamente o Lema 1.9, que $p^{\alpha_1} w' \in p^{\alpha_1+1}A^* \setminus p^{\alpha_1+2}A^*$. De modo análogo,

temos $p^{\beta_1}w'' \in p^{\beta_1+1}A^* \setminus p^{\beta_1+2}A^*$ onde $w'' = v_1p^{\beta_2}v_2 \cdots p^{\beta_l}v_l$. Como $p^{\alpha_1}w' = p^{\beta_1}w''$ resulta que $\alpha_1 = \beta_1$ e $w' = w'' = v_1p^{\beta_2}v_2 \cdots p^{\beta_l}v_l$.

Pela minimalidade de $k = l$ e por $(u_0, \alpha_1, u_1, \dots, \alpha_k, u_k)$ e $(v_0, \beta_1, v_1, \dots, \beta_l, v_l)$ serem formas normais p -estáveis de $u_0p^{\alpha_1}w' = v_0p^{\beta_1}w''$ resulta que $(u_1, \alpha_2, u_2, \dots, \alpha_k, u_k)$ e $(v_1, \beta_2, v_2, \dots, \beta_k, v_k)$ são formas normais p -estáveis de w' . Por indução, concluímos que $(u_1, \alpha_2, u_2, \dots, \alpha_k, u_k) = (v_1, \beta_2, v_2, \dots, \beta_k, v_k)$. $\square$

3.3.3 Uma única variável

Se houver unicamente uma variável na equação, então uma descrição paramétrica do conjunto de todas as soluções pode ser calculada em tempo polinomial. Isto é um exemplo de como as formas normais p -estáveis poderão ser úteis.

Seja $\mathcal{S}$ um conjunto de equações nas palavras onde ocorre exactamente uma variável x , ou seja, $\Omega = \{x\}$. Pela Proposição 3.3 podemos assumir que $\mathcal{S}$ é dado por uma só equação $E = D$ com $E, D \in (A \cup \{x\})^*$.

O passo básico é ver se $\sigma(x) = \epsilon$ é solução singular. Após isso, procuramos somente soluções não-singulares.

Seja $\mathcal{L}$ uma lista de pares (p, r) onde $p \in A^+$ é uma palavra primitiva e $r \in A^*$ é um prefixo $r < p$. Dizemos que $\mathcal{L}$ é completa para a equação $E = D$ se toda a solução não-singular σ tiver a forma $\sigma(x) = p^\alpha r$ para algum expoente $\alpha \geq 0$ e algum par $(p, r) \in \mathcal{L}$.

Suponhamos que uma lista completa e finita $\mathcal{L}$ já foi construída numa primeira fase do algoritmo. Então procedemos do seguinte modo: para cada par $(p, r) \in \mathcal{L}$ testamos se $\sigma(x) = r$ é solução e se $\sigma(x) = pr$ é solução. Depois disso, procuramos (para o par (p, r)) soluções onde $\sigma(x) = p^\alpha r$ com $\alpha \geq 2$. Substituímos todas as ocorrências de x na equação $E = D$ pela expressão $pp^{\alpha-2}pr$, onde α representa uma variável inteira. O problema é então encontrar valores de α tais que $\alpha \geq 2$ e $\sigma(x) = p^\alpha r$ seja solução da equação $E = D$. Usando expressões simbólicas podemos factorizar $\sigma(E)$ e $\sigma(D)$ na sua forma normal p -estável:

$$\begin{aligned}\sigma(E) &= u_0p^{m_1\alpha+n_1}u_1 \cdots p^{m_k\alpha+n_k}u_k, \\ \sigma(D) &= v_0p^{m'_1\alpha+n'_1}v_1 \cdots p^{m'_l\alpha+n'_l}v_l,\end{aligned}$$

com $k, l \geq 0$, $m_i, m'_j \in \mathbb{N}$, $n_i, n'_j \in \mathbb{Z}$, $1 \leq i \leq k$ e $1 \leq j \leq l$. Pela Proposição 3.9, supondo que σ é uma solução, tem-se que $k = l$, $u_i = v_i$ para $0 \leq i \leq k$. Temos então que resolver o sistema linear Diofantino:

$$(m_i - m'_i)\alpha = n'_i - n_i \quad \text{para } 1 \leq i \leq k.$$

Há três casos: ou nenhum, ou exactamente um $\alpha \geq 2$, ou todos os $\alpha \geq 2$ satisfazem estas equações. Construímos então o conjunto de todas as soluções. É claro que para cada par (p, r) os cálculos necessários podem ser feitos em tempo polinomial. De facto,

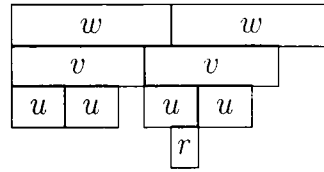
pode-se mostrar que tempo linear é suficiente. A execução do algoritmo depende do cálculo eficiente de uma lista completa e curta $\mathcal{L}$.

Vamos então construir a lista. Suponhamos que $E = ux \dots$ e $D = xv \dots$ onde $u \in A^+$, $v \in A^*$ e ambas as palavras u e v são de comprimento máximo. Seja $p \in A^+$ a raiz primitiva de u , isto é, p é uma palavra primitiva e $u = p^e$ para algum $e \geq 1$. Se σ é uma solução de $E = D$, então σ é também solução de uma equação do tipo $ux = xv$ para alguma palavra $w \in A^+$. Pelo Lema 1.7 temos $u = ab$, $w = ba$ e $\sigma(x) = (ab)^k a$ com $a, b \in A^*$. Como $p^e = ab$, fazendo $a = p^l r$ com $0 \leq l \leq e$ e $r < p$ obtemos $\sigma(x) = (p^e)^k p^l r = p^\alpha r$ com $\alpha \geq 0$ e $r < p$. Definimos a lista de todos os pares (p, r) com $r < p$. Obtemos assim uma lista com $|p|$ elementos.

Há um refinamento do algoritmo feito por Obono, Goralčik e Maksimenko (1994) que observa a existência de uma lista completa de comprimento no máximo logarítmico. Para o efeito, é usada uma análise combinatória mais fina baseada, em particular, no facto seguinte:

Lema 3.10 (Obono, Goralčik, Maksimenko, 1994). Sejam u, v, w palavras tais que u é palavra primitiva, $v \notin u^*$ e $uu < vv < ww$. Então $|u| + |v| \leq |w|$.

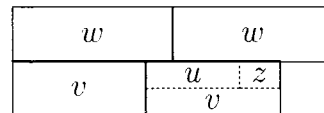
Demonstração. Por redução ao absurdo, suponhamos que $|u| < |w| < |vu|$. Assumimos primeiro que $2|u| \leq |v|$. Então temos $uu \leq v < w$. Como $vv < ww$, pela segunda palavra w , vemos que w tem um prefixo da forma ru com $1 \leq |r| < |u|$:



pois, como $|vu| > |w|$, temos $w = ru \dots$. Logo, temos $w = uu \dots$ e $w = ru \dots$ e portanto, como $|r| < |u|$, u é factor interno de uu , o que é impossível pelo Lema 1.9 visto u ser uma palavra primitiva.

Assim, devemos assumir que $u < v < uu$.

Seja $v = uz$. Então temos $z < u$ e $zu = uy$ para alguma palavra não-vazia y pois $uzuz = vv = uu \dots$. Seja x a raiz primitiva de z . Então, pelo Lema 1.7, $z = x^\beta$ e $u = x^\alpha r$ para alguns inteiros $\alpha \geq \beta \geq 1$ e alguma palavra não-vazia $r < x$ (pois u é uma palavra primitiva). Assim, $v = uz = x^\alpha r x^\beta < w$ e, como



temos $sz = sx^\beta < w$ onde s é um sufixo próprio de $u = x^\alpha r$. Se $|s| \geq |x|$, então $x \leq s$ pois x e s são prefixos de w . Como s é um sufixo próprio de $x^\alpha r < x^{\alpha+1}$, x

é uma palavra primitiva e $s = x \cdots$ resulta, pelo Lema 1.9, que $s = x^\gamma r$ para algum $1 \leq \gamma < \alpha$. Como $sx^\beta < w, u = x^\alpha r < w$ e $\gamma + 1 < \alpha + 1$, temos $sx = x^\gamma r x < x^{\alpha+1}$. Mas isto é impossível pois, como $1 \leq |r| < |x|$ e x é uma palavra primitiva, x seria factor interno de xx . Logo, s é prefixo próprio de x . Se $|s| \leq |x^{\alpha-1}r|$, então, como $x^\alpha r < w$ e $sx < w$, temos $sx \leq x^\alpha r < x^{\alpha+1}$ que é novamente uma contradição pois s é prefixo próprio de x . Note-se também que, se $\alpha > 1$, então é claro que $|s| \leq |x^{\alpha-1}r|$ visto $s < x$. Assim sendo, devemos assumir que $\alpha = 1$ e portanto, como $1 \leq \beta \leq \alpha$, temos $\beta = 1$ e $|s| > |x^{\alpha-1}r| = |r|$. Temos então $u = xr, v = xrx$ e $w = xrx t$ para alguma palavra não-vazia t tal que $ts = u = xr$. Em particular, $t < x$ visto que $|s| > |r|$. Logo, como $uw = xrx t x r x t$ e $v = xrx$, temos $txr < xrx = v < xrx r = uu$. Portanto $tu < uu$ o que é impossível pois u é uma palavra primitiva. Resulta que $|u| + |v| \leq |w|$. $\square$

Nota 3.11. Ao longo da demonstração não foi usada a hipótese de $v \notin u^*$ pelo que poderíamos tê-la excluído do enunciado do lema. No entanto, para não modificarmos a afirmação dos autores, optámos por mantê-la apresentando este comentário.

Definimos $\log \alpha$ como $\max\{1, \lceil \log_2 \alpha \rceil\}$ onde $\lceil n \rceil$ representa o menor inteiro não inferior a n .

Corolário 3.12. Uma palavra $w \in A^*$ de comprimento n tem no máximo $\mathcal{O}(\log n)$ prefixos distintos da forma pp onde p é uma palavra primitiva.

Demonstração. Sejam $w \in A^*, n = |w|$ e r o número de prefixos distintos da forma pp onde p é uma palavra primitiva. Representemos por p_i esses prefixos e sejam $n_i = |p_i|$ com $1 \leq i \leq r$. Suponhamos, sem perda de generalidade, que $p_1 < \cdots < p_r < w$. Então temos, por definição dos p_i , $p_1 p_1 < p_2 p_2 < \cdots < p_r p_r \leq w$. Pelo lema anterior, resulta que

$$|p_i| + |p_{i+1}| \leq |p_{i+2}|$$

com $1 \leq i \leq r-1$ onde $p_{r+1} = w$. Obtemos as seguintes inequações:

$$\begin{array}{ll} a_1 : & n_{r-1} + n_r \leq n \\ a_2 : & n_{r-2} + 2n_{r-1} \leq n \\ a_3 : & 2n_{r-3} + 3n_{r-2} \leq n \\ \vdots & \\ a_k : & f_{k-1}n_{r-k} + f_k n_{r-k+1} \leq n \end{array} \quad \begin{array}{ll} b_1 : & n_{r-2} + n_{r-1} \leq n_r \\ b_2 : & n_{r-3} + n_{r-2} \leq n_{r-1} \\ b_2 : & n_{r-4} + n_{r-3} \leq n_{r-2} \\ \vdots & \\ b_l : & n_{r-l-1} + n_{r-l} \leq n_{r-l+1} \end{array}$$

para $1 \leq k \leq r-1$ e $1 \leq l \leq r-2$. Então temos que

$$f_{r-2}n_1 + f_{r-1}n_2 \leq n \text{ e } f_{r-3}n_2 + f_{r-2}n_3 \leq n. \quad (3.2)$$

Notemos que a sucessão $(f_k)_{k \in \mathbb{N}}$ é a sucessão de Fibonacci definida por recorrência:

$$f_0 = 1, f_1 = 1 \text{ e } f_k = f_{k-1} + f_{k-2} \text{ com } k \geq 2.$$

Assim, como $n_1 < n_2$ temos, por (3.2), que

$$(f_{r-2} + f_{r-1})n_1 \leq n \Leftrightarrow f_r n_1 \leq n \Rightarrow f_r \leq n.$$

Da mesma forma obtemos $f_{r-1}n_2 \leq n \Rightarrow f_{r-1} \leq n$.

Usemos a fórmula de Binet para a sucessão de Fibonacci:

$$f_k = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{k+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{k+1} \right] \text{ com } k \geq 0.$$

Se r for par, então, como $f_r \leq n$, obtemos

$$\left(\frac{1+\sqrt{5}}{2} \right)^{r+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{r+1} \leq \sqrt{5}n$$

e, como $\frac{1-\sqrt{5}}{2}$ é negativo e $r+1$ é ímpar, temos que $-\left(\frac{1-\sqrt{5}}{2}\right)^{r+1}$ é um valor positivo. Resulta, em particular, que

$$\left(\frac{1+\sqrt{5}}{2} \right)^{r+1} \leq \sqrt{5}n$$

e portanto

$$r \leq C \log n.$$

Se r for ímpar, então, como $f_{r-1} \leq n$, obtemos

$$\left(\frac{1+\sqrt{5}}{2} \right)^r - \left(\frac{1-\sqrt{5}}{2} \right)^r \leq \sqrt{5}n$$

e, pelo mesmo raciocínio, concluímos que

$$\left(\frac{1+\sqrt{5}}{2} \right)^r \leq \sqrt{5}n.$$

Logo,

$$r \leq C' \log n.$$

Obtemos assim o resultado pretendido, ou seja, $r \in \mathcal{O}(\log n)$. □

Vejamos a ideia geral do método de Obono et al: recordemos que a equação é dada por $E = ux \cdots$ e $D = xv \cdots$. O conjunto de soluções não-singulares é dividido em duas classes. A primeira contém todas as soluções onde $|\sigma(x)| \geq |u| - |v|$ (como é claro, no caso $|u| \leq |v|$ todas as soluções satisfazem esta condição). Seja w o prefixo de vu tal que $|w| = |u|$. Se σ é uma solução com $|\sigma(x)| \geq |u| - |v|$, então temos $u\sigma(x) = \sigma(x)w$ como se observa:

1º caso: $|u| \leq |v|$

u	$\sigma(x)$
$\sigma(x)$	v

2º caso: $|u| > |v|$

u		$\sigma(x)$
$\sigma(x)$	v	$\sigma(x)$

Por hipótese, temos $|\sigma(x)| + |v| \geq |u|$. No primeiro caso resulta de imediato que $u\sigma(x) = \sigma(x)w$. No segundo caso, como u e v são de comprimento máximo, então após v temos a única variável x . Assim, $u\sigma(x)$ é prefixo de $\sigma(x)v\sigma(x)$. Se $u \leq \sigma(x)$ e como $|u| + |\sigma(x)| < |\sigma(x)| + |v| + |u|$, então $u\sigma(x) < \sigma(x)vu < \sigma(x)v\sigma(x)$. Se $\sigma(x) < u$, então $u\sigma(x) < \sigma(x)v\sigma(x) < \sigma(x)vu$. Logo $u\sigma(x) < \sigma(x)vu$ e portanto $u\sigma(x) = \sigma(x)w$.

Sejam p a raiz primitiva de u e q a raiz primitiva de w . Então $\sigma(x) = p^\alpha r$ para algum $\alpha \geq 0$ e o único prefixo $r < p$ tal que $p = rs$ e $q = sr$. Se p e q não forem palavras conjugadas, então não existe tal solução. Caso contrário, se p e q são palavras conjugadas, incluímos o único par (p, r) em $\mathcal{L}$. Este par cobre todas as soluções onde $|\sigma(x)| \geq |u| - |v|$.

Seja agora σ uma solução não-singular tal que $0 \neq |\sigma(x)| < |u| - |v|$. Isto implica que D tem a forma $D = vx \cdots$ e que $\sigma(x)v\sigma(x) < u\sigma(x)$. Logo, $\sigma(x)v\sigma(x) < uu$ e $ww < vuu$, onde w representa a palavra não-vazia $v\sigma(x)$. Seja q a raiz primitiva de w . Então $qq < vuu$. Há uma única factorização $q = sr$ com $s < q$ tal que $v \in q^*s$. Pelo Lema 1.14 a palavra rs é também primitiva e temos $\sigma(x) = r(sr)^\alpha$ para algum $\alpha \geq 0$ visto $w = v\sigma(x)$ e q ser a raiz primitiva de w . Portanto, é suficiente construir a lista de todas as palavras primitivas q tais que $qq < vuu$. Pelo Corolário 3.12, o número de palavras primitivas q é majorado por $\mathcal{O}(\log |vuu|)$. Se $v = \epsilon$ adicionamos os pares (q, ϵ) a $\mathcal{L}$. Caso contrário, se $v \neq \epsilon$ calculamos para cada q a única factorização $q = sr$ com $s \neq \epsilon$ tal que $v \in q^*s$. Adicionamos todos os pares (rs, r) a $\mathcal{L}$.

Crochemore [9] diz-nos que a lista $\mathcal{L}$ pode ser calculada em tempo $\mathcal{O}(|ED| \log |ED|)$. Conclui-se então que a solubilidade de uma equação $E = D$ numa variável pode ser decidida em tempo $\mathcal{O}(|ED| \log |ED|)$. Não é no entanto clara a existência de um algoritmo com tempo linear.

3.3.4 Restrições num semigrupo

A entrada no algoritmo de Makanin é uma equação $E = D$ com $E, D \in (A \cup \Omega)^*$ juntamente com linguagens racionais $L_x \subseteq A^*$ para todo o $x \in \Omega$. Assumimos que as linguagens são determinadas por autómatos finitos não-determinísticos. Se acontecer que para uma variável nenhuma restrição esteja definida, então simplesmente escrevemos $L_x = A^*$.

Procuramos uma solução $\sigma : \Omega \rightarrow A^*$ tal que $\sigma(E) = \sigma(D)$ e $\sigma(x) \in L_x$ para todo o $x \in \Omega$.

Para uma notação conveniente, daqui em diante não distinguiremos variáveis e constantes na equação. Toda a constante $a \in A$ será substituída pela nova variável x_a , sendo acrescentada a restrição $L_{x_a} = \{a\}$. Contudo, para uma melhor legibilidade, nos exemplos continuaremos a usar constantes.

A partir de agora a equação será dada por

$$x_1 \cdots x_g = x_{g+1} \cdots x_d$$

com $x_i \in \Omega$. De modo a excluir casos triviais, assumimos $1 \leq g < d$ sempre que seja conveniente. O número d é chamado o *comprimento notacional* da equação.

Tal como na Secção 3.1, podemos, num primeiro passo, procurar a existência de soluções singulares. Escolhemos algum $\Omega' \subseteq \Omega$ e substituímos todas as ocorrências de $x \in \Omega'$ pela palavra vazia. Obtemos uma nova equação $E' = D'$ nas variáveis $\Omega \setminus \Omega'$ onde procuramos as soluções não-singulares. Assim, dada uma equação, num passo não-determinístico, transformámo-la numa outra equação onde só estamos interessados nas suas soluções não-singulares. É então suficiente, para uma qualquer equação, procurar somente as soluções não-singulares. Assim, assumimos que $\epsilon \notin L_x$ para qualquer $x \in \Omega$.

Fixamos um semigrupo finito S e um homomorfismo de semigrupos $\varphi : A^+ \rightarrow S$ tal que $L_x = \varphi^{-1}(\varphi(L_x))$ para todo o $x \in \Omega$. Para os próximos objectivos exigimos que φ seja sobrejectiva. O semigrupo S poderá ser visto como a imagem $\varphi(A^+)$ do homomorfismo canónico no produto directo dos monóides sintácticos com respeito a L_x , $x \in \Omega$. Assim sendo, definimos φ do seguinte modo: para cada $x \in \Omega$ seja $\varphi_x : A^+ \rightarrow A^+/\sigma_{L_x}$ onde σ_{L_x} é a congruência sintáctica de L_x . Note-se que φ_x reconhece L_x para todo o $x \in \Omega$. Seja $\varphi : A^+ \rightarrow \prod_{x \in \Omega} A^+/\sigma_{L_x}$ o homomorfismo canónico. Então φ reconhece todas as linguagens L_x . Tomamos S como a imagem $\varphi(A^+)$.

Representamos por S^ϵ o monóide que é obtido pela junção do elemento neutro ϵ a S . Temos então $S^\epsilon \setminus \{\epsilon\} = S$ e o homomorfismo φ é estendido ao homomorfismo de monóides $\varphi : A^* \rightarrow S^\epsilon$. Temos $\varphi^{-1}(\epsilon) = \{\epsilon\}$ e $\varphi(A^+) = S$.

