Universidade do Minho

Problemas de decisão para semigrupos finitos

Dissertação submetida à Escola de Ciências da Universidade do Minho para obtenção do grau de Mestre em Matemática - Especialização em Ensino

Trabalho realizado sob a orientação do
Professor Doutor José Carlos Costa

Rita Maria Araújo Bezerra
Julho 2009

Aos meus pais e marido

Agradecimentos

Ao Professor Doutor José Carlos Costa, pela receptividade sempre demonstrada, pelo encorajamento e ajuda prestada, bem como, pelos conselhos que contribuiram para a conclusão deste trabalho. Por estes motivos, é uma das pessoas responsáveis pela concretização deste projecto.

Aos meus pais que sempre me apoiaram incondicionalmente em todos os meus projectos, assim como todo o carinho e incentivo.

Aos meus familiares e amigos por todo o apoio prestado.

Ao Pedro, de um modo especial, pelo afecto, ajuda, compreensão e estímulo constante.

A todos o meu muito obrigada.

Problemas de decisão em semigrupos finitos
Resumo

Os passos mais importantes no desenvolvimento da teoria de semigrupos finitos foram tomados na década de 1950. Motivados pela teoria dos autómatos finitos, Krohn e Rhodes [29] enunciaram um resultado que permitia definir o grau de complexidade de um semigrupo finito S. Este problema tem sido considerado fundamental na teoria de semigrupos finitos e permanece ainda em aberto.

Vários outros problemas de decisão têm sido importantes no desenvolvimento da teoria de semigrupos finitos.

Um problema de decisão é o de descobrir se existe ou não um algoritmo que é capaz de responder se cada uma das afirmações de uma colecção de instâncias é verdadeira ou não. Se tal algoritmo existir então diz-se que o problema é decidível. Caso contrário diz-se que é indecidível.

Neste trabalho apresentam-se alguns exemplos de problemas de decisão, salientando o Problema da Paragem para Máquinas de Turing (problema histórico) e o Problema da Pertença a uma pseudovariedade. Este último problema é uma das questões centrais desta teoria e consiste num problema de decidir se para um dado semigrupo finito este pertence ou não à pseudovariedade. Um outro problema típico abordado foi o Problema da Palavra, que consiste em decidir quando duas pseudopalavras são ou não iguais numa pseudovariedade.

A motivação principal destes problemas na teoria de semigrupos finitos está relacionado com as aplicações às ciências da computação através da ligação entre semigrupos, linguagens racionais e os autómatos.

O facto de duas pseudovariedades serem decidíveis não implica, por exemplo, que o seu produto semidirecto seja decidível. No entanto, foram surgindo novos conceitos para tentar obter novas formas para resolver alguns dos problemas de decidabilidade. Nesse sentido surgiu o conceito de mansidão, uma propriedade mais forte que a decidabilidade, com o objectivo de provar a decidabilidade de pseudovariedades.

Terminaremos esta monografia com uma breve abordagem destes desenvolvimentos mais recentes.

Decidability problems in finite semigroups
Abstract

The most important steps in the development of the finite semigroups theory were done in the 1950 decade. Motivated by the theory of finite automata, Krohn and Rhodes [29], enunciated a result that allowed to define the degree of complexity of a finite semigroup S. This problem has been considered fundamental in the theory of finite semigroups and remains open.

Several other decision problems have been important in developing the theory of finite semigroups.

One problem of decision is the discovery whether or not there is an algorithm that is able to answer whether each statement of a collection of instances is true or not. If this algorithm exists then it is said that the problem is decidable. Otherwise it is said undecidable.

This work presents some examples of decision problems, emphasizing the Halting Problem for Turing machines (historical problem) and the Membership Problem to a pseudovariety. This last problem is one of the central issues of this theory and is the problem of deciding whether a given finite semigroup belongs or not to a gives pseudovariety. Another typical problem addressed was the Word Problem, which is to decide whether or not two pseudowords are equal in a pseudovariety.

The main motivation of these problems in the finite semigroups theory is related to the applications of computing science by the link between semigroups, rational languages and automata.

The fact that two pseudovarieties is decidable does not imply, for example, that their semidirect product is decidable. However, new concepts were emerging for seeking new ways to solve some decidability problems. In this sense, came the concept of tameness, a property stronger than the decidability, with the aim to prove decidability for pseudovarieties.

We end this monograph with a brief approach to these latest developments.

Conteúdo

Introdução

Nas primeiras décadas do século XX, o estudo da teoria de semigrupos teve uma especial atenção por parte dos investigadores.

A partir da década de 1950 a motivação principal para este estudo deve-se à aplicação às ciências da computação e à forte ligação entre semigrupos, teoria de linguagens racionais e autómatos.

O forte desenvolvimento desta teoria deveu-se em grande parte ao Teorema de Krohn-Rhodes [29], que deu origem ao problema da complexidade de um semigrupo, e também ao teorema das variedades de Eilenberg [26] que estabelece uma correspondência biunívoca entre variedades de linguagens e pseudovariedades.

O conceito de variedade de semigrupos foi introduzido por Birkhoff como sendo uma classe de semigrupos não vazia V fechada para subsemigrupos, imagens homomorfas e produtos directos. Um conceito análogo a este, introduzido por Eilenberg, é o conceito de pseudovariedade, que é uma classe $\mathbf{V}$ de semigrupos finitos definida pelas mesmas propriedades que as variedades, excepto nos produtos directos que têm que ser finitos.

As pseudovariedades permitiram a conexão entre as teorias de linguagens racionais e de semigrupos finitos e contribuíram para o desenvolvimento do estudo de problemas de decisão na teoria de semigrupos.

Mais tarde, Reiterman [37] mostrou que as pseudovariedades podiam ser definidas por pseudoidentidades, que são igualdades entre duas operações implícitas (também conhecidas por pseudopalavras) e que, portanto, desempenham um papel análogo ao das identidades para as variedades de semigrupos.

A noção de operação implícita assume, em particular, um papel fundamental no estudo da decidabilidade do Problema da Pertença (de um semigrupo a uma pseudovariedade) ao qual dedicaremos alguma atenção.

No que se refere à estrutura do presente trabalho este está organizado em termos gerais, por seis partes:

O primeiro capítulo constitui a parte dos preliminares e que tem como objectivo abordar e expôr algumas definições e notações e alguns resultados básicos da teoria de semigrupos. Para mais informações e até mesmo demontrações de resultados poderão ser consultados os livros de Almeida [3], Eilenberg [26] e Howie [28].

No capítulo 2 são abordados os conceitos de linguagem e máquina de Turing. Inicia-se este capítulo com a introdução dos conceitos de alfabeto, palavra, palavra infinita e por último o conceito de linguagem. Antes de se abordar a noção de máquina de Turing foi necessário definir autómatos e referir algumas propriedades importantes nomeadamente sobre a sua ligação às linguagens racionais. São também referidas as ligações entre reconhecimento de linguagens por autómatos, por semigrupos e por máquinas de Turing. Como ilustração dessas ligações são apresentadas os exemplos clássicos de algumas classes importantes de linguagens racionais. As referências que podem ser consultadas para este capítulo são de Costa [21, 24].

O terceiro capítulo inicia-se com os conceitos de variedade de semigrupos e de pseudovariedade de semigrupos. Estabelece-se a bijecção entre pseudovariedades de semigrupos e variedades de linguagens.

No quarto capítulo abordam-se as noções de operação implícita e de pseudoidentidade. Noções fundamentais no estudo da decidabilidade do Problema da Pertença. Posteriormente enuncia-se o Teorema de Reiterman. No final abordam-se alguns exemplos de semigrupos da forma $\overline{\Omega}_A\mathbf{V}$. É o caso das pseudovariedades: **Sl**, **N**, **K**, **D**, **LI** e **J**. Este capítulo é explorado de uma forma similar ao apresentado no livro de Almeida [3].

O capítulo 5 inicia-se com a definição de algoritmo e problema de decisão. É referido o exemplo histórico do Problema da Paragem para Máquinas de Turing. De seguida, de uma forma muito simples, são dados alguns exemplos de outros problemas de decisão para semigrupos.

O sexto e último capítulo tem por objectivo apresentar o Problema da Pertença para classes de semigrupos finitos. Inicia-se o capítulo pela abordagem de um problema histórico, o problema da complexidade de Krohn-Rhodes, pesquisando

as linhas orientadoras seguidas em torno do problema da decidabilidade. No âmbito da tentativa de resolução desse problema surgiram os conceitos de hiperdecidabilidade e mansidão. A prova da mansidão não é simples, em geral. No entanto se uma pseudovariedade for mansa ela é decidível. Por fim termina com alguns exemplos de pseudovariedades que já são conhecidas como sendo mansas. A forma como foi abordado este capítulo teve como referência o artigo de Almeida [5].

Capítulo 1

Preliminares

1.1 Semigrupos

Nos inícios do século XX verificou-se um crescente interesse pelo estudo formal de semigrupos. Desde a década de 1950, e devido à forte ligação natural entre semigrupos e autómatos finitos, que a teoria de semigrupos finitos tem tido uma importância acrescida nas ciências da computação.

Um semigrupo é formalmente constituído por um par ordenado $(S,\cdot)$ onde S é um conjunto não vazio e $\cdot$ é uma operação binária associativa definida sobre S, tal que, $\cdot$ é uma aplicação de $S \times S$ em S, que a cada elemento $(x, y) \in S \times S$ faz corresponder um elemento $x \cdot y$ de S (o qual se designa de *produto* de x por y), e onde, para quaisquer $x, y, z \in S$,

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

Se para quaisquer $x, y \in S$ se tem $x \cdot y = y \cdot x$, então dizemos que $(S,\cdot)$ é um semigrupo *comutativo*.

O número $|S|$ representa a cardinalidade do conjunto S e designa-se por *ordem* de $(S,\cdot)$. Se $|S|$ é finito, então diz-se que $(S,\cdot)$ é um *semigrupo finito*. Caso contrário, diz-se que é um *semigrupo infinito*.

Exemplos 1.1 *1) Seja $S = \{a, b\}$ e $*$ a operação tal que:*

$$a * b = a * a = a \text{ e } b * a = b * b = b.$$

Então $(S,*)$ é um semigrupo finito e $|S| = 2$.

2) O conjunto $\mathbb{Z}$ dos números inteiros relativos munido da operação de adição usual, isto é, $(\mathbb{Z},+)$ é um semigrupo infinito.

3) Dada uma família não vazia $(S_i,\cdot_i)_{i\in I}$ de semigrupos, o seu produto directo $(\prod_{i\in I} S_i,\cdot)$ é um semigrupo cujo conjunto suporte é o produto cartesiano dos S_i $(i\in I)$ e o produto é definido por

$$(s_i)_{i\in I}\cdot(t_i)_{i\in I}=(s_i\cdot_i t_i)_{i\in I}.$$

Convenciona-se que, $(\prod_{i\in\emptyset} S_i,\cdot)$ é o semigrupo trivial, ou seja, o semigrupo com um só elemento.

Sempre que não houver ambiguidades escreveremos frequentemente:

- S para designar um semigrupo $(S,\cdot)$;
- xy em vez de $x\cdot y$;
- x^n $(n\in\mathbb{N})$ em vez de $x\cdots x$, o produto de n elementos todos iguais a x.

Chama-se *monóide* a um semigrupo $(M,\cdot)$ que possui um elemento $e\in M$ tal que, para qualquer $x\in M$,

$$ex=xe=x.$$

Note-se que num monóide M existe apenas um só elemento $e\in M$ que satisfaz as igualdades anteriores. A esse elemento designámo-lo de *(elemento) identidade* e representámo-lo por 1 ou por 1_M.

Se S for um semigrupo sem elemento identidade então é possível acrescentar um novo elemento, 1, ao conjunto S, e para cada $s\in S$ definir

$$1s=s1=s \quad \text{e} \quad 11=1,$$

e então $S\cup\{1\}$ será um monóide. Denotaremos esse monóide por S^1. Ou seja, S^1, é um monóide obtido de S por acréscimo de um elemento identidade. Se S já tem elemento identidade então denotaremos $S^1=S$.

Dizemos que um elemento z de um semigrupo S é um *(elemento) zero à esquerda* se,

$$\forall x \in S,\ zx = z.$$

De forma dual, definimos *zero à direita*. Se existir *zero* (usualmente representado por 0 ou 0_S) de um semigrupo, então, é o único elemento que é simultaneamente zero à esquerda e zero à direita. Neste caso diz-se que S é um semigrupo com zero.

Exemplo 1.2 *Seja $S = \{e, a, f\}$, o semigrupo com a seguinte tabela de Caley:*

$\cdot$	e	a	f
e	e	a	f
a	a	a	f
f	f	f	f

O par $(S, \cdot)$ é um semigrupo, no qual f é o elemento zero e e é o elemento identidade.

Se S for um semigrupo sem elemento *zero*, então é possível acrescentar ao conjunto S um novo elemento 0, e definir, para cada $s \in S$,

$$s0 = 0s = s \quad \text{e} \quad 00 = 0,$$

e então $S \cup \{0\}$ será um semigrupo obtido de S por acréscimo de um elemento zero. Denotaremos esse conjunto por S^0. Se S já tem elemento *zero* então denotaremos $S^0 = S$.

Dado um semigrupo S, diz-se que S é um *semigrupo zero à esquerda* se todos os elementos de S são zeros à esquerda, isto é, se verifica a condição

$$\forall x, y \in S,\ xy = x.$$

De forma dual, define-se um *semigrupo zero à direita*.

Um elemento e de um semigrupo S diz-se um *idempotente* se $e = e^2$. É de notar que num semigrupo os elementos identidade e zero, caso existam, são idempotentes. Representa-se o conjunto dos idempotentes de S por:

$$E(S) = \{e \in S \mid e^2 = e\}.$$

Num semigrupo S, se todos os elementos são idempotentes, isto é, $S = E(S)$ então diz-se que S é um *semigrupo idempotente* ou uma *banda*.

Uma *banda rectangular* é definida como sendo um semigrupo cujo conjunto suporte é da forma $A \times B$, onde A e B são conjuntos não vazios, e cuja multiplicação é dada, para quaisquer $a, a' \in A$ e $b, b' \in B$, por

$$(a, b)(a', b') = (a, b').$$

Facilmente se prova que estes semigrupos são bandas.

Um semigrupo possuindo um único idempotente, sendo esse idempotente um *zero* diz-se *nilpotente*.

Proposição 1.3 *Seja S um semigrupo finito. As condições seguintes são equivalentes:*

1. *S é nilpotente;*
2. *S possui elemento zero e existe $n \in \mathbb{N}$ tal que $S^n = 0$ (a notação S^n tem o significado usual e será formalmente introduzida na secção seguinte);*
3. $\exists n \in \mathbb{N} \quad \forall x_1, \ldots, x_n, y_1, \ldots, y_n \in S, \quad x_1 \cdots x_n = y_1 \cdots y_n.$

Definição 1.4 *Um semigrupo S diz-se localmente trivial se*

$$\forall e \in E(S) \quad \forall s \in S, \quad ese = e.$$

A um semigrupo S chama-se *grupo* se verifica a seguinte propriedade

$$\forall a, b \in S \; \exists x, y \in S, \; ax = b \text{ e } ya = b.$$

Podemos também definir um *grupo* como sendo um monóide G em que

$$\forall x \in G \; \exists x^{-1} \in G, \; x^{-1}x = xx^{-1} = 1_G.$$

Num grupo, os elementos x e x^{-1} são ditos inversos um do outro.

1.2 Subsemigrupos

Sejam A e B dois subconjuntos de um semigrupo S. Representa-se

$$AB = \{ab \in S \mid a \in A,\ b \in B\}.$$

Para quaisquer $A, B, C \subseteq S$, tem-se $(AB)C = A(BC)$. Assim, o conjunto $\mathcal{P}(S)$ das partes de S munido desta multiplicação é um semigrupo, chamado o semigrupo das partes (ou semigrupo potência) de S.

Denotaremos A^n ($n \in \mathbb{N}$), o produto de n subconjuntos todos iguais a A, em vez de $A \cdots A$. Dado um elemento $b \in S$, escreveremos simplesmente Ab (resp. bA) em vez de $A\{b\}$ (resp. $\{b\}A$).

Seja T um subconjunto não vazio de um semigrupo S. Diz-se que T é um *subsemigrupo* de S, e denota-se por $T \leq S$, se T é fechado para a operação em S, ou seja, se

$$\forall x, y \in T,\ xy \in T.$$

De um modo análogo, se $T^2 \subseteq T$ então diz-se que T é um subsemigrupo de S. Como a condição de associatividade se verifica para quaisquer elementos de S, em particular também se verifica para quaisquer elementos de T, donde se conclui que T é um semigrupo.

Exemplos 1.5 *Seja S um semigrupo. Então:*

1) S é um subsemigrupo de S.

2) Se S é um semigrupo com elemento zero e identidade, tem-se que $\{0\}$ e $\{1\}$ são seus subsemigrupos. Mais geralmente, considerando um qualquer elemento e idempotente de S tem-se que $\{e\}$ é um subsemigrupo de S.

Um subsemigrupo T de S, onde T é um *grupo*, é dito um *subgrupo* de S e denotamos por $T \leq_g S$. No caso de S ser um monóide, dizemos que T é um *submonóide* de S se T é um subsemigrupo de S que contém a identidade 1_S e escrevemos $T \leq_m S$.

Exemplos 1.6 *Consideremos $S = \{e, a, f\}$ o semigrupo do Exemplo 1.2. Então:*

1) O subconjunto $\{f, a\}$ é um subsemigrupo de S e é um monóide, mas não é um submonóide de S pois não contém o elemento identidade 1_S (que é o elemento e).

2) O subconjunto $\{f\}$ é um subgrupo de S.

Proposição 1.7 *Seja T um subconjunto não vazio de um semigrupo S. Então são equivalentes as afirmações seguintes:*

(i) T é um subgrupo de S;

(ii) $\forall x \in T,\ xT = Tx = T$.

1.3 Ideais

Consideremos um semigrupo S e I um subconjunto não vazio de S. Dizemos que I é um :

- *ideal à esquerda* de S, e escreve-se $I \trianglelefteq_e S$, se $S^1 I \subseteq I$;
- *ideal à direita* de S, e escreve-se $I \trianglelefteq_d S$, se $IS^1 \subseteq I$;
- *ideal* de S, e escreve-se $I \trianglelefteq S$, se I é simultaneamente ideal à esquerda e ideal à direita de S (o que equivale a ter-se $S^1 I S^1 \subseteq I$).

É de salientar que todo o ideal de S (mesmo que um ideal lateral) é um subsemigrupo de S, mas nem todo o subsemigrupo de S é um ideal de S.

Um ideal I de um semigrupo S é dito um ideal *minimal* de S se,

$$\forall J \trianglelefteq S, \quad J \subseteq I \Rightarrow J = I,$$

ou seja, se I é um ideal minimal para a relação de inclusão. Um ideal minimal, se existir, é único, e dizemos que é o *ideal mínimo* de S. Note-se que nem todos os semigrupos têm ideal minimal. É, por exemplo, o caso de $\mathbb{N}$ munido da multiplicação usual.

A existência de ideal mínimo está assegurada em dois casos importantes.

Exemplos 1.8 *Seja S um semigrupo.*

1) Se S é finito, então S tem ideal mínimo. Facilmente se mostra que esse ideal mínimo é o produto de todos os ideais de S.

2) Se S tem elemento zero, então $\{0\}$ é o ideal mínimo de S.

1.4 Homomorfismos

Definição 1.9 *Sejam S e T dois semigrupos. Uma aplicação $\varphi : S \to T$ diz-se um homomorfismo ou morfismo (de semigrupos) de S em T se*

$$\forall x, y \in S,\ \varphi(xy) = \varphi(x)\varphi(y).$$

Dados dois semigrupos S e T, dizemos ainda que:

- *um homomorfismo φ de S em T é um monomorfismo se φ é uma aplicação injectiva;*
- *T é imagem homomorfa de S se existe um homomorfismo sobrejectivo (dito um epimorfismo) de S em T;*
- *S é isomorfo a T, e escreve-se $S \simeq T$, se existe um homomorfismo bijectivo (dito um isomorfismo) de S em T;*
- *T divide S, e escreve-se $T \prec S$, se T é imagem homomorfa de algum subsemigrupo de S.*

Em geral identificaremos dois semigrupos isomorfos.

Proposição 1.10 *Seja $\phi : S \to T$ um homomorfismo de semigrupos.*

1. *Se $S' \leq S$, então $\phi(S') \leq T$.*
2. *Se $T' \leq T$ e $\phi^{-1}(T') \neq \emptyset$, então $\phi^{-1}(T') \leq S$.*

Este último resultado pode ser usado para apresentar uma definição mais geral de subsemigrupo:

Definição 1.11 *Diz-se que S é subsemigrupo de T se existe um monomorfismo de S em T.*

1.5 Subsemigrupos gerados por uma parte do semigrupo

Se A é um subconjunto não vazio de um semigrupo S, então a família dos subsemigrupos de S que contêm A é não vazia. De facto, em particular, o próprio S é um subsemigrupo. Denota-se por $\langle A\rangle$ o *subsemigrupo de S gerado por A*. Caracteriza-se por ser um subsemigrupo de S que satisfaz as propriedades seguintes:

1) $A \subseteq \langle A\rangle$;

2) Se U é um subsemigrupo de S contendo A, então $\langle X\rangle \subseteq U$

Isto é, $\langle A\rangle$ é o menor subsemigrupo de S que contém A. Também se pode verificar facilmente que $\langle X\rangle$ é formado por todos os elementos de S que são escritos na forma de produtos finitos de elementos de A, ou seja, $a_1a_2\cdots a_n$, com $n \in \mathbb{N}$ e $a_1, a_2, \ldots, a_n \in A$.

Um caso particular, e de algum interesse, é o caso em que o *conjunto de geradores* é um conjunto singular, ou seja, $A = \{a\}$, no qual escreveremos simplesmente $\langle a\rangle$ em vez de $\langle\{a\}\rangle$. Neste caso tem-se

$$\langle a\rangle = \{a, a^2, a^3, \ldots\}.$$

Se $\langle a\rangle$ é um conjunto finito com n elementos, diz-se que o elemento a tem *ordem (finita) n*. Caso contrário, diz-se que tem *ordem infinita*.

O resultado seguinte é fundamental em teoria de semigrupos finitos.

Proposição 1.12 *Se S é um semigrupo finito e $a \in S$, então existe $k \in \mathbb{N}$ tal que a^k é um idempotente.*

Como consequência deste resultado conclui-se que todo o semigrupo finito tem pelo menos um idempotente.

Sendo S um semigrupo, chama-se o *expoente* de S, ao menor inteiro positivo n, caso exista, tal que, para qualquer $a \in S$, a^n é um idempotente.

O resultado seguinte afirma que existe sempre o expoente de um semigrupo finito.

Proposição 1.13 *Seja S um semigrupo finito. Então existe $n \in \mathbb{N}$ tal que para todo o $a \in S$, a^n é um idempotente.*

Demonstração: Consideremos $n = mmc\ \{r_a : a \in S\}$, onde r_a é o menor número natural tal que a^{r_a} é um idempotente. Dado que a Proposição 1.12 garante a existência de r_a, para todo o elemento a de S, então conclui-se que a^n é um idempotente qualquer que seja o $a \in S$. □

O seguinte resultado, que é considerado uma propriedade básica dos semigrupos finitos, pode-se demonstrar facilmente.

Proposição 1.14 *Sejam S um semigrupo finito e $|S|$ o seu cardinal. Então*

$$\forall n \geq |S|, \quad S^n = SE(S)S.$$

1.6 Congruências

Definição 1.15 *Uma relação de equivalência θ sobre um semigrupo S diz-se:*

- *uma congruência esquerda de S, se*

$$\forall a, b, x \in S,\ (a, b) \in \theta \Rightarrow (xa, xb) \in \theta.$$

- *uma congruência direita de S, se*

$$\forall a, b, x \in S,\ (a, b) \in \theta \Rightarrow (ax, bx) \in \theta.$$

- *uma congruência se θ é simultaneamente uma congruência esquerda e direita, o que é equivalente, como se pode provar, a ter-se*

$$\forall a, b, c, d \in S,\ (a, b), (c, d) \in \theta \Rightarrow (ac, bd) \in \theta.$$

Sejam $a \in A$ e R uma relação de equivalência sobre um conjunto A. A *classe de equivalência* de a definida pela relação R é o conjunto

$$[a]_R = \{b \in A \mid a\, R\, b\}.$$

Chama-se *conjunto quociente de A por R*, e representa-se por A/R, como sendo o conjunto de todas as classes de equivalência de R, ou seja,

$$A/R = \{[a]_R \mid a \in A\}.$$

O conjunto quociente S/θ, onde θ é uma congruência sobre o semigrupo S, munido da operação binária, definida para cada $a, b \in S$ por

$$[a]_\theta[b]_\theta = [ab]_\theta$$

é um semigrupo e designa-se de *semigrupo quociente* de S por θ.

A aplicação

$$\begin{array}{rccc} \pi: & S & \to & S/\theta \\ & a & \mapsto & [a]_\theta \end{array}$$

é um epimorfismo, chamado o *epimorfismo canónico de S para S/θ*.

Exemplo 1.16 *Sejam S um semigrupo e I um ideal de S. Designa-se por* congruência de Rees sobre S de núcleo I *a relação de equivalência θ_I sobre S, definida por*

$$a\theta_I b \iff a = b \text{ ou } a, b \in I.$$

O semigrupo quociente S/θ_I representa-se usualmente por S/I.

