

# Grupos Maximais em Semigrupos de Burnside Livres

Alair Pereira do Lago

Tese apresentada ao Instituto de Matemática e Estatística da Universidade de São Paulo para a obtenção do grau de Doutor em Matemática Aplicada.

Orientador: Prof. Dr. Imre Simon.

Área de Concentração: Ciência da Computação.

São Paulo, 27 de abril de 1998.

# Grupos Maximais em Semigrupos de Burnside Livres

Este exemplar corresponde à  
redação final da tese defendida por  
Alair Pereira do Lago e aprovada  
pela comissão julgadora.

São Paulo, 27 de abril de 1998.

Comissão julgadora:

- Prof. Dr. Imre Simon (Universidade de São Paulo, Brasil)
- Prof. Dr. Said Sidki (Universidade de Brasília, Brasil)
- Prof. Dr. Jean-Eric Pin (Universidade de Paris VII, França)
- Prof. Dr. Volker Diekert (Universidade de Stuttgart, Alemanha)
- Prof. Dr. Beigel (Universidade de Lehigh, EUA)

## Resumo

Sejam inteiros  $n \geq 1$  e  $m \geq 1$  quaisquer. Provamos que um grupo maximal de um semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  é um grupo de Burnside livre satisfazendo  $x^m = 1$ . Ademais, provamos que tal grupo é livre sobre um conjunto de geradores cuja cardinalidade é o número ciclomático de um grafo associado à  $\mathcal{J}$ -classe contendo o grupo e descrevemos um tal conjunto de geradores. Caracterizamos estes grafos no caso  $n = 1$  e estendemos clássicos resultados de McLean de forma a calcular a cardinalidade do semigrupo de Burnside livre para todo  $m$  em que a cardinalidade do grupo de Burnside livre satisfazendo  $x^m = 1$  seja conhecida. Se  $n \geq 3$ , este grafo é um circuito e os grupos maximais são grupos cíclicos de ordem  $m$ .

Para todo  $m \geq 2$ , apresentamos exemplos com  $2m - 1$  geradores para  $n = 1$  e para  $n = 2$ . Donde, nestes casos, temos grupos maximais infinitos para  $m$  suficientemente grande. Assim as  $\mathcal{J}$ -classes destes grupos são infinitas, estes semigrupos não são finitos  $\mathcal{J}$ -acima e a classe de congruência associada a um elemento de uma tal  $\mathcal{J}$ -classe infinita é não-reconhecível. Também apresentaremos um exemplo de uma classe de congruência no caso  $n = 2$  e  $m = 2$  que possui duas diferentes palavras de menor comprimento. Boa parte das propriedades que valem para  $n \geq 3$  falham se  $n = 2$  e  $m \geq 2$ .

Em suma, este trabalho apresenta novas e poderosas técnicas que permitem-nos provar importantes propriedades dos semigrupos de Burnside livres para  $n = 2$ , o caso quase completamente desconhecido até agora. De certa forma, o caso  $n = 2$  surpreendentemente apresenta as complexidades dos casos  $n = 1$  e  $n \geq 3$  simultaneamente. Enquanto os grupos maximais são cíclicos de ordem  $m$  para  $n \geq 3$ , eles podem ter mais geradores e podem ser infinitos para  $n \leq 2$ . Enquanto há exatamente  $2^{|A|} - 1$   $\mathcal{J}$ -classes e elas são facilmente caracterizadas no caso  $n = 1$ , há infinitas  $\mathcal{J}$ -classes e elas são difíceis de serem caracterizadas para  $n \geq 2$ .

## Summary

Let  $n \geq 1$  and  $m \geq 1$  be any integers. We show that a maximal group of a free Burnside semigroup satisfying  $x^n = x^{n+m}$  is a free Burnside group satisfying  $x^m = 1$ . Furthermore, we show that such a group is free over a generating set whose cardinality is the cyclomatic number of a graph associated to the  $\mathcal{J}$ -class containing the group and we describe such a generating set. We characterize these graphs in the case  $n = 1$  and we extend classical results of McLean by computing the cardinality of the free Burnside semigroup for every  $m$  such that the cardinality of the free Burnside group satisfying  $x^m = 1$  is known. If  $n \geq 3$ , this graph is a circuit and the maximal groups are cyclic groups of order  $m$ .

For every  $m \geq 2$ , we present examples with  $2m - 1$  generators for  $n = 1$  and for  $n = 2$ . Therefore, in these cases, we have infinite maximal groups for  $m$  large enough. Thus the  $\mathcal{J}$ -classes of these groups are infinite, these semigroups are not finite  $\mathcal{J}$ -above and the congruence class associated with an element of such an infinite  $\mathcal{J}$ -class is not recognizable. We will also present an example of a congruence class in the case  $n = 2$  and  $m = 2$  that has two different shortest words. Many properties that hold for  $n \geq 3$  fail if  $n = 2$  e  $m \geq 2$ .

To sum up, this work presents new and powerful techniques that allows us to prove important properties of the free Burnside semigroups for  $n = 2$ , an almost completely unknown case until now. In some sense, the case  $n = 2$  presents the complexities of the cases  $n = 1$  and  $n \geq 3$  simultaneously. While the maximal groups are cyclic of order  $m$  for  $n \geq 3$ , they can have more generators and can be infinite for  $n \leq 2$ . While there are exactly  $2^{|A|} - 1$   $\mathcal{J}$ -classes which in turn are easily characterized in the case  $n = 1$ , there are infinitely many  $\mathcal{J}$ -classes which are in turn difficult to be characterized for  $n \geq 2$ .

## Agradecimentos

À Mônica

A meus pais

A todos que fazem parte de minha história

---

*Dois vocativos*

A maravilha dá de três cores:  
branca, lilás e amarela,  
seu outro nome é bonina.

Eu sou de três jeitos:  
alegre, triste e mofina,  
meu outro nome eu não sei.

Ó mistério profundo!

Ó amor!

(O coração disparado, Adélia Prado)

# Conteúdo

<b>1</b>	<b>Introdução</b>	<b>1</b>
1.1	Definições preliminares . . . . .	1
1.2	Histórico . . . . .	2
1.3	Nossos resultados . . . . .	5
1.4	Visão geral . . . . .	6
1.5	Conexões com outras áreas . . . . .	10
<b>2</b>	<b>Grafos e árvores</b>	<b>13</b>
2.1	Grafos, passeios e caminhos . . . . .	13
2.2	Árvores conectoras . . . . .	15
2.3	Número ciclomático . . . . .	19
<b>3</b>	<b>Categorias e Grupóides</b>	<b>23</b>
3.1	Categorias e morfismos de categorias . . . . .	24
3.2	Categorias livres e fatorações . . . . .	25
3.3	Congruências e funções preservadas . . . . .	26
3.4	Grupóides e grupos locais . . . . .	27
<b>4</b>	<b>Grupóides de Burnside Livres</b>	<b>29</b>
4.1	Grupóide de Burnside livre . . . . .	29
4.2	Normalização . . . . .	30
4.3	Geradores dos grupos locais . . . . .	32
4.4	Grupos locais livres . . . . .	36
<b>5</b>	<b>Entradas e transições</b>	<b>39</b>
5.1	Relações Green-induzidas . . . . .	39
5.2	Entradas . . . . .	43
5.3	Transições . . . . .	46

5.4	Sistemas de adequações . . . . .	52
<b>6</b>	<b>Monóides de Burnside Livres</b>	<b>57</b>
6.1	O monóide de Burnside livre . . . . .	58
6.2	O teorema dos marcadores . . . . .	58
6.3	Grafo fundamental . . . . .	64
6.4	Digital e inversa . . . . .	67
6.5	Regularidade no monóide de Burnside . . . . .	73
<b>7</b>	<b>Os Grupos Maximais</b>	<b>79</b>
7.1	O lema da substituição . . . . .	79
7.2	O teorema da caracterização . . . . .	92
7.3	O teorema dos grupos maximais . . . . .	96
<b>8</b>	<b>O caso <math>n = 2</math></b>	<b>105</b>
8.1	Grupo maximal com $2m - 1$ geradores . . . . .	106
8.2	Duas palavras curtas congruentes . . . . .	114
<b>9</b>	<b>Os casos <math>n = 1</math> e <math>n \geq 3</math></b>	<b>117</b>
9.1	O caso $n = 1$ . . . . .	118
9.2	O caso $n \geq 3$ . . . . .	125



# Capítulo 1

## Introdução

Neste capítulo, daremos uma breve introdução do problema que estamos estudando: a obtenção de informações estruturais de um semigrupo de Burnside livre qualquer. Antes de apresentarmos na seção 1.3 os principais resultados por nós obtidos, como a caracterização dos grupos maximais destes semigrupos, daremos algumas definições na seção 1.1 para podermos apresentar na seção 1.2 os resultados clássicos e os recentes da área. Na seção 1.4 daremos uma apresentação do conteúdo de cada capítulo deste trabalho e na seção 1.5 veremos algumas conexões com outras áreas da Ciência da Computação.

### 1.1 Definições preliminares

Daremos primeiro algumas definições necessárias aos comentários a serem feitos neste capítulo.

Seja  $A$  um alfabeto finito e sejam  $n$  e  $m$  inteiros satisfazendo as restrições  $n \geq 1$  e  $m \geq 1$ . O conjunto das palavras com letras em  $A$  (inclusive a palavra vazia  $1$ ) é denotado por  $A^*$  e  $A^+$  é o conjunto  $A^* \setminus \{1\}$ . Seja  $\pi$  a relação  $\{(x^{n+m}, x^n) \mid x \in A^+\}$  e seja  $\sim$  a menor congruência<sup>1</sup> que contém  $\pi$ . A classe de congruência de uma palavra  $w \in A^*$  será denotada por  $\tilde{w}$  e  $\mathcal{M}$  denotará o conjunto  $\{\tilde{w} \mid w \in A^*\}$ . A projeção canônica de  $A^*$  sobre  $\mathcal{M}$  induz a multiplicação  $\tilde{u} \cdot \tilde{v} = \widetilde{uv}$ . Onde  $(\mathcal{M}, \cdot)$  é um monóide e temos que  $(\mathcal{M} \setminus \{\tilde{1}\}, \cdot)$  é um semigrupo já que  $\tilde{1} = \{1\}$ . Estes são o monóide e o semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerados por  $A$ . Desde

---

<sup>1</sup>Relembramos que uma relação de congruência é uma relação de equivalência compatível com a multiplicação.

que  $\tilde{1} = \{1\}$  para  $n > 0$ , estudaremos os semigrupos de Burnside livres através dos monóides de Burnside livres. Se permitirmos  $n = 0$ , o monóide é também um grupo e é chamado de grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por  $A$ .

Dada uma relação  $R$  qualquer sobre  $A^*$ , o problema da palavra associado a  $R$  é aquele de decidir se duas palavras  $w$  e  $w'$  quaisquer são congruentes pela menor congruência que contém  $R$  ou não. De outra forma, ele é o problema de decidir se  $w = w'$  ou se existem  $k \geq 1$  e seqüências de palavras  $x_1, \dots, x_k$  e  $y_1, \dots, y_k$  e  $z_1, \dots, z_k$  e  $w_1, \dots, w_k$  tais que  $w = x_1 y_1 z_1$  e  $x_i w_i z_i = x_{i+1} y_{i+1} z_{i+1}$  para  $i = 1, \dots, k-1$  e  $w' = x_k w_k z_k$  e  $(y_i, w_i) \in R \cup R^{-1}$  para  $i = 1, \dots, k$ . Em nosso caso, a relação que nos interessa é  $\pi$ , que depende de  $n$  e  $m$ , e o problema da palavra associado ao monóide  $\mathcal{M}$  é o de decidir se  $x$  e  $y$  estão na mesma classe de congruência por  $\sim$  ou não.

Sejam as relações de Green  $\mathcal{J}$ ,  $\mathcal{D}$ ,  $\mathcal{R}$ ,  $\mathcal{L}$  e  $\mathcal{H}$  definidas como de costume. Elas são equivalências e, em particular, a  $\mathcal{J}$ -classe de um elemento  $x$  é a classe de todos os elementos  $y$  que geram o mesmo ideal principal  $MxM$ . Todas as definições e algumas propriedades serão lembradas na seção 5.1 do capítulo 5. Um semigrupo é dito *finito  $\mathcal{J}$ -acima* se suas  $\mathcal{J}$ -classes são finitas e, dada uma particular  $\mathcal{J}$ -classe, existem finitas  $\mathcal{J}$ -classes acima, onde a ordem é aquela induzida pela inclusão dos ideais principais.

## 1.2 Histórico

Vamos agora exibir algumas propriedades estruturais sobre os semigrupos e grupos de Burnside livres. Quando  $|A| = 1$ , o monóide de Burnside livre  $\mathcal{M}$  é cíclico e finito. Sua estrutura é muito simples e suporemos portanto que  $|A| > 1$  a partir de agora.

O problema de determinar se um grupo de Burnside livre finitamente gerado é finito ou não é extremamente complexo e foi levantado por Burnside em 1902. Denotemos por  $B_{k,m}$  a cardinalidade de  $B(k, m)$ , o grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um conjunto de  $k$  geradores. Na ocasião, Burnside [3] provou a finitude de  $B(k, m)$  para  $m \leq 3$ . Naturalmente que  $B(k, 1)$  é trivial e portanto  $B_{k,1} = 1$ . Como  $B(k, 2)$  é o produto direto de  $k$  cópias de  $\mathbb{Z}_2$ , temos que  $B_{k,2} = 2^k$ . Por resultado de Levi e van der Waerden [22], que pode também ser encontrado no capítulo 18 do clássico livro de M. Hall [15], temos que  $B_{k,3} = 3^{\binom{k}{1} + \binom{k}{2} + \binom{k}{3}} = 3^{\frac{m(m^2+5)}{6}}$ . Em 1940, I.N.Sanov [29] provou a finitude de  $B(k, m)$  para  $m = 4$ . M. Hall [14]

o fez para  $m = 6$  em 1958 e também provou que  $B_{k,6} = 2^a 3^{(b)+(b)+(b)}$  para  $a = 1 + (k-1)3^{(k)+(k)+(k)}$  e  $b = 1 + (k-1)2^k$ .

Por outro lado, sempre supondo  $k \geq 2$ , a infinitude de  $B(k, m)$  foi provada para  $m \geq 4381$  ímpar por Novikov e Adyan [27, 28] em 1968. Em 1975, Adyan [4, 1] melhorou a restrição para  $m \geq 665$  ímpar. Observe que isto implica a infinitude de  $B(k, mi)$  para qualquer inteiro  $i \geq 1$  e  $m \geq 665$  ímpar já que  $B(k, m)$  é imagem homomórfica de  $B(k, mi)$ . Para provar a infinitude de  $B(k, m)$  exceto para um número finito de valores de  $m$ , faltaria prová-lo para o caso em que  $m$  é uma primeira potência de 2. Em 1992, de forma independente, Ivanov [17] anunciou a prova da infinitude de  $B(2, 2^{48})$  e Lysenok [23] anunciou a prova da infinitude de  $B(2, 2^{13})$ . A partir dos trabalhos acima citados, também é demonstrado que os problemas da palavra associados aos respectivos grupos de Burnside livres estudados em cada caso são decidíveis. Isto inclui  $m \geq 665$  ímpar ou  $m \geq 2^{13}$  uma potência de 2. Como já vimos, a infinitude de  $B(k, m)$  implica a infinitude de  $B(k, mi)$  para todo inteiro  $i \geq 1$  e portanto  $B(k, m)$  é infinito sempre que  $k \geq 2$  e  $m \geq 2^{13} \times 665$ . Contudo, a solução do problema da palavra em  $B(k, m)$  não implica o mesmo em  $B(k, mi)$ , ao que se saiba hoje. Nos artigos em suas versões completas, Ivanov [18] prova a infinitude de  $B(k, m)$  para  $k \geq 2$  e qualquer  $m \geq 2^{48}$  e Lysenok [23] fá-lo para qualquer  $m \geq 8000$ . Lysenok também provou a decidibilidade do problema da palavra sempre que  $m \geq 8000$  for múltiplo de 16.

De modo a classificar a estrutura dos semigrupos de Burnside livres satisfazendo  $x^n = x^{n+m}$  temos que dividi-los em três casos:  $n = 1$ ,  $n = 2$  e  $n \geq 3$ . Nosso principal interesse aqui é o caso  $n = 2$  onde a estrutura dos semigrupos de Burnside livres era quase completamente desconhecida até agora.

Comentaremos o caso  $n = 1$  primeiro. O semigrupo idempotente — o semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  para o qual  $n = 1$  e  $m = 1$  — é finito e completamente conhecido [11] desde 1952. De fato, a partir deste clássico trabalho de Green e Rees, fixado  $m \geq 1$ , sabemos que os semigrupos de Burnside livres satisfazendo  $x = x^{1+m}$  gerados por  $A$  são finitos para todo alfabeto finito  $A$  se e só se os grupos de Burnside livres satisfazendo  $x^m = 1$  gerados por  $A$  são finitos para todo alfabeto finito  $A$ . Em particular, os semigrupos são infinitos para  $m \geq 8000$  e finitos para  $m \leq 4$ . Todavia, em qualquer caso, algumas propriedades de finitude permanecem. Por exemplo, eles possuem exatamente  $2^{|A|} - 1$   $\mathcal{J}$ -classes. No

trabalho de Green e Rees também vê-se que qualquer grupo maximal nestes semigrupos deve ser uma imagem homomórfica de um grupo de Burnside livre satisfazendo  $x^m = 1$  e suficiente número de geradores. Contudo, só em 1990, com o trabalho de Kađourek e Polák [19], provou-se que estes grupos maximais são isomorfos a um grupo de Burnside livre. Todas estas provas dependem fortemente do fato que  $n = 1$  e não podem ser facilmente estendidas para outros valores de  $n$ .

Vamos considerar agora os semigrupos de Burnside livres nos casos  $n \geq 2$ . Usando as palavras de Thue-Morse [31] e o trabalho de Brzozowski et al. [2], sabemos que estes semigrupos de Burnside livres são infinitos (estamos considerando  $|A| \geq 2$ ) e possuem infinitas  $\mathcal{J}$ -classes. Em 1970, I. Simon [30] tentou estudar o monóide de Burnside livre satisfazendo  $x^2 = x^3$  gerado por dois geradores e provou que o “frame” das  $\mathcal{R}$ -classes é uma árvore. Estas são praticamente todas as propriedades conhecidas até agora para o caso  $n = 2$ . Enquanto estes semigrupos são infinitos, Brzozowski conjecturou que algumas propriedades de finitude deveriam permanecer verdadeiras para os semigrupos de Burnside livres. Em particular, ele conjecturou que, para  $m = 1$ , qualquer classe de congruência  $\tilde{w}$  deveria ser reconhecível. Motivados pela conjectura de Brzozowski, de Luca e Varricchio [5, 7], McCammond [25], do Lago [8, 9], e Guba [13, 12] produziram uma seqüência de trabalhos que levaram ao descobrimento de muitas propriedades estruturais dos semigrupos de Burnside livres em que  $n \geq 3$  e  $m \geq 1$ . O leitor pode referir-se a nosso trabalho [10] para ver todo o histórico e as provas destas propriedades. De fato, nós efetivamente definimos um sistema de reescritura  $\Sigma$  a partir de  $\pi$  e provamos que as congruências geradas por  $\Sigma$  e por  $\pi$  são as mesmas quando  $n \geq 2$ . (Um leitor interessado nalguma introdução sobre os sistemas de reescritura pode consultar, por exemplo, uma apresentação feita por Huet [16] ou por Klop [20].) Definimos uma propriedade para  $\Sigma$ , chamada *estabilidade*, e mostramos que  $\Sigma$  é estável quando  $n \geq 3$  e  $m \geq 1$ . Algumas das propriedades que seguem a partir da estabilidade de  $\Sigma$ , sem mais hipóteses sobre os valores de  $n$  e de  $m$ , são:

1.  $\Sigma$  é um sistema de reescritura com a propriedade de Church-Rosser;
2. o problema da palavra é decidível;
3. existe uma única palavra de menor comprimento em cada classe de congruência;

4. o “frame” das  $\mathcal{R}$ -classes é uma árvore;
5. existe uma caracterização das  $\mathcal{R}$  e  $\mathcal{L}$ -classes;
6. existe uma caracterização das  $\mathcal{D}$ -classes regulares e das irregulares;
7. as  $\mathcal{H}$ -classes irregulares são todas triviais;
8. os grupos maximais são cíclicos de ordem  $m$ ;
9. o semigrupo é finito  $\mathcal{J}$ -acima;
10. a conjectura de Brzozowski é verdadeira.

O problema da estabilidade de  $\Sigma$  para  $n = 2$  e  $m = 1$  permanece aberto. Caso valha, ela implicará nosso conjunto de propriedades estruturais também neste caso. Contudo, ela não vale para  $n = 2$  e  $m \geq 2$  (como pode-se verificar em nosso trabalho [10]) e novas técnicas têm que ser encontradas nestes casos.

### 1.3 Nossos resultados

O resultado principal deste trabalho apresenta uma propriedade que vale para qualquer  $n \geq 1$  e qualquer  $m \geq 1$ . Provamos que um grupo maximal de um semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  é um grupo de Burnside livre satisfazendo  $x^m = 1$ . Isto contém os resultados de Kađourek e Polák que estudaram o caso  $n = 1$ . Ademais, provamos que tal grupo é livre sobre um conjunto de geradores cuja cardinalidade é o número ciclomático de um grafo associado à  $\mathcal{J}$ -classe contendo o grupo e apresentamos uma descrição explícita de um tal conjunto de geradores. Fruto de uma caracterização dos grafos fundamentais no caso  $n = 1$ , estendemos o resultado de McLean [26] e calculamos a cardinalidade do monóide de Burnside livre para todo  $m$  em que a cardinalidade de qualquer grupo de Burnside livre satisfazendo  $x^m = 1$  é conhecida. Se  $\Sigma$  é estável (em particular, para  $n \geq 3$ ), este grafo é um circuito e os grupos maximais são grupos cíclicos de ordem  $m$ .

Nossa prova vale para qualquer  $n \geq 1$  e qualquer  $m \geq 1$ . Isto é particularmente interessante já que as técnicas anteriores somente poderiam ser aplicadas aos casos particulares a que se destinavam.

Para todo  $m \geq 2$ , apresentamos exemplos com  $2m - 1$  geradores para  $n = 1$  e para  $n = 2$ . Donde, nestes casos, temos grupos maximais

infinitos para  $m$  suficientemente grande. Isto imediatamente implica que as  $\mathcal{J}$ -classes destes grupos são infinitas, que estes semigrupos não são finitos  $\mathcal{J}$ -acima e também que a classe de congruência associada a um elemento de um tal grupo infinito é não-reconhecível. Também apresentaremos um exemplo de uma classe de congruência no caso  $n = 2$  e  $m = 2$  que possui duas diferentes palavras de menor comprimento. Boa parte das propriedades que valem se  $\Sigma$  é estável falham se  $n = 2$  e  $m \geq 2$ .

Encontrar estes exemplos no caso  $n = 2$  requereram o uso de poderosos recursos computacionais. Contudo, todas as afirmativas relativas a estes exemplos serão aqui provadas.

Em suma, este trabalho apresenta novas e poderosas técnicas que permitem-nos provar importantes propriedades dos semigrupos de Burnside livres para  $n = 2$ , o caso quase completamente desconhecido até agora. De certa forma, o caso  $n = 2$  surpreendentemente apresenta as complexidades dos casos  $n = 1$  e  $n \geq 3$  simultaneamente. Enquanto os grupos maximais são cíclicos de ordem  $m$  para  $n \geq 3$ , eles podem ter mais geradores e podem ser infinitos para  $n \leq 2$ . Enquanto existem exatamente  $2^{|A|} - 1$   $\mathcal{J}$ -classes e elas são facilmente caracterizadas no caso  $n = 1$ , existem infinitas  $\mathcal{J}$ -classes e elas são difíceis de serem caracterizadas para  $n \geq 2$ .

## 1.4 Visão geral

No capítulo 2 daremos as definições usuais da teoria de grafos que serão necessárias em nosso trabalho. As aplicações destes conceitos aparecerão primeiramente nas categorias e nos grupóides, que serão estudados e definidos nos capítulos 3 e 4. Posteriormente, elas aparecerão no estudo do grafo fundamental de uma  $\mathcal{D}$ -classe, a ser visto na seção 6.3 do capítulo 6. Estes grafos podem vir a ser infinitos, teoricamente. Infelizmente, a maior parte da literatura de teoria de grafos disponível trata apenas de grafos finitos. Assim, após as definições da seção 2.1, veremos na seção 2.2 alguns resultados elementares da teoria de grafos, que não supõem nenhuma restrição quanto às cardinalidades dos grafos. Estes resultados elementares não consideram passeios infinitos, muitas vezes presentes na teoria de grafos infinitos, e são necessários à boa definição do conceito de número ciclomático de um grafo, na seção 2.3. Este conceito de número ciclomático aparecerá em resultados importantes do nosso trabalho, como nos teoremas 4.7 e 7.6.

No capítulo 3, veremos as definições de categorias e grupóides ne-

cessárias a nosso trabalho. O conceito de categoria generaliza o de monóide e veremos aplicadas às categorias as definições de vários conceitos já conhecidos na teoria de monóides. Isto inclui o de congruência. Nosso objetivo não era, a princípio, o estudo de categorias e grupóides, mas a estrutura dos monóides de Burnside livres. Durante este estudo, apareceram de forma natural alguns grafos — como o grafo fundamental de uma  $\mathcal{D}$ -classe como será visto na seção 6.3 do capítulo 6 — e algumas categorias — como a categoria livre gerada por um grafo e o grupóide de Burnside livre gerado por este grafo. Achamos por bem explicitar estes conceitos, até porque alguns resultados, expressos na linguagem das categorias, poderiam ter suficiente interesse do ponto de vista da teoria de categorias e grupóides. É o caso do teorema 4.7 a ser visto no capítulo 4. O leitor poderá encontrar mais informações sobre categorias no clássico livro de MacLane [24] e importantes resultados conectando a teoria de categorias com a teoria de monóides no trabalho de Tilson [32].

No capítulo 4, definimos um grupóide especial: o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por um grafo fortemente conexo. O resultado principal do capítulo, o teorema 4.7, afirma que os grupos locais deste grupóide são todos isomorfos a um mesmo grupo de Burnside livre satisfazendo  $x^m = 1$ . Também é caracterizado um conjunto de geradores para este grupo livre.

No capítulo 5 começamos a focar nossa atenção ao monóide de Burnside livre propriamente dito. As definições e os resultados presentes no capítulo exigem menos hipóteses porém: supomos apenas que o monóide em questão seja estável. Esta generalidade vale em particular para o resultado que consideramos maximal no capítulo: o lema 5.14. Na seção 5.1 daremos as definições preliminares do capítulo e definiremos as relações Green-induzidas, que dão ao monóide livre  $A^*$  uma estrutura induzida pelas relações de Green no monóide  $\mathcal{M}$  e por um morfismo de  $A^*$  sobre  $\mathcal{M}$ . Nas seções 5.2 e 5.3 veremos as definições das  $\mathcal{D}$ -entradas e das transições e sobre estes conceitos se fundará a constituição de um grafo fundamental de uma  $\mathcal{D}$ -classe de um monóide de Burnside livre, como será visto na seção 6.3 do capítulo 6. Na seção 5.4 veremos uma aplicação importante das transições de uma palavra: o lema 5.14 acima mencionado. Este lema será usado na demonstração do teorema 7.5.

No capítulo 6 apresentaremos o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por um alfabeto  $A$ , para inteiros  $n \geq 1$  e  $m \geq 1$ . Após a definição na seção 6.1, apresentaremos o teorema dos marcadores

(teorema 6.3) na seção 6.2, que prova que uma propriedade do semigrupo idempotente seja válida também para qualquer monóide de Burnside livre. Este resultado era fundamentalmente conhecido desde 1970, quando I. Simon [30] obteve algumas propriedades do semigrupo de Burnside livre satisfazendo  $x^2 = x^3$  gerado por dois geradores. Na seção 6.3 veremos a definição de um conceito central em nosso trabalho: o grafo fundamental de uma  $\mathcal{D}$ -classe de um monóide de Burnside livre. O grafo fundamental se mostrará fortemente conexo como veremos na proposição 6.8 e poderemos futuramente definir o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por este grafo. Veremos também alguns conceitos e propriedades correlatas. Por exemplo, associaremos a uma palavra  $w$  um passeio no grafo fundamental da  $\mathcal{D}$ -classe de  $\tilde{w}$ . Esta é a digital de  $w$  e é um conceito fundamental para caracterizar se duas palavras  $\mathcal{D}'$ -equivalentes são congruentes ou não, como veremos no teorema 7.5 a ser visto no capítulo 7. Vemos também como construir a menor palavra que possui uma certa digital e esta construção será essencial à demonstração da existência de uma classe de congruência com duas palavras de menor comprimento, a ser visto no capítulo 8. Na seção 6.5 veremos algumas propriedades relativas à regularidade de uma  $\mathcal{D}$ -classe de um monóide de Burnside livre. Em particular, na proposição 6.13 veremos que as  $\mathcal{H}$ -classes irregulares são triviais e na proposição 6.14 provamos que qualquer grafo fundamental de uma  $\mathcal{D}$ -classe irregular não possui nenhuma aresta e possui um único vértice.

No capítulo 7 provaremos dois dos resultados mais importantes deste trabalho: o teorema da caracterização (teorema 7.5) e o teorema dos grupos maximais (teorema 7.6). Na demonstração do teorema da caracterização, usaremos vários conceitos vistos no trabalho. Explicitando alguns: o grafo fundamental de uma  $\mathcal{D}$ -classe e o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por este grafo. Este teorema caracteriza quando duas palavras projetadas na mesma  $\mathcal{D}$ -classe são congruentes pela congruência de Burnside. Esta caracterização depende de um conhecimento do grafo fundamental da  $\mathcal{D}$ -classe em questão. Já na seção 7.3 veremos o teorema dos grupos maximais, que não somente usa o teorema da caracterização em sua demonstração, mas também usa o teorema 4.7 visto no capítulo 4. O teorema 7.6 afirma que um grupo maximal num semigrupo de Burnside livre satisfazendo  $x^{n+m} = x^n$  é um grupo de Burnside livre satisfazendo  $x^m = 1$ . Observe que este resultado é conforme aquele já conhecido para  $n \geq 3$  e  $m \geq 1$  onde, pelo teorema 8.16 [10], sabe-se que qualquer grupo maximal é cíclico de ordem  $m$  (o grupo de Burnside livre satisfazendo  $x^m = 1$  gerado



por um único elemento). Há uma substancial evolução no teorema dos grupos maximais já que o mesmo vale para quaisquer  $n \geq 1$  e  $m \geq 1$  e os casos  $n = 1$  e  $n = 2$  têm estruturas muito diferentes daquela vista para  $n \geq 3$  e  $m \geq 1$ . No caso geral, o conjunto sobre o qual o grupo de Burnside é livre pode ter mais que um gerador, ao contrário do caso  $n \geq 3$  e  $m \geq 1$ . Ademais, é caracterizado um conjunto gerador para este grupo de Burnside livre e a cardinalidade do conjunto é o número ciclomático do grafo fundamental da  $\mathcal{D}$ -classe que contém a  $\mathcal{H}$ -classe em questão. Esta diferença se mostra relevante já que no teorema 8.1 a ser visto no capítulo 8 vemos uma  $\mathcal{D}$ -classe regular cujo grafo fundamental tem número ciclomático  $2m - 1$  pelo menos.

No capítulo 8 apresentamos o exemplo de uma  $\mathcal{D}$ -classe regular do monóide de Burnside livre satisfazendo  $x^2 = x^{2+m}$  gerado por um alfabeto de duas letras cujo grafo fundamental tem número ciclomático  $2m - 1$  ao menos. Como consequência, o teorema 7.6 implica que os grupos maximais desta  $\mathcal{D}$ -classe são grupos de Burnside livres satisfazendo  $x^m = 1$  com ao menos  $2m - 1$  geradores. Como discutimos antes, para  $m$  suficientemente grande, sabemos que estes grupos são infinitos pois eles possuem ao menos dois geradores. A proposição 7.8 do capítulo 7 implica então que toda classe de congruência cuja projeção canônica é mapeada num elemento desta  $\mathcal{D}$ -classe com  $\mathcal{H}$ -classes infinitas não é reconhecível. Ao final, veremos o exemplo de uma classe de congruência com duas palavras de menor comprimento. Estes resultados todos contrastam com os monóides de Burnside livres satisfazendo  $x^n = x^{n+m}$  nos casos em que  $n \geq 3$  e  $m \geq 1$  pois, nestes casos, os grupos maximais têm um único gerador (teorema 8.16 [10]), toda classe de congruência é reconhecível (teorema 8.18 [10]) e possui uma única palavra de menor comprimento (teorema 7.3 [10]).

No capítulo 9 aplicaremos os resultados principais deste trabalho a semigrupos de Burnside livres cujas estruturas são bastante conhecidas. Dedicaremos-nos a estudar os casos  $n = 1$  e  $n \geq 3$ . Na seção 9.1 consideraremos o caso  $n = 1$  e caracterizaremos o grafo fundamental de uma  $\mathcal{D}$ -classe de um semigrupo de Burnside livre satisfazendo  $x = x^{m+1}$  no teorema 9.2. Em particular, calcularemos seu número ciclomático. Caso seja conhecida a cardinalidade do grupo de Burnside  $B(k, m)$  para todo inteiro  $k \geq 1$ , calcularemos no corolário 9.3 a cardinalidade de cada  $\mathcal{J}$ -classe de  $\mathcal{M}$  — e portanto a cardinalidade do próprio monóide de Burnside  $\mathcal{M}$ . Isto implica que conheçamos a cardinalidade de  $\mathcal{M}$  em função de  $|A|$  nos casos  $m \leq 3$ , por exemplo. Em 1954, McLean [26] deu uma descrição da cardinalidade de  $\mathcal{M}$  em função de  $|A|$  para o caso  $n = m = 1$  (banda livre com  $|A|$  geradores).

Generalizamos este resultado para qualquer  $m \geq 1$  em que a cardinalidade de  $B(k, m)$  seja conhecida. Para  $m$  suficientemente grande e três geradores em  $A$  ao menos, verificamos que em  $\mathcal{M}$  existe uma  $\mathcal{J}$ -classe com um número infinito de  $\mathcal{R}$ -classes e de  $\mathcal{L}$ -classes. Ademais, toda  $\mathcal{H}$ -classe nesta  $\mathcal{J}$ -classe é um grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um conjunto infinito de geradores. No corolário 9.4 veremos um resultado de Káďourek e Polák [19] que reduz o problema da palavra em  $\mathcal{M}$  ao problema da palavra num grupo de Burnside livre  $B(k, m)$  para  $k$  finito. Isto implica que o problema da palavra seja decidível em  $\mathcal{M}$  mesmo em casos em que  $\mathcal{M}$  é infinito, como nos casos em que  $m \geq 665$  é ímpar ou em que  $m \geq 8000$  é um múltiplo de 16. Na seção 9.2, suporemos  $n \geq 1$  e  $m \geq 1$  e daremos uma nova demonstração do teorema 8.16 [10] que prova que os grupos maximais de um semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  são todos cíclicos de ordem  $m$  quando  $n \geq 3$ . Para tanto, caracterizaremos no teorema 9.5 o grafo fundamental de uma  $\mathcal{D}$ -classe regular do semigrupo de Burnside livre e provaremos que ele é um circuito.

## 1.5 Conexões com outras áreas

Para concluir a introdução, gostaríamos de apontar algumas conexões e motivações desta área, relacionadas à Ciência da Computação. O estudo de periodicidades em palavras aparece em muitas áreas importantes da Ciência da Computação como, por exemplo, busca de padrão e algoritmos de busca. As estruturas de Burnside são definidas por equações que impõem a equivalência de certas potências de palavras em qualquer contexto como acabamos de ver. Este trabalho juntamente com anteriores trabalhos prova que estas estruturas de Burnside comportam-se de forma muito diferente dependendo da quantidade de períodos envolvidos (medidos pelos valores de  $m$  e de  $n$ ). Em vista desta variação, a compreensão da combinatória subjacente é uma intrigante aventura e pode também trazer importantes luzes à compreensão de outras questões da Ciência da Computação que dependam de períodos.

Relembre que o problema da palavra para uma dada relação de palavras é indecidível em geral, mesmo para uma relação finita. Em nosso caso, a relação é  $\pi$ , que depende de  $n$  e  $m$ , e a resposta a este problema da palavra depende fortemente dos valores de  $n$  e  $m$ , como descrito anteriormente.

Uma importante consequência da conjectura de Brzozowski é uma

aplicação que permite uma fácil solução do problema da palavra. De fato, se provarmos construtivamente a conjectura de Brzozowski, temos um autômato finito, dependente de  $x$ , que resolve esta instância do problema da palavra. Isto inclui os casos onde  $n \geq 3$ . Infelizmente, na maior parte dos casos onde  $n = 1$  ou  $n = 2$ , a conjectura de Brzozowski não vale. Contudo, possivelmente, podemos ainda resolver o problema da palavra. Suponha que o grafo fundamental possa ser efetivamente obtido e que o problema da palavra seja decidível para  $n = 0$  e  $m \geq 1$ . Então o teorema 7.5 implica que o problema da palavra é decidível para  $n \geq 1$  e para o mesmo  $m$ . Em particular, isto vale quando  $n = 1$  e  $m$  é ímpar e grande o suficiente, apesar da conjectura de Brzozowski não valer neste caso. Para casos como  $n = 2$ , o problema da palavra permanece aberto.

Este capítulo apresenta uma introdução ao estudo da teoria dos grupos. O objetivo principal é estabelecer os conceitos básicos e as propriedades fundamentais que caracterizam um grupo. A abordagem é feita de forma intuitiva, com exemplos concretos que ajudam a visualizar as abstrações matemáticas envolvidas. O texto discute a importância dos grupos em diversas áreas da matemática e da física, mostrando como eles fornecem uma estrutura poderosa para a análise de simetrias e transformações. Além disso, são introduzidos os conceitos de subgrupo, homomorfismo e isomorfismo, que são essenciais para a compreensão da estrutura interna dos grupos e suas relações com outros grupos. O capítulo termina com uma série de exercícios que permitem ao leitor aplicar os conceitos aprendidos e explorar propriedades mais avançadas dos grupos.

# Capítulo 2

## Grafos e árvores

Neste capítulo daremos as definições usuais da teoria de grafos que serão necessárias a nosso trabalho. As aplicações destes conceitos aparecerão primeiramente nas categorias e nos grupóides, que serão estudados nos capítulos 3 e 4. Posteriormente, elas aparecerão no estudo do grafo fundamental de uma  $\mathcal{D}$ -classe, a ser visto na seção 6.3 do capítulo 6.

Estes grafos podem vir a ser infinitos, teoricamente. Infelizmente, a maior parte da literatura de teoria de grafos disponível trata apenas de grafos finitos. Assim, após as definições da seção 2.1, veremos na seção 2.2 alguns resultados elementares da teoria de grafos, que não supõem nenhuma restrição quanto à cardinalidade do grafo em questão. Estes resultados elementares não consideram passeios infinitos, muitas vezes presentes na teoria de grafos infinitos, e são necessários à boa definição do conceito de número ciclomático de um grafo, na seção 2.3. Este conceito de número ciclomático aparecerá em resultados importantes do nosso trabalho, como nos teoremas 4.7 e 7.6.

Nosso enfoque sobre os grafos privilegiará seu conjunto de arestas, se compararmos com a teoria usual de grafos. Seus vértices praticamente servem apenas para caracterizar a consecutividade ou não de duas arestas. Nossos grafos são dirigidos.

### 2.1 Grafos, passeios e caminhos

Um *grafo dirigido*, ou simplesmente *grafo*, é uma upla  $(V, E, \alpha, \omega)$  onde  $V$  e  $E$  são conjuntos quaisquer munidos de duas funções  $\alpha : E \rightarrow V$  e  $\omega : E \rightarrow V$ . Cada elemento de  $E$  é chamado *aresta de G* e cada elemento de  $V$  é chamado

*vértice* de  $\mathbf{G}$ . O conjunto  $E(\mathbf{G}) = E$  é chamado de *conjunto de arestas* de  $\mathbf{G}$ , o conjunto  $V(\mathbf{G}) = V$  é chamado de *conjunto de vértices* de  $\mathbf{G}$ . As funções  $\alpha$  e  $\omega$  são ditas *início* e *término* respectivamente e também são chamadas genericamente de *funções de incidência*.

Referimo-nos à cardinalidade de  $\mathbf{G}$  como a cardinalidade  $|E(\mathbf{G})|$  de seu conjunto de arestas. Em nosso trabalho, não faremos a priori nenhuma restrição quanto às cardinalidades dos grafos e, usualmente, não teremos nenhum vértice isolado (vértice sem a incidência de nenhuma aresta). Normalmente confundiremos o grafo  $\mathbf{G}$  com seu conjunto de arestas  $E(\mathbf{G})$  deixando implícitas as funções início, término e o conjunto de vértices  $V(\mathbf{G})$ . Quando não explicitado o conjunto de vértices, estaremos supondo  $V(\mathbf{G}) = \alpha(\mathbf{G}) \cup \omega(\mathbf{G})$  onde  $\alpha(\mathbf{G})$  denota o conjunto  $\alpha(E(\mathbf{G}))$  e  $\omega(\mathbf{G})$  denota o conjunto  $\omega(E(\mathbf{G}))$ . Denotaremos que  $b$  é uma aresta do grafo  $\mathbf{G}$  por  $b \in \mathbf{G}$ . Dados dois grafos distintos, freqüentemente nos permitiremos usar os mesmos símbolos  $\alpha$  e  $\omega$  para denotar as funções início (ou término) de ambos.

Seja  $\mathbf{G}$  um grafo. Duas arestas  $x, y \in \mathbf{G}$  são ditas *consecutivas* (e nesta ordem) se  $\omega(x) = \alpha(y)$ . Chamamos de *passeio em  $\mathbf{G}$*  ou simplesmente *passeio* toda seqüência finita de arestas consecutivas de  $\mathbf{G}$ . Sobre cada passeio  $p = b_1 b_2 \cdots b_k$ ,  $k \geq 1$  definimos o *início do passeio*  $\alpha(p) = \alpha(b_1)$  e o *término do passeio*  $\omega(p) = \omega(b_k)$ . Para cada vértice  $v \in V(\mathbf{G})$  definimos  $1_v$  um *passeio vazio local a  $v$* , com início e término em  $v$ . O comprimento de um passeio é o tamanho da seqüência de arestas, sendo que o comprimento dos passeios vazios é 0. Dizemos que dois passeios  $p, q$  são consecutivos (e nesta ordem) se  $\omega(p) = \alpha(q)$ . Dados dois passeios consecutivos  $p$  e  $q$  definimos sua concatenação  $pq$  de forma natural. Observe que  $pq$  começa em  $\alpha(p)$  e termina em  $\omega(q)$ . Não é definida a concatenação de passeios não consecutivos. Observe que se  $p, q$  e  $r$  são passeios consecutivos nesta ordem, então  $(pq)r = p(qr)$ , que equivale a dizer que a operação parcial da concatenação de passeios é associativa quando todas as concatenações são definidas. Quando  $p$  é um passeio que inicia e termina no mesmo vértice  $v$  dizemos que  $p$  é um *passeio fechado sobre  $v$*  ou simplesmente um *passeio fechado*. Uma aresta com mesmo início e término é chamada de *laço*. Um grafo  $\mathbf{G}$  é dito *fortemente conexo* se tem ao menos um vértice e se, para todo par ordenado de vértices, existe um passeio com início no primeiro vértice e término no segundo. Observe que o menor grafo fortemente conexo é o grafo com um único vértice e nenhuma aresta.

Dado um passeio  $p = b_1 b_2 \cdots b_k$ , com  $k \geq 0$ , o conjunto dos vértices

internos de  $p$  é  $\{\omega(b_1), \omega(b_2), \dots, \omega(b_{k-1})\}$ . Dizemos que  $p$  é um *caminho* se os vértices percorridos são sempre distintos; ou seja, para todos  $1 \leq i, j \leq k$  temos que  $\omega(b_i) = \alpha(b_j) \iff i = j - 1$ . Observe que este passeio não pode ser fechado a menos que seja um passeio vazio. Dois passeios  $p, q$  são ditos *coterminais* se têm mesmo início e mesmo término. Dado um passeio  $p = b_1 b_2 \cdots b_k$  sempre existe uma subsequência de  $p$  que seja um caminho coterminal a  $p$ . Um algoritmo simples para a obtenção de um tal caminho é o seguinte: enquanto existirem  $i$  e  $j$  (com  $1 \leq i, j \leq k$  e  $i \neq j - 1$ ) tais que  $\omega(b_i) = \alpha(b_j)$  remova de  $p$  a subsequência não vazia  $b_{i+1} \cdots b_{j-1}$  se  $i < j$  ou a subsequência não vazia  $b_j \cdots b_i$  se  $i \geq j$ . Após cada uma destas remoções,  $p$  continua sendo um passeio com os mesmos início e término. Este algoritmo de fato pára pois as remoções feitas a cada passo são não vazias e ao final do algoritmo o passeio satisfaz a condição necessária para ser um caminho. Um tal caminho que é subsequência do passeio  $p$  será chamado *um caminho associado ao passeio  $p$* . Dados dois vértices  $v, u$  dizemos que a distância de  $v$  a  $u$  é o comprimento do passeio mais curto que inicia em  $v$  e termina em  $u$ .

## 2.2 Árvores conectoras

Dados dois grafos  $\mathbf{T}$  e  $\mathbf{G}$  dizemos que  $\mathbf{T}$  é um *subgrafo de  $\mathbf{G}$*  se  $V(\mathbf{T}) \subseteq V(\mathbf{G})$ , se  $E(\mathbf{T}) \subseteq E(\mathbf{G})$  e se as funções de incidência de  $\mathbf{T}$  forem restrições naturais das funções de incidência de  $\mathbf{G}$ . Neste caso, denotamos  $\mathbf{T} \subseteq \mathbf{G}$  e temos que  $\alpha(\mathbf{T}) \cup \omega(\mathbf{T}) \subseteq V(\mathbf{T}) \subseteq V(\mathbf{G})$ . Se além disso tivermos que  $\alpha(\mathbf{T}) \cup \omega(\mathbf{T}) = V(\mathbf{T})$ , dizemos que  $\mathbf{T}$  é o *subgrafo de  $\mathbf{G}$  induzido por  $E(\mathbf{T})$* , com  $E(\mathbf{T}) \subseteq E(\mathbf{G})$ . Dados os grafos  $\mathbf{T} \subseteq \mathbf{G}$  denotamos por  $\mathbf{G} \setminus \mathbf{T}$  o subgrafo de  $\mathbf{G}$  induzido pelas arestas  $E(\mathbf{G}) \setminus E(\mathbf{T})$ .

Seja  $\mathbf{T}$  um subgrafo de  $\mathbf{G}$  e seja  $v \in V(\mathbf{T}) \subseteq V(\mathbf{G})$  um vértice. Denotaremos por  $\omega_v(\mathbf{T}) \subseteq V(\mathbf{T})$  o conjunto dos términos dos passeios em  $\mathbf{T}$  que começam em  $v$  (usando arestas apenas de  $\mathbf{T}$ ) e por  $\alpha_v(\mathbf{T}) \subseteq V(\mathbf{T})$  o conjunto dos inícios dos passeios em  $\mathbf{T}$  que terminam em  $v$ . Dizemos que  $\mathbf{T}$  é uma *árvore com início  $v$*  se existe exatamente um passeio em  $\mathbf{T}$  de  $v$  a qualquer vértice de  $V(\mathbf{T})$  e dizemos que  $\mathbf{T}$  é uma *árvore com término  $v$*  se existe exatamente um passeio em  $\mathbf{T}$  de qualquer vértice de  $V(\mathbf{T})$  a  $v$ . Dizemos que  $\mathbf{T}$  é uma *árvore com raiz  $v$*  se  $\mathbf{T}$  for uma árvore com início  $v$  ou uma árvore com término  $v$ . Dizemos que  $\mathbf{T}$  é uma *árvore* se existe  $v \in V(\mathbf{G})$  tal que  $\mathbf{T}$  seja uma árvore com raiz  $v$  e dizemos que  $\mathbf{T}$  é uma *árvore conectora de  $\mathbf{G}$*  (ou simplesmente *árvore conectora* se  $\mathbf{G}$  for evidente)

se  $\mathbf{T}$  for uma árvore e se  $V(\mathbf{T}) = V(\mathbf{G})$ . Na teoria de grafos uma árvore conectora é usualmente chamada de árvore geradora. Esta terminologia não será usada aqui para evitar confusão com conjuntos geradores de um monóide ou categoria.

Seja  $\mathbf{G}$  um grafo com funções de incidência  $\alpha$  e  $\omega$  e sejam  $\mathbf{T} \subseteq \mathbf{G}$  e  $V \subseteq V(\mathbf{T}) \subseteq V(\mathbf{G})$ . Dizemos que  $\alpha$  é *injetiva em  $\mathbf{T}$*  se a sua restrição a  $\mathbf{T}$  for injetiva e dizemos que  $\alpha$  é uma *bijecção de  $\mathbf{T}$  em  $V$*  se ela for injetiva em  $\mathbf{T}$  e se  $\alpha(\mathbf{T}) = V$ . A mesma terminologia será usada para  $\omega$ .

Apresentaremos alguns resultados elementares da teoria de grafos que, no entanto, são enunciados apenas para grafos finitos usualmente. Em nossas hipóteses, os grafos podem ser infinitos. Até mesmo não-enumeráveis. Estes resultados são necessários à correta definição do número ciclomático de um grafo.

**Proposição 2.1** *Sejam  $\mathbf{G}$  um grafo,  $v \in V(\mathbf{G})$  um vértice e  $\mathbf{T} \subseteq \mathbf{G}$  uma árvore com início  $v$ . Então*

$$\alpha(\mathbf{T}) \subseteq \omega(\mathbf{T}) \cup \{v\} = \omega_v(\mathbf{T}) = V(\mathbf{T}).$$

*Prova.* Por definição,  $\alpha(\mathbf{T}), \omega(\mathbf{T}), \omega_v(\mathbf{T}) \subseteq V(\mathbf{T})$ . Como  $\mathbf{T}$  é uma árvore com início  $v$ , temos que  $v \in V(\mathbf{T})$ . Ademais, existe um passeio de  $v$  a qualquer vértice de  $V(\mathbf{T})$  e portanto  $V(\mathbf{T}) \subseteq \omega_v(\mathbf{T})$ . Ora, todo passeio que inicia em  $v$  ou é vazio e portanto termina em  $v$ , ou tem uma última aresta e portanto termina num vértice de  $\omega(\mathbf{T})$ . Donde temos que  $\omega_v(\mathbf{T}) \subseteq \omega(\mathbf{T}) \cup \{v\}$ . ■

Observe que podemos formular um resultado dual ao da proposição 2.2 para árvores com término  $v$ . Enfatizamos que o grafo  $\mathbf{G}$  em questão pode ser infinito, e até mesmo não-enumerável. A afirmativa 2 implica que a cardinalidade de qualquer árvore conectora é sempre a mesma:  $|V(\mathbf{G})| - 1$ .

**Proposição 2.2** *Sejam  $\mathbf{G}$  um grafo,  $v \in V(\mathbf{G})$  um vértice,  $T \subseteq E(\mathbf{G})$  um conjunto de arestas e  $\mathbf{T}$  o grafo induzido por  $T$ . Então as afirmativas 1 e 2 são sempre equivalentes e equivalem à afirmativa 3 no caso de  $T$  ser finito:*

1.  $\mathbf{T}$  é uma árvore com início  $v$ ;
2.  $\omega_v(\mathbf{T}) = \omega(\mathbf{T}) \cup \{v\}$  e  $v \notin \omega(\mathbf{T})$  e  $\omega$  é injetiva em  $\mathbf{T}$ ;
3.  $|\omega_v(\mathbf{T})| = |T| + 1$ .



*Prova.* Suponha que a afirmativa 1 seja válida. Vamos provar que a afirmativa 2 seja válida. Da proposição 2.1 temos que  $\omega_v(\mathbf{T}) = \omega(\mathbf{T}) \cup \{v\}$ . Suponha por absurdo que exista uma aresta  $a \in \mathbf{T}$  tal que  $\omega(a) = v$ . Como  $\mathbf{T}$  é uma árvore com início  $v$ , podemos tomar  $p$  o único passeio de  $v$  a  $\alpha(a)$  em  $\mathbf{T}$  e temos que  $p$  e  $pap$  são dois diferentes passeios de  $v$  a  $\alpha(a)$  em  $\mathbf{T}$ , uma contradição com  $\mathbf{T}$  ser uma árvore com início  $v$ . Assim temos que  $v \notin \omega(\mathbf{T})$ . Suponha por absurdo que existam duas arestas distintas  $a, a' \in \mathbf{T}$  tais que  $\omega(a) = \omega(a')$ . Tomando  $p$  e  $p'$  os dois passeios em  $\mathbf{T}$  de  $v$  a  $\alpha(a)$  e a  $\alpha(a')$  respectivamente, temos que  $p'a'$  e  $pa$  são dois diferentes passeios em  $\mathbf{T}$  de  $v$  a  $\omega(a)$  e temos nova contradição. Desta forma temos que  $\omega$  é injetiva em  $\mathbf{T}$ .

Suponha que a afirmativa 2 seja válida. Vamos provar que a afirmativa 1 seja válida. Seja  $u \in \omega_v(\mathbf{T})$ . Primeiro provaremos, por indução na distância  $d$  de  $v$  a  $u$ , que é único o passeio em  $\mathbf{T}$  de  $v$  para  $u$ . Caso  $d = 0$ , dado que  $v \notin \omega(\mathbf{T})$  temos que só o passeio vazio termina em  $v$ . Temos a base da indução. Suporemos agora que  $d > 0$  e que o resultado seja verdadeiro para todos os vértices que distam no máximo  $d - 1$  de  $v$ . Seja  $p$  um passeio qualquer em  $\mathbf{T}$  de  $v$  a  $u$  e seja  $q$  um passeio de comprimento  $d$  de  $v$  a  $u$  em  $\mathbf{T}$ . Como  $\omega$  é uma injeção em  $\mathbf{T}$ , existe exatamente uma aresta  $a \in \mathbf{T}$  que termina em  $u$ . Como  $d > 0$ , os passeios  $p$  e  $q$  são não vazios e temos que  $q$  e  $p$  têm a mesma última aresta  $a$ . Assim  $pa^{-1}$  e  $qa^{-1}$  são dois passeios de  $v$  para o mesmo vértice  $\alpha(a)$ . Como  $qa^{-1}$  tem comprimento  $d - 1$ , temos que a distância de  $v$  a  $\alpha(a)$  é menor ou igual a  $|qa^{-1}| = d - 1$ . Pela hipótese de indução temos que  $qa^{-1} = pa^{-1}$  e portanto que  $p = q$ . Isto prova que é único o passeio em  $\mathbf{T}$  de  $v$  a qualquer vértice de  $\omega_v(\mathbf{T})$ . É suficiente portanto provar que  $V(\mathbf{T}) \subseteq \omega_v(\mathbf{T})$ . Como  $V(\mathbf{T}) = \alpha(\mathbf{T}) \cup \omega(\mathbf{T})$  por  $\mathbf{T}$  ser um subgrafo induzido, como  $\omega_v(\mathbf{T}) = \omega(\mathbf{T}) \cup \{v\}$  por hipótese, para concluir a prova de que  $\mathbf{T}$  é uma árvore com início  $v$ , basta provar que  $\alpha(\mathbf{T}) \subseteq \omega_v(\mathbf{T})$ . Seja  $x$  um vértice qualquer de  $\alpha(\mathbf{T})$  e seja  $a \in \mathbf{T}$  uma aresta tal que  $\alpha(a) = x$ . Como  $\omega(a) \in \omega(\mathbf{T}) \subset \omega_v(\mathbf{T})$ , seja  $p$  o único passeio de  $v$  a  $\omega(a)$ . Como  $v \notin \omega(\mathbf{T})$ , temos que  $v \neq \omega(a)$ . Portanto  $p$  é não vazio e sua última aresta termina em  $\omega(a)$ . Como  $\omega$  é uma injeção em  $\mathbf{T}$ , temos que esta última aresta é  $a$  e que o passeio  $pa^{-1}$  inicia em  $v$  e termina em  $x$ . Assim  $\alpha(\mathbf{T}) \subseteq \omega_v(\mathbf{T})$ , completando a prova de que  $\mathbf{T}$  é uma árvore com início  $v$ .

Suponhamos agora que  $T$  seja finito. Vamos provar que as afirmativas 2 e 3 são equivalentes. Suponha que a afirmativa 2 seja válida. Como  $\omega$  é injetiva em  $\mathbf{T}$  temos que  $|\omega(\mathbf{T})| = |\mathbf{T}|$ . Como  $v \notin \omega(\mathbf{T})$ , temos que  $|\omega_v(\mathbf{T})| = |\omega(\mathbf{T}) \cup \{v\}| = |\omega(\mathbf{T})| + 1 = |\mathbf{T}| + 1$ . Suponha agora que a afirmativa 3 seja válida. Como todo passeio que inicia em  $v$  ou é vazio e portanto

termina em  $v$ , ou tem uma última aresta e portanto termina num vértice de  $\omega(\mathbf{T})$ , temos que  $\omega_v(\mathbf{T}) \subseteq \omega(\mathbf{T}) \cup \{v\}$ . Como  $\omega(\mathbf{T}) = \omega(E(\mathbf{T})) = \omega(T)$ , como  $|\omega_v(\mathbf{T})| = |T| + 1$  por hipótese, sempre por argumento de cardinalidade, temos que: a união  $\omega(\mathbf{T}) \cup \{v\}$  é disjunta;  $|\omega(\mathbf{T})| = |T|$  e portanto  $\omega$  é uma injeção em  $\mathbf{T}$ ; e  $\omega_v(\mathbf{T}) = \omega(\mathbf{T}) \cup \{v\}$ . ■

A proposição 2.3 fornece uma caracterização de grafos fortemente conexos em termos de árvores conectoras. Isto em particular implica que todo grafo fortemente conexo tem uma árvore conectora.

**Proposição 2.3** *Seja  $\mathbf{G}$  um grafo. As seguintes afirmativas são equivalentes:*

1. *O grafo  $\mathbf{G}$  é fortemente conexo;*
2. *Existe um vértice  $v \in V(\mathbf{G})$ , uma árvore conectora  $\mathbf{T} \subseteq \mathbf{G}$  com início  $v$  e uma árvore conectora  $\mathbf{T}' \subseteq \mathbf{G}$  com término  $v$ ;*
3.  *$V(\mathbf{G})$  não é vazio e para todo vértice  $v \in V(\mathbf{G})$ , existem uma árvore conectora  $\mathbf{T} \subseteq \mathbf{G}$  com início  $v$  e uma árvore conectora  $\mathbf{T}' \subseteq \mathbf{G}$  com término  $v$ .*

*Prova.* Naturalmente que o item 3 implica o item 2.

Vamos mostrar que o item 2 implica o item 1. Seja  $v \in V(\mathbf{G})$  um vértice e sejam  $\mathbf{T}, \mathbf{T}' \subseteq \mathbf{G}$  duas árvores conectoras com início  $v$  e com término  $v$  respectivamente. Sejam  $x, y \in V(\mathbf{G})$  dois vértices quaisquer. Tomando  $p$  um passeio de  $x$  para  $v$  na árvore conectora  $\mathbf{T}'$  e tomando  $q$  um passeio de  $v$  para  $y$  na árvore conectora  $\mathbf{T}$  temos que o passeio  $pq$  é um passeio de  $x$  para  $y$  com início em  $x$  e término em  $y$ . Portanto, o grafo  $\mathbf{G}$  é fortemente conexo.

Vamos mostrar que o item 1 implica o item 3. Suponha que o grafo  $\mathbf{G}$  seja fortemente conexo. Por definição,  $V(\mathbf{G}) \neq \emptyset$  e podemos escolher  $v \in V(\mathbf{G})$  um vértice qualquer. Por definição, para cada vértice  $u$ , podemos escolher um passeio de  $v$  a  $u$ . Em particular, podemos escolher  $p_u$ , um passeio de  $v$  a  $u$  de menor comprimento. Naturalmente que a distância de  $v$  a  $u$  é  $|p_u|$ . Ademais, quando  $u \neq v$  temos que  $p_u$  é não vazio e podemos definir  $a_u$  como sendo a última aresta de  $p_u$ . Definimos  $\mathbf{T}$  como o subgrafo de  $\mathbf{G}$  induzido por  $\{a_u \mid u \in V(\mathbf{G}) \setminus \{v\}\}$ . Observe que a função  $\omega$  é uma bijeção de  $\mathbf{T}$  em  $V(\mathbf{G}) \setminus \{v\}$ . Afirmamos que se  $u \neq v$  então  $|p_u| = |p_{\alpha(a_u)}| + 1$ . De fato, sendo  $p_u a_u^{-1}$  e  $p_{\alpha(a_u)}$  dois passeios de  $v$  a  $\alpha(a_u)$ , a partir da minimalidade

de  $p_{\alpha(a_u)}$  temos que  $|p_{\alpha(a_u)}| \leq |p_u a_u^{-1}| = |p_u| - 1$ . Além disso, sendo  $p_u$  e  $p_{\alpha(a_u)} a_u$  dois passeios de  $v$  a  $u$ , a partir da minimalidade de  $p_u$  temos que  $|p_u| \leq |p_{\alpha(a_u)} a_u| = |p_{\alpha(a_u)}| + 1$ . Isto nos permite fazer uma definição indutiva de um novo passeio  $q_u$  que será definido para todo vértice  $u \in V(\mathbf{G})$ . A indução se dará em  $|p_u|$ . Se  $|p_u| = 0$  temos que  $u = v$  e definimos  $q_u$  como sendo o passeio vazio de  $v$  a  $v$ . Se  $|p_u| > 0$ , tendo já sidos definidos todos os passeios  $q_x$  para todo vértice  $x$  tal que  $|p_x| < |p_u|$ , definimos  $q_u$  como sendo o passeio  $q_{\alpha(a_u)} a_u$ . Por uma imediata indução em  $|p_u|$  podemos provar que  $|q_u| = |p_u|$  e que  $q_u$  é um passeio de  $v$  a  $u$  em  $\mathbf{T}$ . Como para todo vértice  $u \in V(\mathbf{G})$  existe um passeio  $q_u$  de  $v$  a  $u$  em  $\mathbf{T}$ , temos que  $\omega_v(\mathbf{T}) = V(\mathbf{G}) = (V(\mathbf{G}) \setminus \{v\}) + \{v\} = \omega(\mathbf{T}) + \{v\}$ . Usando a proposição 2.2 temos que  $\mathbf{T}$  é uma árvore com início  $v$  e, portanto, uma árvore conectora com início  $v$  já que  $\omega_v(\mathbf{T}) = V(\mathbf{G})$ . Analogamente podemos construir uma árvore conectora com término  $v$ . ■

## 2.3 Número ciclomático

Na proposição 2.3 vimos que todo grafo fortemente conexo admite uma árvore conectora. Na proposição 2.2 vimos que qualquer árvore conectora possui a mesma cardinalidade  $|V(\mathbf{G})| - 1$ . O *número ciclomático* de um grafo fortemente conexo  $\mathbf{G}$  é definido como sendo a cardinalidade

$$|\mathbf{G} \setminus \mathbf{T}|,$$

onde  $\mathbf{T}$  é uma árvore conectora qualquer de  $\mathbf{G}$ . Quando o grafo é finito, este número é

$$|\mathbf{G}| - |V(\mathbf{G})| + 1.$$

A proposição 2.4 relaciona o número ciclomático de dois grafos fortemente conexos quando um deles, em particular, é um subgrafo do outro.