Dado S podemos arranjar constantes $t(S) \geq 0$ e $q(S) > 0$ tais que $s^{t(S)+q(S)} = s^{t(S)}$ para qualquer $s \in S^\epsilon$ (pois S é finito). Usaremos uma outra constante $c(S)$ que é definida como o menor múltiplo de $q(S)$ tal que $c(S) \geq \max\{2, t(S)\}$. Vejamos que isto implica $s^{r+\alpha c(S)} = s^{r+\beta c(S)}$ para quaisquer $s \in S$, $r \geq 0$ e $\alpha, \beta \geq 1$:

Lema 3.13. Sejam S um semigrupo, $s \in S^\epsilon$, $t, q \in \mathbb{N}$ tais que $s^{t+q} = s^t$. Sejam $m, n \geq t$ com $m \equiv n \pmod{q}$. Então $s^m = s^n$.

Demonstração. Suponhamos, sem perda de generalidade, que $m \geq n$. Então $m = n + qz$ com $z \geq 0$ e portanto $s^m = s^{m-t+t} = s^{n+qz-t+t} = s^{t+qz+(n-t)} = s^{t+(n-t)} = s^n$. $\square$

Markowsky [24], numa análise mais precisa, mostra que se cada linguagem racional é definida por um autómato não-determinístico com r_x estados, $x \in \Omega$, então, fazendo $r = \sum_{x \in \Omega} r_x$, podemos escolher um semigrupo S tal que

$$|S| \leq 2^{r^2} \text{ e } c(S) \leq r!.$$

No nosso trabalho os majorantes de $|S|$ e $c(S)$ não são relevantes. Estes majorantes serão usados num estudo futuro da complexidade do algoritmo.

3.4 O expoente de periodicidade

Procuramos um majorante eficiente para o expoente de periodicidade numa solução de comprimento mínimo de uma equação (com restrições racionais). Para a conclusão da decidibilidade qualquer majorante eficiente seria suficiente, mas, devido à relação com equações lineares Diofantinas e a técnicas de optimização linear, podemos ser mais precisos.

Teorema 3.14. Seja $d \geq 1$ um número natural, $\varphi : A^* \rightarrow S^\epsilon$ um homomorfismo e $c(S) \geq 2$ definido anteriormente. Podemos calcular um número $e(c(S), d) \in c(S) \cdot 2^{\mathcal{O}(d)}$ que satisfaça a condição:

Dada uma equação nas palavras $x_1 \cdots x_g = x_{g+1} \cdots x_d$ de comprimento notacional d e uma solução $\sigma' : \Omega \rightarrow A^*$ podemos efectivamente encontrar uma solução $\sigma : \Omega \rightarrow A^*$ e uma palavra $w \in A^*$ tais que as seguintes condições se verifiquem:

1. $\varphi\sigma'(x) = \varphi\sigma(x)$ para todo o $x \in \Omega$,
2. $w = \sigma(x_1 \cdots x_g) = \sigma(x_{g+1} \cdots x_d)$,
3. $\exp(w) \leq e(c(S), d)$.

Demonstração. Para $g = 0$ ou $g = d$ temos $\exp(w) = 0$. Seja $1 \leq g < d$. Testando todas as palavras de comprimento até $|\sigma'(x_1 \cdots x_g)|$ encontramos uma solução σ e uma palavra w tal que $w = \sigma(x_1 \cdots x_g) = \sigma(x_{g+1} \cdots x_d)$ é de comprimento mínimo entre todas as soluções σ tais que $\varphi\sigma'(x) = \varphi\sigma(x)$ para todo o $x \in \Omega$. Relembramos que $x_1 \cdots x_g = x_{g+1} \cdots x_d$ é equivalente ao sistema:

$$\begin{array}{ll} x_1 &= y_1, & x_{g+1} &= y_{g+1}, \\ y_1 x_2 &= y_2, & y_{g+1} x_{g+2} &= y_{g+2}, \\ &\vdots & &\vdots \\ y_{g-1} x_g &= y_g, & y_{d-1} x_d &= y_d, \\ && y_g &= y_d. \end{array}$$

Notemos também que $\exp(w) = \exp(\sigma(y_g))$. Depois de uma eliminação óbvia das variáveis $(x_1, x_{g+1}$ e y_d que é substituída por y_g) o sistema é equivalente a um sistema de $d - 2$ equações do tipo

$$xy = z \quad \text{com } x, y, z \in \Omega.$$

Escolhemos uma palavra primitiva $p \in A^+$ tal que $w = up^{\exp(w)}v$ para alguns $u, v \in A^*$. Consideremos uma equação $xy = z$ do sistema anterior e escrevamos as palavras $\sigma(x), \sigma(y), \sigma(z)$ nas suas formas normais p -estáveis:

$$\begin{aligned} \sigma(x) : & (u_0, r_1 + \alpha_1 c(S), u_1, \dots, r_k + \alpha_k c(S), u_k), \\ \sigma(y) : & (v_0, s_1 + \beta_1 c(S), v_1, \dots, s_l + \beta_l c(S), v_l), \\ \text{e } \sigma(z) : & (w_0, t_1 + \gamma_1 c(S), w_1, \dots, t_m + \gamma_m c(S), w_m), \end{aligned}$$

onde os números naturais $r_i, s_i, t_i, \alpha_i, \beta_i$ e γ_i são unicamente determinados por $w, c(S)$ e a condição $0 \leq r_i, s_i, t_i < c(S)$.

Há muitas equações entre as palavras e entre os inteiros. Para $k, l \geq 2$ temos:

$$\begin{aligned} u_0 &= w_0, & \dots, & u_{k-1} = w_{k-1}, \\ r_1 &= t_1, & \dots, & r_{k-1} = t_{k-1}, \\ \alpha_1 &= \gamma_1, & \dots, & \alpha_{k-1} = \gamma_{k-1}, \\ v_1 &= w_{m-l+1}, & \dots, & v_l = w_m, \\ s_2 &= t_{m-l+2}, & \dots, & s_l = t_m, \\ \beta_2 &= \gamma_{m-l+2}, & \dots, & \beta_l = \gamma_m. \end{aligned}$$

Não temos majorantes para k, l ou m mas temos $|k + l - m| \leq 2$. O que acontece exactamente depende da forma normal p -estável do produto $u_k v_0$. Como $u_k, v_0 \notin A^* p^2 A^*$ é suficiente distinguir nove casos:

$$\begin{aligned} (u_k v_0), & (p, t, p), & (p, t, p v'_0), \\ (u'_k p, t, p), & (u'_k p, t, p v'_0), & (p, 0, w', 0, p), \\ (p, 0, w', 0, p v'_0), & (u'_k p, 0, w', 0, p), & (u'_k p, 0, w', 0, p v'_0), \end{aligned}$$

onde $t \in \{0, 1\}$ e $u_k, v_0, u'_k, v'_0, w' \in A^+$. Vamos ver o que acontece em cada um deles:

- Caso $(u_k v_0)$: Acontece quando $u_k = pw, v_0 = w'p$ e $u_k v_0 = pww'p$ com $u_k v_0 \in A^+ \setminus (A^* p^2 A^*)$. As formas normais p -estáveis de $\sigma(x)\sigma(y)$ e $\sigma(z)$ são:

$$\begin{aligned} \sigma(x)\sigma(y) : & (\dots, r_k + \alpha_k c(S), u_k v_0, s_1 + \beta_1 c(S), v_1, \dots) \\ \sigma(z) : & (\dots, t_k + \gamma_k c(S), w_k, t_{k+1} + \gamma_{k+1} c(S), w_{k+1}, \dots) \end{aligned}$$

e portanto $m = k + l$, $\alpha_k = \gamma_k$ e $\beta_1 = \gamma_{k+1}$.

- Caso (p, t, p) com $t \in \{0, 1\}$: Resulta de $u_k = pw, v_0 = w'p$ com $ww' = p^t$. Se $u_k v_0 = p^{2+t}$, então a sua forma normal p -estável é (p, t, p) e a forma normal p -estável de $\sigma(x)\sigma(y)$ é

$$(\dots, u_{k-1}, r_k + \alpha_k c(S) + s_1 + \beta_1 c(S) + (2 + t), v_1, \dots).$$

Temos $r_k + \alpha_k c(S) + s_1 + \beta_1 c(S) + (2 + t) = r_k + s_1 + (2 + t) + (\alpha_k + \beta_1)c(S) = t_k + \gamma_k c(S)$ e também $m = k - 1 + l$.

Por hipótese, $c(S) \geq 2$. Como $r_k, s_1 < c(S)$, temos $r_k + s_1 + (2 + t) < 3c(S)$. Logo, poderemos ter $\gamma_k = c + (\alpha_k + \beta_1)$ com $c \in \{0, 1, 2\}$. Assim, o caso $u_k v_0 = p^{2+t}$ leva à equação:

$$\gamma_k - (\alpha_k + \beta_1) = c \quad \text{com } c \in \{0, 1, 2\}$$

- Caso $(p, t, p v'_0)$ com $t \in \{0, 1\}$: A forma normal p -estável de $\sigma(x)\sigma(y)$ é

$$(\dots, r_k + \alpha_k c(S) + t + 1, p v'_0, s_1 + \beta_1 c(S), v_1, \dots).$$

Temos $m = k + l$ e $r_k + \alpha_k c(S) + t + 1 = t_k + \gamma_k c(S)$. Como $r_k < c(S)$ e $t + 1 \leq 2$ então $r_k + t + 1 < 2c(S)$. Logo, teremos $\alpha_k = \gamma_k$ ou $\alpha_k + 1 = \gamma_k$.

Este caso pode acontecer quando, por exemplo, $p = aba, u_k = abaw$ e $v_0 = w'ababa$ com $ww' = p^t$.

- Caso $(u'_k p, t, p)$: De modo análogo ao anterior iremos ter $\beta_1 = \gamma_{k+1}$ ou $\beta_1 + 1 = \gamma_{k+1}$.
- Caso $(u'_k p, t, pv'_0)$: As formas normais p -estáveis são:

$$\begin{aligned}\sigma(x)\sigma(y) : & (\dots, r_k + \alpha_k c(S), u'_k p, t, pv'_0, s_1 + \beta_1 c(S), v_1, \dots) \\ \sigma(z) : & (\dots, t_k + \gamma_k c(S), w_k, t_{k+1} + \gamma_{k+1} c(S), w_{k+1}, t_{k+2} + \gamma_{k+2} c(S), w_{k+2}, \dots)\end{aligned}$$

obtendo $m = k + l + 1$, $\gamma_k = \alpha_k$, $\gamma_{k+1} = 0$ e $\gamma_{k+2} = \beta_1$.

Podemos encontrar este caso quando $p = aba$, $u_k = ababaw$ e $v_0 = w'ababa$ com $ww' = p^t$.

- Caso $(p, 0, w', 0, p)$: Pode ser produzido se p tiver uma sobreposição como em $p = ababa$. Então teríamos $u_k = pabab$, $v_0 = abap$ e portanto $u_k v_0 = ppbap = pabpp$ e $abp = pba$. Logo, neste caso particular, a forma normal p -estável $u_k v_0$ é $(p, 0, abp, 0, p)$.

Passando ao caso geral, as formas normais p -estáveis são:

$$\begin{aligned}\sigma(x)\sigma(y) : & (\dots, 1 + r_k + \alpha_k c(S), w', 1 + s_1 + \beta_1 c(S), v_1, \dots) \\ \sigma(z) : & (\dots, t_k + \gamma_k c(S), w_k, t_{k+1} + \gamma_{k+1} c(S), w_{k+1}, \dots)\end{aligned}$$

e portanto obtemos $k + l = m$, $t_k + \gamma_k c(S) = r_k + \alpha_k c(S) + 1$ e $t_{k+1} + \gamma_{k+1} c(S) = s_1 + \beta_1 c(S) + 1$. Se $r_k < c(S) - 1$, ou seja, $r_k + 1 < c(S)$, então temos $\alpha_k = \gamma_k$. Caso contrário, $r_k + 1 = c(S)$ visto termos $r_k < c(S)$ e portanto $\alpha_k + 1 = \gamma_k$. Do mesmo modo, se $s_1 < c(S) - 1$ então $\beta_1 = \gamma_{k+1}$. Caso contrário, temos $\beta_1 + 1 = \gamma_{k+1}$.

- Caso $(p, 0, w', 0, pv'_0)$: A forma normal p -estável de $\sigma(x)\sigma(y)$ é:

$$(\dots, r_k + \alpha_k c(S) + 1, w', 0, pv'_0, s_1 + \beta_1 c(S), v_1, \dots).$$

Temos $m = k + l + 1$, $r_k + 1 + \alpha_k c(S) = t_k + \gamma_k c(S)$ e portanto $\alpha_k = \gamma_k$ ou $\alpha_k + 1 = \gamma_k$, $\gamma_{k+1} = 0$ e $\gamma_{k+2} = \beta_1$.

- Caso $(u'_k p, 0, w', 0, p)$: Analogamente ao caso anterior obtemos $s_1 + 1 + \beta_1 c(S) = t_{k+2} + \gamma_{k+2} c(S)$ e portanto $\beta_1 = \gamma_{k+2}$ ou $\beta_1 + 1 = \gamma_{k+2}$, $\alpha_k = \gamma_k$ e $\gamma_{k+1} = 0$.
- Caso $(u'_k p, 0, w', 0, pv'_0)$: Uma forma normal p -estável deste tipo com $u', v', w' \in A^+$ leva a $k + l = m - 2$ e $0 = \gamma_{k+2} = \gamma_{k+1}$:

$$(\dots, r_k + \alpha_k c(S), u'_k p, 0, w', 0, pv'_0, s_1 + \beta_1 c(S), \dots)$$

$$(\dots, t_k + \gamma_k c(S), w_k, t_{k+1} + \gamma_{k+1} c(S), w_{k+1}, t_{k+2} + \gamma_{k+2} c(S), w_{k+2}, t_{k+3} + \gamma_{k+3} c(S), \dots)$$

Temos $m = k + l + 2$, $0 = \gamma_{k+1} = t_{k+1} = \gamma_{k+2} = t_{k+2}$, $\gamma_k = \alpha_k$ e $\gamma_{k+3} = \beta_1$.

Vimos que há várias possibilidades para $u_k v_0$. No entanto, ocorre sempre o mesmo fenómeno. Em primeiro lugar obtemos um grupo de equações triviais do tipo $\gamma = \alpha$ que podem ser eliminadas por renomeação, substituindo γ por α . Todas as equações do tipo $\gamma = 0$ são eliminadas por substituição. Assim, para cada $xy = z$ há no máximo duas equações do tipo $\gamma = \alpha + 1$ ou uma equação do tipo $\gamma - (\alpha + \beta) = c$ com $c \in \{0, 1, 2\}$. Se houver duas equações do tipo $\gamma = \alpha + 1$, então uma delas é eliminada por substituição de γ por $\alpha + 1$. Obtemos, para cada equação $xy = z$, no máximo uma equação não-trivial com o máximo de três variáveis. Procedendo deste modo, nas $d-2$ equações temos várias interações devido à renomeação e substituição. Como exemplo, se em ambas as equações $y_1 x_2 = y_2$ e $y_2 x_3 = y_3$ tivermos a equação não-trivial $\gamma = \alpha + 1$, então poderemos obter, após as substituições referidas, uma equação do tipo $\gamma = \alpha + 2$ na equação $y_2 x_3 = y_3$. Assim, cada equação $xy = z$ leva no máximo a uma equação não-trivial com o máximo de três variáveis. O tipo de equação é

$$c_1 \gamma + i_1 - c_2 \alpha - i_2 - c_3 \beta - i_3 = c$$

onde $0 \leq i_1, i_2, i_3 \leq d-2, 0 \leq c \leq 2, c_1, c_2, c_3 \in \{0, 1\}$. Isto pode ser escrito como

$$c_1 \gamma - c_2 \alpha - c_3 \beta = c' \text{ com } |c'| \leq 2d-2.$$

Os símbolos $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l, \gamma_1, \dots, \gamma_m$ são vistos como variáveis que percorrem números naturais. Regressando à solução σ , que é dada pela palavra w , os símbolos $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l, \gamma_1, \dots, \gamma_m$ representam valores concretos. Alguns deles poderão ser zero. Esses são logo eliminados. A razão é: pela observação feita no fim da Secção 3.3.4, $s^{r+\alpha c(S)} = s^{r+\beta c(S)}$ para todo o $s \in S, r \geq 0$ e $\alpha, \beta \geq 1$, podemos diminuir os valores de α, β e γ até 1 pois a imagem de φ não se altera. No entanto, se alguns forem zero, então esse valor não poderá ser mudado visto a observação só se verificar para $\alpha, \beta, \gamma \geq 1$ e portanto deixaríamos de ter a garantia de não alterar a imagem de φ . Assim sendo, substituímos todos os α, β e γ que tenham valores maiores que zero por $1 + z_\alpha, 1 + z_\beta$ e $1 + z_\gamma$ respectivamente onde as novas variáveis representam valores em $\mathbb{N}$. Por exemplo, a equação

$$\gamma - \alpha - \beta = c'$$

com $\alpha, \beta, \gamma \geq 1$ é transformada na equação linear Diofantina com variáveis inteiras $z_\alpha, z_\beta, z_\gamma \geq 0$ como se segue:

$$z_\gamma - z_\alpha - z_\beta = c' + 1 \text{ com } |c' + 1| \leq 2d-1.$$

Juntando todas as equações do tipo $xy = z$ obtemos um sistema de equações lineares que, depois da substituição e eliminação das variáveis, transformar-se-á num sistema com o máximo de $d-2$ equações e n variáveis inteiras com $n \leq 3(d-2)$. Os valores absolutos dos coeficientes são limitados por 2 e das constantes por $2d-1$. Para cada equação a soma dos quadrados dos coeficientes é limitada por 5. Como exemplo, para o caso $\alpha = \beta \neq \gamma$ e $c_1 = c_2 = c_3 = 1$ obtemos a equação $\gamma - 2\alpha = c'$, equação esta onde a soma dos quadrados dos coeficientes é 5. O sistema linear Diofantino é definido por w e a palavra w fornece uma solução inteira não negativa deste sistema.

Reciprocamente, toda a solução em inteiros não-negativos do sistema produz uma palavra w'' e uma solução $\sigma'' : \Omega \rightarrow A^*$ que satisfaz a condição 2 do teorema. A condição 1 também é satisfeita usando a observação da Secção 3.3.4 já referida nesta demonstração.

Procuremos um majorante para $\exp(w)$. Como w foi escolhida de comprimento minimal, a solução do sistema em inteiros dada por w é uma solução minimal com respeito à ordem parcial de $\mathbb{N}^n$:

$$(\alpha_1, \dots, \alpha_n) \leq (\beta_1, \dots, \beta_n) \text{ se e só se } \alpha_i \leq \beta_i \text{ para qualquer } 1 \leq i \leq n.$$

Para $\vec{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ seja $\|\vec{\alpha}\| = \max\{\alpha_i | 1 \leq i \leq n\}$. Procuremos um majorante para o seguinte valor:

$$e(d) = \max\{\|\vec{\alpha}\| \mid \vec{\alpha} \text{ é solução minimal do sistema de equações lineares Diofantinas com o máximo de } d-2 \text{ equações, } 3(d-2) \text{ variáveis, onde o valor absoluto dos coeficientes é limitado por 2, a soma dos quadrados dos coeficientes em cada equação é limitada por 5 e o valor absoluto das constantes é limitado por } 2d-1\}.$$

Obviamente, há um número finito de sistemas de equações lineares Diofantinas onde o número de equações, variáveis e valor absoluto dos coeficientes e constantes é majorado. L. Dickson [10] diz-nos que para cada sistema o conjunto de soluções minimais é finito. Em E. Domenjoud e A. Tomás [11] encontramos um algoritmo que calcula estas soluções minimais. Logo, o conjunto dos valores de $\|\vec{\alpha}\|$ é finito e efectivamente calculável. Portanto, $e(d)$ é calculável. Como $e(d) + d - 1 \geq \alpha_1, \dots, \beta_1, \dots$ para os valores originais antes das considerações acima, obtemos um majorante do expoente de periodicidade.