Sejam ρ e σ relações binárias sobre um conjunto não vazio A. Denotaremos por ρ^e a *equivalência* sobre A *gerada* por ρ, ou seja, ρ^e é a menor equivalência sobre A que contém ρ. Usaremos a notação $\rho \vee \sigma$ para representar a equivalência gerada por $\rho \cup \sigma$, ou seja,

$$\rho \vee \sigma = (\rho \cup \sigma)^e.$$

Quando as relações ρ e σ comutam, relativamente à composição, o cálculo de $\rho \vee \sigma$ fica bastante simplificado como o mostra o seguinte resultado.

Proposição 1.17 *Se ρ e σ são relações de equivalência sobre um conjunto A tais que $\rho \circ \sigma = \sigma \circ \rho$, então $\rho \vee \sigma = \rho \circ \sigma$.*

Recorde-se que,

$$\rho \circ \sigma = \{(a, b) \in A \times A \mid \exists c \in A \ : (a, c) \in \rho \ \wedge (c, b) \in \sigma\}.$$

1.7 Relações de Green

No ano de 1951, J. Green, introduziu as relações de Green que passaram a desempenhar um papel fundamental no desenvolvimento da teoria de semigrupos. Podemos usar estas relações para definir algumas das mais importantes classes de semigrupos finitos.

Seja S um semigrupo. São cinco as *relações de Green* (nome dado às relações de equivalência sobre S): $\mathcal{R}, \mathcal{L}, \mathcal{J}, \mathcal{H}$ e $\mathcal{D}$. Comecemos por definir $\mathcal{R}, \mathcal{L}$ e $\mathcal{J}$. Sejam $x, y \in S$. Dizemos que:

$$\begin{aligned} x\,\mathcal{R}\,y &\quad \text{se} \quad xS^1 = yS^1, \\ x\,\mathcal{L}\,y &\quad \text{se} \quad S^1x = S^1y, \\ x\,\mathcal{J}\,y &\quad \text{se} \quad S^1xS^1 = S^1yS^1. \end{aligned}$$

É de salientar que estas relações de equivalência estão associadas às relações de *quasi-ordem* (isto é, reflexivas e transitivas) a seguir definidas:

$$\begin{array}{rcll} x \leq_{\mathcal{R}} y & \Leftrightarrow & xS^1 \subseteq yS^1 & \Leftrightarrow \quad x \in yS^1 \\ x \leq_{\mathcal{L}} y & \Leftrightarrow & S^1x \subseteq S^1y & \Leftrightarrow \quad x \in S^1y \\ x \leq_{\mathcal{J}} y & \Leftrightarrow & S^1xS^1 \subseteq S^1yS^1 & \Leftrightarrow \quad x \in S^1yS^1 \end{array}$$

com $x, y \in S$.

Facilmente se conclui que para $\mathcal{K} \in \{\mathcal{R}, \mathcal{L}, \mathcal{J}\}$, e para quaisquer $x, y \in S$ definem-se de forma equivalente as relações

$$x\,\mathcal{K}\,y \quad \text{se e só se} \quad x \leq_{\mathcal{K}} y \quad \text{e} \quad y \leq_{\mathcal{K}} x.$$

Ou seja,

$x\,\mathcal{R}\,y \Leftrightarrow xS^1 = yS^1 \Leftrightarrow xu = y$ e $yv = x$ para alguns $u, v \in S^1$,
$x\,\mathcal{L}\,y \Leftrightarrow S^1x = S^1y \Leftrightarrow ux = y$ e $vy = x$ para alguns $u, v \in S^1$,
$x\,\mathcal{J}\,y \Leftrightarrow S^1xS^1 = S^1yS^1 \Leftrightarrow uxv = y$ e $ryt = x$ para alguns $u, v, r, t \in S^1$.

Da definição anterior facilmente se verifica que:

- $\mathcal{R} \subseteq \mathcal{J}$ e $\mathcal{L} \subseteq \mathcal{J}$;
- $xu \leq_{\mathcal{R}} x$, $ux \leq_{\mathcal{L}} x$ e $uxv \leq_{\mathcal{J}} x$ para qualquer $x \in S$ e quaisquer $u, v \in S^1$.

Podemos definir as duas restantes relações de Green ($\mathcal{H}$ e $\mathcal{D}$) através das relações $\mathcal{R}$ e $\mathcal{L}$, sendo:

$$\mathcal{H} = \mathcal{R} \cap \mathcal{L} \quad \text{e} \quad \mathcal{D} = \mathcal{R} \vee \mathcal{L}.$$

Como é evidente, são válidas as seguintes inclusões entre as relações de Green

$$\mathcal{H} \subseteq \mathcal{R},\mathcal{L} \subseteq \mathcal{D} \subseteq \mathcal{J}.$$

Quando o semigrupo S é comutativo tem-se $\mathcal{H} = \mathcal{R} = \mathcal{L} = \mathcal{D} = \mathcal{J}$.

A relação de quasi-ordem $\leq_{\mathcal{H}}$ sobre S pode ser definida da seguinte forma:

$$x \leq_{\mathcal{H}} y \quad \Leftrightarrow \quad x \leq_{\mathcal{R}} y \quad \text{e} \quad x \leq_{\mathcal{L}} y.$$

O resultado que se segue é de grande importância no estudo dos semigrupos finitos.

Proposição 1.18 *Se S é um semigrupo finito, então $\mathcal{D} = \mathcal{J}$.*

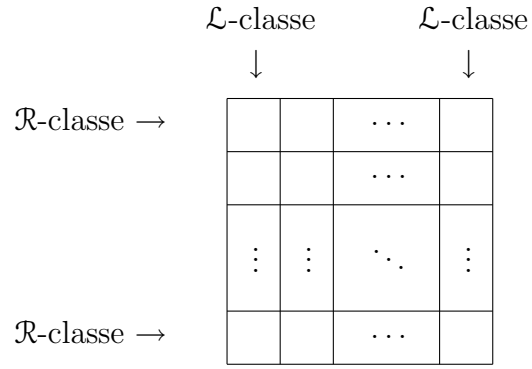
Consideremos um semigrupo S. Seja $\mathcal{K} \in \{\mathcal{R}, \mathcal{L}, \mathcal{J}, \mathcal{H}, \mathcal{D}\}$ uma das relações de Green sobre S. Representaremos por K_x a $\mathcal{K}$-classe contendo um dado elemento $x \in S$.

Se:

- $\mathcal{K}$ é a relação de igualdade em S, ou seja, $K_x = \{x\}$ para todo o $x \in S$, então diz-se que S é $\mathcal{K}$-*trivial*;
- $\mathcal{K}$ é a relação universal em S, ou seja, $K_x = S$ para todo o $x \in S$, então diz-se que S é $\mathcal{K}$-*universal*.

1.8 A estrutura das $\mathcal{D}$-classes

Cada $\mathcal{D}$-classe num semigrupo S é tanto uma união de $\mathcal{R}$-classes como de $\mathcal{L}$--classes, enquanto que a intersecção não vazia de uma $\mathcal{R}$-classe e de uma $\mathcal{L}$-classe é uma $\mathcal{H}$-classe. Esta observação sugere a representação das $\mathcal{D}$-classes como "caixas de ovos",



onde os elementos de cada $\mathcal{D}$-classe são organizados num rectângulo de quadrados e onde cada quadrado constitui uma $\mathcal{H}$-classe. Cada linha representa uma $\mathcal{R}$-classe e cada coluna uma $\mathcal{L}$-classe. Para indicar que uma dada $\mathcal{H}$-classe contém um idempotente é usual escrever um asterisco no quadrado correspondente a essa $\mathcal{H}$-classe.

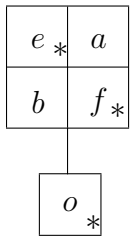
Exemplo 1.19 *Consideremos o semigrupo $B_2 = \{o, e, f, a, b\}$ de matrizes, onde os elementos o, e, f, a, b são, respectivamente, as matrizes*

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

A tabela de Cayley de B_2 é dada por

$\cdot$	o	e	f	a	b
o	o	o	o	o	o
e	o	e	o	a	o
f	o	o	f	o	b
a	o	o	a	o	e
b	o	b	o	f	o

O semigrupo B_2 pode ser representado pelo seguinte diagrama, que descreve a organização dos seus elementos de acordo com as relações de Green.



Como se verifica pelo diagrama, este semigrupo tem duas $\mathcal{D}$-classes ($\{o\}$ e $\{e, b, f, a\}$), três $\mathcal{L}$-classes, três $\mathcal{R}$-classes e cinco $\mathcal{H}$-classes. Este é também um semigrupo $\mathcal{H}$-trivial.

Lema 1.20 (Lema de Green) *Sejam a, b elementos $\mathcal{R}$-equivalentes de um semigrupo S e sejam $s, t \in S^1$ tais que $as = b$ e $bt = a$. Então as correspondências*

$$\begin{array}{rccc} \rho_s : & L_a & \to & L_b \\ & x & \mapsto & xs \end{array} \qquad e \qquad \begin{array}{rccc} \rho_t : & L_b & \to & L_a \\ & x & \mapsto & xt \end{array}$$

são aplicações bijectivas mutuamente inversas que preservam as $\mathcal{H}$-classes.

Demonstração: Mostremos primeiro, que ρ_s está bem definida. Seja $x \in L_a$. Deste modo tem-se que:

$$\begin{aligned} x \in L_a \;&\Rightarrow\; x \mathcal{L}\, a \;\Rightarrow\; S^1x = S^1a \;\Rightarrow\; S^1xs = S^1as \;\Rightarrow\; xs \mathcal{L}\, as \\ &\Rightarrow\; \rho_s(x) \in L_b. \end{aligned}$$

Logo ρ_s é efectivamente uma aplicação de L_a em L_b.

Como por hipótese $x \in L_a$, então existe $u \in S^1$ tal que $x = ua$, donde

$$\rho_t \circ \rho_s(x) = \rho_t(xs) = xst = uast = ubt = ua = x,$$

o que mostra que $\rho_t \circ \rho_s$ é a aplicação identidade sobre L_a. De forma análoga prova-se que ρ_t é uma aplicação de L_b em L_a e que $\rho_s \circ \rho_t$ é a aplicação identidade sobre L_b. Fica então provada a primeira parte do lema.

Falta então provar que ρ_s preserva as $\mathcal{H}$-classes. Para tal consideremos $x, y \in L_a$, e suponhamos que $x \mathcal{H}\, y$. Então $x \mathcal{R}\, y$ e $x \mathcal{L}\, y$. Da segunda condição resulta de imediato que $xs \mathcal{L}\, ys$, isto é, $\rho_s(x) \mathcal{L}\, \rho_s(y)$. Por outro lado, como ρ_s e ρ_t são bijecções mutuamente inversas deduz-se $x = xst$ e $y = yst$, portanto $x \mathcal{R} xs$ e

$y\mathcal{R}ys$. Agora, como $x\mathcal{R}y$ pode concluir-se que $xs\mathcal{R}ys$, isto é, $\rho_s(x)\mathcal{R}\rho_s(y)$. Portanto $\rho_s(x)\mathcal{H}\rho_s(y)$. Reciprocamente, admitindo que $xs\mathcal{H}ys$, deduz-se $xst\mathcal{H}yst$, ou seja, $x\mathcal{H}y$. Mostramos assim que $x\mathcal{H}y$ se e só se $\rho_s(x)\mathcal{H}\rho_s(y)$, portanto, ρ_s preserva as $\mathcal{H}$-classes. Analogamente prova-se que ρ_t preserva as $\mathcal{H}$-classes. □

O Lema de Green admite o seguinte resultado análogo para as $\mathcal{R}$-classes.

Lema 1.21 (Lema de Green (dual)) *Sejam a, b elementos $\mathcal{L}$-equivalentes de um semigrupo S e sejam $s, t \in S^1$ tais que $sa = b$ e $tb = a$. Então as correspondências*

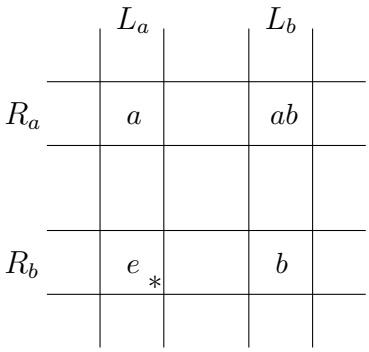
$$\begin{array}{rccc} \lambda_s: & R_a & \to & R_b \\ & x & \mapsto & sx \end{array} \qquad e \qquad \begin{array}{rccc} \lambda_t: & R_b & \to & R_a \\ & x & \mapsto & tx \end{array}$$

são aplicações bijectivas mutuamente inversas que preservam as $\mathcal{H}$-classes.

Como consequência do Lema de Green e do seu dual pode-se provar o seguinte resultado.

Corolário 1.22 *Seja S um semigrupo e sejam a, b elementos de S. Se $a\,\mathcal{D}\,b$, então $|H_a| = |H_b|$.*

Proposição 1.23 *Para quaisquer dois elementos $a, b \in S$, $ab \in R_a \cap L_b$ se e só se $R_b \cap L_a$ contém um idempotente.*



Demonstração: Comecemos por provar a implicação da esquerda para a direita.

Suponhamos que $ab \in R_a \cap L_b$. Então tem-se que $ab\,\mathcal{R}\,a$ e $L_{ab} = L_b$. Logo, pelo Lema de Green, a aplicação $\rho_b : L_a \to L_b$, $x \mapsto xb$, é uma bijecção que preserva as $\mathcal{H}$-classes. Logo, existe $e \in L_a \cap R_b$ tal que $\rho_b(e) = b$, ou seja, $eb = b$.

Dado que $e \mathcal{R} b$, existe $t \in S^1$ tal que $e = bt$. Donde se conclui que $(bt)b = eb = b$, e consequentemente, $e^2 = (bt)(bt) = (btb)t = bt = e$, ou seja, e é um idempotente.

Provemos agora a implicação contrária, da direita para esquerda.

Suponhamos que $R_b \cap L_a$ contém um idempotente. Seja e esse idempotente. Então tem-se que $e = e^2$. Como $e \mathcal{R} b$ e $e \mathcal{L} a$, vem que $er = b$ e $se = a$ para alguns $r, s \in S^1$. Logo,

$$eb = e(er) = (ee)r = er = b \quad \text{e} \quad ae = (se)e = s(ee) = se = a.$$

Como $e \mathcal{R} b$ e $e \mathcal{L} a$, deduz-se que $ae \mathcal{R} ab$ e $eb \mathcal{L} ab$. Ou seja, $a \mathcal{R} ab$ e $b \mathcal{L} ab$. Fica assim provado que $ab \in R_a \cap L_b$. □

Os seguintes corolários podem ser facilmente demonstrados usando os resultados anteriores.

Corolário 1.24 *Seja H uma $\mathcal{H}$-classe de um semigrupo S. As condições seguintes são equivalentes:*

i) H contém um idempotente;

ii) $H^2 \cap H \neq \emptyset$ (i.e., existem $a, b \in H$ tais que $ab \in H$);

iii) $H^2 = H$ e, neste caso, H é um subgrupo de S.

Corolário 1.25 *Sejam S um semigrupo e e um elemento idempotente de S. Então H_e é um subgrupo de S e nenhuma $\mathcal{H}$-classe de S pode conter mais do que um idempotente.*

O resultado que se segue é importante e pode ser facilmente demontrado.

Proposição 1.26 *Seja S um semigrupo finito. Se $a, b \in S$ são tais que $a \leq_{\mathcal{J}} b$, então:*

1. *se $b \leq_{\mathcal{R}} a$ então $a \mathcal{R} b$;*
2. *se $b \leq_{\mathcal{L}} a$ então $a \mathcal{L} b$;*
3. *se $b \leq_{\mathcal{H}} a$ então $a \mathcal{H} b$.*

1.9 Elementos regulares de um semigrupo

Sejam S um semigrupo e $a \in S$. O elemento a diz-se *regular* se existe $x \in S$ tal que $axa = a$. Ao elemento x chama-se *associado* de a. Representa-se por $A(a)$ o conjunto dos associados de a. Se todos os elementos de S são regulares, dizemos que S é um *semigrupo regular*.

Seja $a' \in S$. O elemento a' diz-se um *inverso* de a se

$$aa'a = a \quad \text{e} \quad a'aa' = a'.$$

Ou seja, a' é um inverso de a se $a' \in A(a)$ e $a \in A(a')$. O conjunto dos inversos de a é representado por $V(a)$.

Observação 1.27 *Note-se que:*

- *um elemento de S que admite um inverso é necessariamente regular;*
- *todo o elemento regular tem um inverso;*
- *um elemento pode ter mais do que um inverso.*

Exemplos 1.28 *Sejam S um semigrupo e a um elemento de S.*

1) Se S é um grupo, então S é um semigrupo regular e o conjunto $A(a)$ tem apenas um elemento, que é a^{-1}.

2) Se S é uma banda rectangular, então S é um semigrupo regular e para cada $a \in S$ tem-se $A(a) = S$ e $V(a) = S$.

3) Todo o elemento idempotente é regular.

4) Se $x \in A(a)$, então $xax \in A(a)$.

A proposição seguinte dá-nos várias caracterizações das $\mathcal{D}$-classes regulares de um semigrupo.

Proposição 1.29 *Seja D uma $\mathcal{D}$-classe de um semigrupo finito S. Então, as seguintes condições são equivalentes:*

i) *D é regular;*

ii) *D contém algum elemento regular;*

iii) *cada $\mathcal{R}$-classe de D contém algum idempotente;*

iv) *cada $\mathcal{L}$-classe de D contém algum idempotente;*

v) *D contém algum idempotente;*

vi) *existem $a, b \in D$ tais que $ab \in D$.*

Demonstração: A implicação iii) para v) é evidente. Que v) implica ii) também é evidente. A equivalência entre v) e vi) resulta das Proposições 1.23 e 1.26. Resta então provar as quatro primeiras equivalências.

Seja $a \in D$. O primeiro passo será mostrar que a é regular se e só se R_a contém algum idempotente.

Suponhamos que a é regular. Então $axa = a$, para algum $x \in S$. Considerando $e = ax$, verifica-se que $a \,\mathcal{R}\, e$. Note-se que e é idempotente, dado que, $e = ax = (axa)x = (ax)(ax) = e^2$.

Reciprocamente, se $a \,\mathcal{R}\, e$, para algum idempotente e, então existem $x, y \in S^1$ tais que $ax = e$ e $ey = a$. Deste modo temos que $ea = e(ey) = e^2y = ey = a$, e portanto, que $a = ea = e^2a = axea$, ou seja, que a é regular. De modo análogo, prova-se que a é regular se e só se L_a contém algum idempotente.

Sejam $a, b \in D$ tais que a é regular. Como $a \,\mathcal{D}\, b$, então existe $c \in S$ tal que $a \,\mathcal{R}\, c$ e $c \,\mathcal{L}\, b$. Sabendo que, por hipótese, a é regular, vem que $R_a = R_c$ contém um idempotente e por isso c é regular. Portanto, $L_c = L_b$ contém um idempotente e consequentemente b é regular. Isto estabelece a equivalência das quatro primeiras condições. □

Como referimos acima, algumas classes usuais de semigrupos podem ser definidas/caracterizadas através das relações de Green. Por exemplo, dado um semigrupo S, diz-se/prova-se que S é:

- um *grupo* se e só se $\mathcal{H}$ é a relação universal sobre S.
- *aperiódico* se $\mathcal{H}$ é a relação trivial sobre S.
- *simples*, se $\mathcal{J}$ é a relação universal sobre S.
- *inverso*, se é regular e cada elemento tem um e um só inverso.
- *completamente regular*, se toda a $\mathcal{H}$-classe é um grupo.

Capítulo 2

Linguagens e Máquinas de Turing

A formalização matemática das noções de palavra e linguagem foi introduzida na década de 1950 por linguistas tais como Noam Chomsky.

Uma *linguagem* é definida como sendo um conjunto de palavras. A noção básica desta teoria é pois a de *palavra*, que por sua vez é definida como sendo uma sequência finita de letras.

2.1 Palavras

Chama-se *alfabeto* a um conjunto finito não vazio A. Os elementos de A são chamados *letras*. A uma sequência finita de elementos de A chama-se *palavra* sobre A. A sequência vazia diz-se a *palavra vazia* e representa-se por 1.

Exemplo 2.1 *São exemplos de palavras sobre o alfabeto* $A = \{a, b, c\}$ *as palavras:* 1*,* b*,* c*,* ca*,* $bcacccbbab$*.*

Duas palavras $a_1a_2\cdots a_n$ e $b_1b_2\cdots b_m$ sobre um alfabeto A dizem-se *iguais*, e escreve-se $a_1a_2\cdots a_n = b_1b_2\cdots b_m$, se $n = m$ e $a_i = b_i$ para $i = 1, \ldots, n$.

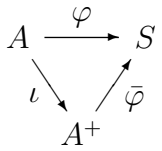
Representa-se por A^* o conjunto de todas as palavras sobre um alfabeto A e por A^+ o conjunto de todas as palavras não vazias sobre A, ou seja, $A^+ = A^* \backslash \{1\}$. Munindo o conjunto A^+ (resp. A^*) com a operação binária $\cdot$ definida, para quaisquer duas palavras $u = a_1 \cdots a_n$ e $v = b_1 \cdots b_m$ de A^+, por

$$u \cdot v = a_1a_2\cdots a_n \cdot b_1b_2\cdots b_m = a_1a_2\cdots a_nb_1b_2\cdots b_m = uv,$$

$$(u \cdot 1 = 1 \cdot u = u \text{ e } 1 \cdot 1 = 1)$$

chamada o *produto (de concatenação)* de palavras, obtém-se um semigrupo (resp. monóide), designado o *semigrupo livre gerado por* A (resp. *monóide livre gerado por* A). A justificação desta designação encontra-se na propriedade do próximo resultado. Ou seja, A^+ é *livre* sobre A no seguinte sentido.

Proposição 2.2 *Seja S um semigrupo. Se $\varphi : A \to S$ é uma aplicação qualquer, existe um e um só morfismo $\overline{\varphi} : A^+ \to S$ tal que o diagrama*



comuta (ou seja, $\varphi = \overline{\varphi} \circ \iota$), onde ι é a aplicação de inclusão de A sobre A^+.

Demonstração: O morfismo $\overline{\varphi}$ é definido, para cada $u = a_1 a_2 \cdots a_n \in A^+$, em que $a_i \in A$ para todo o i, por

$$\overline{\varphi}(u) = \varphi(a_1)\varphi(a_2)\cdots\varphi(a_n),$$

e diz-se o *prolongamento natural* de φ a A^+. □

Note-se que A^* não é um monóide comutativo em geral. Considerando por exemplo, $A = \{a, b\}$, $u = b$ e $v = ab$ obtém-se $uv = bab \neq abb = vu$.

O *comprimento* de uma palavra u sobre um alfabeto A, representa-se por $|u|$ e é o número de ocorrências de letras de A em u. Para $a \in A$, representa-se por $|u|_a$ o número de ocorrências da letra a em u. Considerando A um alfabeto qualquer, $u, v \in A^*$ e $a \in A$ tem-se que

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

Exemplos 2.3 *1. A palavra vazia tem comprimento zero, isto é, $|1| = 0$;*

2. Seja $A = \{a, b, c\}$. Tem-se $|ab| = 2$, $|accbac| = 6$, $|accbac|_a = 2$, $|ab|_c = 0$ e $|accbac|_b = 1$.

O *conteúdo* de uma palavra $u \in A^*$ é o conjunto de todas as letras de A que ocorrem em u e denota-se por $c(u)$.

Se u é uma palavra e $n \in \mathbb{N}_0$, a definição recursiva de u^n é dada por

$$u^n = \begin{cases} 1 & \text{se } n = 0 \\ u^{n-1}u & \text{se } n > 0 \end{cases}$$

A palavra u^n é chamada a potência-n de u. Esta noção de potência de uma palavra possui as seguintes propriedades: se u é uma palavra e $n, m \in \mathbb{N}$, então

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

Sejam u e w duas palavras de A^*. Diz-se que

- u é um *factor* de w se existem $x, y \in A^*$ tais que $w = xuy$;
- u é um *prefixo* (resp. *sufixo*) de w se existe $y \in A^*$ tal que $w = uy$ (resp. $w = yu$);
- u é um *factor próprio* (resp. *sufixo próprio*, *prefixo próprio*) de w se u é um *factor* (resp. *sufixo*, *prefixo*) de w e $u \neq w$.

Seja $k \in \mathbb{N}_0$. Para cada palavra $u \in A^*$ de comprimento maior ou igual a k, denota-se por $p_k(u)$ e $s_k(u)$, respectivamente, o prefixo e o sufixo de u de comprimento k.

Exemplo 2.4 *Para $A = \{a, b, c\}$ e $u = accbac$ os factores de u são 1, a, b, c, ac, cc, cb, ba, acc, ccb, cba, bac, $accb$, $ccba$, $cbac$, $accba$, $ccbac$ e u; os prefixos de u são $p_0(u) = 1$, $p_1(u) = a$, $p_2(u) = ac$, $p_3(u) = acc$, $p_4(u) = accb$, $p_5(u) = accba$ e $p_6(u) = u$. Note-se que todos os prefixos de comprimento menor ou igual a cinco são próprios. Finalmente, 1, c, ac, bac, $cbac$, $ccbac$ e u são sufixos de u.*

Diz-se que uma palavra $u \in A^+$ é *primitiva* se

$$u = v^n, \text{ com } v \in A^+ \text{ e } n \in \mathbb{N} \Rightarrow u = v \text{ (e } n = 1),$$

ou seja, u não é potência de uma outra palavra.