**Proposição 2.4** *Seja  $\mathbf{G}$  um subgrafo fortemente conexo de um grafo  $\mathbf{G}'$  também fortemente conexo. Então o número ciclomático de  $\mathbf{G}$  é no máximo o número ciclomático de  $\mathbf{G}'$ .*

*Prova.* Se  $\mathbf{G} = \mathbf{G}'$ , não há o que provar. Suponha pois que  $E(\mathbf{G}') \setminus E(\mathbf{G}) \neq \emptyset$ .

Seja  $v$  um vértice de  $\mathbf{G}$ . Como  $\mathbf{G}$  é fortemente conexo, podemos escolher  $\mathbf{T} \subseteq \mathbf{G}$  uma árvore conectora de  $\mathbf{G}$  com início  $v$  devido à proposição 2.3. Seja  $0$  um vértice não pertencente a  $V(\mathbf{G}') \supseteq V(\mathbf{G})$  e seja  $V = V(\mathbf{G}') \setminus V(\mathbf{G}) + \{0\}$ . Seja a função  $\delta : V(\mathbf{G}') \rightarrow V$  definida por

$$\delta(u) = \begin{cases} u & \text{se } u \in V(\mathbf{G}') \setminus V(\mathbf{G}); \\ 0 & \text{se } u \in V(\mathbf{G}). \end{cases}$$

Definimos o grafo  $\mathbf{H}$  com conjunto de arestas

$$E(\mathbf{H}) = E(\mathbf{G}') \setminus E(\mathbf{G})$$

com as funções de incidência

$$\alpha' = \delta \circ \alpha \quad \text{e} \quad \omega' = \delta \circ \omega$$

e conjunto de vértices  $V(\mathbf{H}) = \alpha'(\mathbf{H}) \cup \omega'(\mathbf{H})$ . Se  $p$  for um passeio qualquer em  $\mathbf{G}'$ , definimos  $\varphi(p)$  como sendo a subsequência de  $p$  formada apenas pelas arestas de  $\mathbf{H}$  se a mesma for não-vazia ou o passeio vazio local a  $\delta(\alpha(p))$  caso contrário.

Vamos provar que  $\varphi(p)$  é um passeio no grafo  $\mathbf{H}$  de  $\alpha'(\varphi(p)) = \delta(\alpha(p))$  a  $\omega'(\varphi(p)) = \delta(\omega(p))$ . Para tanto faremos uma indução em  $|p|$ . Se  $|p| = 0$ , então  $p$  é um passeio vazio local a  $\alpha(p) = \omega(p)$  e por definição  $\varphi(p)$  é o passeio vazio local a  $\delta(\alpha(p)) = \delta(\omega(p))$ . Suponha agora que  $p = qa$  onde  $q$  é um passeio em  $\mathbf{G}'$  e  $a$  é uma aresta de  $\mathbf{G}'$  tal que  $\alpha(a) = \omega(q)$ . Pela hipótese de indução temos que  $\varphi(q)$  é um passeio em  $\mathbf{H}$  e que  $\alpha'(\varphi(q)) = \delta(\alpha(q))$  e  $\omega'(\varphi(q)) = \delta(\omega(q))$ . Suponha o caso em que  $a \in E(\mathbf{G})$ . Temos por definição que  $\varphi(p) = \varphi(qa) = \varphi(q)$  que por sua vez, já o sabemos, é um passeio em  $\mathbf{H}$ . Assim  $\alpha'(\varphi(p)) = \alpha'(\varphi(q)) = \delta(\alpha(q)) = \delta(\alpha(p))$ . Ademais  $\alpha(a), \omega(a) \in V(\mathbf{G})$  implicam que  $\omega'(\varphi(p)) = \omega'(\varphi(q)) = \delta(\omega(q)) = \delta(\alpha(a)) = 0 = \delta(\omega(a)) = \delta(\omega(p))$ . Suponha agora o caso em que  $a \notin E(\mathbf{G})$ . Temos por definição que  $\varphi(p) = \varphi(qa) = \varphi(q)a$ . Esta seqüência de arestas  $\varphi(q)a$  forma um passeio em  $\mathbf{H}$  pois  $\omega'(\varphi(q)) = \delta(\omega(q)) = \delta(\alpha(a)) = \alpha'(a)$ . Assim  $\alpha'(\varphi(p)) = \alpha'(\varphi(q)a) = \alpha'(\varphi(q)) = \delta(\alpha(q)) = \delta(\alpha(qa)) = \delta(\alpha(p))$  e  $\omega'(\varphi(p)) = \omega'(\varphi(q)a) = \omega'(a) = \delta(\omega(a)) = \delta(\omega(qa)) = \delta(\omega(p))$ .

Vamos provar que o grafo  $\mathbf{H}$  é fortemente conexo e que  $V(\mathbf{H}) = V$ . Sejam  $x$  e  $u$  dois vértices quaisquer de  $V$ . Vamos provar que existe um passeio em  $\mathbf{H}$  de  $x$  a  $u$ . Sejam  $x', u' \in V(\mathbf{G}')$  tais que  $\delta(x') = x$  e  $\delta(u') = u$ . Como  $\mathbf{G}'$  é fortemente conexo, existe um passeio  $p$  de  $x'$  a  $u'$ . Então  $\varphi(p)$  é um passeio

em  $\mathbf{H}$  de  $\alpha'(\varphi(p)) = \delta(\alpha(p)) = \delta(x') = x$  a  $\omega'(\varphi(p)) = \delta(\omega(p)) = \delta(u') = u$  como vimos antes. Para provar que  $\mathbf{H}$  é fortemente conexo, falta-nos apenas provar que  $V(\mathbf{H}) \neq \emptyset$ . Vamos agora provar que  $V(\mathbf{H}) = V$ . Note que  $V(\mathbf{H}) = \alpha'(\mathbf{H}) \cup \omega'(\mathbf{H}) = \delta(\alpha(\mathbf{H}) \cup \omega(\mathbf{H})) \subseteq V = V(\mathbf{G}') \setminus V(\mathbf{G}) + \{0\}$ . Para todo vértice  $u \in V(\mathbf{G}') \setminus V(\mathbf{G})$  existe um passeio  $p$  de  $0$  a  $u$  em  $\mathbf{H}$  e  $u \neq 0$  implica que existe uma última aresta  $a$  de  $p$  e  $u = \omega'(a) \in \omega'(\mathbf{H}) \subseteq V(\mathbf{H})$ . Assim  $V(\mathbf{G}') \setminus V(\mathbf{G}) \subseteq V(\mathbf{H})$ . Caso  $V(\mathbf{G}') \setminus V(\mathbf{G}) \neq \emptyset$ , existe ao menos um tal vértice  $u$  e a primeira aresta  $b$  de  $p$  é tal que  $0 = \alpha'(b) \in \alpha'(\mathbf{H}) \subseteq V(\mathbf{H})$ . Caso  $V(\mathbf{G}') \setminus V(\mathbf{G}) = \emptyset$ , temos que  $\alpha'(b) = \omega'(b) = 0$  para toda aresta  $b \in \mathbf{H}$  e  $E(\mathbf{H}) = E(\mathbf{G}') \setminus E(\mathbf{G}) \neq \emptyset$  implica que  $0 \in V(\mathbf{H})$ .

Assim sendo, podemos escolher  $\mathbf{T}'' \subseteq \mathbf{H}$  uma árvore conectora de  $\mathbf{H}$  com início  $0$  devido à proposição 2.3. Seja  $\mathbf{T}' \subseteq \mathbf{G}'$  o subgrafo induzido por

$$E(\mathbf{T}') = E(\mathbf{T}) \cup E(\mathbf{T}'').$$

Vamos provar que  $\omega$  estabelece bijeções de  $\mathbf{T}$  em  $V(\mathbf{G}) \setminus \{v\}$ , de  $\mathbf{T}''$  em  $V(\mathbf{G}') \setminus V(\mathbf{G})$  e de  $\mathbf{T}'$  em  $V(\mathbf{G}') \setminus \{v\}$ . Como  $\mathbf{T}''$  é uma árvore conectora de  $\mathbf{H}$  com início  $0$ , a partir da proposição 2.2 temos que  $V(\mathbf{H}) = \omega'_0(\mathbf{T}'') = \{0\} \cup \omega'(\mathbf{T}'')$  e  $0 \notin \omega'(\mathbf{T}'')$  e  $\omega'$  é injetiva em  $\mathbf{T}''$ . Isto em particular implica que  $\omega'$  estabelece uma bijeção de  $\mathbf{T}''$  em  $\omega'(\mathbf{T}'') = V(\mathbf{H}) \setminus \{0\} = V \setminus \{0\} = V(\mathbf{G}') \setminus V(\mathbf{G})$ . Como  $\omega' = \delta \circ \omega$ , temos que  $\omega$  é uma bijeção de  $\mathbf{T}''$  em  $\omega(\mathbf{T}'')$  e que  $\delta$  é uma bijeção de  $\omega(\mathbf{T}'')$  em  $\omega'(\mathbf{T}'') = V(\mathbf{G}') \setminus V(\mathbf{G})$ . Da definição de  $\delta$  temos então que  $\omega(\mathbf{T}'') = V(\mathbf{G}') \setminus V(\mathbf{G})$  e que portanto  $\omega$  estabelece uma bijeção de  $\mathbf{T}''$  em  $V(\mathbf{G}') \setminus V(\mathbf{G})$ . Como  $\mathbf{T}$  é uma árvore conectora de  $\mathbf{G}$  com início  $v$ , a partir da proposição 2.2 temos que  $V(\mathbf{G}) = \omega_v(\mathbf{T}) = \{v\} \cup \omega(\mathbf{T})$  e  $v \notin \omega(\mathbf{T})$  e  $\omega$  é injetiva em  $\mathbf{T}$ . Isto em particular implica que  $\omega$  estabelece uma bijeção de  $\mathbf{T}$  em  $\omega(\mathbf{T}) = V(\mathbf{G}) \setminus \{v\}$ . Como a união  $E(\mathbf{T}') = E(\mathbf{T}) \cup E(\mathbf{T}'')$  é disjunta pois  $E(\mathbf{T}) \subseteq E(\mathbf{G})$  e  $E(\mathbf{T}'') \subseteq E(\mathbf{H}) = E(\mathbf{G}') \setminus E(\mathbf{G})$ , como  $\omega(E(\mathbf{T})) = V(\mathbf{G}) \setminus \{v\}$  é disjunto de  $\omega(E(\mathbf{T}'')) = V(\mathbf{G}') \setminus V(\mathbf{G})$ , temos então que  $\omega$  estabelece uma bijeção de  $E(\mathbf{T}') = E(\mathbf{T}) \cup E(\mathbf{T}'')$  em  $V(\mathbf{G}) \setminus \{v\} \cup V(\mathbf{G}') \setminus V(\mathbf{G}) = V(\mathbf{G}') \setminus \{v\}$ , concluindo nossa demonstração.

Vamos provar que  $\mathbf{T}'$  é uma árvore conectora de  $\mathbf{G}'$  com início  $v$ . Dado que  $\omega$  estabelece bijeção de  $\mathbf{T}'$  em  $V(\mathbf{G}') \setminus \{v\}$ , temos que  $\omega$  é injetiva em  $\mathbf{T}'$ , que  $v \notin \omega(\mathbf{T}')$  e que  $V(\mathbf{G}') = \{v\} \cup \omega(\mathbf{T}')$ . Segundo a proposição 2.3, para provar que  $\mathbf{T}'$  é uma árvore conectora de  $\mathbf{G}'$  com início  $v$ , falta-nos apenas provar que  $\omega_v(\mathbf{T}') = V(\mathbf{G}')$ . Equivale a provar que existe um passeio em  $\mathbf{T}'$  de  $v$  a  $u$  para todo  $u \in V(\mathbf{G}')$ . Suponha primeiro o caso em que  $u \in V(\mathbf{G})$ . Assim existe um passeio  $p$  em  $\mathbf{T}$  de  $v$  a  $u$  já que  $\mathbf{T}$  é uma árvore conectora

de  $\mathbf{G}$  com início  $v$ . Este passeio  $p$  é um passeio em  $\mathbf{T}'$  pois  $\mathbf{T} \subseteq \mathbf{T}'$ . Suponha agora o caso em que  $u \in V(\mathbf{G}') \setminus V(\mathbf{G})$ . Assim existe um passeio  $q$  em  $\mathbf{T}''$  de  $0$  a  $u$  já que  $\mathbf{T}''$  é uma árvore conectora de  $\mathbf{H}$  com início  $0$ . Este passeio  $q$  não é vazio pois  $u \in V(\mathbf{G}') \setminus V(\mathbf{G})$  implica que  $\omega'(q) = u \neq 0 = \alpha'(q)$ . Seja  $a$  a primeira aresta de  $q$ . Como  $\delta(\alpha(a)) = \alpha'(a) = \alpha'(q) = 0$ , temos que  $\alpha(a) \in V(\mathbf{G})$ . Assim existe  $p$  um passeio em  $\mathbf{T}$  de  $v$  a  $\alpha(a)$ , já que  $\mathbf{T}$  é uma árvore conectora de  $\mathbf{G}$  com início  $v$ . Temos por fim que  $pq$  é um passeio em  $\mathbf{T}'$  de  $v$  a  $u$ , conforme procurávamos encontrar.

Vamos provar que  $\mathbf{G} \setminus \mathbf{T} \subseteq \mathbf{G}' \setminus \mathbf{T}'$ . Dado que  $E(\mathbf{T}'') \subseteq E(\mathbf{H}) = E(\mathbf{G}') \setminus E(\mathbf{G})$  implica que  $E(\mathbf{T}'') \cap E(\mathbf{G}) = \emptyset$  concluímos portanto que  $E(\mathbf{G} \setminus \mathbf{T}) = E(\mathbf{G}) \setminus E(\mathbf{T}) = E(\mathbf{G}) \setminus (E(\mathbf{T}) \cup E(\mathbf{T}'')) = E(\mathbf{G}) \setminus E(\mathbf{T}') \subseteq E(\mathbf{G}') \setminus E(\mathbf{T}') = E(\mathbf{G}' \setminus \mathbf{T}')$ . O resto segue do fato que  $\mathbf{G} \setminus \mathbf{T}$  e  $\mathbf{G}' \setminus \mathbf{T}'$  são subgrafos de  $\mathbf{G}'$  induzidos por  $E(\mathbf{G} \setminus \mathbf{T})$  e por  $E(\mathbf{G}' \setminus \mathbf{T}')$  respectivamente.

Tendo em vista que  $\mathbf{G} \setminus \mathbf{T} \subseteq \mathbf{G}' \setminus \mathbf{T}'$  podemos concluir que  $|\mathbf{G} \setminus \mathbf{T}| \leq |\mathbf{G}' \setminus \mathbf{T}'|$  e a tese está provada. ■

Da própria demonstração da proposição 2.4 segue o corolário 2.5.

**Corolário 2.5** *Seja  $\mathbf{G}$  um subgrafo fortemente conexo de um grafo  $\mathbf{G}'$  também fortemente conexo. Sejam  $v \in V(\mathbf{G})$  um vértice e  $\mathbf{T} \subseteq \mathbf{G}$  uma árvore conectora de  $\mathbf{G}$  com início  $v$ . Então existe uma árvore  $\mathbf{T}' \subseteq \mathbf{G}'$  conectora de  $\mathbf{G}'$  com início  $v$  tal que  $\mathbf{T} \subseteq \mathbf{T}'$  e  $\mathbf{G} \setminus \mathbf{T} \subseteq \mathbf{G}' \setminus \mathbf{T}'$ .*

## Capítulo 3

# Categorias e Grupóides

Uma categoria pode ser vista como um monóide onde a multiplicação não é completa mas parcial. Esta parcialidade é controlada pela estrutura de conectividade das arestas de um grafo. Em particular, se este grafo possui um único vértice, então esta operação parcial é uma operação total e a categoria é de fato um monóide. Assim o conceito de categoria generaliza o conceito de monóide. Da mesma forma o conceito de grupóide generaliza o conceito de grupo.

Nosso objetivo não é o estudo de categorias e grupóides, mas a estrutura dos monóides de Burnside livres. Durante este processo, apareceram de forma natural alguns grafos — como o grafo fundamental de uma  $\mathcal{D}$ -classe como será visto na seção 6.3 do capítulo 6 — e algumas categorias — como a categoria livre gerada por um grafo, a ser visto neste capítulo; e o grupóide de Burnside livre, a ser visto no capítulo 4. Além disso, alguns resultados nossos, expressos na linguagem das categorias, poderiam ter suficiente interesse do ponto de vista da teoria de categorias e grupóides. Este é o caso do teorema 4.7 a ser visto no capítulo 4.

A este capítulo reservamos as definições gerais da teoria de categorias e as generalizações de conceitos já bastante conhecidos na teoria de monóides. Daremos as definições estritamente necessárias e nosso ponto de vista dá destaque às arestas (ou flechas, ou ainda morfismos segundo terminologia freqüentemente usada na área) em relação aos vértices (ou objetos). O leitor poderá encontrar mais informações sobre categorias no clássico livro de MacLane [24] e importantes resultados conectando a teoria de categorias com a teoria de monóides no trabalho de Tilson [32]. Ao capítulo 4 reservamos uma aplicação destes conceitos a uma particular categoria: o grupóide

de Burnside livre.

### 3.1 Categorias e morfismos de categorias

Uma categoria é um grafo  $\mathcal{C}$  munido de uma operação parcial sobre as arestas. O grafo e a operação parcial devem satisfazer algumas restrições. Dados dois vértices  $v, v'$  definimos o subconjunto  $\mathcal{C}_{v,v'} = \{x \in \mathcal{C} \mid \alpha(x) = v \text{ e } \omega(x) = v'\}$  e denotamos  $\mathcal{C}_{v,v}$  simplesmente por  $\mathcal{C}_v$ . As restrições são as seguintes:

- a operação parcial  $\cdot$ , denotada multiplicativamente, é definida apenas sobre elementos consecutivos e é tal que  $\alpha(x \cdot y) = \alpha(x)$  e  $\omega(x \cdot y) = \omega(y)$ ;
- para cada vértice  $v$  existe  $1_v \in \mathcal{C}_v$ , uma *identidade local a  $v$* . Tais identidades locais satisfazem  $1_{\alpha(x)} \cdot x = x = x \cdot 1_{\omega(x)}$  para todo  $x \in \mathcal{C}$ ;
- a operação parcial  $\cdot$  é associativa, ou seja, dados  $x, y, z \in \mathcal{C}$  consecutivos nesta ordem temos que  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ .

Normalmente nos referiremos à categoria apenas pelo conjunto  $\mathcal{C}$  deixando implícitas as funções início, término (e o conjunto de vértices) e a operação parcial. O conjunto de vértices, é também chamado de *conjunto de objetos de  $\mathcal{C}$*  e é denotado por  $\text{Obj}(\mathcal{C})$ . Dado um elemento  $p$  com mesmo início e término e dado  $k$  um inteiro não negativo, podemos definir a *potência de  $p$  a  $k$*  da maneira natural; ou seja,  $p^0 = 1_{\alpha(p)}$  e  $p^k = p^{k-1} \cdot p$  para  $k > 0$ . A princípio reservaremos a notação  $xy$  para a concatenação dos passeios  $x$  e  $y$  mas quando for claro que estamos trabalhando numa categoria  $\mathcal{C}$  e não estamos nos referindo a passeios no grafo mas a elementos da categoria permitiremos abreviar a notação  $x \cdot y$  para  $xy$  ou  $xy$ .

Dados dois grafos  $\mathbf{G}$  e  $\mathbf{G}'$  com conjunto de vértices  $V$  e  $V'$ , dizemos que uma função  $\varphi : \mathbf{G} \rightarrow \mathbf{G}'$ , é um *morfismo de grafos* se  $\varphi$  preserva a consecutividade das arestas; mais precisamente, se existe uma aplicação  $\delta : V \rightarrow V'$  tal que para toda aresta  $x$  de  $\mathbf{G}$  tenhamos que  $\alpha(\varphi(x)) = \delta(\alpha(x))$  e  $\omega(\varphi(x)) = \delta(\omega(x))$ . Esta aplicação  $\delta$ , existindo, é unicamente determinada em  $\alpha(\mathbf{G}) \cup \omega(\mathbf{G}) = V$  e é chamada de *projeção de vértices induzida por  $\varphi$* . Dadas duas categorias  $\mathcal{C}$  e  $\mathcal{C}'$ , dizemos que uma função  $\varphi : \mathcal{C} \rightarrow \mathcal{C}'$ , é um *morfismo de categorias* se for um morfismo de grafos e se comutar com as operações parciais das categorias, ou seja, se  $x, y \in \mathcal{C}$  são dois elementos



consecutivos, então

$$\varphi(xy) = \varphi(x)\varphi(y).$$

## 3.2 Categorias livres e fatorações

Um grafo  $\mathbf{G} \subseteq \mathcal{C}$  é dito *gerador da categoria  $\mathcal{C}$*  se todos os elementos da categoria, exceto as identidades locais, forem produto de uma seqüência não vazia de elementos de  $\mathbf{G}$ . Dado um grafo qualquer  $\mathbf{G}$ , em geral não é possível definir uma operação parcial de modo que ele seja uma categoria. Se  $\mathbf{G}$  não possui laços locais a cada vértice, não pode haver identidades locais por exemplo. Da mesma forma, se  $\mathbf{G}$  não for transitivo (se existem arestas de  $v_1$  a  $v_2$  e de  $v_2$  a  $v_3$  então existe ao menos uma aresta de  $v_1$  a  $v_3$ ) não existe nenhuma operação parcial tal que este grafo munido dela seja uma categoria. Por outro lado, podemos definir o conjunto  $\mathbf{G}^*$  formado por todos os passeios em  $\mathbf{G}$ , inclusive os passeios vazios locais aos vértices. O conjunto  $\mathbf{G}^*$  munido das funções de incidência dos passeios e da operação de concatenação de passeios forma uma categoria e é gerada pelo grafo  $\mathbf{G}$  (onde cada aresta é identificada com o passeio de comprimento 1 formado pela própria aresta). A categoria  $\mathbf{G}^*$  é chamada de *categoria livre gerada pelo grafo  $\mathbf{G}$* . Dados um grafo  $\mathbf{G}$ , uma categoria  $\mathcal{C}$  e um morfismo de grafos  $\varphi : \mathbf{G} \rightarrow \mathcal{C}$ , existe e é única a extensão deste morfismo de grafos a um morfismo de categorias  $\varphi : \mathbf{G}^* \rightarrow \mathcal{C}$ . Este morfismo de grafos induz uma função  $\delta : V(\mathbf{G}) \rightarrow \text{Obj}(\mathcal{C})$  e para  $p = b_1 b_2 \cdots b_k \in \mathbf{G}^*$  um passeio em  $\mathbf{G}$ , temos que:

$$\varphi(p) = \begin{cases} \varphi(b_1) \cdot \varphi(b_2) \cdot \cdots \cdot \varphi(b_k), & \text{se } k > 0; \\ 1_{\delta(\alpha(p))} = 1_{\delta(\omega(p))}, & \text{se } k = 0. \end{cases}$$

Como de costume, podemos nos referir ao elemento  $\varphi(p)$  da categoria  $\mathcal{C}$  como *avaliação do passeio  $p$  por  $\varphi$* . No caso de  $\mathbf{G}$  ser um subgrafo da categoria  $\mathcal{C}$  a inclusão  $\iota : \mathbf{G} \rightarrow \mathcal{C}$  é um morfismo de grafos e sua extensão  $\iota : \mathbf{G}^* \rightarrow \mathcal{C}$  é chamada simplesmente de *avaliação do passeio  $p$* .

Sejam  $x, y, z$  e  $w$  elementos da categoria  $\mathcal{C}$ . Denotamos por  $x\mathcal{C}$  o conjunto  $\{xy \mid y \in \mathcal{C}\}$ , denotamos por  $\mathcal{C}x$  o conjunto  $\{yx \mid y \in \mathcal{C}\}$  e denotamos por  $\mathcal{C}x\mathcal{C}$  o conjunto  $\{yxz \mid y, z \in \mathcal{C}\}$ . Dizemos que  $x$  é um *prefixo de  $y$*  se  $y \in x\mathcal{C}$ , dizemos que  $x$  é um *sufixo de  $y$*  se  $y \in \mathcal{C}x$  e dizemos que  $x$  é um *fator de  $y$*  se  $y \in \mathcal{C}x\mathcal{C}$ . Denotamos por  $\text{Pref}(x)$ , por  $\text{Suf}(x)$  e por  $\text{Fat}(x)$  respectivamente o conjunto dos prefixos de  $x$ , o de sufixos de  $x$  e o de fatores de  $x$ . Dizemos que  $(x, y, z)$  é uma *fatoração de  $w$*  se  $w = xyz$

e por vezes a denotamos simplesmente por  $w = xyz$  se forem evidentes os elementos  $x$ ,  $y$  e  $z$ . Suponha a partir de agora que  $\mathcal{C} = \mathbf{G}^*$  para um grafo  $\mathbf{G}$ . Assim, permitimo-nos referir a esta fatoração como sendo uma *ocorrência de  $y$  como fator de  $w$*  no caso de  $x$  e  $z$  poderem ser sub-entendidos. Fixado o passeio  $w \in \mathcal{C} = \mathbf{G}^*$ , definimos a ordem parcial  $\leq$  sobre as fatorações de  $w$ , chamada de *ordem das fatorações*, como segue:

$$(x, y, z) \leq (x', y', z') \text{ se e só se } |x| \geq |x'| \text{ e } |z| \geq |z'|.$$

Sobre um conjunto de fatorações de  $w$  incomparáveis por  $\leq$ , podemos definir a *ordem das ocorrências*  $\preceq$  definida por

$$(x, y, z) \preceq (x', y', z') \text{ se e só se } |x| \leq |x'|,$$

ou equivalentemente,  $(x, y, z) \preceq (x', y', z')$  se e só se  $|z| \geq |z'|$ . A ordem estrita de  $\preceq$  é denotada por  $\prec$ . Uma seqüência  $(x_1, y_1, z_1), \dots, (x_k, y_k, z_k)$  de fatorações de  $w$  que forma uma anticadeia segundo  $\leq$  é dita *ordenada por ocorrência* se  $|x_1| < |x_2| < \dots < |x_k|$ .

### 3.3 Congruências e funções preservadas

Uma relação  $\sim$  é uma *congruência sobre uma categoria  $\mathcal{C}$*  se for uma relação de equivalência compatível com a multiplicação na categoria; ou seja, todos os elementos de cada classe de equivalência são coterminais e se  $x, y \in \mathcal{C}$  são dois elementos consecutivos, se  $x' \sim x$  e se  $y' \sim y$  então temos que  $x'y' \sim xy$ . Dada a congruência  $\sim$ , a *categoria quociente  $\mathcal{C}/\sim$*  é a categoria formada pelas classes de congruência de  $\sim$ . O conjunto de objetos é o mesmo da categoria  $\mathcal{C}$  e as funções início e término e a operação parcial são as induzidas da categoria  $\mathcal{C}$ . A projeção canônica de  $\mathcal{C}$  em  $\mathcal{C}/\sim$  é um morfismo de categorias e a composição de um morfismo de categorias com seu inverso é uma congruência.

Seja  $\mathcal{C}$  uma categoria e sejam  $(x, x')$  e  $(t, t')$  pares de  $\mathcal{C} \times \mathcal{C}$ . Dizemos que  $(x, x')$  é uma *substituição por  $(t, t')$*  se existem  $r, s \in \mathcal{C}$  e as fatorações  $x = rts$  e  $x' = rt's$ . Neste caso,  $x$  e  $x'$  são coterminais, bem como  $t$  e  $t'$ . Ademais,  $r \in \mathcal{C}_{\alpha(x), \alpha(t)}$  e  $s \in \mathcal{C}_{\omega(t), \omega(x)}$ . Dado um conjunto  $\pi \subseteq \mathcal{C} \times \mathcal{C}$  de pares de elementos coterminais, dizemos que  $(x, x')$  é uma *substituição por  $\pi$*  se existe par  $(t, t') \in \pi$  tal que  $(x, x')$  é uma substituição por  $(t, t')$ . Dadas duas relações de equivalência  $R$  e  $S$  sobre o mesmo conjunto, dizemos que  $R$

é menor que  $S$  ou que  $R$  é um *refinamento* de  $S$  quando  $R \subseteq S$ . Existe uma *menor congruência que contém*  $\pi$  e é o conjunto dos pares  $(x, x')$  tais que existe uma seqüência de elementos  $x = x_0, x_1, \dots, x_k = x'$  tais que  $(x_i, x_{i+1})$  é uma substituição por  $\pi$  ou por  $\pi^{-1}$  para todo  $i = 0, 1, \dots, k-1$ . Seja  $X \subseteq \mathcal{C}$  um subconjunto qualquer. Dizemos que uma congruência  $\sim$  *satura*  $X$  se  $X$  for a união de classes de congruência de  $\sim$ . Existe uma maior congruência que satura  $X$  e é o conjunto dos pares  $(t, t')$  tais que  $rts \in X \iff rt's \in X$  para todos  $r, s \in \mathcal{C}$ . Esta congruência é chamada *congruência sintática de*  $X$  e é denotada por  $\equiv_X$ . A categoria quociente  $\mathcal{C}/\equiv_X$  é chamada *categoria sintática de*  $X$  e dizemos que  $X$  é *reconhecível* se sua categoria sintática for finita.

Seja  $f$  uma função com domínio  $\mathcal{C}$ . Dizemos que um par ordenado de  $\mathcal{C} \times \mathcal{C}$  *preserva o valor de*  $f$  se é constituído de elementos com mesmo valor por  $f$  e dizemos que uma relação de equivalência em  $\mathcal{C}$  *preserva o valor de*  $f$  se  $f$  assume um único valor em cada classe de equivalência. Pode-se provar imediatamente que a menor congruência que contém  $\pi$  preserva o valor de  $f$  se e só se cada substituição por  $\pi$  preserva o valor de  $f$ .

Vamos definir dois tipos de tais funções  $f$  que serão observadas neste trabalho. Seja  $\mathbf{G}$  um grafo e seja  $P \subseteq \mathbf{G}^*$  um conjunto de passeios. Chamamos de *P-característica* a função  $\chi_P : \mathbf{G}^* \rightarrow \{0, 1\}$  definida por

$$\chi_P(q) = \begin{cases} 1, & \text{se } q \in \mathbf{G}^* P \mathbf{G}^*; \\ 0, & \text{caso contrário.} \end{cases}$$

Seja um inteiro  $m \geq 1$  fixado. Chamamos de *P-ocorrência* a função  $\#_P : \mathbf{G}^* \rightarrow \mathbb{Z}_m$  definida por  $\#_P(q)$  sendo o resto da divisão por  $m$  do número de fatorações maximais  $q = xyz$  tais que  $y \in P$ . Quando  $P$  tem um único elemento  $p$ , permitimo-nos representar  $\chi_P$  e  $\#_P$  simplesmente por  $\chi_p$  e por  $\#_p$ .

### 3.4 Grupóides e grupos locais

Seja uma categoria  $\mathcal{C}$ . Os subconjuntos da forma  $\mathcal{C}_{v,v'}$  com  $v \neq v'$  não são subcategorias já que não incluem as identidades locais a  $v$  e  $v'$ . Já um subconjunto da forma  $\mathcal{C}_v$  munido das funções de incidência e operação induzidas da categoria  $\mathcal{C}$  forma uma subcategoria. Dado um objeto  $v$ , todos os elementos da subcategoria  $\mathcal{C}_v$  são consecutivos, a multiplicação é sempre definida e  $\mathcal{C}_v$  é de fato um monóide onde o elemento neutro é  $1_v$ . Por isto a

subcategoria  $\mathcal{C}_v$  também é chamada de *monóide local a v*. De fato, o conceito de categoria generaliza o de monóide. A categoria  $\mathcal{C}$  é dita um *grupóide* se cada elemento for inversível, ou seja, para todo  $x \in \mathcal{C}$  existe  $y \in \mathcal{C}_{\omega(x), \alpha(x)}$  tal que  $xy = 1_{\alpha(x)}$  e que  $yx = 1_{\omega(x)}$ . Este elemento inverso, existindo, é único pois se  $y$  e  $y'$  são tais inversos, então  $y' = y'1_{\alpha(x)} = y'(xy) = (y'x)y = 1_{\omega(x)}y = y$ . Este inverso será denotado por  $x^{-1}$  como de costume.

Dizemos que a categoria  $\mathcal{C}$  é *fortemente conexa* se o grafo  $\mathcal{C}$  é fortemente conexo. Através da avaliação dos passeios do grafo  $\mathcal{C}$  na categoria  $\mathcal{C}$  isto equivale a dizer que a categoria tem ao menos um objeto e que  $\mathcal{C}_{v,v'} \neq \emptyset$  para todo par ordenado de objetos  $(v, v')$ .

A proposição seguinte dá-nos uma importante propriedade dos monóides locais de grupóides.

**Proposição 3.1** *Todo monóide local de um grupóide é um grupo. Ademais, se o grupóide for fortemente conexo, todos os grupos locais são isomorfos.*

*Prova.* Para ver que os monóides locais são grupos, basta verificar que o inverso no grupóide de um elemento do monóide local também está no monóide local e é de fato o seu inverso no monóide local.

Se  $\mathcal{C}$  é o grupóide, suposto fortemente conexo, se  $v$  e  $v'$  são dois objetos quaisquer, então existe  $z \in \mathcal{C}_{v,v'}$ . Basta verificar que a função  $\varphi : \mathcal{C}_v \rightarrow \mathcal{C}_{v'}$  definida por  $\varphi(x) = z^{-1}xz$  é um isomorfismo de grupos. De fato, temos que:  $\varphi(x)\varphi(y) = z^{-1}xz z^{-1}yz = z^{-1}x1_vyz = z^{-1}xyz = \varphi(xy)$ ; a inversa de  $\varphi$  é dada por  $\varphi^{-1}(x) = zxz^{-1}$ ; e  $\varphi(1_v) = z^{-1}1_vz = 1_{v'}$ . ■

# Capítulo 4

## Grupóides de Burnside Livres

Seja um inteiro  $m \geq 1$ . Neste capítulo definiremos um grupóide especial: o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por um grafo fortemente conexo. O resultado principal do capítulo, o teorema 4.7, afirma que os grupos locais deste grupóide são todos isomorfos a um mesmo grupo de Burnside livre satisfazendo  $x^m = 1$ . Também é caracterizado um grupo de geradores para este grupo livre. Após as definições gerais feitas na seção 4.1, nas seções 4.2 e 4.3 apresentamos as definições e os resultados necessários à demonstração do teorema 4.7 quando  $m \geq 2$ . Demonstração que é reservada à seção 4.4.

### 4.1 Grupóide de Burnside livre

Seja  $\mathbf{G}$  um grafo fortemente conexo cujo conjunto de vértices é  $V$ . Seja  $\mathcal{K} = \mathbf{G}^*$  a categoria livre gerada pelo grafo  $\mathbf{G}$ . Definimos o conjunto  $\pi = \{(x^m, 1_v) \mid \forall v \in V, \forall x \in \mathcal{K}_v\}$  e a congruência  $\cong$  sobre  $\mathcal{K}$  como sendo a menor congruência que contém  $\pi$ . Definimos a categoria  $\mathcal{B}$  como sendo  $\mathcal{B} \stackrel{\text{def}}{=} \mathcal{K}/\cong$  e a cada passeio  $p \in \mathcal{K}$  associamos sua projeção canônica  $\hat{p} \in \mathcal{B}$  que é a classe de congruência de  $p$  por  $\cong$ . Os objetos da categoria  $\mathcal{B}$  são os mesmos que os da categoria  $\mathcal{K}$  que por sua vez são os vértices de  $\mathbf{G}$ . Ademais, a projeção canônica de  $\mathcal{K}$  sobre  $\mathcal{B}$  preserva o início e o fim de cada passeio. Como  $\mathbf{G}$  é um grafo fortemente conexo segue de imediato que  $\mathcal{K}$  e  $\mathcal{B}$  são categorias fortemente conexas. Ademais, podemos verificar que  $\mathcal{B}$  é um grupóide. De fato, seja  $x \in \mathcal{B}$  um elemento qualquer e seja  $p \in \mathcal{K}$  um passeio tal que  $\hat{p} = x$ , podemos tomar  $q \in \mathcal{K}$ , um passeio de  $\omega(p)$  a  $\alpha(p)$ , e definimos

$r = q(pq)^{m-1}$ . Assim temos que  $pr = pq(pq)^{m-1} = (pq)^m \cong 1_{\alpha(p)}$  e que  $rp = q(pq)^{m-1}p = (qp)^m \cong 1_{\omega(p)}$ . Isto implica que  $\widehat{r}$  é o inverso de  $x$ . O grupóide  $\mathcal{B}$  assim definido é o *grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por  $\mathbf{G}$* .

Veremos agora algumas funções preservadas pela congruência  $\cong$ . Referimos o leitor à seção 3.3 do capítulo 3 para a definição da função  $b$ -ocorrência.

**Proposição 4.1** *Para toda aresta  $b \in \mathbf{G}$ , a função  $\#_b : \mathcal{K} \rightarrow \mathbb{Z}_m$  é um morfismo e é preservada pela congruência  $\cong$ .*

*Prova.* Seja  $b \in \mathbf{G}$  uma aresta qualquer. Temos que  $\#_b : \mathcal{K} \rightarrow \mathbb{Z}_m$  é um morfismo pois da definição segue de imediato que  $\#_b(xy) = \#_b(x) + \#_b(y) \pmod{m}$ . Para provar que  $\cong$  preserva  $\#_b$ , é suficiente mostrar que qualquer substituição  $(rx^m s, rs)$  por  $\pi$  preserva a função  $\#_b$ . Ora,  $\forall v \in V(\mathbf{G}), \forall x \in \mathcal{K}_v$  temos que  $\#_b(x^m) = m * \#_b(x) = 0 = \#_b(1_v) \pmod{m}$ . Por fim,  $\#_b(rx^m s) = \#_b(r) + \#_b(x^m) + \#_b(s) = \#_b(r) + 0 + \#_b(s) = \#_b(rs) \pmod{m}$  e concluímos que  $\cong$  preserva  $\#_b$  como previsto. ■

Como  $\mathcal{B}$  é um grupóide fortemente conexo, pela proposição 3.1 temos que os monóides locais  $\mathcal{B}_v$  são grupos isomorfos. Como já adiantamos, veremos no teorema 4.7 que estes grupos são isomorfos a um mesmo grupo de Burnside livre satisfazendo  $x^m = 1$ . Caso  $m = 1$ , não há muita substância nesta afirmativa já que estes grupos são triviais devido à congruência  $\cong$  identificar todo elemento de  $\mathcal{K}_v$  a  $1_v$ , para todo vértice  $v$ . Da mesma forma o grupo de Burnside livre satisfazendo  $x^m = 1$  é trivial. Nas seções 4.2 e 4.3 estaremos supondo  $m \geq 2$ .

## 4.2 Normalização

Supomos que  $m \geq 2$  nesta seção.

Pela proposição 3.1 temos que os monóides locais  $\mathcal{B}_v$  são grupos isomorfos. Assim, fixaremos um particular vértice  $u \in V$  e analisaremos o grupo local  $\mathcal{B}_u$ . Como o grafo  $\mathbf{G}$  é fortemente conexo, usando a proposição 2.3 podemos escolher uma árvore conectora  $\mathbf{T} \subseteq \mathbf{G}$  com início  $u$ . Para todo vértice  $v$ , definimos  $p_v$  como sendo o único passeio em  $\mathbf{T}$  de  $u$  a  $v$  e definimos o *normalizante de  $v$*

$$\gamma_v \stackrel{\text{def}}{=} \widehat{p}_v \in \mathcal{B}_{u,v}.$$

Definimos ainda a *normalização*  $\lambda : \mathbf{G} \rightarrow \mathcal{B}_u$  como sendo

$$\lambda(b) \stackrel{\text{def}}{=} \gamma_{\alpha(b)} \widehat{b} \gamma_{\omega(b)}^{-1}.$$

Esta aplicação  $\lambda$  é um morfismo de grafos e é unicamente estendida ao morfismo de categorias  $\lambda : \mathcal{K} \rightarrow \mathcal{B}_u$ . Mais especificamente, dado  $p = b_1 b_2 \cdots b_k \in \mathcal{K}$  um passeio em  $\mathbf{G}$ , sua *normalização* é:

$$\lambda(p) = \begin{cases} \lambda(b_1) \lambda(b_2) \cdots \lambda(b_k), & \text{se } k > 0; \\ \widehat{1}_u, & \text{se } p \text{ é um passeio vazio.} \end{cases}$$

Na proposição 4.2 caracterizamos a função  $\lambda$  quando aplicada a  $\mathbf{G}$ . Vemos que  $\lambda(\mathbf{T}) = \{\widehat{1}_u\}$  e que somente as arestas de  $\mathbf{T}$  são mapeadas em  $\widehat{1}_u$ . Também vemos que  $\lambda$  estabelece uma injeção em  $\mathbf{G} \setminus \mathbf{T}$ .

**Proposição 4.2** *Sejam  $b \in \mathbf{G}$  e  $b' \in \mathbf{G} \setminus \mathbf{T}$  duas arestas. Sendo  $m \geq 2$ , então temos que:*

- $\lambda(b) = \widehat{1}_u$  se e só se  $b \in \mathbf{T}$ ;
- $\lambda(b) = \lambda(b')$  se e só se  $b = b'$ .

*Prova.* Dada uma aresta  $b' \in \mathbf{G}$  qualquer, a função  $\#_{b'} : \mathcal{K} \rightarrow \mathbb{Z}_m$  é um morfismo e é preservada pela congruência  $\cong$  devido à proposição 4.1. Como os elementos 0 e 1 de  $\mathbb{Z}_m$  são distintos se e só se  $m \geq 2$ , podemos pois supor que  $0 \neq 1$ , pois  $m \geq 2$  por hipótese.

Vamos provar que  $\lambda(b) = \widehat{1}_u$  se e só se  $b \in \mathbf{T}$ . É suficiente provar que  $p_{\omega(b)} \cong p_{\alpha(b)} b$  se e só se  $b \in \mathbf{T}$ . De fato, temos que  $\widehat{1}_u = \lambda(b) \iff \widehat{1}_u = \gamma_{\alpha(b)} \widehat{b} \gamma_{\omega(b)}^{-1} \iff \gamma_{\omega(b)} = \gamma_{\alpha(b)} \widehat{b} \iff \widehat{p_{\omega(b)}} = \widehat{p_{\alpha(b)}} \widehat{b} \iff \widehat{p_{\omega(b)}} = \widehat{p_{\alpha(b)} b} \iff p_{\omega(b)} \cong p_{\alpha(b)} b$ . Suponhamos que  $b \in \mathbf{T}$ . Como  $p_{\omega(b)}$  e  $p_{\alpha(b)} b$  são dois passeios em  $\mathbf{T}$  de  $u$  a  $\omega(b)$  e como  $\mathbf{T}$  é uma árvore com início  $u$  implicando que são únicos os passeios de  $u$  a qualquer vértice, temos que  $p_{\omega(b)} = p_{\alpha(b)} b$  e não mais há o que provar. Suponhamos agora que  $b \notin \mathbf{T}$ . Como as arestas de  $p_{\alpha(b)}$  e de  $p_{\omega(b)}$  são todas de  $\mathbf{T}$ , temos que  $\#_b(p_{\omega(b)}) = 0 \neq 1 = 0 + 1 = \#_b(p_{\alpha(b)}) + \#_b(b) = \#_b(p_{\alpha(b)} b)$  e portanto que  $p_{\omega(b)} \not\cong p_{\alpha(b)} b$  já que a congruência  $\cong$  preserva a função  $\#_b$ .

Podemos definir  $\varphi_b : \mathcal{B} \rightarrow \mathbb{Z}_m$  por  $\varphi_b(x) = \#_b(p)$  onde  $x \in \mathcal{B}$  e  $p \in \mathcal{K}$  é tal que  $x = \widehat{p}$ . Como a congruência  $\cong$  preserva  $\#_b$ , esta função é bem definida e o valor de  $\varphi_b(x)$  não depende da particular escolha de  $p$ . Como  $\#_b : \mathcal{K} \rightarrow \mathbb{Z}_m$  é um morfismo, logo segue que  $\varphi_b$  também o é.

Sejam  $b, b' \in \mathbf{G} \setminus \mathbf{T}$  duas arestas. Vamos provar que  $\lambda(b) = \lambda(b') \iff b = b'$ . Vamos primeiro provar que  $\varphi_{b'}(\gamma_v) = \varphi_{b'}(\gamma_v^{-1}) = 0$  para todo vértice  $v \in V$ . De fato  $\varphi_{b'}(\gamma_v) = \varphi_{b'}(\widehat{p}_v) = \#_{b'}(p_v) = 0$  pois  $p_v$  só tem arestas de  $\mathbf{T}$ . Para concluir esta primeira parte,  $\varphi_{b'}(\gamma_v^{-1}) = 0 + \varphi_{b'}(\gamma_v^{-1}) = \varphi_{b'}(\gamma_v) + \varphi_{b'}(\gamma_v^{-1}) = \varphi_{b'}(\gamma_v \gamma_v^{-1}) = \varphi_{b'}(\widehat{1}_u) = \#_{b'}(1_u) = 0$ . Assim sendo, observe que  $\varphi_{b'}(\lambda(b)) = \varphi_{b'}(\gamma_{\alpha(b)} \widehat{b} \gamma_{\omega(b)}^{-1}) = \varphi_{b'}(\gamma_{\alpha(b)}) + \varphi_{b'}(\widehat{b}) + \varphi_{b'}(\gamma_{\omega(b)}^{-1}) = 0 + \varphi_{b'}(\widehat{b}) + 0 = \#_{b'}(b)$ . Assim, se  $b' \neq b$ , temos que  $\varphi_{b'}(\lambda(b')) = \#_{b'}(b') = 1 \neq 0 = \#_{b'}(b) = \varphi_{b'}(\lambda(b))$  implicando pois que  $\lambda(b) \neq \lambda(b')$ . ■

### 4.3 Geradores dos grupos locais

Como na seção 4.2, supomos que  $m \geq 2$  ao longo desta seção.

Como a proposição 4.2 afirma que a função  $\lambda$  aplica  $\mathbf{T}$  em  $\{\widehat{1}_u\}$  e que somente as arestas de  $\mathbf{T}$  são mapeadas em  $\widehat{1}_u$ , é natural definirmos o grafo  $\mathbf{H}$  por

$$\mathbf{H} = \lambda(\mathbf{G} \setminus \mathbf{T}),$$

isto é,  $\mathbf{H}$  é o subgrafo de  $\mathcal{B}_u$  induzido pelas arestas  $\lambda(b)$  para  $b \in \mathbf{G} \setminus \mathbf{T}$  e possui o único vértice  $u$ . Também na mesma proposição vemos que  $\lambda$  estabelece uma injeção nas arestas de  $\mathbf{G} \setminus \mathbf{T}$ . Assim, a cardinalidade de  $\mathbf{H}$  é

$$|\mathbf{H}| = \text{número ciclomático de } \mathbf{G}.$$

Assim temos o diagrama abaixo:

$$\mathbf{G} \setminus \mathbf{T} \xleftarrow{\lambda} \mathbf{H}$$

$$\mathbf{T} \xrightarrow{\lambda} \widehat{1}_u$$

Seja  $\mathbf{H}^*$  a categoria livre gerada por  $\mathbf{H}$ . Como todas as arestas de  $\mathbf{H}$  são consecutivas,  $\mathbf{H}^*$  é de fato o monóide livre gerado por  $\mathbf{H}$ . Definimos a aplicação  $\theta : \mathbf{G} \longrightarrow \mathbf{H}^*$  por

$$\theta(b) = \begin{cases} 1_u, & \text{se } b \in \mathbf{T}; \\ \lambda(b), & \text{se } b \in \mathbf{G} \setminus \mathbf{T}. \end{cases}$$

Esta aplicação é um morfismo de grafos já que  $\mathbf{H}^*$  tem um único vértice e  $\theta$  é unicamente estendida para o morfismo de categorias  $\theta : \mathcal{K} \longrightarrow \mathbf{H}^*$ .



Definiremos dois morfismos com domínio  $\mathbf{H}^*$ . A inclusão  $\iota : \mathbf{H} \rightarrow \mathcal{B}_u$  é um morfismo de grafos e podemos de forma única estendê-la ao morfismo  $\phi : \mathbf{H}^* \rightarrow \mathcal{B}_u$ , que aplica um passeio de  $\mathbf{H}^*$  no produto em  $\mathcal{B}_u$  da seqüência das arestas do passeio. Para cada vértice  $v \in V(\mathbf{G})$ , podemos escolher um passeio  $q_v \in \mathcal{K}_{v,u}$  tal que  $\hat{q}_v = \gamma_v^{-1} = (\hat{p}_v)^{-1}$ . Assim, podemos definir a função  $\beta : \mathbf{H} \rightarrow \mathcal{K}_u$  que aplica cada  $h \in \mathbf{H}$  em

$$\beta(h) \stackrel{\text{def}}{=} p_{\alpha(b)} b q_{\omega(b)}$$

onde  $b = \lambda^{-1}(h) \in \mathbf{G} \setminus \mathbf{T}$ . Esta função é um morfismo de grafos e podemos de forma única estendê-la ao morfismo  $\beta : \mathbf{H}^* \rightarrow \mathcal{K}_u$ . Mais especificamente, dado  $h_1 h_2 \cdots h_k \in \mathbf{H}^*$  um passeio em  $\mathbf{H}$ , definimos

$$\beta(h_1 h_2 \cdots h_k) = \begin{cases} \beta(h_1) \beta(h_2) \cdots \beta(h_k) & \text{se } k > 0; \\ 1_u, & \text{se } k = 0. \end{cases}$$

O domínio dos morfismos  $\lambda$  e  $\theta$  é  $\mathcal{K}$ , como também ocorre com o morfismo  $\hat{\cdot}$ . Contudo, somente a restrição de  $\hat{\cdot}$  a  $\mathcal{K}_u$  tem imagem em  $\mathcal{B}_u$ . Por este motivo, estamos mais interessados nas restrições dos morfismos  $\lambda$ ,  $\theta$  e  $\hat{\cdot}$  a  $\mathcal{K}_u$ . Considerando estas restrições, estes morfismos podem ser todos representados no diagrama visto na figura 4.1. Em geral, este diagrama não

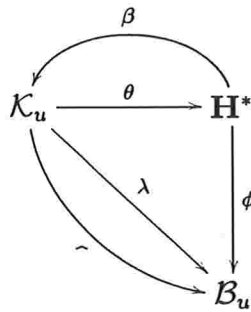


Figura 4.1: Diagrama dos morfismos  $\hat{\cdot}$ ,  $\lambda$ ,  $\theta$ ,  $\phi$  e  $\beta$

comuta. Até porque os morfismos  $\beta$  e  $\theta$  não são inversos um do outro. Todavia, alguns subdiagramas seus comutam, como veremos nas proposições 4.3 e 4.5.

Na proposição 4.3 veremos que são equivalentes a projeção canônica de  $\mathcal{K}$  em  $\mathcal{B}$  e a normalização de passeios quando nos restringimos a passeios

de  $\mathcal{K}_u$ . Também verificamos que a normalização  $\lambda$  pode ser fatorada pelos morfismos  $\theta$  e  $\phi$ . De outra forma, os diagramas vistos na figura 4.2 comutam. Como conseqüência a ser vista no corolário 4.4 temos que o grafo  $\mathbf{H}$  é um grafo



Figura 4.2: Diagramas dos morfismos  $\theta$ ,  $\phi$  e  $\lambda$  bem como  $\hat{\lambda}$  e  $\lambda$

gerador de  $\mathcal{B}_u$  e a normalização revela-se assim uma importante ferramenta no estudo de  $\mathcal{B}_u$ .

**Proposição 4.3** *Seja  $p \in \mathcal{K}$ . Então  $\lambda(p) = \phi(\theta(p)) = \gamma_{\alpha(p)} \hat{p} \gamma_{\omega(p)}^{-1}$ . Em particular temos que  $\hat{p} = \lambda(p) = \phi(\theta(p))$  quando  $p \in \mathcal{K}_u$ .*

*Prova.* Observe que se  $p \in \mathcal{K}_u$  então temos que  $\alpha(p) = \omega(p) = u$  sendo que  $p_u = 1_u$ . Por definição temos então que  $\gamma_{\alpha(p)} = \gamma_{\omega(p)} = \hat{p}_u = \hat{1}_u$ .

Suponha primeiro o caso em que  $p = 1_v$  para algum vértice  $v$ . Da definição temos  $\lambda(p) = \hat{1}_u = \gamma_v \hat{1}_v \gamma_v^{-1} = \gamma_{\alpha(p)} \hat{p} \gamma_{\omega(p)}^{-1}$ . Da mesma forma temos que  $\phi(\theta(p)) = \hat{1}_u = \lambda(p)$ .

Suponha agora o caso em que  $p = b_1 b_2 \cdots b_k \in \mathcal{K}$  com  $k > 0$  e  $b_i \in \mathbf{G}$  para  $i \in \{1, 2, \dots, k\}$ . Para cada  $i \in \{1, 2, \dots, k-1\}$ , temos  $\alpha(b_{i+1}) = \omega(b_i)$  e portanto  $\hat{b}_i \gamma_{\omega(b_i)}^{-1} \gamma_{\alpha(b_{i+1})} = \hat{b}_i \gamma_{\omega(b_i)}^{-1} \gamma_{\omega(b_i)} = \hat{b}_i \widehat{1_{\omega(b_i)}} = \hat{b}_i$ . Assim,  $\lambda(p) = \lambda(b_1) \cdots \lambda(b_k) = \gamma_{\alpha(b_1)} \hat{b}_1 \gamma_{\omega(b_1)}^{-1} \gamma_{\alpha(b_2)} \hat{b}_2 \cdots \hat{b}_{k-1} \gamma_{\omega(b_{k-1})}^{-1} \gamma_{\alpha(b_k)} \hat{b}_k \gamma_{\omega(b_k)}^{-1} = \gamma_{\alpha(b_1)} \hat{b}_1 \cdots \hat{b}_k \gamma_{\omega(b_k)}^{-1} = \gamma_{\alpha(b_1)} \hat{p} \gamma_{\omega(b_k)}^{-1}$  e segue que  $\lambda(p) = \gamma_{\alpha(p)} \hat{p} \gamma_{\omega(p)}^{-1}$ . Seja  $i_1, i_2, \dots, i_l$  a subsequência de  $1, 2, \dots, k$  formada pelos índices  $i$  tais que  $b_i \notin \mathbf{T}$ . Como  $\lambda(b_i) = \hat{1}_u$  sempre que  $b_i \in \mathbf{T}$  devido à proposição 4.2, temos pois que  $\lambda(p) = \lambda(b_1) \lambda(b_2) \cdots \lambda(b_k) = \lambda(b_{i_1}) \lambda(b_{i_2}) \cdots \lambda(b_{i_l})$ . Por fim,  $\phi(\theta(p)) = \phi((\lambda(b_{i_1}), \lambda(b_{i_2}), \dots, \lambda(b_{i_l}))) = \lambda(b_{i_1}) \lambda(b_{i_2}) \cdots \lambda(b_{i_l}) = \lambda(p)$ . ■

**Corolário 4.4** *O grafo  $\mathbf{H}$  é um grafo gerador de  $\mathcal{B}_u$ .*

*Prova.* Como  $\widehat{p} = \phi(\theta(p))$  quando  $p \in \mathcal{K}_u$ , temos que  $\mathcal{B}_u = \widehat{\mathcal{K}_u} = \phi(\theta(\mathcal{K}_u)) \subseteq \phi(\mathbf{H}^*) \subseteq \mathcal{B}_u$  pois os contradomínios de  $\theta$  e de  $\phi$  são respectivamente  $\mathbf{H}^*$  e  $\mathcal{B}_u$ . Como o primeiro e o último termo da cadeia de inclusões é o mesmo termo  $\mathcal{B}_u$ , todas as inclusões são identidades e  $\mathcal{B}_u = \phi(\mathbf{H}^*)$ . ■

Na proposição 4.5 vemos que o morfismo  $\phi : \mathbf{H}^* \rightarrow \mathcal{B}_u$  pode ser fatorado pelos morfismos  $\beta$  e  $\widehat{\cdot}$ . Isto equivale a dizer que o diagrama apresentado na figura 4.3 comuta. A proposição 4.6 completa o estudo do

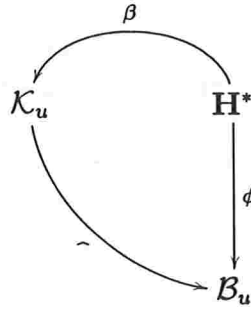


Figura 4.3: Diagrama dos morfismos  $\widehat{\cdot}$ ,  $\phi$  e  $\beta$

morfismo  $\phi$  através de uma caracterização da congruência  $\phi^{-1} \circ \phi$ .

**Proposição 4.5** *Seja  $x \in \mathbf{H}^*$ . Então temos que  $\phi(x) = \widehat{\beta(x)}$ .*

*Prova.* Seja  $h \in \mathbf{H}$  e seja  $b = \lambda^{-1}(h) \in \mathbf{G} \setminus \mathbf{T}$ . Das definições de  $\beta$  e dos passeios da forma  $q_{\omega(b)}$ , temos que  $\widehat{\beta(h)} = p_{\alpha(b)} \widehat{b} q_{\omega(b)} = \widehat{p_{\alpha(b)}} \widehat{b} \widehat{q_{\omega(b)}} = \gamma_{\alpha(b)} \widehat{b} \gamma_{\omega(b)}^{-1} = \lambda(b) = h$ . Assim  $\widehat{\cdot} \circ \beta : \mathbf{H}^* \rightarrow \mathcal{B}_u$  é um morfismo que estende a inclusão  $\iota : \mathbf{H} \rightarrow \mathcal{B}_u$ . Por definição, segue que  $\widehat{\cdot} \circ \beta = \phi$ . ■

**Proposição 4.6** *A congruência  $\phi^{-1} \circ \phi$  é a menor congruência em  $\mathbf{H}^*$  contendo o conjunto  $\{(x^m, 1_u) \mid x \in \mathbf{H}^*\}$ .*

*Prova.* Seja  $\approx$  a menor congruência em  $\mathbf{H}^*$  contendo o conjunto  $\{(x^m, 1_u) \mid x \in \mathbf{H}^*\}$ . Sejam  $x$  e  $x'$  dois passeios quaisquer de  $\mathbf{H}^*$  e sejam  $p, p'$  dois passeios quaisquer de  $\mathcal{K}_u$ .

Vamos provar que se  $x \approx x'$  então  $\beta(x) \cong \beta(x')$ . Equivale a mostrar que a congruência  $\approx$  preserva o valor de  $\widehat{\cdot} \circ \beta$ . É suficiente provar no caso

em que  $(x, x')$  é uma substituição por  $(t^m, 1_u)$ . Supondo a existência de  $r, s, t \in \mathbf{H}^*$  tais  $x = rt^m s$  e  $x' = rs$ , como  $\beta$  é um morfismo de categorias, temos que  $\beta(x) = \beta(rt^m s) = \beta(r) \beta(t)^m \beta(s) \cong \beta(r) \beta(s) = \beta(rs) = \beta(x')$ .

Vamos provar que se  $p \cong p'$  então  $\theta(p) \approx \theta(p')$ . Provaremos que a congruência  $\cong$  preserva a classe de congruência de  $\theta(p)$  por  $\approx$ . É suficiente provar que  $\theta(p) \approx \theta(p')$  quando existem  $r, s, t \in \mathcal{K}$  passeios tais que  $p = rt^m s$  e  $p' = rs$ . Como  $\theta$  é um morfismo de categorias, temos que  $\theta(p) = \theta(rt^m s) = \theta(r) \theta(t)^m \theta(s) \approx \theta(r) \theta(s) = \theta(rs) = \theta(p')$ .

Vamos provar que  $x \approx \theta \circ \beta(x)$ . Faremos uma indução no comprimento de  $x$ . Caso  $x = 1_u$ , não há o que provar já que  $\theta \circ \beta(x) = 1_u$ . Suponhamos pois que  $|x| > 0$ . Seja  $h \in \mathbf{H}$  a última aresta de  $x$ , seja  $y = xh^{-1}$  e suponha por indução que  $y \approx \theta \circ \beta(y)$ . Seja  $b = \lambda^{-1}(h) \in \mathbf{G} \setminus \mathbf{T}$ . Seja  $v \in V(\mathbf{G})$  um vértice qualquer. Ora,  $\widehat{p_v q_v} = \widehat{p_v} \widehat{q_v} = \widehat{p_v} (\widehat{p_v})^{-1} = \widehat{1_u}$  e, portanto,  $p_v q_v \cong 1_u$  implicando pois que  $\theta(p_v q_v) \approx \theta(1_u)$  conforme visto antes. Dado que todas as arestas de  $p_v$  são de  $\mathbf{T}$  temos portanto que  $\theta(p_v) = 1_u$  e também que  $\theta(q_v) = 1_u \theta(q_v) = \theta(p_v) \theta(q_v) = \theta(p_v q_v) \approx \theta(1_u) = 1_u$ . Como  $\beta(h) = p_{\alpha(b)} b q_{\omega(b)}$ , temos que  $\theta \circ \beta(h) = \theta(p_{\alpha(b)} b q_{\omega(b)}) = \theta(p_{\alpha(b)}) \theta(b) \theta(q_{\omega(b)}) \approx 1_u \theta(b) 1_u = h$ . Usando o fato de que  $\theta \circ \beta$  é um morfismo e que  $\approx$  é uma congruência temos finalmente que  $\theta \circ \beta(x) = \theta \circ \beta(yh) = (\theta \circ \beta(y)) (\theta \circ \beta(h)) \approx y h = x$ .

Vamos provar que  $\phi(x) = \phi(x') \iff x \approx x'$ . Suponhamos primeiramente que  $x \approx x'$ . Assim temos que  $\beta(x) \cong \beta(x')$  e que  $\widehat{\beta(x)} = \widehat{\beta(x')}$ . Donde  $\phi(x) = \widehat{\beta(x)} = \widehat{\beta(x')} = \phi(x')$  devido à proposição 4.5. Suponhamos agora que  $\phi(x) = \phi(x')$ . A partir da mesma proposição,  $\widehat{\beta(x)} = \phi(x) = \phi(x') = \widehat{\beta(x')}$ . Assim,  $\beta(x) \cong \beta(x')$  e portanto  $\theta(\beta(x)) \approx \theta(\beta(x'))$ . Finalmente temos que  $x \approx \theta \circ \beta(x) \approx \theta \circ \beta(x') \approx x'$ . ■

## 4.4 Grupos locais livres

Por fim, podemos provar o principal resultado do capítulo:

**Teorema 4.7** *Seja  $m \geq 1$  e seja  $\mathbf{G}$  um grafo fortemente conexo. Seja  $\mathcal{B}$  o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por  $\mathbf{G}$ . Então, os grupos locais  $\mathcal{B}_v$  para  $v \in V(\mathbf{G})$  são isomorfos a um mesmo grupo de Burnside livre satisfazendo  $x^m = 1$ . Ademais, se  $m \geq 2$ , este grupo de Burnside é livre sobre o conjunto de geradores  $\mathbf{H}$ , cuja cardinalidade é o número ciclomático do grafo  $\mathbf{G}$ .*

*Prova.* Suponhamos primeiro que  $m = 1$ . Seja  $v \in V(\mathbf{G})$  e seja  $x \in \mathcal{K}_v$ . Desde que  $(x, 1_v) \in \pi$ , temos que  $x \cong 1_v$ , implicando pois que  $\widehat{x} = \widehat{1}_v$ . Isto prova que o grupo local  $\mathcal{B}_v$  é trivial. De maneira análoga, temos que o grupo de Burnside livre satisfazendo  $x^m = 1$  também é trivial.