Uma condição mais precisa é possível. Kościelski e Pacholski [15] mostraram que $e(d) \in 2^{\mathcal{O}(d)}$. Logo, podemos ter

$$\exp(w) \leq 2 + (c(S) - 1) + (e(d) + d - 1) \cdot c(S) \in c(S) \cdot 2^{\mathcal{O}(d)}.$$

Isto prova o teorema. □

Exemplo 3.15. Sejam $c, n \geq 2$ e seja $S = \mathbb{Z}/c\mathbb{Z}$ o grupo cíclico de c elementos. Fazemos uma restrição racional à variável x_1 definida por

$$L_{x_1} = \{w \in A^+ \mid |w| \equiv 0 \pmod{c}\}.$$

O sistema é dado por

$$\begin{cases} x_1 &= a^c \\ x_2 &= x_1^2 \\ &\vdots \\ x_n &= x_{n-1}^2 \end{cases}$$

A única solução σ é $\sigma(x_i) = a^{c2^{i-1}}$ com $1 \leq i \leq n$. Se transformarmos o sistema numa simples equação segundo a Proposição 3.3, então obtemos

$$x_1 b_1 \cdots x_n b_1 x_1 b_2 \cdots x_n b_2 = a^c b_1 \cdots x_{n-1}^2 b_1 a^c b_2 \cdots x_{n-1}^2 b_2$$

onde $b_1, b_2 \in A$ com $b_1 \neq b_2$, obtemos $\exp(w) = c2^{n-1}$, $d = 4n + 2n + 2c + 4(n-1) = 10n + 2c - 4$ e portanto $e(c(S), d) \in c(S) \cdot 2^{\mathcal{O}(d)}$.

Exemplo 3.16. Apresentamos uma sucessão de equações em que podemos observar que o comprimento de uma solução minimal pode ser muito grande embora o expoente de periodicidade seja majorado por uma constante.

Consideremos o sistema de equações nas palavras

$$\begin{aligned} x_0 &= a, & y_0 &= b, \\ x_i &= x_{i-1} y_{i-1}, & y_i &= y_{i-1} x_{i-1} \quad \text{para } 1 \leq i \leq n. \end{aligned}$$

A única solução é a palavra de Thue-Morse:

$$\sigma(x_n) = abbabaabbaababbabaababbaabbabaab \cdots \quad \text{para } n \geq 5.$$

Temos $|\sigma(x_n)| = 2^n$, mas $\exp(\sigma(x_n)) = 2$.

Exemplo 3.17. Consideremos a equação com restrições racionais:

$$axyz = zxy, \quad L_x = a^2 a^*, \quad L_y = \{a, b\}^* \setminus (a^* \cup b^*) \quad \text{e} \quad L_z = \{a, b\}^+.$$

Um homomorfismo adequado $\varphi : \{a, b\}^+ \rightarrow S$ é dado pelo homomorfismo canónico no semigrupo quociente de $\{a, b\}^+$ que é apresentado pelas seguintes relações:

$$a^2 = a^3, \quad b = b^2 \quad \text{e} \quad ab = ba = aab.$$

Portanto, S é um semigrupo com um zero, $0 = ab$, e tem quatro elementos:

$$S = \{a, a^2, b, 0\}.$$

A constante $c(S) = 2$ satisfaz a condição $s^{r+c(S)} = s^{r+\alpha c(S)}$ para quaisquer $s \in S^\epsilon$, $r \geq 0$ e $\alpha \geq 1$.

Procuramos uma solução σ para a equação $axyz = zxy$. Façamos $\sigma(x) = a^{2+k}$ com $k \geq 0$ para garantirmos que $\sigma(x) \in L_x$. Obtemos a equação $aa^{2+k}yz = za^{2+k}ay$, isto é, $a^{3+k}yz = za^{3+k}y$. Como $L_y = \{a, b\}^* \setminus (a^* \cup b^*)$, então $\sigma(y)$ tem pelo menos um factor a e um factor b . Seja, por exemplo, $\sigma(y) = y'ba^\ell$ com $\ell > 0$. Obtemos $a^{3+k}y'ba^\ell z = za^{3+k}y'ba^\ell$. Como z não pode ser a palavra vazia teremos, pela equação anterior, $\sigma(z) = z'ba^\ell$ ficando $a^{3+k}y'ba^\ell z' = z'ba^\ell a^{3+k}y'$. Façamos $\sigma(y') = a^r$ e $\sigma(z') = a^s$ com $r, s \geq 0$. Assim, $a^{3+k}a^rba^\ell a^s = a^sba^{\ell+3+k}a^r$, ou seja, $a^{3+k+r}ba^{\ell+s} = a^sba^{\ell+3+k+r}$ ficando $3+k+r = s$ e $\ell+s = \ell+3+k+r$. Logo, $s = 3+k+r$. Temos, por exemplo, fazendo $k = 0$, $r = 0$, $s = 3$ e $\ell = 2$, a solução

$$\sigma(x) = a^2, \quad \sigma(y) = ba^2 \quad \text{e} \quad \sigma(z) = a^3ba^2.$$

A palavra primitiva a é tal que $w = \sigma(axyz) = \sigma(zxay) = ua^{\exp(w)}v$ para alguns $u, v \in A^*$. Sejam α, β, γ e δ variáveis inteiras e r, s e t palavras descritas pelas formas normais a -estáveis:

$$r : (a, 2\alpha, a),$$

$$s : (ba, 2\beta, a),$$

$$t : (a, 1 + 2\gamma, aba, 2\delta, a).$$

De modo a obter um sistema de equações lineares Diofantinas escrevemos $arst$ como uma sequência de formas normais a -estáveis:

$$((a), (a, 2\alpha, a), (ba, 2\beta, a), (a, 1 + 2\gamma, aba, 2\delta, a)).$$

A forma normal a -estável resultante é:

$$(a, 2\alpha + 1, aba, 2\beta + 3 + 2\gamma, aba, 2\delta, a).$$

Consideremos agora o membro da direita $tras$. Temos a sequência

$$((a, 1 + 2\gamma, aba, 2\delta, a), (a, 2\alpha, a), (a), (ba, 2\beta, a))$$

cuja forma normal a -estável resultante é:

$$(a, 2\gamma + 1, aba, 2\delta + 2\alpha + 3, aba, 2\beta, a).$$

Obtemos o sistema linear Diofantino:

$$\begin{cases} 2\alpha + 1 = 2\gamma + 1 \\ 2\beta + 2\gamma + 3 = 2\alpha + 2\delta + 3 \\ 2\delta = 2\beta \end{cases} \Leftrightarrow \begin{cases} \alpha = \gamma \\ \beta = \delta \end{cases}$$

Temos

$$\sigma(x) = a^{2+2\alpha}, \quad \sigma(y) = ba^{2+2\beta} \quad \text{e} \quad \sigma(z) = a^{3+2\alpha}ba^{2+2\beta} \quad \forall \alpha, \beta \geq 0$$

que produz soluções da equação que satisfazem as restrições racionais.

Nesta secção majoramos o expoente de periodicidade numa solução de comprimento mínimo. Assim, dada uma equação ela possui solução se e só se tiver uma solução cujo expoente de periodicidade não é superior ao valor calculado. No entanto, no Exemplo 3.16 observamos que existem palavras cujo expoente de periodicidade é baixo mas cujo comprimento poderá ser arbitrariamente grande. Assim, se construíssemos um algoritmo que gerasse palavras cujo expoente de periodicidade fosse menor ou igual ao nosso majorante e testássemos se a palavra era solução da equação, não teríamos a garantia que o algoritmo parasse. Portanto, este majorante por si só não fornece um majorante para o comprimento de uma solução minimal nem resolve o problema da decidibilidade.

3.5 Equações fronteira

3.5.1 Ordens lineares num semigrupo

Suponhamos que $x_1 \cdots x_g = x_{g+1} \cdots x_d$ com $1 \leq g < d$ e $x_i \in \Omega$ para $1 \leq i \leq d$ é uma equação solúvel com restrições racionais e que existe uma solução não-singular σ tal que $\sigma(x_i) = u_i$ com $1 \leq i \leq d$. A equação e a solução definem a palavra $w \in A^+$ e duas factorizações $w = u_1 \cdots u_g = u_{g+1} \cdots u_d$. As posições entre os factores u_i e u_{i+1} com $1 \leq i < g$ ou $g < i < d$ são chamados *cortes*. Por convenção, a primeira e a última posição de w também são cortes e portanto temos no máximo d cortes (poderão existir cortes iguais nos dois membros). Lendo a palavra de corte a corte obtemos uma sequência $(w_1, \dots, w_m)$ tal que $u_i = w_j w_{j+1} \cdots w_{j+k}$ com $1 \leq i \leq d$, $1 \leq j < j+k \leq m$ e $w = w_1 \cdots w_m$ com $w_k \neq \epsilon$, $1 \leq k \leq m$ e $m < d$.

Dizemos que a sequência $(w_1, \dots, w_m)$ refina as duas sequências $(u_1, \dots, u_g)$ e $(u_{g+1}, \dots, u_d)$. Vejamos o que acontece quando passamos ao semigrupo finito S via o homomorfismo φ . Substituímos u_i e w_k por $p_i = \varphi(u_i)$ e $s_k = \varphi(w_k)$ respectivamente.

Duas sequências $(p_1, \dots, p_g) \in S^g$ e $(p_{g+1}, \dots, p_d) \in S^{d-g}$ são refinadas por uma sequência $(s_1, \dots, s_m) \in S^m$ com $m < d$ tal que $p_i = s_j s_{j+1} \cdots s_{j+k}$ com $1 \leq i \leq d$ e $1 \leq j < j+k \leq m$. Dizemos também que $(s_1, \dots, s_m)$ é um *refinamento comum* de $(p_1, \dots, p_g)$ e $(p_{g+1}, \dots, p_d)$.

Contudo, para cada d , há somente um número finito de candidatos para $(s_1, \dots, s_m)$ com $m < d$ pois S é finito. Logo, num passo não-determinístico, podemos encontrar e fixar uma tal sequência $(s_1, \dots, s_m)$ para ser a φ -imagem de $(w_1, \dots, w_m)$.

Uma técnica básica para resolver equações de palavras é a divisão da variável. Trabalhando com a sequência $(s_1, \dots, s_m) \in S^m$, a divisão da variável $x = x'x''$ corresponde à divisão de algum s_i e a encontrar $s'_i, s''_i \in S$ tais que $s_i = s'_i s''_i$. Deste modo, os comprimentos das sequências vão aumentar.

Exemplo 3.18. Consideremos a equação $xauzau = yzbxaby$. A solução dada no Exemplo 1.4 leva às sequências $(ab, a, baba, ba, a, baba)$ e $(aba, ba, b, ab, a, a, b, aba)$ onde $(ab, a, ba, b, a, b, a, a, b, aba)$ é um refinamento comum. Isto pode ser visualizado na figura:

a	b	a	b	a	b	a	b	a	a	b	a	b	a
a	b	a	b	a	b	a	b	a	a	b	a	b	a
a	b	a	b	a	b	a	b	a	a	b	a	b	a

Passando ao semigrupo $S = \{a, a^2, b, 0\}$ do Exemplo 3.17 encontramos uma solução com a sequência $(0, a, 0, b, a, b, a, a, b, 0) \in S^{10}$.

Formalmente, consideremos o semigrupo S e o homomorfismo $\varphi : A^+ \rightarrow S$ da Secção 3.3.4. Uma S -sequência é uma sequência $(s_1, \dots, s_m) \in S^m$ com $m \geq 0$. Uma *representação*

de $(s_1, \dots, s_m)$ é um triplo $(I, \leq, \varphi_I)$ tal que $(I, \leq)$ é um conjunto totalmente ordenado de $m + 1$ elementos e

$$\varphi_I : \{(i, j) \in I \times I \mid i \leq j\} \rightarrow S^\epsilon$$

é uma aplicação que, para alguma bijecção $\rho : I \rightarrow \{0, \dots, m\}$ que respeita a ordem em I , isto é, tal que se $i \leq j$ para $i, j \in I$, então $\rho(i) \leq \rho(j)$, satisfaz a condição

$$\varphi_I(i, j) = s_{\rho(i)+1} \cdots s_{\rho(j)} \in S^\epsilon \text{ para quaisquer } i, j \in I \text{ com } i \leq j.$$

Temos

$$\varphi_I(i, j) = \epsilon \text{ se e só se } i = j,$$

$$\varphi_I(i, k) = \varphi_I(i, j) \varphi_I(j, k) \text{ para quaisquer } i, j, k \in I \text{ com } i \leq j \leq k.$$

A *representação canónica* de $(s_1, \dots, s_m)$ é simplesmente $(I, \leq, \varphi_I)$ onde $I = \{0, \dots, m\}$ e $\varphi_I(i, j) = s_{i+1} \cdots s_j$ para $i, j \in I$ com $i \leq j$. Logo, para a representação canónica, a bijecção ρ é a identidade.

No que se segue, toda a representação $(I, \leq, \varphi_I)$ de alguma S -sequência é chamada uma *ordem linear sobre S* . Quando contarmos ordens lineares sobre S , por convenção, contaremos somente representações canónicas.

Seja $w = a_1 \cdots a_m \in A^*$ com $a_i \in A$ para $1 \leq i \leq m$. O conjunto $\{0, \dots, m\}$ é o *conjunto das posições* de w e, para $0 \leq i \leq j \leq m$, $w(i, j)$ representa o factor $a_{i+1} \cdots a_j$. Em particular, $w = w(0, m) = w(0, i)w(i, m)$ para qualquer $0 \leq i \leq m$. A S -sequência associada à palavra w é definida por $w_S = (\varphi(a_1), \dots, \varphi(a_m))$. A notação w_S também se refere à sua representação canónica $w_S = (\{0, \dots, m\}, \leq, \varphi_w)$. A aplicação φ_w é tal que $\varphi_w(i, j) = \varphi(w(i, j))$ para quaisquer $0 \leq i \leq j \leq m$.

Sejam s, s' duas S -sequências dadas por algumas representações $(I, \leq, \varphi_I)$ e $(I', \leq, \varphi_{I'})$. Dizemos que s' é um *refinamento* de s se existir uma aplicação injectiva $\rho : I \rightarrow I'$ que respeita a ordem em I tal que $\varphi_I(i, j) = \varphi_{I'}(\rho(i), \rho(j))$ para quaisquer $i, j \in I$ com $i \leq j$. Escrevemos $s \leq s'$ ou, mais precisamente, $s \leq_\rho s'$ e $(I, \leq, \varphi_I) \leq_\rho (I', \leq, \varphi_{I'})$. Note-se que, se $s \leq s'$, então podemos escolher representações e um refinamento $(I, \leq, \varphi_I) \leq_\rho (I', \leq, \varphi_{I'})$ tal que $\rho : I \rightarrow I'$ é uma inclusão, isto é, $I \subseteq I'$ e φ_I é a restrição de $\varphi_{I'}$ a I .

Seja s uma S -sequência e $(I, \leq, \varphi_I)$ uma sua representação. Uma palavra $w \in A^*$ é chamada um *modelo* de s (de $(I, \leq, \varphi_I)$ respectivamente) se a S -sequência associada w_S for um refinamento de s , isto é, $(I, \leq, \varphi_I) \leq_\rho w_S$ para algum ρ .

Se w for um modelo de s , então escrevemos $w \models s$ ou $w \models (I, \leq, \varphi_I)$. Por abuso de linguagem, fazemos a seguinte convenção: mal tenhamos escolhido a palavra w como modelo podemos ver I como um subconjunto de posições de w , isto é, ρ torna-se a inclusão e portanto $\varphi_I(i, j) = \varphi(w(i, j))$ para quaisquer $i, j \in I$ com $i \leq j$.

Lema 3.19. Toda a S -sequência $(s_1, \dots, s_m)$ tem um modelo $w \in A^*$.

Demonstração. Como φ é sobrejectiva (e é aqui que se usa a sobrejectividade exigida na Secção 3.3.4), existem palavras não-vazias $w_i \in A^+$ tais que $s_i = \varphi(w_i)$ para todo o i com $1 \leq i \leq m$. Seja $w = w_1 \cdots w_m$. Então $w \models (s_1, \dots, s_m)$. $\square$

Sejam $n \geq 0$ e $\varphi : A^+ \rightarrow S$ um homomorfismo num semigrupo finito S .

1. Um *sistema de equações fronteira* é definido por

$$\mathcal{B} = ((\Gamma, \bar{\cdot}), (I, \leq, \varphi_I), \text{esq}, B)$$

onde Γ é um conjunto com $2n$ variáveis, $\bar{\cdot} : \Gamma \rightarrow \Gamma$ é uma involução sem pontos fixos, isto é, $\bar{\bar{x}} = x$ e $x \neq \bar{x}$ para qualquer $x \in \Gamma$, o triplo $(I, \leq, \varphi_I)$ é uma ordem linear sobre S , $\text{esq} : \Gamma \rightarrow I$ uma aplicação e B um conjunto de *equações fronteira*. Toda a equação fronteira $b \in B$ tem a forma $b = (x, i, \bar{x}, j)$ com $x \in \Gamma$ e $i, j \in I$ tais que $\text{esq}(x) \leq i$ e $\text{esq}(\bar{x}) \leq j$.

2. Uma *solução* de $\mathcal{B}$ é um modelo $w \models (I, \leq, \varphi_I)$ com $w \in A^*$, tal que

$$w(\text{esq}(x), i) = w(\text{esq}(\bar{x}), j) \text{ para qualquer } (x, i, \bar{x}, j) \in B.$$

Relembramos que, se uma palavra $w \in A^*$ é um modelo para $(I, \leq, \varphi_I)$, então vemos I como um subconjunto de posições de w . Assim, faz sentido escrever $w(p, q)$ para $p, q \in I$ com $p \leq q$.

3. Se $\mathcal{B}$ é solúvel então o *expoente de periodicidade*, $\text{exp}(\mathcal{B})$, de $\mathcal{B}$ é definido por

$$\text{exp}(\mathcal{B}) = \min\{\text{exp}(w) \mid w \text{ é solução de } \mathcal{B}\}.$$

Não faremos distinção entre sistemas isomorfos. Em particular, podemos sempre pensar que $\Gamma = \{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\}$ e que $(I, \leq, \varphi_I)$ é a representação canónica de alguma S -sequência, $I = \{0, \dots, m\}$ para alguns $n, m \geq 0$.

Note-se que, se $n = 0$, então não existem variáveis e portanto não existem equações fronteira. Logo, qualquer modelo $w \models (I, \leq, \varphi_I)$ é solução de $\mathcal{B}$. Assim, se $n = 0$, o sistema é solúvel pois, pelo Lema 3.19, o modelo w existe.

Passemos então de equações de palavras para equações fronteira. Consideremos uma equação de palavras $x_1 \cdots x_g = x_{g+1} \cdots x_d$ e uma aplicação $\psi : \Omega \rightarrow S$. Construímos um sistema

$$\mathcal{B} = ((\Gamma, \bar{\cdot}), (I, \leq, \varphi_I), \text{esq}, B)$$

de equações fronteira com as duas propriedades seguintes:

1. Seja $\sigma : \Omega \rightarrow A^+$ uma solução da equação de palavras tal que $\psi = \varphi \circ \sigma$ e seja $v \in A^*$ uma palavra com $v = \sigma(x_1 \cdots x_g) = \sigma(x_{g+1} \cdots x_d)$. Então $w = vv$ é uma solução de $\mathcal{B}$.
2. Seja $w \models (I, \leq, \varphi_I)$ uma solução de $\mathcal{B}$. Então temos $w \in A^*vvA^*$ para algum $v \in A^*$ e existe uma solução da equação de palavras $\sigma : \Omega \rightarrow A^+$ tal que $\psi = \varphi \circ \sigma$ e $v = \sigma(x_1 \cdots x_g) = \sigma(x_{g+1} \cdots x_d)$.