Duas palavras $u, v \in A^+$ dizem-se *conjugadas* se existem $x, y \in A^*$ tais que

$$u = xy, \quad v = yx.$$

Lema 2.5 *Sejam $u, v \in A^+$. Se u é primitiva e v é conjugada de u, então v também é primitiva.*

Demonstração: Seja $v \in A^+$. Suponhamos que v é conjugada de u. Então,

$$\exists w, z \in A^* : \quad u = wz \quad \text{e} \quad v = zw.$$

Suponhamos também que $v = r^k$, onde $r \in A^+$ e $k \in \mathbb{N}$. Então, existem $x, y \in A^*$ e $k_1, k_2 \in \mathbb{N}_0$ tais que $r = xy,\ z = r^{k_1}x,\ w = yr^{k_2}$ e $k_1 + k_2 + 1 = k$. Portanto,

$$u = wz = yr^{k_2}r^{k_1}x = (yx)^k,$$

e como u é primitiva, $k = 1$. Logo, $v = r$. Conclui-se assim que v é primitiva. □

2.2 Palavras infinitas

Seja A um alfabeto. Uma *palavra infinita à direita* sobre A é uma sequência $u = u_1u_2u_3\cdots$ de letras u_i indexadas por $\mathbb{N}$, ou seja, é uma aplicação $u : \mathbb{N} \to A$ tal que $u(n) = u_n$. Representamos por $A^{\mathbb{N}}$, o conjunto de todas as palavras infinitas à direita sobre A.

Define-se, de forma análoga, *palavra infinita à esquerda* sobre o alfabeto A como uma sucessão u de letras de A indexada por $-\mathbb{N}$, e representa-se por $u = \cdots u_{-3}u_{-2}u_{-1}$. Usamos a notação $A^{-\mathbb{N}}$, para representar o conjunto de todas as palavras infinitas à esquerda sobre A.

A notação $u_{[i,j]}$ $(i, j \in \mathbb{N},\ i \leq j)$ representa o factor (finito) $u_iu_{i+1}\cdots u_j$. O factor $u_{[1,j]}$, diz-se um prefixo (finito) de u e denota-se $p_j(u)$. O factor $u_{[i,-1]}$ diz-se um sufixo (finito) de u e denota-se $s_{-i}(u)$.

O produto de uma palavra finita $u = u_1u_2\cdots u_n$ de A^* por uma palavra infinita à direita $v = v_1v_2\cdots$ de $A^{\mathbb{N}}$ é a palavra infinita à direita

$$uv = u_1u_2\cdots u_nv_1v_2\cdots .$$

De forma dual define-se o produto de uma palavra infinita à esquerda v de $A^{-\mathbb{N}}$ por uma palavra finita u de A^*.

Consideremos $u = u_1u_2\cdots u_n$ uma palavra de A^+. Para notar a palavra infinita à direita (resp. à esquerda) obtida por repetição infinita à direita (resp.

à esquerda) da palavra u, escreve-se $u^{+\infty}$ (resp. $u^{-\infty}$). Tem-se então

$$u^{+\infty} = u_1u_2\cdots u_nu_1u_2\cdots u_n\cdots$$

$$u^{-\infty} = \cdots u_1u_2\cdots u_nu_1u_2\cdots u_n.$$

Seja $p \in \mathbb{N}$ e $w \in A^{\mathbb{N}}$. Se existe um natural r tal que para todo o n maior ou igual a r tem-se $w_n = w_{n+p}$, então p diz-se um período último da palavra infinita à direita w e esta diz-se *ultimamente periódica*. Uma palavra $w \in A^{\mathbb{N}}$ ultimamente periódica é da forma $w = uv^{+\infty}$, com $u \in A^*$ e $v \in A^+$. Note-se que, se $u = 1$ a palavra ultimamente periódica é da forma $w = v^{+\infty}$ e diz-se *periódica*.

Dada uma palavra ultimamente periódica w, chama-se *o período último de* w ao menor dos períodos últimos de w. Se $p_0 \in \mathbb{N}$ é o período último de uma palavra $w \in A^{\mathbb{N}}$, então existe um natural minimal r_0 tal que $w_n = w_{n+p_0}$ para todo o n maior ou igual a r_0. Este natural minimal r_0 é designado o *índice* de w. Assim, a palavra w pode escrever-se na dita *forma canónica*, como

$$w = w_1w_2\cdots w_{r_0-1}(w_{r_0}w_{r_0+1}\cdots w_{r_0+p_0-1})^{+\infty},$$

onde $w_1w_2\cdots w_{r_0-1} \in A^*$ e $w_{r_0}w_{r_0+1}\cdots w_{r_0+p_0-1} \in A^+$. O facto de r_0 ser minimal permite concluir que a letra w_{r_0-1} (se $r_0 > 1$) é diferente da letra $w_{r_0+p_0-1}$. Prova-se que a palavra w é periódica se e só se $r_0 = 1$. Portanto, para $u, v, w \in A^+$, se $s_1(u) \neq s_1(v)$, uma igualdade do tipo $uv^{+\infty} = w^{+\infty}$ não é possível. Note-se ainda que a palavra $w_{r_0}\cdots w_{r_0+p_0-1}$ é primitiva pelo facto de p_0 ser o período de w.

Exemplo 2.6 *Seja* $u = bcbab^2ab^2a\cdots$ *uma palavra ultimamente periódica. O período último de* u *é* 3*. Pode escrever-se*

$$u = bcba(b^2a)^{+\infty} = bc(bab)^{+\infty}.$$

Esta última representação de u *verifica* $s_1(bc) = c \neq b = s_1(bab)$*. Logo, esta última será a sua forma canónica.*

Analogamente, uma palavra $w \in A^{-\mathbb{N}}$ diz-se ultimamente periódica se

$$w = v^{-\infty}u \text{ para alguns } u \in A^* \text{ e } v \in A^+.$$

Se u e v forem escolhidas de comprimento mínimo, então $v^{-\infty}u$ é a forma canónica de w. A palavra w diz-se periódica se u é a palavra vazia.

2.3 Linguagens

Chamamos *linguagem sobre um alfabeto* A a um subcojunto de A^*. Assim, o conjunto de todas as linguagens sobre A é $\mathcal{P}(A^*) = \{L | L \subseteq A^*\}$.

Exemplo 2.7 *Seja* $A = \{a, b\}$. *Então* $\emptyset$, $\{1\}$, $\{a\}$, A, $\{bab, aababb, baa\}$, A^+ *e* A^* *são linguagens sobre* A.

Definição 2.8 *Dados um alfabeto* A *e as linguagens* L, K *de* A^*, *definimos:*

(i) O produto de concatenação de L *por* K*:*

$$LK = \{uv \in A^* | u \in L \text{ e } v \in K\}$$

(ii) O subsemigrupo de A^* *gerado por* L, *designado de fecho positivo de* L*:*

$$L^+ = \{u_1 u_2 \cdots u_n | n \in \mathbb{N}, u_i \in L, i = 1, 2, \ldots n\}$$

(iii) O submonóide de A^* *gerado por* L, *designado de estrela ou fecho (de Kleene) de* L*:*

$$L^* = L^+ \cup \{1\}$$

(iv) O quociente à esquerda de L *por* K*:*

$$K^{-1}L = \{v \in A^* | \exists u \in K : uv \in L\}$$

(v) O quociente à direita de L *por* K*:*

$$LK^{-1} = \{v \in A^* | \exists u \in K : vu \in L\}$$

Não distinguiremos, quando tal não der origem a ambiguidades, a palavra u da linguagem $\{u\}$. Consequentemente, escreveremos $u^{-1}L$ e Lu^{-1} em vez de $\{u\}^{-1}L$ e $L\{u\}^{-1}$, respectivamente.

Proposição 2.9 *Seja* L *uma linguagem. Então,*

1) $L = L^1 \subseteq L^+ \subseteq L^+ \cup \{1\} = L^*$;

2) $1 \in L^+$ *se e só se* $1 \in L$;

3) $L^+ = LL^* = L^*L$.

Apresentamos de seguida uma das classes mais importantes de linguagens:

Definição 2.10 *O conjunto* $Rac(A)$*, das linguagens racionais sobre um alfabeto* A*, é o menor conjunto de linguagens sobre* A *tal que:*

i) $\emptyset, \{1\} \in Rac(A)$*;*

ii) $\{a\} \in Rac(A)$ *para todo o* $a \in A$*;*

iii) $Rac(A)$ *é fechado para as operações de união, produto e fecho de Kleene. Ou seja, se* $L, K \in Rac(A)$ *então* $L \cup K,\ LK,\ L^* \in Rac(A)$.

Note-se que, se L é uma linguagem racional sobre um alfabeto A, então $L^+ = L^*L$ também é uma linguagem racional sobre A.

2.4 Autómatos

Definição 2.11 *Um autómato (finito) é um quíntuplo* $\mathcal{A} = (Q, A, \delta, q_0, F)$ *onde*

i) Q *é um conjunto finito não vazio, chamado o conjunto de estados de* $\mathcal{A}$*;*

ii) A *é um alfabeto, chamado o alfabeto (de entrada) de* $\mathcal{A}$*;*

iii) $\delta : Q \times A \to \mathcal{P}(Q)$ *é uma função, designada a função transição de* $\mathcal{A}$*. Cada triplo* (p, a, q)*, em que* $p, q \in Q$ *e* $a \in A$ *são tais que* $q \in \delta(p, a)$*, diz-se uma transição de* $\mathcal{A}$*;*

iv) $q_0 \in Q$ *é dito o estado inicial de* $\mathcal{A}$*;*

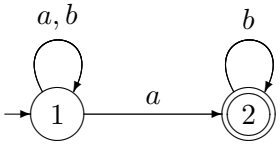
v) $F \subseteq Q$ *é dito o conjunto de estados finais de* $\mathcal{A}$.

Um autómato é usualmente representado por um grafo onde os vértices representam os estados do autómato e as arestas exprimem as transições do autómato. Representa-se ainda o estado inicial do autómato por uma seta (a entrar) e cada estado final por uma circunferência extra.

Exemplo 2.12 *Seja* $\mathcal{A} = (Q, A, \delta, q_0, F)$ *onde* $Q = \{1, 2\}$, $A = \{a, b\}$, $q_0 = 1$, $F = \{2\}$ *e* δ *é a função definida pela tabela seguinte:*

δ	1	2
a	$\{1, 2\}$	$\emptyset$
b	$\{1\}$	$\{2\}$

O autómato $\mathcal{A}$ *é representado pelo diagrama seguinte:*



Um *caminho* em $\mathcal{A}$ é uma sequência finita

$$(q_0, a_1, q_1), (q_1, a_2, q_2), \ldots, (q_{n-1}, a_n, q_n)$$

de transições consecutivas de $\mathcal{A}$, usualmente também representado por

$$q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \cdots q_{n-1} \xrightarrow{a_n} q_n.$$

O estado q_0 é a *origem* do caminho e o estado q_n o seu *término* e diz-se que o caminho *sai* de q_0 e *chega* a q_n. Diz-se também que o caminho *passa pelos estados* $q_0, q_1, \ldots, q_n$. A palavra $a_1 a_2 \cdots a_n$ sobre A é chamada a *etiqueta* do caminho.

Uma palavra $u \in A^*$ diz-se *aceite* ou *reconhecida* pelo autómato $\mathcal{A}$ se u é a etiqueta de pelo menos um caminho bem sucedido em $\mathcal{A}$ (isto é, se o caminho é simulatneamente inicial e final, ou seja, sai de um estado inical e chega a um estado final). Caso contrário diz-se que u é *rejeitada* ou *não reconhecida* por $\mathcal{A}$. A linguagem *aceite* ou *reconhecida* pelo autómato $\mathcal{A}$ é o conjunto, representado por $L(\mathcal{A})$, das palavras aceites por $\mathcal{A}$. Por exemplo, a linguagem reconhecida pelo autómato do exemplo 2.12 é $L(\mathcal{A}) = A^*ab^*$.

Uma linguagem L diz-se *reconhecível* se existe um autómato $\mathcal{A}$ que reconhece L, ou seja, tal que $L = L(\mathcal{A})$.

Podemos agora enunciar o mais importante resultado da teoria de autómatos, que é considerado como o fundador da teoria das linguagens racionais e dos autómatos finitos.

Teorema 2.13 (Kleene, 1954) *Uma linguagem* L *é racional se e só se* L *é reconhecível.*

2.5 Reconhecimento de linguagens por semigrupos

Definição 2.14 *Seja A um alfabeto e L uma linguagem de A^+. Diz-se que L é reconhecida por um semigrupo S se existem um morfismo de semigrupos $\varphi : A^+ \longrightarrow S$ e $P \subseteq S$ tais que*

$$L = \varphi^{-1}(P).$$

Diz-se também neste caso que L é reconhecida pelo morfismo φ.

Uma linguagem de A^+ é dita reconhecível por semigrupos se ela é reconhecida por um semigrupo finito.

As noções de linguagem reconhecível por autómato finito e de linguagem reconhecível por semigrupo finito são equivalentes como mostra o próximo resultado.

Teorema 2.15 *Seja $L \subseteq A^+$ uma linguagem. Então L é reconhecida por um autómato (finito) $\mathcal{A}$ se e só se L é reconhecida por um semigrupo finito.*

Corolário 2.16 *Uma linguagem L é reconhecível se e só se L é reconhecível por semigrupos.*

Seja $L \subseteq A^+$ uma linguagem. Chamamos *congruência sintáctica* de L à congruência σ_L sobre A^+ definida por

$$u\sigma_L v \iff (\forall x, y \in A^*,\ xuy \in L \Leftrightarrow xvy \in L).$$

O *semigrupo sintáctico* de L é o semigrupo quociente $S(L) = A^+/\sigma_L$. O morfismo natural

$$\eta_L : A^+ \longrightarrow S(L)$$

é chamado o *morfismo sintáctico* de L. Note-se que, pela definição de σ_L, tem-se $L = \eta_L^{-1}(\eta_L(L))$, o que mostra que L é reconhecida por η_L.

A seguinte proposição mostra que o semigrupo sintáctico de uma linguagem L é o mais pequeno semigrupo que reconhece L.

Proposição 2.17 *Seja L uma linguagem de A^+. Um semigrupo T reconhece L se e só se $S(L)$ divide T.*

Como consequência desta proposição obtém-se o seguinte resultado:

Corolário 2.18 *Seja L uma linguagem tal que $L \subseteq A^+$. Então L é reconhecível se e só se o seu semigrupo sintáctico $S(L)$ é finito.*

De forma análoga podemos considerar linguagens de monóides livres A^* e aplicar os resultados e definições anteriores a reconhecimento por monóides. Para tal, basta substituir o símbolo $+$ por $*$ e o termo "semigrupo" por "monóide". Em particular, podemos definir o *monóide sintáctico* de L como sendo o *monóide quociente* $M(L) = A^*/\sigma_L$, em que σ_L é a congruência sintáctica definida sobre A^*.

2.6 Exemplos importantes de linguagens racionais

Nesta secção são introduzidas algumas classes importantes de linguagens racionais. Estas classes forneceram os primeiros exemplos da utilidade dos semigrupos para decidir resultados sobre linguagens.

2.6.1 Linguagens livres de estrela

Uma das classes de linguagens racionais mais importante é a das *linguagens livres de estrela*. Esta classe é definida através de uma pequena alteração na definição da classe Rac das linguagens racionais (Definição 2.10), designadamente a substituição do operador estrela pelo operador de complementação.

Definição 2.19 *O conjunto $\mathcal{F}_{\mathbb{S}}(\mathcal{A}^*)$, das linguagens livres de estrela sobre um alfabeto A, é o menor conjunto de linguagens sobre A tal que:*

i) $\emptyset, \{1\} \in \mathcal{F}_{\mathbb{S}}(\mathcal{A}^*)$;

ii) $\forall a \in A,\ \{a\} \in \mathcal{F}_{\mathbb{S}}(\mathcal{A}^*)$;

iii) $\mathcal{F}_{\mathbb{S}}(\mathcal{A}^*)$ *é fechado para as operações de união, produto e complementação. Ou seja, se* $L, K \in \mathcal{F}_{\mathbb{S}}(\mathcal{A}^*)$ *então* $L \cup K,\ LK,\ \overline{L} = A^* \backslash L \in \mathcal{F}_{\mathbb{S}}(\mathcal{A}^*)$.

Como se pode verificar, a classe $\mathcal{F}_{\mathbb{S}}(\mathcal{A}^*)$ das linguagens livres de estrela sobre A é de facto uma subclasse de $\mathcal{R}ac(A^*)$.

Proposição 2.20 *Se L é uma linguagem livre de estrela, então L é racional.*

Exemplo 2.21 *Seja A um alfabeto.*

1) As linguagem A^+ e A^* são livres de estrela pois

$$A^+ = \overline{\overline{\{1\}}} \quad e \quad A^* = \overline{\emptyset}$$

e, por definição $\{1\}$ e $\emptyset$ são livres de estrela e $\mathcal{F}_{\mathbb{S}}(\mathcal{A}^*)$ é fechado para complementação.

2) Toda a linguagem finita é livre de estrela.

3) Supondo que $A = \{a, b, c\}$ e tendo em conta os exemplos anteriores, é agora imediato que as linguagens seguintes são livres de estrela

$$aA^*cA^*,\ (A^+c)\backslash bA^* \cup \{b, ca\},\ aA^+\{b, ac\}A^*.$$

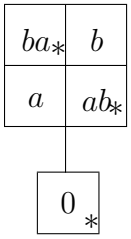
Através destes exemplos constata-se que a utilização da definição é útil para verificar se as linguagens racionais são livres de estrela. No entanto, existem outros exemplos onde a utilização da definição se mostra bastante complexa (por vezes, impossível) para verificar se uma dada linguagem é ou não livre de estrela. O teorema seguinte, provado por Schützenberger [42] em 1965, fornece um critério para decidir se uma dada linguagem racional é livre de estrela. É um resultado profundo e representa um passo importante na caracterização de linguagens através de semigrupos.

Teorema 2.22 (Schützenberger, 1965) *Uma linguagem $L \subseteq A^*$ é livre de estrela se e só se o monóide sintáctico $M(L)$ é finito e aperiódico.*

Exemplo 2.23 *Consideremos a linguagem $L = (ab)^+$ sobre o alfabeto $A = \{a, b\}$. Facilmente pode-se verificar que a congruência sintática σ_L tem cinco classes, que são os elementos de $S(L)$, e que as podemos representar por a, b, ab, ba e 0. Portanto, $S(L) = \{a, b, ab, ba, 0\}$. A sua tabela de Cayley é representada da seguinte forma:*

$\cdot$	a	b	ab	ba	0
a	0	ab	0	a	0
b	ba	0	b	0	0
ab	a	0	ab	0	0
ba	0	b	0	ba	0
0	0	0	0	0	0

Deste modo, a sua estrutura em $\mathcal{J}$-classes é apresentada desta forma:



Como se pode verificar pelo diagrama, o semigrupo $S(L)$ é $\mathcal{H}$-trivial. Logo $S(L)$ é aperiódico. Portanto, pelo Teorema de Schützenberger, L é livre de estrela. Também se poderia verificar que

$$(ab)^+ = (aA^* \cap A^*b) \backslash (A^*aaA^* \cup A^*bbA^*).$$

Como consequência, a linguagem $(ab)^* = (ab)^+ \cup \{1\}$ também é livre de estrela.

2.6.2 Linguagens localmente testáveis

Uma outra classe importante de linguagens racionais é a classe das linguagens localmente testáveis. Neste tipo de classe, comparativamente com as classes anteriormente definidas, exclui-se o operador produto e consideram-se linguagens geradoras um pouco mais gerais. Importante de salientar, é o facto de que, estas linguagens geradoras são ainda livres de estrela. Por este motivo, a classe das linguagens localmente testáveis sobre um alfabeto A é uma subclasse de $\mathcal{F}_S(A^*)$.

Definição 2.24 *O conjunto $\mathcal{L}t(A^+)$, das linguagens localmente testáveis sobre um alfabeto A, é o menor conjunto de linguagens de A^+ tal que:*

i) $uA^*, A^*u, A^*uA^* \in \mathcal{L}t(A^+)$ para todo $u \in A^+$;

ii) Se $L, K \in \mathcal{L}t(A^+)$*, então* $L \cup K, \overline{L} = A^+ \backslash L \in \mathcal{L}t(A^+)$*. Ou seja,* $\mathcal{L}t(A^+)$ *é fechado para as operações de união e complementação.*

Note-se que a intersecção $L \cap K$, de duas linguagens L e K, pode ser obtida a partir de L e K, usando os operadores de união e complementação. Tem-se assim,

$$L \cap K = \overline{\overline{L} \cup \overline{K}}$$

Portanto a classe $\mathcal{L}t(A^+)$ é fechada para as operações de união, intersecção e complementação, ou seja, para todas as operações booleanas. Assim, a classe $\mathcal{L}t(A^+)$ pode ser definida como sendo a álgebra de Boole gerada pelas linguagens da forma uA^*, A^*u e A^*uA^* com $u \in A^+$.

Dado que as linguagens do tipo uA^*, A^*u e A^*uA^* onde $u \in A^+$, são livres de estrela e a classe $\mathcal{F}_S(A^*)$ é fechada para as operações booleanas, infere-se o seguinte resultado.

Teorema 2.25 *Toda a linguagem localmente testável é livre de estrela.*

Passemos agora a estudar alguns exemplos de linguagens localmente testáveis.

Exemplos 2.26 *Seja* A *um alfabeto.*

1) A linguagem A^+ *é localmente testável pois*

$$A^+ = \bigcup_{a \in A} aA^*.$$

2) Toda a linguagem finita é localmente testável. De facto,

$$\{u\} = uA^* \backslash \bigcup_{a \in A} uaA^*.$$

3) A linguagem $L = (ab)^+$*, sobre* $A = \{a, b\}$*, é localmente testável pois*

$$L = (aA^* \cap A^*b) \backslash (A^*aaA^* \cup A^*bbA^*).$$

Para verificar se uma palavra pertence a uma linguagem localmente testável apenas é necessária informação "local".

Dado um semigrupo S e um idempotente $e \in S$, é fácil verificar que

$$eSe = \{ese |\ s \in S\}$$

é um subsemigrupo de S, que é ele próprio um monóide de identidade e. O monóide eSe é chamado um monóide local em S.

Um critério para decidir se uma dada linguagem é localmente testável é fornecido pelo resultado seguinte, obtido por Brzozowski e Simon [20] e por McNaughton [31] por volta de 1973.

Teorema 2.27 *Uma linguagem L, tal que $L \subseteq A^+$, é localmente testável se e só se $S = S(L)$ é finito e eSe é um semireticulado para todo o idempotente e de S.*

2.6.3 Linguagens testáveis aos pedaços

Para finalizar os exemplos de classes de linguagens racionais, falaremos das classes de *linguagens testáveis aos pedaços*. Estas classes, assim como as classes das linguagens localmente testáveis, são álgebras de Boole, e por sua vez, também estão contidas na classe das linguagens livres de estrela. O que a distingue, das linguagens localmente testáveis e das linguagens testáveis aos pedaços, é o conjunto dos respectivos geradores.

Definição 2.28 *O conjunto $\mathcal{T}_p(A^*)$, das linguagens testáveis aos pedaços sobre um alfabeto A, é o menor conjunto de linguagens de A^* tal que:*

i) $A^*a_1A^*a_2A^* \cdots A^*a_nA^* \in \mathcal{T}_p(A^*)$ *para todos* $n \in \mathbb{N}_0$ *e* $a_1, a_2, \ldots, a_n \in A$;

ii) Se $L, K \in \mathcal{T}_p(A^*)$, *então* $L \cup K, \overline{L} = A^* \backslash L \in \mathcal{T}_p(A^*)$. *Ou seja,* $\mathcal{T}_p(A^*)$ *é fechado para as operações de união e complementação.*

Assim, a classe $\mathcal{T}_p(A^*)$ é a álgebra de Boole gerada pelas linguagens da forma

$$A^*a_1A^*a_2A^* \cdots A^*a_nA^*$$

onde $n \in \mathbb{N}_0$ *e* $a_1, a_2, \ldots, a_n \in A$.

Vejamos alguns exemplos simples de linguagens testáveis aos pedaços.

Exemplos 2.29 *Seja A um alfabeto.*

1) Toda a linguagem finita de A^* é testável aos pedaços.

2) Seja $A = \{a, b\}$ e seja $L = A^*abA^*$. A linguagem L pode ser escrita da seguinte forma,

$$L = A^*aA^*bA^*$$

e portanto é testável aos pedaços.

Para as linguagens testáveis aos pedaços também existe um critério para decidir se uma dada linguagem pertence a essa classe, descoberto por Simon [43] no seu trabalho de doutoramento.

Teorema 2.30 *(Simon, 1972) Uma linguagem $L \subseteq A^*$ é testável aos pedaços se e só se $M(L)$ é finito e $\mathcal{J}$-trivial.*

Vejamos dois exemplos onde se poderá aplicar o teorema enunciado.