Suponha agora que  $m \geq 2$ . Considere as definições vistas nas seções 4.2 e 4.3. Seja  $\approx$  a congruência  $\phi^{-1} \circ \phi$ . Pela proposição 4.6, temos que  $\approx$  é a menor congruência em  $\mathbf{H}^*$  contendo o conjunto  $\{(x^m, 1_u) \mid x \in \mathbf{H}^*\}$ . Como já vimos,  $\mathbf{H}$  tem  $u$  como único vértice, todas as arestas são consecutivas e portanto a categoria livre  $\mathbf{H}^*$  é o monóide livre gerado por  $\mathbf{H}$ . Assim o monóide  $\mathbf{H}^*/\approx$  é o grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por  $\mathbf{H}$ . Da proposição 4.2 temos que a normalização estabelece uma bijeção de  $\mathbf{G} \setminus \mathbf{T}$  em  $\mathbf{H}$ , e que portanto a cardinalidade de  $\mathbf{H}$  é o número ciclomático de  $\mathbf{G}$ . Seja  $\delta : \mathbf{H}^* \rightarrow \mathbf{H}^*/\approx$  a projeção canônica. Assim temos que  $\phi^{-1} \circ \phi = \approx = \delta^{-1} \circ \delta$  e é imediato verificar que  $\delta \circ \phi^{-1}$  estabelece um isomorfismo entre  $\mathcal{B}_u$  e  $\mathbf{H}^*/\approx$ . Da proposição 3.1 temos que os grupos locais  $\mathcal{B}_v$ , para  $v \in V(\mathbf{G})$ , são isomorfos a  $\mathcal{B}_u$  e, portanto, ao grupo de Burnside livre  $\mathbf{H}^*/\approx$ . ■

Nalguns exemplos futuros lidaremos com o caso em que  $m = 2$ . Veremos agora que um grupóide/grupo de Burnside livre satisfazendo  $x^2 = 1$  é comutativo.

**Proposição 4.8** *Seja  $\mathcal{C}$  uma categoria e  $u \in \text{Obj}(\mathcal{C})$  um objeto seu. Se  $x^2 = 1_u$  para todo  $x \in \mathcal{C}_u$  então  $xy = yx$  para todo  $x, y \in \mathcal{C}_u$ .*

*Prova.* De fato, se  $x$  e  $y$  são dois elementos quaisquer de  $\mathcal{C}_u$  então  $yx \in \mathcal{C}_u$  e  $xy = (yx)^2xy = yxyxy = yxyxy = yxyxy = yx$ . ■



# Capítulo 5

## Entradas e transições

Ao longo deste capítulo, suporemos  $\mathcal{M}$  um monóide estável. Isto se dará porque os resultados aqui presentes são gerais o suficiente para qualquer monóide estável, apesar do nosso interesse ser o estudo de um particular monóide estável: o monóide de Burnside livre. Esta generalidade vale em particular para o resultado que consideramos maximal neste capítulo: o lema 5.14.

Na seção 5.1 daremos as definições preliminares do capítulo e definiremos as relações Green-induzidas, que dão ao monóide livre  $A^*$  uma estrutura induzida pelas relações de Green no monóide  $\mathcal{M}$  e por um morfismo de  $A^*$  sobre  $\mathcal{M}$ . Nas seções 5.2 e 5.3 veremos as definições de alguns conceitos básicos — as  $\mathcal{D}$ -entradas e as transições respectivamente — bem como alguns resultados envolvendo estes conceitos. Sobre estes conceitos se fundará a constituição de um grafo fundamental de uma  $\mathcal{D}$ -classe de um monóide de Burnside livre, como será visto na seção 6.3 do capítulo 6. Na seção 5.4 veremos uma aplicação importante das transições de uma palavra: o lema 5.14 acima mencionado. Este lema será usado na demonstração do teorema 7.5.

### 5.1 Relações Green-induzidas

Adiantamos que neste capítulo suporemos  $\mathcal{M}$  um monóide estável (a definição segue logo abaixo). Além disso suporemos  $A$  um alfabeto e um morfismo

$$\tilde{\phantom{a}} : A^* \longrightarrow \mathcal{M}$$

onde  $A^*$  é o monóide livre gerado por  $A$ . A imagem de uma palavra  $w \in A^*$  pelo morfismo  $\tilde{\phantom{x}}$  será denotada por  $\tilde{w}$  e definimos a congruência  $\sim$  induzida por  $\tilde{\phantom{x}}$  como sendo

$$w \sim w' \iff \tilde{w} = \tilde{w}'.$$

Nesta seção em particular, também veremos algumas definições e propriedades válidas para monóides quaisquer.

Neste parágrafo, relembremos alguns conceitos elementares da teoria de semigrupos. Em particular as relações de Green e as propriedades relativas aos monóides estáveis, inclusive o conteúdo da proposição 5.2, podem ser encontrados nalgum livro introdutório como o de Lallement [21]. Se  $M$  é um monóide qualquer, as *relações de Green*  $\mathcal{J}$ ,  $\mathcal{R}$ ,  $\mathcal{L}$ ,  $\mathcal{H}$  e  $\mathcal{D}$  são definidas sobre  $M$  como de costume, bem como as quase-ordens  $\leq_{\mathcal{J}}$ ,  $\leq_{\mathcal{R}}$  e  $\leq_{\mathcal{L}}$ . Dados  $x, y \in M$ , definimos:

$$\begin{aligned} x \leq_{\mathcal{J}} y &\iff MxM \subseteq MyM \\ x \leq_{\mathcal{R}} y &\iff xM \subseteq yM \\ x \leq_{\mathcal{L}} y &\iff Mx \subseteq My \\ x \mathcal{J} y &\iff MxM = MyM \\ x \mathcal{R} y &\iff xM = yM \\ x \mathcal{L} y &\iff Mx = My \\ x \mathcal{H} y &\iff x \mathcal{R} y \text{ e } x \mathcal{L} y \\ x \mathcal{D} y &\iff \exists z \in M \mid x \mathcal{R} z \mathcal{L} y \end{aligned}$$

Dizemos que um elemento  $e \in M$  é *idempotente* se  $e = e^2$ . Dizemos que um elemento  $x \in M$  é *regular* se existe  $y \in M$  tal que  $x = xyx$  e, caso contrário, dizemos que  $x$  é *irregular*. A regularidade ou não de um elemento é uma propriedade inerente a uma  $\mathcal{D}$ -classe e toda  $\mathcal{D}$ -classe regular tem ao menos um idempotente. Os subsemigrupos maximais que são grupos são as  $\mathcal{H}$ -classes regulares que possuem um idempotente, que por sinal faz o papel de elemento neutro do grupo. Dizemos que  $M$  é um *monóide estável* se para quaisquer  $x, y, z \in M$  tivermos que:

$$yz \mathcal{J} y \iff yz \mathcal{R} y \quad \text{e} \quad xy \mathcal{J} y \iff xy \mathcal{L} y.$$

Um monóide é dito de *torção* se todos os submonóides monogerados forem finitos. De outra forma, para todo elemento  $x \in M$  existem inteiros  $p, q > 0$  tais que  $x^p = x^{p+q}$ . Como veremos na proposição 5.2, duas classes importantes de monóides estáveis são os monóides finitos e os de torção (onde, veremos



oportunamente, incluem-se os monóides de Burnside livres). Também veremos que  $\mathcal{J} = \mathcal{D}$  quando o monóide é estável.

O morfismo  $\tilde{\phantom{x}} : A^* \longrightarrow \mathcal{M}$  e as relações de Green em  $\mathcal{M}$  induzem outras relações  $\mathcal{J}'$ ,  $\mathcal{R}'$ ,  $\mathcal{L}'$ ,  $\mathcal{H}'$  e  $\mathcal{D}'$  em  $A^*$  da seguinte forma:

$$x \rho' y \iff \tilde{x} \rho \tilde{y}, \text{ para } \rho \in \{\mathcal{J}, \mathcal{R}, \mathcal{L}, \mathcal{H}, \mathcal{D}\}.$$

Estas relações serão chamadas de *relações Green-induzidas pelo morfismo  $\tilde{\phantom{x}}$*  ou simplesmente *relações Green-induzidas* se for claro o morfismo  $\tilde{\phantom{x}}$ . Estas relações são equivalências, já que as relações de Green definidas sobre  $\mathcal{M}$  o são. Como  $\mathcal{D} = \mathcal{R} \vee \mathcal{L}$  segue de imediato que  $\mathcal{D}' = \mathcal{R}' \vee \mathcal{L}'$ . Como  $\mathcal{R}$  é uma congruência à esquerda, segue que  $\mathcal{R}'$  é uma congruência à esquerda. Como  $\mathcal{L}$  é uma congruência à direita, também  $\mathcal{L}'$  o será. Em prestaremos às palavras de  $A^*$  três qualificações importantes vistas nos elementos de  $\mathcal{M}$ : diremos que uma palavra  $w$  é  $\sim$ -idempotente,  $\sim$ -regular ou  $\sim$ -irregular conforme  $\tilde{w}$  seja respectivamente idempotente, regular ou irregular.

Veremos um exemplo destas relações no exemplo 5.1. Definiremos uma particular congruência  $\sim$  sobre  $A^*$  e, a partir desta congruência, definiremos o monóide  $\mathcal{M} = A^*/\sim$  e a projeção canônica  $\tilde{\phantom{x}} : A^* \longrightarrow \mathcal{M}$ . Para a definição de  $\sim$  usaremos a função  $\#_a$  com domínio  $A^*$  definida na seção 3.3 do capítulo 3. Para tanto, estaremos supondo  $m = 2$  no exemplo e portanto  $\#_a$  aplica uma palavra  $w$  na paridade do número de ocorrências de uma letra  $a$  em  $w$ . Também definimos o *conteúdo* de  $w$  por

$$c(w) \stackrel{\text{def}}{=} \text{o conjunto das letras de } A \text{ que ocorrem em } w.$$

A demonstração das afirmativas presentes no exemplo 5.1 é deixada como exercício ao leitor. Este exemplo ilustrará vários outros conceitos a serem definidos ao longo deste capítulo e outras afirmativas sobre sua estrutura serão feitas.

**Exemplo 5.1** *Seja  $\sim$  a congruência em  $A^*$  definida por:*

$$x \sim y \text{ se e só se } c(x) = c(y) \text{ e } \#_a(x) = \#_a(y) \text{ para todo } a \in A.$$

*Seja  $\mathcal{M}$  o monóide  $A^*/\sim$ , seja a projeção canônica  $\tilde{\phantom{x}} : A^* \longrightarrow \mathcal{M}$  e sejam as relações Green-induzidas. Então  $\mathcal{M}$  é isomorfo ao produto cartesiano de  $|A|$  cópias do monóide  $\langle a \mid a = aaa \rangle$  e é comutativo. Ademais  $\mathcal{J}' = \mathcal{D}' = \mathcal{R}' = \mathcal{L}' = \mathcal{H}'$  sendo que  $u \mathcal{J}' v$  se e só se  $c(u) = c(v)$ , para  $u$  e  $v$  palavras quaisquer.*

Na proposição 5.2 vemos que  $\mathcal{J} = \mathcal{D}$  já que o monóide  $\mathcal{M}$  é estável por hipótese. Isto implica que  $\mathcal{J}' = \mathcal{D}'$ , como veremos no corolário 5.3.

**Proposição 5.2** *Valem as seguintes propriedades:*

- *Todo monóide finito é de torção.*
- *Todo monóide de torção é estável.*
- *Num monóide estável, as relações  $\mathcal{J}$  e  $\mathcal{D}$  coincidem.*

*Prova.* Ao contrário do resto do capítulo, nesta demonstração, as relações de Green são definidas sobre um monóide não necessariamente estável.

Que todo monóide finito é de torção, é imediato.

Vamos provar que todo monóide de torção é estável. Vamos primeiro provar que  $xy \mathcal{J} y \iff xy \mathcal{L} y$ . Como  $\mathcal{L} \subseteq \mathcal{J}$ , basta provar que  $xy \mathcal{J} y \implies xy \mathcal{L} y$ . Suponha  $x, y \in \mathcal{M}$  tais que  $xy \mathcal{J} y$ . Então temos que existem elementos  $u, v$  tais que  $y = uxyv$ . Isto implica imediatamente que  $y = (ux)^i y v^i$  para todo  $i \geq 0$ . Se o monóide é de torção, existem  $p, q > 0$  inteiros tais que  $(ux)^p = (ux)^{p+q}$ . Então temos que  $y = (ux)^p y v^p = (ux)^q (ux)^p y v^p = (ux)^q y = (ux)^{q-1} uxy \leq_{\mathcal{L}} xy \leq_{\mathcal{L}} y$  implicando pois que  $xy \mathcal{L} y$ , conforme queríamos demonstrar. De maneira dual podemos provar que  $yz \mathcal{J} y \iff yz \mathcal{R} y$ .

Sejam  $x, y, z, u, v, w$  elementos de um monóide estável tais que  $v \mathcal{J} y$ , que  $v = xyz$  e que  $y = uvw$ . Vamos mostrar que  $v = xyz \mathcal{R} xy \mathcal{L} y \mathcal{R} yz \mathcal{L} xyz = v$ . De fato,  $y = uvw = uxyzw \leq_{\mathcal{J}} yz \leq_{\mathcal{J}} y$ . Assim temos que  $yz \mathcal{J} y$  e portanto que  $yz \mathcal{R} y$  pois o monóide é estável. Como  $\mathcal{R}$  é uma congruência à esquerda, temos que  $xyz \mathcal{J} xy$ . De forma dual provamos que  $xy \mathcal{L} y$  e que  $xyv \mathcal{L} yv$ .

Isto prova que  $\mathcal{J} = \mathcal{D}$  em todo monóide estável. De fato, pelas definições do parágrafo anterior, temos que se  $y \mathcal{J} v$  então  $y \mathcal{R} yz \mathcal{L} xyz = v$ , e portanto  $y \mathcal{D} v$ . ■

**Corolário 5.3** *Sejam  $x, y, z \in A^*$ . Então temos que:*

1.  $\mathcal{J}' = \mathcal{D}'$ ;
2.  $yz \mathcal{D}' y \iff yz \mathcal{R}' y$ ;
3.  $xy \mathcal{D}' y \iff xy \mathcal{L}' y$ ;

$$4. \quad xyz \mathcal{D}' y \iff xyz \mathcal{R}' xy \mathcal{L}' y \mathcal{R}' yz \mathcal{L}' xyz.$$

*Prova.* Como  $\mathcal{M}$  é estável, a proposição 5.2 implica que  $\mathcal{J} = \mathcal{D}$ . Assim,  $x \mathcal{D}' y \iff \tilde{x} \mathcal{D} \tilde{y} \iff \tilde{x} \mathcal{J} \tilde{y} \iff x \mathcal{J}' y$ , seguindo o item 1. Como  $\mathcal{M}$  é estável e  $\mathcal{J} = \mathcal{D}$ , a partir da definição de estabilidade temos que  $\tilde{y}z \mathcal{D} \tilde{y} \iff \tilde{y}z \mathcal{J} \tilde{y} \iff \tilde{y}z \mathcal{R} \tilde{y}$  e que  $\tilde{x}y \mathcal{D} \tilde{y} \iff \tilde{x}y \mathcal{J} \tilde{y} \iff \tilde{x}y \mathcal{L} \tilde{y}$ . Da definição das relações Green-induzidas seguem os itens 2 e 3. Vamos agora provar o item 4. Como  $\mathcal{D}' = \mathcal{R}' \vee \mathcal{L}'$ , segue de imediato que  $y \mathcal{R}' yz \mathcal{L}' xyz \implies xyz \mathcal{D}' y$ . Suponha agora que  $xyz \mathcal{D}' y$  e sejam  $v = xyz$  e  $u, w \in A^*$  tais que  $uvw \sim y$ . Assim,  $\tilde{v} = \tilde{x}\tilde{y}\tilde{z}$  e  $\tilde{y} = \tilde{u}\tilde{v}\tilde{w}$ . A partir da demonstração da proposição 5.2 temos que  $\tilde{v} = \tilde{x}\tilde{y}\tilde{z} \mathcal{R} \tilde{x}\tilde{y} \mathcal{L} \tilde{y} \mathcal{R} \tilde{y}\tilde{z} \mathcal{L} \tilde{x}\tilde{y}\tilde{z} = \tilde{v}$ . Da definição da relações Green-induzidas segue direto que  $xyz \mathcal{R}' xy \mathcal{L}' y \mathcal{R}' yz \mathcal{L}' xyz$ . ■

Dado que estaremos supondo  $\mathcal{M}$  um monóide estável, vale observar que a proposição 3.7 [21], enunciada na proposição 5.4 logo abaixo, possibilita a constituição de definições equivalentes de um monóide estável. O conteúdo da proposição 5.4 vale naturalmente em sua versão dual para as  $\mathcal{L}$ -classes de uma  $\mathcal{J}$ -classe.

**Proposição 5.4** *Seja  $J$  uma  $\mathcal{J}$ -classe de um semigrupo qualquer  $S$ . As seguintes afirmativas são equivalentes:*

1.  $yz \mathcal{J} y \iff yz \mathcal{R} y$  para algum  $y \in J$  e para todo  $z \in S$ ;
2.  $yz \mathcal{J} y \iff yz \mathcal{R} y$  para todo  $y \in J$  e para todo  $z \in S$ ;
3. existe uma  $\mathcal{R}$ -classe em  $J$  que é minimal dentre as  $\mathcal{R}$ -classes em  $J$ ;
4. toda  $\mathcal{R}$ -classe em  $J$  é minimal dentre as  $\mathcal{R}$ -classes em  $J$ .

## 5.2 Entradas

Seja  $w \in A^+$ . Definimos  $\epsilon_R(w)$  a  $\mathcal{R}$ -entrada de  $w$  como sendo o mais curto prefixo de  $w$  que pertence à mesma  $\mathcal{R}'$ -classe de  $w$  e dizemos simplesmente que  $w$  é uma  $\mathcal{R}$ -entrada se  $\epsilon_R(w) = w$ . Observe que  $y$  é a  $\mathcal{R}$ -entrada de  $w$  se e só se  $y$  for uma  $\mathcal{R}$ -entrada e  $w \mathcal{R}' y \in \text{Pref}(w)$ . Ademais, qualquer prefixo  $u$  de  $w$  que tenha comprimento maior ou igual ao de  $\epsilon_R(w)$  está na mesma  $\mathcal{R}'$ -classe de  $w$ . De fato,  $w \mathcal{R}' \epsilon_R(w) \in \text{Pref}(u) \subseteq \text{Pref}(w)$  implica que  $\tilde{w} \leq_{\mathcal{R}} \tilde{u} \leq_{\mathcal{R}} \epsilon_R(w) \mathcal{R} \tilde{w}$ , que por sua vez implica que  $\tilde{u} \mathcal{R} \tilde{w}$ . De forma

dual, definimos  $\epsilon_L(w)$  a  $\mathcal{L}$ -entrada de  $w$  como sendo o mais curto sufixo de  $w$  que pertence à mesma  $\mathcal{L}'$ -classe de  $w$  e dizemos simplesmente que  $w$  é uma  $\mathcal{L}$ -entrada se  $\epsilon_L(w) = w$ . Observe que  $y$  é a  $\mathcal{L}$ -entrada de  $w$  se e só se  $y$  for uma  $\mathcal{L}$ -entrada e  $w \mathcal{L}' y \in \text{Suf}(w)$ . Ademais, qualquer sufixo de  $w$  que tenha comprimento maior ou igual ao de  $\epsilon_L(w)$  está na mesma  $\mathcal{L}'$ -classe de  $w$ .

Relembramos que na seção 3.2 do capítulo 3 definimos fatorações e algumas ordens sobre as mesmas. Sejam  $x, y, z, w \in A^*$ . Dizemos<sup>1</sup> que  $y$  é uma  $\mathcal{D}$ -entrada de  $w$  se  $y$  for um fator de  $w$  e se o único fator de  $y$  na mesma  $\mathcal{D}'$ -classe de  $w$  for o próprio  $y$ . Dizemos simplesmente que  $w$  é uma  $\mathcal{D}$ -entrada se  $w$  for uma  $\mathcal{D}$ -entrada de  $w$ . Observe que  $y$  é uma  $\mathcal{D}$ -entrada de  $w$  se e só se  $y$  for uma  $\mathcal{D}$ -entrada e  $w \mathcal{D}' y \in \text{Fat}(w)$ . Chamamos de *ocorrência de  $\mathcal{D}$ -entrada de  $w$*  a toda fatoração  $(x, y, z)$  de  $w$  tal que  $y$  seja uma  $\mathcal{D}$ -entrada de  $w$ . Neste caso, como nenhum fator próprio de  $y$  está mesma  $\mathcal{D}'$ -classe de  $y$  e de  $w$ , esta fatoração  $(x, y, z)$  é minimal dentre aquelas em que  $y \mathcal{D}' w$ . Existe em geral mais de uma ocorrência de  $\mathcal{D}$ -entrada de  $w$  e as ocorrências de  $\mathcal{D}$ -entradas de  $w$  são incomparáveis por  $\leq$ . Qualquer fator  $u$  de  $w$  que tenha por fator  $y$ , uma  $\mathcal{D}$ -entrada de  $w$ , está na mesma  $\mathcal{D}'$ -classe de  $w$  e de  $y$ . De fato,  $w \mathcal{J}' y \in \text{Fat}(u) \subseteq \text{Fat}(w)$  implica  $\tilde{w} \leq_{\mathcal{J}} \tilde{u} \leq_{\mathcal{J}} \tilde{y} \mathcal{J} \tilde{w}$  e  $\tilde{u} \mathcal{J} \tilde{w}$ . Assim  $u \mathcal{D}' w$  pois  $\mathcal{D}' = \mathcal{J}'$  devido ao item 1 do corolário 5.3.

Considere o exemplo 5.1. Uma vez caracterizadas as relações Green-induzidas, podemos facilmente caracterizar as  $\mathcal{R}$ -entradas,  $\mathcal{L}$ -entradas e  $\mathcal{D}$ -entradas para este caso. Dadas palavras quaisquer  $u$  e  $v$  e letras quaisquer  $a$  e  $b$  temos que:  $ua$  é uma  $\mathcal{R}$ -entrada se e só se  $a \notin c(u)$ ;  $au$  é uma  $\mathcal{L}$ -entrada se e só se  $a \notin c(u)$ ;  $aub$  é uma  $\mathcal{D}$ -entrada se e só se  $a, b \notin c(u)$  e  $a \neq b$ ;  $a$  é uma  $\mathcal{D}$ -entrada. Em particular, dada a palavra  $w = aabcccabcb$  temos que  $\epsilon_R(w) = aabc$ , que  $\epsilon_L(w) = abcb$ , que  $bccca$  é uma  $\mathcal{D}$ -entrada de  $w$  e que  $(a, abc, ccabcb)$  e  $(aabccc, abc, b)$  são duas diferentes ocorrências de  $\mathcal{D}$ -entradas de  $w$ .

Na proposição 5.5 relacionamos o conceito de  $\mathcal{D}$ -entrada com os conceitos de  $\mathcal{R}$ -entrada e  $\mathcal{L}$ -entrada.

**Proposição 5.5** *Uma palavra  $w \in A^+$  é uma  $\mathcal{D}$ -entrada se e só se for simultaneamente uma  $\mathcal{R}$ -entrada e uma  $\mathcal{L}$ -entrada.*

*Prova.* Suponha que  $w$  seja uma  $\mathcal{D}$ -entrada. Observe que  $\epsilon_R(w) \mathcal{D}' w$  pois  $\epsilon_R(w) \mathcal{R}' w$  e  $\mathcal{R}' \subseteq \mathcal{D}'$ . Como  $w$  é o único fator de  $w$  na  $\mathcal{D}'$ -classe de  $w$ ,

<sup>1</sup>Devido à minimalidade da fatoração, seria natural definir o conceito de  $\mathcal{J}$ -entrada impondo a restrição  $y \mathcal{J}' w$ . Para manter compatibilidade com a terminologia de trabalhos anteriores, adotamos as definições atuais, já que os conceitos são equivalentes pois  $\mathcal{J}' = \mathcal{D}'$ .

$\epsilon_R(w) = w$  e  $w$  é uma  $\mathcal{R}$ -entrada. De forma dual provamos que  $w$  é uma  $\mathcal{L}$ -entrada.

Suponha agora que  $w$  seja uma  $\mathcal{R}$ -entrada e uma  $\mathcal{L}$ -entrada. Seja  $(x, y, z)$  uma fatoração de  $w$  em que  $y \mathcal{D}' w$ . Usando o item 4 do corolário 5.3 temos que  $w = xyz \mathcal{R}' xy \mathcal{L}' y \mathcal{R}' yz \mathcal{L}' xyz = w$ . Como  $\epsilon_R(w) = w$  e  $w = xyz \mathcal{R}' xy$  temos que  $z = 1$ . Como  $\epsilon_L(w) = w$  e  $w = xyz \mathcal{L}' yz$  temos que  $x = 1$ . Isto prova que  $w$  é o único fator de  $w$  na  $\mathcal{D}'$ -classe de  $w$  e que, portanto,  $w$  é uma  $\mathcal{D}$ -entrada. ■

Na proposição 5.7, vemos uma caracterização das  $\mathcal{R}$ -entradas: elas têm por sufixo uma  $\mathcal{D}$ -entrada e não há outra ocorrência de  $\mathcal{D}$ -entrada. Vale também a propriedade dual no caso das  $\mathcal{L}$ -entradas. Antes veremos na proposição 5.6 outra propriedade a respeito das  $\mathcal{R}$ -entradas.

**Proposição 5.6** *Um sufixo não vazio de uma  $\mathcal{R}$ -entrada é também uma  $\mathcal{R}$ -entrada e um prefixo não vazio de uma  $\mathcal{L}$ -entrada é também uma  $\mathcal{L}$ -entrada.*

*Prova.* Seja  $u$  uma  $\mathcal{R}$ -entrada e sejam  $a \in A$  e  $u'', u' \in A^*$  tais que  $u = u''u'a$ . Suponha por absurdo que  $\epsilon_R(u'a) \neq u'a$ . Neste caso temos que  $|\epsilon_R(u'a)| < |u'a|$  e portanto que  $|\epsilon_R(u'a)| \leq |u'|$ . Assim temos que  $u' \mathcal{R}' u'a$ . Como  $\mathcal{R}'$  é uma congruência à esquerda, temos que  $u''u' \mathcal{R}' u''u'a = u$ , contradizendo com o fato de que  $\epsilon_R(u) = u = u''u'a$ . De forma dual, provamos que um prefixo não vazio de uma  $\mathcal{L}$ -entrada é também uma  $\mathcal{L}$ -entrada. ■

**Proposição 5.7** *Uma palavra  $w \in A^+$  é uma  $\mathcal{R}$ -entrada se e só se a única ocorrência de  $\mathcal{D}$ -entrada de  $w$  for  $(w\epsilon_L(w)^{-1}, \epsilon_L(w), 1)$ .*

*Prova.* Seja  $(x, y, z)$  a primeira ocorrência de  $\mathcal{D}$ -entrada de  $w$ . Como  $w \mathcal{D}' \epsilon_R(w)$ , há uma  $\mathcal{D}$ -entrada de  $w$  que ocorre no prefixo  $\epsilon_R(w)$ . Como o mais curto prefixo de  $w$  onde ocorre uma  $\mathcal{D}$ -entrada de  $w$  é  $xy$ , segue que  $|\epsilon_R(w)| \geq |xy|$ . Contudo,  $xy \mathcal{R}' w = xyz$  devido ao item 4 do corolário 5.3. Donde  $\epsilon_R(w) = xy$  por definição. O que também implica que  $(x, y, 1)$  é a primeira ocorrência de  $\mathcal{D}$ -entrada de  $\epsilon_R(w)$ , já que qualquer  $\mathcal{D}$ -entrada do prefixo  $\epsilon_R(w) \mathcal{D}' w$  é uma  $\mathcal{D}$ -entrada de  $w$ . Como não pode haver nenhuma ocorrência de  $\mathcal{D}$ -entrada de  $\epsilon_R(w)$  maior que  $(x, y, 1)$  pela ordem  $\preceq$ ,  $(x, y, 1)$  é também a única ocorrência de  $\mathcal{D}$ -entrada de  $\epsilon_R(w)$ . Usando a proposição 5.6, temos que  $\epsilon_L(\epsilon_R(w))$  é uma  $\mathcal{R}$ -entrada. Usando a proposição 5.5, temos que  $\epsilon_L(\epsilon_R(w)) \mathcal{D}' \epsilon_R(w)$  é uma  $\mathcal{D}$ -entrada de  $\epsilon_R(w)$  e portanto  $y = \epsilon_L(\epsilon_R(w))$ .

Assim,  $(\epsilon_R(w)\epsilon_L(\epsilon_R(w))^{-1}, \epsilon_L(\epsilon_R(w)), 1)$  é a única ocorrência de  $\mathcal{D}$ -entrada de  $\epsilon_R(w)$ . O resto segue de que  $w$  é uma  $\mathcal{R}$ -entrada se e só se  $\epsilon_R(w) = w$ . ■

**Corolário 5.8** *A primeira ocorrência de  $\mathcal{D}$ -entrada de uma palavra  $w \in A^+$  é  $(\epsilon_R(w)\epsilon_L(\epsilon_R(w))^{-1}, \epsilon_L(\epsilon_R(w)), \epsilon_R(w)^{-1}w)$ .*

### 5.3 Transições

Chamamos de *transição* toda palavra  $axb$  com  $a, b \in A$  tal que  $\widetilde{ax} \mathcal{D} \widetilde{axb} \mathcal{D} \widetilde{xb} \not\mathcal{D} \widetilde{x}$ . Se além de tudo,  $axb$  for um fator de  $w$  e  $axb \mathcal{D}' w$ , dizemos que  $axb$  é uma *transição de  $w$* . Uma fatoração  $(x, y, z)$  de  $w$  em que  $y$  é uma transição de  $w$  é chamada de *ocorrência de transição de  $w$*  e duas ocorrências de transições de  $w$  são incomparáveis por  $\leq$ . Definimos a *seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$*  como sendo a seqüência de todas as ocorrências de  $\mathcal{D}$ -entradas de  $w$  ordenada por ocorrência e definimos a *seqüência de ocorrências de transições de  $w$*  como sendo a seqüência de todas as ocorrências de transições de  $w$  ordenada por ocorrência. Se  $(x_1, y_1, z_1), (x_2, y_2, z_2), \dots, (x_k, y_k, z_k)$ , para  $k \geq 0$ , é a seqüência de ocorrências de transições de  $w$ , definimos a *seqüência de transições de  $w$*  como sendo a seqüência  $y_1, y_2, \dots, y_k$ .

Considere o exemplo 5.1. Uma vez caracterizada a relação  $\mathcal{D}'$ , podemos facilmente caracterizar as transições para este caso. Temos que uma palavra  $aub$ , com  $a, b \in A$ , é uma transição se e só se  $a = b$  e  $a \notin c(u)$ . Em particular, dada a palavra  $w = aabcccabcb$  temos que a seqüência de transições de  $w$  é  $abccca, bcccab, cabc$  e que a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$  é  $(a, abc, ccabcb), (aa, bccca, bcb), (aabcc, cab, cb), (aabccc, abc, b)$ . Estas seqüências podem ser vistas na figura 5.1, que ilustrará o lema 5.11. Observe ainda que a transição  $bcccab$  tem por prefixo a  $\mathcal{D}$ -entrada  $bccca$ , por sufixo a  $\mathcal{D}$ -entrada  $cab$  e não há nenhuma outra ocorrência de  $\mathcal{D}$ -entrada como fator de  $bcccab$ .

Na proposição 5.9, vemos uma caracterização das transições: elas têm por prefixo uma  $\mathcal{D}$ -entrada, por sufixo outra e não há outra ocorrência de  $\mathcal{D}$ -entrada. De um ponto de vista intuitivo, uma transição de uma palavra constitui uma transição entre duas  $\mathcal{D}$ -entradas que ocorrem consecutivamente nesta palavra.

**Proposição 5.9** *Uma dada palavra não vazia  $w \in A^+$  é uma transição se e só se a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$  for a seqüência  $(1, \epsilon_R(w), \epsilon_R(w)^{-1}w), (w\epsilon_L(w)^{-1}, \epsilon_L(w), 1)$ .*

*Prova.* Suponha que  $(r, s, t)$  seja uma fatoração qualquer de  $w$  em que  $s \mathcal{D}' w$ . Como  $s \mathcal{D}' w$  e  $s \in \text{Fat}(w)$ , qualquer  $\mathcal{D}$ -entrada de  $s$  é uma  $\mathcal{D}$ -entrada de  $w$  e qualquer  $\mathcal{D}$ -entrada de  $w$  que é fator de  $s$  é  $\mathcal{D}$ -entrada de  $s$ . Este fato será usado livremente em nossa demonstração.

Suponha que  $(r, s, t)$  seja uma ocorrência de transição de  $w$ . Vamos provar que existem  $x, y \in \text{Fat}(s)$  tais que  $(r, x, x^{-1}st)$  e  $(rsy^{-1}, y, t)$  sejam duas ocorrências de  $\mathcal{D}$ -entradas consecutivas de  $w$ . Sejam  $a, b \in A$  e  $u \in A^*$  tais que  $s = aub$  e  $w \mathcal{D}' aub \mathcal{D}' au \mathcal{D}' ub \not\mathcal{P}' u$ . Existe uma  $\mathcal{D}$ -entrada  $x$  de  $w$  que ocorre em  $au$  mas não ocorre em  $u$ . Donde  $x \in \text{Pref}(au) \subseteq \text{Pref}(s)$  e a ocorrência de  $\mathcal{D}$ -entrada de  $w$  em questão é  $(r, x, x^{-1}st)$ . Não há outra  $\mathcal{D}$ -entrada  $z$  de  $w$  que ocorra em  $au$  já que teríamos que  $x, z \in \text{Pref}(au)$  implicaria que  $x \in \text{Pref}(z)$  ou  $z \in \text{Pref}(x)$  e portanto  $x = z$  por definição. Da mesma forma, existe uma  $\mathcal{D}$ -entrada  $y$  de  $w$  que ocorre em  $ub$  mas não ocorre em  $u$ . Donde  $y \in \text{Suf}(ub) \subseteq \text{Suf}(s)$ , a ocorrência de  $\mathcal{D}$ -entrada de  $w$  em questão é  $(rsy^{-1}, y, t)$  e não há outra  $\mathcal{D}$ -entrada de  $w$  que ocorra em  $ub$ . Como  $(r, x, x^{-1}st)$  é a única ocorrência de  $\mathcal{D}$ -entrada de  $w$  tal que  $(r, x, x^{-1}st) \leq (r, au, bt)$  e  $(rsy^{-1}, y, t)$  é a única tal que  $(rsy^{-1}, y, t) \leq (ra, ub, t)$ , não existe nenhuma outra ocorrência de  $\mathcal{D}$ -entrada de  $w$  entre estas duas ocorrências.

Suponha  $x, y \in \text{Fat}(s)$  tais que  $(r, x, x^{-1}st)$  e  $(rsy^{-1}, y, t)$  sejam duas ocorrências de  $\mathcal{D}$ -entradas consecutivas de  $w$ . Vamos provar que  $x = \epsilon_R(s)$  e  $y = \epsilon_L(s)$  e  $(r, s, t)$  é uma ocorrência de transição de  $w$ . Como  $(r, x, x^{-1}st)$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w = rst$ ,  $(1, x, x^{-1}s)$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $s$ , e é a primeira. Usando o corolário 5.8 segue que  $(1, x, x^{-1}s) = (\epsilon_R(s)\epsilon_L(\epsilon_R(s)))^{-1}, \epsilon_L(\epsilon_R(s)), \epsilon_R(s)^{-1}s)$ . Desta forma temos  $\epsilon_R(s)\epsilon_L(\epsilon_R(s))^{-1} = 1$  e  $\epsilon_R(s) = \epsilon_L(\epsilon_R(s)) = x$ . De forma dual,  $y = \epsilon_L(s)$ . Vamos agora provar que  $(r, s, t)$  é uma ocorrência de transição de  $w$ . Como  $(r, x, x^{-1}st)$  e  $(rsy^{-1}, y, t)$  são incomparáveis por  $\leq$ , segue que  $x^{-1}s \neq 1$  pois caso contrário teríamos que  $(rsy^{-1}, y, t) \leq (r, s, t) = (r, x, x^{-1}st)$ . Seja  $b$  a última letra de  $x^{-1}s$ , e portanto de  $s$ . Como  $s \neq 1$  e portanto  $x \neq 1$  pois  $x \mathcal{D}' s$ , seja  $a$  a primeira letra de  $x$  e portanto de  $s$ . Seja  $u \in A^*$  tal que  $s = aub$ . Como  $\epsilon_R(s) = x \neq s$ , temos que  $|\epsilon_R(s)| < |s| = |aub|$ . Assim  $|\epsilon_R(s)| \leq |aub| - 1 = |au|$  implica que  $au \mathcal{R}' s$  e portanto que  $au \mathcal{D}' s$ . De forma dual provamos que  $ub \mathcal{D}' s$ . Suponha por absurdo que  $u \mathcal{D}' s$ . Neste caso  $(ra, u, bt)$  é uma fatoração de  $w$  em que  $u \mathcal{D}' s \mathcal{D}' w$  e existe  $(x, y, z) \leq (ra, u, bt)$  uma ocorrência de  $\mathcal{D}$ -entrada de  $w$ . Assim  $|x| \geq |ra| > |r|$  e  $(r, x, x^{-1}st) \prec (x, y, z)$ . Por outro lado,  $|z| \geq |bt| > |t|$  e  $(x, y, z) \prec (rsy^{-1}, y, t)$ , contradizendo a consecutividade das ocorrências de  $\mathcal{D}$ -entradas  $(r, x, x^{-1}st)$  e  $(rsy^{-1}, y, t)$ . Assim  $u \not\mathcal{D}' s$  e  $s$  é uma transição e, portanto,

uma transição de  $w$ .

O resto segue do fato que  $w$  é uma transição se e só se  $(1, w, 1)$  for uma ocorrência de transição de  $w$ . ■

**Corolário 5.10** *Uma fatoração  $(r, s, t)$  é uma ocorrência de transição de uma palavra  $w \in A^+$  se e só se existirem  $x, y \in A^+$  tais que  $(r, x, x^{-1}st)$  e  $(rsy^{-1}, y, t)$  sejam duas ocorrências de  $\mathcal{D}$ -entradas consecutivas de  $w$ . Ademais, neste caso,  $x = \epsilon_R(s)$  e  $y = \epsilon_L(s)$ .*

Considere o exemplo 5.1. Dada a palavra  $w = aabcccabcb$ , já calculamos anteriormente a seqüência de transições de  $w$  e a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$ . Nomeando estes diversos fatores de  $w$  conforme o enunciado do lema 5.11, este exemplo pode ser ilustrado como na figura 5.1. De fato, o lema 5.11 fornece uma transformação que aplicada à seqüência de

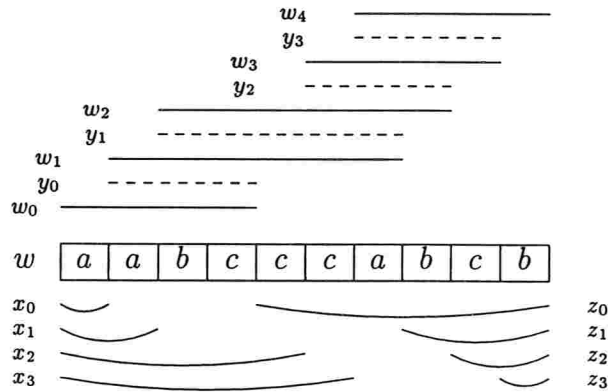


Figura 5.1: Lema 5.11 aplicado à palavra  $w = aabcccabcb$

ocorrências de  $\mathcal{D}$ -entradas de uma palavra  $w$  nos fornece sua seqüência de transições, sua  $\mathcal{R}$ -entrada e sua  $\mathcal{L}$ -entrada. Por outro lado, uma vez conhecidas a seqüência de transições de  $w$ , sua  $\mathcal{R}$ -entrada e sua  $\mathcal{L}$ -entrada, temos uma transformação inversa de modo a obter a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$ .

**Lema 5.11** *Sejam uma palavra  $w \in A^+$  e um inteiro  $k \geq 0$ . Se for conhecida  $(x_0, y_0, z_0), \dots, (x_k, y_k, z_k)$  a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$  então  $\epsilon_R(w) = x_0 y_0$ , a seqüência de transições de  $w$  é  $x_0^{-1} w z_0^{-1}, \dots, x_{k-1}^{-1} w z_{k-1}^{-1}$*



e  $\epsilon_L(w) = y_k z_k$ . Se por outro lado forem conhecidas  $w_0 = \epsilon_R(w)$  a  $\mathcal{R}$ -entrada de  $w$ , sua seqüência de transições  $w_1, \dots, w_k$  e sua  $\mathcal{L}$ -entrada  $w_{k+1} = \epsilon_L(w)$  então

$$\epsilon_L(w_i) = \epsilon_R(w_{i+1}) \text{ para } i \in \{0, \dots, k\}.$$

Ademais, para  $i \in \{0, \dots, k\}$ , definidas as palavras  $y_i = \epsilon_L(w_i) = \epsilon_R(w_{i+1})$  e  $x_i = (w_0 y_0^{-1})(w_1 y_1^{-1}) \cdots (w_i y_i^{-1})$  e  $z_i = (y_i^{-1} w_{i+1}) \cdots (y_{k-1}^{-1} w_k)(y_k^{-1} w_{k+1})$ , então  $(x_0, w_1, z_1), \dots, (x_{k-1}, w_k, z_k)$  é a seqüência de ocorrências de transições de  $w$  e  $(x_0, y_0, z_0), \dots, (x_k, y_k, z_k)$  é a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$ .

*Prova.* A ordem implícita entre as ocorrências de  $\mathcal{D}$ -entradas de  $w$  e entre as ocorrências de transições de  $w$  é a ordem  $\preceq$ .

Afirmamos que se a  $i$ -ésima ocorrência de transição de  $w$  for  $(r, s, t)$  então a  $i$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  é  $(r, \epsilon_R(s), \epsilon_R(s)^{-1} s t)$  e a  $i + 1$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  é  $(r s \epsilon_L(s)^{-1}, \epsilon_L(s), t)$ . De fato isto segue de uma aplicação imediata do corolário 5.10.

Suponha conhecida a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$ :  $(x_0, y_0, z_0), \dots, (x_k, y_k, z_k)$ . Usando o corolário 5.8 temos que  $(x_0, y_0, z_0) = (\epsilon_R(w) \epsilon_L(\epsilon_R(w))^{-1}, \epsilon_L(\epsilon_R(w)), \epsilon_R(w)^{-1} w)$  o que implica que  $\epsilon_R(w) = x_0 y_0$ . De forma dual provamos que  $\epsilon_L(w) = y_k z_k$ . Como a  $i$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  é  $(x_{i-1}, y_{i-1}, z_{i-1})$  e a  $i + 1$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  é  $(x_i, y_i, z_i)$ , para  $i \in \{0, \dots, k\}$ , usando a afirmativa anterior temos que a  $i$ -ésima ocorrência de transição de  $w$  é  $(x_{i-1}, x_{i-1}^{-1} w z_{i-1}^{-1}, z_{i-1})$ . Assim a seqüência de transições de  $w$  é  $x_0^{-1} w z_0^{-1}, \dots, x_{k-1}^{-1} w z_{k-1}^{-1}$ .

A partir de agora, suporemos conhecidas  $w_0 = \epsilon_R(w)$  a  $\mathcal{R}$ -entrada de  $w$ , sua seqüência de transições  $w_1, \dots, w_k$  e sua  $\mathcal{L}$ -entrada  $w_{k+1} = \epsilon_L(w)$ . Sejam definidas as palavras  $y_i = \epsilon_L(w_i)$  e  $x_i = (w_0 y_0^{-1})(w_1 y_1^{-1}) \cdots (w_i y_i^{-1})$  para  $i \in \{0, \dots, k\}$ .

Vamos provar que a  $i + 1$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  é  $(x_i, y_i, t_i)$  onde  $t_i = (x_i y_i)^{-1} w$  para  $i \in \{0, \dots, k\}$ . Faremos uma indução em  $i$ . Dado que  $\epsilon_L(w_0) = y_0$ , que  $w_0 \epsilon_L(w_0)^{-1} = w_0 y_0^{-1} = x_0$  e que  $w_0^{-1} w = (x_0 y_0)^{-1} w = t_0$ , a primeira ocorrência de  $\mathcal{D}$ -entrada de  $w$  é  $(w_0 \epsilon_L(w_0)^{-1}, \epsilon_L(w_0), w_0^{-1} w) = (x_0, y_0, t_0)$  devido ao corolário 5.8, e segue a base da indução. Suponha agora que  $1 \leq i \leq k$  e que a  $i$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  seja  $(x_{i-1}, y_{i-1}, t_{i-1})$ . Como  $i \leq k$ , existe a  $i$ -ésima ocorrência de transição  $(r, w_i, t)$  de  $w$ . Usando a afirmativa, a  $i$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  é  $(r, \epsilon_R(w_i), \epsilon_R(w_i)^{-1} w_i t)$  e a  $i + 1$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  é  $(r w_i \epsilon_L(w_i)^{-1}, \epsilon_L(w_i), t)$ . Assim  $(r, \epsilon_R(w_i), \epsilon_R(w_i)^{-1} w_i t) =$

$(x_{i-1}, y_{i-1}, t_{i-1})$  e temos que  $r = x_{i-1}$  e  $\epsilon_R(w_i) = y_{i-1}$  e  $t_{i-1} = (\epsilon_R(w_i)^{-1}w_i)t$ . Assim  $rw_i\epsilon_L(w_i)^{-1} = x_{i-1}(w_iy_i^{-1}) = x_i$  e  $\epsilon_L(w_i) = y_i$  implicam que a  $i + 1$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  é  $(rw_i\epsilon_L(w_i)^{-1}, \epsilon_L(w_i), t) = (x_i, y_i, t)$ . Desta forma  $t = (x_iy_i)^{-1}w = t_i$  e  $t_{i-1} = (\epsilon_R(w_i)^{-1}w_i)t = (y_{i-1}^{-1}w_i)t_i$ .

Na demonstração do parágrafo anterior, também provamos que a  $i$ -ésima ocorrência de transição de  $w$  é  $(x_{i-1}, w_i, t_i)$ , para  $i \in \{1, \dots, k\}$ . Também provamos que  $\epsilon_R(w_i) = y_{i-1} = \epsilon_L(w_{i-1})$  e que  $t_{i-1} = (y_{i-1}^{-1}w_i)t_i$ , para  $i \in \{1, \dots, k\}$ .

Vamos provar que  $y_i = \epsilon_L(w_i) = \epsilon_R(w_{i+1})$ , para  $i \in \{0, \dots, k\}$ . Também provaremos que  $t_k = y_k^{-1}w_{k+1}$ . Falta-nos apenas provar que  $y_k = \epsilon_L(w_k) = \epsilon_R(w_{k+1})$ . Como a última ocorrência de  $\mathcal{D}$ -entrada de  $w$  é a  $k + 1$ -ésima ocorrência  $(x_k, y_k, t_k)$ , usando o dual do corolário 5.8 temos que  $(x_k, y_k, t_k) = (ww_{k+1}^{-1}, \epsilon_R(w_{k+1}), \epsilon_R(w_{k+1})^{-1}w_{k+1})$ . Portanto temos que  $\epsilon_R(w_{k+1}) = y_k = \epsilon_L(w_k)$ . Ademais,  $t_k = \epsilon_R(w_{k+1})^{-1}w_{k+1} = y_k^{-1}w_{k+1}$ .

Concluiremos a demonstração. Como  $y_i = \epsilon_R(w_{i+1})$ , seja pois  $z_i = (y_i^{-1}w_{i+1}) \cdots (y_{k-1}^{-1}w_k)(y_k^{-1}w_{k+1})$ , para  $i \in \{0, \dots, k\}$ . Temos então que  $z_i = t_i$  para  $i \in \{0, \dots, k\}$ . De fato, isto segue por uma simples indução em  $k - i$  pois  $z_k = (y_k^{-1}w_{k+1}) = t_k$  e  $z_i = (y_i^{-1}w_{i+1})z_{i+1}$  para  $i \in \{0, \dots, k\}$  e  $t_{i-1} = (y_{i-1}^{-1}w_i)t_i$ , para  $i \in \{1, \dots, k\}$ . Como a  $i + 1$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  é  $(x_i, y_i, t_i)$  e  $z_i = t_i$  para  $i \in \{0, \dots, k\}$ , temos então que  $(x_0, y_0, z_0), \dots, (x_k, y_k, z_k)$  é a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$ . Como a  $i$ -ésima ocorrência de transição de  $w$  é  $(x_{i-1}, w_i, t_i)$ , para  $i \in \{1, \dots, k\}$ , temos que  $(x_0, w_1, z_1), \dots, (x_{k-1}, w_k, z_k)$  é a seqüência de ocorrências de transições de  $w$ . ■

Dada uma seqüência aleatória de transições  $w_1, w_2, \dots, w_k$  acabamos de ver no lema 5.11 que uma condição necessária para que exista uma palavra  $w$  tal que esta seqüência seja exatamente a seqüência de transições de  $w$  é que  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{1, \dots, k - 1\}$ . Na proposição 5.12 veremos que esta condição é também suficiente. Também é exibida uma particular palavra  $w$  com esta característica e são obtidas algumas propriedades suas.

**Proposição 5.12** *Seja  $k \geq 1$  um inteiro e seja  $w_1, w_2, \dots, w_k$  uma seqüência de transições tal que  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{1, \dots, k - 1\}$ . Seja a palavra  $w = w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_k)^{-1}w_k)$ . Então:*

1.  $w \mathcal{D}' w_i$ , para  $i \in \{1, \dots, k\}$ ;

2.  $w_1, w_2, \dots, w_k$  é a seqüência de transições de  $w$ ;
3.  $\epsilon_R(w) = \epsilon_R(w_1)$ ;
4.  $\epsilon_L(w) = \epsilon_L(w_k)$ .

*Prova.* Seja  $D$  a  $\mathcal{D}'$ -classe de  $w_1$ . Dado que  $\epsilon_R(w_i) \mathcal{R}' w_i \mathcal{L}' \epsilon_L(w_i)$  para  $i \in \{1, \dots, k\}$  e que  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{1, \dots, k-1\}$ , temos pois que  $\epsilon_R(w_i), w_i, \epsilon_L(w_i) \in D$  para  $i \in \{1, \dots, k\}$ . Devido à proposição 5.9, temos que  $\epsilon_R(w_i)$  e  $\epsilon_L(w_i)$  são  $\mathcal{D}$ -entradas, para  $i \in \{1, \dots, k\}$ .

Provaremos por indução em  $k$ . Suponha primeiro que  $k = 1$ . Neste caso temos que  $w = w_1 = w_k$  é uma transição. Os itens 1, 3 e 4 seguem então de forma imediata. Da proposição 5.9, temos que a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$  é  $(1, \epsilon_R(w_1), \epsilon_R(w_1)^{-1}w_1), (w_1\epsilon_L(w_1)^{-1}, \epsilon_L(w_1), 1)$  implicando pois o item 2 devido ao corolário 5.10.

Suponha  $k \geq 2$ . Seja  $u = w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_{k-1})^{-1}w_{k-1})$  e suponha que a tese valha para  $u$ . Assim, seja  $s = \epsilon_L(u) = \epsilon_L(w_{k-1}) = \epsilon_R(w_k) \in D$  uma  $\mathcal{D}$ -entrada. Sejam ainda  $r = u\epsilon_L(u)^{-1} = us^{-1}$  e  $t = (\epsilon_R(w_k)^{-1}w_k) = s^{-1}w_k$ . Temos que  $(r, s, t)$  é uma fatoração de  $w$  pois  $w = w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_{k-1})^{-1}w_{k-1})(\epsilon_R(w_k)^{-1}w_k) = u(\epsilon_R(w_k)^{-1}w_k) = rst$ . Como  $rs = u \mathcal{L}' \epsilon_L(u) = s$  implica que  $w = rst \mathcal{L}' st = w_k \in D$ , temos que  $w \in D$ . Isto prova o item 1. Como  $w \mathcal{D}' w_1 \in \text{Pref}(w)$ , pelo item 2 do corolário 5.3 temos que  $w \mathcal{R}' w_1$  e portanto que  $\epsilon_R(w) = \epsilon_R(w_1)$ , provando o item 3. Como  $rst = w \mathcal{D}' w_k = st$ ,  $w \mathcal{L}' w_k$  pelo item 3 do corolário 5.3 e portanto  $\epsilon_L(w) = \epsilon_L(w_k)$ , provando o item 4. Falta-nos apenas o item 2.

Observe que  $(r, s, t)$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w = rst$  já que  $w, s \in D$  e  $s$  é uma  $\mathcal{D}$ -entrada. Como  $u \mathcal{D}' ut = w = rw_k \mathcal{D}' w_k$ , temos que as  $\mathcal{D}$ -entradas de  $w$  que ocorrem em  $u$  são  $\mathcal{D}$ -entradas de  $u$  e as que ocorrem em  $w_k$  são  $\mathcal{D}$ -entradas de  $u$ . Por outro lado, as  $\mathcal{D}$ -entradas de  $u$  e as de  $w_k$  são  $\mathcal{D}$ -entradas de  $w$ . Em particular, a ocorrência de  $\mathcal{D}$ -entrada  $(r, s, t)$  de  $w$  induz a ocorrência de  $\mathcal{D}$ -entrada  $(r, s, 1)$  de  $u$ , que é a última ocorrência de  $\mathcal{D}$ -entrada de  $u$ , e induz a ocorrência de  $\mathcal{D}$ -entrada  $(1, s, t)$  de  $w_k$ , que é a primeira ocorrência de  $\mathcal{D}$ -entrada de  $w_k$ . Usando o lema 5.11, seja  $(x_0, y_0, z_0), \dots, (x_{k-2}, y_{k-2}, z_{k-2}), (x_{k-1}, y_{k-1}, z_{k-1}) = (r, s, 1)$  a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $rs = u$ . Usando a proposição 5.9,  $(1, s, t) = (1, \epsilon_R(w_k), \epsilon_R(w_k)^{-1}w_k), (w_k\epsilon_L(w_k)^{-1}, \epsilon_L(w_k), 1)$  é a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $st = w_k$ . Desta forma, deduzimos que  $(x_0, y_0, z_0t), \dots, (x_{k-2}, y_{k-2}, z_{k-2}t), (r, s, t), (rw_k\epsilon_L(w_k)^{-1}, \epsilon_L(w_k), 1)$  é a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $rst = w$ . Note também

que  $(r, s, t) = (x_{k-1}, y_{k-1}, z_{k-1}t) = (r, \epsilon_R(w_k), \epsilon_R(w_k)^{-1}w_k)$ . Para todo  $i \in \{1, \dots, k-1\}$ , temos  $x_{i-1}^{-1}w(z_it)^{-1} = x_{i-1}^{-1}(rst)(z_it)^{-1} = x_{i-1}^{-1}(rs)z_i^{-1} = w_i$  devido ao lema 5.11 aplicado em  $u = rs$  e à hipótese de indução sobre  $u$ . Por outro lado,  $r^{-1}w1^{-1} = st = w_k$ . Devido ao mesmo lema, temos então que a seqüência de transições de  $w$  é  $w_1, \dots, w_{k-1}, w_k$ , o que prova o item 2. ■

## 5.4 Sistemas de adequações

Seja  $e \in A^+$  uma palavra  $\sim$ -idempotente. Seja  $D$  o conjunto das  $\mathcal{D}$ -entradas da  $\mathcal{D}'$ -classe de  $e$ . Dizemos que um *sistema de adequações básico associado a  $e$*  é o par de funções  $(\mu, \eta)$  onde  $\mu : D \rightarrow A^*$ , chamada *adequação esquerda*, e  $\eta : D \rightarrow A^*$ , chamada *adequação direita*, são funções tais que

$$e \sim \mu_d d \eta_d,$$

para todo  $d \in D$ , onde  $\mu_d$  e  $\eta_d$  denotam as aplicações de  $d$  por  $\mu$  e  $\eta$  respectivamente. Existe ao menos um sistema de adequações básico associado a  $e$ . De fato, para todo  $d \in D$  temos que  $d \mathcal{D}' e$ . Portanto existem  $x_d, y_d \in A^*$  tais que  $e \sim x_d d y_d$  e podemos definir  $\eta_d = y_d$  e  $\mu_d = x_d$ . Ademais, existe ao menos um sistema de adequações básico associado a  $e$  tal que

$$d \sim d' \implies \mu_d \sim \mu_{d'} \text{ e } \eta_d \sim \eta_{d'}.$$

Um tal sistema de adequações básico é chamado *coerente*. De fato, dado um sistema de adequações básico  $(\mu, \eta)$  não coerente, pode-se obter um sistema de adequações básico coerente  $(\mu', \eta')$ , por exemplo, definindo  $\mu'_d = \mu_{d'}$  e  $\eta'_d = \eta_{d'}$  onde  $d'$  é a menor palavra (segundo a ordem militar) na classe de congruência de  $d$ .

Dado  $(\mu, \eta)$  um sistema de adequações básico associado a  $e$ , definiremos três novas funções que acrescentadas às funções já existentes formam  $(\mu, \eta, \psi, \psi^R, \psi^L)$ , um *sistema de adequações completo associado a  $e$* , ou simplesmente um *sistema de adequações associado a  $e$* . Seja  $T$  o conjunto das transições da  $\mathcal{D}'$ -classe de  $e$ . Definimos  $\psi : T \rightarrow A^*$  como segue. Para toda transição  $t \in T$ , usando a proposição 5.9, temos que  $(1, \epsilon_R(t), \epsilon_R(t)^{-1}t)$  e  $(t\epsilon_L(t)^{-1}, \epsilon_L(t), 1)$  são as duas únicas ocorrências de  $\mathcal{D}$ -entradas de  $t$ . Assim  $\epsilon_R(t), \epsilon_L(t) \in D$  e podemos definir a *adequação da transição  $t$*  por

$$\psi(t) = \mu_{\epsilon_R(t)} t \eta_{\epsilon_L(t)}.$$

Seja  $R$  o conjunto das  $\mathcal{R}$ -entradas da  $\mathcal{D}'$ -classe de  $e$ . Definimos  $\psi^R : R \rightarrow A^*$  como segue. Para toda  $\mathcal{R}$ -entrada  $r \in R$ , temos que  $(r\epsilon_L(r)^{-1}, \epsilon_L(r), 1)$  é a única ocorrência de  $\mathcal{D}$ -entrada de  $r$  devido à proposição 5.7. Assim  $\epsilon_L(r) \in D$  e podemos definir a *adequação da  $\mathcal{R}$ -entrada  $r$*  por

$$\psi^R(r) = r \eta_{\epsilon_L(r)}.$$

De forma dual, seja  $L$  o conjunto das  $\mathcal{L}$ -entradas da  $\mathcal{D}'$ -classe de  $e$ . Definimos  $\psi^L : L \rightarrow A^*$  como segue. Para toda  $\mathcal{L}$ -entrada  $l \in L$ , definimos a *adequação da  $\mathcal{L}$ -entrada  $l$*  por

$$\psi^L(l) = \mu_{\epsilon_R(l)} l.$$

Um sistema de adequações  $(\mu, \eta, \psi, \psi^R, \psi^L)$  associado a  $e$  é dito *coerente* se o sistema de adequações básico  $(\mu, \eta)$  for coerente.

A proposição seguinte revela algumas propriedades fundamentais das adequações, em relação às relações  $\mathcal{R}'$ ,  $\mathcal{L}'$ ,  $\mathcal{D}'$  e  $\mathcal{H}'$ .

**Proposição 5.13** *Seja  $(\mu, \eta, \psi, \psi^R, \psi^L)$  um sistema de adequações associado a um  $\sim$ -idempotente  $e \in A^+$ . Sejam  $d$  uma  $\mathcal{D}$ -entrada,  $t$  uma transição,  $r$  uma  $\mathcal{R}$ -entrada,  $l$  uma  $\mathcal{L}$ -entrada, todas na  $\mathcal{D}'$ -classe de  $e$ .*

*Então as seguintes afirmações são verdadeiras:*

1.  $\psi(t) \mathcal{H}' e$ ;
2.  $r \mathcal{R}' \psi^R(r) \mathcal{L}' e$ ;
3.  $l \mathcal{L}' \psi^L(l) \mathcal{R}' e$ ;
4.  $d \sim d \eta_d \mu_d d$ ;
5.  $e \mathcal{R}' \mu_d d \mathcal{L}' d \mathcal{R}' d \eta_d \mathcal{L}' e$ .

*Prova.* Vamos primeiro provar o item 5. Temos que  $\mu_d d \eta_d \sim e \mathcal{D}' d$ . Usando o item 4 do corolário 5.3 temos que  $\mu_d d \eta_d \mathcal{R}' \mu_d d \mathcal{L}' d \mathcal{R}' d \eta_d \mathcal{L}' \mu_d d \eta_d$ . O restante segue do fato que  $\mu_d d \eta_d \sim e$ .

Vamos provar o item 4. Usando o item 5, temos que  $\mu_d d \mathcal{L}' d \mathcal{R}' d \eta_d$ . Sejam  $\eta'_d, \mu'_d \in A^*$  tais que  $d \eta_d \eta'_d \sim d$  e  $\mu'_d \mu_d d \sim d$ . Assim temos que  $d \sim d \eta_d \eta'_d \sim \mu'_d \mu_d d \eta_d \eta'_d \sim \mu'_d e \eta'_d \sim \mu'_d e e \eta'_d \sim \mu'_d \mu_d d \eta_d \mu_d d \eta_d \eta'_d \sim \mu'_d \mu_d d \eta_d \mu_d d \sim d \eta_d \mu_d d$ .

Vamos provar o item 3. Por definição, temos que  $\psi^L(l) = \mu_{\epsilon_R(l)} l = \mu_{\epsilon_R(l)} \epsilon_R(l) (\epsilon_R(l)^{-1} l)$ . Usando o item 5, temos que  $\mu_{\epsilon_R(l)} \epsilon_R(l) \mathcal{L}' \epsilon_R(l)$ . Onde

temos que  $\psi^L(l) = \mu_{\epsilon_R(l)}\epsilon_R(l)(\epsilon_R(l)^{-1}l) \mathcal{L}' \epsilon_R(l)(\epsilon_R(l)^{-1}l) = l$  já que  $\mathcal{L}'$  é uma congruência à direita. Acabamos de provar que  $\psi^L(l) \mathcal{L}' l$  e falta-nos agora provar que  $e \mathcal{R}' \psi^L(l)$ . Também do item 5 temos que  $e \mathcal{R}' \mu_{\epsilon_R(l)}\epsilon_R(l)$ . Como  $\epsilon_R(l) \mathcal{R}' l$  devido à definição de  $\mathcal{R}$ -entrada, segue finalmente que  $e \mathcal{R}' \mu_{\epsilon_R(l)}\epsilon_R(l) \mathcal{R}' \mu_{\epsilon_R(l)}l = \psi^L(l)$  pois  $\mathcal{R}'$  é uma congruência à esquerda.

Provamos o item 2 de forma dual ao item 3.