De modo a definir $\mathcal{B}$ começamos com a S -sequência

$$(\psi(x_1), \dots, \psi(x_d)).$$

Seja $(I, \leq, \varphi_I)$ uma sua representação onde $I = \{i_0, \dots, i_d\}$ com $i_0 \leq \dots \leq i_d$. O próximo passo é definir o par $(\Gamma, \bar{\cdot})$ e a aplicação $esq : \Gamma \rightarrow I$. O significado intuitivo de $(\Gamma, \bar{\cdot})$ é que Γ é um novo conjunto de variáveis onde a noção de dual está definida e esq indica a posição mais à esquerda de uma variável numa solução dada. Formalizamos o conceito usando grafos não-dirigidos. Seja (V, E) o grafo com conjunto de vértices $V = \{1, \dots, d\}$ e conjunto de arestas $E = \{(p, q) \in V \times V \mid x_p = x_q\}$. Claramente, cada aresta determina uma variável, mas agora temos uma escolha canónica para definir o dual de $(p, q), (q, p)$. A ideia é a seguinte: para $v = \sigma(x_1 \dots x_g) = \sigma(x_{g+1} \dots x_d)$ e $w = vv$ podemos considerar I como o conjunto de posições de w tal que $w \models (\psi(x_1), \dots, \psi(x_d))$ e as seguintes equações são satisfeitas:

$$w(i_0, i_g) = w(i_g, i_d) \quad \text{e} \quad w(i_{p-1}, i_p) = w(i_{q-1}, i_q) \quad \forall (p, q) \in E.$$

Para a primeira equação introduzimos uma nova variável x_0 e o seu dual $\bar{x}_0$; na outra lista de equações há alguma redundância visto a relação entre arestas ser transitiva. Para $(p, q), (q, r) \in E$ temos, por definição, $(p, r) \in E$, mas as equações $w(i_{p-1}, i_p) = w(i_{q-1}, i_q)$ e $w(i_{q-1}, i_q) = w(i_{r-1}, i_r)$ também implicam $w(i_{p-1}, i_p) = w(i_{r-1}, i_r)$. Logo, não necessitamos da aresta (p, r) para a equação. Para evitar a redundância, seja $F \subseteq E$ uma árvore maximal de (V, E) . Assim, (V, F) é um grafo não-dirigido acíclico. Temos $|F| = 2(d - c)$ onde c é o número de componentes conexas de (V, E) . Para cada $x = (p, q) \in F$ definimos o seu dual e duas posições $esq(x)$ e $dir(x)$:

$$\bar{x} = (q, p), \quad esq(x) = i_{p-1} \quad \text{e} \quad dir(x) = i_p.$$

Notemos que $x \neq \bar{x}$ e $\bar{\bar{x}} = x$ para qualquer $x \in F$. Tomar os duais das variáveis corresponde a inverter o sentido das arestas em (V, F) . Definimos dois elementos extra x_0 e $\bar{x}_0$ com $\bar{\bar{x}_0} = x_0$, definimos $\Gamma = \{x_0, \bar{x}_0\} \cup F$ e ainda:

$$esq(x_0) = i_0, \quad dir(x_0) = i_g = esq(\bar{x}_0) \quad \text{e} \quad dir(\bar{x}_0) = i_d.$$

Isto define o conjunto Γ , a involução sem pontos fixos $\bar{\cdot} : \Gamma \rightarrow \Gamma$ e a aplicação $esq : \Gamma \rightarrow I$. Os elementos de Γ continuam a ser chamados de variáveis.

O último passo da construção é definir o conjunto B de equações fronteira. Deverá ser claro o que faremos. Definimos

$$B = \{(x, dir(x), \bar{x}, dir(\bar{x})) \mid x \in \Gamma\}.$$

Temos de verificar as duas propriedades acima:

1. Seja $\sigma : \Omega \rightarrow A^+$ uma solução tal que $\psi = \varphi \circ \sigma$ e seja $w = vv$ onde $v = \sigma(x_1 \dots x_g) = \sigma(x_{g+1} \dots x_d)$. A palavra w tem posições $0 = i_0 < i_1 < \dots < i_d$, onde i_d é a última posição e as equações seguintes são satisfeitas:

$$w(i_0, i_g) = w(i_g, i_d) \quad \text{e} \quad w(i_{p-1}, i_p) = \sigma(x_p) \quad \text{para } 1 \leq p \leq d.$$

Em particular, $w \models (I, \leq, \varphi_I)$ e w é solução de $\mathcal{B}$.

2. Seja $w \models (I, \leq, \varphi_I)$ uma solução de $\mathcal{B}$. Podemos ver I como um subconjunto de posições de w . Consideremos os factores $w(i_0, i_g)$ e $w(i_g, i_d)$. A equação fronteira $(x_0, \text{dir}(x_0), \bar{x}_0, \text{dir}(\bar{x}_0)) \in B$ implica $w(i_0, i_g) = w(i_g, i_d)$ e segue que $w \in A^*vvA^*$ para $v = w(i_0, i_g)$. Definimos $\sigma : \Omega \rightarrow A^+$ por $\sigma(x_p) = w(i_{p-1}, i_p)$. Como $i_{p-1} < i_p$, então a palavra $\sigma(x_p)$ é não-vazia. Os elementos $(x, \text{dir}(x), \bar{x}, \text{dir}(\bar{x})) \in B$ para $x = (p, q)$ e $\bar{x} = (q, p)$ com $(p, q) \in \Gamma$ implicam $w(i_{p-1}, i_p) = w(i_{q-1}, i_q)$ sempre que $x_p = x_q$. Assim, σ está bem definida. Temos $\varphi\sigma(x_p) = \varphi w(i_{p-1}, i_p) = \psi(x_p)$ visto que $w \models (I, \leq, \varphi_I)$. Finalmente, $v = w(i_0, i_g) = w(i_g, i_d)$ implica $v = \sigma(x_1 \cdots x_g) = \sigma(x_{g+1} \cdots x_d)$.

Assim, a equação de palavras com restrições racionais dadas pela aplicação ψ tem solução se e só se o sistema de equações fronteira for solúvel. A construção do sistema $\mathcal{B}$ pode ser feita em tempo polinomial (e em espaço logarítmico). Devido a esta transformação, o resultado de Makanin segue do Teorema 3.24 (ver pág.78). No Lema 3.26 veremos que a afirmação do teorema é de facto equivalente ao resultado de Makanin.

Exemplo 3.23. Consideremos a equação

$$xyxyz = zyxyx$$

com as restrições racionais

$$L_x = a^+, \quad L_y = \{a, b\}^+ \quad \text{e} \quad L_z = \{a, b\}^+ \setminus (a^+ \cup b^+).$$

Passando ao semigrupo S dado no Exemplo 3.17, $S = \{a, a^2, b, 0\}$ e considerando o homomorfismo canónico $\varphi : \{a, b\}^+ \rightarrow S$ obtemos

$$\varphi(L_x) = \{a, a^2\}, \quad \varphi(L_y) = S \quad \text{e} \quad \varphi(L_z) = \{0\}.$$

Procuramos uma solução não-singular. Façamos, por exemplo, $\sigma(x) = a$. Resulta que $ayayz = zyaya$. Como estamos interessados numa solução não-singular, podemos fazer $\sigma(z) = az'a$ ficando $yayaz' = z'ayay$. Sejam $\sigma(y) = b = \sigma(z')$. Assim, $\sigma(x) = a, \sigma(y) = b$ e $\sigma(z) = aba$, ou seja, a palavra $v = abababa$ soluciona a equação. A transformação que leva ao sistema de equações fronteira é baseada na figura seguinte. A primeira linha representa a palavra $w = vv$ de comprimento 14.

a	b	a	b	a	b	a	a	b	a	b	a	b	a
x_0							$\overline{x_0}$						
x_1	x_2	x_3	x_4	x_5			$\overline{x_5}$	x_6	x_7	$\overline{x_6}$	$\overline{x_7}$		
		$\overline{x_1}$	$\overline{x_2}$					$\overline{x_4}$	$\overline{x_3}$				

De acordo com a figura, representamos a equação por um sistema de equações de

palavras usando um conjunto de 8 variáveis com os seus duais $\{x_0, \overline{x_0}, \dots, x_7, \overline{x_7}\}$:

$$\begin{aligned} x_0 &= x_1 x_2 x_3 x_4 x_5, \\ \overline{x_0} &= \overline{x_5} x_6 x_7 \overline{x_6} \overline{x_7}, \\ \overline{x_1} &= x_3, \\ \overline{x_2} &= x_4, \\ \overline{x_3} &= x_7, \\ \overline{x_4} &= x_6, \\ x_i &= \overline{x_i} \quad \forall 0 \leq i \leq 7. \end{aligned}$$

O sistema parece mais complicado que a equação original mas o modelo é mais claro com a figura. A palavra vv tem posições $0, \dots, 14$. Definimos

$$\begin{aligned} esq(x_0) &= 0, & esq(\overline{x_0}) &= 7, & esq(x_1) &= 0, & esq(\overline{x_1}) &= 2, \\ esq(x_2) &= 1, & esq(\overline{x_2}) &= 3, & esq(x_3) &= 2, & esq(\overline{x_3}) &= 11, \\ esq(x_4) &= 3, & esq(\overline{x_4}) &= 10, & esq(x_5) &= 4, & esq(\overline{x_5}) &= 7, \\ esq(x_6) &= 10, & esq(\overline{x_6}) &= 12, & esq(x_7) &= 11, & esq(\overline{x_7}) &= 13. \end{aligned}$$

O conjunto B de equações fronteira é definido pela lista:

$$\begin{aligned} (x_0, 7, \overline{x_0}, 14), & \quad (x_1, 1, \overline{x_1}, 3), & (x_2, 2, \overline{x_2}, 4), & \quad (x_3, 3, \overline{x_3}, 12), \\ (x_4, 4, \overline{x_4}, 11), & \quad (x_5, 7, \overline{x_5}, 10), & (x_6, 11, \overline{x_6}, 13), & \quad (x_7, 12, \overline{x_7}, 14). \end{aligned}$$

Num passo não-determinístico podemos escolher linguagens $L'_x \subseteq L_x$ e $L'_y \subseteq L_y$ tais que $\varphi(L'_x)$ e $\varphi(L'_y)$ são conjuntos singulares. Como exemplo podemos escolher $L'_x = \{a\}$ e $L'_y = b^*$. Obtemos a S -sequência $(a, b, a, b, 0, 0, b, a, b, a)$. A ordem linear é o triplo $(I, \leq, \varphi)$ onde $I = \{0, 1, 2, 3, 4, 7, 10, 11, 12, 13, 14\}$.

3.6 O teorema basilar

O resto do capítulo é dedicado à prova do teorema seguinte:

Teorema 3.24. É decidível se um sistema de equações fronteira tem solução.

Um passo importante é feito na proposição seguinte: podemos majorar o expoente de periodicidade na procura de uma solução.

Proposição 3.25. Dado um sistema de equações fronteira $\mathcal{B}$, podemos calcular um número $e(\mathcal{B})$ com a propriedade seguinte: se $\mathcal{B}$ é solúvel, então temos $\exp(\mathcal{B}) \leq e(\mathcal{B})$.

Embora pudéssemos basear a prova da proposição nas mesmas técnicas apresentadas na Secção 3.4 iremos prová-la via redução a equações de palavras pois ser-nos-á útil para outros resultados.

Lema 3.26. Há uma redução efectiva da solubilidade de um sistema de equações fronteira $\mathcal{B}$ ao problema da resolução de uma equação de palavras com restrições racionais tal que para toda a solução $w \in A^*$ da equação temos $\exp(\mathcal{B}) \leq \exp(w)$.

Demonstração. Seja $\mathcal{B} = ((\Gamma, \bar{\cdot}), (I, \leq, \varphi_I), \text{esq}, B)$ um sistema de equações fronteira. Podemos assumir que a ordem linear $(I, \leq, \varphi_I)$ é a representação canónica da S -sequência subjacente $s = (s_1, \dots, s_m)$. Introduzimos novas variáveis $y_1, \dots, y_m$ com restrições racionais $\psi(y_p) = s_p$ para $1 \leq p \leq m$.

Para cada equação fronteira $b = (x, i, \bar{x}, j) \in B$ introduzimos a equação de palavras

$$y_{\text{esq}(x)+1} \cdots y_i = y_{\text{esq}(\bar{x})+1} \cdots y_j.$$

Este sistema de equações de palavras com restrições racionais é solúvel se e só se $\mathcal{B}$ é solúvel. De facto, se $w \in A^*$ é solução de $\mathcal{B}$, então, por definição, temos $(I, \leq, \varphi_I) \leq_\rho w_S$ e $\rho(I)$ é um subconjunto de posições de w . Todas as equações de palavras

$$w(\rho(\text{esq}(x)), \rho(i)) = w(\rho(\text{esq}(\bar{x})), \rho(j))$$

são satisfeitas para $(x, i, \bar{x}, j) \in B$. Logo, definindo $\sigma(y_p) = w(\rho(p-1), \rho(p))$ com $1 \leq p \leq m$ leva a uma solução do sistema de equações de palavras.

Reciprocamente, seja $\sigma(y_p) = v_p$ com $1 \leq p \leq m$ uma solução do sistema de equações de palavras. Devido às restrições racionais temos $\psi(y_p) = s_p$ e $v_p \neq \epsilon$ para qualquer $1 \leq p \leq m$. Assim, a palavra $v = \sigma(y_1) \cdots \sigma(y_m)$ é solução de $\mathcal{B}$.

Transformamos o sistema de equações de palavras numa única equação $E = D$ usando a Proposição 3.3 e reduzimos à equação $Ey_1 \cdots y_m = Dy_1 \cdots y_m$. Se w é uma solução desta última equação, então algum sufixo v de w é solução de $\mathcal{B}$. Logo, $\text{exp}(\mathcal{B}) \leq \text{exp}(v) \leq \text{exp}(w)$. Isto mostra o lema. $\square$

Demonstração da Proposição 3.25. Consideremos a equação $Ey_1 \cdots y_m = Dy_1 \cdots y_m$ construída na demonstração do lema anterior. Seja d o comprimento notacional de $Ey_1 \cdots y_m = Dy_1 \cdots y_m$. Então definimos o número $e(\mathcal{B}) = e(c(S), d)$ onde $e(c(S), d)$ é o número calculado no Teorema 3.14 em relação a esta última equação. Podemos escolher w tal que $\text{exp}(w) \leq e(c(S), d)$. Isto prova a proposição. $\square$

3.7 A condição da cadeia convexa

Seja $\mathcal{B} = ((\Gamma, \bar{\cdot}), (I, \leq, \varphi_I), \text{esq}, B)$ um sistema de equações fronteira. Daqui em diante, uma equação fronteira $b = (x, i, \bar{x}, j) \in B$ será também denominada de *tijolo*. A variável x é chamada de *etiqueta* do tijolo $b = (x, i, \bar{x}, j)$. Representaremos um tijolo da seguinte forma:

x	i
$\bar{x}$	j

O tijolo *dual* $\bar{b}$ de $b = (x, i, \bar{x}, j)$ é dado pela inversão do tijolo e é etiquetado de $\bar{x}$:

$\bar{x}$	j
x	i

Suponhamos que B é fechado para duais, isto é, $b \in B$ implica $\bar{b} \in B$, e que há pelo menos um tijolo $b \in B$ com a etiqueta x para todo o $x \in \Gamma$. Para $x \in \Gamma$ seja $B(x) \subseteq B$ o subconjunto de tijolos com etiqueta x . Então $B(x) = \{(x, i_1, \bar{x}, j_1), \dots, (x, i_r, \bar{x}, j_r)\}$ para algum subconjunto não-vazio $\{i_1, \dots, i_r\} \subseteq I$ tal que $esq(x) \leq i_1 \leq \dots \leq i_r$. O *limite direito* de x é definido por $dir(x) = i_r$.

Antes de continuarmos, fazemos algumas suposições adicionais em B . Todas elas são condições necessárias para a solubilidade e facilmente verificadas.

Sejam $(x, i, \bar{x}, j), (y, i, \bar{y}, j), (y, i', \bar{y}, j') \in B$. Assumimos desde já que:

- $esq(x) \leq esq(\bar{x})$ se e só se $i \leq j$,
- $\varphi_I(esq(x), i) = \varphi_I(esq(\bar{x}), j)$,
- $esq(x) \leq esq(y)$ se e só se $esq(\bar{x}) \leq esq(\bar{y})$,
- $i \leq i'$ se e só se $j \leq j'$.

Suponhamos que w é solução de $\mathcal{B}$. Então $w(esq(x), i) = w(esq(\bar{x}), j)$ para qualquer $(x, i, \bar{x}, j) \in B$. Como $esq(x), esq(\bar{x}), i$ e j são posições de w não podemos ter $esq(x) < esq(\bar{x})$ e $i > j$ e vice-versa. De modo análogo, se considerarmos os tijolos $(x, i, \bar{x}, j), (y, i, \bar{y}, j) \in B$ obtemos as igualdades $w(esq(x), i) = w(esq(\bar{x}), j)$ e $w(esq(y), i) = w(esq(\bar{y}), j)$ e portanto se $esq(x) < esq(y)$, então $esq(\bar{x}) < esq(\bar{y})$ e reciprocamente. Analogamente, para os tijolos $(y, i, \bar{y}, j), (y, i', \bar{y}, j') \in B$ temos a última condição. Finalmente, $\varphi_I(esq(x), i) = \varphi(w(esq(x), i)) = \varphi(w(esq(\bar{x}), j)) = \varphi_I(esq(\bar{x}), j)$.

Estas considerações implicam que se $B(x) = \{(x, i_1, \bar{x}, j_1), \dots, (x, i_r, \bar{x}, j_r)\}$ é tal que $esq(x) \leq i_1 \leq \dots \leq i_r$, então também temos $esq(\bar{x}) \leq j_1 \leq \dots \leq j_r$. Em particular, $B(x)$ contém um tijolo $(x, dir(x), \bar{x}, dir(\bar{x}))$. O conjunto $B(x)$ pode ser descrito como se segue:

$$B(x) = \left\{ \begin{array}{|c|c|} \hline x & i_1 \\ \hline \bar{x} & j_1 \\ \hline \end{array}, \begin{array}{|c|c|} \hline x & i_2 \\ \hline \bar{x} & j_2 \\ \hline \end{array}, \dots, \begin{array}{|c|c|} \hline x & dir(x) \\ \hline \bar{x} & dir(\bar{x}) \\ \hline \end{array} \right\}$$

Nas nossas figuras um tijolo $(x, i, \bar{x}, j)$ pode ser colocado em cima de $(y, j', \bar{y}, l)$ se e só se $j = j'$. Obtemos uma destas três configurações:

x	i	x	i	x	i
$\bar{x}$	j	$\bar{x}$	j	$\bar{x}$	j
	y	y	j	y	j
	$\bar{y}$	$\bar{y}$	l	$\bar{y}$	l

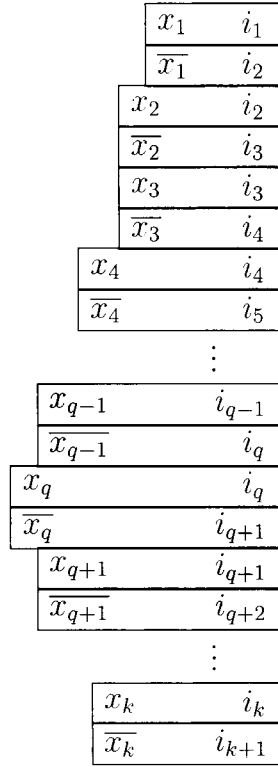


Figura 3.3: Uma cadeia convexa

Cada um destes casos é determinado pela função $esq : \Gamma \rightarrow I$. A figura da esquerda corresponde a $esq(\bar{x}) < esq(y)$, a do centro a $esq(\bar{x}) = esq(y)$ e a da direita a $esq(\bar{x}) > esq(y)$.

Seja $k \geq 1$. Uma *cadeia de comprimento k* é uma sequência de tijolos

$$((x_1, i_1, \bar{x}_1, i_2), (x_2, i_2, \bar{x}_2, i_3), \dots, (x_k, i_k, \bar{x}_k, i_{k+1})), \quad (3.3)$$

onde $(x_p, i_p, \bar{x}_p, i_{p+1}) \in B$ para qualquer $1 \leq p \leq k$.

Para uma cadeia C e uma variável $x \in \Gamma$ definimos o x -*comprimento de C* , $|C|_x$, como o número de tijolos em C com etiqueta x . O *comprimento de uma cadeia C* é a soma $\sum_{x \in \Gamma} |C|_x$.

Uma cadeia C de comprimento k diz-se *convexa* se, para algum índice q com $1 \leq q \leq k$, tivermos:

$$\begin{aligned} esq(\bar{x}_p) &\geq esq(x_{p+1}) && \text{para } 1 \leq p < q, \\ esq(\bar{x}_p) &\leq esq(x_{p+1}) && \text{para } q \leq p < k. \end{aligned}$$

Uma cadeia convexa C diz-se *reduzida* se os tijolos de C forem distintos dois a dois.

Um tijolo $(x, i, \bar{x}, j)$ está *ligado por uma cadeia convexa* a um tijolo $(x', i', \bar{x}', j')$ se existir uma cadeia convexa (3.3) de comprimento k para algum $k \geq 1$ tal que $(x, i, \bar{x}, j) = (x_1, i_1, \bar{x}_1, i_2)$ e $(x', i', \bar{x}', j') = (x_k, i_k, \bar{x}_k, i_{k+1})$.

Notemos que, se $C = (b_1, \dots, b_k)$ é uma cadeia convexa, então o seu dual $\overline{C} = (\overline{b_k}, \dots, \overline{b_1})$ e $(b_p, \dots, b_q)$ com $1 \leq p \leq q \leq k$ são também cadeias convexas. Se $b_p = (x_p, i_p, \overline{x_p}, i_p)$ para algum $1 < p < k$ então $(b_1, \dots, b_{p-1}, b_{p+1}, \dots, b_k)$ é uma cadeia convexa. Se $b_p = b_q$ para algum $1 < p < q \leq k$ então $(b_1, \dots, b_{p-1}, b_q, \dots, b_k)$ é também uma cadeia convexa. Em particular, se dois tijolos estiverem unidos por uma cadeia convexa, então eles estão ligados por alguma cadeia convexa reduzida. A menor cadeia que liga dois tijolos é sempre reduzida.