Exemplos 2.31 *Seja $A = \{a, b\}$ um alfabeto.*

1) A linguagem $L = a^*b^+a^*$ sobre o alfabeto A é testável aos pedaços pois $S(L)$ é $\mathcal{J}$-trivial. Facilmente se pode verificar que $L = A^*bA^* \backslash A^*bA^*aA^*bA^*$.

2) A linguagem $L = (ab)^+$ sobre o alfabeto A não é testável aos pedaços pois, como vimos no exemplo 2.23, $S(L)$ não é $\mathcal{J}$-trivial. No entanto, tal como foi visto anteriormente, esta linguagem é localmente testável.

2.7 Máquinas de Turing

Nesta secção vamos introduzir alguns fundamentos sobre Máquinas de Turing. Na tentativa de responder a algumas questões relacionadas com a noção de "computação", Turing [matemático Inglês, 1912 - 1954] procurou identificar as operações primitivas, fundamentais, envolvidas num processo algorítmico e definiu (na década de 1930) um modelo abstracto de máquina, posteriormente designada por *máquina de Turing*, capaz de realizar essas mesmas operações a partir de regras claramente definidas.

2.7.1 Noções Básicas

Segue-se a definição de máquina de Turing.

Definição 2.32 *Uma máquina de Turing é um septeto* $\mathcal{T} = (Q, A, T, \delta, q_0, q_f, \Delta)$ *onde*

1) Q *é um conjunto finito não vazio, chamado o conjunto de estados de* $\mathcal{T}$*;*

2) A *é um alfabeto, chamado o alfabeto (de entrada) de* $\mathcal{T}$*;*

3) T *é um alfabeto onde* $A \subseteq T$ *e* $Q \cap T = \emptyset$*. Então* T *é dito o alfabeto da fita de* $\mathcal{T}$ *e o conjunto* $T \setminus A$ *é chamado o alfabeto auxiliar de* $\mathcal{T}$*;*

4) $\delta : Q \times T \longrightarrow Q \times T \times \{E, C, D\}$ *é uma função parcial que não está definida em* (q_f, t)*, para cada* $t \in T$*, e é designada a função transição de* $\mathcal{T}$*. O conjunto* $\{E, C, D\}$ *contém os três movimentos possíveis:*

E – *esquerda*;
C – *"centro"(ausência de movimento)*;
D – *direita*;

5) $q_0 \in Q$*, dito o estado inicial de* $\mathcal{T}$*;*

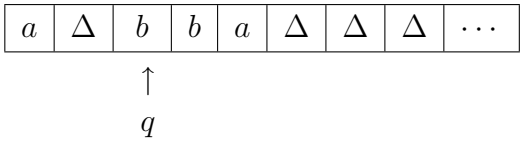
6) $q_f \in Q$*, chamado o estado final de* $\mathcal{T}$*;*

7) $\Delta \in T \setminus A$ *é um símbolo auxiliar, designado o símbolo branco.*

A diferença essencial em relação aos autómatos finitos é que uma máquina de Turing $\mathcal{T} = (Q, A, T, \delta, q_0, q_f, \Delta)$ é dotada de:

1) uma *fita* dividida em células (ou quadrados), infinita para a direita e com uma célula inicial à esquerda. Cada célula tem uma letra de T e em cada instante o número de células não brancas (ou seja células onde não está escrito o símbolo branco Δ) é finito;

2) uma *cabeça* ou *cursor* (de leitura e escrita) posicionada em cada momento numa determinada célula da fita, que permite ler a letra da célula e eventualmente substituir essa letra por outra. Por exemplo, a figura seguinte



representa a fita de uma máquina de Turing em que nas 1ª e 5ª células (a contar da esquerda para a direita) está escrita a letra a, nas 3ª e 4ª células está escrito b e todas as outras estão em branco. A seta indica que a cabeça está posicionada na 3ª célula e a letra q por baixo da seta indica o estado actual da máquina de Turing.

A cabeça pode efectuar movimentos determinados pela função transição. Assim, a igualdade

$$\delta(q,t) = (q', t', m)$$

significa que, quando a máquina está no estado q com a cabeça posicionada numa célula onde está escrita a letra t, a máquina transita para o estado q', substitui a letra t pela letra t' e efectua o movimento m (ou seja, move-se para a esquerda, para a direita ou não se move, conforme m seja E, D ou C).

Seja $\mathcal{T} = (Q, A, T, \delta, q_0, q_f, \Delta)$ uma máquina de Turing. Chama-se *configuração* de $\mathcal{T}$ a um par ordenado $(q, u\underline{t}v)$ onde $q \in Q$, $u, v \in T^*$ e $t \in T$ e tal que:

1) q é o estado actual da máquina;

2) a palavra utv está escrita na fita, o mais à esquerda possível, (ou seja, a primeira letra de utv ocupa a 1ª célula) e todas as células após v estão preenchidas com o símbolo branco Δ;

3) a cabeça está posicionada na célula ocupada pela letra t.

Note-se que uma configuração representa a situação da máquina de Turing (da fita e do cursor) num dado momento.

Seja $\mathcal{T} = (Q, A, T, \delta, q_0, q_f, \Delta)$ uma máquina de Turing. Uma configuração $c = (q, u\underline{t}v)$ de $\mathcal{T}$ diz-se uma configuração de:

- *paragem* se δ não está definida em (q,t) ou, $u = \epsilon$ e $\delta(q,t) = (q', t', E)$;

- *aceitação* se $q = q_f$;
- *rejeição* se c é uma configuração de paragem e $q \neq q_t$;
- *ciclo* se a partir de c não é possível computar uma configuração de paragem.

Podemos ainda afirmar que:

- $(i, \underline{\Delta} w)$ é a configuração *inicial* associada a uma palavra $w \in A^*$;
- uma palavra $w \in A^*$ é *aceite* ou *reconhecida* por $\mathcal{T}$ se existe uma computação de uma configuração de aceitação a partir da configuração inicial associada a w; ou seja, se existe uma computação

$$(q_0, \underline{\Delta} w) \xrightarrow[\mathcal{T}]{*} (q_t, u\underline{t}v)$$

  para uma certa configuração de aceitação $(q_t, u\underline{t}v)$. Caso contrário diz-se que w é *não reconhecida* por $\mathcal{T}$. Partindo da configuração inicial associada a um palavra w, esta poderá não ser aceite por um dos seguintes motivos:

  1. a máquina de Turing pára numa configuração de rejeição;
  2. a máquina de Turing não pára, ou seja, a configuração inicial associada a w é uma configuração de ciclo;

- a linguagem *aceite* ou *reconhecida* por $\mathcal{T}$, representada por $L(\mathcal{T})$, é o conjunto das palavras aceites por $\mathcal{T}$.

O resultado seguinte mostra-nos que uma classe de linguagens reconhecidas por máquinas de Turing contém a classe das linguagens reconhecidas por autómatos finitos.

Teorema 2.33 *Toda a linguagem racional é reconhecida por uma máquina de Turing.*

No entanto, o recíproco deste resultado não é válido.

Tal como foi referido no início desta secção, as máquinas de Turing podem também ser usadas para definir funções.

Na década de 1930, Alonzo Church afirmou que, qualquer função que pode ser calculada por um processo algorítmico, por pessoas ou computadores, é *Turing-computável*. Esta afirmação ficou conhecida como *tese de Church* ou *tese de Church-Turing*.

Deste modo é aceitável que se diga que as linguagens que podem ser reconhecidas algoritmicamente são aquelas que são reconhecíveis por máquinas de Turing.

2.7.2 Linguagens recursivas e linguagens recursivamente enumeráveis

Definição 2.34 *Uma linguagem L diz-se*

- *recursivamente enumerável se existe uma máquina de Turing que reconhece L;*
- *recursiva se L e $\overline{L}$ são recursivamente enumeráveis.*

Note-se que, pela própria definição, todas as linguagens recursivas são recursivamente enumeráveis.

Contudo, o contrário não se verifica. Ou seja, nem todas as linguagens recursivamente enumeráveis são recursivas. O resultado seguinte caracteriza as linguagens recursivas como sendo aquelas que são aceites por máquinas de Turing que param seja qual for o "input". Estas máquinas são por vezes chamadas "algoritmos".

Proposição 2.35 *Se $L \subseteq A^*$ é uma linguagem reconhecida por uma máquina de Turing $\mathcal{T}$ que não admite configurações de ciclo, então L é uma linguagem recursiva.*

As seguintes propriedades são válidas:

Proposição 2.36 *Sejam L e L' linguagens sobre um alfabeto A.*

1. *Se L e L' são recursivas (resp. recursivamente enumeráveis), então $L \cup L'$ e $L \cap L'$ são recursivas (resp. recursivamente enumeráveis).*
2. *Se L é recursiva, então $\overline{L}$ é recursiva.*

O teorema seguinte mostra que as linguagens recursivamente enumeráveis formam uma pequena parte do conjunto de todas as linguagens.

Teorema 2.37 *Existem linguagens não recursivamente enumeráveis sobre qualquer alfabeto A. Mais precisamente, o conjunto das linguagens não recursivamente enumeráveis sobre A é infinito não numerável.*

Demonstração: Prova-se que o conjunto das linguagens recursivamente enumeráveis é um conjunto numerável, enquanto que $\mathcal{P}(A^*)$ (o conjunto de todas as linguagens sobre A) é infinito não numerável. □

Capítulo 3

Variedades

3.1 Variedades de semigrupos

O conceito de variedade de semigrupos foi introduzido por Birkhoff. Uma classe de semigrupos não vazia V é dita uma variedade se é fechada para a formação de subsemigrupos, imagens homomorfas e produtos directos. Se é fechada para a formação de subsemigrupos e imagens homomorfas, então é fechada para a divisão e vice-versa. Portanto, V é uma variedade se é fechada para a divisão e para produtos directos. Como exemplos de classes de semigrupos que formam variedades, referimos as seguintes:

- S, a classe de todos os semigrupos;
- Sl, a classe de todos os semi-reticulados;
- RB, a classe de todas as bandas rectangulares.

Toda a intersecção de variedades é ainda uma variedade. Podemos portanto definir a variedade *gerada* por uma classe $\mathcal{C}$ de semigrupos, denotada por $\mathsf{V}(\mathcal{C})$, como sendo a intersecção de todas as variedades que contêm $\mathcal{C}$.

Seja A um alfabeto. Uma *identidade* de semigrupos sobre A é um par (u, v) de palavras de A^+, normalmente representada pela igualdade $u = v$. Uma identidade do tipo $u = u$ diz-se *trivial*.

Diz-se que um semigrupo S *satisfaz* ou (*verifica*) a identidade $u = v$, e escreve-se $S \vDash u = v$, se para qualquer homomorfismo $\varphi : A^+ \to S$, se tem $\varphi(u) = \varphi(v)$.

Uma classe $\mathcal{C}$ de semigrupos satisfaz um conjunto Σ de identidades, e denotamos por $\mathcal{C} \vDash \Sigma$, se

$$\forall S \in \mathcal{C}\, \forall u = v \in \Sigma,\ S \vDash u = v.$$

Dado um conjunto Σ de identidades, verifica-se que a classe de todos os semigrupos que verificam todas as identidades de Σ é uma variedade. Usamos a notação $[\Sigma]$ para representar essa variedade, dita a variedade *definida* por Σ.

Uma classe de semigrupos $\mathcal{V}$ diz-se *equacional* se existe um conjunto Σ de identidades tal que $\mathcal{V} = [\Sigma]$. Neste caso, diz-se que Σ é uma *base (de identidades)* de $\mathcal{V}$.

O resultado fundamental que se segue, enunciado apenas para semigrupos, foi demonstrado por Birkhoff em 1935 para classes de álgebras do mesmo tipo.

Teorema 3.1 (Birkhoff) *Uma classe de semigrupos é uma variedade se e só se é equacional.*

Exemplo 3.2 *Alguns exemplos de variedades de semigrupos:*

1. *A variedade das bandas, representado por* B*, pode ser definido por*

$$\mathsf{B} = [a^2 = a] = \{S : S \vDash a^2 = a\}$$

2. *A variedade dos semi-reticulados, representado por* Sl*, pode ser definido por*

$$\mathsf{Sl} = [a^2 = a, ab = ba] = \{S : S \vDash a^2 = a \ \ e \ \ S \vDash ab = ba\}$$

3.2 Pseudovariedades de semigrupos

Dispomos de um conceito análogo ao de variedade para classes de semigrupos finitos que é o conceito de *pseudovariedade* de semigrupos (também chamada *variedade de semigrupos finitos*). Este conceito foi introduzido por Eilenberg em 1976.

Uma *pseudovariedade* de semigrupos é uma classe não vazia, $\mathbf{V}$, de semigrupos finitos fechada para a formação de subsemigrupos, imagens homomorfas e produtos directos finitos, ou seja, $\mathbf{V}$ é tal que:

i) se $S \in \mathbf{V}$ e $T \leq S$, então $T \in \mathbf{V}$;

ii) se $S \in \mathbf{V}$ e $\varphi : S \to T$ é um epimorfismo de semigrupos, então $T \in \mathbf{V}$;

iii) se $S_1, \ldots, S_n \in \mathbf{V}$, então $S_1 \times \cdots \times S_n \in \mathbf{V}$.

De modo equivalente, $\mathbf{V}$ é uma pseudovariedade se é fechada para a divisão e para produtos directos finitos.

Exemplo 3.3 *Alguns exemplos de pseudovariedades:*

1. $\mathbf{S}$*, a classe de todos os semigrupos finitos;*
2. $\mathbf{I}$*, a classe constituída pelos semigrupos com um único elemento, chamada a pseudovariedade trivial;*
3. $\mathbf{Sl}$*, a classe de todos os semi-reticulados finitos;*
4. $\mathbf{G}$*, a classe de todos os grupos finitos;*
5. $\mathbf{N}$*, a classe de todos os semigrupos nilpotentes finitos;*
6. $\mathbf{K}$*, a classe de todos os semigrupos finitos S tais que $es = e$ para todos os $e \in E(S)$ e $s \in S$;*
7. $\mathbf{D}$*, a classe de todos os semigrupos finitos S tais que $se = e$ para todos os $e \in E(S)$ e $s \in S$;*
8. $\mathbf{LI}$*, a classe de todos os semigrupos finitos localmente triviais.*

Algumas classes de semigrupos finitos não constituem pseudovariedades. É o caso, por exemplo, da classe de todos os semigrupos regulares finitos.

A intersecção de pseudovariedades é ainda uma pseudovariedade. Considerando $\mathcal{C}$ uma classe de semigrupos finitos, define-se a pseudovariedade gerada por $\mathcal{C}$, e representa-se por $\mathbf{V}(\mathcal{C})$, como sendo a intersecção de todas as pseudovariedades que contêm $\mathcal{C}$. A pseudovariedade $\mathbf{V}(\mathcal{C})$ pode ainda ser definida de uma forma construtiva por:

$$\mathbf{V}(\mathcal{C}) = \{S \in \mathbf{S} : \exists n \in \mathbb{N}\ \exists S_1, \ldots, S_n \in \mathcal{C},\ S \prec S_1 \times \ldots \times S_n\}.$$

No caso de $\mathcal{C}$ ser formada apenas por um semigrupo S, escreve-se simplesmente $\mathbf{V}(S)$ para designar a pseudovariedade gerada por $\mathcal{C}$, que também é designada por *pseudovariedade gerada por* S.

3.2.1 Pseudovariedades não equacionais

Seja Σ um conjunto de identidades. A classe de todos os semigrupos finitos que verificam todas as identidades de Σ é uma pseudovariedade, que se representa por $[\![\Sigma]\!]$ e dizemos que é *definida* por Σ.

Uma pseudovariedade $\mathbf{V}$ diz-se *equacional* se existe um conjunto Σ de identidades tal que $\mathbf{V} = [\![\Sigma]\!]$. Neste caso, diz-se que Σ é uma *base de identidades* de $\mathbf{V}$. As pseudovariedades seguintes são equacionais

$$\mathbf{S} = [\![a = a]\!],\ \mathbf{I} = [\![a = b]\!],\ \mathbf{B} = [\![a = a^2]\!],\ \mathbf{Sl} = [\![ab = ba, a = a^2]\!].$$

Pelo contrário, as pseudovariedades $\mathbf{G}$ e $\mathbf{N}$ não satisfazem identidades não triviais. Portanto tem-se o seguinte resultado.

Proposição 3.4 *Toda a pseudovariedade, distinta de* $\mathbf{S}$*, contendo* $\mathbf{G}$ *ou* $\mathbf{N}$ *é não equacional.*

Como já referimos, nem todas as pseudovaridades são equacionais. No entanto, todas podem ser definidas ultimamente através de identidades, como mostra o teorema seguinte.

Teorema 3.5 (Eilenberg-Schützenberger [26]) *Uma classe não vazia* $\mathcal{U}$ *de semigrupos finitos é uma pseudovariedade se e só se existe uma sucessão* $(u_n = v_n)_{n\in\mathbb{N}}$ *de identidades tal que*

$$\mathcal{U} = \{S \in \mathbf{S} : \exists p \in \mathbb{N}\ \forall n \geq p,\ S \vDash u_n = v_n\}.$$

Ou seja, $\mathcal{U}$ *é constituída pelos semigrupos finitos que satisfazem todas as identidades* $u_n = v_n$*, a partir de uma certa ordem. Dizemos nesse caso, que* $\mathcal{U}$ *é definida ultimamente pela sucessão* $(u_n = v_n)_{n\in\mathbb{N}}$.

Como exemplos, apresentamos:

- $\mathbf{G} = \{S \in \mathbf{S} : \exists p \in \mathbb{N}\ \forall n \geq p,\ S \vDash a^{n!}b = ba^{n!} = b\}$;
- $\mathbf{N} = \{S \in \mathbf{S} : \exists p \in \mathbb{N}\ \forall n \geq p,\ S \vDash a^n b = ba^n = a^n\}$;
- $\mathbf{R} = \{S \in \mathbf{S} : \exists p \in \mathbb{N}\ \forall n \geq p,\ S \vDash (ab)^n = (ab)^n a\}$;

- $\mathbf{J} = \{S \in \mathbf{S} : \exists p \in \mathbb{N}\ \forall n \geq p,\ S \vDash (ab)^n a = (ab)^n = b(ab)^n\}$.

onde **R** e **J** denotam as pseudovariedades dos semigrupos finitos $\mathcal{R}$-triviais e $\mathcal{J}$--triviais, respectivamente.

Esta notação pode ser bastante simplificada se utilizarmos pseudoidentidades. Este conceito será estudado mais à frente no capítulo 4.

3.3 Variedades de Linguagens

Já vimos as variedades e as variedades de semigrupos finitos. Para finalizar, vamos estudar as variedades de linguagens. Existe um resultado que faz uma correspondência biunívoca entre variedades de linguagens e pseudovariedades de semigrupos, que é o teorema das variedades de Eilenberg.

A uma correspondência $\mathcal{C}$ que associa a cada alfabeto A um conjunto de linguagens reconhecíveis de A^+, representado por $\mathcal{C}(A^+)$, chama-se uma *classe de linguagens reconhecíveis*.

Definição 3.6 *Uma variedade de linguagens é uma classe $\mathcal{V}$ de linguagens reconhecíveis tal que, para todos os alfabetos A e B, tem-se*

(i) $\mathcal{V}(A^+)$ *é uma álgebra de Boole;*

(ii) para todo o morfismo $\varphi : A^+ \to B^+, L \in \mathcal{V}(B^+)$ *implica* $\varphi^{-1}(L) \in \mathcal{V}(A^+)$*;*

(iii) se $L \in \mathcal{V}(A^+)$ *e* $a \in A$*, então* $a^{-1}L, La^{-1} \in \mathcal{V}(A^+)$.

Seja **V** uma pseudovariedade e $\mathcal{V}$ a classe de linguagens reconhecíveis que associa a cada alfabeto A o conjunto $\mathcal{V}(A^+)$ das linguagens L de A^+ que são reconhecidas por um semigrupo de **V** (o que, pela Proposição 2.17, equivale a ter-se $S(L) \in \mathbf{V}$). Pode-se mostrar que, a classe $\mathcal{V}$ representa efectivamente uma variedade de linguagens. Para além disso, tem-se o seguinte resultado fundamental.

Teorema 3.7 *(Eilenberg, 1976) A correspondência* $\mathbf{V} \mapsto \mathcal{V}$ *define uma bijecção entre as pseudovariedades de semigrupos e as variedades de linguagens.*

Nos exemplos seguintes iremos descrever as variedades de linguagens associadas, pelo teorema de Eilenberg, a certas pseudovariedades.

Exemplos 3.8 *Seja A um alfabeto.*

- $\mathcal{N}(A^+)$ *é o conjunto das linguagens finitas ou cofinitas de* A^+.
- $\mathcal{S}l(A^*)$ *é a álgebra de Boole gerada pelas linguagens da forma* A^*aA^* *onde* a *é uma letra de* A.

Os exemplos seguintes resultam dos Teoremas 2.22, 2.27 e 2.30 (ver secção 2.6):

Exemplos 3.9 *Alguns exemplos da correspondência de Eilenberg:*

- $\mathbf{A} \longmapsto \{$*linguagens livres de estrela*$\}$
- $\mathbf{LSl} \longmapsto \{$*linguagens localmente testáveis*$\}$
- $\mathbf{J} \longmapsto \{$*linguagens testáveis aos pedaços*$\}$,

onde $\mathbf{A}$ *é a pseudovariedade dos semigrupos finitos aperiódicos e* $\mathbf{LSL}$ *é a pseudovariedade dos semigrupos finitos* S *tais que* eSe *é um semireticulado para todo o idempotente* e *de* S.

Capítulo 4

Operações Implícitas

A noção de operação implícita assume um papel fundamental no estudo da decidibilidade do problema da pertença. Após o estudo deste conceito vamos apresentar alguns exemplos de como decidir, quando dadas duas palavras, se elas são ou não iguais numa pseudovariedade.

4.1 Teorema de Reiterman

Vamos começar por definir o conceito de operação implícita.

Definição 4.1 *Sejam* $\mathbf{V}$ *uma pseudovariedade e* $A = \{a_1, \ldots, a_n\}$ *um alfabeto de cardinalidade* $n \in \mathbb{N}$. *Define-se uma operação ímplicita A-ária (ou n-ária) sobre* $\mathbf{V}$ *como sendo uma família* $\pi = (\pi_S)_{S \in \mathbf{V}}$ *em que*

- *para cada* $S \in \mathbf{V}$,

$$\begin{array}{rccc} \pi_S : & S^n & \to & S \\ & (s_1, \ldots s_n) & \mapsto & \pi_S(s_1, \ldots s_n) \end{array}$$

  é uma função;

- *para qualquer homomorfismo* $\varphi : S \to T$ *com* $S, T \in \mathbf{V}$, *o diagrama seguinte comuta, ou seja,* $\varphi \circ \pi_S = \pi_T \circ \varphi^n$

$$\begin{array}{ccc} S^n & \xrightarrow{\pi_S} & S \\ {\scriptstyle \varphi^n}\downarrow & & \downarrow{\scriptstyle \varphi} \\ T^n & \xrightarrow{\pi_T} & T \end{array}$$

O conjunto de todas as operações implícitas A-árias sobre $\mathbf{V}$ é representado por $\overline{\Omega}_A\mathbf{V}$ (ou $\overline{\Omega}_n\mathbf{V}$). As operações implícitas são também designadas pseudopalavras.

O conjunto $\overline{\Omega}_A\mathbf{V}$ munido da operação binária definida por:

$$\forall \pi, \theta \in \overline{\Omega}_A\mathbf{V}\ \forall S \in \mathbf{V} \quad \forall s_1, s_2, \ldots, s_n \in S$$

$$(\pi \cdot \theta)_S(s_1, \ldots, s_n) = \pi_S(s_1, \ldots, s_n) \cdot \theta_S(s_1, \ldots, s_n)$$

forma um semigrupo.

Vejamos alguns exemplos de operações implícitas sobre $\mathbf{V}$.

Exemplos 4.2 *1) Os exemplos mais simples são as operações explícitas que passamos a definir.*

Para cada $i \in \{1, \ldots, n\}$, a_i é uma operação implícita, a que chamamos de projecção sobre a i-ésima componente, e é definida para qualquer $S \in \mathbf{V}$ como sendo a aplicação

$$\begin{array}{rccc} (a_i)_S : & S^n & \to & S \\ & (s_1, \ldots, s_n) & \mapsto & s_i \end{array}$$

Vejamos que esta aplicação satisfaz a Definição 4.1.

- *A aplicação $(a_i)_S : S^n \to S$ tal que $(a_i)_S(s_1, \ldots, s_n) = s_i$ é trivialmente uma função.*
- *Seja $\varphi : S \to T$ um homomorfismo. Temos que:*

$$\varphi \circ (a_i)_S(s_1, \ldots, s_n) = \varphi(s_i)$$

e

$$(a_i)_T \circ \varphi^n(s_1, \ldots, s_n) = (a_i)_T(\varphi(s_1), \ldots, \varphi(s_n)) = \varphi(s_i).$$

Donde concluímos que $\varphi \circ \pi_S = \pi_T \circ \varphi^n$, para $\pi = a_i$.

Portanto, a_i é uma operação implícita.

O subsemigrupo de $\overline{\Omega}_A\mathbf{V}$ gerado pelo conjunto das projecções $A = \{a_1, \ldots, a_n\}$ denota-se por $\Omega_A\mathbf{V}$ (ou $\Omega_n\mathbf{V}$) e os seus elementos dizem-se operações explícitas A-árias (ou n-árias) sobre $\mathbf{V}$, também chamadas pseudopalavras finitas.