Vamos provar o item 1. Por definição,  $\psi(t) = \mu_{\epsilon_R(t)}t\eta_{\epsilon_L(t)}$ . Primeiro provaremos que  $\psi(t) \mathcal{D}' e$ . Usando o item 5, temos que  $\epsilon_L(t)\eta_{\epsilon_L(t)} \mathcal{R}' \epsilon_L(t)$ . Onde temos que  $t\eta_{\epsilon_L(t)} \mathcal{R}' t$  pois  $\mathcal{R}'$  é uma congruência à esquerda implica que  $t\eta_{\epsilon_L(t)} = (t\epsilon_L(t)^{-1})\epsilon_L(t)\eta_{\epsilon_L(t)} \mathcal{R}' (t\epsilon_L(t)^{-1})\epsilon_L(t) = t$ . De maneira dual, segue imediatamente que  $\mu_{\epsilon_R(t)}t \mathcal{L}' t$  e, como  $\mathcal{L}'$  é uma congruência à direita,  $\mu_{\epsilon_R(t)}t\eta_{\epsilon_L(t)} \mathcal{L}' t\eta_{\epsilon_L(t)} \mathcal{R}' t$ . Logo,  $e \mathcal{D}' t \mathcal{D}' \mu_{\epsilon_R(t)}t\eta_{\epsilon_L(t)} = \psi(t)$ , conforme queríamos provar. Como definimos  $\psi(t)$  por  $\mu_{\epsilon_R(t)}t\eta_{\epsilon_L(t)}$ , temos que  $\epsilon_R(t)$  e  $\epsilon_L(t)$  são duas  $\mathcal{D}$ -entradas e estão na mesma  $\mathcal{D}'$ -classe de  $e$ . Usando o item 5 sobre  $\epsilon_R(t)$ , temos que  $\mu_{\epsilon_R(t)}\epsilon_R(t) \mathcal{R}' e$ . Como  $\mu_{\epsilon_R(t)}\epsilon_R(t)$  é prefixo de  $\psi(t) \mathcal{D}' e$ , temos que  $\psi(t) \mathcal{R}' e$  e devido ao item 2 do corolário 5.3. Usando o item 5 sobre  $\epsilon_L(t)$ , temos que  $\epsilon_L(t)\eta_{\epsilon_L(t)} \mathcal{L}' e$ . Como  $\epsilon_L(t)\eta_{\epsilon_L(t)}$  é sufixo de  $\psi(t) \mathcal{D}' e$ , temos que  $\psi(t) \mathcal{L}' e$  e devido ao item 3 do corolário 5.3. Isto prova que  $\psi(t) \mathcal{H}' e$ . ■

Considere o exemplo 5.1. Seja a palavra  $w = abcccabcb$  e seja  $e = abbcc$  uma palavra  $\sim$ -idempotente na mesma  $\mathcal{D}'$ -classe de  $w$ . Seja  $D$  o conjunto das  $\mathcal{D}$ -entradas na mesma  $\mathcal{D}'$ -classe de  $e$ . Uma vez caracterizadas as  $\mathcal{D}$ -entradas e a relação  $\mathcal{D}'$ , é imediato verificar que  $D = \{a_1a_2^k a_3 \mid k \in \mathbb{N} \setminus \{0\}\}$  e  $(a_1, a_2, a_3)$  é uma permutação qualquer de  $(a, b, c)$ . Também podemos definir o sistema de adequações básico  $(\mu, \eta)$  coerente associado a  $e$  onde  $\mu : D \rightarrow A^*$  e  $\eta : D \rightarrow A^*$  são definidas por  $\mu_d = 1$  e  $\eta_d = a^{\#_a(d)}b^{\#_b(d)}c^{\#_c(d)}$ . Em particular, para as  $\mathcal{D}$ -entradas que ocorrem em  $w$ , temos que  $\eta_{abc} = \eta_{bccca} = \eta_{cab} = abc$  e  $\mu_{abc} = \mu_{bccca} = \mu_{cab} = 1$ . Assim, temos que  $\psi^R(\epsilon_R(w)) = \psi^R(abc) = abcabc$  e que  $\psi^L(\epsilon_L(w)) = \psi^L(abcb) = abcb$ . Ademais, visto que a seqüência de transições de  $w$  é  $abcccab, bcccab, cabcb$ , temos que  $\psi(abcccab) = abcccababc$ , que  $\psi(bcccab) = bcccababc$  e que  $\psi(cabcb) = cabcbabc$ . Por fim, seja definida a palavra  $w' = \psi^R(\epsilon_R(w))\psi(abcccab)\psi(bcccab)\psi(cabcb)\psi^L(\epsilon_L(w)) = abcabc abcccab bcccab abc cabcb abcb$ . Note que  $c(w) = \{a, b, c\} = c(w')$ , que  $\#_a(w) = 3 \bmod 2 = 11 \bmod 2 = \#_a(w')$ , que  $\#_b(w) = 3 \bmod 2 = 11 \bmod 2 = \#_b(w')$  e que  $\#_c(w) = 4 \bmod 2 = 14 \bmod 2 = \#_c(w')$ . Por definição portanto, temos que  $w \sim w'$ . O lema 5.14 afirma esta propriedade para o caso geral e revela uma interessante aplicação dos sistemas de ade-

quações à seqüência de transições de uma palavra. O dito lema será usado na demonstração do teorema 7.5.

**Lema 5.14** *Seja  $(\mu, \eta, \psi, \psi^R, \psi^L)$  um sistema de adequações associado a um  $\sim$ -idempotente e  $\in A^+$ . Seja  $w \in \mathcal{D}'$  e seja  $w_1, w_2, \dots, w_k$  sua seqüência de transições. Então*

$$w \sim \psi^R(\epsilon_R(w))\psi(w_1)\psi(w_2)\cdots\psi(w_k)\psi^L(\epsilon_L(w)).$$

*Prova.* Sejam  $w_0 = \epsilon_R(w)$  e  $w_{k+1} = \epsilon_L(w)$ . A partir do lema 5.11 temos então que  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{0, \dots, k\}$ . Para  $i \in \{0, \dots, k\}$ , sejam as palavras  $y_i = \epsilon_L(w_i) = \epsilon_R(w_{i+1})$  e  $x_i = (w_0 y_0^{-1})(w_1 y_1^{-1}) \cdots (w_i y_i^{-1})$  e  $z_i = (y_i^{-1} w_{i+1}) \cdots (y_{k-1}^{-1} w_k)(y_k^{-1} w_{k+1})$ . A partir do mesmo lema, a seqüência de ocorrências de transições de  $w$  é  $(x_0, w_1, z_1), \dots, (x_{k-1}, w_k, z_k)$  e a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$  é  $(x_0, y_0, z_0), \dots, (x_k, y_k, z_k)$ .

Seja  $z_{k+1} = 1$ . Assim  $x_k w_{k+1} z_{k+1} = x_k y_k z_k = w$ . Vamos provar que  $y_i z_i = w_{i+1} z_{i+1}$  para  $i = 0, \dots, k$ . De fato, como  $x_i y_i z_i = w = x_i w_{i+1} z_{i+1}$ , temos então que  $w_{i+1} z_{i+1} = x_i^{-1} w = y_i z_i$ .

Vamos provar que  $y_i \sim y_i \eta_{y_i} \mu_{y_i} y_i$ , para  $i = 0, \dots, k$ . De fato, como  $(x_i, y_i, z_i)$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$ , temos que  $y_i$  é uma  $\mathcal{D}$ -entrada na mesma  $\mathcal{D}'$ -classe de  $w$ . Como  $y_i \in \mathcal{D}'$  e  $w \in \mathcal{D}'$ , temos que  $y_i \sim y_i \eta_{y_i} \mu_{y_i} y_i$  devido ao item 4 da proposição 5.13.

Vamos provar que  $w \sim \psi^R(\epsilon_R(w))\psi(w_1)\cdots\psi(w_j)\mu_{\epsilon_R(w_{j+1})}w_{j+1}z_{j+1}$ , para  $j \in \{0, 1, 2, \dots, k\}$ . Para tanto faremos uma indução finita em  $j$ . Vamos primeiro provar a base da indução. Suponha que  $j = 0$ . Já vimos anteriormente que  $y_0 z_0 = w_1 z_1$  e que  $y_0 \sim y_0 \eta_{y_0} \mu_{y_0} y_0$ . Desta forma temos que  $w = x_0 y_0 z_0 \sim x_0 y_0 \eta_{y_0} \mu_{y_0} y_0 z_0 = x_0 y_0 \eta_{y_0} \mu_{y_0} w_1 z_1 = w_0 \eta_{\epsilon_L(w_0)} \mu_{\epsilon_R(w_1)} w_1 z_1 = \psi^R(w_0) \mu_{\epsilon_R(w_1)} w_1 z_1 = \psi^R(\epsilon_R(w))\psi(w_1)\cdots\psi(w_j)\mu_{\epsilon_R(w_{j+1})}w_{j+1}z_{j+1}$ . Suponha que  $1 \leq j \leq k$ . Já vimos que  $y_j \sim y_j \eta_{y_j} \mu_{y_j} y_j$ . Considerando que  $y_j = \epsilon_L(w_j)$  é sufixo de  $w_j$ , segue então que  $w_j \sim w_j \eta_{y_j} \mu_{y_j} y_j$ . Também já vimos que  $y_j z_j = w_{j+1} z_{j+1}$ . Assim, temos que  $\mu_{\epsilon_R(w_j)} w_j z_j \sim \mu_{\epsilon_R(w_j)} w_j \eta_{y_j} \mu_{y_j} y_j z_j = \mu_{\epsilon_R(w_j)} w_j \eta_{\epsilon_L(w_j)} \mu_{y_j} y_j z_j = \psi(w_j) \mu_{\epsilon_R(w_{j+1})} w_{j+1} z_{j+1}$ . A partir da hipótese de indução para  $j - 1$  temos que  $w \sim \psi^R(\epsilon_R(w))\psi(w_1)\cdots\psi(w_{j-1})\mu_{\epsilon_R(w_j)} w_j z_j \sim \psi^R(\epsilon_R(w))\psi(w_1)\cdots\psi(w_{j-1})\psi(w_j)\mu_{\epsilon_R(w_{j+1})} w_{j+1} z_{j+1}$ .

Por fim temos que  $\mu_{\epsilon_R(w_{k+1})} w_{k+1} z_{k+1} = \mu_{\epsilon_R(w_{k+1})} w_{k+1} = \psi^L(w_{k+1}) = \psi^L(\epsilon_L(w))$  e portanto que  $w \sim \psi^R(\epsilon_R(w))\psi(w_1)\cdots\psi(w_k)\mu_{\epsilon_R(w_{k+1})} w_{k+1} z_{k+1} = \psi^R(\epsilon_R(w))\psi(w_1)\cdots\psi(w_k)\psi^L(\epsilon_L(w))$ . ■

Considerando as definições vistas no lema 5.14, temos pois que  $w \sim \psi^R(\epsilon_R(w))\psi(w_1)\psi(w_2)\cdots\psi(w_k)\psi^L(\epsilon_L(w))$ . Naturalmente podemos nos

perguntar se há alguma relação entre a seqüência de transições de  $w$  e a seqüência de transições de  $\psi^R(\epsilon_R(w))\psi(w_1)\psi(w_2)\cdots\psi(w_k)\psi^L(\epsilon_L(w))$ . Considerando nosso exemplo, a seqüência de transições de  $w = aabcccabcb$  é  $(abccca, bcccab, cabc)$  e com um pouco de cálculo pode-se verificar que a seqüência de transições de  $w' = aabcabc abcccaabc bcccababc cabcabc abcb$  é  $(abca, bcab, cabc, abca, bcab, cabc) abccca (bcccaab, caabc, abcbccca) bcccab (cababc, abcca, bccab) cabc (abca, bcab, cabc, abca, bcab, cabc)$ . De forma geral, pode-se provar que se  $w_1, w_2, \dots, w_k$  é a seqüência de transições de  $w$ , então a seqüência de transições de  $\psi^R(\epsilon_R(w))\psi(w_1)\psi(w_2)\cdots\psi(w_k)\psi^L(\epsilon_L(w)) \sim w$  é  $s_0, w_1, s_1, w_2, s_2, \dots, w_k, s_k$  onde  $s_i$  é a seqüência de transições de  $y_i\eta_{y_i}\mu_{y_i}y_i$  para  $i \in \{0, 1, \dots, k\}$  e  $y_i = \epsilon_L(w_i)$  para  $i \in \{1, 2, \dots, k\}$  e  $y_0 = \epsilon_R(w_1)$ . Note-se ainda que  $\epsilon_R(y_i\eta_{y_i}\mu_{y_i}y_i) = \epsilon_L(y_i\eta_{y_i}\mu_{y_i}y_i) = y_i$ , para  $i \in \{1, 2, \dots, k\}$ .

De forma parecida com o que será feito na definição do grafo fundamental de uma  $\mathcal{D}$ -classe de um monóide de Burnside livre na seção 6.3 do capítulo 6, pode-se definir um grafo com conjunto de vértices formado pelas  $\mathcal{D}$ -entradas de uma certa  $\mathcal{D}'$ -classe, com conjunto de arestas formado pelas transições desta mesma  $\mathcal{D}'$ -classe e com funções de incidência definidas por  $\alpha(t) = \epsilon_R(t)$  e  $\omega(t) = \epsilon_L(t)$ . Assim sendo, à seqüência de transições de uma palavra nesta  $\mathcal{D}$ -classe corresponde um passeio neste grafo. No passeio  $s_0, w_1, s_1, w_2, s_2, \dots, w_k, s_k$  acima visto, cada segmento  $s_i$  é um passeio fechado sobre o vértice  $y_i$ . De fato, cada sistema de adequações básico associado a um  $\sim$ -idempotente qualquer desta  $\mathcal{D}$ -classe define um conjunto de passeios  $s_d$  onde, para cada vértice  $d$ , o passeio  $s_d$  é um passeio fechado sobre o vértice  $d$ .

Na seção 6.3 do capítulo 6 definiremos o grafo fundamental de um monóide de Burnside livre. Este grafo fundamental é imagem de um morfismo de grafos cujo domínio é o grafo acima descrito, como veremos oportunamente. Este morfismo de grafos identificará vértices congruentes e arestas congruentes.



## Capítulo 6

# Monóides de Burnside Livres

Neste capítulo, apresentaremos o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por um alfabeto  $A$ , para inteiros  $n \geq 1$  e  $m \geq 1$ . Após a definição na seção 6.1, apresentaremos o teorema dos marcadores (teorema 6.3) na seção 6.2, que prova ser que uma propriedade do semigrupo idempotente seja válida também para qualquer monóide de Burnside livre. Logo após veremos uma aplicação imediata do teorema 6.3 aos sistemas de adequações coerentes. Esta aplicação será usada no capítulo 7 durante a demonstração do teorema 7.5, que trata de uma caracterização da congruência de Burnside.

Na seção 6.3 veremos a definição de um conceito central em nosso trabalho: o grafo fundamental de uma  $\mathcal{D}$ -classe de um monóide de Burnside livre. O grafo fundamental se mostrará fortemente conexo como veremos na proposição 6.8 e poderemos futuramente definir o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por este grafo. Veremos também alguns conceitos e propriedades correlatas. Por exemplo, associaremos a uma palavra  $w$  que é projetada na  $\mathcal{D}$ -classe um passeio no grafo fundamental. Esta é a digital de  $w$  e é um conceito fundamental para caracterizar se duas palavras  $\mathcal{D}'$ -equivalentes são congruentes ou não, como veremos no teorema 7.5 a ser visto no capítulo 7. Vemos também como construir a menor palavra que possui uma certa digital e esta construção será essencial à demonstração da existência de uma classe de congruência com duas palavras de menor comprimento, a ser visto no capítulo 8.

Na seção 6.5 veremos algumas propriedades relativas à regularidade de uma  $\mathcal{D}$ -classe de um monóide de Burnside livre. Em particular, na proposição 6.13 veremos que as  $\mathcal{H}$ -classes irregulares são triviais e na

proposição 6.14 provamos que qualquer grafo fundamental de uma  $\mathcal{D}$ -classe irregular não possui nenhuma aresta e possui um único vértice.

## 6.1 O monóide de Burnside livre

Suponha  $A$  um alfabeto qualquer e suponha  $n$  e  $m$  inteiros tais que  $n \geq 1$  e  $m \geq 1$ . Seja  $\pi = \{(x^{n+m}, x^n) \mid x \in A^+\}$  e seja  $\sim$  a menor congruência sobre  $A^*$  que contém  $\pi$ . Definimos o *monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$*  como sendo o monóide quociente  $\mathcal{M} \stackrel{\text{def}}{=} A^*/\sim$ . Definimos  $\tilde{\phantom{x}}$  o morfismo canônico

$$\tilde{\phantom{x}}: A^* \longrightarrow \mathcal{M}$$

que aplica uma palavra  $w \in A^*$  em sua classe de congruência  $\tilde{w} \in \mathcal{M}$ . Observe que  $w \sim w' \iff \tilde{w} = \tilde{w}'$ . Podendo ser implícitos o alfabeto  $A$  e os inteiros  $n$  e  $m$ , muitas vezes referiremo-nos à congruência  $\sim$  simplesmente por *congruência de Burnside*. Definimos o *semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$*  como sendo  $\mathcal{M} \setminus \{\tilde{1}\}$ .

Para todo elemento  $x \in \mathcal{M}$  temos que  $x^n = x^{n+m}$ . De fato, se  $w \in A^*$  é tal que  $\tilde{w} = x$ , como  $\tilde{\phantom{x}}$  é um morfismo, temos então que  $x^n = (\tilde{w})^n = \tilde{w}^n \sim \tilde{w}^{n+m} = (\tilde{w})^{n+m} = x^{n+m}$ . Isto em particular implica que  $\mathcal{M}$  é um monóide de torção e por conseguinte estável devido à proposição 5.2. A partir da mesma proposição,  $\mathcal{J} = \mathcal{D}$ . Definimos então as relações Green-induzidas sobre  $A^*$ , como visto no capítulo 5. Se  $n = m = 1$ , o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$  é também chamado de *banda livre gerada por  $A$*  ou *monóide idempotente livre gerado por  $A$*  (já que para todo  $x \in \mathcal{M}$  temos que então  $x = x^2$ ).

## 6.2 O teorema dos marcadores

A banda livre gerada por um conjunto finito de geradores é finita e bem conhecida desde 1952 devido ao clássico trabalho de Green e Rees [11]. Pode-se calcular a cardinalidade da banda livre em função da cardinalidade do conjunto gerador, como pode ser visto no trabalho de McLean [26]. De fato, o trabalho de Green e Rees estuda os monóides de Burnside livres  $\mathcal{M}$  satisfazendo  $x^n = x^{n+m}$  para os casos em que  $n = 1$  e  $m \geq 1$  e caracteriza a

estrutura das  $\mathcal{J}$ -classes,  $\mathcal{R}$ -classes e  $\mathcal{L}$ -classes destes monóides, que é fundamentalmente a mesma independentemente dos valores de  $m$ . Contudo, aquele trabalho pouco informa sobre a estrutura interna das  $\mathcal{H}$ -classes, a não ser o fato que os grupos maximais são quocientes de um grupo de Burnside livre satisfazendo  $x^m = 1$ . O conceito-chave envolvido no trabalho é o *conteúdo de uma palavra*  $w$  que já definimos por

$$c(w) \stackrel{\text{def}}{=} \text{o conjunto das letras de } A \text{ que ocorrem em } w.$$

Além dos artigos originais, uma boa referência para o assunto é o livro de Lallement [21]. Na seção 3 do capítulo 10 desta referência, pode ser encontrada uma demonstração completa para a proposição 6.1, em que sintetizamos alguns resultados sobre a estrutura fornecida pelas relações de Green. Em particular, o item 1 garante-nos que  $\mathcal{M}$  tem exatamente  $2^{|A|}$   $\mathcal{J}$ -classes. No caso do item 8, temos uma banda livre e, como as  $\mathcal{H}$ -classes são triviais, segue que as relações  $\sim$  e  $\mathcal{H}'$  coincidem e o referido item é uma consequência imediata dos itens 2 e 5. De fato, todas as relações Green-induzidas são caracterizadas na proposição 6.1.

**Proposição 6.1** *Sejam inteiros  $n = 1$  e  $m \geq 1$ , seja  $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por um alfabeto  $A$  e sejam as relações Green-induzidas pelo morfismo canônico  $\tilde{\cdot} : A^* \rightarrow \mathcal{M}$ . Dadas as palavras  $w, w', u$  e  $u'$  e as letras  $a$  e  $a'$ , temos que:*

1.  $w \mathcal{J}' w'$  se e só se  $c(w) = c(w')$ ;
2.  $w \mathcal{R}' w'$  se e só se  $\epsilon_R(w) \sim \epsilon_R(w')$ ;
3.  $\epsilon_R(w) = ua$  se e só se  $ua \in \text{Pref}(w)$  e  $a \notin c(u) = c(w) \setminus \{a\}$ ;
4. duas  $\mathcal{R}$ -entradas  $ua$  e  $u'a'$  são congruentes se e só se  $a = a'$  e  $u \sim u'$ ;
5.  $w \mathcal{L}' w'$  se e só se  $\epsilon_L(w) \sim \epsilon_L(w')$ ;
6.  $\epsilon_L(w) = au$  se e só se  $au \in \text{Suf}(w)$  e  $a \notin c(u) = c(w) \setminus \{a\}$ ;
7. duas  $\mathcal{L}$ -entradas  $au$  e  $a'u'$  são congruentes se e só se  $a = a'$  e  $u \sim u'$ ;
8. se  $m = 1$ , então  $w \sim w'$  se e só se  $\epsilon_R(w) \sim \epsilon_R(w')$  e  $\epsilon_L(w) \sim \epsilon_L(w')$ .

Note que o item 1 da proposição 6.1 caracteriza a relação  $\mathcal{J}'$ . Assim temos condições de caracterizar as  $\mathcal{D}$ -entradas e as transições do monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  para o caso em que  $n = 1$ .

**Proposição 6.2** *Sejam inteiros  $n = 1$  e  $m \geq 1$ , seja  $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por um alfabeto  $A$  e sejam as relações Green-induzidas pelo morfismo canônico  $\tilde{\cdot} : A^* \rightarrow \mathcal{M}$ . Então:*

1. as  $\mathcal{D}$ -entradas são as letras e as palavras da forma  $aub$  com  $a, b \in A$  e  $u \in A^*$  e  $a, b \notin c(u)$  e  $a \neq b$ ;
2. as transições são as palavras da forma  $aua$  com  $a \in A$  e  $u \in A^*$  e  $a \notin c(u)$ .

*Prova.* A partir do item 1 da proposição 6.1 temos que duas palavras estão na mesma  $\mathcal{D}'$ -classe se e só se têm o mesmo conteúdo já que  $\mathcal{J}' = \mathcal{D}'$ . Usaremos extensivamente este fato.

Vamos provar o item 1. O único fator próprio de uma letra é a palavra vazia, que tem conteúdo diferente e portanto está numa  $\mathcal{D}'$ -classe distinta. Isto implica que toda letra é uma  $\mathcal{D}$ -entrada. Suponha que  $a, b \in A$  e  $u \in A^*$  sejam tais que  $a, b \notin c(u)$  e  $a \neq b$ . Temos que  $c(aub) = \{a\} + \{b\} + c(u)$  e o único fator de  $aub$  que possui o mesmo conteúdo é o próprio  $aub$ . Assim, nenhum fator próprio de  $aub$  está na mesma  $\mathcal{D}'$ -classe e  $aub$  é uma  $\mathcal{D}$ -entrada. Seja  $w$  uma  $\mathcal{D}$ -entrada. Se  $|w| = 1$ ,  $w$  é constituído de uma letra. Suponha pois que  $|w| \geq 2$ . Sejam  $a, b \in A$  e  $u \in A^*$  tais que  $w = aub$ . Como  $au \mathcal{P}' aub$  temos que  $c(au) \neq c(aub) = c(au) \cup \{b\}$ . Assim  $b \neq a$  e  $b \notin c(u) \subseteq c(au)$ . Da mesma forma,  $ub \mathcal{P}' aub$  implica que  $a \notin c(u)$ .

Vamos provar o item 2. Suponha primeiro  $a \in A$  e  $u \in A^*$  tais que  $a \notin c(u)$ . Assim  $c(au) = c(aua) = c(ua) = c(u) + \{a\} \neq c(u)$ . Isto prova que  $au \mathcal{D}' au$  e portanto que  $aua$  é uma transição. Suponha agora  $a, b \in A$  e  $u \in A^*$  tais que  $aub$  seja uma transição. Como  $u \mathcal{P}' au$  temos que  $c(u) \neq c(au) = \{a\} \cup c(u)$ . Assim  $a \notin c(u)$ . Analogamente,  $u \mathcal{P}' ub$  implica que  $b \notin c(u)$ . Como  $au \mathcal{D}' ub$  temos que  $\{a\} + c(u) = c(au) = c(ub) = \{b\} + c(u)$ . Como  $a, b \notin c(u)$ , segue então que  $a = b$ . ■

Em 1970 [30] I. Simon estudou o monóide de Burnside livre satisfazendo  $x^2 = x^3$  gerado por um conjunto de dois geradores e tentou obter algumas propriedades finitas para o monóide. De fato, acabava-se de descobrir que este monóide era infinito, por trabalho de Brzozowski et al. [2].

Algumas propriedades válidas no monóide idempotente livre foram provadas para este monóide livre. Isto inclui alguns resultados sobre a estrutura das  $\mathcal{R}$ -classes (e das  $\mathcal{L}$ -classes) listados acima, mais precisamente os ítems 2 e 4 (e os ítems 5 e 7), que de fato foram mostrados para os casos  $n \geq 2$  e  $m = 1$ . O teorema 6.3 que se segue generaliza estes resultados para quaisquer valores  $n \geq 1$  e  $m \geq 1$ , embora sua demonstração seja essencialmente a mesma vista em [30].

**Teorema 6.3 (teorema dos marcadores)** *Sejam inteiros  $n \geq 1$  e  $m \geq 1$ , seja  $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por um alfabeto  $A$  e sejam as relações Green-induzidas pelo morfismo canônico  $\tilde{\cdot} : A^* \rightarrow \mathcal{M}$ . Sejam  $w, w' \in A^+$  duas palavras tais que  $w \mathcal{R}' w'$  e sejam  $u$  e  $u'$  suas respectivas  $\mathcal{R}$ -entradas. Então:*

- $u \sim u'$ ;
- a última letra de  $u$  é a mesma última letra de  $u'$ ;
- $ua^{-1} \sim u'a^{-1}$  onde  $a$  é a última letra de  $u$  e de  $u'$ .

*Prova.* Seja  $f$  uma função que aplica  $A^+$  em  $\mathcal{M} \times A$  definida da seguinte forma: se  $y$  é a  $\mathcal{R}$ -entrada de  $x$  e  $a$  é a última letra de  $y$  então  $f(x) \stackrel{\text{def}}{=} (\widetilde{ya^{-1}}, a)$ . É suficiente provar que  $f(w) = f(w')$ .

Vamos provar que a congruência  $\sim$  preserva  $f$ . É suficiente provar que se  $(x, x')$  é uma substituição por  $\{(t^{n+m}, t^n) \mid t \in A^+\}$ , então  $x$  e  $x'$  assumem o mesmo valor por  $f$ . Sejam pois  $r, s, t \in A^*$  tais que  $x = rt^{n+m}s$  e que  $x' = rt^ns$ . Sejam  $u, v, v' \in A^*$  e  $a \in A$  tais que  $ua$  seja a  $\mathcal{R}$ -entrada de  $x = uav$  e que  $uavv' \sim ua$ . Assim temos que  $f(x) = (\tilde{u}, a)$ . Como  $rt^{n+m}s = x = uav$ , temos que  $rt^n, rt^{n+m}, u$  e  $ua$  são prefixos de  $x$ . Conforme os comprimentos destes prefixos, temos os seguintes três casos a considerar:

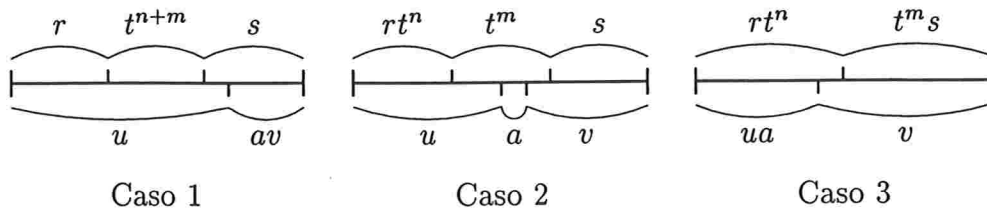


Figura 6.1: Representação de  $rt^{n+m}s = x = uav$

1. Suponha que  $|rt^{n+m}| \leq |u|$ . Neste caso  $rt^{n+m} \in \text{Pref}(u)$  e  $av \in \text{Suf}(s) \subseteq \text{Suf}(x')$ . (Vide a figura 6.1.) Seja  $u' = x'(av)^{-1}$ . Notemos que  $u' = x'(av)^{-1} = (rt^n s)(av)^{-1} = (rt^n)(s(av)^{-1}) \sim (rt^{n+m})(s(av)^{-1}) = (rt^{n+m}s)(av)^{-1} = x(av)^{-1} = u$ . Assim temos que  $u'avv' \sim uavv' \sim ua \sim u'a$ . Isto em particular implica que  $u'a \mathcal{R}' u'av = x'$ . Suponha por absurdo que  $u' \mathcal{R}' x'$ . Assim temos que existe  $v'' \in A^*$  tal que  $u' \sim x'v''$ . Daí segue que  $u \sim u' \sim x'v'' = u'avv'' \sim uavv'$  e que  $u \mathcal{R}' uav = x$ , contradizendo com o fato de  $ua$  ser  $\mathcal{R}$ -entrada de  $x$ . Isto prova que  $u' \mathcal{R}' x'$  e portanto que  $u'a$  é a  $\mathcal{R}$ -entrada de  $x'$ . Para concluir este caso, temos que  $f(x) = (\tilde{u}, a) = (\tilde{u}', a) = f(x')$  pois  $u \sim u'$ .
2. Suponha que  $|rt^{n+m}| \geq |ua| > |rt^n|$ . Neste caso temos que  $|u| \geq |rt^n|$  e portanto que  $rt^n \in \text{Pref}(u)$  e que  $ua \in \text{Pref}(rt^{n+m})$ . (Vide a figura 6.1.) Assim temos que  $\text{Pref}(rt^n) \subset \text{Pref}(u) \subset \text{Pref}(ua) \subseteq \text{Pref}(rt^{n+m})$ . Como  $rt^n \sim rt^{n+m}$  temos então que  $rt^n \sim rt^{n+m} \mathcal{R}' u \mathcal{R}' ua$  o que contradiz com o fato de que  $ua$  é a  $\mathcal{R}$ -entrada de  $x$ . Este caso não ocorre.
3. Suponha que  $|rt^n| \geq |ua|$ . Neste caso temos que  $ua \in \text{Pref}(rt^n) \subseteq \text{Pref}(x')$ . (Vide a figura 6.1.) Como  $ua \mathcal{R}' x \sim x'$  e como  $u \mathcal{R}' x \sim x'$  temos que  $ua$  é a  $\mathcal{R}$ -entrada de  $x'$ . Para concluir este caso temos então que  $f(x) = (\tilde{u}, a) = f(x')$ .

Vamos agora provar que  $f(w) = f(w')$ . Como  $w \mathcal{R}' w'$ , seja  $z \in A^*$  tal que  $wz \sim w'$ . Assim temos que  $f(wz) = f(w')$  já que  $f$  é preservada por  $\sim$ . Como  $w \mathcal{R}' wz$  temos que as  $\mathcal{R}$ -entradas de  $w$  e de  $wz$  coincidem e portanto  $f(w) = f(wz) = f(w')$ . ■

Relembramos que o “frame” das  $\mathcal{R}$ -classes é um grafo dirigido onde os vértices são as  $\mathcal{R}$ -classes e existe uma aresta com rótulo  $g$  de  $R$  para  $R'$  se e só se existirem  $x \in R$  e um gerador  $g$  tais que  $xg \in R'$ . Se a  $\mathcal{R}$ -entrada de uma palavra  $w \in A^+$  for  $ua$  onde  $a \in A$ , o teorema 6.3 implica que a  $\mathcal{R}$ -classe de  $\tilde{w}$  recebe uma única aresta no frame e esta aresta é proveniente da  $\mathcal{R}$ -classe de  $\tilde{u}$  e possui rótulo  $\tilde{a}$ . Segue facilmente então o corolário 6.4.

**Corolário 6.4** *O frame das  $\mathcal{R}$ -classes de  $\mathcal{M}$  é uma árvore.*

No corolário 6.5 aplicamos o teorema 6.3 de modo a caracterizar quando duas  $\mathcal{D}$ -entradas são congruentes.

**Corolário 6.5** *Duas  $\mathcal{D}$ -entradas  $aub$  e  $a'u'b'$ , com  $a, a', b, b' \in A$  e  $u, u' \in A^*$ , são congruentes se e só se  $a = a'$  e  $b = b'$  e  $u \sim u'$ . Ademais, a menor  $\mathcal{D}$ -entrada numa classe de congruência é também a menor palavra nesta classe.*

*Prova.* Naturalmente,  $a = a'$  e  $b = b'$  e  $u \sim u'$  implicam que  $aub \sim a'u'b'$ . Suponha agora que  $aub \sim a'u'b'$ . Usando a proposição 5.5, temos que  $aub$  e  $a'u'b'$  são duas congruentes  $\mathcal{L}$ -entradas e, pelo dual do teorema 6.3, temos que  $a = a'$  e  $ub \sim u'b'$ . Dado que  $ub$  e  $u'b'$  são duas  $\mathcal{R}$ -entradas devido à proposição 5.6, usando o teorema 6.3 segue que  $b = b'$  e que  $u \sim u'$ .

Vamos agora provar que a menor  $\mathcal{D}$ -entrada numa classe de congruência é também a menor palavra na mesma classe de congruência. Seja  $d$  uma  $\mathcal{D}$ -entrada tal que  $d$  seja a menor  $\mathcal{D}$ -entrada em sua classe de congruência e seja  $d'$  a menor palavra tal que  $d' \sim d$ . Temos então que  $\epsilon_R(d') \sim \epsilon_R(d) = d \sim d'$  devido ao teorema 6.3 e à proposição 5.5. De forma dual temos que  $\epsilon_L(d') \sim d'$ . Como  $d'$  é a menor palavra em sua classe de congruência e os seus fatores  $\epsilon_R(d')$  e  $\epsilon_L(d')$  são tais que  $\epsilon_R(d') \sim \epsilon_L(d') \sim d'$ , temos que estes fatores não podem ser próprios, implicando pois que  $d'$  é uma  $\mathcal{R}$ -entrada, uma  $\mathcal{L}$ -entrada e portanto uma  $\mathcal{D}$ -entrada devido à proposição 5.5. Isto prova que  $d' = d$ . ■

Veremos agora uma aplicação do teorema 6.3 para os sistemas de adequações. Seja  $(\mu, \eta, \psi, \psi^R, \psi^L)$  um sistema de adequações associado a um  $\sim$ -idempotente  $e \in A^+$ . Dadas duas transições  $t, t'$  na  $\mathcal{D}'$ -classe de  $e$ , naturalmente podemos nos perguntar se  $t \sim t'$  implica que  $\psi(t) \sim \psi(t')$ . Em geral, esta implicação não é verdadeira. Na proposição seguinte veremos que, no caso de um monóide de Burnside livre, é suficiente para tanto que o sistema de adequações seja coerente. Relembramos que o sistema de adequações é coerente se, para quaisquer  $\mathcal{D}$ -entradas  $d \sim d'$  na mesma  $\mathcal{D}'$ -classe de  $e$ , tivermos que  $\mu_d \sim \mu_{d'}$  e  $\eta_d \sim \eta_{d'}$ .

**Proposição 6.6** *Seja  $(\mu, \eta, \psi, \psi^R, \psi^L)$  um sistema de adequações associado a um  $\sim$ -idempotente  $e \in A^+$ . Sejam  $t$  e  $t'$  duas transições,  $r$  e  $r'$  duas  $\mathcal{R}$ -entradas,  $l$  e  $l'$  duas  $\mathcal{L}$ -entradas, todas na  $\mathcal{D}'$ -classe de  $e$ .*

*Se o sistema for coerente, então temos que:*

1.  $t \sim t' \implies \psi(t) \sim \psi(t')$ ;
2.  $r \sim r' \implies \psi^R(r) \sim \psi^R(r')$ ;
3.  $l \sim l' \implies \psi^L(l) \sim \psi^L(l')$ .

*Prova.* Vamos provar o item 1. Devido à proposição 5.9  $(1, \epsilon_R(t), \epsilon_R(t)^{-1}t)$  e  $(t\epsilon_L(t)^{-1}, \epsilon_L(t), 1)$  são ocorrências de  $\mathcal{D}$ -entradas de  $t$ , o que implica que  $\epsilon_R(t)$  e  $\epsilon_L(t)$  são duas  $\mathcal{D}$ -entradas e estão na  $\mathcal{D}'$ -classe de  $t$  e de  $e$ . Analogamente,  $\epsilon_R(t')$  e  $\epsilon_L(t')$  são duas  $\mathcal{D}$ -entradas e estão na mesma  $\mathcal{D}'$ -classe de  $e$ , podendo pois serem definidas as adequações  $\mu_{\epsilon_R(t)}$ ,  $\eta_{\epsilon_L(t)}$ ,  $\mu_{\epsilon_R(t')}$  e  $\eta_{\epsilon_L(t')}$ . Suponha que  $t \sim t'$ . Assim  $\epsilon_R(t) \sim \epsilon_R(t')$  devido ao teorema 6.3 e de forma dual temos que  $\epsilon_L(t) \sim \epsilon_L(t')$ . Dado que o sistema de adequações é coerente,  $\mu_{\epsilon_R(t)} \sim \mu_{\epsilon_R(t')}$  e  $\eta_{\epsilon_L(t)} \sim \eta_{\epsilon_L(t')}$ . Assim concluímos que  $\psi(t) = \mu_{\epsilon_R(t)} t \eta_{\epsilon_L(t)} \sim \mu_{\epsilon_R(t')} t' \eta_{\epsilon_L(t')} = \psi(t')$ .

Vamos provar o item 2. Tendo em vista que  $(r\epsilon_L(r)^{-1}, \epsilon_L(r), 1)$  é uma fatoração de  $r$  devido à proposição 5.7, temos que  $\epsilon_L(r)$  é uma  $\mathcal{D}$ -entrada na mesma  $\mathcal{D}'$ -classe de  $r$  e de  $e$ . Analogamente,  $\epsilon_L(r')$  é uma  $\mathcal{D}$ -entrada na  $\mathcal{D}'$ -classe de  $e$  e podem ser definidas as adequações à direita  $\eta_{\epsilon_L(r)}$  e  $\eta_{\epsilon_L(r')}$ . Suponha que  $r \sim r'$ . Logo  $\epsilon_L(r) \sim \epsilon_L(r')$  devido ao dual do teorema 6.3 e, desde que o sistema de adequações é coerente,  $\eta_{\epsilon_L(r)} \sim \eta_{\epsilon_L(r')}$ . Concluímos pois que  $\psi^R(r) = r \eta_{\epsilon_L(r)} \sim r' \eta_{\epsilon_L(r')} = \psi^R(r')$ .

Provamos o item 3 de forma dual ao item 2. ■

### 6.3 Grafo fundamental

Seja  $D$  uma  $\mathcal{D}$ -classe qualquer do semigrupo de Burnside livre  $\mathcal{M} \setminus \{\tilde{1}\}$ . Seja

$$V = \{\tilde{d} \in D \mid d \text{ é uma } \mathcal{D}\text{-entrada}\}$$

e seja

$$E = \{\tilde{t} \in D \mid t \text{ é uma transição}\}.$$

Qualquer transição  $t$  tem por prefixo a  $\mathcal{D}$ -entrada  $\epsilon_R(t)$  e por sufixo a  $\mathcal{D}$ -entrada  $\epsilon_L(t)$ , devido à proposição 5.9. Assim definimos a função  $\alpha : E \rightarrow V$  por

$$\alpha(\tilde{t}) = \widetilde{\epsilon_R(t)}$$

onde  $t$  é uma transição tal que  $\tilde{t} \in E$ . Esta definição não depende da particular escolha de  $t$  pois se  $t'$  é tal que  $\tilde{t}' = \tilde{t}$  então o teorema 6.3 implica que  $\widetilde{\epsilon_R(t')} = \widetilde{\epsilon_R(t)}$ . De forma dual, definimos a função  $\omega : E \rightarrow V$  por

$$\omega(\tilde{t}) = \widetilde{\epsilon_L(t)}$$



onde  $t$  é uma transição tal que  $\tilde{t} \in E$ . Esta definição também não depende da particular escolha de  $t$  pois se  $t'$  é tal que  $\tilde{t}' = \tilde{t}$  então o dual do teorema 6.3 implica que  $\epsilon_L(\tilde{t}') = \epsilon_L(\tilde{t})$ . Assim sendo, podemos definir  $\mathbf{G} = (V, E, \alpha, \omega)$  um grafo onde o conjunto de vértices é  $V$ , o conjunto de arestas é  $E$  e as funções de incidência são  $\alpha$  e  $\omega$ . Este grafo  $\mathbf{G}$  assim definido é chamado de *grafo fundamental de  $D$*  (ou grafo fundamental de qualquer elemento de  $D$ ). Adiantamos que o grafo fundamental  $\mathbf{G}$  é fortemente conexo, como será visto na proposição 6.8.

Veremos agora um exemplo um pouco mais imediato destes conceitos. Este exemplo também será o ponto de partida para a ilustração de outros conceitos a serem vistos ainda neste capítulo. O exemplo a ser considerado é o da  $\mathcal{D}$ -classe de  $\tilde{abc}$  na banda livre gerada por  $\{a, b, c\}$ , como veremos no exemplo 6.7.

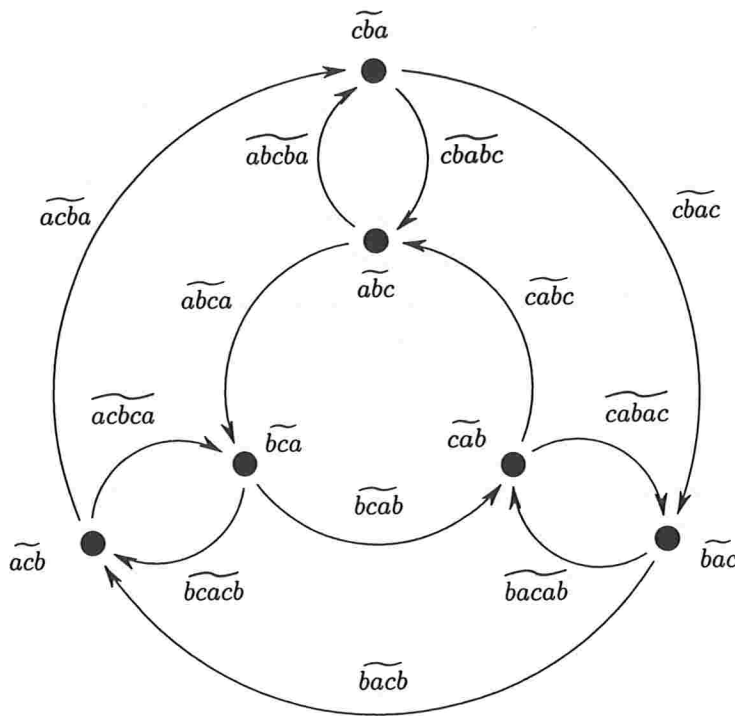


Figura 6.2: Grafo fundamental da  $\mathcal{D}$ -classe de  $\tilde{abc}$  na banda livre

**Exemplo 6.7** Seja  $A = \{a, b, c\}$ , seja  $n = m = 1$  e seja  $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$ . Então o grafo fundamental da  $\mathcal{D}$ -classe de  $\widetilde{abc}$  é o grafo definido na figura 6.2.

*Prova.* Seja  $\mathbf{G}$  o grafo fundamental da  $\mathcal{D}$ -classe de  $\widetilde{abc}$ . Toda palavra na  $\mathcal{D}'$ -classe de  $abc$  tem conteúdo  $A$  devido ao fato de que  $\mathcal{D}' = \mathcal{J}'$  e ao item 1 da proposição 6.1.

Vamos calcular  $V(\mathbf{G})$ . Usando o item 1 da proposição 6.2, segue facilmente que uma palavra  $w$  é uma  $\mathcal{D}$ -entrada na  $\mathcal{D}'$ -classe de  $abc$  se e só se existirem um inteiro  $k \geq 1$  e  $(a_1, a_2, a_3)$  uma permutação de  $(a, b, c)$  tais que  $w = a_1 a_2^k a_3$ . Usando o corolário 6.5, temos que duas tais  $\mathcal{D}$ -entradas  $w = a_1 a_2^k a_3$  e  $w' = a'_1 a_2^{k'} a'_3$  são congruentes se e só se  $a_1 = a'_1$ ,  $a_3 = a'_3$ , e  $a_2^k \sim a_2^{k'}$ . Note que  $a_2^k \sim a_2^{k'}$  se e só se  $a_2 = a'_2$ . Assim,  $V(\mathbf{G}) = \{\widetilde{a_1 a_2 a_3} \mid (a_1, a_2, a_3) \text{ é uma permutação qualquer de } (a, b, c)\}$ .

Vamos calcular  $E(\mathbf{G})$ . Usando o item 2 da proposição 6.2, segue facilmente que uma palavra  $a_1 u a_2$ , com  $a_1, a_2 \in A$ , é uma transição na  $\mathcal{D}'$ -classe de  $abc$  se e só se  $a_1 = a_2$  e  $c(u) = A \setminus \{a_1\}$ . Precisamos caracterizar quais destas transições estão na mesma classe de congruência. Naturalmente que duas tais transições  $a_1 u a_1$  e  $a'_1 u' a'_1$  são congruentes se  $a_1 = a'_1$  e  $u \sim u'$ . Se  $a_1 = a$ , por exemplo, os possíveis valores para  $u$  são  $bc$ ,  $cb$ ,  $bc b$  ou  $cb c$  já que qualquer outra palavra de conteúdo  $\{b, c\}$  está na classe de congruência de uma destas palavras. (Referimos o leitor ao trabalho de Green e Rees [11] para a verificação desta afirmativa.) Assim,  $E(\mathbf{G}) = \{\widetilde{a_1 a_2 a_3 a_1}, \widetilde{a_1 a_2 a_3 a_2 a_1} \mid (a_1, a_2, a_3) \text{ é uma permutação qualquer de } (a, b, c)\}$ . Ademais, duas destas 12 transições acima são diferentes. Para provar este fato basta notar que dentre as 12 palavras da forma  $a_1 a_2 a_3 a_1$  ou  $a_1 a_2 a_3 a_2 a_1$ ,  $abca$  e  $abcba$  são as únicas cuja  $\mathcal{R}$ -entrada é  $abc$ . Todas as demais têm uma  $\mathcal{R}$ -entrada não congruente a  $abc$ . Assim, só estas estão na mesma  $\mathcal{R}'$ -classe devido ao teorema 6.3. Como elas possuem  $\mathcal{L}$ -entradas que não são congruentes, não estão na mesma  $\mathcal{L}'$ -classe devido ao dual do mesmo teorema e não são congruentes portanto. Outra maneira de provar este fato é antecipar o uso do corolário 7.4 a ser visto no capítulo 7.

Quanto à aplicação das funções de incidência às arestas, é imediato verificar que as incidências são aquelas representadas na figura 6.2. ■

Como já comentamos antes, o grafo fundamental de uma  $\mathcal{D}$ -classe de  $\mathcal{M} \setminus \{\tilde{1}\}$  é fortemente conexo. É o que nos prova a proposição 6.8.

**Proposição 6.8** *Todo grafo fundamental de uma  $\mathcal{D}$ -classe de um semigrupo de Burnside livre é fortemente conexo.*

*Prova.* Seja  $\mathbf{G}$  um grafo fundamental qualquer. Como existe ao menos uma  $\mathcal{D}$ -entrada numa  $\mathcal{D}'$ -classe, existe ao menos um vértice em  $V(\mathbf{G})$ . Sejam  $v, v' \in V(\mathbf{G})$  dois vértices quaisquer e sejam  $d$  e  $d'$  duas  $\mathcal{D}$ -entradas tais que  $\tilde{d} = v$  e  $\tilde{d}' = v'$ . Seja  $w$  tal que  $d \mathcal{R}' w \mathcal{L}' d'$ . Como  $\epsilon_R(d) = d = \epsilon_L(d)$  devido à proposição 5.5, usando o teorema 6.3 e seu dual temos  $\epsilon_R(w) \sim \epsilon_R(d) = d$  e  $\epsilon_L(\epsilon_R(w)) \sim \epsilon_L(d) = d$ . De maneira dual provamos que  $\epsilon_R(\epsilon_L(w)) \sim d'$ . Daí, o passeio  $\sigma(w)$  é um passeio de  $\epsilon_L(\widetilde{\epsilon_R(w)}) = \tilde{d} = v$  a  $\epsilon_R(\widetilde{\epsilon_L(w)}) = \tilde{d}' = v'$ . ■

## 6.4 Digital e inversa

Seja  $w \in A^+$  uma palavra e seja  $\mathbf{G}_w$  o grafo fundamental da  $\mathcal{D}$ -classe de  $w$ . Seja  $w_1, \dots, w_k$  a seqüência de transições de  $w$  e seja  $y_0 = \epsilon_L(\epsilon_R(w))$ . A partir do corolário 5.8 temos que  $y_0 = \epsilon_L(\epsilon_R(w)) \mathcal{D}' w$  é uma  $\mathcal{D}$ -entrada. A função<sup>1</sup>  $\sigma : A^+ \rightarrow \cup_{w \in A^+} \mathbf{G}_w^*$  define a *digital de  $w$*  como sendo o passeio em  $\mathbf{G}_w$ :

$$\sigma(w) = \begin{cases} (\widetilde{w_1}, \widetilde{w_2}, \dots, \widetilde{w_k}), & \text{se } k > 0; \\ 1_{\widetilde{y_0}}, & \text{se } k = 0. \end{cases}$$

Este é um passeio de  $\epsilon_L(\widetilde{\epsilon_R(w)})$  para  $\epsilon_R(\widetilde{\epsilon_L(w)})$ . De fato, sendo  $w_0 = \epsilon_R(w)$  e  $w_{k+1} = \epsilon_L(w)$  e  $y_k = \epsilon_R(\epsilon_L(w))$ , o lema 5.11 implica que  $\epsilon_L(\epsilon_R(w)) = \epsilon_L(w_0) = y_0 = \epsilon_R(w_1)$  e que  $\epsilon_R(\epsilon_L(w)) = \epsilon_R(w_{k+1}) = y_k = \epsilon_L(w_k)$ . Se  $k = 0$ , temos que o início do passeio  $\sigma(w)$  é  $\alpha(\sigma(w)) = \alpha(1_{\widetilde{y_0}}) = \widetilde{y_0} = \epsilon_L(\widetilde{\epsilon_R(w)})$  e que o término do mesmo passeio é  $\omega(\sigma(w)) = \omega(1_{\widetilde{y_0}}) = \widetilde{y_0} = \widetilde{y_k} = \epsilon_R(\widetilde{\epsilon_L(w)})$ . Se  $k > 0$ , temos que o início do passeio  $\sigma(w)$  é  $\alpha(\sigma(w)) = \alpha(\widetilde{w_1}) = \epsilon_R(\widetilde{w_1}) = \epsilon_L(\widetilde{\epsilon_R(w)})$  e que o término do mesmo passeio é  $\omega(\sigma(w)) = \omega(\widetilde{w_k}) = \epsilon_L(w_k) = \epsilon_R(\widetilde{\epsilon_L(w)})$ .

Seja  $\mathbf{G}$  um grafo fundamental qualquer e seja  $\mathcal{K} = \mathbf{G}^*$  a categoria livre gerada por  $\mathbf{G}$ . Vamos agora definir uma função<sup>2</sup>  $\tau : \mathcal{K} \rightarrow A^+$  que faz o papel da inversa da função  $\sigma$ , como veremos na proposição 6.11:

- se  $p = 1_v$  onde  $v \in V$ , definimos  $\tau(p)$  como a menor<sup>3</sup>  $\mathcal{D}$ -entrada  $d$  tal

<sup>1</sup>Esta função não é um morfismo.

<sup>2</sup>Esta função também não é um morfismo.

<sup>3</sup>Relembramos que a ordem implícita em  $A^*$  é a ordem militar.

que  $\tilde{d} = v$ ;

- se  $p = b_1 b_2 \cdots b_k \in \mathcal{K}$  com  $k \geq 1$  e  $b_i \in \mathbf{G}$  para  $i \in \{1, 2, \dots, k\}$ , definimos  $\tau(p) = w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_k)^{-1}w_k)$  onde  $w_i$  é a menor transição tal que  $b_i = \tilde{w}_i$ , para  $i \in \{1, 2, \dots, k\}$ .

Um leitor mais atento pode ter notado alguma semelhança entre a palavra  $\tau(p)$  definida para um passeio não vazio e a palavra definida na proposição 5.12. Esta semelhança será bem explorada, como veremos à frente na proposição 6.11.

Considere o exemplo 6.7. Seja dada a palavra  $w = babcbabac$ . Dado que  $c(w) = A = c(abc)$ , temos  $w \mathcal{D}' abc$  e o grafo fundamental de  $\tilde{w}$  é aquele visto no exemplo 6.7. A seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$  é  $(b, abc, babac)$ ,  $(bab, cba, bac)$ ,  $(babcbabac, bac, 1)$ , a seqüência de ocorrências de transições de  $w$  é  $(b, abcba, bac)$ ,  $(bab, cbabac, 1)$  e a seqüência de transições de  $w$  é  $abcba, cbabac$ . Note que  $cbabac \sim cbac$ . Assim sendo, a digital de  $w$  é  $\sigma(w) = (\widetilde{abcba}, \widetilde{cbac})$ , que é um passeio de  $\widetilde{abc} = \epsilon_L(\epsilon_R(w))$  a  $\widetilde{bac} = \epsilon_R(\epsilon_L(w))$ . Considere agora o passeio  $p = (\widetilde{abcba}, \widetilde{cbac})$ . Pode-se provar, e não o faremos aqui, que as palavras  $x$  tais que o símbolo  $\tilde{x}$  aparece na figura 6.2 são as menores palavras em suas classes de congruência. Assim,  $\tau(p) = abcba((cba)^{-1}cbac) = abcba c = abcbac$ .

Dada uma transição qualquer, na proposição 6.9 veremos uma maneira de construir uma transição diferente mas ainda congruente à primeira transição.

**Proposição 6.9** *Sejam  $r$  uma  $\mathcal{R}$ -entrada que é sufixo de uma transição  $w$  e  $r'$  uma  $\mathcal{R}$ -entrada congruente a  $r$ . Então  $(wr^{-1})r'$  é uma transição congruente a  $w$ .*

*Prova.* A partir do teorema 6.3 temos que existe uma letra  $b \in A$  e palavra  $x$  tais que:  $r' = xb$ ,  $b \in \text{Suf}(r)$  e  $x \sim rb^{-1}$ . Como  $b \in \text{Suf}(r) \subseteq \text{Suf}(w)$ , como  $w$  é uma transição, podemos escolher  $a \in A$  e  $u \in A^*$  tais que  $w = aub$ . Por definição,  $au \mathcal{D}' aub = w$ . Do item 2 do corolário 5.3 temos que  $au \mathcal{R}' aub$ , implicando pois que  $w = aub$  não é uma  $\mathcal{R}$ -entrada e que  $r \neq w$ . Assim, temos que  $|wr^{-1}| \geq 1 = |a|$  e portanto que  $a \in \text{Pref}(wr^{-1})$  pois  $a, wr^{-1} \in \text{Pref}(w)$ . Podemos então definir  $v = a^{-1}wr^{-1}$ . Dado que  $x \sim rb^{-1}$ , temos pois que  $vx \sim vrb^{-1} = (a^{-1}wr^{-1})(rb^{-1}) = a^{-1}wb^{-1} = u$ . Como  $aub = w$  é uma transição, por definição temos que  $au \mathcal{D}' aub \mathcal{D}' ub \mathcal{P}' u$ . Como

$u \sim vx$ , segue de imediato que  $avx \mathcal{D}' avxb \mathcal{D}' vxb \mathcal{P}' vx$ . Assim  $(wr^{-1})r' = ((avr)r^{-1})r' = avr' = avxb$  é uma transição congruente à transição  $aub = w$ .

■

Na proposição 6.10 veremos algumas propriedades de uma menor transição em sua classe de congruência. Esta proposição ser-nos-á necessária a uma caracterização da função  $\tau$ .

**Proposição 6.10** *Seja  $w$  a menor transição em sua classe de congruência. As seguintes afirmativas são verdadeiras:*

- $\epsilon_R(w)$  e  $\epsilon_L(w)$  são as menores  $\mathcal{D}$ -entradas em suas respectivas classes de congruência;
- se  $u$  é uma transição congruente a  $w$  temos que  $w\epsilon_L(w)^{-1} \leq u\epsilon_L(u)^{-1}$  e  $\epsilon_R(w)^{-1}w \leq \epsilon_R(u)^{-1}u$ .

*Prova.* Vamos primeiro provar que  $\epsilon_R(w)$  e  $\epsilon_L(w)$  são as menores  $\mathcal{D}$ -entradas em suas respectivas classes de congruência. Como  $w$  é uma transição, temos que  $(1, \epsilon_R(w), \epsilon_R(w)^{-1}w)$  e  $(w\epsilon_L(w)^{-1}, \epsilon_L(w), 1)$  são as únicas ocorrências de  $\mathcal{D}$ -entradas de  $w$  e são distintas devido à proposição 5.9. Como as ocorrências de  $\mathcal{D}$ -entradas são distintas,  $\epsilon_R(w) \neq w \neq \epsilon_L(w)$  pois caso contrário teríamos que  $\epsilon_R(w)^{-1}w = 1$  ou  $w\epsilon_L(w)^{-1} = 1$ , implicando pois que as ocorrências de  $\mathcal{D}$ -entradas em questão seriam comparáveis pela ordem  $\leq$  e contradizendo com a minimalidade das ocorrências de  $\mathcal{D}$ -entradas. Seja  $x$  a menor  $\mathcal{D}$ -entrada na classe de congruência de  $\epsilon_L(w)$ . Como acabamos de provar,  $x$  é também a menor palavra em sua classe de congruência. Da proposição 5.5 temos que  $x$  é uma  $\mathcal{R}$ -entrada. Usando a proposição 6.9 temos que  $(w\epsilon_L(w)^{-1})x$  é uma transição na mesma classe de congruência de  $w$ . Da minimalidade de  $x$ , temos que  $x \leq \epsilon_L(w)$ , o que implica que  $(w\epsilon_L(w)^{-1})x \leq (w\epsilon_L(w)^{-1})\epsilon_L(w) = w$ . Da minimalidade da transição  $w$  temos então que  $w = (w\epsilon_L(w)^{-1})x$  e portanto que  $x = (w\epsilon_L(w)^{-1})^{-1}w = \epsilon_L(w)$ . De maneira dual provamos que  $\epsilon_R(w)$  é a menor  $\mathcal{D}$ -entrada em sua classe de congruência.

Seja  $u$  uma transição congruente à transição  $w$ . Vamos provar que  $w\epsilon_L(w)^{-1} \leq u\epsilon_L(u)^{-1}$  e  $\epsilon_R(w)^{-1}w \leq \epsilon_R(u)^{-1}u$ . Primeiro provaremos que  $w\epsilon_L(w)^{-1} \leq u\epsilon_L(u)^{-1}$ . Dado que  $(w\epsilon_L(w)^{-1}, \epsilon_L(w), 1)$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$  devido à proposição 5.9, temos que  $\epsilon_L(w)$  é uma  $\mathcal{D}$ -entrada. De maneira análoga,  $\epsilon_L(u)$  é uma  $\mathcal{D}$ -entrada. Assim, temos que  $\epsilon_L(w)$  e  $\epsilon_L(u)$  são  $\mathcal{R}$ -entradas devido à proposição 5.5. Como  $\epsilon_L(w) \sim \epsilon_L(u)$  devido ao dual

do teorema 6.3, usando a proposição 6.9 temos pois que  $(u\epsilon_L(u)^{-1})\epsilon_L(w)$  é uma transição e que  $(u\epsilon_L(u)^{-1})\epsilon_L(w) \sim u \sim w$ . A partir da minimalidade da transição  $w$  em sua classe de congruência, temos  $(w\epsilon_L(w)^{-1})\epsilon_L(w) = w < (u\epsilon_L(u)^{-1})\epsilon_L(w)$  e portanto  $w\epsilon_L(w)^{-1} < u\epsilon_L(u)^{-1}$ . De maneira dual podemos provar que  $\epsilon_R(w)^{-1}w \leq \epsilon_R(u)^{-1}u$ . ■

Como adiantamos junto às definições, a função  $\tau$  faz o papel da inversa da função  $\sigma$ . Mais precisamente, dado um passeio  $p$  num grafo fundamental, a proposição 6.11 prova que  $\sigma(\tau(p)) = p$  e que  $\tau(p)$  é de fato a menor palavra com digital  $p$ . Também veremos uma caracterização da  $\mathcal{R}$ -entrada e da  $\mathcal{L}$ -entrada de  $\tau(p)$ , que como a maior parte destes resultados, é fruto de uma aplicação direta da proposição 5.12. Aquela proposição tem seu valor e utilidade mesmo no caso da seqüência de transições considerada não ser formada pelas menores transições em suas respectivas classes de congruência. Em particular, provar que uma palavra é a menor palavra em sua classe de congruência pode ser muito difícil, como veremos no estudo do exemplo a ser apresentado no capítulo 8.

Antes da proposição 6.11 propriamente dita, consideraremos um exemplo. Considere o exemplo 6.7. Seja dada a palavra  $w = babcbabac$  e seja  $p = (\widetilde{abcba}, \widetilde{cbac})$ . Já vimos na página 68 que  $w \mathcal{D}' abc$  e que o grafo fundamental de  $\widetilde{w}$  é aquele visto no exemplo 6.7. Também vimos que  $\sigma(w) = p$  e que  $\tau(p) = abcba((cba)^{-1}cbac) = abcbac$ . Note que  $c(\tau(p)) = A = c(abc)$  e que, portanto,  $\tau(p) \mathcal{D}' abc$ . A seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $\tau(p)$  é  $(1, abc, bac), (ab, cba, c), (abc, bac, 1)$ , a seqüência de ocorrências de transições de  $\tau(p)$  é  $(1, abcba, c), (ab, cbac, 1)$  e a seqüência de transições de  $\tau(p)$  é  $abcba, cbac$ . Assim temos que  $\sigma(\tau(p)) = (\widetilde{abcba}, \widetilde{cbac}) = p$ . Note também que  $w$  e  $\tau(p)$  têm a mesma digital  $p$  mas nem são congruentes. De fato, não estão nem na mesma  $\mathcal{R}'$ -classe devido ao teorema 6.3 pois  $\epsilon_R(\tau(p)) = \epsilon_R(abcbac) = abc$  e  $\epsilon_R(w) = \epsilon_R(babcbabac) = babc$  e  $babc \not\sim abc$ .

**Proposição 6.11** *Seja  $\mathbf{G}$  um grafo fundamental qualquer e seja  $p$  um passeio em  $\mathbf{G}$ . Então:*

1.  $\widetilde{\tau(p)}$  está na  $\mathcal{D}$ -classe da qual  $\mathbf{G}$  é o grafo fundamental;
2.  $\sigma(\tau(p)) = p$ ;
3.  $\epsilon_R(\tau(p)) = \tau(1_{\alpha(p)})$ ;
4.  $\epsilon_L(\tau(p)) = \tau(1_{\omega(p)})$ ;

5.  $\tau(pq) = \tau(p)(\epsilon_R(\tau(q))^{-1}\tau(q))$  para  $p, q \in \mathbf{G}^*$  passeios consecutivos;
6.  $\tau(p)$  é a menor palavra com digital  $p$ ;
7.  $|\tau(p)| = |\tau(1_{\alpha(p)})| + \sum_{i=1}^k |\epsilon_R(\tau(b_i))^{-1}\tau(b_i)|$  onde  $p = b_1b_2 \cdots b_k$  com  $k \geq 0$  e  $b_i \in \mathbf{G}$  para  $i = 1, \dots, k$ .

*Prova.* Seja  $\mathcal{K} = \mathbf{G}^*$  a categoria livre gerada por  $\mathbf{G}$ .

Afirmamos que se  $p = b_1b_2 \cdots b_k \in \mathcal{K}$  com  $k \geq 1$  e se  $w_i$  é a menor transição tal que  $b_i = \widetilde{w}_i \in \mathbf{G}$ , para  $i \in \{1, 2, \dots, k\}$ , então  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{1, 2, \dots, k-1\}$ . De fato, a proposição 6.10 implica que  $\epsilon_L(w_i)$  e  $\epsilon_R(w_{i+1})$  são as menores palavras em suas respectivas classes de congruência, que é a mesma classe pois  $\epsilon_L(w_i) = \omega(\widetilde{w}_i) = \omega(b_i) = \alpha(b_{i+1}) = \alpha(\widetilde{w}_{i+1}) = \epsilon_R(w_{i+1})$ .