Seja $\mathcal{F} \subseteq I$ um subconjunto. Um tijolo $(x, i, \overline{x}, j) \in B$ é chamado *base* ou *suporte* de $\mathcal{F}$ se $j \in \mathcal{F}$. Dizemos que $\mathcal{B}$ satisfaz a *condição da cadeia convexa* (com respeito a $\mathcal{F}$), se todo o tijolo $b \in B$ puder ligar-se por alguma cadeia convexa a alguma base de $\mathcal{F}$. O conjunto $\mathcal{F}$ é também denominado o conjunto de *índices finais*.

No que se segue, concentrar-nos-emos em sistemas solúveis e precisaremos de mais algumas notações. Seja $\mathcal{B} = ((\Gamma, ^-), (I, \leq, \varphi_I), esq, B)$ um sistema solúvel de equações fronteira e $w \in A^*$ tal que $w \models (I, \leq, \varphi_I)$ é uma solução de $\mathcal{B}$. Como w é uma solução, podemos assumir que I é um subconjunto de posições de w . Para todo o $x \in \Gamma$ definimos uma palavra $w(x) \in A^*$ por

$$w(x) = w(esq(x), dir(x)).$$

Isto também permite introduzir a definição de *w-comprimento* para $x \in \Gamma$. Definimos

$$|x|_w = |w(x)|.$$

Mais ainda, para cada tijolo $b = (x, i, \overline{x}, j) \in B$ definimos também o seu *w-comprimento* por

$$|b|_w = |w(esq(x), i)| = i - esq(x).$$

Para todo o $x \in \Gamma$ e todo o $b \in B$ temos $w(x) = w(\overline{x})$, $|x|_w = |\overline{x}|_w$, $|b|_w = |\overline{b}|_w$, e $|b|_w \leq |x|_w$ se x for a etiqueta de b . Um tijolo é completamente determinado pela sua etiqueta e o seu *w-comprimento* $|b|_w$. No lema seguinte obtemos um majorante do número de tijolos num sistema de equações fronteira. Trata-se de um lema de C. Gutiérrez [12] que sofreu uma ligeira alteração da responsabilidade do autor desta monografia.

Lema 3.27 (Gutiérrez, 1998). Sejam $n, m, f \in \mathbb{N}$, $\mathcal{B} = ((\Gamma, ^-), (I, \leq, \varphi_I), esq, B)$ um sistema solúvel de equações fronteira e $w \models (I, \leq, \varphi_i)$ uma solução de $\mathcal{B}$. Sejam $|\Gamma| = 2n$, $\mathcal{F} \subseteq I$ e $|\mathcal{F}| = f$. Suponhamos que todo o tijolo $b \in B$ pode ser ligado por uma cadeia convexa C a uma base de $\mathcal{F}$ tal que, para cada $x \in \Gamma$, o número de tijolos em C com etiqueta x é no máximo m , isto é, $|C|_x \leq m$. Então podemos limitar o cardinal de B por

$$|B| \leq 2n \cdot f \cdot (m+1)^{2n}.$$

Demonstração. Consideremos uma cadeia convexa C de comprimento k tal que $|C|_x \leq m$ para todo o $x \in \Gamma$ onde o último tijolo é uma base:

$$C = ((x_1, i_1, \overline{x_1}, i_2), (x_2, i_2, \overline{x_2}, i_2), \dots, (x_k, i_k, \overline{x_k}, i_{k+1})).$$

Existem $2n$ possíveis etiquetas para o primeiro tijolo. Calculemos um majorante para o número de possíveis w -comprimentos do primeiro tijolo $(x_1, i_1, \overline{x_1}, i_2)$. O w -comprimento do primeiro tijolo é determinado pela soma do w -comprimento do último tijolo $(x_k, i_k, \overline{x_k}, i_{k+1})$ e dos valores $esq(x_{i+1}) - esq(\overline{x_i})$ para $i = k - 1, \dots, 1$ (que são a diferença dos w -comprimentos de b_{i+1} e b_i). Notemos que $i \in I$ representa a posição na solução w logo $esq(x_{i+1}) - esq(\overline{x_i}) \in \mathbb{Z}$. Portanto, o w -comprimento do primeiro tijolo é

$$i_{k+1} - esq(\overline{x_k}) + esq(x_k) - esq(\overline{x_{k-1}}) + \dots + esq(x_2) - esq(\overline{x_1}).$$

Podemos reordenar as parcelas desta soma obtendo uma expressão do tipo

$$i_{k+1} - esq(x_1) + \sum_{x \in \Gamma} m_x \cdot (esq(x) - esq(\overline{x}))$$

onde, por hipótese, $0 \leq m_x \leq m$. O valor $esq(x_1)$ é completamente determinado pela etiqueta x_1 e i_{k+1} é uma base. Logo, podem ser produzidos no máximo

$$f \cdot (m + 1)^{2n}$$

valores diferentes usando estas somas, quando a etiqueta x_1 é fixada. Então, há no máximo

$$2n \cdot f \cdot (m + 1)^{2n}$$

primeiros tijolos diferentes. Mas isto é também um majorante do número de tijolos de B pois, pela condição da cadeia convexa, cada tijolo pode ser ligado à base por uma tal cadeia. $\square$

Todo o sistema de equações fronteira $\mathcal{B}$ satisfaz, trivialmente, a condição da cadeia convexa com respeito ao conjunto I . Além disso, se construirmos $\mathcal{B}$ começando por uma equação nas palavras $x_1 \dots x_g = x_{g+1} \dots x_d$ com $1 \leq g < d$, teremos $|I| \leq d$. As regras de transformação que estudaremos na secção seguinte não aumentam o número $2n$ das variáveis nem a soma $2n + f$. Aumentam os cardinais de I e de B . Contudo, o lema anterior diz que um grande número de equações fronteira (ou seja, um conjunto grande de tijolos) faz com que haja longas cadeias convexas de modo a que a condição da cadeia convexa seja satisfeita (figurativamente: muitos tijolos constróiem *arranha-céus*). Em seguida, veremos que longas cadeias convexas levam a torres dominó com grandes alturas e portanto a um minorante do expoente de periodicidade em qualquer solução.

Proposição 3.28. *Sejam $n, m \in \mathbb{N}$ e $\mathcal{B} = ((\Gamma, ^-), (I, \leq, \varphi_I), esq, B)$ um sistema solúvel de equações fronteira com $|\Gamma| = 2n$. Seja $w \models (I, \leq, \varphi_I)$ uma solução de $\mathcal{B}$. Suponhamos que há pelo menos uma cadeia convexa reduzida C tal que $m \leq |C|_x$ para algum $x \in \Gamma$. Então temos o seguinte minorante para o expoente de periodicidade da solução w :*

$$m \leq 2n \cdot (exp(w) + 1).$$

Demonstração. A hipótese implica $n \neq 0$, logo $w \neq \epsilon$. A proposição é trivial para $m \leq 4n$. Portanto, seja $n \geq 1$ e $m > 4n$. Definimos $h = \lceil \frac{m}{2n} \rceil$. Temos $h \geq 3$.

Seja $C = (b_1, \dots, b_k)$ uma cadeia convexa reduzida tal que $m \leq |C|_x$ para algum $x \in \Gamma$. Seja $b_p = (x_{i_p}, i_p, \overline{x_{i_p}}, i_{p+1})$ para $1 \leq p \leq k$. Definimos $m' = \lceil \frac{m}{2} \rceil$ e, por dualidade, substituindo C por $\overline{C}$ e x por $\overline{x}$, podemos assumir que a etiqueta x ocorre pelo menos m' vezes na parte superior da cadeia convexa como vemos na figura seguinte:

	x_1	i_1
	$\overline{x_1}$	i_2
	x_2	i_2
	$\overline{x_2}$	i_3
	x_3	i_3
	$\overline{x_3}$	i_4
	x_4	i_4
	$\overline{x_4}$	i_5
	$\vdots$	$\vdots$
	$x_{k'}$	$i_{k'}$
	$\overline{x_{k'}}$	$i_{k'+1}$

onde $k' \leq k$. Temos

$$esq(\overline{x_1}) \geq esq(x_2), esq(\overline{x_2}) \geq esq(x_3), \dots, esq(\overline{x_{k'-1}}) \geq esq(x_{k'}).$$

No que se segue, necessitamos de uma cadeia apropriada onde a etiqueta do último tijolo tem w -comprimento mínimo. De modo a encontrarmos tal cadeia, examinamos os $|x_i|_w$ -comprimentos, $1 \leq i \leq k'$, das etiquetas dos tijolos da cadeia $(b_1, \dots, b_{k'})$ da direita para a esquerda. Como $|\Gamma| = 2n$, há no máximo n w -comprimentos. Encontramos a sequência de índices

$$0 = p_0 < p_1 < \dots < p_{n'-1} < p_{n'} = k'$$

tal que $n' \leq n$ e, para quaisquer q, j onde $p_{j-1} < q \leq p_j$ com $1 \leq j \leq n'$, temos

$$|x_q|_w \geq |x_{p_j}|_w.$$

De outro modo, o primeiro índice que escolhemos é k' . Começamos a subir na cadeia comparando os $|x_i|_w$ -comprimentos, $1 \leq i < k'$, com $|x_{k'}|_w$. Se encontrarmos um tijolo b_p com $|x_p|_w < |x_{k'}|_w$, então escolhemos esse índice e continuamos o mesmo processo comparando agora os $|x_i|_w$ -comprimentos, $1 \leq i < p$, com $|x_p|_w$. Em particular, em cada intervalo $[p_{j-1} + 1, p_j]$ a última etiqueta x_{p_j} tem w -comprimento mínimo. Como $n' \leq n$, pelo princípio do “pombal”, há pelo menos um índice $j \in \{1, \dots, n'\}$ tal que o número de ocorrências da etiqueta x no intervalo $[p_{j-1}, p_j]$ é no mínimo

$$\lceil \frac{m}{2n} \rceil.$$

Concluimos que existe uma cadeia convexa $C = (b_1, \dots, b_l)$ e uma variável $x \in \Gamma$ com as seguintes propriedades:

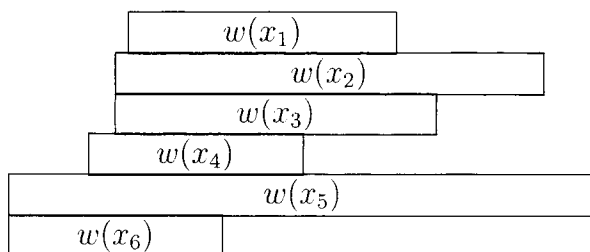
$$\begin{aligned} |C|_x &= \lceil \frac{m}{2n} \rceil, \\ esq(\overline{x}_p) &\geq esq(x_{p+1}) \quad \text{para } 1 \leq p < l, \\ |x_p|_w &\geq |x_l|_w \quad \text{para } 1 \leq p \leq l. \end{aligned}$$

Lembremos que $h = \lceil \frac{m}{2n} \rceil$. Temos $h \geq 3$ e a etiqueta x ocorre exactamente h vezes na cadeia convexa reduzida C . Cortando a sequência podemos assumir que x é a primeira etiqueta x_1 .

Este é o ponto onde ligamos a cadeia à sequência de palavras

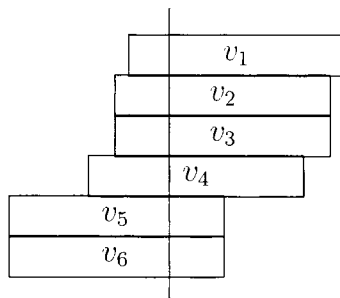
$$(w(x_1), \dots, w(x_l)).$$

Obtemos uma torre de palavras onde $w(x_l)$ tem comprimento mínimo e a palavra $w(x_1)$ ocorre no mínimo h vezes. Dizemos no mínimo pois poderá existir uma etiqueta x_i com $x_i \neq x_1, 1 < i \leq l$, tal que $w(x_1) = w(x_i)$.



Esta figura descreve certas igualdades entre factores das palavras. Notemos que, se $(x_1, i_1, \overline{x}_1, i_2)$ está colocado em cima de $(x_2, i_2, \overline{x}_2, i_3)$, então temos $w(esq(x_1), i_1) = w(esq(\overline{x}_1), i_2)$ que é sufixo de $w(esq(x_2), i_2) = w(esq(\overline{x}_2), i_3)$. Assim, $w(x_1) = w(\overline{x}_1)$ e $w(x_2) = w(\overline{x}_2)$ têm um factor comum. Isto acontece em todos os tijolos da cadeia.

Definimos $v_p \in A^*$ como o prefixo de $w(x_p) = w(esq(x_p), dir(x_p))$ de comprimento $|w(x_l)| = |v_l|$ e fazemos $u_p = w(esq(x_p), i_p)$ para $1 \leq p \leq l$. Como $|u_p| \leq |w(esq(x_l), i_l)| \leq |v_l| = |v_p|$ pois escolhemos a parte superior da cadeia convexa inicial, a palavra u_p é um prefixo de v_p para qualquer $1 \leq p \leq l$. A sequência $(v_1, \dots, v_l)$ pode ser arranjada numa torre de palavras que tem uma melhor configuração: todas as palavras v_p têm o mesmo comprimento.



A linha vertical corresponde à factorização $v_p = u_p u'_p$ com $1 \leq p \leq l$.

Finalmente, seja $\{q_1, q_2, \dots, q_h\}$ o conjunto dos h índices onde os tijolos têm etiqueta x_1 . Como a cadeia convexa que conduz a esta torre é reduzida (este é o único ponto onde o facto de ser reduzida é usado), temos $u_{q_i} \neq u_{q_j}$ para quaisquer $1 \leq i, j \leq h$ com $i \neq j$. Obtemos

$$0 \leq |u_{q_1}| < |u_{q_2}| < \dots < |u_{q_h}|.$$

Mais ainda, temos $v_1 = v_{q_1} = v_{q_2} = \dots = v_{q_h}$. Omitimos todas as outras palavras na torre acima e vemos que a palavra v_1 está arranjada numa torre dominó de altura h e $h \geq 2$. Usando o Lema 3.7 obtemos $h - 1 \leq \exp(v_1) \leq \exp(w)$ pois v_1 é factor de w e portanto

$$\left(h - 1 \leq \exp(w) \wedge h \geq \frac{m}{2n}\right) \Rightarrow \frac{m}{2n} \leq \exp(w) + 1 \Leftrightarrow m \leq 2n \cdot (\exp(w) + 1).$$

□

Corolário 3.29. Sejam $n, f \in \mathbb{N}$ e $\mathcal{B} = ((\Gamma, ^-), (I, \leq, \varphi_I), \text{esq}, B)$ um sistema solúvel de equações fronteira que satisfaz a condição da cadeia convexa com respeito a algum subconjunto $\mathcal{F} \subseteq I$. Sejam $|\Gamma| = 2n$ e $|\mathcal{F}| = f$. Então temos

$$|B| \leq 2n \cdot f \cdot (2n(\exp(\mathcal{B}) + 1) + 1)^{2n}.$$

Se $|\Gamma|, |\mathcal{F}| \in \mathcal{O}(d)$ e $\exp(\mathcal{B}) \in 2^{\mathcal{O}(d + \log c(S))}$, então temos

$$|B| \in 2^{\mathcal{O}(d^2 + d \log c(S))}.$$

Demonstração. Seja m o máximo x -comprimento de uma cadeia convexa reduzida com $x \in \Gamma$. Pelo Lema 3.27 temos

$$|B| \leq 2n \cdot f \cdot (m + 1)^{2n}.$$

Escolhemos uma solução w tal que $\exp(w) = \exp(\mathcal{B})$. Pela Proposição 3.28 temos

$$m \leq 2n(\exp(w) + 1).$$

Juntando as condições obtemos

$$|B| \leq 2n \cdot f \cdot (2n(\exp(w) + 1) + 1)^{2n} = 2n \cdot f \cdot (2n(\exp(\mathcal{B}) + 1) + 1)^{2n}.$$

Temos

$$\begin{aligned} |B| &\leq c_1 d \cdot c_2 d \cdot [c_1 d \cdot (2^{c_3(d + \log(c(S)))} + 1) + 1]^{c_1 d} \\ &\leq c' (c'' \cdot 2^{c_3(d + \log(c(S)))})^{c_1 d} \\ &\leq c''' \cdot 2^{c_4(d^2 + d \log(c(S)))} \\ &\leq 2^{c(d^2 + d \log(c(S)))} \end{aligned}$$

para alguns $c_1, c_2, c_3, c_4, c', c'', c''', c \in \mathbb{R}$ e portanto

$$|B| \in 2^{\mathcal{O}(d^2 + d \log c(S))}.$$

□

3.8 As regras de transformação

Estamos aptos a definir as *regras de transformação* (não-determinísticas) do Algoritmo de Makanin. Se aplicarmos uma regra a um sistema $\mathcal{B} = ((\Gamma, -), (I, \leq, \varphi_I), \text{esq}, B)$, o novo sistema representar-se-á por $\mathcal{B}' = ((\Gamma', -), (I', \leq, \varphi_{I'}), \text{esq}', B')$. As regras de transformação têm a propriedade seguinte:

Se $\mathcal{B} = ((\Gamma, -), (I, \leq, \varphi_I), \text{esq}, B)$ satisfaz a condição da cadeia convexa com respeito a um subconjunto $\mathcal{F} \subseteq I$, então $\mathcal{B}'$ satisfaz a condição da cadeia convexa com respeito a algum subconjunto $\mathcal{F}' \subseteq I'$ tal que $|\Gamma'| + |\mathcal{F}'| \leq |\Gamma| + |\mathcal{F}|$.

Assim, se começarmos com um sistema $\mathcal{B}_0$ onde $|\Gamma_0| = 2n_0$ e $|I_0| \leq d$, então durante todo o procedimento o cardinal do conjunto de índices finais será menor ou igual a $2n_0 + d$.

Dizemos que uma regra (não-determinística) é *correcta no sentido descendente* se a seguinte condição se verificar:

Se $w \in A^*$ é uma solução de $\mathcal{B}$, então algum sufixo w' de w é uma solução de $\mathcal{B}'$ e ainda se tem $|\Gamma'| < |\Gamma|$ ou $|w'| < |w|$.

Assim, aplicando a sistemas solúveis pelo menos uma sequência de escolhas de regras correctas no sentido descendente leva ao término, ou seja, obtemos $|\Gamma'| = 0$ e, como já foi visto atrás, o sistema $\mathcal{B}'$ é solúvel ou obtemos $w' = \epsilon$ como modelo de $\mathcal{B}'$.

Dizemos que uma regra (não-determinística) é *correcta no sentido ascendente* se se verificar a condição:

Se $w' \in A^*$ é uma solução de $\mathcal{B}'$, então existe uma palavra $w \in A^*$ que é solução de $\mathcal{B}$.

Regra 1. Se houver algum $x \in \Gamma$ com $\text{esq}(x) = \text{dir}(x)$ então eliminamos os tijolos

$$(x, \text{dir}(x), \bar{x}, \text{dir}(\bar{x})) \text{ e } (\bar{x}, \text{dir}(\bar{x}), x, \text{dir}(x))$$

de B . Eliminamos x e $\bar{x}$ de Γ .

Obviamente, a Regra 1 é correcta no sentido ascendente e descendente visto termos $w(i, i) = \epsilon$ para todas as palavras w e todas as posições i de w . Logo, o conjunto das soluções é o mesmo. De modo a preservar a condição da cadeia convexa, introduzimos dois índices finais. Seja $x \in \Gamma$ tal que $\text{esq}(x) = \text{dir}(x)$ e suponhamos que $x, \bar{x}$ foram eliminadas pela Regra 1. Definimos $\mathcal{F}' = \mathcal{F} \cup \{\text{esq}(x), \text{esq}(\bar{x})\}$. Consideremos a cadeia convexa $C = (b_1, \dots, b_m)$ onde para algum $1 < p \leq m$ o tijolo b_p tem a forma $b_p = (x, \text{dir}(x), \bar{x}, \text{dir}(\bar{x}))$. Assim, o tijolo b_p foi cancelado. No entanto, o

tijolo b_1 está ligado a b_{p-1} por uma cadeia convexa e b_{p-1} é agora uma base visto que $esq(x) = dir(x) \in \mathcal{F}'$. Assim, se $\mathcal{B}$ satisfaz a condição da cadeia convexa com respeito a $\mathcal{F}$, então o sistema $\mathcal{B}'$ (depois de aplicarmos a Regra 1) satisfaz também a condição da cadeia convexa com respeito a $\mathcal{F}'$. Temos

$$|\Gamma'| + |\mathcal{F}'| \leq |\Gamma| + |\mathcal{F}|.$$

A desigualdade estrita resulta de termos $\mathcal{F} \cap \{esq(x), esq(\bar{x})\} \neq \emptyset$.