Note-se que as operações explícitas n-árias são operações implícitas n-árias induzidas pelas palavras de A^+. Por exemplo, considere-se $u = a_1a_3a_2a_1$. Para cada $S \in \mathbf{V}$, seja $u_S : S^n \to S$ tal que para cada $(s_1, \ldots, s_n) \in S^n$ tem-se

$$\begin{aligned} &u_S(s_1, \ldots, s_n) = \\ &= (a_1)_S(s_1, \ldots, s_n)(a_3)_S(s_1, \ldots, s_n)(a_2)_S(s_1, \ldots, s_n)(a_1)_S(s_1, \ldots, s_n) \quad = \\ &= s_1s_3s_2s_1. \end{aligned}$$

2) Suponhamos que $a \in A$. Para além das operações explícitas, uma outra operação implícita muito usual é a chamada potência-ω, denotada por a^ω. Recorde-se que para um semigrupo finito S e $s \in S$, existe um único idempotente da forma s^k, com $k \geq 1$, que se representa por s^ω.

A potência-ω é a operação implícita a^ω sobre $\mathbf{V}$ definida para cada $S \in \mathbf{V}$ e $s \in S$ por

$$\begin{array}{rccc} (a^\omega)_S : & S & \to & S \\ & s & \mapsto & s^\omega \end{array}$$

Verifiquemos que de facto $\varphi(s^\omega) = \varphi(s)^\omega$, para todo o $s \in S$ e para qualquer homomorfismo $\varphi : S \to T$.

Dado que s^ω é idempotente e φ é um homomorfismo, tem-se que

$$\varphi(s^\omega) = \varphi(s^\omega \cdot s^\omega) = \varphi(s^\omega) \cdot \varphi(s^\omega),$$

e por conseguinte $\varphi(s^\omega)$ é idempotente. Por outro lado, por definição de s^ω, existe $n \in \mathbb{N}$ tal que $s^\omega = s^n$. Assim, e tendo em consideração que φ é um homomorfismo obtém-se

$$\varphi(s^\omega) = \varphi(s^n) = \varphi(s)^n$$

Portanto, $\varphi(s)^n$ é idempotente, e consequentemente $\varphi(s^\omega) = \varphi(s)^\omega$.

A partir do alfabeto, usando um número finito de vezes a multiplicação e a potência-ω, obtêm-se novas operações implícitas, chamadas palavras-ω. O conjunto destas palavras-ω representa-se por $\Omega_A^\omega\mathbf{V}$.

Por exemplo, sendo $A = \{a, b, c\}$, a expressão $x = a(ba^\omega c(ab)^\omega)^\omega aba(aca)^\omega ba$ representa uma palavra-ω.

Note-se que, se $\pi = (\pi_S)_{S\in\mathbf{V}}$ é uma operação implícita sobre $\mathbf{V}$ e $\mathbf{W}$ é uma pseudovariedade contida em $\mathbf{V}$, então $(\pi_S)_{S\in\mathbf{W}}$ é uma operação implícita sobre $\mathbf{W}$ que denotaremos por $p_{\mathbf{V},\mathbf{W}}(\pi)$. A aplicação

$$\begin{array}{rccc} p_{\mathbf{V},\mathbf{W}}: & \overline{\Omega}_A\mathbf{V} & \to & \overline{\Omega}_A\mathbf{W} \\ & (\pi_S)_{S\in\mathbf{V}} & \mapsto & (\pi_S)_{S\in\mathbf{W}} \end{array}$$

será designada a *projecção natural* de $\overline{\Omega}_A\mathbf{V}$ sobre $\overline{\Omega}_A\mathbf{W}$. No caso de $\mathbf{V}$ ser a pseudovariedade $\mathbf{S}$, usaremos a notação simplificada $p_{\mathbf{W}}$ para designar $p_{\mathbf{S},\mathbf{W}}$.

Podemos agora estender a noção de identidade à noção de pseudoidentidade.

Chama-se *pseudoidentidade* a um par (π, ρ), com $\pi, \rho \in \overline{\Omega}_A\mathbf{V}$, que representamos habitualmente por $\pi = \rho$. Dizemos que um semigrupo $S \in \mathbf{V}$ verifica ou satisfaz uma *pseudoidentidade* $\pi = \rho$, com $\pi, \rho \in \overline{\Omega}_A\mathbf{V}$, e escrevemos $S \models \pi = \rho$, se $\pi_S = \rho_S$. Uma classe $\mathcal{C}$ de semigrupos finitos satisfaz um conjunto de pseudoidentidades Σ, e notamos $\mathcal{C} \models \Sigma$, se

$$\forall S \in \mathcal{C} \ \ \forall \pi = \rho \in \Sigma, \ S \models \pi = \rho.$$

Da mesma forma que para as identidades, se Σ é um conjunto de *pseudoidentidades* sobre $\mathbf{V}$, $[\![\Sigma]\!]$ denota a classe de todos os semigrupos finitos de $\mathbf{V}$ que verificam as *pseudoidentidades* de Σ. Prova-se que $[\![\Sigma]\!] = \{S \in \mathbf{V} : S \vDash \Sigma\}$ é uma pseudovariedade e dizemos que é definida por Σ.

Algumas das pseudovariedades já referidas anteriormente podem agora ser apresentadas de forma simplificada.

Vejamos alguns exemplos de pseudovariedades definidas por pseudoidentidades:

$$\begin{aligned} \mathbf{G} &= [\![a^\omega b = ba^\omega = b]\!] \\ \mathbf{N} &= [\![a^\omega b = ba^\omega = a^\omega]\!] \\ \mathbf{LI} &= [\![a^\omega ba^\omega = a^\omega]\!] \\ \mathbf{K} &= [\![a^\omega b = a^\omega]\!] \end{aligned}$$

$$\begin{aligned}
\mathbf{D} &= [\![ba^\omega = a^\omega]\!] \\
\mathbf{R} &= [\![(ab)^\omega = (ab)^\omega a]\!] \\
\mathbf{L} &= [\![(ab)^\omega = b(ab)^\omega]\!] \\
\mathbf{J} &= [\![(ab)^\omega a = (ab)^\omega = b(ab)^\omega]\!] \\
&= [\![(ab)^\omega = (ba)^\omega, a^\omega = a^{\omega+1}]\!] \\
\mathbf{A} &= [\![a^\omega = a^{\omega+1}]\!].
\end{aligned}$$

Teorema 4.3 (Reiterman) *Uma classe* $\mathbf{V}$ *de semigrupos finitos é uma pseudovariedade se e só se* $\mathbf{V} = [\![\Sigma]\!]$ *para algum conjunto* Σ *de pseudoidentidades.*

Consideremos uma pseudovariedade de semigrupos $\mathbf{V}$. A noção de conteúdo pode agora ser extendida aos elementos de $\overline{\Omega}_A\mathbf{V}$. Tal trabalho é devido a Azevedo [17].

Dizemos que $\pi \in \overline{\Omega}_A\mathbf{V}$ depende de a_i se:

$$\exists S \in \mathbf{V} \quad \exists s_1, \ldots, s_{i-1}, r, r', s_{i+1}, \ldots, s_n \in S :$$

$$\pi_S(s_1, \ldots, s_{i-1}, r, s_{i+1}, \ldots, s_n) \neq \pi_S(s_1, \ldots, s_{i-1}, r', s_{i+1}, \ldots, s_n),$$

ou seja, a função $\pi_S : S^n \longrightarrow S$ depende da i-ésima componente. O conjunto de todos os a_i dos quais π depende, designa-se o *conteúdo* de π e denota-se por $c(\pi)$.

Lema 4.4 (Azevedo [17]) *Sejam* $\mathbf{V}$ *uma pseudovariedade qualquer e* $\pi \in \overline{\Omega}_A\mathbf{V}$. *Se* $a_i \in c(\pi)$, *então existem* $\pi_1, \pi_2 \in (\overline{\Omega}_A\mathbf{V})^1$ *tais que* $\pi = \pi_1 a_i \pi_2$.

No caso de $\mathbf{V}$ ser uma pseudovariedade que contém $\mathbf{Sl}$ veremos mais tarde que a aplicação conteúdo, c, coincide com a projecção $p_{\mathbf{V},\mathbf{Sl}}$ de $\overline{\Omega}_A\mathbf{V}$ sobre $\overline{\Omega}_A\mathbf{Sl}$.

Em $\overline{\Omega}_A\mathbf{V}$ pode ser definida uma estrutura topológica que iremos de seguida resumir.

Para cada semigrupo $S \in \mathbf{V}$, existe uma aplicação natural

$$\begin{array}{rccc}
\alpha_S : & \overline{\Omega}_A\mathbf{V} & \to & S^{S^n} \\
& \pi & \mapsto & \pi_S
\end{array}$$

que induz uma aplicação injectiva

$$\begin{array}{rccc} \alpha_{\mathbf{V}}: & \overline{\Omega}_A\mathbf{V} & \to & \prod_{S\in\mathbf{V_0}} S^{S^n} \\ & \pi & \mapsto & (\pi_S)_S \end{array}$$

onde $\mathbf{V_0}$ é um conjunto numerável que contém um representante de cada classe de isomorfismo dos elementos de $\mathbf{V}$. Podemos então interpretar $\overline{\Omega}_A\mathbf{V}$ como um subsemigrupo de $\prod_{S\in\mathbf{V_0}} S^{S^n}$.

Consideremos agora os semigrupos finitos munidos da topologia discreta, o produto cartesiano $\prod_{S\in\mathbf{V_0}} S^{S^n}$ munido da topologia produto e $\overline{\Omega}_A\mathbf{V}$ como um subespaço topológico de $\prod_{S\in\mathbf{V_0}} S^{S^n}$ através da aplicação $\alpha_{\mathbf{V}}$.

Proposição 4.5 (Almeida [3]) *Com as definições acima, $\overline{\Omega}_A\mathbf{V}$ é um semigrupo topológico compacto no qual o subespaço $\Omega_A\mathbf{V}$ é denso.*

A topologia de $\overline{\Omega}_A\mathbf{V}$ pode ainda ser vista como a topologia induzida por uma distância d, que descrevemos de seguida.

Seja $r : \overline{\Omega}_A\mathbf{V} \times \overline{\Omega}_A\mathbf{V} \to \mathbb{N}_0 \cup \{+\infty\}$ uma aplicação definida por:

$$r(\pi,\rho) = min\{|S| \ : S \in \mathbf{V}, \quad \pi_S \neq \rho_S\}$$

onde, por convenção, tomamos $min\ \emptyset = +\infty$. Definimos agora uma distância d sobre $\overline{\Omega}_A\mathbf{V}$ fazendo

$$\begin{array}{rccc} d: & \overline{\Omega}_A\mathbf{V} \times \overline{\Omega}_A\mathbf{V} & \to & \mathbb{R}_0^+ \\ & (\pi,\rho) & \mapsto & \left\{ \begin{array}{cc} 2^{-r(\pi,\rho)} & \text{se } r(\pi,\rho) \text{ é finito} \\ 0 & \text{se } r(\pi,\rho) = +\infty \end{array} \right. \end{array}$$

Verifica-se ainda que esta aplicação d é mesmo uma ultramétrica.

Proposição 4.6 (Almeida [3]) *A topologia anteriormente definida sobre $\overline{\Omega}_A\mathbf{V}$ é induzida por d.*

Proposição 4.7 (Almeida [3]) *O espaço métrico $(\overline{\Omega}_A\mathbf{V}, d)$ é o completado do subespaço $(\Omega_A\mathbf{V}, d)$.*

Tendo em consideração o que foi exposto, note-se que uma sucessão $(\pi_n)_{n\in\mathbb{N}}$ de operações implícitas A-árias sobre $\mathbf{V}$ converge para $\pi \in \overline{\Omega}_A\mathbf{V}$ se e só se, para todo $S \in \mathbf{V}$, $\pi_S = (\pi_n)_S$ a partir de uma certa ordem, ou seja, se e só se a sucessão $(\pi_n)_{n\in\mathbb{N}}$ coincide ultimamente com π em cada $S \in \mathbf{V}$.

Exemplo 4.8 *O limite da sucessão de operações explícitas* $(a^{n!})_{n\in\mathbb{N}}$ *sobre* $\mathbf{V}$ *é a operação implícita* a^ω *sobre* $\mathbf{V}$*. De facto,*

$$a^\omega = \lim_{n\to\infty} a^{n!} \Leftrightarrow \forall S \in \mathbf{V} \quad \exists p \in \mathbb{N} \quad \forall n \geq p \quad S \models a^\omega = a^{n!}$$

Para cada $S \in \mathbf{V}$ *seja* $p = n_s$ *o expoente de* S*. Então* $S \models a^\omega = a^{n_s}$*. Ora* $S \models a^{n!} = a^{n_s}$ *para* $n \geq n_s$*. Portanto, tem-se que* $a^{n!} \longrightarrow a^\omega$*.*

Note-se que devido ao semigrupo topológico $\overline{\Omega}_A\mathbf{V}$ ser compacto se tem a seguinte propriedade útil.

Corolário 4.9 *Toda a sequência de elementos de* $\overline{\Omega}_A\mathbf{V}$ *admite alguma subsequência convergente.*

Exemplo 4.10 *Seja* $(u_n)_{n\in\mathbb{N}}$ *uma sequência de elementos de* $\overline{\Omega}_A\mathbf{V}$ *definida por:*

$$u_n = \begin{cases} ab & \text{se } n \text{ é ímpar} \\ ba & \text{se } n \text{ é par} \end{cases}$$

Temos que $(u_{2k})_{k\in\mathbb{N}} \longrightarrow ba$ *e* $(u_{2k-1})_{k\in\mathbb{N}} \longrightarrow ab$*.*

4.2 Exemplos de semigrupos da forma $\overline{\Omega}_A\mathbf{V}$

Fixemos um alfabeto com n elementos, $A = \{a_1, \ldots, a_n\}$. Os exemplos mais simples de semigrupos da forma $\overline{\Omega}_A\mathbf{V}$ são aqueles em que a pseudovariedade $\mathbf{V}$ é gerada por um conjunto finito de semigrupos, tal como refere o resultado seguinte [13].

Proposição 4.11 *Seja* $\mathbf{V}$ *uma pseudovariedade de semigrupos. Então as seguintes afirmações são equivalentes:*

1. $\mathbf{V}$ *é gerado por um conjunto finito de semigrupos;*
2. $\overline{\Omega}_A\mathbf{V} = \Omega_A\mathbf{V}$*;*
3. $\Omega_A\mathbf{V}$ *é finito.*

4.2.1 Pseudovariedade Sl

Comecemos por estudar a pseudovariedade **Sl** dos semi-reticulados. Recorde-se que

$$\mathbf{Sl} = [\![ab = ba; a^2 = a]\!].$$

Esta pseudovariedade é um dos casos onde a operação implícita a^ω é explícita. De facto,

$$\forall S \in \mathbf{Sl} \quad \forall s \in S \quad (a^\omega)_S(s) = s^\omega = s,$$

o que mostra que a^ω é a operação explícita a sobre **Sl**.

Como a pseudovariedade **Sl** é gerada pelo semi-reticulado $\mathcal{U}_1 = \{0, 1\}$ ([36]) em que 0 é um zero e 1 é a identidade, ela é, em particular, gerada por um conjunto finito de semigrupos. Portanto, pela Proposição 4.11, $\overline{\Omega}_A\mathbf{Sl} = \Omega_A\mathbf{Sl}$ e $\Omega_A\mathbf{Sl}$ é finito.

O resultado seguinte permite-nos decidir acerca da igualdade de duas quaisquer operações implícitas sobre **Sl**.

Proposição 4.12 *Sejam $\pi, \rho \in \overline{\Omega}_A\mathbf{S}$. Então $\mathbf{Sl} \vDash \pi = \rho$ se e só se $c(\pi) = c(\rho)$.*

Demonstração: Note-se que,

$$\mathbf{Sl} \vDash \pi = \rho \Leftrightarrow \forall S \in \mathbf{Sl}, \quad S \vDash \pi = \rho.$$

Comecemos por provar a implicação da esquerda para a direita. Suponhamos que existe $a_r \in A$ tal que a_r pertence ao conteúdo de π mas não pertence ao conteúdo de ρ.

Consideremos o semigrupo $\mathcal{U}_1$ de **Sl**. Considerando $s_1 = \ldots = s_{r-1} = 1$, $s_r = 0$, $s_{r+1} = \ldots = s_n = 1$, verifica-se que

$$\pi_{\mathcal{U}_1}(s_1, \ldots, s_n) = 0 \quad \text{e} \quad \rho_{\mathcal{U}_1}(s_1, \ldots, s_n) = 1,$$

e portanto, $\pi_{\mathcal{U}_1} \neq \rho_{\mathcal{U}_1}$ donde, $\mathbf{Sl} \nvDash \pi = \rho$.

Para provar a implicação contrária suponhamos que π e ρ têm o mesmo conteúdo. Usando a identidade $ab = ba$ e o facto de π e ρ coincidirem com operações explícitas sobre **Sl** obtém-se que

$$\mathbf{Sl} \vDash \pi = a_1{}^{i_1} a_2{}^{i_2} \ldots a_n{}^{i_n} \quad \text{e} \quad \mathbf{Sl} \vDash \rho = a_1{}^{j_1} a_2{}^{j_2} \ldots a_n{}^{j_n}$$

para alguns $i_p, j_p \in \mathbb{N}_0$ tais que $i_p = 0$ se e só se $j_p = 0$.

Finalmente, através da identidade $a^2 = a$ deduz-se

$\mathbf{Sl} \vDash \pi = {a_1}^{k_1}{a_2}^{k_2} \dots {a_n}^{k_n} = \rho$ onde $k_r \in \{0, 1\}$. Portanto, $\mathbf{Sl} \vDash \pi = \rho$. □

A proposição anterior prova que o semigrupo $\overline{\Omega}_A\mathbf{Sl}$ é isomorfo ao semigrupo $(\mathcal{P}(A), \cup)$.

O seguinte resultado permite-nos verificar que a função conteúdo é particularmente bem comportada para toda a pseudovariedade contendo **Sl**.

Proposição 4.13 (Azevedo [18]) *Seja* $\mathbf{V}$ *uma pseudovariedade contendo* **Sl**. *Então, a função*

$$c : \ \overline{\Omega}_A\mathbf{V} \ \longrightarrow \ \overline{\Omega}_A\mathbf{Sl}$$

é o único homomorfismo contínuo tal que $c(a_i) = \{a_i\}$ *para* $i = 1, \dots, n$. *Ou seja,* c *é a projecção canónica de* $\overline{\Omega}_A\mathbf{V}$ *sobre* $\overline{\Omega}_A\mathbf{Sl}$.

Exemplo 4.14 *Consideremos uma pseudovariedade* $\mathbf{V}$ *tal que* $\mathbf{Sl} \subseteq \mathbf{V}$. *Seja* $A = \{a, b, c, d\}$. *Sejam* $\pi, \rho \in \Omega_A^\omega\mathbf{S}$, *tais que:*

- $\pi = (ab^\omega)^\omega ca$
- $\rho = abb^\omega(ad^\omega)^{\omega+1}$

Note-se que as operações implícitas π *e* ρ *não têm o mesmo conteúdo, uma vez que* $c(\pi) = \{a, b, c\}$ *e* $c(\rho) = \{a, b, d\}$. *Portanto, pela proposição 4.12, as palavras-*ω π *e* ρ *representam sobre* **Sl** *diferentes palavras.*

Logo, a pseudovariedade **Sl** *não satisfaz a igualdade entre* π *e* ρ.

4.2.2 Pseudovariedade N

Consideremos a pseudovariedade dos semigrupos nilpotentes $\mathbf{N} = [\![a^\omega = 0]\!]$.

Comecemos por mostrar que

$$\mathbf{N} = \bigcup_{r \geq 1} [\![a_1 \cdots a_r = 0]\!].$$

Consideremos $\mathbf{N}_r = [\![a_1 \cdots a_r = 0]\!]$. Pretendemos mostrar que $\mathbf{N} = \bigcup_{r \in \mathbb{N}} \mathbf{N}_r$.

Comecemos por mostrar que $\mathbf{N}_r \subseteq \mathbf{N}$, para todo $r \geq 1$.

Seja $r \in \mathbb{N}$. Como $\mathbf{N}_r \vDash a_1 \cdots a_r = 0$, em particular, substituindo cada a_i, $i \in 1, \ldots, r$, por a^ω resulta que $\mathbf{N}_r \vDash a^\omega \cdots a^\omega = 0$. Como a^ω é idempotente vem que $\mathbf{N}_r \vDash a^\omega = 0$. Portanto, $\mathbf{N}_r \subseteq \mathbf{N}$ para todo $r \in \mathbb{N}$.

Vamos agora mostrar que $\mathbf{N} \subseteq \bigcup_{r\geq 1} \mathbf{N}_r$. Seja $S \in \mathbf{N}$. Queremos mostrar que S satisfaz a igualdade $a_1 \cdots a_r = 0$, para algum $r \in \mathbb{N}$. Sejam $s_1, \ldots, s_r \in S$, com $r \geq |S|$. Então pela Proposição 1.14 tem-se

$$S^r = SE(S)S,$$

e, portanto, existem $x, z \in S$ e $y = y^\omega \in E(S)$ tais que

$$s_1 \cdots s_r = xy^\omega z.$$

Dado que $S \in \mathbf{N}$ e $\mathbf{N} \vDash a^\omega = 0$, também, $S \vDash a^\omega = 0$. Consequentemente, em S tem-se que $s_1 \cdots s_r = x.0.z = 0$. Assim, para todo o $S \in \mathbf{N}$, $S \vDash a_1 \cdots a_r = 0$ para algum $r \geqslant 1$. E, portanto, conclui-se que $S \in \mathbf{N}_r$.

Conclui-se assim que $\mathbf{N} = \bigcup_{\mathbf{r}\in\mathbb{N}} \mathbf{N_r}$.

Para cada $r \in \mathbb{N}$, seja $I_r = A^{\geq r}$ o ideal de A^+ constituído por todas as palavras de comprimento superior ou igual a r. Consideremos ainda o quociente de Rees A^+/I_r, em que os elementos do ideal I_r são identificados com um só ponto (o qual é um zero). Verifica-se portanto que o conjunto S_r, constituído por todas as palavras sobre A de comprimento inferior a r e por um zero,

$$S_r = \{u \in A^+ : |u| < r\} \cup \{0\},$$

munido do produto definido para todos os $u, v \in S_r \backslash \{0\}$ por

$$u \cdot v = \begin{cases} uv & \text{se } |uv| < r \\ 0 & \text{caso contrário} \end{cases}$$

e

$$u \cdot 0 = 0 = 0 \cdot u$$

é um semigrupo isomorfo ao quociente de Rees referido.

Em particular, o semigrupo S_r pertence a $\mathbf{N}$, pois $S_r \vDash a_1 \cdots a_r = 0$. Verifiquemos que qualquer identidade válida em S_r é consequência desta.

Suponhamos que $u = v$ é uma identidade sobre S tal que $S_r \vDash u = v$.

1) Se $|u| < r$, então $|v| < r$, pois, caso contrário, como $S_r \vDash a_1 \cdots a_r = 0$, v seria identificada com o elemento 0 e consequentemente, teriamos $S_r \nvDash u = v$. Para além disso $u = v$, ou seja, u e v são a mesma palavra.

2) Suponhamos agora que $|u| \geqslant r$. Então $|v| \geqslant r$. Se $u = a_1 \cdots a_s$ e $v = b_1 \cdots b_t$ com $s, t \geq r$, tem-se

$$S_r \vDash a_1 \cdots a_r a_{r+1} \cdots a_s = 0 \cdot a_{r+1} \cdots a_s = 0 = 0 \cdot b_{r+1} \cdots b_t = b_1 \cdots b_r b_{r+1} \cdots b_t$$

Verificou-se assim que, a identidade $u = v$ em S_r é obtida a partir da identidade $a_1 \cdots a_r = 0$.

Logo, $S_r \simeq \Omega_A[\![a_1 \ldots a_r = 0]\!]$. Os semigrupos S_r $(r \geqslant 1)$ formam um conjunto gerador da pseudovariedade $\mathbf{N}$ nos quais podemos testar a validade de possíveis propriedades de $\mathbf{N}$. Neste contexto, estes semigrupos são designados como *semigrupos-teste*.

Proposição 4.15 *A pseudovariedade* $\mathbf{N}$ *só satisfaz identidades triviais.*

Desta proposição resulta que $\Omega_A\mathbf{N} \simeq \mathbf{A}^+$, ou seja, cada operação explícita sobre $\mathbf{N}$ escreve-se de modo único à custa dos elementos $a_1, \ldots, a_n$. De um modo geral, caso se verifique que uma dada pseudovariedade $\mathbf{V}$ contém a pseudovariedade $\mathbf{N}$, então as operações explícitas podem ser caracterizadas através do seguinte corolário:

Corolário 4.16 *Se* $\mathbf{V}$ *é uma pseudovariedade de semigrupos tal que* $\mathbf{N} \subseteq \mathbf{V}$, *então* $\Omega_A\mathbf{V} = \mathbf{A}^+$.