Vamos provar os itens 1 e 2. Suponhamos primeiramente o caso em que  $|p| = 0$ . Seja  $v \in V(\mathbf{G})$  tal que  $p = 1_v$  e seja  $d$  a menor  $\mathcal{D}$ -entrada tal que  $\widetilde{d} = v$ . Assim temos, por definição, que  $\tau(p) = \tau(1_v) = d$ , e  $\widetilde{\tau(p)} = v \in V(\mathbf{G})$  está na  $\mathcal{D}$ -classe da qual  $\mathbf{G}$  é o grafo fundamental. Como  $d$  é uma  $\mathcal{D}$ -entrada,  $(1, d, 1)$  é a única ocorrência de  $\mathcal{D}$ -entrada de  $d$ . A seqüência de transições de  $d$  é então vazia e  $d = \epsilon_L(\epsilon_R(d))$  devido ao lema 5.11. Além do mais, temos que  $\sigma(d) = 1_{\widetilde{d}} = 1_v = p$ , o que prova que  $\sigma(\tau(p)) = \sigma(d) = p$ . Suponhamos agora que  $p = b_1b_2 \cdots b_k \in \mathcal{K}$  com  $k \geq 1$ . Seja  $w_i$  a menor transição tal que  $b_i = \widetilde{w}_i \in \mathbf{G}$ , para  $i \in \{1, 2, \dots, k\}$ . Assim  $\tau(p) = w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_k)^{-1}w_k)$ . Como afirmamos antes,  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{1, 2, \dots, k-1\}$ . Usando o item 1 da proposição 5.12 temos pois que  $\widetilde{\tau(p)} \mathcal{D} \widetilde{w}_1$  que por sua vez está na  $\mathcal{D}$ -classe da qual  $\mathbf{G}$  é o grafo fundamental. Usando o item 2 da mesma proposição temos que a seqüência de transições de  $\tau(p)$  é  $w_1, \dots, w_k$  e portanto  $\sigma(\tau(p)) = (\widetilde{w}_1, \dots, \widetilde{w}_k) = b_1 \cdots b_k = p$ .

Vamos provar os itens 3 e 4. Suponhamos primeiramente o caso em que  $|p| = 0$ . Seja  $v \in V(\mathbf{G})$  tal que  $p = 1_v$  e seja  $d$  a menor  $\mathcal{D}$ -entrada tal que  $\widetilde{d} = v$ . Assim temos, por definição, que  $\tau(p) = \tau(1_v) = d$ . Usando a proposição 5.5, temos que  $\epsilon_R(d) = d = \epsilon_L(d)$ . Como  $d = \tau(p) = \tau(1_v)$  e  $v = \alpha(p) = \omega(p)$ , temos então que  $\epsilon_R(\tau(p)) = \epsilon_R(d) = d = \tau(1_v) = \tau(1_{\alpha(p)})$  e que  $\epsilon_L(\tau(p)) = \epsilon_L(d) = d = \tau(1_v) = \tau(1_{\omega(p)})$ . Suponhamos agora que  $p = b_1b_2 \cdots b_k \in \mathcal{K}$  com  $k \geq 1$ . Seja  $w_i$  a menor transição tal que  $b_i = \widetilde{w}_i \in \mathbf{G}$ , para  $i \in \{1, 2, \dots, k\}$ . Assim  $\tau(p) = w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_k)^{-1}w_k)$ . Devido à proposição 6.10 temos que  $\epsilon_R(w_1)$  é a menor  $\mathcal{D}$ -entrada em sua classe de congruência. Isto em particular implica que  $\epsilon_R(w_1) = \tau(1_{\widetilde{\epsilon_R(w_1)}}) = \tau(1_{\alpha(\widetilde{w}_1)}) =$

$\tau(1_{\alpha(p)})$ . Como afirmamos antes,  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{1, 2, \dots, k-1\}$ . Usando o item 3 da proposição 5.12 temos que  $\epsilon_R(\tau(p)) = \epsilon_R(w_1) = \tau(1_{\alpha(p)})$ . De forma dual, provamos que  $\epsilon_L(\tau(p)) = \epsilon_L(w_k) = \tau(1_{\omega(p)})$ .

Vamos provar o item 5. Suponha primeiramente o caso em que  $|q| = 0$ . O item 3 implica que  $\epsilon_R(\tau(q)) = \tau(1_{\alpha(q)}) = \tau(q)$  e portanto que  $\tau(p)(\epsilon_R(\tau(q))^{-1}\tau(q)) = \tau(p)(\tau(q)^{-1}\tau(q)) = \tau(p) = \tau(pq)$ . Suponhamos agora o caso em que  $|p| = 0$ . O item 3 implica que  $\tau(p) = \tau(1_{\omega(p)}) = \tau(1_{\alpha(q)}) = \epsilon_R(\tau(q))$  e portanto que  $\tau(p)(\epsilon_R(\tau(q))^{-1}\tau(q)) = \epsilon_R(\tau(q))(\epsilon_R(\tau(q))^{-1}\tau(q)) = \tau(q) = \tau(pq)$ . Suponhamos agora o caso em que  $|p| \neq 0 \neq |q|$ . Seja  $pq = b_1b_2 \cdots b_k \in \mathcal{K}$  com  $k \geq 2$  e seja  $j$  um inteiro tal que  $p = b_1b_2 \cdots b_j$  e  $q = b_{j+1}b_{j+2} \cdots b_k$ . Assim, temos que  $w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_k)^{-1}w_k) = \tau(p)$  e portanto que  $\tau(pq) = w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_k)^{-1}w_k) = \tau(p)u$  onde  $u = (\epsilon_R(w_{j+1})^{-1}w_{j+1}) \cdots (\epsilon_R(w_k)^{-1}w_k)$ . Como afirmamos antes,  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{1, 2, \dots, k-1\}$ . Do item 3 da proposição 5.12, temos que  $\epsilon_R(w_{j+1}) = \epsilon_R(\tau(q))$ . Como  $u = (\epsilon_R(w_{j+1})^{-1}w_{j+1}) \cdots (\epsilon_R(w_k)^{-1}w_k) = \epsilon_R(w_{j+1})^{-1}\tau(q) = \epsilon_R(\tau(q))^{-1}\tau(q)$ , deduzimos portanto que  $\tau(pq) = \tau(p)u = \tau(p)(\epsilon_R(\tau(q))^{-1}\tau(q))$ , conforme queríamos demonstrar.

Vamos provar o item 6. Suponha primeiramente o caso em que  $|p| = 0$ . Seja  $v \in V(\mathbf{G})$  tal que  $p = 1_v$ . Suponha  $w$  uma palavra qualquer tal que  $\sigma(w) = 1_v$ . Assim a seqüência de transições de  $w$  é vazia e, devido ao lema 5.11, temos que  $w$  possui a única ocorrência de  $\mathcal{D}$ -entrada  $(x_0, y_0, z_0)$  e  $y_0 = \epsilon_L(\epsilon_R(w))$ . A partir da definição de  $\sigma$  temos que  $1_v = \sigma(w) = 1_{\tilde{y}_0}$  implicando pois que  $\tilde{y}_0 = v = \tau(1_v)$ . A partir da minimalidade de  $\tau(1_v)$  temos que  $\tau(p) = \tau(1_v) \leq y_0 \leq x_0y_0z_0 = w$ , provando pois que  $\tau(p)$  é a menor palavra que possui digital  $p$  neste caso. Suponhamos agora o caso em que  $|p| > 0$ . Seja  $p = b_1b_2 \cdots b_k \in \mathcal{K}$  com  $k \geq 1$ . Seja  $w$  uma palavra qualquer tal que  $\sigma(w) = p = b_1b_2 \cdots b_k$ . Da definição de  $\sigma$ , seja  $w_1, \dots, w_k$  a seqüência de transições de  $w$ . Assim temos que  $\tilde{w}_i = b_i$  para  $i \in \{1, 2, \dots, k\}$ . Sejam  $w_0 = \epsilon_R(w)$  e  $w_{k+1} = \epsilon_L(w)$ . A partir do lema 5.11 temos então que  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{0, \dots, k\}$ . Para  $i \in \{0, \dots, k\}$ , sejam definidas as palavras  $y_i = \epsilon_L(w_i) = \epsilon_R(w_{i+1})$  e  $x_i = (w_0y_0^{-1})(w_1y_1^{-1}) \cdots (w_iy_i^{-1})$  e  $z_i = (y_i^{-1}w_{i+1}) \cdots (y_{k-1}^{-1}w_k)(y_k^{-1}w_{k+1})$ . A partir do mesmo lema, a seqüência de ocorrências de transições de  $w$  é  $(x_0, w_1, z_1), \dots, (x_{k-1}, w_k, z_k)$  que por sua vez implica que  $w = x_0w_1z_1 = x_0w_1(y_1^{-1}w_2) \cdots (y_{k-1}^{-1}w_k)(y_k^{-1}w_{k+1}) = x_0w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_k)^{-1}w_k)z_k$ . Sejam  $w'_1, \dots, w'_k$  as menores transições tais que  $w'_i = \tilde{w}_i = b_i$  para qualquer inteiro  $i \in \{1, 2, \dots, k\}$ . Da minimalidade de cada  $w'_i$  em sua classe de congruência, temos que  $w'_1 \leq w_1$  e que



$\epsilon_R(w'_i)^{-1}w'_i \leq \epsilon_R(w_i)^{-1}w_i$  para  $i \in \{2, 3, \dots, k\}$  devido à proposição 6.10. Assim, segue de imediato que  $\tau(p) = w'_1(\epsilon_R(w'_2)^{-1}w'_2) \cdots (\epsilon_R(w'_k)^{-1}w'_k) \leq x_0w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_k)^{-1}w_k)z_k = w$ , provando pois que  $\tau(p)$  é a menor palavra que possui digital  $p$  também neste caso.

Vamos provar o item 7. Caso  $p$  seja o passeio vazio, temos então que  $p = 1_{\alpha(p)}$  e portanto  $|\tau(p)| = |\tau(1_{\alpha(p)})|$ . Suponhamos agora que  $p = b_1b_2 \cdots b_k \in \mathcal{K}$  com  $k \geq 1$ . Seja  $w_i$  a menor transição tal que  $b_i = \tilde{w}_i \in \mathbf{G}$ , para  $i \in \{1, 2, \dots, k\}$ . Assim  $\tau(p) = w_1(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_k)^{-1}w_k) = \epsilon_R(w_1)(\epsilon_R(w_1)^{-1}w_1)(\epsilon_R(w_2)^{-1}w_2) \cdots (\epsilon_R(w_k)^{-1}w_k)$ . Como afirmamos antes,  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{1, 2, \dots, k-1\}$ . Por um lado, a partir do item 3 da proposição 5.12 obtemos que  $\epsilon_R(w_1) = \epsilon_R(\tau(p)) = \tau(1_{\alpha(p)})$ . Por outro lado, temos que  $w_i = \tau(b_i)$  para qualquer inteiro  $i \in \{1, 2, \dots, k\}$ . Assim sendo, temos então que  $\tau(p) = \epsilon_R(w_1)(\epsilon_R(w_1)^{-1}w_1) \cdots (\epsilon_R(w_k)^{-1}w_k) = \tau(1_{\alpha(p)})(\epsilon_R(\tau(b_k))^{-1}\tau(b_k)) \cdots (\epsilon_R(\tau(b_1))^{-1}\tau(b_1))$  o que implica que  $|\tau(p)| = |\tau(1_{\alpha(p)})| + \sum_{i=1}^k |\epsilon_R(\tau(b_i))^{-1}\tau(b_i)|$ . ■

## 6.5 Regularidade no monóide de Burnside

Nesta seção veremos algumas propriedades relativas à regularidade de uma  $\mathcal{D}$ -classe de um monóide de Burnside livre. Na proposição 6.14 veremos que o grafo fundamental de uma  $\mathcal{D}$ -classe irregular não possui nenhuma aresta e possui um único vértice e na proposição 6.13 veremos que as  $\mathcal{H}$ -classes irregulares são triviais. Note porém que no caso  $n = 1$ , qualquer elemento do monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  é regular.

Primeiro, veremos um exemplo de uma  $\mathcal{D}$ -classe irregular. Como o monóide  $\mathcal{M}$  é regular quando  $n = 1$ , nosso exemplo deverá supôr  $n \geq 2$ . Para não pegar uma  $\mathcal{D}$ -classe sem nenhuma estrutura, como a  $\mathcal{D}$ -classe de uma letra, consideraremos uma  $\mathcal{D}$ -classe com  $m \times m$  elementos como a do exemplo 6.12. Relembramos que o “eggbox picture” de uma  $\mathcal{D}$ -classe é uma representação matricial da  $\mathcal{D}$ -classe onde em cada elemento da matriz temos uma  $\mathcal{H}$ -classe, em cada linha temos uma  $\mathcal{R}$ -classe e em cada coluna temos uma  $\mathcal{L}$ -classe.

**Exemplo 6.12** *Seja  $A = \{a, b\}$ , sejam inteiros  $n \geq 2$  e  $m \geq 1$  e seja  $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$ . Então a  $\mathcal{D}'$ -classe de  $a^n b^n$  é  $\{a^i b^j \mid i \geq n, j \geq n\}$ , ela não possui nenhuma transição*

$\widetilde{a^n b^n}$	$\widetilde{a^n b^n b}$	...	$\widetilde{a^n b^n b^{m-1}}$
$\widetilde{aa^n b^n}$	$\widetilde{aa^n b^n b}$	...	$\widetilde{aa^n b^n b^{m-1}}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\widetilde{a^{m-1} a^n b^n}$	$\widetilde{a^{m-1} a^n b^n b}$	...	$\widetilde{a^{m-1} a^n b^n b^{m-1}}$

Figura 6.3:  $\mathcal{D}$ -classe de  $\widetilde{a^n b^n}$ , com  $n \geq 2$ 

e sua única  $\mathcal{D}$ -entrada é  $a^n b^n$ . Ademais, a  $\mathcal{D}$ -classe de  $\widetilde{a^n b^n}$  é irregular, suas  $\mathcal{H}$ -classes são triviais e seu “eggbox picture” é aquele da figura 6.3.

*Prova.* Seja  $D = \{a^i b^j \mid i \geq n, j \geq n\}$ . É imediato provar que as funções  $\chi_{a^n}$ ,  $\chi_{b^n}$ ,  $\#_a$  e  $\#_b$  são funções preservadas por  $\sim$ .

Vamos mostrar que a  $\mathcal{D}'$ -classe de  $a^n b^n$  é  $D$ . Qualquer palavra em  $D$  tem  $a^n b^n$  por fator e é fator de  $a^{n+km} b^{n+km} \sim a^n b^n$  para  $k$  suficientemente grande. Isto prova que qualquer palavra de  $D$  está na mesma  $\mathcal{D}'$ -classe de  $a^n b^n$ . Temos também que  $D$  é saturado por  $\sim$ . De fato, se  $x \in D$  e  $(x, y)$  é uma substituição por  $(t^{n+m}, t^n)$  ou por  $(t^n, t^{n+m})$  para alguma palavra  $t$  então  $n \geq 2$  implica que  $t = a^k$  ou  $t = b^k$  para algum  $k \geq 1$  e portanto  $y \in D$ . Seja  $w$  uma palavra na  $\mathcal{D}'$ -classe de  $a^n b^n$ . Então existem palavras  $u, u'$  tais que  $uwu' \sim a^n b^n$ . Como  $a^n b^n \in D$  e  $D$  é saturado por  $\sim$  então  $uwu' \in D$  e  $w$  é um fator de uma palavra de  $D$ . Por outro lado existem  $v, v' \in A^*$  tais que  $va^n b^n v' \sim w$ . Como  $\chi_{a^n}(va^n b^n v') = 1 = \chi_{b^n}(va^n b^n v')$  e  $\chi_{a^n}$  e  $\chi_{b^n}$  são funções preservadas por  $\sim$  segue então que  $\chi_{a^n}(w) = 1 = \chi_{b^n}(w)$ . Como  $a^n$  e  $b^n$  são fatores de  $w$  que por sua vez é fator de uma palavra de  $D$ , segue então que  $w$  é da forma  $a^i b^j$  para algum  $i \geq n$  e algum  $j \geq n$ . Assim  $w \in D$ .

É evidente que a única palavra  $w$  cujo único fator que está em  $D$  é a própria  $w$  é a palavra  $w = a^n b^n$ . Assim, a única  $\mathcal{D}$ -entrada em  $D$  é  $a^n b^n$ . Da proposição 5.9, temos que qualquer transição em  $D$  tem seqüência de ocorrências de  $\mathcal{D}$ -entradas de comprimento 2. Não é o que ocorre com as palavras de  $D$  onde existe uma única ocorrência da  $\mathcal{D}$ -entrada  $a^n b^n$  como fator.

Como não há nenhuma palavra da forma  $a^i b^j a^i b^j$  com  $i \geq n$  e  $j \geq n$

em  $D$ , não existe palavra  $\sim$ -idempotente em  $D$  e portanto cada palavra na  $\mathcal{D}'$ -classe  $D$  é  $\sim$ -irregular.

Duas palavras  $w = a^i b^j$  e  $w' = a^{i'} b^{j'}$  de  $D$  são congruentes se e só se  $\#_a(w) = \#_a(w')$  e  $\#_b(w) = \#_b(w')$ . De fato, como  $\sim$  preserva  $\#_a$  e  $\#_b$ ,  $w \sim w'$  implica que  $\#_a(w) = \#_a(w')$  e  $\#_b(w) = \#_b(w')$ . Por outro lado,  $i, i' \geq n$  e se  $\#_a(w) = \#_a(w')$  então  $i \bmod m = i' \bmod m$ . Isto implica que  $a^i \sim a^{i'}$ . De maneira análoga, temos que  $\#_b(w) = \#_b(w')$  implica que  $b^j \sim b^{j'}$ . Assim  $\#_a(w) = \#_a(w')$  e  $\#_b(w) = \#_b(w')$  implicam que  $w = a^i b^j \sim a^{i'} b^{j'} = w'$ .

Usando a proposição 5.7, as  $\mathcal{R}$ -entradas de  $D$  são as palavras de  $D$  com sufixo  $a^n b^n$  e portanto são as palavras da forma  $a^i b^n$  para  $i \geq n$ . Duas tais  $\mathcal{R}$ -entradas  $a^i b^n$  e  $a^j b^n$  são congruentes se e só se  $\#_a(a^i b^n) = \#_a(a^j b^n)$  se e só se  $i = j \pmod{m}$ . Assim temos  $m$   $\mathcal{R}'$ -classes em  $D$  devido ao teorema 6.3. De maneira dual, as  $\mathcal{L}$ -entradas de  $D$  são as palavras da forma  $a^n b^j$  para  $j \geq n$  e duas tais  $\mathcal{L}$ -entradas  $a^n b^i$  e  $a^n b^j$  são congruentes se e só se  $i = j \pmod{m}$  e temos ao todo  $m$   $\mathcal{L}'$ -classes em  $D$ . Como duas palavras  $w = a^i b^j$  e  $w' = a^{i'} b^{j'}$  de  $D$  são congruentes se e só se  $\#_a(w) = \#_a(w')$  e  $\#_b(w) = \#_b(w')$ , temos ao todo  $m \times m$  classes de congruência possíveis. Como são  $m$  as  $\mathcal{R}'$ -classes e são  $m$  as  $\mathcal{L}'$ -classes, cada  $\mathcal{H}'$ -classe tem exatamente uma classe de congruência e as  $\mathcal{H}$ -classes da  $\mathcal{D}$ -classe de  $\widetilde{a^n b^n}$  são todas triviais. Assim temos o “eggbox picture” da figura 6.3. ■

Provaremos agora que algumas das propriedades vistas no exemplo 6.12 são gerais quando a  $\mathcal{D}$ -classe é irregular. Na proposição 6.13 veremos que as  $\mathcal{H}$ -classes irregulares são triviais. Observe que este resultado é conforme aquele já conhecido para  $n \geq 3$  e  $m \geq 1$ , como pode ser visto no corolário 8.15 [10].

**Proposição 6.13** *Sejam inteiros  $n \geq 1$  e  $m \geq 1$ . Então as  $\mathcal{H}$ -classes irregulares de um monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado pelo alfabeto  $A$  são todas triviais.*

*Prova.* Seja uma  $\mathcal{D}$ -classe irregular do monóide  $\mathcal{M}$ . Basta provar que uma  $\mathcal{H}$ -classe desta  $\mathcal{D}$ -classe é trivial, já que todas as demais têm a mesma cardinalidade. Seja  $u$  uma  $\mathcal{D}$ -entrada tal que  $\tilde{u}$  esteja nesta  $\mathcal{D}$ -classe. Basta provar que a existência de um segundo elemento na  $\mathcal{H}$ -classe de  $\tilde{u}$  implica que  $\tilde{u}$  é regular.

Suponha que exista uma palavra  $v$  tal que  $v \mathcal{H}' u$  e  $v \not\sim u$ . Como  $v \mathcal{L}' u$ , existem palavras  $x$  e  $y$  tais que  $xu \sim v$  e  $yv \sim u$ . Seja  $u_0 = u$  e seja

$u_{i+1} = \epsilon_R(yxu_i)$  para todo  $i \in \mathbb{N}$ .

Vamos provar que  $u_i \sim u \sim (yx)^i u$  e que  $u_i \in \text{Pref}((yx)^i u)$ . Faremos uma indução em  $i$ . No caso  $i = 0$  temos que  $u_0 = u = (yx)^0 u$ . Suponha que  $i \geq 0$ , que  $u_i \sim u \sim (yx)^i u$  e que  $u_i \in \text{Pref}((yx)^i u)$ . Observe que  $(yx)^{i+1} u = yx((yx)^i u) \sim yxu \sim u$  implica que  $u_{i+1} = \epsilon_R((yx)^{i+1} u) \sim \epsilon_R(u) = u$  devido ao teorema 6.3 e à proposição 5.5. Como  $u_i \in \text{Pref}((yx)^i u)$ , temos que  $u_{i+1} = \epsilon_R(yxu_i) \in \text{Pref}(yxu_i) \subseteq \text{Pref}(yx(yx)^i u) = \text{Pref}((yx)^{i+1} u)$ .

Seja  $z_i = u_i^{-1}((yx)^i u)$  para todo  $i \in \mathbb{N}$ . Vamos provar que  $|z_{i+1}| > |z_i|$  para todo  $i \in \mathbb{N}$ . Fixemos  $i \in \mathbb{N}$ . Observe que  $xu_i \sim xu \sim v \mathcal{R}' u$  implica que  $\epsilon_R(xu_i) \sim \epsilon_R(u) = u$  devido ao teorema 6.3 e à proposição 5.5. Assim  $\epsilon_R(xu_i) \sim u \not\sim v \sim xu \sim xu_i$  implica que  $\epsilon_R(xu_i) \neq xu_i$  e portanto que  $|\epsilon_R(xu_i)| < |xu_i|$ . Dado que  $\epsilon_R(xu_i) \mathcal{R}' xu_i$  implica que  $y\epsilon_R(xu_i) \mathcal{R}' yxu_i$ , temos que  $|u_{i+1}| = |\epsilon_R(yxu_i)| \leq |y\epsilon_R(xu_i)| = |y| + |\epsilon_R(xu_i)| < |y| + |xu_i| = |yxu_i|$ . Assim  $|z_{i+1}| = |u_{i+1}^{-1}((yx)^{i+1} u)| = |(yx)^{i+1} u| - |u_{i+1}| > |(yx)^{i+1} u| - |yxu_i| = |(yx)^i u| - |u_i| = |u_i^{-1}((yx)^i u)| = |z_i|$ .

Vamos provar que  $\tilde{u}$  é regular. Seja  $k = |u|$ . Dado que  $|z_k| > |z_{k-1}| > \dots > |z_1| > |z_0|$  e  $z_0 = u_0^{-1} u = 1$ , temos pois que  $|z_k| \geq k = |u|$ . Assim  $u_k \in \text{Pref}((yx)^k)$  pois  $u_k, (yx)^k \in \text{Pref}((yx)^k u)$  e  $|u_k| = |(yx)^k u| - |z_k| \leq |(yx)^k u| - |u| = |(yx)^k|$ . Podemos pois definir  $u' = u_k^{-1} (yx)^k$ . Por fim, temos que  $u \sim (yx)^k u = u_k (u_k^{-1} (yx)^k) u \sim u u' u$  implica que  $\tilde{u} = \tilde{u} \tilde{u}' \tilde{u}$ , e  $\tilde{u}$  é regular por definição. ■

No corolário 6.15 veremos que uma palavra de uma  $\mathcal{D}'$ -classe  $\sim$ -irregular possui uma única ocorrência de  $\mathcal{D}$ -entrada como fator e que todas as  $\mathcal{D}$ -entradas de uma tal  $\mathcal{D}'$ -classe são congruentes. Observe que este resultado é conforme aquele já conhecido para  $n \geq 3$  e  $m \geq 1$ , como pode ser visto no corolário 8.14 [10]. Este resultado pode ser melhor sintetizado na proposição 6.14 onde provamos que o grafo fundamental de uma  $\mathcal{D}$ -classe irregular não possui nenhuma aresta e possui um único vértice. Este grafo é fortemente conexo.

**Proposição 6.14** *O grafo fundamental de uma  $\mathcal{D}$ -classe irregular de um monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por um alfabeto  $A$ , com  $n \geq 1$  e  $m \geq 1$ , não possui nenhuma aresta e possui um único vértice.*

*Prova.* Seja  $D$  uma  $\mathcal{D}$ -classe de  $\mathcal{M} \setminus \{\tilde{1}\}$  e seja  $\mathbf{G}$  o grafo fundamental de  $D$ .

Suponha que exista uma aresta  $b \in \mathbf{G}$ . Vamos mostrar que  $D$  é uma  $\mathcal{D}$ -classe regular. Seja  $w$  a menor transição tal que  $\tilde{w} = b$ . Usando

a proposição 6.10, seja  $u = \epsilon_R(w)$  a menor  $\mathcal{D}$ -entrada em sua classe de congruência e seja  $k = |u|$ . Observe que  $\tilde{u} = \alpha(b) \in V(\mathbf{G}) \subseteq D$ . Como  $\mathbf{G}$  é fortemente conexo devido à proposição 6.8, podemos escolher um passeio  $q$  em  $\mathbf{G}$  de  $\omega(b)$  a  $\alpha(b) = \tilde{u}$ . Assim,  $bq$  é um passeio fechado de  $\tilde{u}$  a  $\tilde{u}$ , bem como o passeio  $p = (bq)^k$ . Como  $\tau(1_{\alpha(p)}) = \tau(1_{\omega(p)}) = \tau(1_{\tilde{u}}) = u$ , usando os itens 3 e 4 da proposição 6.11 temos que  $\epsilon_R(\tau(p)) = \epsilon_L(\tau(p)) = u$  e  $\tau(p) \mathcal{H}' u$ . Usando o item 7 da mesma proposição, temos que  $|\tau(p)| \geq |\tau(1_{\alpha(p)})| + k|\epsilon_R(\tau(b))^{-1}\tau(b)| = |u| + k|\epsilon_R(w)^{-1}w| \geq |u| + k = |\epsilon_R(\tau(p))| + |\epsilon_L(\tau(p))|$  pois  $|\epsilon_R(w)^{-1}w| \geq 1$  é uma consequência do corolário 5.10. Assim podemos definir  $u' = \epsilon_R(\tau(p))^{-1}\tau(p)\epsilon_L(\tau(p))^{-1} = u^{-1}\tau(p)u^{-1}$  e temos que  $\tilde{u} \mathcal{H} \tau(p) = \widetilde{u'u} = \tilde{u}\tilde{u}'\tilde{u}$ . Caso  $D$  fosse irregular, teríamos que suas  $\mathcal{H}$ -classes seriam triviais devido à proposição 6.13, implicando pois que  $\tilde{u} = \tilde{u}'\tilde{u}$  e portanto que  $\tilde{u}$ , e portanto  $D$ , seria regular. Assim  $D$  é uma  $\mathcal{D}$ -classe regular.

Como o grafo  $\mathbf{G}$  é fortemente conexo devido à proposição 6.8,  $\mathbf{G}$  possui um vértice ao menos. Como também não possui arestas caso  $D$  seja irregular, não pode possuir mais que um vértice neste caso. ■

**Corolário 6.15** *Toda transição é  $\sim$ -regular, toda palavra  $\sim$ -irregular tem uma única ocorrência de  $\mathcal{D}$ -entrada e quaisquer  $\mathcal{D}$ -entradas na mesma  $\mathcal{D}'$ -classe  $\sim$ -irregular são congruentes.*

Na proposição 6.16 caracterizamos as  $\mathcal{R}$ -entradas regulares (e por dualidade as  $\mathcal{L}$ -entradas regulares) em termos das transições.

**Proposição 6.16** *Seja  $w$  uma palavra  $\sim$ -regular. Então  $w$  é uma  $\mathcal{R}$ -entrada se e só se  $w$  for sufixo próprio não vazio de uma transição em sua  $\mathcal{D}'$ -classe.*

*Prova.* Seja  $t$  uma transição na  $\mathcal{D}'$ -classe de  $w$  e suponha que  $w$  seja sufixo próprio não vazio de  $t$ . Sejam  $a, b \in A$  e  $u \in A^*$  tais que  $t = aub$ . Assim  $ub \mathcal{P}' u$  e portanto  $ub \mathcal{R}' u$  implicando pois que  $ub$  é uma  $\mathcal{R}$ -entrada. Como  $w$  é sufixo próprio de  $t$  temos que  $|w| < |t| = |aub| = 1 + |ub|$  e  $|w| \leq |ub|$ . Como  $w, ub \in \text{Suf}(t)$ , temos que  $w$  é um sufixo não vazio de  $ub$ . Usando a proposição 5.6, temos que  $w$  é uma  $\mathcal{R}$ -entrada.

Suponha que  $w$  seja uma  $\mathcal{R}$ -entrada. Assim  $w$  é uma palavra não vazia. Como  $w$  é  $\sim$ -regular, seja  $x \in A^*$  tal que  $w \sim wxw$ . Da proposição 5.7 temos que  $\epsilon_L(w)$  é uma  $\mathcal{D}$ -entrada de  $w$  e seja  $y = w\epsilon_L(w)^{-1}$ . Assim  $(y, \epsilon_L(w), xw)$  e  $(wx, y, w)$  são duas ocorrências de  $\mathcal{D}$ -entradas de

$wxw$ . Seja pois  $(r, s, v)$  a penúltima ocorrência de  $\mathcal{D}$ -entrada de  $wxw$ . Como  $(wxy, \epsilon_L(w), 1)$  é com certeza a última, usando o corolário 5.10, temos que  $(r, sv, 1)$  é uma ocorrência de transição de  $wxw$ . Note que  $sv$  não é sufixo de  $w$   $\mathcal{D}'$   $sv$  pois neste caso teríamos duas ocorrências de  $\mathcal{D}$ -entradas de  $sv$  devido à proposição 5.9, e estas seriam duas ocorrências de  $\mathcal{D}$ -entradas de  $w$ , contradizendo com a proposição 5.7. Como  $rsv = wxw$ , temos então que  $|w| < |sv|$  e  $w$  é um sufixo próprio da transição  $sv$ . ■

# Capítulo 7

## Os Grupos Maximais

Neste capítulo provaremos dois dos resultados mais importantes deste trabalho: o teorema da caracterização (teorema 7.5) e o teorema dos grupos maximais (teorema 7.6). O primeiro será demonstrado na seção 7.2 e usará o fortemente combinatório lema 7.3 que será visto na seção 7.1. Também fará uso do lema 5.14 visto no capítulo 5. Na demonstração do teorema da caracterização, usaremos vários conceitos vistos no trabalho. Explicitando alguns: o grafo fundamental de uma  $\mathcal{D}$ -classe, o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por este grafo e um sistema de adequações coerente. Já na seção 7.3 veremos o teorema dos grupos maximais, que não somente usa o teorema da caracterização em sua demonstração, mas também usa o teorema 4.7 visto no capítulo 4.

Neste capítulo suporemos um alfabeto  $A$  bem como inteiros  $n \geq 1$  e  $m \geq 1$ . Sejam  $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$  (que é estável como vimos antes), a congruência de Burnside  $\sim$  e a projeção canônica  $\tilde{\cdot} : A^* \rightarrow \mathcal{M}$ . Sejam também definidas as relações Green-induzidas.

### 7.1 O lema da substituição

A inofensiva proposição 7.1 merece algumas considerações. Quando  $n \geq 3$  e  $m \geq 1$ , o semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  é bem conhecido devido a outro trabalho deste autor [10]. Em particular, o teorema 8.12 [10] mostra que as  $\mathcal{D}$ -entradas de  $\mathcal{D}$ -classes regulares que são as menores palavras em suas classes de congruência correspondem a curtos de

produções de  $\Sigma$ . Neste contexto, a proposição 7.1 que se segue é muito semelhante à proposição 4.10 [10].

**Proposição 7.1** *Seja  $w$  uma  $\mathcal{D}$ -entrada, seja  $v \in A^*$  e seja  $x \in \text{Suf}(w) \cap \text{Pref}(v^{n+m})$ . Então temos que  $|x| \leq |v^n|$ .*

*Prova.* Suponha por absurdo que  $|x| > |v^n|$ . Seja  $u = (wx^{-1})$  e seja  $w' = uv^n$ . Como  $v^n, x \in \text{Pref}(v^{n+m})$ , temos que  $w = ux$  e  $w' = uv^n$  são prefixos de  $uv^{n+m}$ . Como  $|w'| = |uv^n| = |u| + |v^n| < |u| + |x| = |ux| = |w|$ . Assim temos que  $w'$  é um prefixo próprio de  $w$ . Como  $uv^n \in \text{Pref}(ux) \subseteq \text{Pref}(uv^{n+m}) \sim uv^n$ , temos que  $w' = uv^n \mathcal{R}' ux = w$ . Assim temos uma contradição com o fato de que  $w'$  é prefixo próprio de  $w$  e com o fato de que  $\epsilon_R(w) = w$  devido à proposição 5.5. ■

Como foi feito no capítulo 6, onde o exemplo 6.7 serviu de base à ilustração de vários conceitos ao longo daquele capítulo, teremos um exemplo que será o ponto de partida para a ilustração dos resultados a serem vistos neste capítulo. Agora, precisaremos de um exemplo em que  $m > 1$  e consideraremos um conjunto gerador de duas letras, para simplificar nossos cálculos. O exemplo a ser considerado é o da  $\mathcal{D}$ -classe de  $\tilde{ab}$  no monóide de Burnside livre satisfazendo  $x = x^3$  gerado por  $\{a, b\}$  a ser visto no exemplo 7.2. A prova de que o grafo fundamental da  $\mathcal{D}$ -classe de  $\tilde{ab}$  é o grafo apresentado na figura 7.1 poderia ser feita mais facilmente que no caso do exemplo 6.7 a partir das proposições 6.1 e 6.2 e dos corolários 6.5 e 7.4. Não provaremos agora já que o teorema 9.2 dará uma prova mais geral. Ademais, os resultados propriamente ditos não dependem dele.

**Exemplo 7.2** *Seja  $A = \{a, b\}$ , sejam  $n = 1$  e  $m = 2$  e seja  $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$ . Então o grafo fundamental da  $\mathcal{D}$ -classe de  $\tilde{ab}$  é o grafo definido na figura 7.1.*

O lema da substituição (lema 7.3) é bastante combinatório e extenso. Supondo que  $(w', w)$  seja uma substituição por  $(v^{n+m}, v^n)$ , o lema 7.3 implica que  $\sigma(w') = \sigma(w)$  se  $v^n \mathcal{D}' w$  e que  $(\sigma(w'), \sigma(w))$  é uma substituição por  $(x^m, 1_u)$  para algum passeio  $x$  no grafo fundamental de  $\tilde{w}$ , com início e término num mesmo vértice  $u$ , se  $v^n \mathcal{D}' w$ . Antes porém, consideraremos uma verificação destes fatos para palavras na  $\mathcal{D}'$ -classe tratada no exemplo 7.2.

Considere o exemplo 7.2. Seja dada a palavra  $w = abbaaab$ . Como  $c(w) = c(ab)$  temos pois que  $w \mathcal{D}' ab$  devido ao item 1 da proposição 6.1 e o grafo fundamental de  $\tilde{w}$  é aquele visto no exemplo 7.2. Assim,



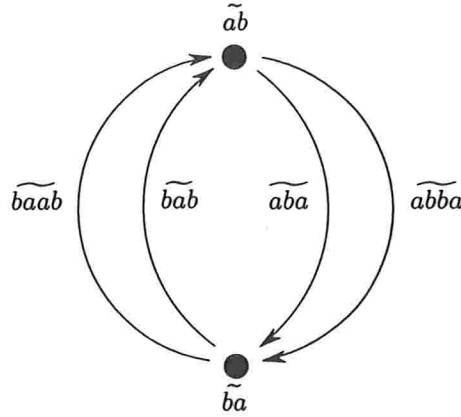


Figura 7.1: Grafo fundamental da  $\mathcal{D}$ -classe de  $\widetilde{ab}$  no monóide de Burnside livre satisfazendo  $x = x^3$  gerado por  $\{a, b\}$

$(1, ab, baaab), (ab, ba, aab), (abbaa, ab, 1)$  é a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$  implicando pois que a seqüência de transições de  $w$  é  $w_1, w_2 = abba, baaab$  devido ao lema 5.11. Assim  $\sigma(w) = (\widetilde{abba}, \widetilde{baaab}) = (\widetilde{abba}, \widetilde{bab})$ . Seja a palavra  $w' = abbaabaabaaab$ . Sua seqüência de ocorrências de  $\mathcal{D}$ -entradas é  $(1, ab, baabaabaaab), (ab, ba, abaabaaab), (abba, ab, aabaaab), (abbaa, ba, abaaab), (abbaaba, ab, aab), (abbaabaa, ba, aab), (abbaabaabaa, ab, 1)$  e usando o lema 5.11 temos que sua seqüência de transições é  $w'_1, w'_2, w'_3, w'_4, w'_5, w'_6 = abba, baab, aba, baab, aba, baaab$ . Como  $\widetilde{baaab} = \widetilde{bab}$ , obtemos então  $\sigma(w') = (\widetilde{abba}, \widetilde{baab}, \widetilde{aba}, \widetilde{baab}, \widetilde{aba}, \widetilde{bab})$ . Observe que  $(w, w')$  é uma substituição por  $(baa, (baa)^3)$ , que  $baa \mathcal{D}' w$  e que  $w'_1 = w_1, w'_6 = w_2$  e  $w'_4, w'_5 = w'_2, w'_3$ , de acordo com o item 2 do lema 7.3. Ademais,  $(\sigma(w'), \sigma(w))$  é uma substituição por  $((\widetilde{baab}, \widetilde{aba})^2, 1_{\widetilde{ba}})$ . Seja  $w'' = abbab$ . Sua seqüência de ocorrências de  $\mathcal{D}$ -entradas é  $(1, ab, bab), (ab, ba, b), (abba, ab, 1)$  e sua seqüência de transições é  $abba, bab$ . Assim  $\sigma(w'') = (\widetilde{abba}, \widetilde{bab})$ . Observe que  $(w'', w)$  é uma substituição por  $(a, a^3)$ , que  $a \mathcal{P}' w$ , que as seqüências de transições têm mesmo comprimento e suas transições são, sequencialmente, duas a duas congruentes, como no item 1 do lema 7.3. Ademais,  $\sigma(w) = (\widetilde{abba}, \widetilde{bab}) = \sigma(w'')$ .

**Lema 7.3 (lema da substituição)** *Sejam  $w, w', v \in A^+$  e  $s, t \in A^*$  tais que  $w = sv^nt$  e  $w' = sv^{n+m}t$ . Seja  $w_1, w_2, \dots, w_k$  a seqüência de transições de  $w$  e seja  $w'_1, w'_2, \dots, w'_k$  a seqüência de transições de  $w'$ .*

1. Se  $v^n \mathcal{D}' w$  então:

- (a)  $k' = k$ ;
- (b)  $w'_i \sim w_i$ , para  $i = 1, \dots, k$ .

2. Se  $v^n \mathcal{D}' w$  então existem  $l > 0$  e  $0 \leq j \leq k$  tais que:

- (a)  $k' = k + ml$ ;
- (b)  $w'_i = w_i$ , para  $i = 1, \dots, j$ ;
- (c)  $w'_{j+i} = w'_{j+i+l} = \dots = w'_{j+i+(m-1)l}$ , para  $i = 1, \dots, l$ ;
- (d)  $w'_i = w_{i-ml}$ , para  $i = j + ml + 1, \dots, k'$ .

*Prova.* Sejam  $w_0 = \epsilon_R(w)$  e  $w_{k+1} = \epsilon_L(w)$ . A partir do lema 5.11 temos então que  $\epsilon_L(w_i) = \epsilon_R(w_{i+1})$  para  $i \in \{0, \dots, k\}$ . Para  $i \in \{0, \dots, k\}$ , sejam as palavras  $y_i = \epsilon_L(w_i) = \epsilon_R(w_{i+1})$  e  $x_i = (w_0 y_0^{-1})(w_1 y_1^{-1}) \dots (w_i y_i^{-1})$  e  $z_i = (y_i^{-1} w_{i+1}) \dots (y_{k-1}^{-1} w_k)(y_k^{-1} w_{k+1})$ . A partir do mesmo lema, a seqüência de ocorrências de transições de  $w$  é  $(x_0, w_1, z_1), \dots, (x_{k-1}, w_k, z_k)$  e a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$  é  $(x_0, y_0, z_0), \dots, (x_k, y_k, z_k)$ . Sejam  $w'_0 = \epsilon_R(w')$  e  $w'_{k'+1} = \epsilon_L(w')$ . A partir do lema 5.11 temos então que  $\epsilon_L(w'_i) = \epsilon_R(w'_{i+1})$  para  $i \in \{0, \dots, k'\}$ . Para  $i \in \{0, \dots, k'\}$ , sejam definidas as palavras  $y'_i = \epsilon_L(w'_i) = \epsilon_R(w'_{i+1})$  e  $x'_i = (w'_0 y'_0{}^{-1})(w'_1 y'_1{}^{-1}) \dots (w'_i y'_i{}^{-1})$  e  $z'_i = (y'_i{}^{-1} w'_{i+1}) \dots (y'_{k'-1}{}^{-1} w'_{k'}) (y'_{k'}{}^{-1} w'_{k'+1})$ . A partir do mesmo lema, a seqüência de ocorrências de transições de  $w'$  é  $(x'_0, w'_1, z'_1), \dots, (x'_{k'-1}, w'_{k'}, z'_{k'})$  e a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w'$  é  $(x'_0, y'_0, z'_0), \dots, (x'_{k'}, y'_{k'}, z'_{k'})$ .

Ao conjunto das ocorrências de  $\mathcal{D}$ -entradas de  $w$  chamaremos de  $F$  e ao conjunto das ocorrências de  $\mathcal{D}$ -entradas de  $w'$  chamaremos de  $F'$ . Relembramos que estes conjuntos são incomparáveis segundo a ordem das fatorações  $\leq$  — definida por  $(x, y, z) \leq (x', y', z')$  se e só se  $|x| \geq |x'|$  e  $|z| \geq |z'|$  — e que são totalmente ordenados pela ordem das ocorrências — definida por  $(x, y, z) \prec (x', y', z')$  se e só se  $|x| < |x'|$  (ou equivalentemente por  $(x, y, z) \prec (x', y', z')$  se e só se  $|z| < |z'|$ ). Os conjuntos  $F$  e  $F'$  são totalmente ordenados por  $\prec$  e esta será a ordem natural a ser considerada nos mesmos. Dizemos que uma função  $\varphi : F \rightarrow F'$  preserva a ordem se dados  $f, g \in F$  tais que  $f \prec g$  então temos que  $\varphi(f) \prec \varphi(g)$ . Ademais, para  $C, D \subseteq F$  (ou  $C, D \subseteq F'$ ) dizemos que  $C \prec D$  se toda fatoração em  $C$  for menor que qualquer fatoração em  $D$ .

Seja  $f = (x, y, z) \in F$ . Como  $w = xyz = sv^nt$ , temos que existem quatro casos possíveis a serem analisados:

1.  $|x| < |s|$  e  $|z| \geq |t|$ ;
2.  $|x| < |s|$  e  $|z| < |t|$ ;
3.  $|x| \geq |s|$  e  $|z| \geq |t|$ ;
4.  $|x| \geq |s|$  e  $|z| < |t|$ .

Estes quatro casos definem um particionamento das fatorações de  $F$  em  $F_1$ ,  $F_2$ ,  $F_3$  e  $F_4$  conforme as fatorações se enquadrem nos casos 1, 2, 3 ou 4, respectivamente. Como  $w' = sv^{n+m}t$ , uma fatoração  $f' = (x, y, z) \in F'$  pode enquadrar-se nos mesmos quatro casos e da mesma forma definimos as partições de  $F'$ :  $F'_1$ ,  $F'_2$ ,  $F'_3$  e  $F'_4$ . Das definições, segue de imediato que  $F_1 \prec F_2 \cup F_3 \prec F_4$  e que  $F'_1 \prec F'_2 \cup F'_3 \prec F'_4$ .

Vamos provar que  $v^n \mathcal{D}' w \iff v^{n+m} \mathcal{D}' w' \iff F_3 \neq \emptyset \iff F'_3 \neq \emptyset \implies F_2 = \emptyset = F'_2$ . Como  $v^n \sim v^{n+m}$  e  $w \sim w'$ , temos de imediato que  $v^n \mathcal{D}' w \iff v^{n+m} \mathcal{D}' w'$ . Vamos primeiro provar que  $v^n \mathcal{D}' w \iff F_3 \neq \emptyset \implies F_2 = \emptyset$ . Suponha que  $v^n \mathcal{D}' w$ . Seja  $(x, y, z)$  uma ocorrência de  $\mathcal{D}$ -entrada de  $v^n$ . Como  $v^n \mathcal{D}' w = sv^nt$ , temos que  $(sx, y, zt)$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$ . Como  $(sx, y, zt) \in F_3$ , temos que  $F_3 \neq \emptyset$ . Suponha agora que  $F_3 \neq \emptyset$  e seja  $(x, y, z) \in F_3$ . Da própria definição de  $F_3$ , temos que  $(x, y, z) \leq (s, v^n, t)$  e que  $y \in \text{Fat}(v^n) \subseteq \text{Fat}(w)$ . Como qualquer fator de  $w$  que tenha por fator uma  $\mathcal{D}$ -entrada de  $w$  está na  $\mathcal{D}'$ -classe de  $w$ , segue de imediato que  $v^n \mathcal{D}' w$ . Caso exista  $f \in F_2$ , das próprias definições de  $F_3$  e  $F_2$ , temos que  $(x, y, z) \leq (s, v^n, t) < f$ , o que é uma contradição com a minimalidade da ocorrência de  $\mathcal{D}$ -entrada  $f$ . De maneira análoga podemos provar que  $v^{n+m} \mathcal{D}' w' \iff F'_3 \neq \emptyset \implies F'_2 = \emptyset$ .

Construiremos uma função  $\varphi : F \longrightarrow F'$  que preserve a ordem e é injetiva. A mesma será definida por partes e terá o seguinte comportamento em cada  $F_i$ :

1.  $\varphi$  estabelece uma bijeção de  $F_i$  em  $F'_i$ , para  $i = 1, 2, 4$ ;
2.  $\varphi$  estabelece uma injeção de  $F_3$  em  $F'_3$ , e para todo  $(x', y', z') \in F'_3$  temos que  $(x', y', z') \in \varphi(F_3) \iff |z'| \geq |v^m t|$ .

Observemos primeiramente que o fato de que  $\varphi$  (ou qualquer restrição sua a um domínio menor) preserve a ordem já implica que  $\varphi$  é injetiva. De fato, se  $\varphi$  preserve a ordem, dadas  $f$  e  $f'$  duas fatorações distintas em

$F$ , temos que  $f \prec f'$  ou  $f' \prec f$  já que  $\prec$  é uma ordem total em  $F$ . Assim,  $\varphi(f) \prec \varphi(f')$  ou  $\varphi(f') \prec \varphi(f)$ , respectivamente. Em qualquer caso,  $\varphi(f) \neq \varphi(f')$  e  $\varphi$  é injetiva.

Vamos definir  $\varphi|_{F_1}$ . Seja  $f = (x, y, z) \in F_1$ . Assim  $xyz = sv^nt$  e  $|x| < |s|$  e  $|z| \geq |t|$ . Definimos  $\varphi(f) = f' = (x', y', z') = (x, y, (zt^{-1})v^mt)$ . Como  $x'y'z' = xy(zt^{-1})v^mt = ((xyz)t^{-1})v^mt = ((sv^nt)t^{-1})v^mt = sv^nv^mt = w'$ , temos que  $f'$  é uma fatoração de  $w'$ . Como  $(x, y, z)$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$ , temos que  $y' = y$  é uma  $\mathcal{D}$ -entrada e que  $y' = y \mathcal{D} w \sim w'$ . Assim  $f' = (x', y', z')$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ . Como  $|x'| = |x| < |s|$ , como  $|z'| = |z| + |v^m| \geq |t| + |v^m| \geq |t|$ , temos que  $f' \in F'_1$ . Assim  $\varphi|_{F_1}$  é bem definida e temos que  $\varphi|_{F_1} : F_1 \rightarrow F'_1$ .

Vamos provar que  $\varphi|_{F_1}$  é uma bijeção de  $F_1$  em  $F'_1$  e que preserva a ordem. De fato, dadas duas fatorações  $(x, y, z)$  e  $(x', y', z')$  em  $F_1$ , temos que  $(x, y, z) \prec (x', y', z') \iff |x| < |x'| \iff (x, y, (zt^{-1})v^mt) \prec (x', y', (z't^{-1})v^mt) \iff \varphi|_{F_1}((x, y, z)) \prec \varphi|_{F_1}((x', y', z'))$ , o que prova que  $\varphi|_{F_1}$  preserva a ordem. Isto implica que  $\varphi|_{F_1}$  é injetiva conforme visto antes. Falta-nos provar que  $\varphi(F_1) = F'_1$ . Para tanto tomemos  $f' = (x', y', z') \in F'_1$  uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ . Assim  $x'y'z' = sv^{n+m}t$  e  $|x'| < |s|$  e  $|z'| \geq |t|$ . Primeiro mostraremos que  $|z'| \geq |v^{n+m}t|$ . Caso  $|z'| \geq |v^{n+m}t|$  nem há o que provar. Considere o caso em que  $|z'| < |v^{n+m}t|$ . Daí,  $z'$  é sufixo de  $v^{n+m}t$  já que  $x'y'z' = sv^{n+m}t$ . Seja pois  $u = (v^{n+m}t)z'^{-1}$ . Como  $f'$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ , temos que  $y'$  é uma  $\mathcal{D}$ -entrada. Como  $su = s(v^{n+m}t)z'^{-1} = (sv^{n+m}t)z'^{-1} = w'z'^{-1} = (x'y'z')z'^{-1} = x'y'$  e  $|x'| < |s|$  temos que  $u \in \text{Suf}(y')$ . Como  $uz' = v^{n+m}t$  e  $|z'| \geq |t|$ , temos que  $u \in \text{Pref}(v^{n+m})$ . Pela proposição 7.1 temos que  $|u| \leq |v^n|$ , donde  $uz' = v^{n+m}t$  implica que  $|z'| \geq |v^mt|$ . Vide a figura 7.2. Assim podemos

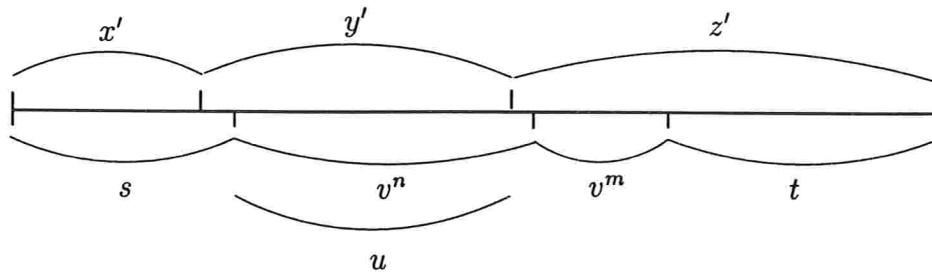


Figura 7.2: Fatoração  $f'$  em  $F'_1$

definir  $f = (x, y, z) = (x', y', z'(v^m t)^{-1}t)$ . Como  $xyz = x'y'(z'(v^m t)^{-1}t) = (x'y'z')(v^m t)^{-1}t = w'(v^m t)^{-1}t = (sv^n v^m t)(v^m t)^{-1}t = sv^n t = w$ , temos que  $f$  é uma fatoração de  $w$ . Como  $f'$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ , temos que  $y = y'$  é uma  $\mathcal{D}$ -entrada e  $y = y' \mathcal{D}' w' \sim w$ . Assim  $f$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$ . Como  $|x| = |x'| < |s|$ , como  $|z| = |z'| - |v^m| \geq |v^m t| - |v^m| = |t|$ , temos que  $f \in F_1$ . É fácil verificar que  $\varphi(f) = f'$ . Daí concluímos que  $\varphi(F_1) = F'_1$ .

Vamos definir  $\varphi|_{F_4}$ . Seja  $f = (x, y, z) \in F_4$ . Assim  $xyz = sv^n t$  e  $|x| \geq |s|$  e  $|z| < |t|$ . Definimos  $\varphi(f) = f' = (x', y', z') = (sv^m(s^{-1}x), y, z)$ . Como  $x'y'z' = sv^m(s^{-1}x)yz = sv^m(s^{-1}(xyz)) = sv^m(s^{-1}(sv^n t)) = sv^m v^n t = w'$ , temos que  $f'$  é uma fatoração de  $w'$ . Como  $(x, y, z)$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$ , temos que  $y' = y$  é uma  $\mathcal{D}$ -entrada e que  $y' = y \mathcal{D}' w \sim w'$ . Assim  $f' = (x', y', z')$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ . Como  $|x'| = |x| + |v^m| \geq |s| + |v^m| \geq |s|$ , como  $|z'| = |z| < |t|$ , temos que  $f' \in F'_4$ . Assim  $\varphi|_{F_4}$  é bem definida e temos que  $\varphi|_{F_4} : F_4 \rightarrow F'_4$ .

Vamos provar que  $\varphi|_{F_4}$  é uma bijeção de  $F_4$  em  $F'_4$  e que preserva a ordem. Dadas duas fatorações  $(x, y, z)$  e  $(x', y', z')$  em  $F_4$ , temos que  $(x, y, z) \prec (x', y', z') \iff |x| < |x'| \iff |x| + |v^m| < |x'| + |v^m| \iff |sv^m(s^{-1}x)| < |sv^m(s^{-1}x')| \iff (sv^m(s^{-1}x), y, z) \prec (sv^m(s^{-1}x'), y, z) \iff \varphi|_{F_4}((x, y, z)) \prec \varphi|_{F_4}((x', y', z'))$ , o que prova que  $\varphi|_{F_4}$  preserva a ordem. Isto implica que  $\varphi|_{F_4}$  é injetiva conforme visto antes. De forma perfeitamente dual à prova de  $\varphi(F_1) = F'_1$  vista na prova de que  $\varphi|_{F_1}$  é uma bijeção, podemos provar que  $\varphi(F_4) = F'_4$ .

Vamos definir  $\varphi|_{F_2}$  e mostrar que  $\varphi|_{F_2}$  preserva a ordem e é uma bijeção de  $F_2$  em  $F'_2$ . Adiantamos que  $\varphi|_{F_2}$  será definida por  $\varphi|_{F_2}((x, y, z)) = (x, (y(tz^{-1})^{-1})v^m(tz^{-1}), z)$ . Primeiramente, fixemos  $x$  um prefixo próprio de  $s$  e  $z$  um sufixo próprio de  $t$ . Definiremos algumas palavras e fatorações em função de  $x$  e  $z$ . Definamos  $y = (x^{-1}s)v^n(tz^{-1})$ ,  $x' = x$ ,  $z' = z$  e  $y' = (x^{-1}s)v^{n+m}(tz^{-1})$ . Definamos  $f = (x, y, z)$  e  $f' = (x', y', z')$ . Assim temos que  $f$  é uma fatoração de  $w$  pois  $xyz = x(x^{-1}s)v^n(tz^{-1})z = sv^n t = w$  e  $f'$  é uma fatoração de  $w'$  pois  $x'y'z' = x(x^{-1}s)v^{n+m}(tz^{-1})z = sv^{n+m}t = w'$ . Vamos primeiro provar que  $f$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$  se e só se  $f'$  for uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ . Seja  $a$  a primeira letra de  $(x^{-1}s)$ , e portanto de  $y$  e de  $y'$ . Seja  $b$  a última letra de  $(tz^{-1})$ , e portanto de  $y$  e de  $y'$ . Ora,  $y = (x^{-1}s)v^n(tz^{-1}) \sim (x^{-1}s)v^{n+m}(tz^{-1}) = y'$ . Ademais temos que  $yb^{-1} = ((x^{-1}s)v^n(tz^{-1}))b^{-1} = (x^{-1}s)v^n((tz^{-1})b^{-1}) \sim (x^{-1}s)v^{n+m}((tz^{-1})b^{-1}) = ((x^{-1}s)v^{n+m}(tz^{-1}))b^{-1} = y'b^{-1}$ . De forma dual podemos provar que  $a^{-1}y \sim a^{-1}y'$ . Assim temos que  $y \mathcal{R}' yb^{-1} \iff y' \mathcal{R}' y'b^{-1}$

e que  $y \mathcal{L}' a^{-1}y \iff y' \mathcal{L}' a^{-1}y'$ . Portanto,  $y = \epsilon_R(y) \iff y \mathcal{R}' yb^{-1} \iff y' \mathcal{R}' y'b^{-1} \iff y' = \epsilon_R(y')$  e  $y = \epsilon_L(y) \iff y \mathcal{L}' a^{-1}y \iff a^{-1}y' \mathcal{L}' a^{-1}y' \iff y' = \epsilon_L(y')$ . Usando a proposição 5.5, segue de imediato que  $y$  é uma  $\mathcal{D}$ -entrada se e só se  $y'$  for uma  $\mathcal{D}$ -entrada. Como  $y \mathcal{D}' w \iff y' \mathcal{D}' w'$ , temos que  $f$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$  se e só se  $f'$  for uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ , concluindo a primeira parte da demonstração. Como para toda ocorrência de  $\mathcal{D}$ -entrada em  $F_2$  existem  $x$  e  $z$  tais que a ocorrência de  $\mathcal{D}$ -entrada em questão seja  $f$ , sendo que neste caso a fatoração  $f'$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$  com  $f' \in F'_2$ , definimos  $\varphi(f) = f'$ . De fato, esta definição coincide com a definição que já havíamos adiantado pois  $(y(tz^{-1})^{-1})v^m(tz^{-1}) = ((x^{-1}s)v^n(tz^{-1})(tz^{-1})^{-1})v^m(tz^{-1}) = (x^{-1}s)v^n v^m(tz^{-1}) = y'$ . Dadas duas fatorações  $(x_i, y_i, z_i)$  e  $(x_j, y_j, z_j)$  em  $F_2$ ,  $(x_i, y_i, z_i) \prec (x_j, y_j, z_j) \iff |x_i| < |x_j| \iff (x_i, (y_i(tz_i^{-1})^{-1})v^m(tz_i^{-1}), z_i) \prec (x_j, (y_j(tz_j^{-1})^{-1})v^m(tz_j^{-1}), z_j) \iff \varphi|_{F_2}((x_i, y_i, z_i)) \prec \varphi|_{F_2}((x_j, y_j, z_j))$ , o que prova que  $\varphi|_{F_2}$  preserva a ordem. Isto implica que  $\varphi|_{F_2}$  é injetiva conforme visto antes. Também verificamos que  $\varphi(F_2) = F'_2$  pois para toda ocorrência de  $\mathcal{D}$ -entrada em  $F'_2$  existem  $x$  e  $z$  tais que a ocorrência de  $\mathcal{D}$ -entrada em questão seja  $f'$ , sendo que neste caso  $f$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$  com  $f \in F_2$  e  $f' = \varphi(f)$ .

Vamos definir  $\varphi|_{F_3}$ . Seja  $f = (x, y, z) \in F_3$ . Assim  $xyz = sv^nt$  e  $|x| \geq |s|$  e  $|z| \geq |t|$ . Definimos  $\varphi(f) = f' = (x', y', z') = (x, y, (zt^{-1})v^mt)$ . Como  $x'y'z' = xy(zt^{-1})v^mt = ((xyz)t^{-1})v^mt = ((sv^nt)t^{-1})v^mt = sv^nv^mt = w'$ , temos que  $f'$  é uma fatoração de  $w'$ . Como  $(x, y, z)$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$ , temos que  $y' = y$  é uma  $\mathcal{D}$ -entrada e que  $y' = y \mathcal{D}' w \sim w'$ . Assim  $f' = (x', y', z')$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ . Como  $|x'| = |x| \geq |s|$ , como  $|z'| = |z| + |v^m| \geq |t| + |v^m| \geq |t|$ , temos que  $f' \in F'_3$ . Assim  $\varphi|_{F_3}$  é bem definida e temos que  $\varphi|_{F_3} : F_3 \rightarrow F'_3$ .

Vamos provar que  $\varphi|_{F_3}$  é uma injeção de  $F_3$  em  $F'_3$ , que preserva a ordem e que se  $(x', y', z') \in F'_3$  então  $(x', y', z') \in \varphi(F_3) \iff |z'| \geq |v^mt|$ . Dadas duas fatorações  $(x, y, z)$  e  $(x', y', z')$  em  $F_3$ , temos que  $(x, y, z) \prec (x', y', z') \iff |x| < |x'| \iff (x, y, (zt^{-1})v^mt) \prec (x', y', (z't^{-1})v^mt) \iff \varphi|_{F_3}((x, y, z)) \prec \varphi|_{F_3}((x', y', z'))$ , o que prova que  $\varphi|_{F_3}$  preserva a ordem. Isto implica que  $\varphi|_{F_3}$  é injetiva conforme visto antes. Falta-nos provar que se  $(x', y', z') \in F'_3$  então  $(x', y', z') \in \varphi(F_3) \iff |z'| \geq |v^mt|$ . Seja  $f' = (x', y', z') \in F'_3$  uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ . Suponha que  $f' \in \varphi(F_3)$  e seja  $f = (x, y, z) \in F_3$  tal que  $\varphi(f) = f'$ . Da definição de  $\varphi$  temos que  $|z'| = |(zt^{-1})v^mt| = |z| + |v^m| \geq |t| + |v^m| = |v^mt|$ . Suponha agora que  $|z'| \geq |v^mt|$ . Assim podemos definir  $x = x'$ ,  $y = y'$ ,  $z = (z'(v^mt)^{-1})t$  e  $f =$

$(x, y, z)$ . Como  $xyz = x'y'(z'(v^m t)^{-1})t = (x'y'z')(v^m t)^{-1}t = w'(v^m t)^{-1}t = (sv^n v^m t)(v^m t)^{-1}t = sv^n t = w$ , temos que  $f$  é uma fatoração de  $w$ . Como  $f'$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ , temos que  $y = y'$  é uma  $\mathcal{D}$ -entrada e  $y = y' \mathcal{D}' w' \sim w$ . Assim  $f$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w$ . Como  $|x| = |x'| \geq |s|$ , como  $|z| = |z'| - |v^m| \geq |v^m t| - |v^m| = |t|$ , temos que  $f \in F_3$ . É fácil verificar que  $\varphi(f) = f'$  e portanto que  $f' \in \varphi(F_3)$ .