Regra 2. Se existir algum $x \in \Gamma$ com $esq(x) = esq(\bar{x})$, então eliminamos todos os tijolos $(x, j, \bar{x}, j)$ e $(\bar{x}, j, x, j)$ de B . Eliminamos x e $\bar{x}$ de Γ .

Relembramos que para $(x, i, \bar{x}, j) \in B$ temos $esq(x) = esq(\bar{x})$ se e só se $i = j$. Então, se $esq(x) = esq(\bar{x})$, todos os tijolos de etiqueta x têm a forma $(x, j, \bar{x}, j)$. Assim, para todo o tijolo $(x, j, \bar{x}, j) \in B$ com $esq(x) = esq(\bar{x})$ temos trivialmente $w(esq(x), j) = w(esq(\bar{x}), j)$ para todas as palavras w . Logo, o conjunto das soluções é o mesmo. Mais uma vez, a Regra 2 é correcta nos sentidos ascendente e descendente. Para a condição da cadeia convexa, consideremos a cadeia convexa $C = (b_1, \dots, b_m)$ onde $b_p = (x, j, \bar{x}, j)$ para algum $1 < p \leq m$. Se tivermos $p < m$, então $C' = (b_1, \dots, b_{p-1}, b_{p+1}, b_m)$ é uma cadeia convexa menor que liga b_1 a uma base. Para $p = m$ temos $j \in \mathcal{F}$. Logo, b_{m-1} é também uma base. Temos

$$|\Gamma'| + |\mathcal{F}'| < |\Gamma| + |\mathcal{F}|.$$

Regra 3. Seja $l = \min(I)$. Se $l \notin esq(\Gamma)$, então cancelamos o índice l de I . Isto significa que substituímos a ordem linear sobre S pela sub-ordem induzida $(I', \leq, \varphi_{I'})$ onde $I' = I \setminus \{l\}$.

É claro que a condição da cadeia convexa não é afectada por esta regra. Obviamente, a regra é correcta no sentido descendente. Para vermos que é correcta no sentido ascendente, seja $(I, \leq, \varphi_I)$ dada pela S -sequência $(s_1, \dots, s_m)$ e seja $w' \in A^*$ a solução do novo sistema depois de aplicada a Regra 3 de modo que $\min(I')$ é a primeira posição de w' . Por definição de S -sequência, existe uma palavra não-vazia $u \in A^+$ com $\varphi(u) = s_1$. Então a primeira posição de w' não é igual à primeira posição na palavra uw' e uw' é uma solução de $\mathcal{B}$. Para outros usos podemos escolher u tal que $|u| \leq |S|$ como se mostra no seguinte lema:

Lema 3.30. Sejam A um alfabeto, S um semigrupo finito e $\varphi : A^+ \rightarrow S$ uma aplicação sobrejectiva. Então, para todo o $s \in S$, existe $u \in A^+$ tal que $\varphi(u) = s$ e $|u| \leq |S|$.

Demonstração. Como φ é sobrejectiva, existe $v \in A^+$ tal que $\varphi(v) = s$. Se $|v| \leq |S|$, então podemos tomar $u = v$. Suponhamos que $|v| > |S|$. Seja v_n o prefixo de comprimento n de v . Então $v = v_n w_n$ para algum $w_n \in A^*$. Consideremos o conjunto

$$\{\varphi(v_n) : n = 1, \dots, |S| + 1\}.$$

Como S é finito, existem $1 \leq i < j \leq |S| + 1$ tal que $\varphi(v_i) = \varphi(v_j)$. Temos $\varphi(v) = \varphi(v_j)\varphi(w_j) = \varphi(v_i)\varphi(w_j) = \varphi(v_i w_j)$ e $|v_i w_j| < |v|$. O resultado segue por indução. $\square$

A próxima regra é mais complexa. É o coração do Algoritmo. Antes de a aplicarmos a um sistema $\mathcal{B} = ((\Gamma, \cdot), (I, \leq, \varphi_I), esq, B)$, aplicamos as Regras 1, 2 e 3 sempre que possível. Em particular, assumimos que $esq(x) < dir(x)$, $esq(x) \neq esq(\bar{x})$ para qualquer $x \in \Gamma$ e que existe algum $x \in \Gamma$ com $esq(x) = \min(I)$.

Regra 4. Definimos $l = \min(I)$ e $r = \max\{dir(x) \mid x \in \Gamma, esq(x) = l\}$. Notemos que $l \in esq(\Gamma)$, logo existe $r \in I$ e tem-se $l < r$. Escolhemos (e fixamos) algum $x_0 \in \Gamma$ com $esq(x_0) = l$ e $dir(x_0) = r$. Definimos $l^* = esq(\bar{x}_0)$ e $r^* = dir(\bar{x}_0)$. Definimos a *fronteira crítica* $c \in I$ por $c = \min\{c', r\}$ onde

$$c' = \min\{esq(x) \mid x \in \Gamma, r < dir(x)\}.$$

Notemos que, como $l = \min(I) = esq(x_0)$ e $esq(x_0) \neq esq(\bar{x}_0)$, então $r = dir(x_0) < dir(\bar{x}_0) = r^*$ pelas suposições feitas no início da Secção 3.7. Logo, o mínimo c' e portanto a fronteira crítica c existem. Temos $l < c \leq r < r^*$. A ordem de r e l^* depende do sistema mas não é importante.

Definimos o subconjunto $T \subseteq I$ das *posições de transporte* por

$$T = \{i \in I \mid i \leq c\} \cup \{i \in I \mid \exists (x, i, \bar{x}, j) \in B : esq(x) < c\}.$$

Notemos que $\min(T) = l$ e que $i \in T$ para todo o $(x_0, i, \bar{x}_0, j) \in B$. Mais ainda, como $esq(x) < c$ implica $dir(x) \leq r$, temos $\max(T) = r$.

Dividimos a Regra em seis passos:

Passo 1. Escolhemos uma extensão admissível $(I^*, \leq, \varphi_{I^*})$ de $(I, \leq, \varphi_I)$ por T em $[l^*, r^*]$. Por convenção, identificamos I como subconjunto de I^* e portanto $I \subseteq I^*$ e existe um subconjunto $T^* \subseteq I^*$ com $\min(T^*) = l^*$ e $\max(T^*) = r^*$ tal que T^* está em bijecção com T e respeita a ordem em T . Para cada $i \in T$ a posição correspondente em T^* é representada por i^* . Com estas notações fazemos uma restrição na extensão admissível: consideramos somente aquelas extensões onde, em primeiro lugar, $i < i^*$ para qualquer $i \in T$ e, em segundo, para qualquer $(x, i, \bar{x}, j) \in B$ com $esq(x) < c$ temos

$$\begin{aligned} esq(x)^* = esq(\bar{x}) &\Leftrightarrow i^* = j, \\ esq(x)^* < esq(\bar{x}) &\Leftrightarrow i^* < j. \end{aligned}$$

Em particular, para todos os tijolos $(x_0, i, \bar{x}_0, j)$ temos $i^* = j$. Se tal extensão não for possível então o Passo 1 não pode ser completado e a Regra 4 não é aplicável.

Passo 2. Introduzimos uma nova variável x_ν e o seu dual $\bar{x}_\nu$. Definimos $esq(x_\nu) = c$ e $esq(\bar{x}_\nu) = c^*$. Para todo o $i \in T$ tal que existe algum $(x, i, \bar{x}, j) \in B$ com $esq(x) < c \leq i$ introduzimos novos tijolos $(x_\nu, i, \bar{x}_\nu, i^*)$ e $(\bar{x}_\nu, i^*, x_\nu, i)$.

Passo 3. Enquanto houver uma variável $x \in \Gamma$ com $esq(x) < c$ substitui-se $esq(x)$ por $esq'(x) = esq(x)^*$ e substituem-se todos os tijolos $(x, i, \bar{x}, j)$, $(\bar{x}, j, x, i) \in B$ por $(x', i^*, \bar{x}, j)$ e $(\bar{x}, j, x', i^*)$.

Para dispormos de alguma notação seja x uma variável antes do Passo 3 e x' a variável correspondente depois de aplicarmos o passo. Do mesmo modo, seja $b = (x, i, \bar{x}, j)$ um tijolo antes do Passo 3 e $b' = (x', i', \bar{x}', j')$ o tijolo correspondente após a aplicação do passo. Se $esq(x) = esq'(x')$ então podemos escrever $x = x'$. Em particular, $x_\nu = x'_\nu, \bar{x}_\nu = \bar{x}'_\nu, \bar{x}_0 = \bar{x}'_0$ mas $x_0 \neq x'_0$.

Para $b = (x, i, \bar{x}, j)$ e $b' = (x', i', \bar{x}', j')$ há quatro casos:

$$\begin{aligned} b' &= (x', i^*, \bar{x}', j^*) && \text{se } esq(x) < c, \quad esq(\bar{x}) < c, \\ b' &= (x', i^*, \bar{x}, j) && \text{se } esq(x) < c, \quad c \leq esq(\bar{x}), \\ b' &= (x, i, \bar{x}', j^*) && \text{se } c \leq esq(x), \quad esq(\bar{x}) < c, \\ b' &= (x, i, \bar{x}, j) && \text{se } c \leq esq(x), \quad c \leq esq(\bar{x}). \end{aligned}$$

Notemos que após o Passo 3 todos os tijolos $(x_0, i, \bar{x}_0, j) \in B$ têm a forma $(x'_0, i^*, \bar{x}_0, i^*)$.

Passo 4. Definimos o novo conjunto de índices finais

$$\mathcal{F}' = \{i^* \in I^* \mid i < c \wedge i \in F\} \cup \{i \in F \mid c \leq i\}.$$

Passo 5. Cancelamos todos os tijolos com etiqueta x'_0 ou $\bar{x}_0$, isto é, cancelamos todos os tijolos da forma $(x'_0, i^*, \bar{x}_0, i^*)$ ou $(\bar{x}_0, i^*, x'_0, i^*)$. Em seguida, cancelamos as variáveis x_0 e $\bar{x}_0$.

Passo 6. Substituímos I^* por $I' = \{i \in I^* \mid c \leq i\}$ e consideramos a ordem linear $(I', \leq, \varphi_{I'})$ induzida por $(I^*, \leq, \varphi_{I^*})$.

Após o Passo 6 a regra de transformação está concluída. O novo sistema é representado por $\mathcal{B}' = ((\Gamma', -), (I', \leq, \varphi_{I'}), esq', B')$.

Lema 3.31. Temos $|\Gamma'| = |\Gamma|$ e $|\mathcal{F}'| \leq |\mathcal{F}|$.

Demonstração. No Passo 2 novas variáveis x_ν e $\bar{x}_\nu$ foram introduzidas mas no Passo 5 as variáveis x'_0 e $\bar{x}_0$ foram canceladas. Logo, $|\Gamma'| = |\Gamma|$. O conjunto de índices finais foi modificado no Passo 4 de forma que $|\mathcal{F}'| \leq |\mathcal{F}|$. $\square$

O lema seguinte é usado para majorar o cardinal de I durante o processo de transformação.

Lema 3.32. Sejam $\beta' = |\{(x', i', \bar{x}', j') \in B' \mid esq'(x') < i'\}|$ e $\beta = |\{(x, i, \bar{x}, j) \in B \mid esq(x) < i\}|$. Então temos

$$2|I'| - \beta' \leq 2|I| - \beta.$$

Demonstração. A desigualdade pode ser destruída quer por uma nova posição $i^* \in T^* \setminus I$ quer pelo cancelamento dos tijolos $(x'_0, i^*, \bar{x}_0, i^*)$ e $(\bar{x}_0, i^*, x'_0, i^*)$ no Passo 5, onde $i^* < i$. O cancelamento dos tijolos envolve também uma posição do tipo $i^* \in$

T^* . Se $(x'_0, i^*, \overline{x}_0, i^*)$ é cancelado onde $l^* < i^*$, então $i^* = j$ para algum $j \in I \setminus \{l\}$. Em particular, i^* não é uma nova posição e portanto os dois casos não ocorrem simultaneamente. É então suficiente ver que, para cada $i^* \in T^* \setminus \{l^*\}$, dois novos tijolos são introduzidos no Passo 2 ou uma posição é cancelada no Passo 6. Assim, o balanço total será negativo ou zero.

Consideremos as posições $i^* \in T^* \setminus \{l^*\}$ uma a uma. Se $c^* < i^*$, então, por definição de T e pelo Passo 2, há dois novos tijolos $(x_\nu, i, \overline{x}_\nu, i^*)$ e $(\overline{x}_\nu, i^*, x_\nu, i) \in B'$ e temos $esq(x_\nu) < i$ e $esq(\overline{x}_\nu) < i^*$. Consideremos depois $i^* = c^*$. Pelo menos uma posição (a l) é cancelada no Passo 6. Depois, seja $l^* < i^* < c^*$, isto é, $l < i < c$. A posição i é cancelada no Passo 6. Temos então a conclusão do lema. $\square$

Lema 3.33. A Regra 4 é correcta no sentido descendente.

Demonstração. Seja $w \in A^*$ uma solução de $\mathcal{B}$. Como $w \models (I, \leq, \varphi_I)$, podemos ver I como um subconjunto de posições de w com $l = 0$. Seja $w = vv'$ onde $v = w(l, c)$. A palavra v é um prefixo não-vazio de $w(l, r)$. A palavra $w(l, r)$ é um prefixo de w e ao mesmo tempo um outro factor de w' . Temos $w(l, r) = w(l^*, r^*)$ com $l < l^*$ devido ao tijolo $(x_0, r, \overline{x}_0, r^*) \in B$. O conjunto T é um subconjunto de posições de $w(l, r)$, logo encontramos o correspondente subconjunto T^* de posições de $w(l^*, r^*)$. A união $I \cup T^*$ leva a uma extensão admissível $(I^*, \leq, \varphi_{I^*})$ tal que, primeiro, $i < i^*$ para todo $i \in T$ e, segundo, $w(j, k) = w(j^*, k^*)$ para todos os $j, k \in T$ com $j \leq k$. Uma inspecção cuidada mas simples da Regra 4 mostra-nos que $w' \models (I', \leq, \varphi_{I'})$ e w' é uma solução de $\mathcal{B}'$. $\square$

Lema 3.34. A Regra 4 é correcta no sentido ascendente.

Demonstração. Seja $w' \in A^*$ uma solução de $\mathcal{B}'$. Como $w' \models (I', \leq, \varphi_{I'})$, podemos ver I' como um subconjunto de posições de w' onde c é a primeira posição de w' . Definimos $v = w'(l^*, c^*)$ e seja $w = vv'$. Então temos $w \models (I^*, \leq, \varphi_{I^*})$ tal que $v = w(l, c) = w(l^*, c^*)$. Com a ajuda dos tijolos $(x_\nu, i, \overline{x}_\nu, i^*)$, concluímos que $w(j, k) = w(j^*, k^*)$ para todos os $j, k \in T$ com $j \leq k$. Assim, temos $w(esq(x), i) = w(esq(\overline{x}), j)$ para todo o $(x, i, \overline{x}, j) \in B$. Como $I \subseteq I^*$, temos que $w \models (I, \leq, \varphi_I)$ e w é uma solução de $\mathcal{B}$. $\square$

Finalmente, mostramos que a Regra 4 preserva a condição da cadeia convexa. No Passo 1 é imediato, nos restantes usamos os lemas que se seguem.

Lema 3.35. O Passo 2 preserva a condição da cadeia convexa com respeito ao conjunto $\mathcal{F}$.

Demonstração. Os novos tijolos do Passo 2 têm a forma $(x_\nu, i, \overline{x}_\nu, i^*)$ e $(\overline{x}_\nu, i^*, x_\nu, i)$ para todos os $(x, i, \overline{x}, j) \in B$ tal que $esq(x) < c = esq(x_\nu) \leq i$. Como $(x, i, \overline{x}, j) \in B$ pode ser ligado por uma cadeia convexa a uma base, é suficiente considerar a seguinte figura:

	x_ν	i
	$\overline{x}_\nu$	i^*
	$\overline{x}_\nu$	i^*
	x_ν	i
x		i
$\overline{x}$		j

Logo, os dois novos tijolos podem ser ligados por uma cadeia convexa a uma base e portanto o Passo 2 preserva a condição da cadeia convexa. $\square$

Lema 3.36. Seja $C = (b_1, \dots, b_m)$ uma cadeia convexa antes do Passo 3 que liga b_1 a b_m . Então, após o Passo 3, existe uma cadeia convexa C' que liga b'_1 a b'_m .

Demonstração. Observemos localmente a cadeia convexa

$$C = (\dots, (x, i, \overline{x}, j), (y, j, \overline{y}, k), \dots).$$

Por simetria (trabalhando com os tijolos e a cadeia dual), podemos assumir que $esq(\overline{x}) \geq esq(y)$. Ilustramos esta parte da cadeia com a figura:

		$\vdots$
	x	i
	$\overline{x}$	j
y		j
$\overline{y}$		k
		$\vdots$

Esta é a situação antes do Passo 3. Após este denotemos os tijolos correspondentes por $(x', i', \overline{x}', j')$ e $(y', j'', \overline{y}', k')$. Isto leva à seguinte figura:

		$\vdots$
	x'	i'
	$\overline{x}'$	j'
		$\vdots$
y'		j''
$\overline{y}'$		k'
		$\vdots$

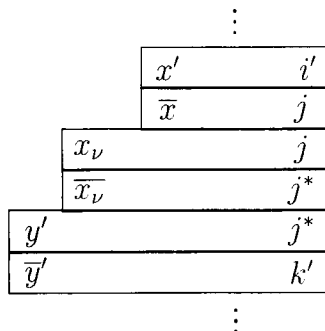
A questão está em se se tem $j' = j''$. Se $j' = j^*$ ou $j'' = j$, então temos $esq(\overline{x}) < c$ ou $esq(y) \geq c$ e, como $esq(y) < esq(\overline{x})$ (ver figura), resulta que $j' = j''$. Logo a cadeia não partirá neste local. Consideremos os casos $j' = j$ e $j'' = j^*$. Isto equivale a

$$esq(y) < c \leq esq(\overline{x}) < j.$$

Com a ajuda do tijolo $(x_\nu, j, \overline{x}_\nu, j^*)$ introduzido no Passo 2 podemos unir a cadeia partida. Temos

$$esq(x_\nu) = c \leq esq(\overline{x}) \quad e \quad esq'(y') < c^* = esq(\overline{x}_\nu)$$

e obtemos a seguinte figura:

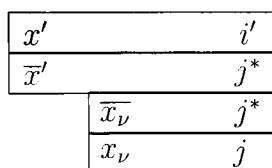


Fazendo esta transformação sempre que necessário construímos a cadeia convexa C' . □

Notemos que a cadeia C' construída poderá conter muitos tijolos da forma $(x'_0, i^*, \overline{x}_0, i^*)$ e $(\overline{x}_0, i^*, x'_0, i^*)$. Estes tijolos serão somente cancelados no Passo 5. De facto, a sua presença no seguinte lema é bastante útil.

Lema 3.37. Após o Passo 4 a condição da cadeia convexa é satisfeita com respeito ao conjunto $\mathcal{F}'$.

Demonstração. Seja b' um tijolo após o Passo 3 e b o tijolo correspondente antes do Passo 3. Este tijolo b está ligado por uma cadeia convexa a uma base $(x, i, \overline{x}, j)$ com $j \in \mathcal{F}$. O lema anterior constata que após o Passo 3 o tijolo b' está ligado por uma cadeia convexa ao tijolo correspondente $(x', i', \overline{x}', j')$. Para $j < c$ temos $esq(\overline{x}) < c$ e $j' = j^* \in \mathcal{F}'$. Logo $(x', i', \overline{x}', j^*)$ é uma base. Para $j' = j$ temos $c \leq j$ e por isso $j \in \mathcal{F}'$ estando este caso também resolvido. O outro caso é $c \leq j$ e $j' = j^*$, ou seja, quando $esq(\overline{x}) < c \leq j$. Pelo Passo 2 existe um tijolo $(\overline{x}_\nu, j^*, x_\nu, j)$ e temos $esq'(\overline{x}') < c^* = esq(\overline{x}_\nu)$. Podemos pôr o tijolo $(x', i', \overline{x}', j^*)$ colado à base $(\overline{x}_\nu, j^*, x_\nu, j)$. Como $j \in \mathcal{F} \cap \mathcal{F}'$, j é de facto uma base após o Passo 4. Obtemos a figura:



□

Lema 3.38. Os Passos 5 e 6 preservam a condição da cadeia convexa com respeito ao conjunto $\mathcal{F}'$.