Vejamos agora o que se passa com as pseudopalavras infinitas. Consideremos $(w_n)_n$ uma sucessão em $\Omega_A\mathbf{N}$ tal que $(w_n)_n$ converge em $\overline{\Omega}_A\mathbf{N}$, digamos para $\pi \in \overline{\Omega}_A\mathbf{N}$. Ora,

$$\begin{aligned} \lim w_n = \pi \quad &\Leftrightarrow \lim(w_n)_S = \pi_S, \ \forall S \in \mathbf{N} \\ &\Leftrightarrow \lim(w_n)_{S_r} = \pi_{S_r}, \ \forall r \in \mathbb{N} \end{aligned}$$

pois como já referimos, os semigrupos S_r formam um conjunto gerador da pseudovariedade $\mathbf{N}$. Temos então uma das seguintes situações:

1) $|w_n| \nrightarrow \infty$, ou seja, $\exists p \in \mathbb{N} : \forall n \in \mathbb{N}\ |w_n| \leq p$. Dado que, para $r > p$, $(w_n)_n$ converge em S_r, deduz-se que w_n é ultimamente constante, digamos igual a u. Então $(w_n)_n$ converge em $\overline{\Omega}_A\mathbf{N}$ para $u \in A^+$.

2) $|w_n| \to \infty$, ou seja, $\forall r \in \mathbb{N}, |w_n| \geq r$ a partir de uma certa ordem, que depende de r. Então $w_n = 0$ em S_r a partir dessa ordem, o que mostra que $(w_n)_n$ converge para 0 em cada S_r. Conclui-se assim que π é um zero de $\overline{\Omega}_A\mathbf{N}$, que notamos por 0.

Portanto $\overline{\Omega}_A\mathbf{N} = \Omega_A\mathbf{N} \cup \{0\}$, ou seja, $\overline{\Omega}_A\mathbf{N}$ é obtido de $\Omega_A\mathbf{N}$ acrescentando um "ponto no infinito" o qual é um zero. O produto em $\overline{\Omega}_A\mathbf{N}$ é dado para todos os $u, v \in A^+$ por:

$$u \cdot v = uv$$

$$u \cdot 0 = 0 = 0 \cdot u.$$

No exemplo que se segue trata-se o problema da palavra sobre a pseudovariedade $\mathbf{N}$. Consideremos o exemplo abaixo mencionado com o objectivo de verificar que existem alterações na satisfação de pseudoidentidades quando se consideram pseudovariedades distintas.

Exemplo 4.17 *Consideremos as seguintes operações implícitas* $\pi, \rho, \tau, \beta \in \Omega^\omega\mathbf{S}$*:*

- $\pi = (ab^\omega)^\omega ca$
- $\rho = abb^\omega(ad^\omega)^{\omega+1}$
- $\tau = bc^2ab^3ac$
- $\delta = ab^2c^3b$

A projecção de cada uma das operações implícitas sobre o semigrupo $\Omega_A^\omega\mathbf{N}$ *é a seguinte:*

- $p_\mathbf{N}(\pi) = 0$
- $p_\mathbf{N}(\rho) = 0$
- $p_\mathbf{N}(\tau) = bc^2ab^3ac$

- $p_{\mathbf{N}}(\delta) = ab^2c^3b$

Dado que as pseudopalavras π e ρ são operações não explícitas, são identificadas sobre $\mathbf{N}$ com o elemento 0. Logo, $\mathbf{N} \vDash \pi = \rho$. Apesar das palavras δ e τ serem ambas explícitas, ou seja, δ e τ estão em A^+, elas não representam a mesma palavra de A^+, portanto são distintas sobre a pseudovariedade $\mathbf{N}$. Logo, $\mathbf{N} \nvDash \delta = \tau$. Note-se ainda que, dadas duas pseudopalavras γ e η de $\overline{\Omega}_A\mathbf{S}$, se γ é explícita e η não, então na pseudovariedade $\mathbf{N}$ a igualdade entre γ e η nunca é satisfeita.

4.2.3 Pseudovariedade K

Consideremos a pseudovariedade $\mathbf{K}$ dos semigrupos nos quais os idempotentes são zeros à esquerda, $\mathbf{K} = [\![a^\omega b = a^\omega]\!]$. Verifiquemos que podemos escrevê-la como:

$$\mathbf{K} = \bigcup_{r\geq 1} [\![a_1 \cdots a_r b = a_1 \cdots a_r]\!].$$

Consideremos $\mathbf{K}_r = [\![a_1 \cdots a_r b = a_1 \cdots a_r]\!]$. Vamos mostrar que $\mathbf{K} = \bigcup_{r\geq 1} \mathbf{K}_r$.

Comecemos por mostrar que $\mathbf{K}_r \subseteq \mathbf{K}\ \forall r \geq 1$.

Seja $r \in \mathbb{N}$. Como $\mathbf{K}_r \vDash a_1 \cdots a_r b = a_1 \cdots a_r$ em particular substituindo cada $a_i,\ i \in \{1, \ldots, r\}$ por a^ω, tem-se que $\mathbf{K}_r \vDash a^\omega \cdots a^\omega b = a^\omega \cdots a^\omega$. Dado que a^ω é idempotente, conclui-se que $\mathbf{K}_r \vDash a^\omega b = a^\omega$. Portanto, para todo o r, tem-se $\mathbf{K}_r \subseteq \mathbf{K}$.

Vamos agora mostrar que $\mathbf{K}_r \subseteq \mathbf{K}$ para algum $r \in \mathbb{N}$.

Sejam $S \in \mathbf{K}$ e $s_1, \ldots, s_r, t \in S$ com $r \geq |S|$. Então pela Proposição 1.14 existem $x, z \in S$ e $y = y^\omega \in E(S)$ tais que

$$s_1 \cdots s_r = xy^\omega z$$

donde

$$s_1 \cdots s_r t = xy^\omega zt.$$

Uma vez que y^ω é idempotente de S e $S \in \mathbf{K}$, então y^ω é um zero à esquerda. Consequentemente, $xy^\omega z = xy^\omega = xy^\omega zt$. Portanto, tem-se $s_1 \cdots s_r t = s_1 \cdots s_r$. Donde, para todo o $S \in \mathbf{K}$, $S \vDash a_1 \cdots a_r b = a_1 \cdots a_r$, para algum $r \in \mathbb{N}$.

Conclui-se assim que $\mathbf{K} = \bigcup_{r\in\mathbb{N}} \mathbf{K}_r$.

Como $\mathbf{N} \subseteq \mathbf{K}$, deduz-se do Corolario 4.16 que $\Omega_A\mathbf{K} = \mathbf{A}^+$.

Para cada $r \in \mathbb{N}$ consideremos o semigrupo

$$\Omega_A[\![a_1 \dots a_r b = a_1 \dots a_r]\!].$$

De forma análoga ao caso de $\mathbf{N}$, prova-se que $S_r \cong \Omega_A[\![a_1 \dots a_r b = a_1 \dots a_r]\!]$ onde S_r é o conjunto formado por todas as palavras sobre A de comprimento inferior ou igual a r, e onde o produto é dado para todos os $u, v \in S_r$ por

$$u \cdot v = \begin{cases} uv & \text{se } |uv| \leq r \\ p_r(uv) & \text{se } |uv| > r. \end{cases}$$

Os semigrupos S_r formam um conjunto gerador da pseudovariedade $\mathbf{K}$.

Vamos agora mostrar que uma sucessão $(w_n)_n$ de A^+ converge em $\overline{\Omega}_A\mathbf{K}$ se e só se é ultimamente constante, ou $|w_n| \longrightarrow \infty$ e

$$\forall r \in \mathbb{N}\ \exists n_r \in \mathbb{N},\ i, j \geq n_r \Rightarrow w_i \text{ e } w_j \text{ têm o mesmo prefixo de comprimento } r.$$

Seja $(w_n)_n$ uma sucessão de $\Omega_A\mathbf{K}$ e suponhamos que $(w_n)_n$ converge em $\overline{\Omega}_A\mathbf{K}$, digamos para $\pi \in \overline{\Omega}_A\mathbf{K}$. Uma vez que os semigrupos S_r formam um conjunto gerador da pseudovariedade $\mathbf{K}$, $(w_n)_n$ converge em cada S_r e, portanto, ou $w_n = u$ para algum $u \in A^+$ e para todo o n suficientemente grande, ou $|w_n| \longrightarrow \infty$ e $p_r(w_n)$ é constante para todo o n suficientemente grande. Conclui-se assim que, ou $\pi = u$ é explícita, ou π não é explícita e é um zero à esquerda em cada S_r e portanto π é um zero à esquerda. No caso de π não ser explícita conclui-se ainda o seguinte.

Corolário 4.18 *Se $\pi \in \overline{\Omega}_A\mathbf{K} \backslash \Omega_A\mathbf{K}$, então π pode ser identificada com a palavra infinita à direita*

$$a_1 a_2 a_3 \dots \in A^{\mathbb{N}}$$

em que a_i é a i-ésima letra de π, isto é, se $(w_n)_n$ é uma sucessão de operações explícitas a convergir para π, então a_i é a i-ésima letra de todos os termos de w_n a partir de uma certa ordem.

Deste corolário conclui-se que $\overline{\Omega}_A\mathbf{K} = A^+ \cup A^{\mathbb{N}}$, ou seja, o semigrupo das operações implícitas sobre $\mathbf{K}$ é formado pelas palavras de A^+ e pelas palavras infinitas à direita sobre A.

O produto em $\overline{\Omega}_A\mathbf{K}$ define-se, para todos os $u, v \in A^+$ e todos os $w, z \in A^{\mathbb{N}}$, por

$$\begin{aligned} u \cdot v &= uv; \\ u \cdot w &= uw; \\ w \cdot u &= w = w \cdot z. \end{aligned}$$

O semigrupo $\Omega_A^\omega\mathbf{K}$ é formado pelas palavras finitas e pelas palavras infinitas à direita ultimamente periódicas.

Vejamos o exemplo seguinte que nos permite ilustrar tal facto.

Exemplo 4.19 *Consideremos as seguintes operações implícitas* $\pi, \rho, \beta, \tau, \delta \in \Omega_A^\omega\mathbf{S}$*:*

- $\pi = (ab)^\omega ca$
- $\rho = abb^\omega(ad)^{\omega+1}$
- $\beta = ((ab)^\omega bc^\omega)^\omega(da)^\omega d$
- $\tau = bc^2ab^3ac$
- $\delta = ab^2c^3b$

A projecção de cada uma das operações implícitas sobre o semigrupo $\Omega_A^\omega\mathbf{K}$ *é dada, respectivamente, por:*

- $p_\mathbf{K}(\pi) = (ab)^{+\infty}$
- $p_\mathbf{K}(\rho) = ab^{+\infty}$
- $p_\mathbf{K}(\beta) = (ab)^{+\infty}$
- $p_\mathbf{K}(\tau) = bc^2ab^3ac$
- $p_\mathbf{K}(\delta) = ab^2c^3b$

Analisando as projecções verifica-se que as pseudopalavras π e β representam a mesma palavra sobre $\mathbf{K}$. No entanto, $\mathbf{K} \not\models \pi = \rho$, pois $(ab)^{+\infty}$ e $ab^{+\infty}$ são palavras infinitas à direita distintas. As palavras τ e δ são explícitas e como não representam a mesma palavra finita são distintas sobre $\mathbf{K}$. Logo, $\mathbf{K} \not\models \tau = \delta$.

4.2.4 Pseudovariedade D

O estudo das operações implícitas sobre a pseudovariedade $\mathbf{D} = [\![ba^\omega = a^\omega]\!]$ é feito de forma dual à pseudovariedade anterior, uma vez que se trata da pseudovariedade dos semigrupos cujos idempotentes são zeros à direita. Deste modo, para a pseudovariedade $\mathbf{D}$ tem-se que o semigrupo $\overline{\Omega}_A\mathbf{D}$ é formado por palavras de A^+ e palavras infinitas à esquerda sobre A. O produto em $\overline{\Omega}_A\mathbf{D}$ define-se, para todos os $u, v \in A^+$ e todos os $w, z \in A^{-\mathbb{N}}$, por

$$\begin{aligned} u \cdot v &= uv; \\ w \cdot u &= wu; \\ u \cdot w &= w = z \cdot w; \end{aligned}$$

O semigrupo $\Omega_A^\omega\mathbf{D}$ é formado pelas palavras de A^+ e pelas palavras infinitas à esquerda sobre A ultimamente periódicas. Passemos agora à análise do exemplo onde é tratado o problema da palavra, agora sobre a pseudovariedade $\mathbf{D}$.

Exemplo 4.20 *Consideremos as palavras $\pi, \rho, \beta, \delta, \tau \in \Omega_A^\omega\mathbf{S}$ definidas no Exemplo 4.19. A projecção de cada uma delas sobre o semigrupo $\Omega_A^\omega\mathbf{D}$ é dada respectivamente por:*

- $p_{\mathbf{D}}(\pi) = (ab)^{-\infty}ca$
- $p_{\mathbf{D}}(\rho) = (ad)^{-\infty}$
- $p_{\mathbf{D}}(\beta) = (ad)^{-\infty}$
- $p_{\mathbf{D}}(\tau) = bc^2ab^3ac$
- $p_{\mathbf{D}}(\delta) = ab^2c^3b$

Verifica-se que as pseudopalavras β e ρ representam sobre $\mathbf{D}$ a mesma palavra. Como $(ab)^{-\infty}ca$ e $(ad)^{-\infty}$ são palavras infinitas à esquerda distintas, então $\mathbf{D} \not\models \pi = \beta$. Para as palavras τ e δ o tratamento é idêntico ao realizado para a pseudovariedade $\mathbf{K}$. Portanto, $\mathbf{D} \not\models \tau = \delta$.

4.2.5 Pseudovariedade LI

Analisemos agora a pseudovariedade $\mathbf{LI} = [\![a^\omega b a^\omega = a^\omega]\!]$ dos semigrupos localmente triviais, também dada por

$$\mathbf{LI} = \bigcup_{r\geq 1} [\![a_1 \cdots a_r b c_1 \cdots c_r = a_1 \cdots a_r c_1 \cdots c_r]\!].$$

Como $\mathbf{N} \subseteq \mathbf{LI}$, deduz-se do Corolário 4.16 que $\Omega_A\mathbf{LI} = A^+$.

Prova-se que uma sucessão $(w_n)_n$ de $\Omega_A\mathbf{LI}$ converge em $\overline{\Omega}_A\mathbf{LI}$ se e só se é ultimamente constante, ou $|w_n| \longrightarrow \infty$ e

$$\forall r \in \mathbb{N}\ \exists t_r \in \mathbb{N} \quad i,j \geq t_r \ \Rightarrow\ w_i \text{ e } w_j \text{ têm o mesmo prefixo e sufixo de comprimento } r.$$

Então, as operações implícitas não explícitas sobre **LI** podem ser identificadas com o conjunto $\{(w,w') : w \in A^{\mathbb{N}}, w' \in A^{-\mathbb{N}}\}$, ou seja, $\overline{\Omega}_A\mathbf{LI} = \mathbf{A}^+ \cup (\mathbf{A}^{\mathbb{N}} \times \mathbf{A}^{-\mathbb{N}})$. O produto em $\overline{\Omega}_A\mathbf{LI}$ é dado, para todos os $u, v \in A^+$ e todos os (w,z), $(w',z') \in A^{\mathbb{N}} \times A^{-\mathbb{N}}$, por

$$\begin{aligned} u \cdot v &= uv; \\ u \cdot (w,z) &= (uw,z); \\ (w,z) \cdot u &= (w,zu); \\ (w,z) \cdot (w',z') &= (w,z'). \end{aligned}$$

Note-se que $\mathbf{K} \cap \mathbf{D} = \mathbf{N}$ e $\mathbf{K} \vee \mathbf{D} = \mathbf{LI}$. A segunda igualdade é uma consequência imediata do estudo das operações implícitas sobre **K**, **D** e **LI** e do resultado seguinte, que resulta do Teorema de Reiterman.

Proposição 4.21 *Sejam* $\mathbf{V}$ *e* $\mathbf{W}$ *duas pseudovariedades e sejam* $\pi, \rho \in \overline{\Omega}_A\mathbf{S}$ *duas operações implícitas. Então*

$$\mathbf{V} \vee \mathbf{W} \vDash \pi = \rho \quad \textit{se e só se} \quad \mathbf{V}, \mathbf{W} \vDash \pi = \rho.$$

Demonstração: Se $\mathbf{V} \vee \mathbf{W}$ satisfaz a pseudoidentidade $\pi = \rho$, então é imediato que $\mathbf{V}$ e $\mathbf{W}$ também a satisfazem.

Reciprocamente, suponhamos que $\mathbf{V}$ e $\mathbf{W}$ satisfazem a pseudoidentidade $\pi = \rho$. Suponhamos ainda que $\mathbf{V} \vee \mathbf{W} \nvDash \pi = \rho$.

Pelo Teorema de Reiterman sabemos que $\mathbf{V} \vee \mathbf{W} = [\![\mathbf{\Sigma}]\!]$ onde Σ é uma base de pseudoidentidades. Então $\pi = \rho \notin \Sigma$. Logo existe uma pseudovariedade $\mathbf{Z}$ tal que $\mathbf{Z} = [\![\Sigma \cup \{\pi = \rho\}]\!] \subsetneqq \mathbf{V} \vee \mathbf{W}$.

Dado que $\mathbf{V}, \mathbf{W} \subseteq \mathbf{Z}$ pois $\mathbf{V} \vDash \pi = \rho$ e $\mathbf{W} \vDash \pi = \rho$, isto é absurdo pois por definição de supremo, $\mathbf{V} \vee \mathbf{W}$ é a menor pseudovariedade que contém $\mathbf{V}$ e $\mathbf{W}$. □

Portanto, o estudo do problema da palavra sobre **LI** está interligado ao estudo sobre **K** e **D**. Aplicando directamente a proposição anterior e tendo em conta o que já foi escrito sobre as pseudovariedades **K** e **D**, podemos concluir em particular que a igualdade entre duas quaisquer palavras-ω só se verifica se as projecções de cada uma delas sobre o semigrupo $\Omega_A^\omega\mathbf{K}$ e sobre o semigrupo $\Omega_A^\omega\mathbf{D}$ forem iguais.

Exemplo 4.22 *Considerem-se as seguintes palavras* $\pi, \rho \in \Omega_A^\omega\mathbf{S}$.

- $\pi = abb^\omega(ad)^{\omega+1}$
- $\rho = ((ab^\omega)^\omega bc^\omega)^\omega(da)^\omega d$

A projecção de uma pseudopalavra não explícita sobre o semigrupo $\Omega_A^\omega\mathbf{LI}$ *é o par constituído pelas projecções dessa mesma operação sobre os semigrupos* $\Omega_A^\omega\mathbf{K}$ *e* $\Omega_A^\omega\mathbf{D}$, *respectivamente. Portanto,*

- $p_{\mathbf{LI}}(\pi) = (ab^{+\infty}, (ad)^{-\infty})$
- $p_{\mathbf{LI}}(\rho) = (ab^{+\infty}, (ad)^{-\infty})$

Deste modo verifica-se que $\mathbf{K} \vDash \pi = \rho$ e também $\mathbf{D} \vDash \pi = \rho$. Pelo que foi dito anteriormente, como $p_{\mathbf{LI}}(\pi)$ e $p_{\mathbf{LI}}(\rho)$ coincidem, conclui-se que, $\mathbf{LI} \vDash \pi = \rho$.

4.2.6 Pseudovariedade DS

Com o objectivo de estudar as operações implícitas sobre a pseudovariedade **J** será necessário em primeiro lugar estudar algumas propriedades das operações implícitas sobre a pseudovariedade **DS**.

Esta pseudovariedade está definida por $\mathbf{DS} = [\![[(ab)^\omega(ba)^\omega(ab)^\omega]^\omega = (ab)^\omega]\!]$.

Note-se que $\mathbf{Sl} \subseteq \mathbf{J} \subseteq \mathbf{DS}$. Logo as pseudovariedades **J** e **DS** verificam a condição da Proposição 4.13.

Vejamos que esta pseudovariedade pode ser caracterizada em termos de propriedades das relações de Green dos seus membros.

Proposição 4.23 *Seja S um semigrupo finito. São equivalentes as condições seguintes.*

1. $S \in \mathbf{DS}$;
2. *as $\mathcal{D}$-classes regulares de S são subsemigrupos;*
3. *cada $\mathcal{H}$-classe regular de S é um grupo;*
4. *se $r, s \in S$ são tais que $r \leq_{\mathcal{J}} s$ e r é regular, então $rs \mathcal{J} sr \mathcal{J} r$;*
5. *para cada idempotente $e \in S$, o conjunto dos elementos de S que estão $\mathcal{J}$ acima de e, isto é, $\{s \in S | \ e \leq_{\mathcal{J}} s\}$, é um subsemigrupo de S.*

Corolário 4.24 *Seja $\mathbf{V}$ uma subpseudovariedade de $\mathbf{DS}$. Se $\pi, \rho \in \overline{\Omega}_A\mathbf{V}$ são tais que $\pi \leq_{\mathcal{J}} \rho$ e π é regular, então $\pi\rho \mathcal{J} \rho\pi \mathcal{J} \pi$.*

O resultado seguinte é de particular interesse para o estudo a que nos propomos, as operações implícitas sobre $\mathbf{J}$. Caracteriza as $\mathcal{J}$-classes regulares de $\overline{\Omega}_A\mathbf{V}$, quando $\mathbf{V}$ é uma subpseudovariedade de $\mathbf{DS}$ que contém $\mathbf{Sl}$.

Proposição 4.25 *Seja $\mathbf{V}$ uma subpseudovariedade de $\mathbf{DS}$ que contém $\mathbf{Sl}$ e sejam π e ρ elementos regulares de $\overline{\Omega}_A\mathbf{V}$. Então*

$$\pi \leq_{\mathcal{J}} \rho \Leftrightarrow c(\rho) \subseteq c(\pi).$$

Além disso $\mathbf{DS}$ é a maior pseudovariedade com esta propriedade.

Note-se que se $\mathbf{V} \subseteq \mathbf{DS}$, mas $\mathbf{Sl} \nsubseteq \mathbf{V}$, então $\mathbf{V}$ pode falhar esta propriedade. Por exemplo, $\overline{\Omega}_A\mathbf{G}$ consiste numa única $\mathcal{J}$-classe (uma vez que é um grupo) mas $c(x_1) = \{x_1\}$ e $c(x_1^\omega) = \emptyset$.

Como consequência desta última proposição temos o seguinte resultado.

Corolário 4.26 *Seja $\mathbf{V}$ uma subpseudovariedade de $\mathbf{DS}$ contendo $\mathbf{Sl}$ e sejam π e ρ elementos de $\overline{\Omega}_A\mathbf{V}$. Se π é regular e $c(\rho) \subseteq c(\pi)$, então $\pi\rho$ (resp. $\rho\pi$) é regular e $\pi \mathcal{R} \pi\rho$ (resp. $\pi \mathcal{L} \rho\pi$).*

Para o que se segue torna-se necessário primeiramente introduzir algumas noções.

Sejam $w, u \in A^+$. Seja $u = a_{i_1} \cdots a_{i_k}$. Dizemos que u é uma subpalavra de w se existe uma factorização de w da forma $w = w_0 a_{i_1} w_1 \cdots a_{i_k} w_k$ com $w_0, \ldots, w_k \in A^*$. Denotaremos por $\left[\begin{array}{c} w \\ u \end{array} \right]$ o máximo dos inteiros r tais que u^r é uma subpalavra de w.

Por exemplo, $\left[\begin{array}{c} baccac \\ c \end{array} \right] = 3$, $\left[\begin{array}{c} bacbabc \\ bc \end{array} \right] = 2$ e $\left[\begin{array}{c} bacbabc \\ cb \end{array} \right] = 1$.

Sejam $u \in A^+$ e $\mathbf{V}$ uma pseudovariedade que contém $\mathbf{J}$. Então a definição anterior pode ser generalizada a todos os elementos $\pi \in \overline{\Omega}_A \mathbf{V}$.

Proposição 4.27 (Almeida [3]) *Seja $\mathbf{V}$ uma pseudovariedade contendo $\mathbf{J}$. Para cada alfabeto A e cada $u \in A^+$, a função*

$$\begin{array}{ccc} A^+ & \longrightarrow & \mathbb{N}_0 \\ w & \mapsto & \left[\begin{array}{c} w \\ u \end{array} \right] \end{array}$$

é uniformemente contínua para a topologia induzida pela distância d e portanto prolonga-se de forma única a uma função contínua

$$\begin{array}{ccc} \overline{\Omega}_A \mathbf{V} & \longrightarrow & \mathbb{N}_0 \cup \{\infty\} \\ \pi & \mapsto & \left[\begin{array}{c} \pi \\ u \end{array} \right] \end{array}$$

onde $\mathbb{N}_0 \cup \{\infty\}$ está munido da topologia do compactificado com um ponto do espaço discreto $\mathbb{N}_0$.

Enquanto que o conteúdo serve para separar as $\mathcal{J}$-classes regulares dos semigrupos $\overline{\Omega}_A \mathbf{V}$, com $\mathbf{V}$ no intervalo $[\mathbf{J}, \mathbf{DS}]$, os parâmetros $\left[\begin{array}{c} - \\ u \end{array} \right]$ podem ser utilizados para identificar os elementos regulares.

Lema 4.28 (Almeida [3]) *Sejam $S \in \mathbf{DS}$ e $w \in A^+$, com $c(w) = \{x_{i_1}, \ldots, x_{i_k}\}$ e seja $u = x_{i_1} \cdots x_{i_k}$. Se $\left[\begin{array}{c} w \\ u \end{array} \right] > |S|$ então $S \vDash w^{\omega+1} = w$.*

O resultado seguinte dá-nos a caracterização dos elementos regulares de $\overline{\Omega}_A\mathbf{DS}$.