Em suma, definimos:

$$\varphi((x, y, z)) = \begin{cases} (x, y, (zt^{-1})v^m t), & \text{se } (x, y, z) \in F_1 + F_3; \\ (x, (y(tz^{-1})^{-1})v^m(tz^{-1}), z), & \text{se } (x, y, z) \in F_2; \\ (sv^m(s^{-1}x), y, z), & \text{se } (x, y, z) \in F_4. \end{cases}$$

Suponha que  $v^n \mathcal{D}' w$ . Vamos concluir a demonstração para este caso (item 1 do enunciado) provando que  $k = k'$  e que  $w_i \sim w'_i$  para  $i = 1, \dots, k$ . Como já vimos anteriormente, neste caso, temos que  $F_3 = F'_3 = \emptyset$ . Já vimos também que  $F_1 \prec F_2 \prec F_4$  e que  $F'_1 \prec F'_2 \prec F'_4$ . Como  $\varphi|_{F_i}$  preserva a ordem e estabelece bijeção de  $F_i$  em  $F'_i$ , para  $i = 1, 2, 4$ , temos que  $\varphi$  estabelece bijeção de  $F$  em  $F'$  e preserva a ordem. Assim,  $k = k'$  e temos o subitem 1a. Seja  $f_i = (x_i, y_i, z_i)$  e  $f'_i = (x'_i, y'_i, z'_i)$  para  $i = 0, 1, \dots, k$ . Como  $\varphi$  preserva a ordem, como as seqüências de ocorrências de  $\mathcal{D}$ -entradas de  $w$  e de  $w'$  são ordenadas por ocorrência, temos que  $\varphi(f_i) = f'_i$  para  $i = 0, 1, \dots, k$ . Fixemos  $i \in \{1, \dots, k\}$ . Para provar que  $w_i = x_{i-1}^{-1} w z_i^{-1} \sim x'_{i-1}^{-1} w' z'_i^{-1} = w'_i$  analisaremos a que partições pertencem  $f_{i-1}$  e  $f_i$ . Temos três casos a analisar:

1.  $f_{i-1}, f_i \in F_1$ . Neste caso temos que  $x'_{i-1} = x_{i-1}$  e que  $z'_i = (z_i t^{-1})v^m t$ . Assim temos que  $w'_i = x'_{i-1}^{-1} w' z'_i^{-1} = x_{i-1}^{-1} (sv^n v^m t)((z_i t^{-1})v^m t)^{-1} = x_{i-1}^{-1} (sv^n)(z_i t^{-1})^{-1} = x_{i-1}^{-1} (sv^n t) z_i^{-1} = x_{i-1}^{-1} w z_i^{-1} = w_i$ .
2.  $f_{i-1} \in F_1 \cup F_2$  e  $f_i \in F_2 \cup F_4$ . Neste caso temos que  $x'_{i-1} = x_{i-1}$  e  $|x_{i-1}| < |s|$ . Também temos que  $z'_i = z_i$  e  $|z_i| < |t|$ . Assim temos que  $w'_i = x'_{i-1}^{-1} w' z'_i^{-1} = x_{i-1}^{-1} (sv^{n+m} t) z_i^{-1} = (x_{i-1}^{-1} s) v^{n+m} (t z_i^{-1}) \sim (x_{i-1}^{-1} s) v^n (t z_i^{-1}) = x_{i-1}^{-1} (sv^n t) z_i^{-1} = x_{i-1}^{-1} w z_i^{-1} = w_i$ .
3.  $f_{i-1}, f_i \in F_4$ . Neste caso temos que  $x'_{i-1} = sv^m(s^{-1}x_{i-1})$  e que  $z'_i = z_i$ . Assim temos  $w'_i = x'_{i-1}^{-1} w' z'_i^{-1} = (sv^m(s^{-1}x_{i-1}))^{-1} (sv^m v^n t) z_i^{-1} = (s^{-1}x_{i-1})^{-1} (v^n t) z_i^{-1} = x_{i-1}^{-1} (sv^n t) z_i^{-1} = x_{i-1}^{-1} w z_i^{-1} = w_i$ .

Em suma, provamos o subitem 1b pois nos casos 1 e 3 vimos que  $w'_i = w_i$ , e no item 2 vimos que  $w'_i \sim w_i$ .

Suporemos a partir de agora que  $v^n \mathcal{D}' w$ . Isto implica, como já vimos, que  $F_3 \neq \emptyset \neq F'_3$  e  $F_2 = \emptyset = F'_2$ . Seja  $f_i = (x_i, y_i, z_i)$  para  $i = 0, 1, \dots, k$  e seja  $f'_i = (x'_i, y'_i, z'_i)$  para  $i = 0, 1, \dots, k'$ . Já vimos que  $f'_i \in \varphi(F_3) \implies |z'_i| \geq |v^m t|$  e que  $f'_i \in F'_3 \setminus \varphi(F_3) \implies |t| \leq |z'_i| < |v^m t|$ . Isto em particular implica que  $\varphi(F_3) \prec F'_3 \setminus \varphi(F_3)$ . Vamos particionar  $F'_3 \setminus \varphi(F_3)$  em  $\{G_{m-1}, \dots, G_0\}$  onde

$$f'_i \in G_h \iff |v^h t| \leq |z'_i| < |v^{h+1} t|$$

para  $h = 0, 1, \dots, m-1$ , para cada  $f'_i \in F'_3 \setminus \varphi(F_3)$ . Assim  $\varphi(F_3) \prec G_{m-1} \prec \dots \prec G_0$ . Seja  $H_0 = \{f'_i \in F'_3 \mid |s| \leq |x'_i| < |sv|\}$ .

Vamos definir uma função  $\theta : F'_3 \setminus G_0 \longrightarrow F'_3 \setminus H_0$  por

$$\theta((x, y, z)) = (sv(s^{-1}x), y, z(vt)^{-1}t).$$

Suponhamos que  $f = (x, y, z) \in F'_3 \setminus G_0$ . Assim temos que  $xyz = sv^{n+m}t$ , que  $|x| \geq |s|$ , que  $|z| \geq |vt|$  e podemos de fato definir  $\theta(f) = f' = (x', y', z') = (sv(s^{-1}x), y, z(vt)^{-1}t)$ . Por conseguinte, podemos verificar que  $f'$  é uma fatoração de  $w'$  já que  $x'y'z' = sv(s^{-1}x)yz(vt)^{-1}t = sv(s^{-1}(xyz)(vt)^{-1})t = sv(s^{-1}(sv^{n+m}t)(vt)^{-1})t = sv(v^{n+m-1})t = sv^{n+m}t = w'$ . Como  $f$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ , temos que  $y' = y$  é uma  $\mathcal{D}$ -entrada e que  $y' = y \mathcal{D}' w'$ . Assim  $f'$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ . Como  $|z'| = |z| - |v| \geq |vt| - |v| = |t|$ , como  $|x'| = |x| + |v| \geq |sv|$ , temos que  $f' \in F'_3 \setminus H_0$ . Assim  $\theta$  é bem definida e temos que  $\theta : F'_3 \setminus G_0 \longrightarrow F'_3 \setminus H_0$ .

Vamos mostrar que  $\theta : F'_3 \setminus G_0 \longrightarrow F'_3 \setminus H_0$  é uma bijeção que preserva a ordem e que  $\theta^{-1}((x, y, z)) = (s(sv)^{-1}x, y, (zt^{-1})vt)$ . Vamos primeiro provar que  $\theta$  preserva a ordem. De fato, dadas duas fatorações  $(x, y, z)$  e  $(x', y', z')$  em  $F'_3 \setminus G_0$ , temos que  $(x, y, z) \prec (x', y', z') \iff |x| < |x'| \iff |x| + |v| < |x'| + |v| \iff |sv(s^{-1}x)| < |sv(s^{-1}x')| \iff (sv(s^{-1}x), y, z(vt)^{-1}t) \prec (sv(s^{-1}x'), y', z'(vt)^{-1}t) \iff \theta((x, y, z)) \prec \theta((x', y', z'))$ , o que prova que  $\theta$  preserva a ordem. Isto implica que  $\theta$  é injetiva conforme visto antes. Falta-nos calcular  $\theta^{-1}$  e provar que  $\theta(F'_3 \setminus G_0) = F'_3 \setminus H_0$ . Para tanto tomemos  $f' = (x', y', z') \in F'_3 \setminus H_0$ . Assim temos que  $|x'| \geq |sv|$  e  $|z'| \geq |t|$ . Definamos  $f = (x, y, z) = (s(sv)^{-1}x', y', (z't^{-1})vt)$ . Temos que  $f$  é uma fatoração de  $w'$  pois  $s(sv)^{-1}x'y'(z't^{-1})vt = s((sv)^{-1}(x'y'z')t^{-1})vt = s((sv)^{-1}(sv^{n+m}t)t^{-1})vt = s(v^{n+m-1})vt = sv^{n+m}t = w'$ . Como  $f'$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ , temos que  $y = y'$  é uma  $\mathcal{D}$ -entrada e  $y = y' \mathcal{D}' w'$ . Assim  $f$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $w'$ . Como  $|x| = |x'| - |v| \geq |sv| - |v| = |s|$ , como  $|z| = |z'| + |v| \geq |t| + |v| = |vt|$ , temos que  $f \in F'_3 \setminus G_0$ . É fácil verificar



que  $\theta(f) = f'$  e que portanto  $\theta^{-1}((x', y', z')) = (s(sv)^{-1}x', y', (z't^{-1})vt)$ . Daí concluímos que  $\theta(F'_3 \setminus G_0) = F'_3 \setminus H_0$ .

Por ora, seja  $h \in \{0, \dots, m-2\}$ . Vamos mostrar que  $\theta|_{G_{h+1}} : G_{h+1} \rightarrow G_h$  é uma bijeção. Naturalmente,  $G_{h+1}, G_h \subseteq F'_3 \setminus \varphi(F_3) \subseteq F'_3$ . Como  $h+1 > 0$ , de fato  $G_{h+1} \subseteq F'_3 \setminus G_0$ . Suponha  $f = (x, y, z) \in G_{h+1}$ . Por definição, temos que  $|v^{h+1}t| \leq |z| < |v^{h+2}t|$ . Como  $\theta((x, y, z)) = (sv(s^{-1}x), y, z(vt)^{-1}t)$  e  $|z(vt)^{-1}t| = |z| - |vt| + |t| = |z| - |v|$ , temos que  $|v^h t| \leq |z(vt)^{-1}t| < |v^{h+1}t|$  o que implica que  $\theta(f) \in G_h$ . Isto prova que  $\theta(G_{h+1}) \subseteq G_h$ . Suponha  $f' = (x', y', z')$  qualquer fatoração em  $G_h$ . Por definição, temos que  $|v^h t| \leq |z'| < |v^{h+1}t|$ . Antes de prosseguir, provaremos que  $G_h \subseteq F'_3 \setminus H_0$ . Suponha por absurdo que  $f' \in H_0$ . Neste caso temos que  $|s| \leq |x'| < |sv|$ . Como  $(sv, v^{n+m-h-2}, v^{h+1}t)$  é uma fatoração de  $w'$  e  $|z'| < |v^{h+1}t|$  e  $|x'| < |sv|$ , temos que  $v^{n+m-h-2}$  é fator próprio de  $y'$ . Portanto  $v^n$  é fator próprio de  $y'$  pois  $h \leq m-2$  implica que  $v^n \in \text{Fat}(v^{n+m-h-2})$ . Isto é uma contradição com o fato de que  $y'$  é  $\mathcal{D}$ -entrada de  $w'$  e  $v^n \mathcal{D}' w' \sim w'$ . Assim,  $G_h \subseteq F'_3 \setminus H_0$ . Como  $\theta^{-1}((x', y', z')) = (s(sv)^{-1}x', y', (z't^{-1})vt)$  e  $|(z't^{-1})vt| = |z'| - |t| + |vt| = |z'| + |v|$ , temos que  $|v^{h+1}t| \leq |(z't^{-1})vt| < |v^{h+2}t|$  o que implica que  $\theta^{-1}(f') \in G_{h+1}$ . Isto prova que  $\theta(G_{h+1}) \supseteq G_h$ . Assim  $\theta(G_{h+1}) = G_h$ . Como  $\theta$  é bijeção, segue que  $\theta|_{G_{h+1}} : G_{h+1} \rightarrow G_h$  também o é.

Vamos definir  $l$  e  $j$  tais que  $\varphi(f_i) = f'_i$  se  $0 \leq i \leq j$  e  $\varphi(f_i) = f'_{i+ml}$  se  $j+1 \leq i \leq k$ . Já vimos que  $F$  pode ser particionado em  $\{F_1, F_3, F_4\}$  com  $F_1 \prec F_3 \prec F_4$ . Já vimos que  $F'$  pode ser particionado em  $\{F'_1, \varphi(F_3), F'_3 \setminus \varphi(F_3), F'_4\}$  com  $F'_1 \prec \varphi(F_3) \prec F'_3 \setminus \varphi(F_3) \prec F'_4$ . Como  $\varphi$  estabelece bijeções que preservam a ordem de  $F_1$  em  $F'_1$ , de  $F_3$  em  $\varphi(F_3)$  e de  $F_4$  em  $F'_4$ , temos que  $\varphi$  preserva a ordem em  $F$ . Ademais,  $|F'_1 + \varphi(F_3)| = |F_1 + F_3|$  e  $|F'_4| = |F_4|$ . Como  $F_3 \neq \emptyset$ , seja  $j = |F_1 + F_3| - 1$  tal que  $f_j$  seja a maior fatoração em  $F_3$ , segundo  $\prec$ . Então se  $0 \leq i \leq j$ , temos que  $f_i \in F_1 + F_3$ , e que  $\varphi(f_i) = f'_i \in F'_1 \cup \varphi(F_3)$ . Como  $\theta$  estabelece bijeção de  $G_{h+1}$  em  $G_h$  para  $h \in \{0, \dots, m-2\}$ , seja  $l$  a única cardinalidade de cada  $G_h$ , para  $h \in \{0, \dots, m-1\}$ . Assim a cardinalidade  $F'_3 \setminus \varphi(F_3)$  é  $ml$ . Assim, se  $j+1 \leq i \leq k$ , temos que  $f_i \in F_4$  e que  $\varphi(f_i) = f'_{i+ml} \in F'_4$ .

Em particular, temos que  $f'_k = \varphi(f_k) = f'_{k+ml}$ , o que implica que  $k' = k + ml$ .

Observe que  $G_h = \{f'_i \mid j + (m-1-h)l + 1 \leq i \leq j + (m-h)l\}$  pois  $F'_3 \setminus \varphi(F_3)$  pode ser particionado em  $\{G_{m-1}, \dots, G_0\}$  e  $G_{m-1} \prec \dots \prec G_0$ . Como  $\theta$  preserva a ordem e estabelece bijeção entre  $G_{h+1}$  e  $G_h$  para  $h \in \{0, \dots, m-2\}$ , temos que  $\theta(f'_i) = f'_{i+l}$  para  $j < i \leq j + (m-1)l$ .

Vamos mostrar que  $l > 0$  e que  $\theta(f'_i) = f'_{i+l}$  também para  $i = j$ . Como  $f'_j = \varphi(f_j) \in \varphi(F_3) \subseteq F'_3 \setminus G_0$ , temos que  $\theta(f'_j)$  é definido e seja  $j'$  tal que  $f'_{j'} = \theta(f'_j) = (sv(s^{-1}x'_j), y'_j, z'_j(vt)^{-1}t)$ . Assim segue que  $|x'_{j'}| = |sv(s^{-1}x'_j)| = |x'_j| + |v|$  e que  $f'_j \prec f'_{j'}$ . Vamos primeiro mostrar que  $f'_{j'} \in G_{m-1}$ . Temos que  $|z'_{j'}| = |z'_j(vt)^{-1}t| = |z'_j| - |v|$ . Como  $f'_j \in \varphi(F_3)$ , temos que  $|z'_j| \geq |v^m t|$  e portanto que  $|z'_{j'}| = |z'_j| - |v| \geq |v^m t| - |v| = |v^{m-1}t|$ . Suponha por absurdo que  $f'_{j'} \in \varphi(F_3)$ . Neste caso, já que  $\varphi$  preserva a ordem, temos que  $f_j = \varphi^{-1}(f'_j) \prec \varphi^{-1}(f'_{j'}) \in \varphi^{-1}(\varphi(F_3)) = F_3$ , contradizendo com a escolha de  $j$ . Assim,  $f'_{j'} \notin \varphi(F_3)$ . Como  $f'_{j'} \in F'_3 \setminus \varphi(F_3)$ , temos que  $|z'_{j'}| < |v^m t|$ . Como  $|v^{m-1}t| \leq |z'_{j'}| < |v^m t|$ , temos que  $f'_{j'} \in G_{m-1}$  conforme queríamos demonstrar. Donde,  $l = |G_{m-1}| > 0$ . Falta-nos provar que  $\theta(f'_j) = f'_{j+l}$ . Vamos primeiro provar que  $f'_{j'}$  é o maior elemento de  $G_{m-1}$  segundo a ordem  $\prec$ . Suponha por absurdo que exista  $p'$  tal que  $f'_{p'} \in G_{m-1}$  e  $f'_{j'} \prec f'_{p'}$ . Assim  $|v^{m-1}t| \leq |z'_{p'}| < |v^m t|$ . Como  $f'_{j'} = \theta(f'_j) \in F'_3 \setminus H_0$ , temos que  $|x_{p'}| > |x_{j'}| \geq |sv|$  e  $f'_{p'} \in F'_3 \setminus H_0$ . Assim,  $\theta^{-1}(f'_{p'})$  é definida e seja  $p$  tal que  $f'_p = \theta^{-1}(f'_{p'}) = (s(sv)^{-1}x'_{p'}, y'_{p'}, (z'_{p'}t^{-1})vt) \in F'_3 \setminus G_0 \subseteq F'_3$ . Assim  $|z'_p| = |(z'_{p'}t^{-1})vt| = |z'_{p'}| + |v| \geq |v^{m-1}t| + |v| = |v^m t|$ . Donde,  $f'_p \in \varphi(F_3)$  e  $f_p \in F_3$ . Como  $\theta$  preserva a ordem e  $f'_{j'} \prec f'_{p'}$ , temos que  $f'_j = \theta^{-1}(f'_{j'}) \prec \theta^{-1}(f'_{p'}) = f'_p$ . Como  $\varphi$  preserva a ordem, temos que  $f_j = \varphi^{-1}(f'_j) \prec \varphi^{-1}(f'_p) = f_p \in F_3$ , o que é uma contradição com a escolha de  $j$ . Assim não existe tal  $p'$  e  $f'_{j'}$  é o maior elemento de  $G_{m-1}$  conforme desejávamos provar. Como este maior elemento é justamente  $f'_{j+l}$ , temos finalmente que  $\theta(f'_j) = f'_{j+l}$ .

Vamos provar que  $x'_{j+ml} = sv^m(s^{-1}x_j)$ . De fato,  $f'_{j+ml} = \theta^m(f'_j) = (sv^m(s^{-1}x'_j), y'_j, z'_j(v^m t)^{-1}t)$ . Como  $f'_j = \varphi(f_j)$ , temos que  $x'_j = x_j$ . Assim  $x'_{j+ml} = sv^m(s^{-1}x_j)$ .

Vamos concluir a demonstração para o caso  $v^n \mathcal{D}' w$  (item 2 do enunciado). Já escolhemos os inteiros  $l$  e  $j$  conforme desejado. Já provamos que  $k' = k + ml$ , implicando o subitem 2a. Suponha que  $1 \leq i \leq j$ . Assim  $f_{i-1}, f_i \in F_1 + F_3$ . Como  $f'_{i-1} = \varphi(f_{i-1})$  e  $f'_i = \varphi(f_i)$ , a partir da definição de  $\varphi$  segue  $x'_{i-1} = x_{i-1}$  e  $z'_i = (z_i t^{-1})v^m t$ . Assim  $w'_i = x'_{i-1}{}^{-1} w' z'_i{}^{-1} = x_{i-1}{}^{-1} (sv^n v^m t) ((z_i t^{-1})v^m t)^{-1} = x_{i-1}{}^{-1} (sv^n) (z_i t^{-1})^{-1} = x_{i-1}{}^{-1} (sv^n t) z_i{}^{-1} = x_{i-1}{}^{-1} w z_i{}^{-1} = w_i$ . Isto prova o subitem 2b. Suponha agora que  $j+1 \leq i \leq j+(m-1)l$ . Assim  $f'_i \in (F'_3 \setminus \varphi(F_3)) \setminus G_0$ . Neste caso temos que  $f'_{i+l} = \theta(f'_i)$  e que  $f'_{i+l-1} = \theta(f'_{i-1})$ . Da definição de  $\theta$  temos que  $x'_{i+l-1} = sv(s^{-1}x'_{i-1})$  e que  $z'_{i+l} = z'_i(vt)^{-1}t$ . Assim temos  $w'_{i+l} = x'_{i+l-1}{}^{-1} w' z'_{i+l}{}^{-1} = (sv(s^{-1}x'_{i-1}))^{-1} (sv^{n+m}t) (z'_i(vt)^{-1}t)^{-1} = (s^{-1}x'_{i-1})^{-1} (v^{n+m-1}) (z'_i(vt)^{-1})^{-1} = x'_{i-1}{}^{-1} (sv^{n+m-1}vt) z'_i{}^{-1} = x'_{i-1}{}^{-1} w' z'_i{}^{-1} = w'_i$ . Isto prova o subitem 2c. Supo-

nha por fim que  $j + ml + 1 \leq i \leq k + ml$ . Neste caso temos que  $f_{i-ml} \in F_4$ . Como  $f'_i = \varphi(f_{i-ml})$ , a partir da definição de  $\varphi$  segue que  $z'_i = z_{i-ml}$ . Caso  $j + ml + 1 < i$ , temos que  $f_{i-ml-1} \in F_4$ , que  $f'_{i-1} = \varphi(f_{i-ml-1})$  e da definição de  $\varphi$  segue que  $x'_{i-1} = sv^m(s^{-1}x_{i-ml-1})$ . Caso  $j + ml + 1 = i$ , como  $x'_{j+ml} = sv^m(s^{-1}x_j)$  também segue  $x'_{i-1} = sv^m(s^{-1}x_{i-ml-1})$ . De toda forma temos que  $x'_{i-1}{}^{-1}w' = (sv^m(s^{-1}x_{i-ml-1}))^{-1}(sv^mv^nt) = (s^{-1}x_{i-ml-1})^{-1}(v^nt) = x_{i-ml-1}{}^{-1}(sv^nt) = x_{i-ml-1}{}^{-1}w$  e portanto que  $w'_i = x'_{i-1}{}^{-1}w'z'_i{}^{-1} = x_{i-ml-1}{}^{-1}wz_{i-ml}{}^{-1} = w_{i-ml}$ . Isto prova o subitem 2d e conclui nossa demonstração. ■

No corolário 7.4 vemos uma aplicação do lema 7.3 que nos leva à caracterização das transições congruentes.

**Corolário 7.4** *Duas transições  $aub$  e  $a'u'b'$ , com  $a, a', b, b' \in A$  e  $u, u' \in A^*$ , são congruentes se e só se  $a = a'$  e  $b = b'$  e  $u \sim u'$ . Ademais, a menor transição numa classe de congruência é também a menor palavra nesta classe.*

*Prova.* Seja  $\delta$  uma função que aplica uma palavra  $w \in A^+$  no conjunto  $\{(a, \tilde{u}, b) \mid a, b \in A \text{ e } u \in A^* \text{ e } aub \text{ é uma transição de } w\}$ .

Vamos provar que  $\sim$  preserva  $\delta$ . Para tanto basta considerar o caso em que tenhamos  $w, w', v \in A^+$  e  $s, t \in A^*$  tais que  $w = sv^nt$  e  $w' = sv^{n+mt}$  e provar que  $\delta(w) = \delta(w')$ . Considere todas as definições do lema 7.3 bem como as de sua demonstração. Caso  $v^n \mathcal{D}' w$ , o item 2 do lema 7.3 implica que toda transição de  $w$  é transição de  $w'$  e vice-versa, não mais tendo o que provar. Suponhamos agora que  $v^n \mathcal{P}' w$ . Neste caso vimos que  $k = k'$  e que  $w_i \sim w'_i$  para  $i = 1, \dots, k$ . Fixemos  $i \in \{1, \dots, k\}$ . Seja  $f_i = (x_i, y_i, z_i)$  e  $f'_i = (x'_i, y'_i, z'_i)$ . Como vimos na demonstração do caso  $v^n \mathcal{P}' w$  no lema 7.3, temos três casos de acordo com a pertinência de  $f_{i-1}$  e de  $f_i$  às partições  $F_1, F_2$  e  $F_4$ . Nos casos 1 e 3 supúnhamos que  $f_{i-1}, f_i \in F_1$  ou que  $f_{i-1}, f_i \in F_4$ , respectivamente. Em ambos os casos vimos que  $w_i = w'_i$ , o que naturalmente implica que  $\delta(w_i) = \delta(w'_i)$  nestes casos. No item 2 supúnhamos que  $f_{i-1} \in F_1 \cup F_2$  e  $f_i \in F_2 \cup F_4$ . Neste caso vimos que  $x'_{i-1} = x_{i-1}$  e  $|x_{i-1}| < |s|$  e  $z'_i = z_i$  e  $|z_i| < |t|$ . Assim vimos que  $w'_i = x'_{i-1}{}^{-1}w'z'_i{}^{-1} = x_{i-1}{}^{-1}(sv^{n+mt})z_i{}^{-1} = (x_{i-1}{}^{-1}s)v^{n+mt}(tz_i{}^{-1}) \sim (x_{i-1}{}^{-1}s)v^n(tz_i{}^{-1}) = x_{i-1}{}^{-1}(sv^nt)z_i{}^{-1} = x_{i-1}{}^{-1}wz_i{}^{-1} = w_i$ . Como  $|x_{i-1}| < |s|$  e  $|z_i| < |t|$ , sejam  $a$  a primeira letra de  $(x_{i-1}{}^{-1}s)$  e  $b$  a última letra de  $(tz_i{}^{-1})$ . Como  $(x_{i-1}{}^{-1}s)$  é prefixo de  $w_i$  e de  $w'_i$  temos que  $a$  é a primeira letra de  $w_i$  e de  $w'_i$ . Da mesma forma, temos que  $b$  é a última letra de  $w_i$  e de  $w'_i$ . Assim  $a^{-1}w'_ib^{-1} = (a^{-1}(x_{i-1}{}^{-1}s))v^{n+mt}((tz_i{}^{-1})b^{-1}) \sim$

$(a^{-1}(x_{i-1}^{-1}s))v^n((tz_i^{-1})b^{-1}) = a^{-1}w_ib^{-1}$ . Como a seqüência de transições de  $w_i$  de é a própria  $w_i$  e a de  $w'_i$  de é a própria  $w'_i$ , temos pois que  $\delta(w_i) = \{(a, \widetilde{a^{-1}w_ib^{-1}}, b)\} = \{(a, \widetilde{a^{-1}w'_ib^{-1}}, b)\} = \delta(w'_i)$ . Donde  $\delta(w_i) = \delta(w'_i)$  em qualquer caso. Por fim, segue que  $\delta(w) = \cup_{i=1}^k \delta(w_i) = \cup_{i=1}^k \delta(w'_i) = \delta(w')$ .

Sejam duas transições  $aub$  e  $a'u'b'$ , com  $a, a', b, b' \in A$  e  $u, u' \in A^*$ . Naturalmente,  $a = a'$  e  $b = b'$  e  $u \sim u'$  implicam que  $aub \sim a'u'b'$ . Suponha agora que  $aub \sim a'u'b'$ . Neste caso, como  $\sim$  preserva  $\delta$ , temos que  $\{(a', \widetilde{u'}, b')\} = \delta(a'u'b') = \delta(aub) = \{(a, \widetilde{u}, b)\}$  e portanto que  $a = a'$  e  $b = b'$  e  $u \sim u'$ .

Seja uma transição  $aub$  com  $a, b \in A$  e  $u \in A^*$  tal que  $aub$  seja a menor transição na respectiva classe de congruência e seja  $w$  a menor palavra desta classe. Vamos provar que  $w = aub$ . Como  $\sim$  preserva  $\delta$ , temos que  $\delta(w) = \delta(aub) = \{(a, \widetilde{u}, b)\}$  e portanto que existe  $au'b$  uma transição de  $w$  tal que  $u' \sim u$ . Assim  $w \sim aub \sim au'b \in \text{Fat}(w)$  implicando pois que  $w = au'b$  devido à escolha de  $w$ . Como  $w$  é uma transição na classe de  $aub$ , que é a menor transição em sua classe de congruência, temos que  $w = aub$ . ■

## 7.2 O teorema da caracterização

Considere o exemplo 7.2. Seja  $\mathcal{K}$  a categoria livre gerada pelo grafo fundamental  $\mathbf{G}$  visto na figura 7.1 e sejam  $p = (\underline{aba}, \underline{bab})$  e  $q = (\underline{aba}, \underline{baab})$  dois passeios de  $\mathcal{K}$  com início e término em  $\underline{ab}$ . Seja  $\mathcal{B}$  o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por  $\mathbf{G}$ , seja  $\widehat{\cdot} : \mathcal{K} \rightarrow \mathcal{B}$  a projeção canônica e seja  $\cong$  a congruência associada a esta projeção. Observando que a congruência  $\sim$  preserva a primeira e a última letra de uma palavra bem como as funções  $\#_a$  e  $\#_b$ , verifica-se facilmente que toda palavra  $x$  tal que o símbolo  $\widetilde{x}$  aparece na figura 7.1 é a menor palavra em sua classe de congruência. Sejam então definidas as palavras  $u = \tau(p) = abab$  e  $v = \tau(q) = abaab$  e  $w = \tau(pq) = ababaab$  e  $w' = \tau(qp) = abaabab$ . Observe que  $\sigma(ab) = 1_{\underline{ab}}$  devido à definição e que  $\sigma(u) = p$  e  $\sigma(v) = q$  e  $\sigma(w) = pq$  e  $\sigma(w') = qp$  devido ao item 2 da proposição 6.11. Temos que  $\epsilon_R(ab) = \epsilon_R(u) = \epsilon_R(v) = \epsilon_R(w) = \epsilon_R(w') = \epsilon_L(ab) = \epsilon_L(u) = \epsilon_L(v) = \epsilon_L(w) = \epsilon_L(w') = ab$  devido à proposição 6.11 e à proposição 5.5. Portanto  $ab, u, v, w$  e  $w'$  são palavras na mesma  $\mathcal{H}'$ -classe devido ao teorema 6.3 e seu dual. Como a avaliação destas palavras pelas funções  $\#_a$  e  $\#_b$  é aquela descrita na tabela 7.1 e estas funções são preservadas por  $\sim$ , segue que duas quaisquer das palavras  $ab, u, v, w$  e  $w'$  não são congruentes,

exceto possivelmente  $w$  e  $w'$ . Por outro lado, como a avaliação das digitais das palavras  $ab$ ,  $u$ ,  $v$ ,  $w$  e  $w'$  pelas funções  $\#_{\widetilde{bab}}$  e  $\#_{\widetilde{baab}}$  é aquela descrita na tabela 7.1 — e podemos verificar que estas funções são preservadas por  $\cong$

	$ab$	$u$	$v$	$w$	$w'$
$\#_a$	1	0	1	0	0
$\#_b$	1	0	0	1	1

	$\sigma(ab)$	$\sigma(u)$	$\sigma(v)$	$\sigma(w)$	$\sigma(w')$
$\#_{\widetilde{bab}}$	0	1	0	1	1
$\#_{\widetilde{baab}}$	0	0	1	1	1

Tabela 7.1: Avaliação das palavras  $ab$ ,  $u$ ,  $v$ ,  $w$  e  $w'$  pelas funções  $\#_a$  e  $\#_b$  e de suas digitais pelas funções  $\#_{\widetilde{bab}}$  e  $\#_{\widetilde{baab}}$

— segue que duas quaisquer das digitais das palavras  $ab$ ,  $u$ ,  $v$ ,  $w$  e  $w'$  não são congruentes por  $\cong$ , exceto possivelmente  $\sigma(w)$  e  $\sigma(w')$ . De fato, a proposição 4.8 implica que  $\sigma(w) = pq \cong qp = \sigma(w')$  e, por outro lado,  $w \sim w'$  como provaremos agora. Como a  $\mathcal{H}$ -classe de  $\widetilde{ab}$  é um grupo pois possui o idempotente  $e = \widetilde{abab}$ , qualquer elemento  $h$  desta  $\mathcal{H}$ -classe é tal que  $h^2 = e$  pois se  $g \in \mathcal{M}$  é tal que  $gh = e$  então  $h^3 = h$  implica que  $h^2 = eh^2 = gh^3 = gh = e$ . Assim,  $\widetilde{ab}$  e  $\widetilde{abaab}$  são dois elementos desta  $\mathcal{H}$ -classe e a proposição 4.8 implica que  $\widetilde{w} = \widetilde{ababaab} = \widetilde{ab} \widetilde{abaab} = \widetilde{abaab} \widetilde{ab} = \widetilde{abaabab} = \widetilde{w}'$ .

Em suma, de todas as palavras  $ab$ ,  $u$ ,  $v$ ,  $w$  e  $w'$  na mesma  $\mathcal{H}'$ -classe vista acima, as únicas palavras que são congruentes por  $\sim$  são aquelas cujas digitais são congruentes por  $\cong$ . No teorema 7.5 provaremos que esta não é uma coincidência mas uma propriedade válida para uma  $\mathcal{H}$ -classe qualquer de qualquer monóide de Burnside livre. No teorema 7.5 caracterizamos quando duas palavras com imagem por  $\sim$  nesta  $\mathcal{D}$ -classe representam o mesmo elemento ou não em termos de suas  $\mathcal{R}$ -entradas,  $\mathcal{L}$ -entradas e digitais. Esta caracterização é parcial no sentido que o problema da palavra ainda não é resolvido. Algumas questões ainda ficam pendentes como: saber se  $w \mathcal{D}' w'$ ; construir efetivamente o grafo fundamental; saber se  $\epsilon_R(w) \sim \epsilon_R(w')$ ; etc. Porém, outros resultados nossos já apontam a resposta a algumas destas perguntas: este é o caso dos corolários 6.5, 7.4 e 6.15 e da proposição 6.16.

Poderíamos evitar os conceitos de categorias e grupóides no enunciado do teorema 7.5 ao enunciá-lo com  $\mathbf{G}^*$  sendo um monóide livre sobre o

alfabeto  $\mathbf{G}$  e  $\mathcal{B}$  sendo o grupo de Burnside livre satisfazendo  $x^m = 1$  gerado pelo alfabeto  $\mathbf{G}$ . Estes conceitos seriam mais difíceis de serem evitados na demonstração do teorema 7.5 e em particular na demonstração do teorema 7.6, já que precisamos impor a restrição de que nem toda seqüência aleatória de arestas forma um passeio em  $\mathbf{G}$ .

**Teorema 7.5 (teorema da caracterização)** *Sejam  $A$  um alfabeto,  $n \geq 1$  e  $m \geq 1$  inteiros. Duas palavras  $w$  e  $w'$  que são canonicamente projetadas numa mesma  $\mathcal{D}$ -classe do semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$  são identificadas por esta projeção se e só se as seguintes condições forem satisfeitas:*

1. as  $\mathcal{R}$ -entradas de  $w$  e de  $w'$  são identificadas por esta projeção;
2. as  $\mathcal{L}$ -entradas de  $w$  e de  $w'$  são identificadas por esta projeção;
3. as digitais de  $w$  e de  $w'$  são identificadas pela projeção canônica da categoria livre gerada pelo grafo fundamental  $\mathbf{G}$  da  $\mathcal{D}$ -classe em questão sobre o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por  $\mathbf{G}$ .

*Prova.* Suponhamos primeiramente o caso em que a  $\mathcal{D}$ -classe em questão seja irregular. Neste caso, a proposição 6.14 implica que o grafo fundamental desta  $\mathcal{D}$ -classe não possui arestas e possui um único vértice  $u$ . Assim  $\sigma(w) = \sigma(w') = 1_u$  e o item 3 é sempre satisfeito. Usando o teorema 6.3 e seu dual temos que  $\tilde{w} \mathcal{R} \tilde{w}' \iff \epsilon_R(w) = \epsilon_R(w')$  e que  $\tilde{w} \mathcal{L} \tilde{w}' \iff \epsilon_L(w) = \epsilon_L(w')$ . Como a  $\mathcal{H}$ -classe de  $\tilde{w}$  é trivial devido à proposição 6.13, temos pois que  $\tilde{w} = \tilde{w}' \iff \tilde{w} \mathcal{H} \tilde{w}' \iff \tilde{w} \mathcal{R} \tilde{w}'$  e  $\tilde{w} \mathcal{L} \tilde{w}' \iff \epsilon_R(w) = \epsilon_R(w')$  e  $\epsilon_L(w) = \epsilon_L(w')$  se e só se as afirmativas 1, 2 e 3 forem satisfeitas.

Suponha a partir de agora que a  $\mathcal{D}$ -classe em questão seja regular. Podemos escolher  $e \in A^+$  tal que  $\tilde{e}$  seja um idempotente nesta  $\mathcal{D}$ -classe. Seja  $\mathbf{G}$  o grafo fundamental de  $\tilde{e}$  e seja  $\mathcal{K} = \mathbf{G}^*$  a categoria livre gerada por  $\mathbf{G}$ . O grafo fundamental  $\mathbf{G}$  é fortemente conexo devido à proposição 6.8 e portanto  $\mathcal{B}$ , o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por  $\mathbf{G}$ , pode ser definido. Temos também  $\hat{\cdot}$  a projeção canônica de  $\mathcal{K} = \mathbf{G}^*$  sobre  $\mathcal{B}$ .

Seja  $w_0 = \epsilon_R(w)$ , seja  $w_1, \dots, w_k$  a seqüência de transições de  $w$  e seja  $w_{k+1} = \epsilon_L(w)$ . Seja  $w'_0 = \epsilon_R(w')$ , seja  $w'_1, \dots, w'_{k'}$  a seqüência de transições de  $w'$  e seja  $w'_{k'+1} = \epsilon_L(w')$ . Assim, temos que  $\sigma(w) = (\tilde{w}_1, \tilde{w}_2, \dots, \tilde{w}_k)$  e que  $\sigma(w') = (\tilde{w}'_1, \tilde{w}'_2, \dots, \tilde{w}'_{k'})$ .

Suponha que  $w \sim w'$ . Vamos provar as afirmativas 1, 2 e 3. A afirmativa 1 é uma consequência do teorema 6.3. Já a afirmativa 2 tem uma demonstração dual. Vamos provar a afirmativa 3 provando que a congruência  $\sim$  preserva o valor da função  $\widehat{\circ} \sigma$ . Para tanto, é suficiente supor o caso em que  $(w', w)$  é uma substituição por  $(v^{n+m}, v^n)$ , para algum  $v \in A^+$ . Sejam  $s, t \in A^*$  tais que  $w = sv^n t$  e  $w' = sv^{n+m} t$ . Suponha primeiro o caso em que  $v^n \mathcal{D}' w$ . Pelo item 1 do lema 7.3 temos que  $k' = k$  e que  $w'_i \sim w_i$ , para  $i = 1, \dots, k$ . Assim temos que  $\sigma(w') = (\widetilde{w}'_1, \widetilde{w}'_2, \dots, \widetilde{w}'_k) = (\widetilde{w}_1, \widetilde{w}_2, \dots, \widetilde{w}_k) = \sigma(w)$ . Suponhamos agora que  $v^n \mathcal{D}' w$ . Pelo item 2 do lema 7.3 temos que existem  $l > 0$  e  $0 \leq j \leq k$  tais que:  $k' = k + ml$ ;  $w'_i = w_i$ , para  $i = 1, \dots, j$ ;  $w'_{j+i} = w'_{j+i+l} = \dots = w'_{j+i+(m-1)l}$ , para  $i = 1, \dots, l$ ; e  $w'_i = w_{i-ml}$ , para  $i = j + ml + 1, \dots, k'$ . Assim temos que  $\sigma(w') = (\widetilde{w}'_1, \dots, \widetilde{w}'_j, \widetilde{w}'_{j+1}, \dots, \widetilde{w}'_{j+ml}, \widetilde{w}'_{j+ml+1}, \dots, \widetilde{w}'_{k'}) = (\widetilde{w}_1, \dots, \widetilde{w}_j) (\widetilde{w}'_{j+1}, \dots, \widetilde{w}'_{j+l})^m (\widetilde{w}_{j+1}, \dots, \widetilde{w}_k) \cong (\widetilde{w}_1, \dots, \widetilde{w}_j, \widetilde{w}_{j+1}, \dots, \widetilde{w}_k) = \sigma(w)$  que por sua vez implica que  $\widehat{\sigma}(w') = \widehat{\sigma}(w)$ .

Suponha a partir de agora que as afirmativas 1, 2 e 3 sejam satisfeitas. Queremos mostrar que  $w \sim w'$ .

Relembramos que dadas duas palavras  $u$  e  $v$ , então  $u \sim v \iff \widetilde{u} = \widetilde{v}$ . Usaremos esta propriedade extensivamente. Seja  $(\mu, \eta, \psi, \psi^R, \psi^L)$  um sistema de adequações coerente associado a  $e$ . Seja  $H$  a  $\mathcal{H}$ -classe de  $\widetilde{e}$ . Assim  $H$  é um subsemigrupo de  $\mathcal{M}$  que é um grupo. A identidade do grupo é  $\widetilde{e}$ .

Vamos provar que se  $x \in H$  então  $x^m = e$ . Seja  $u \in A^*$  tal que  $x = \widetilde{u}$ . Como  $\widetilde{\phantom{x}}$  é um morfismo e  $u^{n+m} \sim u^n$ , temos que  $x^n = (\widetilde{u})^n = \widetilde{u}^n = \widetilde{u^{n+m}} = (\widetilde{u})^{n+m} = x^{n+m}$ . Como  $H$  é um grupo, temos então que  $e = (x^n)^{-1} x^n = (x^n)^{-1} x^{n+m} = (x^n)^{-1} x^n x^m = ex^m = x^m$ .

Podemos munir  $H$  com funções de incidência  $\alpha$  e  $\omega$  que aplicam cada elemento de  $H$  num mesmo vértice. É imediato verificar que  $H$  é uma categoria.

Vamos definir um morfismo de categorias  $\varphi : \mathcal{K} \rightarrow H$ . Como consequência do item 1 da proposição 5.13 temos que  $\widetilde{\phantom{x}} \circ \psi$  aplica em  $H$ . Assim, podemos definir primeiramente o morfismo de grafos  $\varphi : \mathbf{G} \rightarrow H$  por  $\varphi(\widetilde{u}) = \widetilde{\psi(u)}$  onde  $u$  é uma transição tal que  $\widetilde{u} \in \mathbf{G}$ . Esta definição não depende da particular escolha de  $u$ . De fato, se  $u$  e  $u'$  são duas transições tais que  $\widetilde{u} = \widetilde{u'}$ , como o sistema de adequações é coerente, então a proposição 6.6 implica que  $\widetilde{\psi(u)} = \widetilde{\psi(u')}$ . Como  $\mathcal{K} = \mathbf{G}^*$  é a categoria livre gerada por  $\mathbf{G}$ , este morfismo de grafos pode ser unicamente estendido a um morfismo de

categorias  $\varphi : \mathcal{K} \rightarrow H$ , que é definido por

$$\varphi((\tilde{u}_1, \tilde{u}_2, \dots, \tilde{u}_k)) = \widetilde{\psi(u_1)}\widetilde{\psi(u_2)} \cdots \widetilde{\psi(u_k)}.$$

Vamos provar que  $\cong$  preserva o valor de  $\varphi$ . Sejam  $p, p' \in \mathcal{K}$  tais que  $p \cong p'$ . Queremos provar que  $\varphi(p) = \varphi(p')$ . É suficiente supôr o caso em que  $(p', p)$  é uma substituição por  $(t^m, 1_v)$  onde  $v \in V(\mathbf{G})$  e  $t \in \mathcal{K}_v$ . Sejam assim  $r \in \mathcal{K}_{\alpha(p), v}$  e  $s \in \mathcal{K}_{v, \omega(p)}$  tais que  $p' = rt^m s$  e que  $p = rs$ . Como já vimos,  $x^m = e$  para qualquer  $x \in H$ . Dado que  $\varphi$  é um morfismo, temos finalmente que  $\varphi(p') = \varphi(rt^m s) = \varphi(r)\varphi(t)^m\varphi(s) = \varphi(r)e\varphi(s) = \varphi(r)\varphi(s) = \varphi(rs) = \varphi(p)$ .

Vamos provar que  $w' \sim w$ . A partir da afirmativa 1, temos que  $w_0 = \epsilon_R(w) \sim \epsilon_R(w') = w'_0$ . Assim temos que  $\widetilde{\psi^R(w_0)} = \widetilde{\psi^R(w'_0)}$  já que o sistema de adequações é coerente. A partir da afirmativa 2, temos que  $w_{k+1} = \epsilon_L(w) \sim \epsilon_L(w') = w'_{k'+1}$ . Assim temos que  $\widetilde{\psi^L(w_{k+1})} = \widetilde{\psi^L(w'_{k'+1})}$  já que o sistema de adequações é coerente. Como  $\sigma(w) \cong \sigma(w')$  devido à afirmativa 3, temos que  $\varphi(\sigma(w)) = \varphi(\sigma(w'))$  pois  $\cong$  preserva o valor de  $\varphi$ . Da definição de  $\varphi$  temos que  $\varphi(\sigma(w)) = \widetilde{\psi(w_1)}\widetilde{\psi(w_2)} \cdots \widetilde{\psi(w_k)}$  e similarmente que  $\varphi(\sigma(w')) = \widetilde{\psi(w'_1)}\widetilde{\psi(w'_2)} \cdots \widetilde{\psi(w'_{k'})}$ . Ora, usando o lema 5.14 sobre  $w$  e sobre  $w'$  temos que  $\tilde{w} = \widetilde{\psi^R(w_0)}\widetilde{\psi(w_1)}\widetilde{\psi(w_2)} \cdots \widetilde{\psi(w_k)}\widetilde{\psi^L(w_{k+1})} = \widetilde{\psi^R(w_0)}\varphi(\sigma(w))\widetilde{\psi^L(w_{k+1})} = \widetilde{\psi^R(w'_0)}\varphi(\sigma(w'))\widetilde{\psi^L(w'_{k'+1})} = \widetilde{\psi^R(w'_0)}\widetilde{\psi(w'_1)}\widetilde{\psi(w'_2)} \cdots \widetilde{\psi(w'_{k'})}\widetilde{\psi^L(w'_{k'+1})} = \tilde{w}'$ , conforme desejávamos provar. ■

### 7.3 O teorema dos grupos maximais

Nesta seção nos dedicaremos ao teorema dos grupos maximais (teorema 7.6) e algumas de suas aplicações. Em sua demonstração usaremos o teorema 7.5 e o teorema 4.7 visto no capítulo 4. Antes porém veremos um exemplo de modo a ilustrar o teorema.

Considere o exemplo 7.2. Seja  $H$  a  $\mathcal{H}$ -classe de  $\tilde{ab}$ . Seja o alfabeto  $B = \{r, s, t\}$  e seja  $\varphi : B^+ \rightarrow A^+$  um morfismo definido nos geradores por  $\varphi(r) = ab$ ,  $\varphi(s) = abaabab$  e  $\varphi(t) = abbab$ . Vamos provar que  $H = \widetilde{\varphi(B^+)}$ . Se  $v \in B^+$  então  $\epsilon_R(\varphi(v)) = \epsilon_L(\varphi(v)) = ab$  devido à proposição 6.1 e, portanto,  $\widetilde{\varphi(v)} \in H$ . Seja  $h \in H$  e seja uma palavra  $w$  tal que  $\tilde{w} = h$ . Como  $ab \mathcal{H}' w$  e  $w$  é  $\sim$ -regular, temos que existem  $x, y, z \in A^*$  tais que  $wyw \sim w \sim$



$abx \sim zab$ . Assim  $w \sim wyw \sim abxyzab$  e podemos supôr que  $w \in abA^*ab$ . Como  $a^i \sim a^{i-2}$  e  $b^i \sim b^{i-2}$  sempre que  $i \geq 3$ , podemos substituir qualquer ocorrência de um fator  $a^3$  (ou  $b^3$ ) em  $w$  por  $a$  (ou  $b$ ). Portanto podemos supôr que existam  $k \geq 2$  e seqüências  $i_2, \dots, i_k$  e  $j_1, \dots, j_{k-1}$  de inteiros em  $\{1, 2\}$  tais que  $w = ab^{j_1}a^{i_2}b^{j_2} \dots a^{i_k}b$ . É suficiente provar que existe uma palavra na imagem de  $\varphi$  na mesma classe de congruência de  $w$ . Para tanto, faremos uma indução em  $k$ . Seja  $C = \{abab, abbab, abaab, abbaab\}$ . Note que existe uma palavra de  $\varphi(B^+)$  na classe de congruência de cada palavra de  $C$  pois temos que  $abab = \varphi(rr)$ , que  $abbab = \varphi(t)$ , que  $abaab \sim abaababab = \varphi(sr)$  e que  $abbaab \sim abbababaab \sim \varphi(t)\varphi(sr) = \varphi(tsr)$ . Assim,  $ab^{j_{k-1}}a^{i_k}b \in C$  e podemos definir  $u_k \in \{rr, t, sr, tsr\}$  tal que  $ab^{j_{k-1}}a^{i_k}b \sim \varphi(u_k)$ . Se  $k = 2$ , temos que  $w = ab^{j_1}a^{i_2}b \sim \varphi(u_2)$  e temos a base da indução. Suponha agora que  $k \geq 3$  e que exista  $u \in B^+$  tal que  $ab^{j_1}a^{i_2}b^{j_2} \dots a^{i_{k-1}}b \sim \varphi(u)$ . Como  $ab \sim ababab$  é fator de  $a^{i_{k-1}}b^{j_{k-1}}$  temos pois que  $w = ab^{j_1}a^{i_2}b^{j_2} \dots a^{i_{k-1}}b^{j_{k-1}}a^{i_k}b \sim ab^{j_1}a^{i_2}b^{j_2} \dots a^{i_{k-1}}b ab^{j_{k-1}}a^{i_k}b \sim \varphi(u)\varphi(r)\varphi(u_k) = \varphi(uru_k)$  e segue a tese.

Continuando o exemplo acima, temos que  $\sim$  preserva as funções  $\#_a$  e  $\#_b$ . Não é difícil provar que  $\sim$  preserva a função  $\#_{b(aa)+b}$  onde  $\#_{b(aa)+b}(w)$  é a paridade do número de ocorrências de fatores da forma  $ba^i b$  com  $i$  par. Avaliando estas funções em  $\varphi(D)$  para  $D = \{rr, r, t, rt, s, rs, ts, rts\} \subset B^+$ , temos a tabela 7.2. Isto prova que as oito palavras de  $\varphi(D)$  são duas a duas não congruentes e portanto  $H = \widetilde{\varphi(B^+)}$  tem cardinalidade 8 ao menos. Ora,  $H$  é um grupo gerado pelo conjunto  $\varphi(B)$ , de cardinalidade 3, que é também o número ciclômático do grafo fundamental visto no exemplo 7.2. Como  $h \in H$  implica que  $h^3 = h$ , temos então que  $e = h^{-1}h = h^{-1}h^3 = eh^2 = h^2$  onde  $e \in H$  é a identidade do grupo  $H$ . Afirmamos que o grupo de Burnside livre satisfazendo  $x^2 = 1$  gerado por um conjunto de cardinalidade 3 é isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$  que por sua vez possui cardinalidade 8 (a proposição 4.8 ajuda a verificar esta afirmativa). Assim podemos concluir que  $H$ , a  $\mathcal{H}$ -classe de  $\tilde{ab}$ , é o grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um conjunto cuja a cardinalidade é o número ciclômático do grafo fundamental de  $ab$ .

O conteúdo do teorema 7.6 é justamente este: um grupo maximal em um semigrupo de Burnside livre satisfazendo  $x^{n+m} = x^n$  é um grupo de Burnside livre satisfazendo  $x^m = 1$ . Observe que este resultado é conforme aquele já conhecido para  $n \geq 3$  e  $m \geq 1$  onde, pelo teorema 8.16 [10], sabe-se que qualquer grupo maximal é cíclico de ordem  $m$  (o grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um único elemento). Há uma substancial evolução no teorema dos grupos maximais já que o mesmo vale para quaisquer

	$\varphi(rr)$	$\varphi(r)$	$\varphi(t)$	$\varphi(rt)$	$\varphi(s)$	$\varphi(rs)$	$\varphi(ts)$	$\varphi(rts)$
$\#_a$	0	1	0	1	0	1	0	1
$\#_b$	0	1	1	0	1	0	0	1
$\#_{b(aa)+b}$	0	0	0	0	1	1	1	1

Tabela 7.2: Avaliação das palavras de  $\varphi(D)$  pelas funções  $\#_a$  e  $\#_b$  e  $\#_{b(aa)+b}$ 

$n \geq 1$  e  $m \geq 1$  e os casos  $n = 1$  e  $n = 2$  têm estruturas muito diferentes daquela vista para  $n \geq 3$  e  $m \geq 1$ . No caso geral, o conjunto sobre o qual o grupo de Burnside é livre pode ter mais que um gerador, ao contrário do caso  $n \geq 3$  e  $m \geq 1$ . Ademais, é caracterizado um conjunto gerador para este grupo de Burnside livre e a cardinalidade do conjunto é o número ciclomático do grafo fundamental da  $\mathcal{H}$ -classe em questão. Esta diferença se mostra relevante quando no teorema 8.1 a ser visto no capítulo 8 vemos uma  $\mathcal{D}$ -classe regular cujo grafo fundamental tem número ciclomático  $2m - 1$  pelo menos. Esta é uma  $\mathcal{D}$ -classe de um monóide de Burnside livre satisfazendo  $x^2 = x^{2+m}$  gerado por um alfabeto de duas letras.

Como discutimos na introdução, para  $m$  suficientemente grande, sabemos ser infinito um grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um conjunto com pelo menos dois geradores. A proposição 7.8 a ser vista logo após mostrar-nos-á que as classes de congruência cuja projeção canônica é mapeada num elemento de uma  $\mathcal{D}$ -classe com  $\mathcal{H}$ -classes infinitas não são reconhecíveis. Este resultado contrasta completamente com aquele visto no teorema 8.18 [10], onde a reconhecibilidade das classes de congruência era garantida para  $n \geq 3$  e  $m \geq 1$ .

**Teorema 7.6 (teorema dos grupos maximais)** *Sejam inteiros  $n \geq 1$  e  $m \geq 1$  e seja  $A$  um alfabeto qualquer. Um grupo maximal em um semigrupo de Burnside livre satisfazendo  $x^{n+m} = x^n$  gerado por  $A$  é um grupo de Burnside livre satisfazendo  $x^m = 1$ . Ademais, se  $m \geq 2$ , este grupo de Burnside é livre sobre um conjunto de geradores cuja cardinalidade é o número ciclomático do grafo fundamental da  $\mathcal{D}$ -classe que contém o grupo.*

*Prova.* Considere  $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^{n+m} = x^n$  gerado por  $A$ . Considere um grupo maximal qualquer em  $\mathcal{M} \setminus \{\tilde{1}\}$ . Este grupo maximal é uma  $\mathcal{H}$ -classe regular de  $\mathcal{M}$  que contém um idempotente. Seja  $e \in A^+$  tal que este idempotente seja  $\tilde{e}$  e seja  $\mathbf{G}$  o grafo fundamental

desta  $\mathcal{D}$ -classe. Seja  $d$  uma  $\mathcal{D}$ -entrada na  $\mathcal{D}'$ -classe de  $e$  tal que  $d$  seja a menor  $\mathcal{D}$ -entrada em sua classe de congruência, seja  $u = \tilde{d} \in V(\mathbf{G})$  e seja  $H_u$  a  $\mathcal{H}$ -classe de  $u$ .

Vamos provar que  $\tilde{w} \in H_u \iff \epsilon_R(w) \sim \epsilon_L(w) \sim d$  para toda palavra  $w$ . Seja  $w$  uma palavra qualquer. Suponha primeiro que  $\epsilon_R(w) \sim \epsilon_L(w) \sim d$ . Assim  $w \mathcal{R}' \epsilon_R(w) \sim d$  e  $w \mathcal{L}' \epsilon_L(w) \sim d$  implicam que  $w \mathcal{H}' d$  e portanto que  $\tilde{w} \mathcal{H} \tilde{d} = u$ . Suponha agora que  $\tilde{w} \in H_u$ . Assim  $\tilde{w} \mathcal{H} u = \tilde{d}$  e  $w \mathcal{H}' d$ . Da proposição 5.5 temos que  $\epsilon_R(d) = d = \epsilon_L(d)$ . Como  $w \mathcal{R}' d$ , usando o teorema 6.3 temos que  $\epsilon_R(w) \sim \epsilon_R(d) = d$ . Como  $w \mathcal{L}' d$ , usando o dual do teorema 6.3 temos que  $\epsilon_L(w) \sim \epsilon_L(d) = d$ .

Vamos definir uma função  $\varphi : H_u \rightarrow \mathcal{B}_u$ . Seja  $h \in H_u$  e seja  $w$  uma palavra tal que  $\tilde{w} = h$ . Assim, definimos

$$\varphi(\tilde{w}) = \widehat{\sigma(w)}.$$

Esta definição não depende da particular escolha de  $w$  pois, se  $w' \in A^+$  é tal que  $\tilde{w}' = h = \tilde{w}$ , o teorema 7.5 implica que  $\widehat{\sigma(w)} = \widehat{\sigma(w')}$ . Vamos provar que  $\varphi$  aplica  $H_u$  em  $\mathcal{B}_u$ . Como vimos antes,  $\epsilon_R(w) \sim \epsilon_L(w) \sim d$  pois  $\tilde{w} = h \in H_u$ . Donde  $\epsilon_L(w) \mathcal{R}' d$  e usando o teorema 6.3 temos que  $\epsilon_R(\epsilon_L(w)) \sim \epsilon_R(d) = d$  já que  $\epsilon_R(d) = d$  devido à proposição 5.5. De maneira dual provamos que  $\epsilon_L(\epsilon_R(w)) \sim d$ . Como  $\sigma(w)$  é um passeio de  $\epsilon_L(\epsilon_R(w)) = \tilde{d} = u$  para  $\epsilon_R(\epsilon_L(w)) = \tilde{d} = u$  temos que  $\widehat{\sigma(w)} \in \mathcal{B}_u$ .

Vamos provar que  $\varphi$  é uma bijeção e calcular sua inversa. Vamos primeiro provar que  $\varphi$  é uma injeção. Sejam  $h, h' \in H_u$  e suponha que  $\varphi(h) = \varphi(h')$ . Sejam  $w, w' \in A^+$  tais que  $\tilde{w} = h$  e  $\tilde{w}' = h'$ . Assim  $w' \mathcal{D}' w \mathcal{D}' d$  e, conforme já vimos, temos que  $\epsilon_R(w') = \epsilon_R(w) = \tilde{d} = \epsilon_L(w') = \epsilon_L(w)$ . Tendo em vista que  $\widehat{\sigma(w)} = \varphi(h) = \varphi(h') = \widehat{\sigma(w')}$ , a partir do teorema 7.5, temos que  $w \sim w'$  e que, portanto,  $h = \tilde{w} = w' = h'$ . Isto prova que  $\varphi$  é injetiva. Vamos agora provar que  $\varphi$  é sobrejetora. Seja  $x$  um elemento qualquer de  $\mathcal{B}_u$  e seja  $p \in \mathcal{K}$  tal que  $\widehat{p} = x$ . A partir da definição de  $\tau$ , temos que  $\widehat{\tau(1_u)} = u$ . Usando os itens 3 e 4 da proposição 6.11 temos que  $\widehat{\tau(p)} \mathcal{R} \epsilon_R(\tau(p)) = \tau(1_{\alpha(p)}) = \tau(1_u) = u = \tau(1_{\omega(p)}) = \epsilon_L(\tau(p)) \mathcal{L} \widehat{\tau(p)}$ . Assim temos que  $\widehat{\tau(p)} \mathcal{H} u$ . Tendo em vista que  $\varphi(\widehat{\tau(p)}) = \widehat{\sigma(\tau(p))} = \widehat{p} = x$  devido ao item 2 da proposição 6.11, concluímos que  $\varphi$  é sobrejetora. Também provamos que

$$\varphi^{-1}(\widehat{p}) = \widehat{\tau(p)}$$

e que esta imagem inversa não depende da particular escolha de  $p$  que projeta em  $\widehat{p}$  pois  $\varphi$  é injetiva como vimos.

Vamos definir uma função  $\delta : H_u \rightarrow H_{\tilde{e}}$ . Seja  $(\mu, \eta)$  um sistema de adequações básico para  $e$ . Seja  $h$  um elemento qualquer de  $H_u$ . Definimos

$$\delta(h) = \widetilde{\mu}_d h \widetilde{\eta}_d.$$

Note que a definição das funções de adequação à direita e à esquerda implicam que  $\delta(u) = \delta(\widetilde{d}) = \widetilde{\mu}_d \widetilde{d} \widetilde{\eta}_d = \tilde{e}$ . Usando o lema de Green e seu dual, temos que  $\delta$  é uma bijeção de  $H_u$  em  $H_{\tilde{e}}$ .

Vamos provar que  $\delta \circ \varphi^{-1}$  é um isomorfismo de grupos de  $\mathcal{B}_u$  em  $H_{\tilde{e}}$ . Como  $\varphi : H_u \rightarrow \mathcal{B}_u$  e  $\delta : H_u \rightarrow H_{\tilde{e}}$  são bijeções, temos que  $\delta \circ \varphi^{-1} : \mathcal{B}_u \rightarrow H_{\tilde{e}}$  é uma bijeção. Temos também que  $\delta(\varphi^{-1}(\widehat{1}_u)) = \delta(\widetilde{\tau(1_u)}) = \delta(u) = \delta(\widetilde{d}) = \widetilde{\mu}_d \widetilde{d} \widetilde{\eta}_d = \tilde{e}$  implicando pois que  $\delta \circ \varphi^{-1}$  mapeia identidade em identidade. Só nos falta provar que  $\delta \circ \varphi^{-1}$  é um morfismo. Sejam  $x, x' \in \mathcal{B}_u$  dois elementos quaisquer. Sejam  $p, p' \in \mathcal{K}_u$  tais que  $\widehat{p} = x$  e  $\widehat{p}' = x'$ . Como  $d$  é a menor  $\mathcal{D}$ -entrada em sua classe de congruência temos que  $d = \tau(1_u) = \tau(1_{\omega(p)}) = \epsilon_L(\tau(p)) \in \text{Suf}(\tau(p))$  devido ao item 3 da proposição 6.11. De modo análogo temos que  $d = \tau(1_u) = \tau(1_{\alpha(p')}) = \epsilon_R(\tau(p')) \in \text{Pref}(\tau(p'))$ . Assim, usando o item 5 da proposição 6.11 bem como o item 4 da proposição 5.13 temos que  $\tau(pp') = \tau(p)(\epsilon_R(\tau(p'))^{-1}\tau(p')) = (\tau(p)d^{-1})d(d^{-1}\tau(p')) \sim (\tau(p)d^{-1})d\eta_d\mu_d d(d^{-1}\tau(p')) = \tau(p)\eta_d\mu_d\tau(p')$ . Por fim, concluímos que  $\varphi^{-1}(xx') = \varphi^{-1}(\widehat{pp'}) = \varphi^{-1}(\widetilde{pp'}) = \tau(pp') = \tau(p)\eta_d\mu_d\tau(p') = \tau(p)\widetilde{\eta}_d\widetilde{\mu}_d\tau(p') = \varphi^{-1}(\widehat{p})\widetilde{\eta}_d\widetilde{\mu}_d\varphi^{-1}(\widehat{p}') = \varphi^{-1}(x)\widetilde{\eta}_d\widetilde{\mu}_d\varphi^{-1}(x')$  e portanto que  $\delta(\varphi^{-1}(xx')) = \widetilde{\mu}_d\varphi^{-1}(x)\widetilde{\eta}_d\widetilde{\mu}_d\varphi^{-1}(x')\widetilde{\eta}_d = \delta(\varphi^{-1}(x))\delta(\varphi^{-1}(x'))$ . Isto prova que  $\delta \circ \varphi^{-1}$  é um morfismo, conforme queríamos demonstrar.