Demonstração. O Passo 5 é um caso especial de uma aplicação da Regra 2. O Passo 6 é um caso especial das aplicações da Regra 3. Em particular, a condição da cadeia convexa é preservada. $\square$

Estes lemas conduzem-nos à seguinte proposição:

Proposição 3.39. *A Regra 4 é correcta nos sentidos ascendente e descendente e a condição da cadeia convexa é preservada.*

Exemplo 3.40. Consideremos a equação $x_1 \cdots x_g = x_{g+1} \cdots x_d$ com $1 \leq g < d$ e a aplicação $\psi : \Omega \rightarrow S$ que determina as restrições racionais. Seja

$$\mathcal{B} = ((\Gamma, ^-), (I, \leq, \varphi_I), esq, B)$$

o sistema de equações fronteira construído na Secção 3.5.2. Temos que $(I, \leq, \varphi_I)$ representa a S -sequência

$$(\psi(x_1), \dots, \psi(x_g), \psi(x_{g+1}), \dots, \psi(x_d)).$$

Assumimos que se trata da representação canónica, $I = \{0, \dots, d\}$. O conjunto Γ contém duas variáveis x_0 e $\bar{x}_0$ tais que $esq(x_0) = 0, dir(x_0) = g = esq(\bar{x}_0)$ e $dir(\bar{x}_0) = d$. O conjunto B contém no máximo $2d$ equações fronteira ou tijolos sendo um deles o seguinte:

x_0	g
$\bar{x}_0$	d

Temos $|I| = d + 1$ e $|\Gamma| = |B| \leq 2d$. Se a equação nas palavras tiver uma solução não-singular que satisfaz as restrições racionais, então $exp(\mathcal{B}) \leq 2 \cdot e(c(S), d)$ onde $e(c(S), d)$ é o valor calculado na Secção 3.4.

As Regras 1, 2 e 3 não são aplicadas a $\mathcal{B}$. Vejamos a Regra 4. Temos

$$x_0 = x_0, \quad l = 0, \quad c = g = r = l^* \quad \text{e} \quad c^* = g^* = r^* = d.$$

O conjunto T de posições de transporte é $T = \{0, \dots, g\}$ e o conjunto dos índices finais $\mathcal{F}$ é $\mathcal{F} = I$.

No Passo 1 temos de escolher alguma extensão admissível de $(I, \leq, \varphi_I)$ por T em $[g, d]$. Em geral, não é claro que tal extensão exista. Segundo a hipótese de $x_1 \cdots x_g = x_{g+1} \cdots x_d$ ter uma solução não-singular $\sigma : \Omega \rightarrow A^+$ com $\varphi \circ \sigma = \psi$ podemos continuar. Seja $v = \sigma(x_1 \cdots x_g)$ e assumimos que v tem comprimento minimal entre todas as soluções que satisfazem as restrições racionais dadas por ψ . Com a ajuda da palavra v o Passo 1 pode ser completado: definimos $w = vv$ obtendo assim

$$w \models (\psi(x_1), \dots, \psi(x_d)).$$

O conjunto de posições de w é $\{0, \dots, m, m+1, \dots, 2m\}$ onde $m = |v|$. O facto de w ser um modelo de $(I, \leq, \varphi_I)$ resulta da aplicação injectiva

$$\rho : \{0, \dots, d\} \rightarrow \{0, \dots, 2m\}$$

que respeita a ordem em I . Definimos $T^* = \{m + \rho(i) \mid 0 \leq i \leq g\}$ e $I^* = \rho(I) \cup T^*$. Como I^* é um subconjunto de posições de w , é induzida uma sub-ordem linear sobre S denotada por $(I^*, \leq, \varphi_{I^*})$. Temos $|I^*| \leq d + g$. Após renomeação assumimos $I^* = \{0, \dots, d\} \cup T^*$ e $T^* = \{0^*, \dots, g^*\}$ onde $0^* = c = g$ e $c^* = g^* = d$. Isto completa o Passo 1. Como, na realidade, não conhecemos v , a escolha de I^* é uma escolha não-determinística.

Os passos seguintes são determinísticos. No Passo 2 introduzimos novas variáveis x_ν e $\bar{x}_\nu$ com $esq(x_\nu) = g = dir(x_\nu)$ e $esq(\bar{x}_\nu) = d = dir(\bar{x}_\nu)$ pois, nesta equação, todo o tijolo $(x, i, \bar{x}, j) \in B$ com $esq(x) < c = g \leq i$ é tal que $i \leq c = g$.

No Passo 3 transportamos a estrutura do intervalo $[0, g]$ para $[0^*, g^*] = [g, d]$. Se continuarmos a ver I^* como subconjunto de posições de w , então temos um transporte de posições do primeiro para o segundo factor v na palavra $w = vv$.

No Passo 4 definimos

$$\mathcal{F}' = \{i \in I^* \mid g \leq i\}.$$

No Passo 5 cancelamos os tijolos $(x_0, d, \bar{x}_0, d)$ e $(\bar{x}_0, d, x_0, d)$ e as variáveis x_0 e $\bar{x}_0$.

No Passo 6 substituímos I^* por $I' = \mathcal{F}'$.

A Regra 4 está finalizada. A cardinalidade de I' é majorada por d . Seja $\mathcal{B}'$ o novo sistema. Então a palavra v é uma solução, $v \models (I', \leq, \varphi_{I'})$.

Como $esq(x_\nu) = dir(x_\nu) = g$, podemos aplicar a Regra 1 que cancela os tijolos $(x_\nu, g, \bar{x}_\nu, d)$ e $(\bar{x}_\nu, d, x_\nu, g)$ e as variáveis x_ν e $\bar{x}_\nu$ (que são desnecessárias). Após este passo temos o novo sistema $\mathcal{B}'' = ((\Gamma_0'', -), (I_0'', \leq, \varphi_{I_0''), esq_0'', B_0'')$. Temos $|I_0''| \leq d$ e $|\Gamma_0''| = |B_0''| \leq 2(d-1)$. A palavra v é agora solução de $\mathcal{B}''$ e portanto $exp(\mathcal{B}'') \leq exp(v)$. Assim, podemos escolher $e(\mathcal{B}'') = e(c(S), d)$.

3.9 A prova do teorema basilar

A prova do Teorema 3.24 está agora reduzida ao trabalho num grafo dirigido finito. Temos, inicialmente, um sistema de equações fronteira

$$\mathcal{B}_0 = ((\Gamma_0, -), (I_0, \leq, \varphi_{I_0}), esq_0, B_0).$$

Podemos assumir que $\mathcal{B}_0$ satisfaz as suposições feitas no início da Secção 3.7 pois, caso contrário, $\mathcal{B}_0$ não seria solúvel. Trivialmente, o sistema $\mathcal{B}_0$ satisfaz a condição da cadeia convexa com respeito ao conjunto $\mathcal{F}_0 = I_0$.

Sejam $2n_0 = |\Gamma_0|$ e $f_0 = |\mathcal{F}_0| = |I_0|$. De acordo com a Proposição 3.25 escolhemos um número $e(\mathcal{B}_0)$ de modo a que $\mathcal{B}_0$ não seja solúvel ou $\exp(w) \leq e(\mathcal{B}_0)$ para alguma solução w de $\mathcal{B}_0$. Definimos o inteiro

$$\beta_{\max} = 2n_0 \cdot (2n_0 + f_0)(2n_0(e(\mathcal{B}_0) + 1) + 1)^{2n_0}.$$

Notemos que este valor está definido de modo a satisfazer o Corolário 3.29 para um conjunto de índices finais com cardinalidade majorada por $2n_0 + f_0$.

Consideremos o grafo dirigido $\mathcal{G}$, o *grafo de procura do Algoritmo de Makanin*, definido como se segue: os *vértices* de $\mathcal{G}$ são os sistemas de equações fronteira $\mathcal{B} = ((\Gamma, -), (I, \leq, \varphi_I), \text{esq}, B)$ onde:

$$\begin{aligned} |\Gamma| &\leq 2n_0, \\ |I| &\leq \frac{n_0+2}{2} \cdot \beta_{\max}, \\ |B| &\leq \beta_{\max}. \end{aligned}$$

Para os sistemas $\mathcal{B}$ e $\mathcal{B}' \in \mathcal{G}$ definimos uma aresta de $\mathcal{B}$ para $\mathcal{B}'$ sempre que houver uma regra de transformação aplicável a $\mathcal{B}$ e $\mathcal{B}'$ for o resultado da respectiva transformação. Um sistema $\mathcal{B} \in \mathcal{G}$ com um conjunto vazio de variáveis é chamado um *vértice final*.

Temos $\mathcal{B}_0 \in \mathcal{G}$ e $\mathcal{G}$ tem um número finito de vértices. Logo, é suficiente mostrar a seguinte afirmação: o sistema $\mathcal{B}_0$ tem solução se e só se existe um caminho dirigido em $\mathcal{G}$ de $\mathcal{B}_0$ até um vértice final.

A implicação recíproca é trivial visto as regras de transformação serem correctas no sentido ascendente e os vértices finais serem sistemas solúveis pelo Lema 3.19. Para a implicação directa, suponhamos que $\mathcal{B}_0$ é solúvel e seja $w_0 \models (I_0, \leq, \varphi_{I_0})$ uma solução que satisfaz $\exp(w_0) \leq \exp(\mathcal{B}_0)$.

Seja $M \geq 0$ e suponhamos que existe uma sequência de sistemas solúveis $(\mathcal{B}_0, \mathcal{B}_1, \dots, \mathcal{B}_M)$ com $M \geq 0$ tal que as seguintes propriedades são satisfeitas para qualquer $1 \leq k \leq M$:

1. $\mathcal{B}_k = ((\Gamma_k, -), (I_k, \leq, \varphi_{I_k}), \text{esq}_k, B_k)$ é o sistema resultante de uma transformação aplicada a $\mathcal{B}_{k-1}$;
2. $\mathcal{B}_k$ tem uma solução $w_k \models (I_k, \leq, \varphi_{I_k})$ tal que w_k é sufixo de w_{k-1} ;
3. $|\Gamma_k| \leq |\Gamma_{k-1}|$ ou $|w_k| < |w_{k-1}|$;
4. $\mathcal{B}_k$ satisfaz a condição da cadeia convexa com respeito a algum subconjunto $\mathcal{F}_k \subseteq I_k$ com $|\mathcal{F}_k| + |\Gamma_k| \leq 2n_0 + f_0$.

Se $\mathcal{B}_M$ é um sistema de equações fronteira sem variáveis, então paramos. Caso contrário, como $\mathcal{B}_M$ é solúvel, podemos aplicar uma regra de transformação. Consequentemente, a sequência pode ser continuada por algum sistema solúvel $\mathcal{B}_{M+1}$ que satisfaz as propriedades acima. Contudo, a terceira propriedade implica que $M \leq 2n_0 + |w_0|$ pois, como $|\Gamma_0| = 2n_0$, temos a garantia de, ao fim de $M = 2n_0 + |w_0|$

passos, obtermos $|\Gamma_M| = 0$ ou $w_M = \epsilon$. Logo, temos a garantia de obtermos um sistema sem variáveis ou um sistema com a palavra vazia como modelo. Suponhamos que $\mathcal{B}_M$ é esse sistema. Vamos mostrar que $\mathcal{B}_k$ é vértice de $\mathcal{G}$ para qualquer $0 \leq k \leq M$. Isto completa a demonstração visto obtermos um caminho dirigido de $\mathcal{B}_0$ a $\mathcal{B}_M$ e $\mathcal{B}_M$ ser um vértice final.

Temos de verificar que $|\Gamma_k| \leq 2n_0$, $|I_k| \leq \frac{n_0+2}{2} \cdot \beta_{\max}$ e $|B_k| \leq \beta_{\max}$.

O caso $|\Gamma_k| \leq 2n_0$ é trivial. A segunda propriedade implica que $\exp(\mathcal{B}_k) \leq \exp(w_k) \leq \exp(w_0) \leq e(\mathcal{B}_0)$. Pelo Corolário 3.29 e a quarta propriedade temos $|B_k| \leq \beta_{\max}$. O próximo lema produz uma desigualdade que nos dará o majorante desejado da cardinalidade de qualquer I_k .

Lema 3.41. Para $0 \leq k \leq M$ definimos $\beta_k = |\{(x, i, \bar{x}, j) \in B_k \mid esq_k(x) < i\}|$. Então para todo $1 \leq k \leq M$ temos

$$2|I_k| - \beta_k + \frac{|\Gamma_k|}{2} \cdot \beta_{\max} \leq 2|I_{k-1}| - \beta_{k-1} + \frac{|\Gamma_{k-1}|}{2} \cdot \beta_{\max}$$

Demonstração. Consideremos a regra aplicada para passar de $\mathcal{B}_{k-1}$ para $\mathcal{B}_k$. Para as Regras 1 e 2 temos:

$$\begin{aligned} |\Gamma_k| &= |\Gamma_{k-1}| - 2, \\ |I_k| &= |I_{k-1}|, \\ \beta_{k-1} - \beta_k &\leq \beta_{\max}. \end{aligned}$$

Para a Regra 3 temos

$$\begin{aligned} |\Gamma_k| &= |\Gamma_{k-1}|, \\ |I_k| &= |I_{k-1}| - 1, \\ \beta_k &= \beta_{k-1}. \end{aligned}$$

Finalmente, para a Regra 4 temos

$$|\Gamma_k| = |\Gamma_{k-1}|$$

e o Lema 3.32 diz-nos que

$$2|I_k| - \beta_k \leq 2|I_{k-1}| - \beta_{k-1}.$$

A conclusão segue. □

Uma consequência do lema anterior e como $\beta_k \leq \beta_{\max}$ é:

$$2|I_k| - \beta_k + \frac{|\Gamma_k|}{2} \cdot \beta_{\max} \leq 2|I_0| - \beta_0 + \frac{|\Gamma_0|}{2} \cdot \beta_{\max}$$

e portanto

$$\begin{aligned} 2|I_k| &\leq 2|I_0| - \beta_0 + \frac{|\Gamma_0|}{2} \cdot \beta_{\max} + \beta_k - \frac{|\Gamma_k|}{2} \cdot \beta_{\max} \\ &\leq 2|I_0| + \frac{|\Gamma_0|}{2} \cdot \beta_{\max} + \beta_k \\ &\leq 2|I_0| + n_0 \cdot \beta_{\max} + \beta_{\max} \\ &\leq 2|I_0| + (n_0 + 1) \cdot \beta_{\max} \end{aligned}$$

para qualquer $0 \leq k \leq M$. Como $|I_0| \leq \frac{1}{2}\beta_{\max}$, obtemos $|I_k| \leq \frac{n_0+2}{2}\beta_{\max}$. Logo, $\mathcal{B}_k \in \mathcal{G}$ para todo o $0 \leq k \leq M$. Isto prova o teorema e portanto o Algoritmo de Makanin.

3.10 Conclusão

Finalizamos o capítulo com uma explicação menos técnica do funcionamento do Algoritmo de Makanin com o intuito de explicar de forma abreviada quais são os seus ingredientes essenciais. Fazemos também uma breve referência ao estudo da complexidade do Algoritmo.

Dado um sistema de equações no monóide livre (com restrições racionais) transformamo-lo, usando a Proposição 3.3, numa única equação cujo conjunto de soluções é igual ao conjunto de soluções do sistema inicial. Seguidamente, construímos o sistema de equações fronteira como foi explicado na Secção 3.5. Estas equações fronteira fornecem o comprimento relativo das variáveis nas possíveis soluções. Além disso, a ordem linear do sistema obriga a que as soluções do sistema satisfaçam as restrições racionais. Tal como foi construído, o sistema de equações fronteira tem solução se e só se a equação de palavras tiver solução.

Na Secção 3.6 demonstrámos uma proposição que afirma que, se um sistema de equações fronteira é solúvel, então existe uma solução com expoente de periodicidade majorado pelo valor $e(\mathcal{B})$ calculado na Secção 3.4.

A definição de cadeia convexa na Secção 3.7 é essencial para a obtenção do resultado. O majorante do expoente de periodicidade produz um majorante do comprimento máximo das cadeias convexas reduzidas (Proposição 3.28). Se a condição da cadeia convexa for satisfeita, o comprimento máximo das cadeias convexas reduzidas produz um majorante do número de equações fronteira (Corolário 3.29).

O sistema de equações fronteira inicial satisfaz a condição da cadeia convexa por motivos triviais. Aplicamos a este sistema as regras de transformação definidas na Secção 3.8. Estas regras satisfazem a condição da cadeia convexa. A sua aplicação conduz a uma solução da equação ou introduz mais equações fronteira. Mas o número de equações fronteira é majorado. Assim, temos a garantia de que o Algoritmo pára.

A ideia principal das regras de transformação é o transporte de posições da esquerda para a direita juntamente com uma divisão das variáveis. Assim, se w for uma solução de um sistema de equações $\mathcal{B}$, então algum sufixo w' de w será solução do sistema de equações $\mathcal{B}'$ resultante da aplicação de uma regra de transformação a $\mathcal{B}$. Recordemos a ideia de cada uma destas regras. A Regra 1 elimina as variáveis do sistema de equações fronteira cuja possível solução é a palavra vazia. A Regra 2 elimina equações fronteira triviais: quando o transporte de posições faz coincidir duas variáveis x e $\bar{x}$. A Regra 3 elimina as posições que foram transportadas para novas posições. Assim, passaremos a trabalhar na procura do sufixo w' da solução inicial w . Notemos que, se $w = uw'$, então

o prefixo u foi transportado e é visto como um factor de w' . Logo, após encontrarmos a solução w' , obtemos a solução inicial w . A Regra 4, a mais complexa, escolhe, num passo não-determinístico, as novas posições para as posições de transporte. Todas as variáveis que têm início neste prefixo são também levadas para as novas posições. Além disso, todas aquelas que iniciam neste prefixo e finalizam no sufixo cuja solução será (supostamente) w' produzem novas variáveis e equações fronteira que correspondem aos sufixos das variáveis que são prefixos da suposta palavra w' .

A aplicação destas regras leva-nos à construção do chamado *grafo de procura* do Algoritmo, o grafo dirigido apresentado na Secção 3.9: os vértices são os sistemas de equações fronteira $\mathcal{B}$ onde o cardinal do número de equações fronteira é majorado. Uma aresta dirigida de $\mathcal{B}$ para $\mathcal{B}'$ é definida sempre que houver uma regra de transformação aplicável a $\mathcal{B}$ e $\mathcal{B}'$ for o resultado dessa transformação. O sistema terá solução se e só se existir um caminho dirigido do vértice inicial, que é o sistema de equações fronteira inicial, até um vértice final, com um conjunto vazio de variáveis.

Durante a apresentação não nos focamos nas condições de decidibilidade necessárias para podar o *grafo de procura*. Claro que uma poda estratégica seria extremamente importante para a implementação do Algoritmo visto que o grafo poderá ser muito grande. No entanto, ela não contribui para a compreensão do Algoritmo.

Volker Diekert [17] faz um breve estudo da complexidade do Algoritmo de Makanin e apresenta o resultado:

O espaço requerido pelo Algoritmo de Makanin para equações no monóide livre com restrições racionais é no máximo exponencial. Mais precisamente, temos o majorante de complexidade seguinte:

$$DSPACE(2^{\mathcal{O}(d^2 + dr \log r)})$$

onde r é o número definido na página 63.

Neste artigo podemos também encontrar uma lista de referências bibliográficas que um leitor mais interessado no estudo da complexidade poderá consultar. Citamos, em particular, o desenvolvimento feito por C. Gutiérrez [12] que mostra que o espaço requerido para o Algoritmo de Makanin não excede EXPSPACE. Trata-se da afirmação feita por Diekert que continua a ser o menor espaço requerido para o pleno desenvolvimento do Algoritmo de Makanin.

Notemos que este resultado não nos fornece nenhuma conclusão acerca da complexidade do problema da solubilidade das equações no monóide livre. Em 1999 W. Plandowski cria um novo caminho para solucionar equações no monóide livre que é independente do trabalho de Makanin e que requer um espaço polinomial. Primeiro, em [25], mostra que o problema da solubilidade de equações no monóide livre é resolvido em NEXPTIME. Depois, em [26], mostra que o espaço requerido é PSPACE. Um ingrediente importante do trabalho de Plandowski é o uso de dados comprimidos. É um problema interessante, ainda em aberto, se o uso dos dados comprimidos poderá

também diminuir o majorante da complexidade no método de Makanin, de espaço exponencial para espaço polinomial.

Capítulo 4

Equações em grupos livres que não são finitamente aproximáveis

Em 1983, G. S. Makanin [22] descreveu um algoritmo que reconhece a solubilidade de qualquer equação num grupo livre. Este algoritmo não se assemelha ao algoritmo descrito no capítulo anterior sendo mais elaborado e de difícil compreensão.

Dada uma equação num grupo livre dizemos que ela possui a propriedade de ser *finitamente aproximável* se a equação tiver solução em F se e só se tiver solução em todo o quociente finito de F .