Teorema 4.29 (Almeida [3]) *Seja* $\mathbf{V}$ *uma pseudovariedade tal que* $\mathbf{J} \subseteq \mathbf{V} \subseteq \mathbf{DS}$ *e seja* $\pi \in \overline{\Omega}_A\mathbf{V}$. *Diz-se que* π *é regular se e só se* $\begin{bmatrix} \pi \\ u \end{bmatrix} \in \{0, +\infty\}$ *para algum* $u \in A^+$.

Para terminar, segue-se um resultado que nos garante que cada operação implícita sobre $\mathbf{DS}$ é um produto finito de operações explícitas e de operações implícitas regulares.

Teorema 4.30 *Seja* A *um alfabeto. Toda a operação implícita* $\pi \in \overline{\Omega}_A\mathbf{S}$ *admite uma factorização da forma:*

$$\pi = u_0\pi_1u_1 \dots \pi_ku_k.$$

onde

- $u_i \in A^*$ *para todo o* $i \in \{0, \dots, k\}$, *e* $u_0 \neq 1$ *se* $\pi = u_0$;
- *a restrição a* $\mathbf{DS}$ *de cada* $\pi_1, \dots, \pi_k \in \overline{\Omega}_A\mathbf{S}$ *é regular;*
- *se* $u_i = 1$, *com* $i \in \{1, \dots, k-1\}$ *então* $c(\pi_i)$*e* $c(\pi_{i+1})$ *são* $\subseteq$*-incomparáveis;*
- *para todo o* $i \in \{1, \dots, k\}$ *tal que* $u_i \neq 1$*(resp.* $u_{i-1} \neq 1$*), a primeira (resp. última) letra de* u_i *(resp.* u_{i-1}*) não pertence ao conteúdo de* π_i.

Este resultado é útil para o estudo que se segue.

4.2.7 Pseudovariedade J

Vamos agora fazer o estudo das operações implícitas sobre a pseudovariedade, $\mathbf{J} = [\![(ab)^\omega a = (ab)^\omega = b(ab)^\omega]\!] = [\![(ab)^\omega = (ba)^\omega, a^\omega = a^{\omega+1}]\!]$, dos semigrupos $\mathcal{J}$-triviais.

Note-se que $\mathbf{N} \subseteq \mathbf{J}$ e portanto $\Omega_A\mathbf{J} = \mathbf{A}^+$. Por outro lado, como $\overline{\Omega}_A\mathbf{J}$ é um semigrupo $\mathcal{J}$-trivial, os seus elementos regulares são idempotentes e pela Proposição 4.25 esses elementos são completamente determinados pelo seu conteúdo. Por conseguinte, as operações implícitas regulares sobre $\mathbf{J}$ podem ser

identificadas com pseudopalavras da forma u^ω onde u é uma palavra sem letras repetidas. Assim, em termos algébricos (Teorema 4.30), podemos construir todos os elementos de $\overline{\Omega}_A\mathbf{J}$ a partir das projecções $a_1, \ldots, a_n$, utilizando um número finito de vezes duas operações: a multiplicação e a operação a^ω. Resulta então que $\overline{\Omega}_A\mathbf{J}$ coincide com $\Omega^\omega_A\mathbf{J}$.

Proposição 4.31 (Almeida [3]) *O ω-semigrupo $\Omega^\omega_A\mathbf{J}$ é livre sobre A, na ω-variedade gerada por $\mathbf{J}$.*

De seguida mostraremos como resolver o problema da palavra, que neste caso coincide com o problema da ω-palavra, para $\overline{\Omega}_A\mathbf{J}$. Ou seja, mostraremos como determinar de forma efectiva quando é que dois ω-termos nos geradores $a_1, \ldots, a_n$ são o mesmo elemento em $\overline{\Omega}_A\mathbf{J}$.

Para atacar este problema comecemos por tratar um outro. Como identificar a ω-variedade gerada por $\mathbf{J}$? Consideremos primeiro a ω-variedade V definida pelo conjunto Σ das identidades seguintes:

1) $(ab)c = a(bc)$;

2) $(ab)^\omega = (ba)^\omega = (a^\omega b^\omega)^\omega$;

3) $a^\omega a = a^\omega = aa^\omega$;

4) $(a^\omega)^\omega = a^\omega$.

Lema 4.32 *As identidades seguintes são consequências de Σ:*

i) $a^\omega a^\omega = a^\omega$;

ii) $(ab)^\omega a = (ab)^\omega = b(ab)^\omega$;

iii) $t^\omega = v^\omega$ *onde t é um termo e u é um produto, em qualquer ordem, das letras que ocorrem em t.*

Tendo em consideração as identidades de Σ e as suas consequências (Lema 4.32), podemos então proceder à redução de qualquer termo em $\{a_1, \ldots, a_n\}$ aplicando as regras seguintes:

r.1) eliminar parenteses no que respeita à aplicação da operação binária de multiplicação;

r.2) substituir por v^ω qualquer subtermo da forma t^ω, onde v é o produto, por ordem estritamente crescente dos índices, das variáveis que ocorrem em t;

r.3) absorver em factores da forma v^ω quaisquer factores adjacentes nos quais ocorrem apenas variáveis de v.

Estas regras designam-se de *regras de redução* e de facto reduzem o comprimento dos termos. Assim, só se podem aplicar um número finito de vezes a um dado termo.

Por outro lado, a aplicação de uma das regras não colide nem impede a aplicação de uma das outras. Temos então um sistema de regras de redução *noetheriano*, ou de terminação finita, e confluente, isto quer dizer, se de um termo t, por aplicação das regras de redução obtemos dois termos t_1 e t_2 distintos, então, aplicando as regras de redução necessárias a t_1 e t_2 chegamos em ambos os casos a um termo comum t_3. Devido a estas propriedades é possível a partir de um qualquer ω-termo t sobre V, obter um único termo minimal t'. O termo t' diz-se minimal no sentido de não ser possível, por aplicação das regras de redução referidas, obter um outro termo sobre V distinto de t'. Neste caso diz-se que t' é a forma canónica de t.

Passemos então a descrever as formas canónicas em estudo. Um ω-termo é chamado explícito ou uma palavra se nele não ocorre a operação unária. Se ele é da forma t^ω para algum termo t, então diz-se um idempotente. O conteúdo $c(t)$ de um dado termo t é o conjunto das variáveis que nele ocorrem. Portanto as formas canónicas são os termos da forma

$$t = t_1 t_2 \cdots t_k,$$

onde

fc.1) cada t_i é uma palavra ou um idempotente;

fc.2) cada termo idempotente t_i é da forma v^ω, onde v é um produto de variáveis com os índices em ordem estritamente crescente;

fc.3) para dois termos idempotentes consecutivos t_i e t_{i+1}, os conjuntos $c(t_i)$ e $c(t_{i+1})$ são $\subseteq$-incomparáveis;

fc.4) dois termos consecutivos t_i e t_{i+1} não são ambos palavras;

fc.5) se t_i é uma palavra e t_{i+1} é um idempotente então a última letra de t_i não está em $c(t_{i+1})$;

fc.6) se t_{i+1} é uma palavra e t_i é um idempotente então a primeira letra de t_{i+1} não está em $c(t_i)$.

No caso de se verificar a coincidência das formas canónicas de dois termos r_1 e r_2, escreveremos $r_1 \simeq r_2$. Note-se que a variedade V contém $\mathbf{J}$, pois todos os semigrupos $\mathcal{J}$-triviais satisfazem as identidades de Σ. Designando por $F_A\mathsf{V}$ o ω-semigrupo V-livre sobre $A = \{a_1, \ldots, a_n\}$ temos portanto um homomorfismo sobrejectivo de ω-semigrupos tal que para cada $i \in \{1, \ldots, n\}$ tem-se

$$\begin{array}{rcl} \varphi : F_A\mathsf{V} & \longrightarrow & \overline{\Omega}_A\mathbf{J} \\ a_i & \mapsto & a_i \end{array}$$

Consideremos sobre $\overline{\Omega}_A\mathbf{J}$ a relação $\equiv$ definida por:

$$\pi \equiv \rho \quad \text{se} \quad \pi \text{ e } \rho \text{ têm as mesmas sub-palavras } v \in \Omega_A\mathbf{S}.$$

No que se segue o principal objectivo é mostrar que para dois termos t_1 e t_2, temos que

$$t_1 \simeq t_2 \Leftrightarrow \varphi(t_1) \equiv \varphi(t_2). \tag{4.1}$$

A implicação no sentido da esquerda para a direita é fácil de mostrar, uma vez que, Σ deduz a igualdade entre qualquer termo e a sua forma canónica. De facto,

$$t_1 \simeq t_2 \Rightarrow t_1 = t_2 \text{ em } F_A\mathsf{V} \Rightarrow \varphi(t_1) = \varphi(t_2) \Rightarrow \varphi(t_1) \equiv \varphi(t_2).$$

Para provar a implicação contrária basta distinguir diferentes formas canónicas pela extracção de sub-palavras das suas imagens por φ. Começamos por isolar o problema combinatório subjacente, definindo uma operação correspondente à extracção de sub-palavras directamente ao nível dos termos.

Da equivalência (4.1) e tendo em consideração a sequência de implicações apresentada, deduz-se que φ é uma bijecção (de facto φ é sobrejectiva e $\varphi(t_1) = \varphi(t_2) \Rightarrow \varphi(t_1) \equiv \varphi(t_2) \Leftrightarrow t_1 \simeq t_2 \Rightarrow t_1 = t_2$ em $F_A\mathsf{V}$), que $\simeq$ induz a igualdade em $F_A\mathsf{V}$ e ainda que $\equiv$ é a relação de igualdade em $\overline{\Omega}_A\mathbf{J}$.

Para o que se segue consideremos um termo t fixado, em forma canónica, com a factorização $t = t_1 \cdots t_r$ satisfazendo as condições $(fc.1 - 6)$. Dizemos que uma

palavra u pode ser extraída do termo t se existe uma factorização $u = u_1 \cdots u_r$ tal que

i. se t_i é explícito, então u_i é uma sub-palavra de t_i;

ii. se t_i é idempotente, então $c(u_i) \subseteq c(t_i)$.

Uma tal factorização de u diz-se um modo de extrair u de t.

Para um inteiro $k \geq 1$, denotamos por $t^{(k)}$ o termo obtido de t substituindo cada factor v^ω por v^k.

Lema 4.33 *Para uma palavra v são equivalentes as condições seguintes:*

1. *v é uma sub-palavra de $\varphi(t)$;*

2. *v é uma sub-palavra de $t^{(k)}$ para algum k;*

3. *v pode ser extraída de t.*

É importante salientar que os termos são expressões finitas nas variáveis e nas operações, e portanto não existe grande liberdade para proceder à extracção de palavras. Por conseguinte, o resultado que se segue é de grande interesse. A notação $\|t\|$ é utilizada para representar o número de factores idempotentes de t mais a soma dos comprimentos dos factores explícitos de t.

Lema 4.34 *Seja $k > \|t\|$. Então, para extrair de t uma palavra tendo um factor da forma w^k, com $|w| > 0$, tem-se necessariamente que um dos factores w daquela potência é extraído de algum factor idempotente e portanto, todos eles podem ser extraídos desse mesmo factor idempotente.*

O resultado que se segue, tal como pretendido, estabelece a equivalência (4.1).

Teorema 4.35 *Dois ω-termos têm a mesma forma canónica se e só se as operações sobre $\mathbf{J}$ por eles induzidas têm as mesmas sub-palavras.*

Do estudo anterior resultam as seguintes conclusões importantes.

Teorema 4.36 *Para todo o alfabeto A, $\overline{\Omega}_A\mathbf{J}$ é o semigrupo livre com uma operação unária a^ω sobre A na variedade definida pelas identidades $(ab)^\omega = (ba)^\omega = (a^\omega b^\omega)^\omega$ e $a^\omega a = a^\omega = aa^\omega = (a^\omega)^\omega$. Dois termos nas variáveis $a_1, \ldots, a_n$ coincidem em $\overline{\Omega}_A\mathbf{J}$ se e só se eles têm a mesma forma canónica em relação às regras de redução $(r.1-3)$. Em particular o problema da palavra para $\overline{\Omega}_A\mathbf{J}$ é decidível.*

Podemos falar da forma canónica de uma operação implícita sobre $\mathbf{J}$, uma vez que o homomorfismo φ é uma bijecção. Para obter uma definição directa deste conceito é apenas necessário substituir a palavra "termo" por "operação" na definição de forma canónica de termos. Recordemos que um elemento idempotente de $\overline{\Omega}_A\mathbf{J}$ é completamente caracterizado pelo seu conteúdo. Assim, um idempotente de $\overline{\Omega}_A\mathbf{J}$ pode ser denotado por (B) onde B é o seu conteúdo.

Teorema 4.37 *Seja A um alfabeto. Toda a operação implícita $\pi \in \overline{\Omega}_A\mathbf{J}$ admite uma factorização da forma*

$$\pi = u_0(B_1)u_1 \cdots (B_k)u_k$$

onde

- *$u_i \in A^*$ para todo $0 \leq i \leq k$, e $u_0 \neq 1$ se $\pi = u_0$;*
- *se $u_i = 1$, com $1 \leq i \leq k-1$, então B_i e B_{i+1} são $\subseteq$-incomparáveis;*
- *para todo $1 \leq i \leq k$, tal que $u_{i-1} \neq 1$, a última letra de u_{i-1} não aparece em B_i;*
- *para todo $1 \leq i \leq k$, tal que $u_i \neq 1$ a primeira letra de u_i não aparece em B_i.*

Uma factorização de π deste tipo é dita em forma canónica.

Teorema 4.38 *Sejam $\pi = u_0(B_1)u_1 \cdots (B_k)u_k$ e $\rho = v_0(C_1)v_1 \cdots (C_m)v_m$ duas factorizações em forma canónica de elementos de $\overline{\Omega}_A\mathbf{J}$. Então são equivalentes as condições seguintes:*

1. $\pi = \rho$;
2. *π e ρ têm as mesmas sub-palavras;*
3. $k = m$, $u_0 = v_0$, $u_i = v_i$ e $B_i = C_i$ $(i = 1, \ldots, k)$.

Para finalizar este capítulo, vejamos um exemplo concreto.

Exemplo 4.39 *Consideremos o alfabeto $A = \{a, b, c, d\}$. Sejam π, ρ e $\beta \in \Omega_A^\omega\mathbf{S}$ três operações implícitas definidas por:*

- $\pi = abb^\omega ac(ad)^{\omega+1}$;
- $\rho = ((ab^\omega)^\omega bc^\omega)^\omega d(ad)^\omega$;
- $\beta = (ca^\omega b)^\omega bd(ad^\omega a)^\omega$.

Por aplicação das regras de redução, anteriormente referidas, obtemos as projecções de π, ρ e β sobre o semigrupo $\Omega_A^\omega\mathbf{J}$, que são dadas, respectivamente, por:

- $p_\mathbf{J}(\pi) = a(\{b\})ac(\{a, d\})$;
- $p_\mathbf{J}(\rho) = (\{a, b, c\})(\{a, d\})$;
- $p_\mathbf{J}(\beta) = (\{a, b, c\})(\{a, d\})$.

Dado que as formas canónicas de $p_\mathbf{J}(\rho)$ e de $p_\mathbf{J}(\beta)$ são coincidentes conclui-se que $\mathbf{J} \vDash \rho = \beta$. No entanto, $p_\mathbf{J}(\pi)$ e $p_\mathbf{J}(\rho)$ admitem formas canónicas distintas, e portanto, $\mathbf{J} \nvDash \pi = \rho$.

Resumindo, o problema da palavra para o semigrupo $\overline{\Omega}_A\mathbf{J}$ é resolvido descrevendo regras de transformação de operações que permitem reduzir a "complexidade" das operações até obter "formas canónicas" para as operações. A igualdade de duas operações, no semigrupo em causa, é então testada construindo as suas formas canónicas pela aplicação das regras de redução e verificando se elas são iguais.

Capítulo 5

Decidabilidade

Existem várias questões de decidabilidade relacionadas com a teoria de semigrupos finitos. Existem muitos tipos de problemas de decisão. De entre eles destaca-se o famoso problema da pertença que está intimamente ligado com técnicas para o estudo de pseudovariedades, que foi abordado no capítulo 4.

Historicamente, o primeiro problema de decisão que se mostrou ser insolúvel foi o Problema da Paragem de uma Máquina de Turing. Antes de o abordarmos é necessário dar uma definição de algoritmo e de problema de decisão.

5.1 Problema de decisão

Um *problema de decisão* é uma colecção de questões cada uma das quais admite como resposta sim ou não.

Antes de mais é útil referir algumas breves considerações sobre o significado sobre o termo algoritmo, que neste conteúdo poderá ser entendido como um sinónimo de procedimento mecânico. Não é só interessante estudar os algoritmos mas também como eles reagem quando lhes são atribuídos determinados dados. Se quisermos mostrar que uma dada propriedade não é decidível, temos que mostrar que nenhum algoritmo nos permite testar a sua validade, o que é manifestamente difícil se não se tiver o conhecimento exacto do que é um algoritmo.

Suponhamos que temos uma colecção de instâncias, uma frase sobre essas instâncias e queremos saber se para cada instância essa frase é verdadeira ou

falsa. Um procedimento de decisão é um algoritmo que providencia uma resposta para cada instância num número finito de passos. O problema de descobrir esse algoritmo é um *problema de decisão*. O problema é dito *decidível* se esse algoritmo existe, e em caso contrário é *indecidível*.

Por exemplo, o problema de decisão seguinte é efectivamente decidível pelo algoritmo de Euclides:

$$\begin{aligned} \text{instância} &: p,\ q \in \mathbb{Z} \\ \text{declaração} &: p \text{ e } q \text{ são primos entre si} \end{aligned}$$

Na década de 1930 foram propostas formalizações das noções de algoritmo e de procedimento de decisão. Um pouco tempo antes, em 1900, *D. Hilbert*, no congresso internacional de matemáticos, propôs 23 problemas que influenciaram profundamente a direcção da investigação matemática do século seguinte. O décimo problema era encontrar um procedimento que determinasse se uma dada equação diofantina arbitrária podia ou não resolvida em inteiros. Só em 1970 é que *Y. Matijasevich* mostrou que tal procedimento não existe. Ou seja, o problema é indecidível. Em 1917 *Hilbert* expandiu o seu décimo problema a um problema de decidabilidade, num número finito de passos pré-determinados, da verdade ou falsidade de uma dada frase numa dada teoria matemática. Em 1937, *A. Turing* mostrou que este problema não era resolúvel.

Vamos ser mais específicos com as noções de instância, declaração (frase) e algoritmo na nossa definição de problema de decisão.

Uma teoria, onde é para ser aplicado um procedimento de decisão, deve envolver apenas um número finito de símbolos para operações, conectivos lógicos, pontuação, variáveis, etc; as fórmulas devem ser de comprimento finito e os algoritmos devem envolver um número finito de instruções. A teoria pode ser codificada por palavras de A^* de algum alfabeto finito A.

Recorde-se que uma máquina de Turing, tal como foi visto na Subsecção 2.7.1, consiste num conjunto finito Q de estados (incluindo o estado inicial q_0 e o estado final q_f), um alfabeto finito A e o símbolo Δ, que passa agora a ser visto como o símbolo 1 (o elemento identidade de A^*) e uma função parcial $\delta : (A \cup \{1\}) \times Q \times \{E, C, D\}$. As letras consecutivas de A que fazem um input são inseridas nos quadrados consecutivos a partir do segundo, enquanto que os outros quadrados contêm o Δ. A máquina começa no estado q_0 lendo o primeiro

quadrado. Suponhamos que nalgum passo a máquina está no estado q e que está a ler a letra x em algum quadrado, então, de seguida executam-se as componentes de $\delta(x, q)$ que são respectivamente, uma letra que substitui x no seu quadrado, o próximo estado da máquina e o próximo quadrado que vai ser lido (E, C, D são respectivamente o quadrado da esquerda, o mesmo, o da direita). A máquina pára quando atinge o estado q_f, ou quando tem instruções insuficientes para continuar. Pode não parar de vez.

Podemos agora então dar uma definção mais completa de algoritmo.

Definição 5.1 *Um algoritmo é uma máquina de Turing que pára para a configuração inicial de qualquer palavra.*

Uma *solução* para um problema de decisão é um algoritmo que fornece a resposta para cada instância do problema. Cada instância do problema é codificada e a resposta a essa instância é sim se o algoritmo pára no estado final q_f. Caso pare num instante diferente, a resposta é não.

Um problema que admite uma solução diz-se *solúvel* ou *decidível*. Caso contrário diz-se *insolúvel* ou *indecidível*.

5.2 Problema da Paragem para Máquinas de Turing

Consideremos o seguinte:

instância : Uma máquina de Turing T sobre A e uma entrada I
declaração : T pára para I

Só existe um número contável de máquinas de Turing e de entradas sobre um alfabeto A. Uma máquina de Turing pode ser vista como uma função $T : A^+ \longrightarrow A^* \cup \{\infty\}$ com uma entrada idêntica à que foi atrás definida e a correspondente saída sendo o que está na fita quando a máquina está no estado q_f ou, quando a máquina não pára, a saída é ∞. Turing assumiu que o Problema da Paragem é decidível e consequentemente, para cada máquina de Turing T e cada input $x \in A^+$, a saída $T(x) \in A^* \cup \{\infty\}$ pode ser computada. Mais tarde, Turing obtém uma contradição por um argumento análogo ao argumento de

diagonalização de Cantor que mostra que o conjunto dos números reais é inumerável. Portanto, o Problema da Paragem é indecidível.

Em meados da década de 1930, *A. Church* mostrou que se a Teoria Elementar dos Números é consistente então ela inclui problemas indecidíveis. A descoberta da indecidabilidade do Problema da Paragem, ou de outro qualquer problema de decisão, é significante porque ele potencialmente permite mostrar a indecidabilidade de um dado problema. De facto, mostrando que um problema indecidível se "reduz" a um dado problema, conclui-se que o problema dado também é indecidível.

Existem actualmente muitos problemas de decisão em matemática que já sabemos serem indecidíveis.

5.3 Alguns problemas de decisão para semigrupos

5.3.1 Problema da Palavra

Sejam A um conjunto finito e $R \subseteq A^+ \times A^+$ uma relação. Consideremos um semigrupo S. Diz-se que S é definido por uma apresentação $< A, R >$ se é isomorfo ao semigrupo quociente A^+/ρ_R, em que ρ_R denota a menor congruência sobre A^+ que contém R. O Problema da Palavra para $S =< A, R >$ traduz-se no seguinte:

$$\begin{aligned} \text{instância} &: u,\ v \in A^+ \\ \text{declaração} &: u = v \text{ em } S \end{aligned}$$

Mostra-se que um semigrupo livre finitamente gerado e qualquer semigrupo finito têm problemas da palavra decidíveis, bem como os membros de várias classes de semigrupos.

É comum dizer que uma classe de semigrupos tem problema da palavra solúvel se cada um dos seus membros tem essa propriedade.

A classe $\mathbf{S}$ de todos os semigrupos finitos tem problema de palavra solúvel, mas a classe S de todos os semigrupos não tem.

Teorema 5.2 ([19]) *Um semigrupo finitamente apresentado tem problema de palavra decidível se e só se está mergulhado num semigrupo simples que por sua vez mergulha num semigrupo finitamente apresentado.*

5.3.2 Problema da Finitude

O Problema da Finitude pode ser enunciado da seguinte forma:

$$\begin{aligned} \text{instância} &: S \text{ é um semigrupo finitamente apresentado} \\ \text{declaração} &: S \text{ é finito} \end{aligned}$$

O Problema de *Burnside* de 1902 é um refinamento deste problema no sentido em que tem a mesma declaração mas cuja instância é um semigrupo S finitamente gerado que satisfaz a identidade $x^{p+n} = x^n$ para alguns $p, n \in \mathbb{N}$. Morse e Hedlund concluiram que existe um semigrupo 3-gerado infinito que satisfaz $x^2 = 0$ e um semigrupo 2-gerado infinito que satisfaz $x^3 = 0$. Também, Adian e Novikov ([19]) mostraram que grupos relativamente livres finitamente gerados com expoente ímpar > 665 são infinitos.

Dado isto coloca-se a seguinte questão:

Problema 1 *Existe algum semigrupo com Problema da Finitude indecidível?*

5.3.3 Problema Equacional

O Problema Equacional para uma variedade V de semigrupos com uma base de identidades finita sobre um conjunto numerável A de variáveis, pode ser traduzido da seguinte forma:

$$\begin{aligned} \text{instância} &: u,\ v \in A^+ \\ \text{declaração} &: u = v \text{ é uma identidade para } \mathsf{V} \end{aligned}$$

Este problema é solúvel se e só se o problema da palavra em $F_A(\mathsf{V})$ é solúvel. O problema da palavra para objectos livres em variedades de semigrupos atraiu muitas atenções nos últimos 30 anos. Por exemplo é solúvel para variedades tais como S e para qualquer variedade de semigrupo unária de semigrupos completamente regulares e para semigrupos inversos juntamente com várias das suas subvariedades.