Para concluir, temos que o grupo maximal  $H_{\tilde{e}}$  é isomorfo ao grupo local  $\mathcal{B}_u$  que por sua vez é isomorfo a um grupo de Burnside livre satisfazendo  $x^m = 1$  devido ao teorema 4.7. Ademais, se  $m \geq 2$ , o mesmo teorema implica que este grupo é livre sobre o conjunto de geradores cuja cardinalidade é o número ciclomático do grafo fundamental  $\mathbf{G}$ . ■

Uma pergunta natural que podemos nos fazer no teorema 7.6 é o de se podemos exibir um conjunto de geradores para o grupo de Burnside livre satisfazendo  $x^m = 1$ . O corolário 7.7 apresenta um tal conjunto. Antes observe que como um grafo fundamental  $\mathbf{G}$  é fortemente conexo devido à proposição 6.8, fixado um vértice  $u$  e usando a proposição 2.3, podemos

escolher uma árvore conectora  $\mathbf{T} \subseteq \mathbf{G}$  com início  $u$  e uma árvore conectora  $\mathbf{T}' \subseteq \mathbf{G}$  com término  $u$ .

**Corolário 7.7** *Sejam:*

- $n \geq 1$  e  $m \geq 2$  inteiros;
- $A$  um alfabeto qualquer;
- $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$ ;
- $e \in A^+$  uma palavra  $\sim$ -idempotente;
- $\mathbf{G}$  o grafo fundamental de  $\tilde{e}$ ;
- $u \in V(\mathbf{G})$  um vértice qualquer;
- $\mathbf{T} \subseteq \mathbf{G}$  uma árvore conectora com início  $u$ ;
- $\mathbf{T}' \subseteq \mathbf{G}$  uma árvore conectora com término  $u$ ;
- $d$  uma  $\mathcal{D}$ -entrada tal que  $\tilde{d} = u$ ;
- $\mu_d$  e  $\eta_d$  palavras tais que  $e \sim \mu_d \eta_d$ .

Para todo vértice  $v \in V(\mathbf{G})$ , sejam  $p_v$  o único passeio em  $\mathbf{T}$  de  $u$  a  $v$  e  $q_v$  o único passeio em  $\mathbf{T}'$  de  $v$  a  $u$ . Seja  $\delta : \mathbf{G} \setminus \mathbf{T} \rightarrow \mathbf{G}^*$  a função definida por  $\delta(b) = p_{\alpha(b)} b q_{\omega(b)} (p_{\omega(b)} q_{\omega(b)})^{m-1}$  e seja  $\varphi : \mathbf{G} \setminus \mathbf{T} \rightarrow \mathcal{M}$  a função definida por  $\varphi(b) = \mu_d \tau(\delta(b)) \eta_d$ .

Então  $\varphi$  é uma injeção e a  $\mathcal{H}$ -classe de  $\tilde{e}$  é um grupo de Burnside livre satisfazendo  $x^m = 1$  gerado pelo conjunto  $\varphi(\mathbf{G} \setminus \mathbf{T})$ , cuja cardinalidade é o número ciclomático de  $\mathbf{G}$ . Seja  $u = \tilde{ab} \in V(\mathbf{G})$ .

Considere o exemplo 7.2. Sejam  $e = abab \sim abababab$  uma palavra  $\sim$ -idempotente. Como  $e \mathcal{D}' ab$  devido ao item 1 da proposição 6.1, seja  $\mathbf{G}$  o grafo fundamental de  $\tilde{e}$  exibido na figura 7.1. Seja  $\mathbf{T}$  o subgrafo de  $\mathbf{G}$  induzido pela aresta  $\tilde{aba}$  e  $\mathbf{T}'$  o subgrafo de  $\mathbf{G}$  induzido pela aresta  $\tilde{bab}$ . Então  $\mathbf{T} \subseteq \mathbf{G}$  é uma árvore conectora com início  $\tilde{ab}$  e  $\mathbf{T}' \subseteq \mathbf{G}$  é uma árvore conectora com término  $\tilde{ab}$ . Sejam as palavras  $\mu_{ab} = 1$  e  $\eta_{ab} = ab$ . Assim  $e = \mu_{ab} \eta_{ab}$ . Seja a função  $\delta : \mathbf{G} \setminus \mathbf{T} \rightarrow \mathbf{G}^*$  definida acima. Seja  $\varphi : B^+ \rightarrow A^+$  a função definida na página página 7.2. Vimos naquela página que  $\widetilde{\varphi(B)} = \varphi(\{r, s, t\})$

é um conjunto de geradores para a  $\mathcal{H}$ -classe de  $\widetilde{ab}$ , que é a mesma de  $\widetilde{e}$ . Note que  $\varphi(r) = ab \sim ababab = \tau((\widetilde{aba}, \widetilde{bab}))ab = \mu_{ab}\tau(\delta(\widetilde{bab}))\eta_{ab}$ , que  $\varphi(s) = abaabab = \tau((\widetilde{aba}, \widetilde{baab}))ab = \mu_{ab}\tau(\delta(\widetilde{baab}))\eta_{ab}$  e que  $\varphi(t) = abbab \sim abbababab = \tau((\widetilde{abba}, \widetilde{bab}, \widetilde{aba}, \widetilde{bab}))ab = \mu_{ab}\tau(\delta(\widetilde{abba}))\eta_{ab}$ . Como as arestas de  $\mathbf{G} \setminus \mathbf{T}$  são justamente  $\{\widetilde{bab}, \widetilde{baab}, \widetilde{abba}\}$ , os geradores  $\varphi(B)$  são os mesmos obtidos ao se aplicar o corolário 7.7.

Como anunciamos antes, a proposição 7.8 mostra-nos que a classe de congruência cuja projeção canônica é mapeada num elemento de uma  $\mathcal{D}$ -classe onde as  $\mathcal{H}$ -classes são infinitas não é reconhecível. Esta proposição pode ser encontrada no trabalho de de Luca e Varricchio [6].

**Proposição 7.8** *Sejam  $A$  um alfabeto qualquer,  $M$  um monóide qualquer,  $\widetilde{\cdot} : A^* \rightarrow M$  um morfismo sobrejetor,  $H$  uma  $\mathcal{H}$ -classe infinita de  $M$  e  $h \in H$ . Então a classe de congruência  $\{w \in A^* \mid \widetilde{w} = h\}$  não é reconhecível.*

*Prova.* Seja  $\sim$  a congruência em  $A^*$  definida por  $w \sim w' \iff \widetilde{w} = \widetilde{w}'$ .

Seja  $X = \{w \in A^* \mid \widetilde{w} = h\}$  e seja  $\equiv_X$  a congruência sintática gerada por  $X$ . Relembramos que duas palavras  $w$  e  $w'$  são tais que  $w \equiv_X w'$  se e só se  $xwy \in X \iff xw'y \in X$  para todos  $x, y \in A^*$ . Seja  $S = A^*/\equiv_X$  o monóide sintático de  $X$  e seja  $\widehat{\cdot} : A^* \rightarrow S$  o morfismo canônico que aplica uma palavra  $w$  em sua classe de congruência  $\widehat{w}$ .

Vamos provar que a cardinalidade de  $H$  é um limitante inferior para a cardinalidade de  $S$ . Seja  $\varphi : S \rightarrow H$  uma função parcial definida por  $\varphi(s) = \widetilde{u}$  sempre que existir  $u \in A^*$  tal que  $\widehat{u} = s$  e  $\widetilde{u} \in H$ . Vamos primeiro mostrar que  $\varphi$  é bem definida e que a definição de  $\varphi(s)$  não depende da particular escolha de  $u$ . Seja  $s \in S$  e sejam duas palavras  $u$  e  $u'$  tais que  $\widehat{u} = \widehat{u}' = s$  e  $\widetilde{u}, \widetilde{u}' \in H$ . Escolhendo  $w \in X$ , e portanto  $\widetilde{w} = h \in H$ , temos então que  $u \mathcal{H}' w \mathcal{H}' u'$ . Como  $u \mathcal{R}' w$ , existem  $y, y' \in A^*$  tais que  $uy \sim w$  e  $wy' \sim u$ . Assim  $uy \in X$ . Como  $u \equiv_X u'$ , temos então que  $u'y \in X$  e portanto  $u'y \sim w$ . Como  $u \mathcal{L}' u'$ , existem  $x, x' \in A^*$  tais que  $xu \sim u'$  e  $x'u' \sim u$ . Assim temos que  $w \sim u'y \sim xuy \sim xw$  e portanto que  $u \sim wy' \sim xwy' \sim xu \sim u'$ . Como  $u \sim u'$ , temos que  $\widetilde{u} = \widetilde{u}'$  e a definição de  $\varphi(s)$  não depende da particular escolha de  $u$ . Vamos agora mostrar que  $\varphi$  é sobrejetora. Como  $\widetilde{\cdot}$  é um morfismo sobrejetor, para todo  $x \in H$  podemos escolher uma palavra  $u$  tal que  $\widetilde{u} = x$ . Por definição,  $\varphi(\widehat{u}) = \widetilde{u} = x$  e, portanto,  $\varphi$  é sobrejetora. Para terminar, como  $\varphi$  é uma função sobrejetora que aplica um subconjunto de  $S$  sobre  $H$ , temos que  $|S| \geq |H|$ .

Como  $|S| \geq |H|$  e a cardinalidade de  $H$  é infinita por hipótese, temos que a cardinalidade de  $S$  também é infinita e  $X$  não é reconhecível por definição. ■





# Capítulo 8

## O caso $n = 2$

Suporemos  $n = 2$  e  $m \geq 2$  neste capítulo, salvo menção contrária. Sejam  $A = \{a, b\}$  um alfabeto de duas letras e  $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$ . Seja  $\sim$  a congruência de Burnside em questão e  $\tilde{\cdot} : A^* \rightarrow \mathcal{M}$  o morfismo canônico. Neste capítulo, os símbolos 3, 5, 7 denotarão os prefixos de  $(ba)^4$  de comprimentos inteiros 3, 5, 7, respectivamente. (Ex: 5 =  $babab$ .)

Nosso principal objetivo neste capítulo é apresentar o exemplo de uma  $\mathcal{D}$ -classe regular de  $\mathcal{M}$  cujo grafo fundamental tem número ciclomático  $2m - 1$  ao menos. Como conseqüência, o teorema 7.6 implica que os grupos maximais desta  $\mathcal{D}$ -classe são grupos de Burnside livres satisfazendo  $x^m = 1$  com ao menos  $2m - 1$  geradores. Para  $m$  suficientemente grande, estes grupos são infinitos e as classes de congruência projetadas em elementos da  $\mathcal{D}$ -classe não são reconhecíveis. Isto será visto no teorema 8.1 e nos corolários 8.2 e 8.3. Antes veremos que a congruência de Burnside em questão preserva algumas funções. Ao final veremos o exemplo de uma classe de congruência com duas palavras de menor comprimento. Estes resultados todos contrastam com os monóides de Burnside livres satisfazendo  $x^n = x^{n+m}$  nos casos em que  $n \geq 3$  e  $m \geq 1$  pois, nestes casos, os grupos maximais têm um único gerador (teorema 8.16 [10]) e toda classe de congruência tem uma única palavra de menor comprimento (teorema 7.3 [10]).

## 8.1 Grupo maximal com $2m - 1$ geradores

Nosso exemplo mencionado é a  $\mathcal{D}$ -classe de  $\tilde{55}$  e provaremos algumas de suas propriedades. Este exemplo relaciona-se a outros exemplos vistos em outros trabalhos. Em particular, I. Simon estudou a  $\mathcal{D}$ -classe de  $\tilde{55}$  em [30] para o caso  $n = 2$  e  $m = 1$ . Nosso trabalho [10] que estuda os monóides de Burnside livres satisfazendo  $x^n = x^{n+m}$ , para os casos em que  $n \geq 3$  e  $m \geq 1$ , define um sistema de reescritura  $\Sigma$  e a primeira produção de  $\Sigma$  que não é da forma  $(x^{n+m}, x^n)$  quando  $m = 1$  é também relacionada a esta mesma  $\mathcal{D}$ -classe (exemplo 4.5 [10]). Este mesmo exemplo (dependente de  $n$  e  $m$ ) é o contraexemplo que prova que  $\Sigma$  não é estável para  $n = 2$  e  $m \geq 2$ , como mencionamos no capítulo 1.

Não é difícil provar que  $\sim$  preserva as funções  $\#_a$ ,  $\#_b$ ,  $\#_{bb}$  e  $\#_{bbabb}$ , cujas definições, relembremos, encontram-se na seção 3.3 do capítulo 3. Dados um conjunto  $U$  de palavras, dadas duas palavras quaisquer  $w$  e  $w'$ , se  $\sim$  preserva a função  $\chi_U$  e se  $\chi_U(w) \neq \chi_U(w')$  então pode-se provar que  $w \not\mathcal{D}' w'$ . Definimos os conjuntos  $U_1 = abab(b^m)^*ba = \{ababb^{mk}ba, k = 0, 1, \dots\}$ ,  $U_2 = bab(b^m)^*bab$  e  $U_3 = ab(b^m)^*baba$ . Para  $i = 1, 2, 3$ , denotaremos a função  $\chi_{U_i}$  por  $\chi_i$ . Pode-se provar que a congruência  $\sim$  preserva  $\chi_1$ ,  $\chi_2$  e  $\chi_3$ .

Seja  $\mathbf{G}$  o grafo apresentado na figura 8.1. No teorema 8.1 vemos que este grafo é um subgrafo do grafo fundamental da  $\mathcal{D}$ -classe de  $\tilde{55}$ .

**Teorema 8.1** *O grafo  $\mathbf{G}$  apresentado na figura 8.1 é um subgrafo do grafo fundamental da  $\mathcal{D}$ -classe de  $\tilde{55}$ .*

*Prova.* Considere as palavras  $d_0, d_1, d_2, A, B, C$  como definidas na figura 8.1. Para  $i$  em  $\{1, 2, \dots, m-1\}$ , definimos  $D_i = a35(ab)^i3a$  e  $E_i = ab53^i5ba$ . Seja  $\mathbf{G}'$  o grafo fundamental da  $\mathcal{D}$ -classe de  $\tilde{55}$  com funções de incidência  $\alpha$  e  $\omega$ .

Afirmamos que se uma dada palavra  $w$  for tal que:

- $\exists x \mathcal{D}' 55$  que é fator de uma palavra na classe de congruência de  $w$  e;
- $w$  é fator de uma palavra na classe de congruência de  $55$ ,

então  $w$  está na  $\mathcal{D}'$ -classe de  $55$ . Esta afirmativa será livremente usada nesta demonstração. Realmente, o primeiro fato implica que  $\tilde{w} \leq_{\mathcal{J}} \tilde{x} \mathcal{J} \tilde{55}$  e o segundo implica que  $\tilde{55} \leq_{\mathcal{J}} \tilde{w}$ . Assim  $\tilde{w} \mathcal{J} \tilde{55}$  e o item 1 do corolário 5.3 implica que  $w \mathcal{D}' 55$  já que o monóide  $\mathcal{M}$  é estável.

As funções  $\#_u$  e  $\chi_U$  serão usadas para provar que duas palavras dadas não são congruentes ou não estão na mesma  $\mathcal{D}'$ -classe. Dois casos

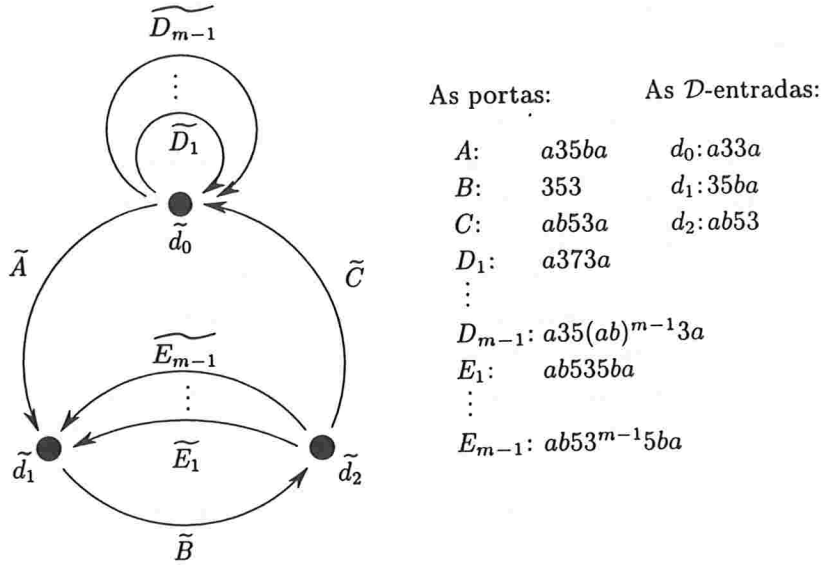


Figura 8.1: O grafo  $G$

requerem uma prova especial, contudo. Nós devemos provar que  $35(ab)^i3 \mathcal{P}'$   $55 \mathcal{P}' b53^i5b$  para  $i = 1, 2, \dots, m - 1$ . Estas provas são um tanto técnicas e não serão completamente feitas aqui. No caso de  $35(ab)^i3$ , nós provamos que qualquer palavra na classe de congruência de  $35(ab)^i3$  possui exatamente um fator maximal de período  $ab$  com ao menos quatro letras. No caso de  $b53^i5b$ , nós provamos que existem exatamente dois tais fatores na classe de congruência de  $b53^i5b$  e que eles são não contíguos. Estes fatos implicam que  $55$  não pode ser um fator de nenhuma palavra na classe de congruência de  $35(ab)^i3$  ou na classe de congruência de  $b53^i5b$  e que  $35(ab)^i3 \mathcal{P}' 55 \mathcal{P}' b53^i5b$ .

Vamos provar que as palavras  $d_0, d_1$  e  $d_2$  são  $\mathcal{D}$ -entradas na  $\mathcal{D}'$ -classe de  $55$ . Vamos primeiro provar que as palavras  $d_0, d_1$  e  $d_2$  estão na  $\mathcal{D}'$ -classe de  $55$ . Todas elas são fatores de  $555$  e portanto fatores de  $555^m \sim 55$ . Dado que  $55$  é um fator de  $(ab)^{2+m}(ba)^{2+m} \sim (ab)^2(ba)^2 = a33a = d_0$ , que  $55$  é um fator de  $355^m ba = (3ba)^{2+m} \sim (3ba)^2 = 35ba = d_1$ , que  $55$  é um fator de  $ab55^m 3 = (ab3)^{2+m} \sim (ab3)^2 = ab53 = d_2$ , temos que as palavras  $d_0, d_1$  e  $d_2$  estão na  $\mathcal{D}'$ -classe de  $55$ . Agora, vamos provar que elas são  $\mathcal{D}$ -entradas. Desde que  $\chi_3(d_0) = 1 \neq 0 = \chi_3(d_0 a^{-1})$ , temos que  $d_0 \mathcal{P}' d_0 a^{-1}$ . Como  $\chi_1(d_0) = 1 \neq 0 = \chi_1(a^{-1} d_0)$ , temos que  $d_0 \mathcal{P}' a^{-1} d_0$ . Assim,  $(1, d_0, 1)$  é uma

ocorrência de  $\mathcal{D}$ -entrada e segue que  $d_0$  é uma  $\mathcal{D}$ -entrada. De modo análogo,  $\chi_1(d_1) = 1 \neq 0 = \chi_1(d_1 a^{-1})$  e  $\chi_2(d_1) = 1 \neq 0 = \chi_2(b^{-1} d_1)$  implicam que  $d_1$  é uma  $\mathcal{D}$ -entrada e  $\chi_2(d_2) = 1 \neq 0 = \chi_2(d_2 b^{-1})$  e  $\chi_3(d_2) = 1 \neq 0 = \chi_3(a^{-1} d_2)$  implicam que  $d_2$  é uma  $\mathcal{D}$ -entrada.

Vamos mostrar que  $\tilde{d}_0$ ,  $\tilde{d}_1$  e  $\tilde{d}_2$  são três vértices distintos do grafo fundamental  $\mathbf{G}'$ . De fato, como  $d_0$ ,  $d_1$  e  $d_2$  são  $\mathcal{D}$ -entradas na  $\mathcal{D}'$ -classe de 55, temos que  $\tilde{d}_0, \tilde{d}_1, \tilde{d}_2 \in V(\mathbf{G}')$  por definição. Para concluir, estes vértices são distintos pois:  $\#_{bb}(d_0) = 1 \neq 2 = \#_{bb}(d_1) = \#_{bb}(d_2)$  implica que  $d_1 \not\sim d_0 \not\sim d_2$ ; a congruência  $\sim$  preserva a primeira letra numa classe de congruência implica que  $d_2 \not\sim d_1$ .

Vamos provar que  $A$  é uma transição na  $\mathcal{D}'$ -classe de 55 e que  $\alpha(\tilde{A}) = \tilde{d}_0$  e  $\omega(\tilde{A}) = \tilde{d}_1$ . Como  $A$  é fator de  $b A 35^{m-1} = ba35ba35^{m-1} = 5555^{m-1} \sim 55$  e  $d_0 \mathcal{D}' 55$  é fator de  $d_0 bba = a33abba = a35ba = A$ , temos que  $A \mathcal{D}' 55$ . Ademais,  $A = a35ba = d_0 bba$  também implica que  $A \mathcal{R}' d_0$  devido ao item 2 do corolário 5.3. Assim  $\epsilon_R(A) = d_0$  pois  $d_0$  é uma  $\mathcal{R}$ -entrada devido à proposição 5.5. De forma análoga,  $A = a35ba = ad_1$  implica que  $A \mathcal{L}' d_1$  devido ao item 3 do corolário 5.3. Assim  $\epsilon_L(A) = d_1$  pois  $d_1$  é uma  $\mathcal{L}$ -entrada devido à proposição 5.5. Desde que  $\chi_1(a^{-1} A a^{-1}) = \chi_1(35b) = 0 \neq 1 = \chi_1(A)$ , segue que  $a^{-1} A a^{-1} \not\mathcal{P}' A$ . Como  $d_0$  é prefixo de  $d_0 b b = a35b = A a^{-1}$  que é prefixo de  $A \mathcal{R}' d_0$ , segue que  $A a^{-1} \mathcal{R}' A$ . Tendo em vista que  $a^{-1} A = 35ba = d_1 \mathcal{L}' A$ , temos por definição que  $A$  é uma transição. Assim  $\tilde{A} \in \mathbf{G}'$  e, por definição,  $\alpha(\tilde{A}) = \widetilde{\epsilon_R(A)} = \tilde{d}_0$  e  $\omega(\tilde{A}) = \widetilde{\epsilon_L(A)} = \tilde{d}_1$ .

Vamos provar que  $B$  é uma transição na  $\mathcal{D}'$ -classe de 55 e que  $\alpha(\tilde{B}) = \tilde{d}_1$  e  $\omega(\tilde{B}) = \tilde{d}_2$ . Como  $B$  é fator de  $ba B ab5^{m-1} = ba353ab5^{m-1} = 5555^{m-1} \sim 55$  e  $d_1 \mathcal{D}' 55$  é fator de  $d_1 b = 35bab = B$ , temos que  $B \mathcal{D}' 55$ . Ademais,  $B = 35bab = d_1 b$  também implica que  $B \mathcal{R}' d_1$  devido ao item 2 do corolário 5.3. Assim  $\epsilon_R(B) = d_1$  pois  $d_1$  é uma  $\mathcal{R}$ -entrada devido à proposição 5.5. De forma análoga,  $B = bab53 = bd_2$  implica que  $B \mathcal{L}' d_2$  devido ao item 3 do corolário 5.3. Assim  $\epsilon_L(B) = d_2$  pois  $d_2$  é uma  $\mathcal{L}$ -entrada devido à proposição 5.5. Desde que  $\chi_2(b^{-1} B b^{-1}) = \chi_2(ab5ba) = 0 \neq 1 = \chi_2(B)$ , segue que  $b^{-1} B b^{-1} \not\mathcal{P}' B$ . Como  $B b^{-1} = d_1 \mathcal{R}' B$  e  $b^{-1} B = d_2 \mathcal{L}' B$ , temos por definição que  $B$  é uma transição. Assim  $\tilde{B} \in \mathbf{G}'$  e, por definição,  $\alpha(\tilde{B}) = \widetilde{\epsilon_R(B)} = \tilde{d}_1$  e  $\omega(\tilde{B}) = \widetilde{\epsilon_L(B)} = \tilde{d}_2$ .

Vamos provar que  $C$  é uma transição na  $\mathcal{D}'$ -classe de 55 e que  $\alpha(\tilde{C}) = \tilde{d}_2$  e  $\omega(\tilde{C}) = \tilde{d}_0$ . Como  $C$  é fator de  $3 C b5^{m-1} = 3ab53ab5^{m-1} = 5555^{m-1} \sim 55$  e  $d_2 \mathcal{D}' 55$  é fator de  $d_2 a = ab53a = C$ , temos que  $C \mathcal{D}' 55$ .

Ademais,  $C = ab53a = d_2 a$  também implica que  $C \mathcal{R}' d_2$  devido ao item 2 do corolário 5.3. Assim  $\epsilon_R(C) = d_2$  pois  $d_2$  é uma  $\mathcal{R}$ -entrada devido à proposição 5.5. De forma análoga,  $C = ab53a = abbd_0$  implica que  $C \mathcal{L}' d_0$  devido ao item 3 do corolário 5.3. Assim  $\epsilon_L(C) = d_0$  pois  $d_0$  é uma  $\mathcal{L}$ -entrada devido à proposição 5.5. Desde que  $\chi_3(a^{-1}Ca^{-1}) = \chi_3(b53) = 0 \neq 1 = \chi_3(C)$ , segue que  $a^{-1}Ca^{-1} \not\mathcal{P}' C$ . Como  $d_0$  é sufixo de  $bbd_0 = bba33a = b53a = a^{-1}C$  que é sufixo de  $C \mathcal{L}' d_0$ , segue que  $a^{-1}C \mathcal{L}' C$ . Tendo em vista que  $Ca^{-1} = ab53 = d_2 \mathcal{R}' C$ , temos por definição que  $C$  é uma transição. Assim  $\tilde{C} \in \mathbf{G}'$  e, por definição,  $\alpha(\tilde{C}) = \widetilde{\epsilon_R(C)} = \tilde{d}_2$  e  $\omega(\tilde{C}) = \widetilde{\epsilon_L(C)} = \tilde{d}_0$ .

Vamos provar que as palavras  $D_i$ , para  $i = 1, 2, \dots, m - 1$ , estão na  $\mathcal{D}'$ -classe de 55. Fixemos  $i$  em  $\{1, 2, \dots, m - 1\}$ . Como  $d_0$  é um fator de  $d_0 b(ab)^i 3a = a33ab(ab)^i 3a = a35(ab)^i 3a = D_i$ , é suficiente provar que  $D_i$  é um fator de uma palavra na classe de congruência de 55. Note que  $5(ab)^i = b(ab)^{2+i} = (ba)^{2+i}b = (ba)^i 5$ . Sejam pois  $x = 5(ab)^i = (ba)^i 5$  e  $y = 5x5^{m-1}$ . Vamos primeiro provar por indução em  $k \geq 1$  que  $y^k \sim 5x^k 5^{m-1}$ . A base de indução segue da definição de  $y$ . Suponha pois que  $k \geq 2$  e que  $y^{k-1} \sim 5x^{k-1} 5^{m-1}$ . Note que  $x5^m x = (ba)^i 55^m 5(ab)^i \sim (ba)^i 5^m 5(ab)^i = xx$ . Assim temos que  $y^k = y^{k-1} y \sim 5x^{k-1} 5^{m-1} y = 5x^{k-1} 5^{m-1} 5x5^{m-1} = 5x^{k-2} x5^m x 5^{m-1} \sim 5x^{k-2} xx5^{m-1} = 5x^k 5^{m-1}$ , completando a primeira parte da prova. Tendo em vista que  $5 = (ba)^2 b \sim (ba)^{2+m} b = (ba)^{m-i} x$  e  $5 = b(ab)^2 \sim b(ab)^{2+m} = x(ab)^{m-i}$ , temos que  $y^m \sim 5x^m 5^{m-1} = 5x^m 5^{m-2} \sim (ba)^{m-i} xx^m x (ab)^{m-i} 5^{m-2} \sim (ba)^{m-i} xx(ab)^{m-i} 5^{m-2} \sim 555^{m-2} = 5^m$ . Para concluir, podemos verificar que  $D_i = a3x3a$  é um fator de  $5x5^{m-1} = y$ , que por sua vez é um fator de  $y^m 55 \sim 5^m 55 \sim 55$ .

Vamos provar que as palavras  $D_i$ , para  $i = 1, 2, \dots, m - 1$ , são transições na  $\mathcal{D}'$ -classe de 55 e que  $\alpha(\tilde{D}_i) = \omega(\tilde{D}_i) = \tilde{d}_0$ . Fixemos  $i$  em  $\{1, 2, \dots, m - 1\}$ . Como  $d_0 \mathcal{D}' 55 \mathcal{D}' D_i$  e  $d_0 b(ab)^i 3a = a33ab(ab)^i 3a = a35(ab)^i 3a = D_i$  temos que  $D_i \mathcal{R}' d_0$  devido ao item 2 do corolário 5.3. Assim  $\epsilon_R(D_i) = d_0$  pois  $d_0$  é uma  $\mathcal{R}$ -entrada devido à proposição 5.5. Como  $D_i a^{-1} = d_0 b(ab)^i 3$  é um prefixo de  $D_i$  de comprimento maior que  $\epsilon_R(D_i) = d_0$ , temos que  $D_i a^{-1} \mathcal{R}' D_i$ . De forma análoga, como  $d_0 \mathcal{D}' D_i$  e  $a3b(ab)^i d_0 = a3b(ab)^i a33a = a3b(ab)^i (ab)^2 3a = a3b(ab)^2 (ab)^i 3a = a35(ab)^i 3a = D_i$  temos que  $D_i \mathcal{L}' d_0$  devido ao item 3 do corolário 5.3. Assim  $\epsilon_L(D_i) = d_0$  pois  $d_0$  é uma  $\mathcal{L}$ -entrada devido à proposição 5.5. Como  $a^{-1}D_i = 3b(ab)^i d_0$  é um sufixo de  $D_i$  de comprimento maior que  $\epsilon_L(D_i) = d_0$ , temos que  $a^{-1}D_i \mathcal{L}' D_i$ . Tendo em vista que  $a^{-1}D_i \mathcal{L}' D_i \mathcal{R}' D_i a^{-1}$  e que  $a^{-1}D_i a^{-1} = 35(ab)^i 3 \not\mathcal{P}' 55 \mathcal{D}' D_i$  como discutido antes,  $D_i$  é uma transição por definição. Assim

$\widetilde{D}_i \in \mathbf{G}'$  e, por definição,  $\alpha(\widetilde{D}_i) = \epsilon_R(\widetilde{D}_i) = \widetilde{d}_0$  e  $\omega(\widetilde{D}_i) = \epsilon_L(\widetilde{D}_i) = \widetilde{d}_0$ .

Vamos provar que as palavras  $E_i$ , para  $i = 1, 2, \dots, m-1$ , estão na  $\mathcal{D}'$ -classe de 55. Fixemos  $i$  em  $\{1, 2, \dots, m-1\}$ . Desde que  $d_2 \mathcal{D}' 55$  e  $d_2$  é um fator de  $d_2 3^{i-1} 5ba = ab5 33^{i-1} 5ba = ab53^i 5ba = E_i$  é suficiente provar que  $E_i$  é um fator de uma palavra na classe de congruência de 55.<sup>1</sup> Vamos primeiro provar que  $3(53^i)^m 53 \sim 353$ . Desde que 3 é simultaneamente um prefixo e um sufixo de 5, temos que  $35 \sim 3^m 35$  e  $53 \sim 533^m$ . Assim temos  $3(53^i)^m 53 \sim 3^m 3(53^i)^m 533^m = 3^{m-i}(33^i ba)(33^i ba)^m(33^i ba)b3^{m-i} \sim 3^{m-i}(33^i ba)(33^i ba)b3^{m-i} = 3^m 3533^m \sim 353$ , completando pois a primeira parte da prova. Isto imediatamente implica que  $555 \sim 5(53^i)^m 55$ . Observe também que  $3^i 53^i = 3^{i-1}(3ba)(3ba)b3^{i-1} \sim 3^{i-1}(3ba)(3ba)^m(3ba)b3^{i-1} = 3^i 5^m 53^i$ . Donde,  $55 \sim 5^{m-1} 555 \sim 5^{m-1} 5(53^i)^m 55 = 5^m(53^i)^{m-2} 5 3^i 53^i 55 \sim 5^m(53^i)^{m-2} 53^i 5^m 53^i 55 = (5^m(53^i)^{m-1} 5^{m-1}) 55 3^i 55 = z 55(3^i 55)$  onde  $z = 5^m(53^i)^{m-1} 5^{m-1}$ . Aplicando novamente, temos então que  $55 \sim z(55)(3^i 55) \sim z^2 55(3^i 55)^2 \sim z^2 55(3^i 55)^2(3^i 55)^m \sim 55(3^i 55)^m$ . Por fim, desde que  $E_i$  é um fator de  $55(3^i 55)^m \sim 55$ , completamos a prova de que  $E_i \mathcal{D}' 55$ .

Vamos provar que as palavras  $E_i$ , para  $i = 1, 2, \dots, m-1$ , são transições na  $\mathcal{D}'$ -classe de 55 e que  $\alpha(\widetilde{E}_i) = \widetilde{d}_2$  e  $\omega(\widetilde{E}_i) = \widetilde{d}_1$ . Fixemos  $i$  em  $\{1, 2, \dots, m-1\}$ . Como  $d_2 \mathcal{D}' 55 \mathcal{D}' E_i$  e  $d_2 3^{i-1} 5ba = ab5 33^{i-1} 5ba = ab53^i 5ba = E_i$  temos que  $E_i \mathcal{R}' d_2$  devido ao item 2 do corolário 5.3. Assim  $\epsilon_R(E_i) = d_2$  pois  $d_2$  é uma  $\mathcal{R}$ -entrada devido à proposição 5.5. Como  $E_i a^{-1} = d_2 3^{i-1} 5b$  é um prefixo de  $E_i$  de comprimento maior que  $\epsilon_R(E_i) = d_2$ , temos que  $E_i a^{-1} \mathcal{R}' E_i$ . De forma análoga, como  $d_1 \mathcal{D}' 55 \mathcal{D}' E_i$  e  $ab53^{i-1} d_1 = ab5 33^{i-1} 5ba = ab53^i 5ba = E_i$  temos que  $E_i \mathcal{L}' d_1$  devido ao item 3 do corolário 5.3. Assim  $\epsilon_L(E_i) = d_1$  pois  $d_1$  é uma  $\mathcal{L}$ -entrada devido à proposição 5.5. Como  $a^{-1} E_i = b53^{i-1} d_1$  é um sufixo de  $E_i$  de comprimento maior que  $\epsilon_L(E_i) = d_1$ , temos que  $a^{-1} E_i \mathcal{L}' E_i$ . Tendo em vista que  $a^{-1} E_i \mathcal{L}' E_i \mathcal{R}' E_i a^{-1}$  e que  $a^{-1} E_i a^{-1} = b53^i 5b \mathcal{D}' 55 \mathcal{D}' E_i$  como discutido antes,  $E_i$  é uma transição por definição. Assim  $\widetilde{E}_i \in \mathbf{G}'$  e, por definição,  $\alpha(\widetilde{E}_i) = \epsilon_R(\widetilde{E}_i) = \widetilde{d}_2$  e  $\omega(\widetilde{E}_i) = \epsilon_L(\widetilde{E}_i) = \widetilde{d}_1$ .

Vamos provar que  $\widetilde{A}, \widetilde{B}, \widetilde{C}, \widetilde{D}_i, \widetilde{E}_i$ , para  $i \in \{1, 2, \dots, m-1\}$ , são arestas distintas do grafo fundamental  $\mathbf{G}'$ . Por ora, fixemos  $i \in \{1, 2, \dots, m-1\}$ . Como cada uma das palavras  $A, B, C, D_i$  e  $E_i$  são transições na  $\mathcal{D}'$ -

<sup>1</sup>A prova deste fato é relativamente curta, apesar de ser mais complexa que no caso de  $D_i$ . É um tanto simples para ser verificada, mesmo que tenha sido difícil obter sua prova. A existência das palavras  $E_i$  na  $\mathcal{D}'$ -classe de 55, fato revelado através de nossas computações, era inesperada por nós.

classe de  $\tilde{55}$ , temos por definição que  $\tilde{A}$ ,  $\tilde{B}$ ,  $\tilde{C}$ ,  $\tilde{D}_i$  e  $\tilde{E}_i$  são arestas do grafo fundamental  $\mathbf{G}'$ . Elas são naturalmente distintas pois as funções de incidência assumem valores distintos em cada uma destas cinco transições:  $\alpha(\tilde{A}) = \tilde{d}_0$  e  $\omega(\tilde{A}) = \tilde{d}_1$ ;  $\alpha(\tilde{B}) = \tilde{d}_1$  e  $\omega(\tilde{B}) = \tilde{d}_2$ ;  $\alpha(\tilde{C}) = \tilde{d}_2$  e  $\omega(\tilde{C}) = \tilde{d}_0$ ;  $\alpha(\tilde{D}_i) = \omega(\tilde{D}_i) = \tilde{d}_0$ ;  $\alpha(\tilde{E}_i) = \tilde{d}_2$  e  $\omega(\tilde{E}_i) = \tilde{d}_1$ . Falta-nos apenas provar que  $\tilde{D}_i \neq \tilde{D}_j$  e que  $\tilde{E}_i \neq \tilde{E}_j$  para distintos  $i$  e  $j$  em  $\{1, 2, \dots, m-1\}$ . Assim, considere  $i \in \{1, 2, \dots, m-1\}$  qualquer e  $j \in \{1, 2, \dots, m-1\} \setminus \{i\}$ . Como  $\#_a(D_i) = 6 + i \neq 6 + j = \#_a(D_j)$ , temos que  $D_i \not\sim D_j$ . Desde que  $\#_a(E_i) = 6 + i \neq 6 + j = \#_a(E_j)$ , temos que  $E_i \not\sim E_j$ , concluindo pois nossa prova.

Isto completa a prova de que o grafo  $\mathbf{G}$  é um subgrafo do grafo fundamental  $\mathbf{G}'$ . ■

Observe que o número ciclomático do grafo  $\mathbf{G}$  é  $2m - 1$ . No corolário 8.2 usamos as informações do grafo fundamental da  $\mathcal{D}$ -classe de  $\tilde{55}$  para inferir propriedades das  $\mathcal{H}$ -classes desta  $\mathcal{D}$ -classe.

**Corolário 8.2** *Todos os grupos maximais na  $\mathcal{D}$ -classe de  $\tilde{55}$  são grupos de Burnside livres satisfazendo  $x^m = 1$  com ao menos  $2m - 1$  geradores. Para  $m$  suficientemente grande, estes grupos são infinitos e as classes de congruência de  $A^*$  projetadas sobre elementos desta  $\mathcal{D}$ -classe não são reconhecíveis.*

*Prova.* Seja  $\mathbf{G}'$  o grafo fundamental da  $\mathcal{D}$ -classe de  $\tilde{55}$ . O grafo  $\mathbf{G}$  apresentado na figura 8.1 é fortemente conexo e podemos escolher a árvore conectora  $\mathbf{T} = \{\tilde{A}, \tilde{B}\}$  com início  $\tilde{d}_0$ . Assim o número ciclomático de  $\mathbf{G}$  é  $|\mathbf{G}| - |\mathbf{T}| = (2(m-1) + 3) - 2 = 2m - 1$ . O teorema 8.1 implica que  $\mathbf{G}$  é um subgrafo de  $\mathbf{G}'$ . A proposição 2.4 implica que o número ciclomático de  $\mathbf{G}'$  é pelo menos  $2m - 1$ . Usando o teorema 7.6, segue então que os grupos maximais na  $\mathcal{D}$ -classe de  $\tilde{55}$  são grupos de Burnside livres satisfazendo  $x^m = 1$  com ao menos  $2m - 1$  geradores. O restante segue do fato de que estes grupos são infinitos para  $m$  suficientemente grande como discutido no capítulo 1 e da proposição 7.8. ■

No corolário 8.3 exibimos um conjunto gerador de cardinalidade  $2m - 1$  para um grupo de Burnside livre satisfazendo  $x^m = 1$  contido na  $\mathcal{H}$ -classe de  $\tilde{55}$ . Observe que  $5(ab)^i$  é o prefixo de  $(ba)^{2+m}$  de comprimento  $5 + 2i$ .

**Corolário 8.3** *Seja  $x_i = \widetilde{5(ab)^i}$  definido para  $i = 1, \dots, m-1$  e seja o conjunto  $H = \{\widetilde{5^{m+1}}, \widetilde{5x_1 5^{m-1}}, \dots, \widetilde{5x_{m-1} 5^{m-1}}, \widetilde{5^2 35^{2m-1}}, \dots, \widetilde{5^2 3^{m-1} 5^{2m-1}}\}$ . Então  $H$  tem cardinalidade  $2m-1$  e o subsemigrupo de  $\mathcal{M}$  gerado por  $H$  é um grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por  $H$  e sua identidade é o idempotente  $\widetilde{5^m}$ .*

*Prova.* Seja  $e = 5^m$ . Assim  $\tilde{e} = \widetilde{5^m} = \widetilde{5^{m+m}} = \widetilde{5^m 5^m} = \tilde{e}\tilde{e}$  e  $\tilde{e}$  é um idempotente de  $\mathcal{M} \setminus \{1\}$ . Note que  $e \mathcal{H}' 55$  pois  $55 \sim e55 = 55e$  e  $e = 55 5^{m-2} = 5^{m-2} 55$ . Seja pois  $\mathbf{G}'$  o grafo fundamental de  $\tilde{e}$ . Seja  $\mathbf{G}$  o grafo definido na figura 8.1 e sejam as  $\mathcal{D}$ -entradas e as transições definidas naquela figura. Temos que  $\{\tilde{A}, \tilde{B}\}$  e  $\{\tilde{B}, \tilde{C}\}$  são árvores conectoras de  $\mathbf{G}$  com início  $\tilde{d}_0$  e término  $\tilde{d}_0$  respectivamente. Definimos  $\mathbf{X} = \mathbf{G} \setminus \{\tilde{A}, \tilde{B}\}$ . Pelo teorema 8.1 temos que  $\mathbf{G}$  é um subgrafo de  $\mathbf{G}'$  e usando o corolário 2.5 e seu dual, temos que existem árvores conectoras  $\mathbf{T} \subseteq \mathbf{G}'$  com início  $\tilde{d}_0$  e  $\mathbf{T}' \subseteq \mathbf{G}'$  com término  $\tilde{d}_0$  tais que  $\{\tilde{A}, \tilde{B}\} \subseteq \mathbf{T}$  e  $\{\tilde{B}, \tilde{C}\} \subseteq \mathbf{T}'$  e  $\mathbf{X} = \mathbf{G} \setminus \{\tilde{A}, \tilde{B}\} \subseteq \mathbf{G}' \setminus \mathbf{T}$ . Para todo vértice  $v \in V(\mathbf{G}')$ , sejam  $p_v$  o único passeio em  $\mathbf{T}$  de  $\tilde{d}_0$  a  $v$  e  $q_v$  o único passeio em  $\mathbf{T}'$  de  $v$  a  $\tilde{d}_0$ . Definimos a função  $\delta : \mathbf{G}' \setminus \mathbf{T} \rightarrow (\mathbf{G}')^*$  por  $\delta(b) = p_{\alpha(b)} b q_{\omega(b)} (p_{\omega(b)} q_{\omega(b)})^{m-1}$  e a função  $\varphi : \mathbf{G}' \setminus \mathbf{T} \rightarrow \mathcal{M}$  por  $\varphi(b) = \mu_{d_0} \tau(\delta(b)) \eta_{d_0}$  onde  $\mu_{d_0} = b$  e  $\eta_{d_0} = b5^{m-2}$ . Note que  $e = 5^m = 55 5^{m-2} = b a 33 a b 5^{m-2} = \mu_{d_0} d_0 \eta_{d_0}$ .

Usando o corolário 7.7 temos que  $\varphi$  é uma injeção e que a  $\mathcal{H}$ -classe de  $\tilde{e}$  é o grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por  $\varphi(\mathbf{G}' \setminus \mathbf{T})$  cuja cardinalidade é o número ciclomático de  $\mathbf{G}'$ .

Note que  $\mathbf{X} = \mathbf{G} \setminus \{\tilde{A}, \tilde{B}\} = \{\tilde{C}, \tilde{D}_1, \dots, \tilde{D}_{m-1}, \tilde{E}_1, \dots, \tilde{E}_{m-1}\}$ .

Vamos calcular  $\delta(x)$ , para todo  $x \in \mathbf{X}$ . Vamos primeiro calcular  $\delta(\tilde{C})$ . Assim temos que  $p_{\alpha(\tilde{C})} = p_{\tilde{d}_2} = (\tilde{A}, \tilde{B})$ , que  $p_{\omega(\tilde{C})} = p_{\tilde{d}_0} = 1_{\tilde{d}_0}$  e que  $q_{\omega(\tilde{C})} = q_{\tilde{d}_0} = 1_{\tilde{d}_0}$ . Portanto  $\delta(\tilde{C}) = p_{\alpha(\tilde{C})}(\tilde{C}) q_{\omega(\tilde{C})} (p_{\omega(\tilde{C})} q_{\omega(\tilde{C})})^{m-1} = (\tilde{A}, \tilde{B}, \tilde{C})$ . Fixemos  $i \in \{1, \dots, m-1\}$ . Vamos agora calcular  $\delta(\tilde{D}_i)$ . Como  $\alpha(\tilde{D}_i) = \omega(\tilde{D}_i) = \tilde{d}_0$ , como  $p_{\tilde{d}_0} = q_{\tilde{d}_0} = 1_{\tilde{d}_0}$ , temos pois que  $\delta(\tilde{D}_i) = (\tilde{D}_i)$ . Por fim, vamos calcular  $\delta(\tilde{E}_i)$ . Observe que  $p_{\alpha(\tilde{E}_i)} = p_{\tilde{d}_2} = (\tilde{A}, \tilde{B})$ , que  $q_{\omega(\tilde{E}_i)} = q_{\tilde{d}_1} = (\tilde{B}, \tilde{C})$  e que  $p_{\omega(\tilde{E}_i)} = p_{\tilde{d}_1} = (\tilde{A})$ . Assim temos que  $\delta(\tilde{E}_i) = (\tilde{A}, \tilde{B}, \tilde{E}_i, \tilde{B}, \tilde{C})(\tilde{A}, \tilde{B}, \tilde{C})^{m-1}$ .

Vamos definir palavras  $w_x$  tais que  $\sigma(w_x) = \delta(x)$  e que  $\epsilon_R(w_x) = \epsilon_L(w_x) = d_0$ , para todo  $x \in \mathbf{X}$ . Seja  $w_{\tilde{C}} = A(\epsilon_R(B)^{-1}B)(\epsilon_R(C)^{-1}C) = a35ba b a = b^{-1} 555 b^{-1}$ . A partir do item 2 da proposição 5.12 temos que



a seqüência de transições de  $w_{\tilde{C}}$  é  $A, B, C$  e a partir do item 1 temos que  $w_{\tilde{C}} \mathcal{D}' A \mathcal{D}' e$ . Portanto  $\sigma(w_{\tilde{C}}) = (\tilde{A}, \tilde{B}, \tilde{C}) = \delta(\tilde{C})$ . Usando o item 3 da proposição 5.12 temos que  $\epsilon_R(w_{\tilde{C}}) = \epsilon_R(A) = d_0$  e usando o item 4 da mesma proposição temos que  $\epsilon_L(w_{\tilde{C}}) = \epsilon_L(C) = d_0$ . Fixemos  $i \in \{1, \dots, m-1\}$ . Seja  $w_{\tilde{D}_i} = D_i = b^{-1} 5x_i 5 b^{-1}$ . Como  $w_{\tilde{D}_i} = D_i$  é uma transição na  $\mathcal{D}'$ -classe de  $e$ , temos que a seqüência de transições de  $w_{\tilde{D}_i}$  é  $D_i$  e portanto  $\sigma(w_{\tilde{D}_i}) = (\tilde{D}_i) = \delta(\tilde{D}_i)$ . Usando o item 3 da proposição 5.12 temos que  $\epsilon_R(w_{\tilde{D}_i}) = \epsilon_R(D_i) = d_0$  e usando o item 4 da mesma proposição temos que  $\epsilon_L(w_{\tilde{D}_i}) = \epsilon_L(D_i) = d_0$ . Por fim, seja  $w_{\tilde{E}_i} = A(\epsilon_R(B)^{-1}B)(\epsilon_R(E_i)^{-1}E_i)(\epsilon_R(B)^{-1}B)(\epsilon_R(C)^{-1}C)((\epsilon_R(A)^{-1}A)(\epsilon_R(B)^{-1}B)(\epsilon_R(C)^{-1}C))^{m-1} = a35ba b 3^{i-1} 5ba b a (bba b a)^{m-1} = b^{-1} 553^i 555^{m-1} b^{-1}$ . A partir do item 2 da proposição 5.12, a seqüência de transições de  $w_{\tilde{E}_i}$  é  $A, B, E_i, B, C, (A, B, C)^{m-1}$  e  $w_{\tilde{E}_i} \mathcal{D}' A \mathcal{D}' e$  devido ao item 1 da mesma proposição. Portanto  $\sigma(w_{\tilde{E}_i}) = (\tilde{A}, \tilde{B}, \tilde{E}_i, \tilde{B}, \tilde{C})(\tilde{A}, \tilde{B}, \tilde{C})^{m-1} = \delta(\tilde{C})$ . Usando o item 3 da proposição 5.12 temos que  $\epsilon_R(w_{\tilde{E}_i}) = \epsilon_R(A) = d_0$  e usando o item 4 da mesma proposição temos que  $\epsilon_L(w_{\tilde{E}_i}) = \epsilon_L(C) = d_0$ .

Observe que  $H = \{\mu_{d_0} \widetilde{w_x \eta_{d_0}} \mid x \in \mathbf{X}\}$ .

Vamos provar que  $\mu_{d_0} \widetilde{w_x \eta_{d_0}} = \varphi(x)$ , para todo  $x \in \mathbf{X}$ . Fixemos um particular  $x \in \mathbf{X}$ . Da definição de  $\delta$ , todo passeio da forma  $\delta(b)$  para  $b \in \mathbf{G}' \setminus \mathbf{T}$  é tal que  $\alpha(\delta(b)) = \alpha(p_{\alpha(b)}) = \tilde{d}_0 = \omega(q_{\omega(b)}) = \omega(\delta(b))$ . Devido aos itens 3 e 4 da proposição 6.11, temos então que  $\epsilon_R(\tau(\delta(x))) = \tau(1_{\alpha(\delta(x))}) = \tau(1_{\tilde{d}_0}) = \tau(1_{\omega(\delta(x))}) = \epsilon_L(\tau(\delta(x)))$ . Como  $\tau(1_{\tilde{d}_0}) \sim d_0 = \epsilon_R(w_x) = \epsilon_L(w_x)$ , segue então que  $\epsilon_R(\tau(\delta(x))) \sim \epsilon_R(w_x)$  e que  $\epsilon_L(\tau(\delta(x))) \sim \epsilon_L(w_x)$ . Como vimos antes,  $\delta(x) = \sigma(w_x)$  e portanto, usando o item 2 da proposição 6.11, temos que  $\sigma(\tau(\delta(x))) = \delta(x) = \sigma(w_x)$ . Podemos pois usar o teorema 7.5 de modo a obter  $\tau(\delta(x)) = \tilde{w}_x$ . Assim temos que  $\mu_{d_0} \widetilde{w_x \eta_{d_0}} = \tilde{\mu}_{d_0} \tilde{w}_x \tilde{\eta}_{d_0} = \tilde{\mu}_{d_0} \tau(\delta(x)) \tilde{\eta}_{d_0} = \mu_{d_0} \tau(\delta(x)) \eta_{d_0} = \varphi(x)$ , o que conclui nossa prova.

Por fim, tendo em vista que  $\mathbf{X} \subseteq \mathbf{G}' \setminus \mathbf{T}$ , concluímos então que  $H = \{\mu_{d_0} \widetilde{w_x \eta_{d_0}} \mid x \in \mathbf{X}\} = \{\varphi(x) \mid x \in \mathbf{X}\} = \varphi(\mathbf{X}) \subseteq \varphi(\mathbf{G}' \setminus \mathbf{T})$  e a cardinalidade de  $H$  é  $|H| = |\varphi(\mathbf{X})| = |\mathbf{X}| = 2m - 1$  pois  $\varphi$  é injetiva em  $\mathbf{G}' \setminus \mathbf{T} \supseteq \mathbf{X}$ . ■

Usando complexos resultados computacionais, nós verificamos que o grafo apresentado na figura 8.1 é o próprio grafo fundamental da  $\mathcal{D}$ -classe em questão para os casos  $m = 2$  e  $m = 3$ . Uma prova geral deste fato depende de resultados combinatórios que devem ser ainda caracterizados. Para o caso  $m = 2$ , podemos obter um resultado análogo ao corolário 8.2

independentemente do teorema 7.6. Neste caso,  $2m - 1 = 3$  e podemos exibir três palavras na  $\mathcal{H}'$ -classe de 55 cujas classes de congruência geram um grupo isomorfo ao grupo de Burnside livre satisfazendo  $x^2 = 1$  gerado por um conjunto de três geradores. Este grupo livre é isomorfo a  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$  e as palavras em questão são 555, 575 e 55355. O subgrupo gerado através de suas classes de congruência é  $\{\widetilde{55}, \widetilde{555}, \widetilde{575}, \widetilde{55355}, \widetilde{5755}, \widetilde{555355}, \widetilde{575355}, \widetilde{5755355}\}$  e pode-se provar que eles são diferentes uns dos outros analisando os valores de  $\#_a$ ,  $\#_b$  e  $\#_{bbabb}$ . Estes fatos motivam-nos a seguinte conjectura:

**Conjectura 1** *O grafo fundamental da  $\mathcal{D}$ -classe de  $\widetilde{55}$  é o grafo  $\mathbf{G}$  apresentado na figura 8.1.*

## 8.2 Duas palavras curtas congruentes

A proposição 8.4 mostrar-nos-á um exemplo de uma classe de congruência, no caso  $n = 2$ ,  $m = 2$ , que possui duas palavras mais curtas. Este resultado contrasta completamente com aquele visto no teorema 7.3 [10], onde demonstra-se serem únicas as palavras de menor comprimento numa classe de congruência projetada sobre elementos de um monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  em que  $n \geq 3$  e  $m \geq 1$ .

**Proposição 8.4** *Sejam os inteiros  $n = 2$  e  $m = 2$  e o grafo  $\mathbf{G}$  definido na figura 8.1. Sejam  $p = (\widetilde{A}, \widetilde{B}, \widetilde{C})$  e  $q = (\widetilde{D}_1)$  dois passeios em  $\mathbf{G}$ . Então as palavras  $\tau(pq)$  e  $\tau(qp)$  são duas diferentes palavras de menor comprimento na mesma classe de congruência.*

*Prova.* Seja  $\mathbf{G}'$  o grafo fundamental de  $\widetilde{55}$ . Do teorema 8.1 temos que  $\mathbf{G}$  é um subgrafo de  $\mathbf{G}'$ . Da proposição 6.8 temos que o grafo fundamental  $\mathbf{G}'$  é fortemente conexo. Seja pois  $\mathcal{B}$  o grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por  $\mathbf{G}'$ . Sejam ainda definidos  $u = \widetilde{d}_0$  um vértice de  $\mathbf{G}'$ ,  $\mathcal{K} = \mathbf{G}'^*$  a categoria livre gerada por  $\mathbf{G}'$ ,  $\widehat{\phantom{x}}$  a projeção canônica de  $\mathcal{K}$  sobre  $\mathcal{B}$  e  $\cong$  a congruência em  $\mathcal{K}$  associada a este morfismo. Assim  $p = (\widetilde{A}, \widetilde{B}, \widetilde{C}) \in \mathcal{K}_u$  e  $q = (\widetilde{D}_1) \in \mathcal{K}_u$ . Seja  $B$  o conjunto de arestas  $\{\widetilde{A}, \widetilde{B}, \widetilde{C}, \widetilde{D}_1\}$ .

Note que  $\tau(pq) \neq \tau(qp)$ , até porque o item 2 da proposição 6.11 implica que  $\sigma(\tau(pq)) = pq \neq qp = \sigma(\tau(qp))$ .

Vamos provar que  $\tau(pq) \sim \tau(qp)$  e que  $|\tau(pq)| = |\tau(qp)|$ . De fato, deduzimos que  $\tau(pq) \sim \tau(qp)$  devido ao teorema 7.5 já que usando o

item 2 da proposição 6.11 temos que  $\sigma(\tau(pq)) = pq \cong (qp)^2pq = qpqppq \cong qpqq \cong qp = \sigma(\tau(qp))$  e usando os itens 3 e 4 da mesma proposição temos que  $\epsilon_R(\tau(pq)) = \epsilon_L(\tau(pq)) = \epsilon_R(\tau(qp)) = \epsilon_L(\tau(qp)) = \tau(1_u)$ . Ademais, usando o item 7 da proposição 6.11 temos que  $|\tau(pq)| = |\tau(1_u)| + \sum_{b \in B} |\epsilon_R(\tau(b))^{-1}\tau(b)| = |\tau(qp)|$ .

Vamos provar que  $\tau(pq)$  é uma palavra mais curta em sua classe de congruência. Seja  $w$  uma palavra qualquer tal que  $w \sim \tau(pq)$ . Usando o teorema 7.5, temos que  $\sigma(w) \cong \sigma(\tau(pq)) = pq$  devido ao item 2 da proposição 6.11, o que também implica que  $\alpha(\sigma(w)) = \alpha(pq)$ . Como  $\sigma(w) \cong pq$  e  $\cong$  preserva as funções da forma  $\#_b$  para  $b \in \mathbf{G}'$  devido à proposição 4.1 temos então que  $\#_b(\sigma(w)) = \#_b(pq) = 1$  para todo  $b \in B$ . Usando o item 6 da proposição 6.11 temos pois que  $w \geq \tau(\sigma(w))$  e portanto que  $|w| \geq |\tau(\sigma(w))| \geq |\tau(1_{\alpha(\sigma(w))})| + \sum_{b \in B} |\epsilon_R(\tau(b))^{-1}\tau(b)| = |\tau(1_{\alpha(pq)})| + \sum_{b \in B} |\epsilon_R(\tau(b))^{-1}\tau(b)| = |\tau(pq)|$ .

Para concluir, vimos que  $\tau(pq) \neq \tau(qp)$ , que  $\tau(pq) \sim \tau(qp)$ , que  $|\tau(pq)| = |\tau(qp)|$  e que qualquer palavra na classe de congruência de  $\tau(pq)$  tem comprimento ao menos  $|\tau(pq)|$ . ■

De fato, pode-se provar que  $d_0, d_1, d_2, A, B, C, D_i$  e  $E_i$  são as únicas palavras de menor comprimento em suas respectivas classes de congruência. Isto implica que  $\tau((\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})) = b^{-1}5575b^{-1}$  e  $\tau((\tilde{D}, \tilde{A}, \tilde{B}, \tilde{C})) = b^{-1}5755b^{-1}$ .



## Capítulo 9

### Os casos $n = 1$ e $n \geq 3$

Neste capítulo aplicaremos os resultados principais deste trabalho a semigrupos de Burnside livres cujas estruturas são bastante conhecidas. Suporemos  $A$  um alfabeto qualquer e inteiros  $n$  e  $m$  inteiros tais que  $n \geq 1$  e  $m \geq 1$ . Suporemos  $\mathcal{M}$  o monóide de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$  e  $\sim$  o morfismo canônico  $\tilde{\sim} : A^* \rightarrow \mathcal{M}$  e  $\sim$  a congruência de Burnside associada.

Na seção 9.1 consideraremos o caso  $n = 1$  e caracterizaremos os grafos fundamentais das  $\mathcal{D}$ -classes de  $\mathcal{M} \setminus \{\tilde{1}\}$  no teorema 9.2. Em particular, calcularemos seu número ciclomático. Por ora, fixemos  $n = 1$  e  $m \geq 1$ . Para todo inteiro  $k \geq 1$ , supondo conhecida a cardinalidade de  $B(k, m)$ , o grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um conjunto de  $k$  geradores, calcularemos no corolário 9.3 a cardinalidade de cada  $\mathcal{J}$ -classe de  $\mathcal{M}$  — e portanto a cardinalidade do próprio monóide de Burnside  $\mathcal{M}$ . Isto implica que conheçamos a cardinalidade de  $\mathcal{M}$  em função de  $|A|$  nos casos  $m \leq 3$ , por exemplo. Em 1954, McLean [26] deu uma descrição da cardinalidade de  $\mathcal{M}$  em função de  $|A|$  para o caso  $n = m = 1$  (banda livre com  $|A|$  geradores). Generalizamos este resultado para qualquer  $m \geq 1$  em que a cardinalidade de  $B(k, m)$  seja conhecida. Para  $m$  suficientemente grande e três geradores em  $A$  ao menos, verificamos que em  $\mathcal{M}$  existe uma  $\mathcal{J}$ -classe com um número infinito de  $\mathcal{R}$ -classes e de  $\mathcal{L}$ -classes. Ademais, toda  $\mathcal{H}$ -classe nesta  $\mathcal{J}$ -classe é um grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um conjunto infinito de geradores. No corolário 9.4 veremos um resultado de Kadourek e Polák [19] que reduz o problema da palavra em  $\mathcal{M}$  ao problema da palavra num grupo de Burnside livre  $B(k, m)$  para  $k$  finito. Isto implica que o problema da palavra seja decidível em  $\mathcal{M}$  mesmo em casos em que  $\mathcal{M}$

é infinito, como nos casos em que  $m \geq 665$  é ímpar ou em que  $m \geq 8000$  é um múltiplo de 16.

Na seção 9.2 daremos uma nova demonstração do teorema 8.16 [10] que prova que os grupos maximais de  $\mathcal{M} \setminus \{\tilde{1}\}$  são todos cíclicos de ordem  $m$  quando  $n \geq 3$ . Para tanto caracterizaremos no teorema 9.5 o grafo fundamental de uma  $\mathcal{D}$ -classe regular de  $\mathcal{M} \setminus \{\tilde{1}\}$  e provaremos que ele é um circuito. O teorema 9.5 fará uso extensivo de resultados presentes em nosso trabalho [10] que tratam da estrutura destes semigrupos.

## 9.1 O caso $n = 1$

Suporemos ao longo desta seção que  $n = 1$  e que  $m \geq 1$  é um inteiro fixado qualquer. Caracterizaremos o grafo fundamental de uma  $\mathcal{D}$ -classe qualquer de  $\mathcal{M}$  no teorema 9.2. Em particular, calcularemos seu número ciclomático e, por conseguinte, a cardinalidade da  $\mathcal{J}$ -classe em questão e do monóide  $\mathcal{M}$ . Estes cálculos são feitos recursivamente na cardinalidade do conjunto de geradores e supõem conhecidas a cardinalidade de um grupo de Burnside livre satisfazendo  $x^m = 1$ , dada a cardinalidade do conjunto de geradores. Isto implica que conheçamos a cardinalidade de  $\mathcal{M}$  em função de  $|A|$  nos casos  $m \leq 3$ , por exemplo.

Dados  $X \subseteq \mathcal{M}$  e  $W \subseteq A^*$  dizemos que  $W$  é uma representação de  $X$  se  $\sim$  estabelece uma bijeção entre  $W$  e  $X$ . Dada uma palavra  $w \in A^*$ , a classe de congruência  $\tilde{w}$  é um elemento de  $\mathcal{M}$  e definimos a função  $\text{rep} : \mathcal{M} \rightarrow A^*$ , chamada *representante*, como sendo

$\text{rep}(\tilde{w})$  é a menor palavra na classe de congruência  $\tilde{w}$ .