G. Sabbagh levantou a seguinte questão: é ou não verdade que toda a equação num grupo livre é finitamente aproximável? Se assim for temos dois *semi-algoritmos* para resolver o problema: um gera sucessivamente todos os candidatos a soluções e testa, um a um, se o são, parando em caso afirmativo; o outro gera sucessivamente todos os quocientes finitos de F verificando, em cada um, se ele fornece uma prova de que a equação não tem solução no quociente finito. Se a resposta for *não*, o *semi-algoritmo* pára, concluindo que a equação não tem solução em F .

G. Baumslag [6] mostrou que para uma equação da forma $x^{-1}ux = v$ ou $x^p = u$, onde $u, v \in F$, x é uma variável e p um primo, a resposta é afirmativa. A. Khelif [14] provou que para uma equação da forma $x^n = u$ ou $[x, y] = v$, com $u, v \in F$, x, y variáveis e n um inteiro, a resposta também é afirmativa.

Se a resposta à questão de Sabbagh fosse afirmativa, então teríamos uma prova alternativa ao resultado de Makanin.

T. Coulbois e A. Khelif [8] dão como exemplo a seguinte equação que não é finitamente aproximável em F :

$$[x^2a, y^{-1}z^2by] = t^3 \quad (4.1)$$

onde a, b são elementos distintos de um conjunto de geradores livres de F e x, y, z e t são variáveis. Dedicamos o capítulo à prova deste resultado terminando com uma generalização.

Seja F um grupo livre não-comutativo. Consideremos a equação (4.1). Em primeiro lugar, mostramos que (4.1) tem uma solução em qualquer quociente finito de F . Seja $G = F/N$ um quociente finito de F . Como todo o elemento de G tem ordem finita, existem dois inteiros α e β tais que $a^{2\alpha+1}$ e $b^{2\beta+1}$ são elementos cuja ordem é uma potência de 2. Sejam $P = \langle a^{2\alpha+1} \rangle$ e $Q = \langle b^{2\beta+1} \rangle$. Como todo o 2-subgrupo está contido num 2-subgrupo de Sylow, existem dois 2-subgrupos de Sylow P' e Q' tais que $P \leq P'$ e $Q \leq Q'$. Por um teorema de Sylow, os 2-subgrupos de Sylow P' e Q' são conjugados. Logo, existe um elemento $g \in G$ tal que $a^{2\alpha+1}$ e $g^{-1}b^{2\beta+1}g$ estão no 2-subgrupo de Sylow P' . Assim, estes dois elementos geram um 2-subgrupo de G . O comutador destes dois elementos está também neste 2-subgrupo. Queremos mostrar que é um cubo, ou seja, que temos a igualdade

$$[a^{2\alpha+1}, g^{-1}b^{2\beta+1}g] = h^3 \quad (4.2)$$

com $h \in G$.

Proposição 4.1. *Seja G um 2-grupo finito. Então o homomorfismo*

$$\begin{aligned} \varphi_G : G &\rightarrow G \\ x &\mapsto x^3 \end{aligned}$$

é sobrejectivo.

Demonstração. Seja 2^n a ordem de G . Procedemos por indução sobre n sendo a base de indução trivial: o único grupo de ordem 2 é, a menos de isomorfismo, $\mathbb{Z}/2\mathbb{Z}$ e $\varphi_{\mathbb{Z}/2\mathbb{Z}}$ é obviamente sobrejectiva. Suponhamos que, para todo o 2-grupo com ordem inferior a 2^n , φ_G é sobrejectiva. Seja G um grupo com $|G| = 2^n$. Seja H um subgrupo maximal de G . Então $|H| = 2^{n-1}$ e, por hipótese de indução,

$$\begin{aligned} H &\rightarrow H \\ x &\mapsto x^3 \end{aligned}$$

é sobrejectiva. Logo, $H \subseteq \text{Im } \varphi_G$. Se todo o elemento de G estiver contido num subgrupo maximal, então $\text{Im } \varphi_G = G$. Caso contrário, G é cíclico e portanto $G \simeq \mathbb{Z}/2^n\mathbb{Z}$. Mas, considerando o homomorfismo

$$\begin{aligned} \varphi : \mathbb{Z}/2^n\mathbb{Z} &\rightarrow \mathbb{Z}/2^n\mathbb{Z} \\ x &\mapsto 3x \end{aligned}$$

temos que $3x \equiv c \pmod{2^n}$ se e só se $x \equiv c \pmod{2^n}$ visto que $\text{mdc}(2, 3) = 1$. Portanto, φ é sobrejectiva e o resultado segue. $\square$

Resulta que (4.2) se verifica. Fazendo $x = a^\alpha$, $y = g$, $z = b^\beta$ e $t = h$ concluímos que (4.1) tem solução em G .

Mostramos agora que (4.1) não tem solução em F . Na Secção 2.2 vimos que um comutador é uma potência própria num grupo livre se e só se é trivial. Consequentemente, se (4.1) tem solução em F , então a equação

$$[x^2a, y^{-1}z^2by] = 1 \quad (4.3)$$

também tem solução em F . Logo, a equação (4.3) também tem solução em qualquer quociente finito de F .

Consideremos o homomorfismo

$$\varphi: F \rightarrow UT_3(\mathbb{Z}/2\mathbb{Z})$$

tal que

$$\varphi(a) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad \varphi(b) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

onde $UT_3(\mathbb{Z}/2\mathbb{Z})$ é o grupo das matrizes unitriangulares superiores de dimensão 3 sobre o grupo $\mathbb{Z}/2\mathbb{Z}$.

Sejam

$$\varphi(x) = \begin{pmatrix} 1 & x_1 & x_2 \\ 0 & 1 & x_3 \\ 0 & 0 & 1 \end{pmatrix}, \quad \varphi(y) = \begin{pmatrix} 1 & y_1 & y_2 \\ 0 & 1 & y_3 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad \varphi(z) = \begin{pmatrix} 1 & z_1 & z_2 \\ 0 & 1 & z_3 \\ 0 & 0 & 1 \end{pmatrix}$$

com $x_i, y_i, z_i \in \mathbb{Z}/2\mathbb{Z}$ para todo o $i \in \{1, 2, 3\}$. Com um cálculo simples obtemos

$$\varphi(x^2a) = \begin{pmatrix} 1 & 1 & x_1x_3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \varphi(x^2a)^{-1} = \begin{pmatrix} 1 & -1 & -x_1x_3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\varphi(y^{-1}z^2by) = \begin{pmatrix} 1 & 0 & -y_1 + z_1z_3 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \varphi(y^{-1}z^2by)^{-1} = \begin{pmatrix} 1 & 0 & y_1 - z_1z_3 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

e portanto

$$\varphi([x^2a, y^{-1}z^2by]) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq 1.$$

Isto prova que a equação (4.3) e, conseqüentemente, a equação (4.1) não tem solução em F .

Resulta que (4.1) não é finitamente aproximável.

De modo análogo, substituindo os primos 2 e 3 pelos primos p e q respectivamente e considerando o homomorfismo

$$\varphi: F \rightarrow UT_3(\mathbb{Z}/p\mathbb{Z})$$

tal que

$$\varphi(a) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad \varphi(b) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

podemos mostrar a proposição seguinte:

Proposição 4.2. *Toda a equação da forma*

$$[x^p a, y^{-1} z^p b y] = t^q \quad (4.4)$$

onde a e b são elementos distintos de um conjunto de geradores livres de F , x , y , z e t são variáveis e p e q primos distintos não é finitamente aproximável.

Nota 4.3. Na demonstração da proposição, a existência de dois inteiros α e β tais que $a^{p\alpha+1}$ e $b^{p\beta+1}$ têm ordem uma potência de p pode ser provada como se segue. Suponhamos que a ordem de a no quociente finito é $n = p^k r$ onde p não divide r . Notemos que o subgrupo gerado por a é isomorfo a $\mathbb{Z}/n\mathbb{Z}$, para a adição mod n , e portanto existe um isomorfismo que envia a em 1. Os múltiplos de a cuja ordem é uma potência de p são os múltiplos de r . Trata-se portanto de resolver a seguinte congruência em x e y :

$$ry \equiv 1 + px \pmod{n}.$$

Como $\text{mdc}(n, p) = p$, esta congruência tem solução se e só se p dividir $ry - 1$ para algum y , ou seja, se e só se a congruência

$$ry \equiv 1 \pmod{p}$$

tiver solução. Ora, esta congruência tem solução porque $\text{mdc}(p, r) = 1$.

Este resultado fornece um conjunto de equações que não são finitamente aproximáveis. No entanto, a fronteira entre as equações que possuem ou não esta propriedade está muito longe de ser identificada.

Epílogo

Terminamos este trabalho recapitulando as observações, as conclusões e os problemas que nos foram surgindo.

Como resposta ao problema de decidibilidade de sistemas de equações no monóide livre, estudamos profundamente o funcionamento do Algoritmo de Makanin. É um método que se baseia na fusão de duas factorizações da mesma palavra, palavra esta que corresponde à solução de uma variável. Esta fusão propagar-se-á sempre que exista uma nova ocorrência da variável na equação. Na factorização mais fina, obtida após todas as comparações, construímos as possíveis soluções. É claro que o problema não é tão trivial como parece. O facto de não sabermos nem as soluções nem o comprimento das soluções de cada uma das variáveis faz com que este processo seja não-determinístico e a complexidade do espaço requerido seja exponencial. No entanto, o majorante do expoente de periodicidade e, consequentemente, o majorante do número de equações fronteira que vamos construindo permite-nos considerar somente algumas escolhas e construir um grafo que nos garante a solução do nosso problema. A inserção de restrições racionais nas variáveis do sistema não aumentou a complexidade do algoritmo mas permite que este abranja outros sistemas de equações.

Se o leitor considera o Algoritmo de Makanin para equações no monóide livre rebuscado e intrincado, surpreender-se-á com um Algoritmo para equações no grupo livre ainda mais complicado. Tendo em vista um estudo alternativo da decidibilidade de equações no grupo livre começamos por estudar alguns exemplos de equações. Na equação da Secção 2.1 reduzimos o trabalho no grupo livre ao trabalho no monóide livre e chegámos ao nosso resultado usando somente uma análise combinatória profunda e por vezes exaustiva. Na equação da Secção 2.2 recorremos a resultados bem conhecidos da Teoria de Grupos e obtivemos uma prova mais rápida e talvez mais inteligível para um leitor que se sente familiarizado com a linguagem mais elementar da Teoria de Grupos. Enunciamos, mas não provamos, uma generalização destas equações e identificamos um conjunto de equações para as quais conseguimos reconhecer todas as soluções. No entanto, estamos ainda muito longe de resolver o problema de decidibilidade por métodos clássicos da Teoria de Grupos.

Numa tentativa de o resolver, apresentamos um algoritmo de decidibilidade proposto por Sabbagh para equações finitamente aproximáveis. O seu funcionamento é muito simples. Elaboram-se dois *semi-algoritmos*: um gera sucessivamente todos os candi-

dados a soluções e testa, um a um, se o são; o outro gera sucessivamente todos os quocientes finitos do grupo e testa, um a um, se a equação não tem solução em cada quociente finito. O algoritmo pára numa das situações: ou com a resposta *sim* do primeiro semi-algoritmo, ou com a resposta *não* do segundo. Acontece que nem todas as equações têm a propriedade de serem finitamente aproximáveis. Apresentamos nesta monografia uma família de equações que não têm esta propriedade. Fizemos referência [6, 14] a dois exemplos de equações finitamente aproximáveis. Trabalhos recentes de C. J. Ash [4], L. Ribes e P. A. Zalesskiĭ [27, 28] e de J. Almeida e M. Delgado [2, 3] caminham no intuito de clarificar a fronteira entre os sistemas que possuem ou não possuem a referida propriedade.

Bibliografia

- [1] J. Almeida, *Finite Semigroups and Universal Algebra*, World Scientific, Singapore, 1994. English translation.
- [2] J. Almeida and M. Delgado, *Sur certains systèmes d'équations avec contraintes dans un groupe libre*, Portugal. Math. **56** (1999) 409–417.
- [3] ———, *Sur certains systèmes d'équations avec contraintes dans un groupe libre-addenda*, Portugal. Math. **58** (2001) 379–387.
- [4] C. J. Ash, *Inevitable graphs: a proof of the type $\{II\}$ conjecture and some related decision procedures*, Int. J. Algebra Comput. **1** (1991) 127–146.
- [5] G. Baumslag, *Some aspects of groups with unique roots*, Acta Math. **104** (1960) 217–303.
- [6] ———, *Residual nilpotence and relations in free groups*, Journal of Algebra **2** (1965) 271–282.
- [7] M. Cohen, W. Metzler, and A. Zimmermann, *What does a basis of $F(a, b)$ look like?*, Math. Ann. **257** (1981) 435–445.
- [8] T. Coulbois and A. Khelif, *Equations in free groups are not finitely approximable*, Proc. Amer. Math. Soc. **127** (1999) 963–965.
- [9] M. Crochemore, *An optimal algorithm for computing the repetitions in a word*, Inform. Proc. Letters **12** (1981) 244–250.
- [10] L. E. Dickson, *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors*, Amer. J. Math. **35** (1913) 413–422.
- [11] E. Domenjoud and A. P. Tomás, *From Elliot-MacMahon to an algorithm for general linear constraints on naturals*, in Proc. 1st Int. Conf. Principles Practice Constraint Programming (CP'95), Cassis (France), Lecture Notes in Computer Science **976** (1995) 18–35.
- [12] C. Gutiérrez, *Satisfiability of word equations with constants is in exponential space*, in Foundations of Computer Science (FOCS 98) (1998) 112–119. IEEE Computer Society Press, Los Alamitos, California.

- [13] M. Hall, *The Theory of Groups*, AMS Chelsea Pub., New York, 1976.
- [14] A. Khelif, *Some properties of free groups and their profinite completions*. in preparation.
- [15] A. Kościelski and L. Pacholski, *Complexity of Makanin's Algorithm*, J. Assoc. Comput. Mach. **43** (1996) 670–684. Preliminary version in Foundations of Computer Science (FOCS 90), 824–829.
- [16] M. Lothaire, *Combinatorics on Words*, Addison-Wesley, Reading, Mass., 1983.
- [17] ———, *Algebraic Combinatorics on Words*, Cambridge University Press, Cambridge, 2002.
- [18] R. C. Lyndon, *The equation $a^2b^2 = c^2$ in free groups*, Michigan Math. J. **6** (1959) 89–95.
- [19] R. C. Lyndon and M. P. Schützenberger, *The equation $a^M = b^N c^P$ in a free group*, Michigan Math. J. **9** (1962) 289–298.
- [20] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*, Dover, New York, 1976.
- [21] G. S. Makanin, *The problem of solvability of equations in a free semigroup*, Math. Sb. (N. S.) **103** (1977) 147–236. In Russian. English translation in: Math. USSR-Sb. **32** (1977) 129–198.
- [22] ———, *Equations in a free group*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982) 1199–1273. In Russian. English translation in: Math. USSR-Izv. **21** (1983) 483–546.
- [23] ———, *Decidability of the universal and positive theories of a free group*, Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984) 735–749. In Russian. English translation in: Math. USSR-Izv. **25** (1985) 75–88.
- [24] G. Markowsky, *Bounds on the index and period of a binary relation on a finite set*, Semigroup Forum **13** (1977) 253–259.
- [25] W. Plandowski, *Satisfiability of word equations with constants is in NEXPTIME*, In Theory of Computing (STOC 99) (1999) 721–725. ACM Press.
- [26] ———, *Satisfiability of word equations with constants is in PSPACE*, In Foundations of Computer Science (FOCS 99) (1999) 495–500. IEEE Computer Society Press.
- [27] L. Ribes and P. A. Zalesskiĭ, *On the profinite topology on a free group*, Bull. London Math. Soc. **25** (1993) 37–43.
- [28] ———, *Conjugacy separability of amalgamated free products of groups*, J. Algebra **179** (1996) 751–774.

- [29] J. Rotman, *An Introduction on the Theory of Groups*, Springer-Verlag, New York, 1995.
- [30] M. P. Schützenberger, *Sur l'équation $a^{2+n} = b^{2+m}c^{2+p}$ dans un groupe libre*, C. R. Acad. Sci. Paris, Sér. A **248** (1959) 2435–2436.
- [31] E. Schenkman, *The equation $a^n b^n = c^n$ in a free group*, Annals Math. **70** (1959) 562–564.
- [32] K. U. Schulz, *Makanin's algorithm for word equations: Two improvements and a generalization*, In Schulz, K. U. (Ed.) (1992). *Word equations and Related Topics (IWWERT 90)*, Vol. 572 of Lect. Comp. Sci., pp. 85–150. Springer Verlag.

Índice remissivo

- alfabeto, 18
 - letras, 18
- base, 82
- cadeia, 81
 - comprimento, 81
 - condição da cadeia convexa, 82
 - convexa, 81
 - reduzida, 81
 - x -comprimento, 81
- comutador, 28
- congruência sintáctica, 19
- conjunto das posições, 72
- corte, 71
- elemento básico, 44
- equação, 20
 - comprimento notacional, 63
 - finitamente aproximável, 101
 - sistema de, 20
 - comprimento notacional, 48
 - quadrático, 20
 - solução, 20
 - não-singular, 20
 - singular, 20
- equações fronteira, 75
 - sistema de, 75
 - expoente de periodicidade, 75
 - solução, 75
- extensão admissível, 73
- extensão natural, 18
- factor, 19
 - comum, 21
 - prefixo, 19
 - próprio, 19
 - sufixo, 19
- fronteira crítica, 89
- grafo de procura, 96
 - vértice, 96
 - final, 96
- grupo, 18
 - livre de base X , 23
 - localmente a propriedade $\mathcal{P}$, 28
- índices finais, 82
- inverso, 18
 - formal, 24
- linguagem, 18
 - racional, 18
 - reconhecida por um semigrupo, 18
 - reconhecível, 19
- lista, 58
 - completa, 58
- modelo, 72
- monóide, 17
 - morfismo de, 17
 - submonóide, 17
 - gerado por X , 17
- ordem linear, 72
 - sub-ordem, 73
- palavra, 18
 - comprimento, 19
 - conjugadas, 21
 - expoente de periodicidade, 56
 - forma normal p -estável, 57
 - multiplicação, 24
 - primitiva, 22
 - reduzida, 24
 - ciclicamente, 25
 - sobreposição, 21

- vazia, 18
- posições de transporte, 89
- racional, 18
- refinamento, 72
 - refinamento comum, 71
- regras de transformação, 87
 - correcta no sentido ascendente, 87
 - correcta no sentido descendente, 87
- representação, 71
 - canónica, 72
- S -sequência, 71
- semigrupo, 17
 - livre, 18
 - morfismo de, 17
 - sintáctico, 19
 - subsemigrupo, 17
 - gerado por X , 17
- suporte, 82
- tijolo, 79
 - dual, 79
 - etiqueta, 79
 - w -comprimento, 82
 - w -comprimento, 82
- torre dominó, 55

Índice de símbolos

aplicações

$\bar{}$, 75
 ι , 24
 ϕ , 24
 σ , 20
 φ , 63
 dir , 80
 esq , 75
 $|w|$, 19
 $||\mathcal{S}||$, 48

comutador

$[x, y]$, 28

conjuntos

A , 18
 B , 75
 I , 72
 L , 18
 L_x , 62
 $\text{Red}(A)$, 24
 T , 89
 Γ , 75
 Ω , 20
 $\mathcal{B}$, 75
 $\mathcal{F}$, 82
 $\mathcal{L}$, 58
 $\mathcal{S}$, 48
 $\overline{A}$, 24

elementos do grupo

$\phi(u)$, 24
 x^{-1} , 18

grupos

F , 41
 G , 25

inteiros

$\beta_{\max}$, 96
 $[n]$, 60

$\log \alpha$, 60

c , 89
 $c(S)$, 63
 d , 63
 $e(\mathcal{B})$, 78
 $e(c(S), d)$, 64
 $\text{exp}(\mathcal{B})$, 75
 $\text{exp}(w)$, 56
 $|C|_x$, 81
 $|b|_w$, 82
 $|x|_w$, 82

monóides

A^* , 18
 M , 24
 S^ϵ , 63
 X^* , 17

operações

$*$, 17
 $+$, 17
 $\cdot$, 24
 $\cdot$, 18

palavras

ϵ , 18
 $\bar{a}$, 24
 $\bar{u}$, 24
 $w(x)$, 82

relações

$<$, 20
 $\leq$, 20
 $\prec$, 19
 σ_L , 19

semigrupos

A^+ , 18
 A^+/σ_L , 19
 S , 63
 $\text{Sint } L$, 19

X^+ , 17

outros

$(I, \leq, \varphi_I)$, 72

C , 81

$\mathcal{G}$, 96

$\mathcal{O}(g(n))$, 48

$\models$, 72

$b = (x, i, \bar{x}, j)$, 75