O Problema da Palavra para semigrupos livres de *Burnside* de índice ≥ 3 foi provado ser solúvel nos primeiros anos da última década. *Murskii* [33] mostrou que existe uma variedade de semigrupos que tem problema equacional indecidível.

À primeira vista o problema equacional parece não ter relevância para pseudovariedades porque uma pseudoidentidade relaciona termos de semigrupos profinitos inumeráveis. No entanto o problema torna-se sensível se restringirmos a nossa atenção para pseudoidentidades que são também identidades. O Problema Equacional Fraco (ou Fraco-ω) para uma pseudovariedade $\mathbf{V}$ com bases finitas de pseudovariedades sobre um conjunto numerável de variáveis A pode ser representado por

$$\begin{array}{rcl} \text{instância} & : & u,\ v \in A^+ (\text{ou } u, v \in \Omega_A^\omega \mathbf{S} \text{ respectivamente}) \\ \text{declaração} & : & u = v \text{ é uma pseudoidentidade para } \mathbf{V} \end{array}$$

Para qualquer variedade V o problema equacional e o problema equacional fraco coincidem para V_{fin}, a pseudovariedade dos membros finitos de V. Pela descrição de Almeida [3] de $\overline{\Omega}_A\mathbf{J}$, onde $\mathbf{J}$ é a pseudovariedade de semigrupos finitos $\mathcal{J}$-triviais, existe uma projecção natural de $\Omega_A^\omega\mathbf{S}$ para $\overline{\Omega}_A\mathbf{J}$ e o problema equacional Fraco-ω é solúvel para $\mathbf{J}$. Por [1] existe uma pseudovariedade que tem Problema Equacional Fraco indecidível.

5.3.4 Problema da Identidade

O Problema da Identidade para uma variedade V finitamente baseada pode ser traduzido por

$$\begin{array}{rcl} \text{instância} & : & \text{Um conjunto finito de identidades } \Sigma \quad \text{sobre A e } u, v \in A^+ \\ \text{declaração} & : & u = v \text{ é uma identidade para } \mathsf{V} \cap [\Sigma] \end{array}$$

Este problema requer que o Problema Equacional seja uniformemente solúvel para todas as subpseudovariedades finitamente baseadas de V. Tal como o Problema Equacional, podemos formular o Problema da Identidade Fraco (ou Fraco-ω) para uma pseudovariedade. A variedade S tem Problemas de Identidade indecidível [33] e a pseudovariedade $\mathbf{S}$ tem Problema de Identidade Fraco indecidível [1].

Capítulo 6

Desenvolvimentos

A teoria de semigrupos finitos não se tornou um campo autónomo com os seus próprios conjuntos de problemas e métodos que de alguma maneira se individualizou como uma área matemática. Tal só se verificou após uma forte motivação exterior em teóricos da ciência da computação.

Os passos cruciais nesta direcção foram tomados na década de 1950 e podem ser considerados como parte das fundações da ciência da computação.

Motivado mais geralmente por aplicações dos autómatos e visando uma teoria de decomposição de máquinas de estado finito, Krohn e Rhodes estudaram em meados de 1960 a decomposição em cascata de autómatos e a associação do produto em coroa a decomposições de semigrupos finitos. De uma forma mais sintética, os problemas de decisão estudados em linguagens tranformaram-se em problemas de decisão em semigrupos finitos.

Krohn e Rhodes propuseram como uma medida de complexidade de um semigrupo finito o menor número de componentes de grupo em tal decomposição. Com aplicações em vista, eles questionavam-se se a função de complexidade poderia ser efectivamente computada. Este problema tem sido central na teoria de semigrupos finitos.

6.1 Um problema histórico: O problema da complexidade de Krohn-Rhodes

Como uma observação preliminar, é importante notar que o produto semidirecto de duas pseudovariedades decidíveis não é necessariamente decidível. Enquanto que esta era na generalidade aceite como sendo o caso, a demonstração foi apenas feita recentemente. É devido a Rhodes [38] que estendeu ao produto semidirecto e ao produto de Malcev resultados similares provados anteriormente por Albert, Baldinger e Rhodes para supremos [1].

A noção de localidade foi introduzida por Tilson [44] em ligação com o problema proposto por Eilenberg [26] que diz respeito a produtos semidirectos com a pseudovariedade **D**. Tilson começou por estender o conceito de pseudovariedade ao contexto de categorias e semigrupóides (definidos como categorias sem a exigência de identidades locais). As arestas (ou morfismos na terminologia standard) em cada vértice (ou objectos) de um semigrupóide, se existir pelo menos um, forma um semigrupo com a composição, que é designado de semigrupo local nesse vértice.

Desde cedo, precursores do trabalho de Tilson podem ser encontrados nos trabalhos de Brzozowski, Simon, McNaughton sobre as linguagens localmente testáveis mas também em Knast, onde o nível 1 da hierarquia de Brzozowski foi caracterizado e computado. Todos estes trabalhos anteriores estavam relacionados com problemas sobre considerações teóricas de linguagens.

Desenvolvendo desde cedo as ideias de Rhodes, Tilson [44] também desenvolveu um semigrupóide derivado $D(\tau)$ naturalmente associado a um morfismo relacional $\tau : S \longrightarrow T$ e mostrou que um semigrupo finito S pertence a um produto semidirecto $\mathbf{V} * \mathbf{W}$ se e só se existe um morfismo relacional $\tau : S \longrightarrow T$ para algum $T \in \mathbf{W}$ tal que $D(\tau) \in g\mathbf{V}$.

Um morfismo relacional $\tau : S \longrightarrow T$ para $S, T \in \mathbf{S}$ é uma relação binária $\tau \subseteq S \times T$ tal que $\tau(s) \subseteq T$ e $\tau(s_1)\tau(s_2) \subseteq \tau(s_1 s_2)\ \forall s, s_1, s_2 \in S$.

Acontece que existem algumas ligações entre produtos semidirectos e produtos de Malcev, particularmente quando o segundo factor é uma pseudovariedade de grupos. Verificou-se que, $\mathbf{V} * \mathbf{H} \subseteq \mathbf{V}\ m\ \mathbf{H}$ para qualquer pseudovariedade $\mathbf{H}$ de grupos e, em caso de $\mathbf{V}$ ser uma pseudovariedade local a igualdade mantém-se. No entanto essa igualdade mantém-se também noutras situações. Apesar de

muita coisa ser conhecida sobre os produtos directos e de Malcev, o problema $\mathbf{V} * \mathbf{H} = \mathbf{V}\ m\ \mathbf{H}$ para pseudovariedades de grupos $\mathbf{H}$ continua ainda em estudo.

O modelo teórico de C. J. Ash tornou-se bem conhecido no campo dos semigrupos finitos através da demonstração que uma pseudovariedade gerada por todos os semigrupos inversos finitos (que é o produto semidirecto $\mathbf{Sl} * \mathbf{G}$) consiste em todos os semigrupos finitos cujos idempotentes comutam [15].

Nessa altura, Ash estudou sistematicamente operadores tais como o supremo, a potênciação e o produto semidirecto. As técnicas envolvidas em tais estudos eram essencialmente sintáticas, no sentido em que (pseudo)identidades e objectos livres (profinitos) eram os ingredientes principais. Estas ferramentas foram desenvolvidas pelo autor a partir da caracterização de pseudovariedades partindo de pseudoidentidades.

Um problema abordado por Ash, e sugerido por I. Simon, consistia na computação do produto semidirecto $\mathbf{Sl} * \mathbf{L}$, onde $\mathbf{L}$ é a pseudovariedade de todos os semigrupos finitos $\mathcal{L}$-triviais. Um passo essencial neste trabalho foi dado por Weil e Almeida [14] que obtiveram uma base geral de pseudoidentidades para produtos semidirectos $\mathbf{V} * \mathbf{W}$. Infelizmente foram descobertas falhas na demonstração deste conhecido "teorema da base". Embora seja válido em alguns casos importantes, a sua validade em geral continua por provar.

Este teorema foi usado em muitas pesquisas ao longo dos anos desde a sua descoberta em 1993. Felizmente, a maior parte das aplicações não dependem do "teorema da base". Pelo menos, talvez a mais marcante aplicação uma anunciada e mais tarde usada na redução do problema da complexidade de Krohn-Rhodes, não depende deste passo defeituoso.

Eventualmente, um método completamente geral de usar o "teorema da base" foi derivado da propriedade algorítmica da pseudovariedade que foi chamada de hiperdecidabilidade [4]: se $g\mathbf{V}$ é decidível e admite uma base de pseudoidentidades sobre grafos com no máximo n vértices, onde n é um dado número natural, e $\mathbf{W}$ é hiperdecidível então $\mathbf{V} * \mathbf{W}$ é decidível. A validade deste resultado persiste desde que não dependa do caso defeituoso do "teorema da base".

6.2 Problema da Pertença para classes de semigrupos finitos

A questão principal da teoria de pseudovariedades de semigrupos é a de determinar, para uma dada pseudovariedade $\mathbf{V}$, se existe algum algoritmo que permita resolver o seguinte problema:

$$\begin{aligned} \text{instância} &: \text{Um semigrupo finito } S \\ \text{declaração} &: S \in \mathbf{V}. \end{aligned}$$

Se tal algoritmo existir é usual dizer simplesmente que $\mathbf{V}$ é decidível.

O problema é parcialmente dominante devido à versão do teorema da pseudovariedade de Krohn-Rhodes e ao teorema da variedade de Eilenberg. Almeida provou que existem pseudovariedades finitamente baseadas de semigrupos finitos que não são decidíveis. Se $\mathbf{V}$ é uma pseudovariedade com uma base finita de pseudoidentidades, cada uma das quais pode ser testada em qualquer semigrupo finito, então $\mathbf{V}$ é decidível. Então uma tarefa natural quando é dada uma pseudovariedade é a tentativa de encontrar uma base finita para as suas pseudoidentidades. No entanto, a condição não é necessária.

Algumas pseudovariedades foram estudadas intensivamente por causa das suas conexões com variedades de linguagens. Em particular, $\mathbf{A}$, a classe dos semigrupos aperiódicos, consiste precisamente em semigrupos que reconhecem linguagens livres de estrela e $\mathbf{J}$, a classe dos semigrupos $\mathcal{J}$-triviais, é feita de semigrupos finitos que reconhecem linguagens regulares testáveis aos pedaços. Ambas são pseudovariedades decidíveis. No entanto, existem longos impasses em resolver problemas da pertença na teoria das linguagens.

O Problema da Pertença para pseudovariedades obtidas através da combinação de pseudovariedades decidíveis com operações tais como, supremo, produto de Malcev e produto semidirecto foi intensivamente estudado durante cerca de 25 anos. Isto, por causa da complexidade do problema associado com o Teorema de Krohn-Rhodes.

Teorema 6.1 *Para cada semigrupo finito S existe um $n \geq 0$ tal que $S \in \mathbf{A} * (\mathbf{G} * \mathbf{A})^n$. O menor n que verifica esta condição é chamado a complexidade de S.*

O problema de determinar a complexidade de um semigrupo é, desde que foi descoberto, um dos principais problemas da teoria de semigrupos finitos. E está intimamente relacionado com a decidibilidade de produtos semidirectos iterados envolvendo as pseudovariedades dos grupos e dos semigrupos aperiódicos.

Problema 2 *Dado um operador* $\mathcal{O}$ *e pseudovariedades (decidíveis)* $\mathbf{V_1}, \ldots, \mathbf{V_n}$*, determinar se* $\mathcal{O}(\mathbf{V_1}, \ldots, \mathbf{V_n})$ *é decidível e, em caso afirmativo, encontrar algoritmos eficientes para testar o Problema da Pertença.*

Os operadores mais comuns, tais como, supremo, produto semidirecto e produto de Malcev, não preservam a decidibilidade. Em particular, como referimos anteriormente, Rhodes [29] mostrou que existem pseudovariedades decidíveis cujo produto semidirecto não é decidível. Deste facto surgiu a necessidade de estabelecer condições mais fortes que a decidibilidade, na expectativa de que as pseudovariedades obtidas pela aplicação de operadores a pseudovariedades com tais propriedades fossem decidíveis.

Os produtos de Malcev e os produtos semidirectos podem ser definidos em termos relacionais. Então,

$$\mathbf{U}\ m\ \mathbf{V} = \{s \in S : \ \exists \text{ um morfismo relacional } \tau : S \longrightarrow T \in \mathbf{V} \text{ tal que } \tau^{-1}(e) \in \mathbf{U}\ \forall e \in \mathbf{E}(\mathbf{T})\}$$

$$\mathbf{U} * \mathbf{V} = \{s \in S : \ \exists \text{ um morfismo relacional } \tau : S \longrightarrow T \in \mathbf{V} \text{ tal que } D(\tau) \in g\mathbf{U}\}$$

Aqui $D(\tau)$ é o semigrupo derivado de τ de Tilson e $g\mathbf{U}$ é a variedade de semigrupóides gerada por membros de $\mathbf{U}$.

Existem vários supremos de pseudovariedades que são conhecidas serem decidíveis porque são finitamente baseadas [3]. No entanto existem exemplos de supremos de pseudovariedades, tais como, $\mathbf{J} \vee \mathbf{B}$ ($\mathbf{B}$ a pseudovariedade das bandas finitas) e $\mathbf{J} \vee \mathbf{G}$, que são decidíveis mas que não são finitamente baseadas.

Surge então o Problema da Decidabilidade Forte para uma pseudovariedade, e que consiste em verificar se existe um algoritmo que resolva o seguinte problema:

instância : $S \in \mathbf{S}$ *e* $A \subseteq S$
declaração : para cada morfismo relacional $\tau : S \longrightarrow T \in \mathbf{V}$ $\exists t \in T$ tal que $A \subseteq \tau^{-1}(t)$.

Este é mais forte que o problema da decidabilidade para $\mathbf{V}$, pois uma pseudovariedade fortemente decidível é decidível.

Rhodes e Steinberg [39] mostraram que o problema da identidade fraco em $\mathbf{V}$ é indecidível quando $\mathbf{V}$ não é fortemente decidível. Este facto foi usado para demonstrar a decidabilidade de uma pseudovariedade que não é fortemente decidível.

Almeida e Weil [14] exploraram as bases de produtos semidirectos de pseudovariedades decidíveis. Almeida [4] foi então conduzido para uma noção ainda mais forte que a de decidabilidade forte, o conceito de hiperdecidabilidade. Por conveniência na descrição do Problema de Hiperdecidabilidade identifica-se um morfismo relacional $\tau : S \longrightarrow T$ com a sua extensão canónica $\tau : S^1 \longrightarrow T^1$.

Este problema consiste em verificar se existe um algoritmo que resolva o seguinte problema:

instância : Um grafo finito Γ, $S \in \mathbf{S}$ e uma transformação $\gamma : \Gamma \longrightarrow S^1$
declaração : para cada morfismo relacional $\tau : S \longrightarrow T \in \mathbf{V}$ $\exists$ uma transformação $\beta : \Gamma \longrightarrow T^1$ tal que $(\gamma(x), \beta(x)) \in \tau$ e para cada aresta $e \in \Gamma$, com $e\alpha$ e $e\omega$ como sendo o vértice inicial e final, respectivamente, $\beta(e\alpha)\beta(e) = \beta(e\omega)$

A pseudovariedade $\mathbf{V}$ é chamada hiperdecidível se o problema anterior é decidível. Almeida [4] mostrou que para pseudovariedades $\mathbf{U}$ e $\mathbf{V}$ de semigrupos finitos, se $g\mathbf{U}$ tem um conjunto de pseudoidentidades definido escritos em grafos com pelo menos um número inteiro de vértices n, se $g\mathbf{U}$ é decidível e se $\mathbf{V}$ é hiperdecidível então $\mathbf{U}*\mathbf{V}$ é decidível.

Obter algoritmos efectivos para hiperdecidabilidade é frequentemente uma tarefa árdua.

Para o que se segue é necessário introduzir o conceito de assinatura implícita.

Uma assinatura implícita é um conjunto de operações implícitas σ contendo a multiplicação $a \cdot b$. Para um alfabeto A e uma pseudovariedade $\mathbf{V}$, denotamos por

$\Omega_A^\sigma \mathbf{V}$ o σ-subsemigrupo de $\overline{\Omega}_A \mathbf{V}$ gerado por A. Os elementos de $\Omega_A^\sigma \mathbf{V}$ dizem-se σ-palavras sobre $\mathbf{V}$. De uma forma mais geral, uma assinatura implícita é um conjunto de operações implícitas contendo a multiplicação.

Uma pseudovariedade $\mathbf{V}$ diz-se σ-mansa se: $\mathbf{V}$ é recursivamente enumerável, $\mathbf{V}$ é σ-redutível e o problema da σ-palavra é decidível para $\mathbf{V}$. Se uma pseudovariedade $\mathbf{V}$ é σ-mansa para alguma assinatura σ, tal que σ é recursivamente enumerável e é constituída por operações implícitas computáveis, então $\mathbf{V}$ diz-se mansa.

A mansidão implica a decidibilidade. É um conceito mais forte que hiperdecidabilidade, com propriedades mais fortes embora mais fácil de perceber. No entanto a questão de saber se a mansidão é útil para provar a decidibilidade de pseudovariedades obtidas pela aplicação dos operadores de pseudovariedades mais comuns é ainda um problema em aberto.

De facto, em [8], Almeida e Steinberg pensaram ter conseguido provar que o produto semidirecto $\mathbf{V}_1 * \cdots * \mathbf{V}_n$ de pseudovariedades mansas seria uma pseudovariedade decidível. Dado que a pseudovariedade $\mathbf{G}$ dos grupos é mansa [16], a validade de tal resultado teria como corolário que a função complexidade de Krohn-Rhodes poderia ser efectivamente calculada. Este resultado ficaria apenas dependente da demonstração de que a pseudovariedade A é mansa, resultado enunciado por Rhodes mas ainda não publicado. No entanto, a prova de que o produto semidirecto iterado de pseudovariedades mansas seria decidível baseava-se no "teorema da base" cuja validade foi posta em causa e ainda não foi demonstrada.

Em geral, provar a mansidão de uma pseudovariedade não é simples. Sabe-se já que existem algumas pseudovariedades que são mansas. No entanto, muitas outras bem conhecidas continuam a ser investigadas e estudadas. Sabe-se por exemplo que:

- $\mathbf{G}$ é mansa [16].
- $\mathbf{K}$ e $\mathbf{D}$ são mansas [11].
- $\mathbf{Ab}$ é mansa [9].
- $\mathbf{LSl} = \mathbf{Sl} * \mathbf{D}$ é mansa [25].
- $\mathbf{R}$ é mansa [10].

Bibliografia

[1] D. Albert, R. Baldinger e J. Rhodes, Undecidability of the identity problem for finite semigroups, *J. Symbolic Logic* **57** (1992) 179-192.

[2] J. Almeida. The algebra of implicit operations, *Algebra Universalis* **26** (1989) 16-72.

[3] J. Almeida. *Finite semigroups and Universal Algebra*, World Scientific, Singapore, 1994.

[4] J. Almeida. Hyperdecidable pseudovarieties and the calculation of semidirect products, *Int. J. Algebra Comput.* **9** (1999) 241-261.

[5] J. Almeida. Some Key Problems on Finite Semigroups, *Semigroup Forum* **64** (2002).

[6] J. Almeida e A. Azevedo. Implicit operations on certain classes of semigroups, em S. Goberstein e P. Higgins (Eds.), Proc. of Chico Conf., *Semigroups and their applications*, D. Reidel (1987) 1-11.

[7] J. Almeida, A. Azevedo e M. Zeitoun. Pseudovariety joins involving $\mathcal{J}$-trivial and completely regular semigroups, *Int. J. Algebra and computation* **9** (1999) 99-112.

[8] J. Almeida e B. Steinberg. On the decidability of iterated semidirect products and applications to complexity, *Proc. London Math Soc.* **80** (2000) 50-74.

[9] J. Almeida e M. Delgado. Tameness of the pseudovariety of abelian groups, Int. J. Algebra and Computation **15** (2005) 327-338.

[10] J. Almeida, J. C. Costa e M. Zeitoun. Tameness of pseudovariety joins involving $\mathbf{R}$, *Monatshefte für Mathematik* **146** (2005) 89-111.

[11] J. Almeida e M. Zeitoun. Tameness of some locally trivial pseudovarieties, Communications in Algebra **31** (2003) 61-77.

[12] J. Almeida e M. Zeitoun. An automata-theoretical approach to the word problem for ω-terms over **R**, *Theoret. Comput. Sci.* **370** (2007) 131-169.

[13] J. Almeida e P Weil. Relatively free profinite monoids : an introduction and examples, em J. Fountain (Ed.), *Semigroups, formal languages and groups*, Kluwer (1995) 73-117.

[14] J. Almeida e P Weil. Profinite categories and semidirect products, *J. Pure Appl. Algebra* **123**, (1995) 1-50.

[15] C. Ash. Finite semigroups with commuting idempotents, *J. Austral. Math. Soc., Ser. A* **43** (1987) 81-90.

[16] C. Ash. Inevitable graphs: A proof of the type II conjecture and some related decision procedures, *Int. J. Algebra and Comput.* **1** (1991) 127-146.

[17] A. Azevedo. *Operações implícitas sobre pseudovariedades de semigrupos. Aplicações.* Tese de Doutoramento, Universidade do Porto, 1989.

[18] A. Azevedo. The join of the pseudovarieties **J** with permutative pseudovarieties, em Almeida e al.(Eds.), *Lattices, Semigroups and Universal Algebra*, Plenum, New York (1990) 1-11.

[19] W. W. Boone e G. Higman. *An algebraic characterisation of groups with soluble word problem*, J. Austral. Math. Soc., **18** (1974) 41-53.

[20] J. Brzozowski e I. Simon. *Characterization of locally testable events*, Discrete Mathematics 4 (1973) 243-271.

[21] J. C. Costa. *Autómatos e máquinas de Turing*, publicação do Departamento de Matemática da Universidade do Minho, 2004.

[22] J. C. Costa. Quelques intersections de variétés de semigroupes finis et de variétés de langages, opérations implicites. Tese de Doutoramento, Universidade de Paris **6**, 1998.

[23] J. C. Costa. *Tópicos de Álgebra*, Manuscrito, Universidade do Minho, 2004.

[24] J. C. Costa. *Tópicos de Semigrupos e Linguagens*, Manuscrito, Universidade do Minho, 2006.

[25] J. C. Costa e M. L. Teixeira. Tameness of the pseudovariety **LSl**, *Int. J. Algebra and Computation* **14** (2004) 627-654.

[26] S. Eilenberg. *Automata, Languages and Machines*, Vol. B, Academic Press, New York, 1976.

[27] P. A. Grillet. *Semigroups: An Introduction to the Structure Theory*, Marcel Dekker, New York, 1995.

[28] J. Howie. *Fundamentals of Semigroups Theory*, Oxford University Press, New York, 1995.

[29] K. Krohn e J. Rhodes. Algebraic theory of machines I - Prime decomposition theorem for finite semigroups and machines, *Trans. Amer. Math. Soc.* **116** (1965) 450-464.

[30] Lothaire. *Combinatorics on words*, Addison-Welsey Publishing Company, 1983.

[31] R. McNaughton. Algebraic decision procedures for local testability, *Math. System and Theory* **8** (1974) 60-76.

[32] M. Morse e G. A. Hedlund. Symbolic dynamics, *Amer. J. Math.* **60** (1938) 815-866.

[33] V. L. Murskii. Some examples of varieties of semigroups. *Mat. Zametki* **3** 663-670, (1968).

[34] C. Nogueira. *O problema da ω-palavra para pseudovariedades de semigrupos.* Tese de Mestrado, Universidade do Minho, 2006.

[35] P. S. Novikov e S. I. Adian. On finite periodic groups, I, II, III, IV. *Akad. Nauk. SSSR* **32** (1968) 212-244, 251-524, 709-731.

[36] J.-E. Pin. *Variétés de langages formels*, Masson, Paris, 1984.

[37] J. Reiterman. The Birkhoff theorem for finite algebras, *Algebra Universalis* **14** (1982) 1-10.

[38] J. Rhodes. Undecidability, automata and pseudovarieties of finite semigroups, *Int. J. Algebra Comput.* **9** (1999) 455-473.

[39] J. Rhodes e B. Steinberg. Pointlike sets, hyperdecidability and the identity problem for finite semigroups, *Int. J. Algebra and Comput.* **9** (1999) 475-481.

[40] M. Sapir. Problems of Burnside type ande the finite basis property in varieties of semigroups, *Izv. Akad. Nauk. SSSR* **51** (1987) 319-340.

[41] M. Sapir. Weak word problem for finite semigroups, ed J. Rhodes *Monoids and Semigroups with Applications*, World Scientific, Singapore (1991).

[42] M. Schützenberger. On finite monoids having only trivial subgroups, *Inform. and Control* **8** (1965) 190-194.

[43] I. Simon. *Hierarchies of events with dot-depth one*. Tese de doutoramento. University of Waterloo, 1972.

[44] B. Tilson. Categories as algebra: an essential ingredient in the theory of monoids. *J. Pure and Applied Algebra* **48** (1987) 83-198.

[45] P. Trotter. Decidability problems in finite semigroups. *Semigroups, Algorithms, Automata and Languages, Eds. G. Gomes, J.-E. Pin e P. Silva*, World Scientific, Singapore. (2002) 501-515.

[46] P. Vieira. Palavras finitas e infinitas. Dissertação de Mestrado, Universidade de Lisboa, 2003.

Índice