Note que  $\text{rep}(X) = \{\text{rep}(x) \mid x \in X\}$  é uma particular representação de  $X$  onde  $\sim$  estabelece uma bijeção entre  $\text{rep}(X)$  e  $X$  e sua inversa é  $\text{rep}$ . Observe que  $\text{rep}(\mathcal{M})$  é fechada por fatores, já que todo fator de uma menor palavra em sua classe de congruência deve ser ele próprio um menor fator em sua classe de congruência. Devido ao item 1 da proposição 6.1, toda  $\mathcal{J}$ -classe de  $\mathcal{M}$  pode ser associada a um subconjunto de  $B \subseteq A$  de tal forma que a  $\mathcal{J}'$ -classe associada a esta  $\mathcal{J}$ -classe seja o conjunto das palavras de conteúdo  $B$ . Esta associação será feita estensivamente nesta seção. Dado um sub-alfabeto  $B \subseteq A$ , definimos

$$M(B, m) \stackrel{\text{def}}{=} \text{rep}(\tilde{B}^*),$$

o conjunto dos representantes do monóide de Burnside livre satisfazendo  $x = x^{1+m}$  gerado por  $B$ , que é um submonóide de  $\mathcal{M}$ . Também definimos

$$J(B, m) \stackrel{\text{def}}{=} \{w \in \text{rep}(\mathcal{M}) \mid c(w) = B\},$$

o subconjunto de  $M(B, m)$  formado pelas palavras de conteúdo  $B$ . Definimos ainda

$$\mathbf{G}(B, m) \stackrel{\text{def}}{=} \text{ o grafo fundamental de } J(B, m),$$

como também definimos

$$B(k, m),$$

o grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um conjunto de  $k \geq 0$  geradores. Por fim, dado um inteiro  $k \geq 0$  e  $B_k$  um subalfabeto de  $A$  com cardinalidade  $k$ , definimos as cardinalidades:

$$J_{k,m} \stackrel{\text{def}}{=} |J(B_k, m)| \quad (9.1)$$

$$\mathbf{G}_{k,m} \stackrel{\text{def}}{=} |\mathbf{G}(B_k, m)| \quad (9.2)$$

$$M_{k,m} \stackrel{\text{def}}{=} |M(B_k, m)| \quad (9.3)$$

$$B_{k,m} \stackrel{\text{def}}{=} |B(k, m)|. \quad (9.4)$$

Na proposição 9.1 caracterizamos as  $\mathcal{R}$ -entradas de uma  $\mathcal{D}'$ -classe, calculando assim quantas  $\mathcal{R}$ -classes possui uma  $\mathcal{J}$ -classe de  $\mathcal{M}$ .

**Proposição 9.1** *Seja  $J$  uma  $\mathcal{J}$ -classe de  $\mathcal{M}$  e seja  $B \subseteq A$  o conteúdo que caracteriza  $J$ . Então o conjunto das  $\mathcal{R}$ -entradas de palavras em  $\text{rep}(J)$  é*

$$\epsilon_R(\text{rep}(J)) = \{wa \mid a \in B, w \in J(B \setminus \{a\}, m)\} \subseteq \text{rep}(J)$$

e a função que aplica  $w \in \epsilon_R(\text{rep}(J))$  na  $\mathcal{R}$ -classe de  $\tilde{w}$  estabelece uma bijeção entre  $\epsilon_R(\text{rep}(J))$  e o conjunto das  $\mathcal{R}$ -classes de  $J$ .

*Prova.* Vamos provar que  $\epsilon_R(\text{rep}(J)) \subseteq \text{rep}(J)$ . Seja  $x \in J$ . Como  $\text{rep}(\mathcal{M})$  é fechada por fatores, temos que  $\epsilon_R(\text{rep}(x)) \in \text{Pref}(\text{rep}(x)) \subseteq \text{rep}(\mathcal{M})$ . Para terminar, basta observar que  $x = \text{rep}(x) \mathcal{R} \epsilon_R(\text{rep}(x))$  implica que  $\epsilon_R(\text{rep}(x)) \in J$  e também que  $\epsilon_R(\text{rep}(x)) = \text{rep}(\epsilon_R(\text{rep}(x))) \subseteq \text{rep}(J)$ .

Vamos provar que a função que aplica  $w \in \epsilon_R(\text{rep}(J))$  na  $\mathcal{R}$ -classe de  $\tilde{w}$  estabelece uma bijeção entre  $\epsilon_R(\text{rep}(J))$  e o conjunto das  $\mathcal{R}$ -classes

de  $J$ . Sejam  $x, y \in J$ . É suficiente provar que  $x \mathcal{R} y \iff \epsilon_R(\text{rep}(y)) = \epsilon_R(\text{rep}(x))$ . Dado que  $\epsilon_R(\text{rep}(x)), \epsilon_R(\text{rep}(y)) \in \text{rep}(J)$ , temos  $\epsilon_R(\text{rep}(x)) \sim \epsilon_R(\text{rep}(y)) \iff \epsilon_R(\text{rep}(x)) = \epsilon_R(\text{rep}(y))$ . Como  $\text{rep}(x) = x$ , usando o teorema 6.3 segue que  $x \mathcal{R} y \iff \text{rep}(x) \mathcal{R} \text{rep}(y) \iff \text{rep}(x) \mathcal{R}' \text{rep}(y) \iff \epsilon_R(\text{rep}(x)) \sim \epsilon_R(\text{rep}(y)) \iff \epsilon_R(\text{rep}(y)) = \epsilon_R(\text{rep}(x))$ .

Vamos provar que  $\epsilon_R(\text{rep}(J)) = \{wa \mid a \in B, w \in J(B \setminus \{a\}, m)\}$ . Seja  $ua \in \epsilon_R(\text{rep}(J))$  uma  $\mathcal{R}$ -entrada, com  $a \in A$ . Do item 3 da proposição 6.1, temos que  $a \notin c(u)$ . Como  $\widetilde{ua} \in J$ , temos que  $c(ua) = B$ . Assim  $c(u) = B \setminus \{a\}$ . Como  $\text{rep}(M)$  é fechada por fatores, temos que  $u \in \text{Pref}(ua) \subseteq \text{Pref}(\text{rep}(J)) \subseteq \text{rep}(M)$ . Portanto  $u \in J(B \setminus \{a\}, m)$  por definição. Isto prova que  $\epsilon_R(\text{rep}(J)) \subseteq \{wa \mid a \in B, w \in J(B \setminus \{a\}, m)\}$ . Seja agora uma palavra  $vb$ , com  $b \in B$  e  $v \in J(B \setminus \{b\}, m)$ . Do item 3 da proposição 6.1 temos que  $vb$  é uma  $\mathcal{R}$ -entrada. Como  $c(vb) = c(v) \cup c(b) = B \setminus \{b\} \cup \{b\} = B$ , temos que  $\widetilde{vb} \in J$ . Do item 4 da proposição 6.1 logo segue que  $vb$  é a menor palavra em sua classe de congruência se e só se  $v$  o for. Como  $v \in J(B \setminus \{b\}, m)$  o é,  $vb = \text{rep}(\widetilde{vb}) \in \text{rep}(J)$ . Isto prova que  $\{wa \mid a \in B, w \in J(B \setminus \{a\}, m)\} \subseteq \epsilon_R(\text{rep}(J))$ . ■

No teorema 9.2 caracterizamos o grafo fundamental de uma  $\mathcal{D}$ -classe do semigrupo de Burnside livre satisfazendo  $x = x^{1+m}$ . Na figura 9.1 vemos uma aplicação deste teorema à  $\mathcal{D}$ -classe de  $\widetilde{ab}$ . Observe que o número ciclomático do grafo fundamental desta  $\mathcal{D}$ -classe é  $2m - 1$ . Na figura 9.2 vere-

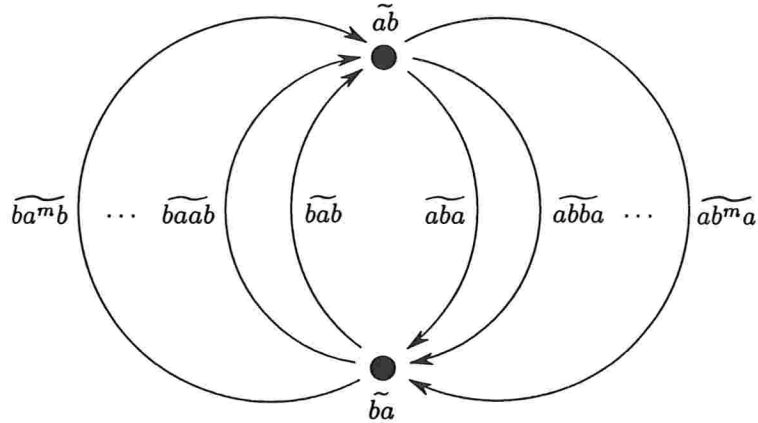


Figura 9.1: Grafo fundamental da  $\mathcal{D}$ -classe de  $\widetilde{ab}$

mos uma aplicação deste teorema à  $\mathcal{D}$ -classe de  $\widetilde{abc}$ . Observe que o número



de vértices do grafo fundamental desta  $\mathcal{D}$ -classe é  $6m$  e o número de arestas é  $12m^2 B_{2m-1,m}$ . Para o caso  $m = 1$  temos número ciclomático  $12 - 6 + 1 = 7$  e este é exatamente o grafo fundamental visto na figura 6.2. Para  $m = 2$ , teremos  $12 \times 2^2 \times 2^3 - 6 \times 2 + 1 = 384 - 12 + 1 = 373$ . Para  $m \geq 8000$ , temos que  $B_{2m-1,m}$  é infinito e o número ciclomático do grafo fundamental em questão é infinito. Isto implica que as  $\mathcal{H}$ -classes da  $\mathcal{D}$ -classe de  $\widetilde{abc}$  são grupos de Burnside livres satisfazendo  $x^m = 1$ . Estes grupos já seriam infinitos se houvessem apenas dois geradores. Neste caso, o próprio número de geradores destes grupos de Burnside livres é infinito. A proposição 9.1 e sua dual implicam que há infinitas  $\mathcal{R}$ -classes e infinitas  $\mathcal{L}$ -classes nesta  $\mathcal{D}$ -classe.

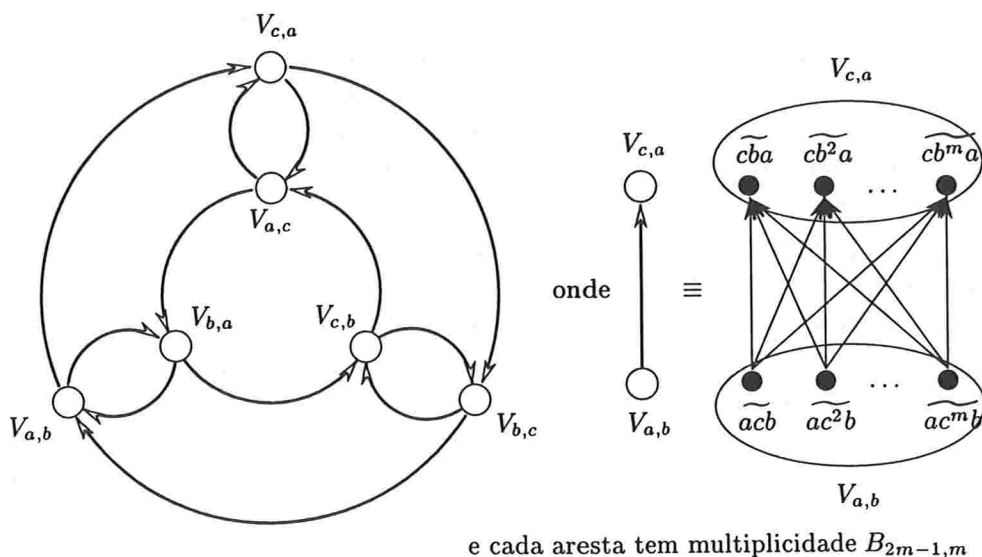


Figura 9.2: Grafo fundamental da  $\mathcal{D}$ -classe de  $\widetilde{abc}$

**Teorema 9.2** *Seja um inteiro  $m \geq 1$ . Seja  $J$  uma  $\mathcal{J}$ -classe de um semigrupo de Burnside livre satisfazendo  $x = x^{1+m}$  gerado por um alfabeto  $A$  e seja  $B \subseteq A$  o conteúdo associado a  $J$ . Seja  $\mathbf{G} = \mathbf{G}(B, m)$  o grafo fundamental de  $J$ . Se  $B = \{a\}$  então  $V(\mathbf{G}) = \{\widetilde{a}\}$  e  $E(\mathbf{G}) = \{\widetilde{aa}\}$ . Se  $|B| \geq 2$ , então*

$V(\mathbf{G})$  e  $E(\mathbf{G})$  possuem as representações

$$\begin{aligned} \text{rep}(V(\mathbf{G})) &= \{awb \mid a \in B, b \in B \setminus \{a\}, w \in J(B \setminus \{a, b\}, m)\}, \\ \text{rep}(E(\mathbf{G})) &= \{awa \mid a \in B, w \in J(B \setminus \{a\}, m)\}. \end{aligned}$$

Ademais, dados dois vértices  $\tilde{u}, \tilde{v} \in V(\mathbf{G})$ , existe uma aresta de  $\tilde{u}$  a  $\tilde{v}$  se e só se a primeira letra de  $u$  for a última letra de  $v$  e, neste caso, existem exatamente  $B_{(\mathbf{G}_{|B|-1}, m), m}$  arestas de  $\tilde{u}$  a  $\tilde{v}$ .

*Prova.* Seja  $\mathcal{M} \setminus \{1\}$  o semigrupo livre em questão. Usando o item 1 da proposição 6.1, podemos definir  $D$  a  $\mathcal{D}'$ -classe que projeta na  $\mathcal{D}$ -classe em questão e temos que  $D = \{w \in A^* \mid c(w) = B\}$ .

Suponha que  $B = \{a\}$ . O item 1 da proposição 6.2 garante-nos que a única  $\mathcal{D}$ -entrada em  $D$  é  $a$ . O item 2 da mesma proposição, por sua vez, implica que  $aa$  é a única transição. Assim  $V(\mathbf{G}) = \{\tilde{a}\}$  e  $E(\mathbf{G}) = \{\tilde{aa}\}$ . Observe que o número ciclomático de  $\mathbf{G}$  é  $|E(\mathbf{G})| - |V(\mathbf{G})| + 1 = 1 - 1 + 1 = 1$ . A propósito, a  $\mathcal{D}$ -classe em questão possui uma única  $\mathcal{H}$ -classe e é  $\{\tilde{a}, \tilde{aa}, \dots, \tilde{a}^m\}$ , com cardinalidade  $m = B_{1, m}$ .

Suponha a partir de agora que  $|B| \geq 2$ . Procuraremos calcular as representações  $\text{rep}(V(\mathbf{G}))$  e  $\text{rep}(E(\mathbf{G}))$ .

Vamos provar que  $\text{rep}(V(\mathbf{G}))$  é calculada como sendo  $\text{rep}(V(\mathbf{G})) = \{awb \mid a \in B, b \in B \setminus \{a\}, w \in J(B \setminus \{a, b\}, m)\}$ . A partir do item 1 da proposição 6.2 temos que as  $\mathcal{D}$ -entradas em  $D$  são da forma  $aub$ , com  $a, b \in B$  e  $a \neq b$  e  $c(u) = B \setminus \{a, b\}$ . Por outro lado, duas tais  $\mathcal{D}$ -entradas  $aub$  e  $a'u'b'$  são congruentes se e só se  $a = a'$  e  $b = b'$  e  $u \sim u'$ , devido ao corolário 6.5. Ademais, o mesmo corolário implica que  $aub$  é a menor  $\mathcal{D}$ -entrada em sua classe de congruência se e só se for também a menor palavra nesta classe se e só se  $u$  for a menor palavra em sua classe de congruência. Isto implica que  $aub \in \text{rep}(V(\mathbf{G}))$  se e só se  $a, b \in B$  e  $a \neq b$  e  $c(u) = B \setminus \{a, b\}$  e  $u = \text{rep}(\tilde{u})$  se e só se  $aub \in \{awb \mid a \in B, b \in B \setminus \{a\}, w \in J(B \setminus \{a, b\}, m)\}$ .

Vamos provar que  $\text{rep}(E(\mathbf{G})) = \{awa \mid a \in B, w \in J(B \setminus \{a\}, m)\}$ . O item 2 da proposição 6.2 garante-nos que as transições em  $D$  são as palavras da forma  $aua$  com  $a \in A$  e  $u \in B^*$  e  $c(u) = B \setminus \{a\}$ . Por outro lado, duas tais transições  $aua$  e  $a'u'a'$ , com  $a, a' \in B$ , são congruentes se e só se  $a = a'$  e  $u \sim u'$  devido ao corolário 7.4. Ademais, o mesmo corolário implica que uma tal transição  $aua$  é a menor transição em sua classe de congruência se e só se  $aua = \text{rep}(\tilde{aua})$  se e só se  $u = \text{rep}(\tilde{u})$  se e só se  $aua \in \{awa \mid a \in B, w \in J(B \setminus \{a\}, m)\}$ .

Vamos finalizar a prova. Sejam  $\tilde{u}, \tilde{v} \in V(\mathbf{G})$ . Dado que  $\sim$  preserva a primeira e a última letra das palavras, podemos supôr que  $u, v \in \text{rep}(V(\mathbf{G}))$ . Suponha que existam  $a \in B$  e  $u', v' \in B^*$  tais que  $u = au'$  e  $v = v'a$ . Como vimos antes,  $c(u') = c(v') = B \setminus \{a\} = c(u'v')$  e a proposição 6.2 garante-nos que  $uv = au'v'a$  é uma transição na mesma  $\mathcal{D}'$ -classe de  $u$ . Como  $u$  e  $v$  são  $\mathcal{D}$ -entradas de  $uv$ , temos que  $\epsilon_R(uv) = u$  e  $\epsilon_L(uv) = v$  devido à proposição 5.9. Por definição,  $\tilde{u}\tilde{v}$  é uma aresta de  $\mathbf{G}$  com início em  $\tilde{u}$  e término em  $\tilde{v}$ . Suponha a partir de agora que  $awa \in \text{rep}(E(\mathbf{G}))$  seja tal que  $\widetilde{awa}$  seja uma aresta de  $\mathbf{G}$  com início em  $\tilde{u}$  e término em  $\tilde{v}$ . Pelo corolário 7.4 temos que  $\widetilde{awa}$  é uma transição. Portanto  $\widetilde{awa}$  é uma aresta de  $\mathbf{G}$  com início em  $\epsilon_R(awa) = \tilde{u}$  e término em  $\epsilon_L(awa) = \tilde{v}$ . Usando a proposição 6.10 temos que  $\epsilon_R(awa)$  e  $\epsilon_L(awa)$  são as menores palavras em suas respectivas classes de congruência. Bem como o são  $u$  e  $v$ . Assim,  $u = \epsilon_R(awa) \in \text{Pref}(awa)$  tem  $a$  por primeira letra e  $v = \epsilon_L(awa) \in \text{Suf}(awa)$  tem  $a$  por última letra. Para terminar, falta-nos provar que há exatamente  $B_{(\mathbf{G}_{|B|-1,m},m)}$  arestas de  $\tilde{u}$  a  $\tilde{v}$ . Sejam  $u', v' \in B^*$  tais que  $u = au'$  e  $v = v'a$ . Como vimos antes,  $c(u') = c(v') = B \setminus \{a\} = c(w)$ . Ademais, não é difícil provar que  $u' = \epsilon_R(w) = \epsilon_R(w')$  e que  $v' = \epsilon_L(w) = \epsilon_L(w')$  para toda palavra  $w' \in J(B \setminus \{a\}, m)$  tal que  $w' \mathcal{H}' w$ . Assim os possíveis valores de  $w$  são as palavras de  $J(B \setminus \{a\}, m)$  que estão na  $\mathcal{R}'$ -classe de  $u'$  e na  $\mathcal{L}'$ -classe de  $v'$ . O restante segue do fato que a cardinalidade de uma  $\mathcal{H}'$ -classe em  $J(B \setminus \{a\}, m)$  é  $B_{(\mathbf{G}_{|B|-1,m},m)}$ , devido ao teorema 7.6. ■

No corolário 9.3 calculamos a cardinalidade exata de  $\mathcal{M}$ ,  $M_{|A|,m}$ , para todo  $m$  tal que  $B_{k,m}$  seja conhecido para todo  $k$ . Este resultado generaliza aquele de McLean [26].

**Corolário 9.3** *Seja um inteiro  $m \geq 1$ . Suponha conhecida a cardinalidade  $B_{k,m}$  em função de  $k$  e de  $m$ , para todo  $k$ . Então as seguintes cardinalidades podem ser calculadas de forma recorrente:*

$$J_{k,m} = \begin{cases} 1 & \text{se } k = 0; \\ (kJ_{k-1,m})^2 B_{(\mathbf{G}_{k,m},m)} & \text{se } k \geq 1; \end{cases} \quad (9.5)$$

$$\mathbf{G}_{k,m} = \begin{cases} 1 & \text{se } k = 1; \\ kJ_{k-1,m} - k(k-1)J_{k-2,m} + 1 & \text{se } k \geq 2; \end{cases} \quad (9.6)$$

$$M_{k,m} = \sum_{i=0}^k \binom{k}{i} J_{i,m}. \quad (9.7)$$

*Prova.* Considere as definições feitas no teorema 9.2. Seja  $k$  a cardinalidade de  $B$ .

Vamos provar a equação 9.5. Observe que  $J(\emptyset, m) = \{1\}$  e que portanto  $J_{0,m} = 1$ . Suponhamos pois que  $B \neq \emptyset$ . Usando a proposição 9.1, temos que  $\epsilon_R(\text{rep}(J)) = \{wa \mid a \in B, w \in J(B \setminus \{a\}, m)\}$  e que existe uma bijeção entre  $\epsilon_R(\text{rep}(J))$  e o conjunto das  $\mathcal{R}$ -classes de  $J$ . Assim,  $J$  possui  $|\epsilon_R(\text{rep}(J))| = |\{wa \mid a \in B, w \in J(B \setminus \{a\}, m)\}| = |B| \times |J(B \setminus \{a\}, m)| = kJ_{k-1,m}$   $\mathcal{R}$ -classes. De forma dual,  $J$  possui  $kJ_{k-1,m}$   $\mathcal{L}$ -classes e, portanto,  $(kJ_{k-1,m})^2$   $\mathcal{H}$ -classes. Por outro lado, devido ao teorema 7.6 e ao fato de que toda  $\mathcal{H}$ -classe em  $J$  possui um idempotente, cada  $\mathcal{H}$ -classe de  $J$  é um grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um conjunto com  $\mathbf{G}_{|B|,m}$  geradores, possuindo então cardinalidade  $B_{\mathbf{G}_{k,m},m}$ . Assim  $J_{k,m} = |J| = (kJ_{k-1,m})^2 B_{\mathbf{G}_{k,m},m}$ .

Vamos provar a equação 9.6. Suponha que  $B \neq \emptyset$  e seja  $k$  a cardinalidade de  $B$ . Assim é definido o grafo fundamental de  $J$  e, pelo teorema 9.2, o mesmo possui  $|\{awb \mid a \in B, b \in B \setminus \{a\}, w \in J(B \setminus \{a, b\}, m)\}| = |B| \times |B \setminus \{a\}| \times |J(B \setminus \{a, b\}, m)| = k(k-1)J_{k-2,m}$  vértices. Do mesmo teorema, o referido grafo possui  $|\{awa \mid a \in B, w \in J(B \setminus \{a\}, m)\}| = |B| \times |J(B \setminus \{a\}, m)| = kJ_{k-1,m}$  arestas. Assim o número ciclomático de  $\mathbf{G}(B, m)$  é  $\mathbf{G}_{k,m} = kJ_{k-1,m} - k(k-1)J_{k-2,m} + 1$ .

Vamos provar a equação 9.7. O monóide  $M(B, m)$  possui  $2^k$   $\mathcal{J}$ -classes ao todo, correspondendo aos possíveis conteúdos associados às  $\mathcal{J}$ -classes. Suponha  $0 \leq i \leq k$ . Assim  $M(B, m)$  possui  $\binom{k}{i}$   $\mathcal{J}$ -classes cujo conteúdo associado tem cardinalidade  $i$ . Cada uma delas com cardinalidade  $J_{i,m}$ . Concluimos então que  $M_{k,m} = \sum_{i=0}^k \binom{k}{i} J_{i,m}$ . ■

Substituindo a equação 9.6 em 9.5 obtemos a equação 9.8:

$$J_{k,m} = \begin{cases} 1 & \text{se } k = 0; \\ m & \text{se } k = 1; \\ (kJ_{k-1,m})^2 B_{(kJ_{k-1,m} - k(k-1)J_{k-2,m} + 1), m} & \text{se } k \geq 1; \end{cases} \quad (9.8)$$

No corolário 9.4 veremos um resultado de Kađourek e Polák [19] que reduz o problema da palavra em  $\mathcal{M}$  ao problema da palavra num grupo de Burnside livre  $B(k, m)$  para  $k$  finito. Isto implica que o problema da palavra seja decidível em  $\mathcal{M}$  mesmo em casos em que  $\mathcal{M}$  é infinito, como nos casos em que  $m \geq 665$  é ímpar ou em que  $m \geq 8000$  é um múltiplo de 16. Apesar de ser infinito  $B(k, m)$  para quaisquer  $m \geq 8000$  e  $k \geq 2$ , não se sabe correntemente se o problema da palavra é decidível em todos estes casos.

**Corolário 9.4** *Seja um inteiro  $m \geq 1$ . Suponha decidível o problema da palavra num grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um conjunto finito. Então é decidível o problema da palavra num monóide de Burnside livre satisfazendo  $x = x^{m+1}$  gerado por um conjunto finito.*

*Prova.* Sejam  $w, w' \in A^*$ . Queremos decidir se  $w \sim w'$ . Do item 1 da proposição 6.1 temos que  $w \mathcal{J}' w' \iff c(w) = c(w')$ . O conteúdo de uma palavra é trivialmente calculável. Caso  $c(w) \neq c(w')$ , forçosamente temos que  $w \not\sim w'$ . Suponha pois, a partir de agora, que  $c(w) = c(w')$ . Faremos uma indução em  $|c(w)|$ . Se  $c(w) = \emptyset$ , então  $w = w' = 1$  e não mais há o que fazer. Suponha pois que o problema seja solúvel para quaisquer palavras com conteúdo estritamente menor que  $c(w)$ . Como  $\mathcal{J}'$  é efetivamente caracterizável pelo seu conteúdo, a partir da proposição 6.2 sabemos calcular a seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$  e de  $w'$ . A partir do lema 5.11 calculamos então a  $\mathcal{R}$ -entrada, a seqüência de transições e a  $\mathcal{L}$ -entrada de  $w$  e fazemos o mesmo para  $w'$ . A partir da nossa hipótese de indução e do teorema 6.3 podemos decidir se  $\epsilon_R(w) \sim \epsilon_R(w')$ . De forma dual, podemos decidir se  $\epsilon_L(w) \sim \epsilon_L(w')$ . De acordo com o teorema 7.5 falta-nos apenas decidir se  $\sigma(w) \cong \sigma(w')$ . A partir do corolário 7.4 e da nossa hipótese de indução, sabemos decidir se duas transições são congruentes ou não. De posse da seqüência de transições de  $w$  podemos então calcular sua digital  $\sigma(w)$  e da mesma forma podemos calcular  $\sigma(w')$ . Estes passeios são congruentes por  $\cong$  se e somente se, olhados como palavras no alfabeto finito  $B = \{b \mid b \text{ é uma aresta de } \sigma(w) \text{ ou de } \sigma(w')\}$ , estas palavras forem congruentes no grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por  $B$ . Como por hipótese, é decidível se  $\sigma(w)$  e  $\sigma(w')$  são congruentes neste grupo de Burnside, é também decidível se  $\sigma(w) \cong \sigma(w')$ . ■

## 9.2 O caso $n \geq 3$

Nesta seção suporemos  $n \geq 3$ . Daremos uma nova demonstração do teorema 8.16 [10] que prova que os grupos maximais de  $\mathcal{M}$  são cíclicos de ordem  $m$  quando  $n \geq 3$ . Este é o conteúdo do corolário 9.6, conseqüência de uma aplicação do teorema 7.6 ao teorema 9.5, que por sua vez caracteriza o grafo fundamental de uma  $\mathcal{D}$ -classe regular de  $\mathcal{M}$  e prova que ele é um circuito. Usaremos extensivamente os resultados presentes em nosso trabalho [10] em

sua demonstração. Veremos primeiro várias definições e resultados presentes em [10].

Definimos a *sobreposição* de duas palavras  $u$  e  $v$  por:  $u \rightleftharpoons v \stackrel{\text{def}}{=} \max(\text{Suf}(u) \cap \text{Pref}(v))$ . Em outras palavras, é o mais longo sufixo de  $u$  que é também um prefixo de  $v$ . Dizemos que  $u \in A^+$  (possivelmente mais comprido que  $w$ ) é um *período de  $w$*  se  $w$  for um fator de alguma potência de  $u$  (se  $w \in \text{Fat}(u^*) = \cup_k \text{Fat}(u^k)$ ). Neste caso, também dizemos que  $i = |u|$  é um *período de  $w$* . Se este inteiro  $i$  for também o menor inteiro possível dizemos que ele é o *menor período de  $w$*  e denotamos:  $i = \text{per}(w)$ . Neste caso, também dizemos que a palavra  $u$  é um *menor período de  $w$* . Note que se  $u$  for um período de  $w$  então  $u$  é um período de qualquer fator de  $w$ . Duas palavras  $w$  e  $w'$  são ditas *conjugadas* se existirem palavras  $u$  e  $v$  tais que  $w = uv$  e  $w' = vu$ . Uma palavra  $w$  é dita *primitiva* se  $w = u^k$  implica  $k = 1$  e  $u = w$ . Para todo par  $\tau = (l, s) \in A^+ \times A^+$  dizemos que  $l$  é o *longo de  $\tau$*  enquanto  $s$  é o *curto de  $\tau$* , respectivamente denotados por  $l_\tau$  e  $s_\tau$ . Definimos  $\Omega$ , uma relação em  $A^+$ , com segue:  $\Omega \stackrel{\text{def}}{=} \{(l, s) \mid s \text{ é simultaneamente um prefixo e um sufixo próprio de } l \text{ e } s^{-1}l \text{ é uma } m\text{-potência}\}$ . Cada elemento de  $\Omega$  é chamado de *produção*. Para toda produção  $\tau$  definimos a *base de  $\tau$*  por  $\text{bas}(\tau) \stackrel{\text{def}}{=} (|l_\tau| - |s_\tau|)/m$ . Também definimos a *base esquerda de  $\tau$* ,  $b_L(\tau)$ , pelo prefixo de  $l_\tau$  de comprimento  $\text{bas}(\tau)$ ; e a *base direita de  $\tau$* ,  $b_R(\tau)$ , pelo sufixo de  $l_\tau$  de comprimento  $\text{bas}(\tau)$ . Podemos ver um exemplo destas definições na figura 9.3. Definimos uma ordem parcial  $\preceq$  em  $\Omega \times \Omega$  por

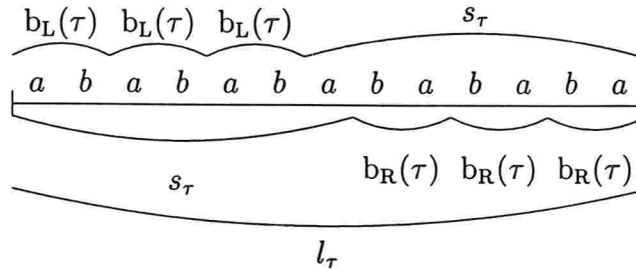


Figura 9.3: Exemplo de uma produção de base 2 em que  $m = 3$

$(l, s) \preceq (l', s') \stackrel{\text{def}}{\iff} \exists u, v \in A^+ \mid l' = ulv \text{ e } s' = usv$ . Como as bases direita e esquerda de uma mesma produção são palavras conjugadas, o seguinte conceito é bem definido: duas produções  $\tau$  e  $\sigma$  são *conjugadas* se  $b_R(\tau)$

(ou  $b_L(\tau)$ ) e  $b_R(\sigma)$  (ou  $b_L(\sigma)$ ) são conjugadas. Dizemos que a produção  $\tau$  é *estável* se  $\text{per}(s_\tau) = \text{bas}(\tau)$ . Um conjunto de produções é dito *estável* se toda produção dele for estável. Dadas uma palavra  $w$  e uma produção  $\sigma$  definimos a relação  $\text{era}_{\text{suff}}$  como  $\sigma \text{ era}_{\text{suff}} w \stackrel{\text{def}}{\iff} |w \Rightarrow l_\sigma| > |s_\sigma|$  e, neste caso, dizemos que  $\sigma$  *apaga um sufixo de  $w$* . Assim, podemos definir  $\dashv : A^* \times \Omega \longrightarrow A^*$  a operação binária *apagamento de sufixo* por

$$w \dashv \sigma \stackrel{\text{def}}{=} \begin{cases} (w(w \Rightarrow l_\sigma)^{-1}) s_\sigma & \text{se } \sigma \text{ era}_{\text{suff}} w; \\ w & \text{caso contrário.} \end{cases}$$

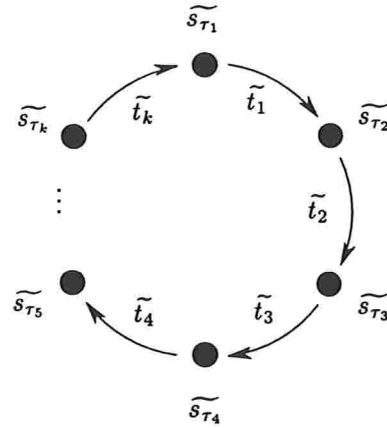
Neste caso dizemos que  $w \dashv \sigma$  é *w apagado à direita por  $\sigma$* .

Um leitor mais interessado pode encontrar a definição de  $\Sigma$ , uma relação em  $A^+$ , na seção 4.5 [10]. Para nós, são suficientes alguns resultados sobre  $\Sigma$ . A proposição 4.9 [10] por exemplo implica que  $\Sigma \subseteq \Omega$ , que as produções de  $\Sigma$  são minimais por  $\preceq$  e que suas bases direita e esquerda são primitivas. Como  $n \geq 3$ , a partir do teorema 6.7 [10] e do corolário 6.11 [10] temos que  $\Sigma$  é estável. Em [10] o estudo de  $\mathcal{M} \setminus \{\tilde{1}\}$  é feito através de seu isomorfo  $\mathcal{S}$  definido na seção 8.2 [10]. O conjunto  $\mathcal{S}$  é o conjunto de todas as palavras de  $A^+$  que são mínimas em suas respectivas classes de congruência e o produto de duas palavras  $u, v \in \mathcal{S}$  é a menor palavra na classe de congruência de  $uv$ . A partir do teorema 7.3 [10] temos que  $\mathcal{S}$  é o conjunto formado por todas as palavras de  $A^+$  que não possuem nenhum longo de  $\Sigma$  entre seus fatores ( $\Sigma$  é um sistema de Reescritura [16, 20] com a propriedade de Church-Rosser e portanto toda classe de congruência possui um único elemento na forma normal: o menor elemento da classe). O conjunto  $\mathcal{S}$  é fechado por fatores não vazios e a proposição 3.1 [10] implica que todo fator próprio não vazio de uma produção em  $\Sigma$  está em  $\mathcal{S}$ .

**Teorema 9.5** *Sejam inteiros  $n \geq 3$  e  $m \geq 1$ . O grafo fundamental de uma  $\mathcal{D}$ -classe regular de um semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  é um circuito como o da figura 9.4.*

*Prova.* Pretendemos caracterizar o grafo fundamental de uma  $\mathcal{D}$ -classe regular de  $\mathcal{M} \setminus \{\tilde{1}\}$ . Antes veremos duas afirmativas referentes às produções de  $\Sigma$  que serão usadas livremente nesta demonstração.

Afirmamos que  $b_L(\sigma) \in \text{Pref}(s_\sigma)$  e que  $s_\sigma \in \text{Pref}(b_L(\sigma)^*)$  para toda produção  $\sigma \in \Sigma$ . De fato, como estamos supondo que  $n \geq 3$  e portanto  $\sigma$  é estável, temos que  $|b_L(\sigma)| = \text{bas}(\sigma) = \text{per}(s_\sigma) \leq |s_\sigma|$  e portanto  $b_L(\sigma) \in$



$\tau_1, \dots, \tau_k$  formam um conjunto maximal de produções conjugadas de  $\Sigma$  em que  $s_{\tau_i}$  é a  $i$ -ésima  $\mathcal{D}$ -entrada e  $t_i$  é a  $i$ -ésima transição de  $b_L(\tau_1)s_{\tau_1}$ , para  $i = 1, \dots, k$

Figura 9.4: Grafo fundamental de uma  $\mathcal{D}$ -classe regular para  $n \geq 3$

$\text{Pref}(s_\sigma)$  já que  $s_\sigma, b_L(\sigma) \in \text{Pref}(l_\sigma)$ . Pelo dual do corolário 3.4 [10] temos que  $s_\sigma \in \text{Pref}(b_L(\sigma)^*)$ .

Afirmamos que duas produções conjugadas  $\tau$  e  $\tau'$  em  $\Sigma$  são iguais se e só se  $b_L(\tau) = b_L(\tau')$  se e só se  $s_\tau \in \text{Fat}(s_{\tau'})$ . De fato, obviamente  $\tau = \tau'$  implica que  $b_L(\tau) = b_L(\tau')$  e que  $s_\tau \in \text{Fat}(s_{\tau'})$ . Suponha que  $s_\tau \in \text{Fat}(s_{\tau'})$ . Como  $b_L(\tau) \in \text{Pref}(s_\tau)$  implica que  $|b_L(\tau)| \leq |s_\tau|$ , a proposição 4.1 [10] implica que  $\tau \preceq \tau'$ . Como as produções de  $\Sigma$  são incomparáveis por  $\preceq$  por definição, temos que  $\tau = \tau'$ . Suponha agora que  $b_L(\tau) = b_L(\tau')$ . Assim,  $s_{\tau'}, s_\tau \in \text{Pref}(b_L(\tau)^*)$  e  $s_\tau \in \text{Fat}(s_{\tau'})$  ou  $s_{\tau'} \in \text{Fat}(s_\tau)$ . De qualquer forma, como acabamos de ver, segue que  $\tau = \tau'$ .

Vamos agora caracterizar os vértices de  $\mathbf{G}$ . Seja  $v \in V(\mathbf{G})$  e seja  $w_v \in A^+$  a menor  $\mathcal{D}$ -entrada tal que  $v = \widetilde{w}_v$ . Do corolário 6.5 temos que  $w_v$  é a menor palavra em sua classe de congruência e que portanto  $w_v \in \mathcal{S}$ . A partir do teorema 8.12 [10], temos que existe  $\mathcal{T} \subset \Sigma$  uma classe de produções conjugadas tais que  $\{w_v \mid v \in V(\mathbf{G})\} = \{s_\tau \mid \tau \in \mathcal{T}\}$ . Assim  $V(\mathbf{G}) = \{\widetilde{s}_\tau \mid \tau \in \mathcal{T}\}$ .

Seja  $k = |\mathcal{T}|$  e seja  $\tau_1$  uma produção qualquer escolhida em  $\mathcal{T}$ . Seja  $w = b_L(\tau_1)s_{\tau_1}$ . Afirmamos que  $w \mathcal{D}' s_{\tau_1}$ . De fato,  $\widetilde{s}_{\tau_1} = \widetilde{t}_{\tau_1} = b_L(\tau_1)^m s_{\tau_1} = b_L(\tau_1)^{m-1} \widetilde{w} \leq_{\mathcal{L}} \widetilde{w} = b_L(\tau_1) \widetilde{s}_{\tau_1} \leq_{\mathcal{L}} \widetilde{s}_{\tau_1}$  implica que  $s_{\tau_1} \mathcal{L}' w$ .

Afirmamos que toda  $\mathcal{D}$ -entrada de  $w$  está em  $\mathcal{S}$  e é da forma  $s_\tau$  para algum  $\tau \in \mathcal{T}$ . De fato, qualquer  $\mathcal{D}$ -entrada de  $w$  é fator próprio de



$w = b_L(\tau_1)s_{\tau_1} \in \text{Fat}(b_L(\tau_1)^m s_{\tau_1}) = \text{Fat}(l_{\tau_1})$  e pertence então a  $\mathcal{S}$ . A definição de  $\mathcal{T}$  e o fato de que  $w \mathcal{D}' s_{\tau_1}$  completam a prova.

Seja  $\tau \in \mathcal{T}$ . Sejam definidas as palavras  $u$  e  $v$  tais que  $b_L(\tau_1) = uv$  e  $b_L(\tau) = vu$ . Como  $b_L(\tau_1)$  e  $b_L(\tau)$  são palavras conjugadas, são também períodos das mesmas palavras devido ao lema 3.2 [10].

Vamos provar que  $s_\tau$  é um fator de  $w$ . Temos que  $w \in \text{Suf}(l_{\tau_1})$  tem período  $b_L(\tau_1)$  e portanto  $b_L(\tau) = vu$  é período de  $w$  e de seu sufixo  $v s_{\tau_1} = vuv(b_L(\tau)^{-1}s_{\tau_1})$ . Assim  $b_L(\tau)$  é período e prefixo de  $s_\tau$  e de  $vs_{\tau_1}$ . Usando o dual do corolário 3.4 [10], temos que  $s_\tau, vs_{\tau_1} \in \text{Pref}(b_L(\tau)^*)$  e portanto  $s_\tau \in \text{Pref}(vs_{\tau_1})$  ou  $vs_{\tau_1} \in \text{Pref}(s_\tau)$ . Caso  $s_\tau \in \text{Pref}(vs_{\tau_1}) \subseteq \text{Fat}(uvs_{\tau_1}) = \text{Fat}(w)$  a tese já está provada. Caso  $vs_{\tau_1} \in \text{Pref}(s_\tau)$ , temos que  $s_{\tau_1} \in \text{Fat}(s_\tau)$  e, a partir de afirmativa anterior, segue que  $\tau = \tau_1$  e  $s_\tau = s_{\tau_1} \in \text{Fat}(b_L(\tau_1)s_{\tau_1}) = \text{Fat}(w)$  provando a tese.

Vamos provar que existe uma única ocorrência de  $s_\tau$  como fator de  $w$ , a não ser que  $\tau = \tau_1$ , onde  $(1, s_\tau, s_\tau^{-1}w)$  e  $(ws_\tau^{-1}, s_\tau, 1)$  são as duas únicas ocorrências de  $s_\tau$  como fator de  $w$ . Suponha que  $(r', s_\tau, s')$  e  $(r, s_\tau, s)$  sejam duas ocorrências de  $s_\tau$  em  $w$ , com  $|s'| > |s|$  e  $|r'| < |r|$ . Seja  $x = s_\tau s' s^{-1} = r'^{-1}(r' s_\tau s') s^{-1} = r'^{-1}(r s_\tau s) s^{-1} = r'^{-1} r s_\tau$ . Devido à proposição 3.3 [10],  $x$  possui período  $s' s^{-1}$ . Note que  $x \in \text{Fat}(w) \subseteq \text{Fat}(l_{\tau_1})$  tem período  $b_L(\tau_1)$ , e portanto  $b_L(\tau)$ , e note que  $|x| = |s_\tau s' s^{-1}| = |s_\tau| + |s' s^{-1}| \geq |b_L(\tau)| + |s' s^{-1}|$ . Assim,  $b_L(\tau)$  é uma potência de uma palavra de comprimento  $\text{gcd}(|b_L(\tau)|, |s' s^{-1}|)$  devido ao teorema 3.1 [10]. Como  $b_L(\tau)$  é primitiva, temos pois que  $\text{gcd}(|b_L(\tau)|, |s' s^{-1}|) = |b_L(\tau)|$ . Como  $s_\tau \in \text{Fat}(s_{\tau_1})$  implica  $\tau = \tau_1$ , segue que  $s_\tau$  não pode ser fator próprio de  $s_{\tau_1}$ . Dado que  $rs_\tau s = w = b_L(\tau_1)s_{\tau_1}$  temos que  $|r| \leq |b_L(\tau_1)|$  e  $r \in \text{Pref}(b_L(\tau_1))$ . Dado que  $x = s_\tau s' s^{-1} = r'^{-1} r s_\tau$ , temos que  $|s' s^{-1}| = |r'^{-1} r| \leq |r| \leq |b_L(\tau_1)| = |b_L(\tau)| = \text{gcd}(|b_L(\tau)|, |s' s^{-1}|)$ . Assim,  $|r'^{-1} r| = |s' s^{-1}| = |b_L(\tau)| = |b_L(\tau_1)|$ . Como  $r \in \text{Pref}(b_L(\tau_1))$ , temos pois que  $r = b_L(\tau_1)$  e  $r' = 1$ . Assim  $b_L(\tau_1)s_\tau s = w = b_L(\tau_1)s_{\tau_1}$  implica que  $s_\tau \in \text{Fat}(s_{\tau_1})$  e, como vimos em afirmativa anterior, que  $\tau = \tau_1$ . Isto implica que  $s = w(rs_\tau)^{-1} = w(b_L(\tau_1)s_{\tau_1})^{-1} = 1$ . Concluindo,  $(r', s_\tau, s') = (1, s_\tau, s_\tau^{-1}w)$  e  $(r, s_\tau, s) = (ws_\tau^{-1}, s_\tau, 1)$  são as duas únicas ocorrências de  $s_\tau$  como fator de  $w$ .

Podemos pois nomear as diferentes produções de  $\mathcal{T}$  por  $\tau_1, \tau_2, \dots, \tau_k$  de tal forma que a  $i$ -ésima ocorrência de  $\mathcal{D}$ -entrada de  $w$  seja do fator  $s_{\tau_i}$ , para  $i \in \{1, 2, \dots, k\}$ . Seja  $z_{k+1} = z_1$ . Temos também que o comprimento da seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$  é  $k+1$  e a  $i$ -ésima  $\mathcal{D}$ -entrada a ocorrer em  $w$  é  $s_{\tau_i}$ , para  $i \in \{1, 2, \dots, k+1\}$ . Usando o lema 5.11, temos que existem exatamente  $k$  ocorrências de transições em  $w$ . Seja  $t_i$  a

$i$ -ésima transição a ocorrer em  $w$ . Do corolário 5.10 temos que  $\epsilon_R(t_i) = s_{\tau_i}$  e que  $\epsilon_L(t_i) = s_{\tau_{i+1}}$ , para  $i \in \{1, 2, \dots, k\}$ . Assim temos que  $\tilde{t}_i \in E(\mathbf{G})$  e  $\alpha(\tilde{t}_i) = \widetilde{s_{\tau_i}}$  e  $\omega(\tilde{t}_i) = \widetilde{s_{\tau_{i+1}}}$ , para  $i \in \{1, 2, \dots, k\}$ . As  $k$  arestas  $\tilde{t}_1, \dots, \tilde{t}_k$  são todas distintas entre si já que são aplicadas a diferentes vértices por  $\alpha$ .

Vamos provar que toda aresta  $\mathbf{G}$  é da forma  $\tilde{t}_i$ , para algum  $i \in \{1, 2, \dots, k\}$ . Seja  $b \in E(\mathbf{G})$  e seja  $t \in A^+$  a menor transição tal que  $b = \tilde{t}$ . Do corolário 7.4 temos que  $t$  é a menor palavra em sua classe de congruência e portanto  $t \in \mathcal{S}$ . Da proposição 6.10 temos que  $\epsilon_R(t)$  e  $\epsilon_L(t)$  são as menores  $\mathcal{D}$ -entradas em suas respectivas classes de congruência, que por sua vez são as menores palavras em suas classes de congruência devido ao corolário 6.5. Assim, temos que  $\epsilon_R(t), \epsilon_L(t) \in \mathcal{S}$ . Seja  $\tau_i \in \mathcal{T}$  tal que  $s_{\tau_i} = \epsilon_R(t)$  e seja  $\tau_j \in \mathcal{T}$  tal que  $s_{\tau_j} = \epsilon_L(t)$ . Em  $\mathcal{S}$ ,  $s_{\tau_i}$  e  $t$  estão na mesma  $\mathcal{R}$ -classe e a proposição 5.9 implica que  $s_{\tau_i} = \epsilon_R(t) \neq t$ . Usando a proposição 8.7 [10] temos que existe  $\sigma \in \Sigma$  tal que  $\sigma$  era<sub>suff</sub>  $t$  com  $\text{bas}(\sigma) \leq \text{bas}(\tau_i)$ . Como  $s_{\tau_j} \in \text{Suf}(t)$  e  $\sigma$  era<sub>suff</sub>  $t$ , a proposição 6.3 [10] implica que  $\text{bas}(\tau_j) \leq \text{bas}(\sigma)$  e portanto  $\text{bas}(\tau_j) \leq \text{bas}(\sigma) \leq \text{bas}(\tau_i) = \text{bas}(\tau_j)$ . Daí  $\text{bas}(\sigma) = \text{bas}(\tau_i)$  e a mesma proposição 8.7 [10] implica então que  $\sigma = \tau_i$  e que  $s_{\tau_i} = t \# \tau_i = (t \rightleftharpoons l_{\tau_i})^{-1} s_{\tau_i}$ . Assim  $t = t \rightleftharpoons l_{\tau_i} \in \text{Pref}(l_{\tau_i})$ . Sejam as palavras  $u$  e  $v$  tais que  $b_L(\tau_1) = uv$  e  $b_L(\tau_i) = vu$  com  $v \neq 1$ . Temos que  $vs_{\tau_1} \in \text{Suf}((uv)^m s_{\tau_1}) = \text{Suf}(l_{\tau_1})$  tem período  $b_L(\tau_1)$ . Como  $b_L(\tau_1)$  e  $b_L(\tau_i)$  são palavras conjugadas, o lema 3.2 [10] implica que também  $b_L(\tau_i) = vu$  é período de  $vs_{\tau_1} = vu v (b_L(\tau_i))^{-1} s_{\tau_1}$ . Assim  $b_L(\tau_i)$  é período e prefixo de  $l_{\tau_i}$  e de  $vs_{\tau_1}$ . Usando o dual do corolário 3.4 [10], temos que  $l_{\tau_i}, vs_{\tau_1} \in \text{Pref}(b_L(\tau_i)^*)$  e que  $t \in \text{Pref}(l_{\tau_i}) \subseteq \text{Pref}(b_L(\tau_i)^*)$ . Suponha por absurdo que  $|t| > |vs_{\tau_1}|$ . Neste caso temos que  $vs_{\tau_1} \in \text{Pref}(t)$  e  $(v, s_{\tau_1}, (vs_{\tau_1})^{-1}t)$  é uma ocorrência de  $\mathcal{D}$ -entrada de  $t$ , o que contradiz com a proposição 5.9 já que  $v \neq 1 \neq (vs_{\tau_1})^{-1}t$ . Assim podemos supôr que  $|t| \leq |vs_{\tau_1}|$  e portanto  $t \in \text{Pref}(vs_{\tau_1}) \subseteq \text{Fat}(uvs_{\tau_1}) = \text{Fat}(w)$ . Isto prova que  $t$  é uma transição de  $w$  pois  $t \mathcal{D}' w$ . Ademais,  $t = t_i$  já que  $t_i$  é a única transição de  $w$  cuja  $\mathcal{R}$ -entrada é  $s_{\tau_i}$ .

Como  $V(\mathbf{G})$  e  $E(\mathbf{G})$  têm a mesma cardinalidade  $k$ , o número ciclômico de  $\mathbf{G}$  é  $|E(\mathbf{G})| - |V(\mathbf{G})| + 1 = 1$ . ■

**Corolário 9.6** *Sejam inteiros  $n \geq 3$  e  $m \geq 1$ . Os grupos maximais de um semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  são cíclicos de ordem  $m$ .*

*Prova.* O grafo fundamental de uma  $\mathcal{D}$ -classe regular de  $\mathcal{M} \setminus \{\tilde{1}\}$  é um cir-

cuito devido ao teorema 9.5 e tem, portanto, número ciclomático 1. Usando o teorema 7.6, temos que um grupo maximal de  $\mathcal{M} \setminus \{\tilde{1}\}$  é um grupo de Burnside livre satisfazendo  $x^m = 1$  gerado por um único gerador: o grupo cíclico de ordem  $m$ . ■



# Bibliografia

- [1] S. I. Adian. *The Burnside problem and identities in groups*, volume 95 of *Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas]*. Springer-Verlag, Berlin-New York, 1979. Translated from the Russian by John Lennox and James Wiegold.
- [2] J. Brzozowski, K. Culik, and A. Gabrielian. Classification of non-counting events. *J. Comp. Syst. Sci.*, 5:41–53, 1971.
- [3] W. Burnside. On an unsettled question in the theory of discontinues groups. *Quart. J. Math.*, 33:230–238, 1902.
- [4] Adyan, S. I. *The Burnside problem and identities in groups*. Izdat. “Nauka”, Moscow, 1975.
- [5] A. de Luca and S. Varricchio. On non-counting regular classes. In M.S.Paterson, editor, *Automata, Languages and Programming*, pages 74–87, Berlin, 1990. Springer-Verlag. Lecture Notes in Computer Science, 443.
- [6] A. de Luca and S. Varricchio. On finitely recognizable semigroups. *Acta Inform.*, 29(5):483–498, 1992.
- [7] A. de Luca and S. Varricchio. On non-counting regular classes. *Theoretical Computer Science*, 100:67–104, 1992.
- [8] A. P. do Lago. Sobre os semigrupos de Burnside  $x^n = x^{n+m}$ . Master’s thesis, Instituto de Matemática e Estatística da Universidade de São Paulo, November 1991.
- [9] A. P. do Lago. On the Burnside semigroups  $x^n = x^{n+m}$ . In I. Simon, editor, *LATIN’92*, volume 583 of *Lecture Notes in Computer Science*, pages 329–43, Berlin, 1992. Springer-Verlag.

- [10] A. P. do Lago. On the Burnside semigroups  $x^n = x^{n+m}$ . *Int. J. of Algebra and Computation*, 6(2):179–227, 1996.
- [11] J. A. Green and D. Rees. On semigroups in which  $x^r = x$ . *Proc. Cambridge Philos. Soc.*, 48:35–40, 1952.
- [12] V. S. Guba. The word problem for the relatively free semigroup satisfying  $t^m = t^{m+n}$  with  $m \geq 3$ . *Int. J. of Algebra and Computation*, 2(3):335–348, 1993.
- [13] V. S. Guba. The word problem for the relatively free semigroup satisfying  $t^m = t^{m+n}$  with  $m \geq 4$  or  $m = 3, n = 1$ . *Int. J. of Algebra and Computation*, 2(2):125–140, 1993.
- [14] J. Hall, Marshall. Solution of the Burnside problem for exponent six. *Illinois J. Math.*, 2:764–786, 1958.
- [15] J. Hall, Marshall. *The Theory of Groups*. The Macmillan Company, New York, 1959.
- [16] G. Huet and D. C. Oppen. Equations and rewrite rules: a survey. In R. V. Book, editor, *Formal Language Theory, Perspectives and Open Problems*, pages 349–405, New York, NY, 1980. Academic Press.
- [17] S. V. Ivanov. On the Burnside problem on periodic groups. *Bull. Amer. Math. Soc. (N.S.)*, 27(2):257–260, 1992.
- [18] S. V. Ivanov. The free Burnside groups of sufficiently large exponents. *Internat. J. Algebra Comput.*, 4(1-2):ii+308, 1994.
- [19] L. Kađourek, Jiříand Polák. On free semigroups satisfying  $x^r \simeq x$ . *Simon Stevin*, 64(1):3–19, 1990.
- [20] J. W. Klop. Term rewriting systems: from church-rosser to knuth-bendix and beyond. In M.S.Paterson, editor, *Automata, Languages and Programming*, pages 350–369, Berlin, 1990. Springer-Verlag. Lecture Notes in Computer Science, 443.
- [21] G. Lallement. *Semigroups and Combinatorial Applications*. John Wiley & Sons, New York, NY, 1979.

- [22] F. W. Levi and B. L. van der Waerden. Über eine besondere klasse von gruppen. *Abh. Math. Sem. Hamburg*, 9:154–158, 1933.
- [23] I. G. Lysënok. Infinity of Burnside groups of period  $2^k$  for  $k \geq 13$ . *Uspekhi Mat. Nauk*, 47(2(284)):201–202, 1992.
- [24] S. MacLane. *Categories for the working mathematician*. Springer-Verlag, New York, 1971. Graduate Texts in Mathematics, Vol. 5.
- [25] J. McCammond. The solution to the word problem for the relatively free semigroups satisfying  $t^a = t^{a+b}$  with  $a \geq 6$ . *Int. J. of Algebra and Computation*, 1:1–32, 1991.
- [26] D. McLean. Idempotent semigroups. *Amer. Math. Monthly*, 61:110–113, 1954.
- [27] P. S. Novikov and S. I. Adjan. Infinite periodic groups. I. *Izv. Akad. Nauk SSSR Ser. Mat.*, 32:212–244, 1968.
- [28] P. S. Novikov and S. I. Adjan. Infinite periodic groups. II. *Izv. Akad. Nauk SSSR Ser. Mat.*, 32:251–524, 1968.
- [29] I. Sanov. Solution of Burnside’s problem for expoent 4. *Leningrad. Gos. Univ. Uchen. Zap. Ser. Mat.*, 10:166–170, 1940. (Russian).
- [30] I. Simon. Notes on non-counting languages of order 2. manuscript, 1970.
- [31] A. Thue. Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen. *Norske Vid. Selsk. Skr. I Mat. Nat. Kl.*, 1:1–67, 1912.
- [32] B. Tilson. Categories as algebra: an essential ingredient in the theory of monoids. *J. Pure Appl. Algebra*, 48(1-2):83–198, 1987.





# Lista de Figuras

4.1	Diagrama dos morfismos $\hat{\cdot}$ , $\lambda$ , $\theta$ , $\phi$ e $\beta$ . . . . .	33
4.2	Diagramas dos morfismos $\theta$ , $\phi$ e $\lambda$ bem como $\hat{\cdot}$ e $\lambda$ . . . . .	34
4.3	Diagrama dos morfismos $\hat{\cdot}$ , $\phi$ e $\beta$ . . . . .	35
5.1	Lema 5.11 aplicado à palavra $w = aabcccabcb$ . . . . .	48
6.1	Representação de $rt^{n+m}s = x = uav$ . . . . .	61
6.2	Grafo fundamental da $\mathcal{D}$ -classe de $\widetilde{abc}$ na banda livre . . . . .	65
6.3	$\mathcal{D}$ -classe de $\widetilde{a^n b^n}$ , com $n \geq 2$ . . . . .	74
7.1	Grafo fundamental da $\mathcal{D}$ -classe de $\widetilde{ab}$ no monóide de Burnside livre satisfazendo $x = x^3$ gerado por $\{a, b\}$ . . . . .	81
7.2	Fatoração $f'$ em $F'_1$ . . . . .	84
8.1	O grafo $\mathbf{G}$ . . . . .	107
9.1	Grafo fundamental da $\mathcal{D}$ -classe de $\widetilde{ab}$ . . . . .	120
9.2	Grafo fundamental da $\mathcal{D}$ -classe de $\widetilde{abc}$ . . . . .	121
9.3	Exemplo de uma produção de base 2 em que $m = 3$ . . . . .	126
9.4	Grafo fundamental de uma $\mathcal{D}$ -classe regular para $n \geq 3$ . . . . .	128



# Lista de Tabelas

- 7.1 Avaliação das palavras  $ab$ ,  $u$ ,  $v$ ,  $w$  e  $w'$  pelas funções  $\#_a$  e  $\#_b$  e de suas digitais pelas funções  $\#_{\widetilde{bab}}$  e  $\#_{\widetilde{baab}}$  . . . . . 93
- 7.2 Avaliação das palavras de  $\varphi(D)$  pelas funções  $\#_a$  e  $\#_b$  e  $\#_{b(aa)+b}$  98

LISTA DE TABELAS

1. Tabela 1.1 - Descrição das variáveis utilizadas no modelo de regressão logística.

# Índice

- adequação da  $\mathcal{L}$ -entrada  $l$ , 53
- adequação da  $\mathcal{R}$ -entrada  $r$ , 53
- adequação da transição  $t$ , 52
- adequação direita, 52
- adequação esquerda, 52
- apagamento de sufixo, 127
- apagamento de um sufixo por uma produção, 127
- aresta de  $\mathbf{G}$ , 13
- arestas consecutivas, 14
- árvore, 15
- árvore com início  $v$ , 15
- árvore com raiz  $v$ , 15
- árvore com término  $v$ , 15
- árvore conectora, 15
- árvore conectora de  $\mathbf{G}$ , 15
- avaliação do passeio  $p$ , 25
- avaliação do passeio  $p$  por  $\varphi$ , 25
  
- banda livre gerada por  $A$ , 58
- base de  $\tau$ , 126
- base direita de  $\tau$ , 126
- base esquerda de  $\tau$ , 126
- bijeção de  $\mathbf{T}$  em  $V$ , 16
  
- caminho, 15
- caminho associado a um passeio, 15
- $P$ -característica, 27
- categoria fortemente conexa, 28
  
- categoria livre gerada por um grafo, 25
- categoria quociente, 26
- categoria sintática de  $X$ , 27
- congruência de Burnside, 58
- congruência sintática de  $X$ , 27
- congruência sobre uma categoria  $\mathcal{C}$ , 26
- conjunto de arestas de  $\mathbf{G}$ , 14
- conjunto de objetos de  $\mathcal{C}$ , 24
- conjunto de produções estável, 127
- conjunto de vértices de  $\mathbf{G}$ , 14
- conteúdo de  $w$ , 41
- curto de  $\tau$ , 126
  
- digital de  $w$ , 67
  
- $\mathcal{D}$ -entrada, 44
- $\mathcal{D}$ -entrada de  $w$ , 44
- $\mathcal{L}$ -entrada, 44
- $\mathcal{L}$ -entrada de  $w$ , 44
- $\mathcal{R}$ -entrada, 43
- $\mathcal{R}$ -entrada de  $w$ , 43
- estabilidade de um monóide, 40
  
- fator de  $y$ , 25
- fatoração de  $w$ , 25
- finitude  $\mathcal{J}$ -acima, 2
- funções de incidência, 14
  
- gerador da categoria, 25

- grafo, 13  
 grafo dirigido, 13  
 grafo fortemente conexo, 14  
 grafo fundamental de  $D$ , 65  
 grupóide, 28  
 grupóide de Burnside livre satisfazendo  $x^m = 1$  gerado por  $G$ , 30  
 idempotência, 40  
 $\sim$ -idempotente, 41  
 identidade local a  $v$ , 24  
 início de uma aresta, 14  
 início do passeio, 14  
 injetividade em  $T$ , 16  
 $\sim$ -irregular, 41  
 irregularidade, 40  
 laço, 14  
 longo de  $\tau$ , 126  
 menor congruência que contém  $\pi$ , 27  
 menor período de  $w$ , 126  
 monóide de torção, 40  
 monóide idempotente livre gerado por  $A$ , 58  
 monóide local a  $v$ , 28  
 morfismo de categorias, 24  
 morfismo de grafos, 24  
 normalização, 31  
 normalizante de  $v$ , 30  
 número ciclomático, 19  
 $P$ -ocorrência, 27  
 ocorrência de  $y$  como fator de  $w$ , 26  
 ocorrência de  $\mathcal{D}$ -entrada de  $w$ , 44  
 ocorrência de transição de  $w$ , 46  
 ordem das fatorações, 26  
 ordem das ocorrências, 26  
 palavra primitiva, 126  
 palavras conjugadas, 126  
 passeio, 14  
 passeio em  $G$ , 14  
 passeio fechado, 14  
 passeio fechado sobre  $v$ , 14  
 passeio vazio local a  $v$ , 14  
 passeios coterminais, 15  
 período de  $w$ , 126  
 potência de  $p$  a  $k$ , 24  
 prefixo de  $y$ , 25  
 preservação do valor de uma função, 27  
 produção estável, 127  
 produções conjugadas, 126  
 projeção de vértices induzida, 24  
 reconhecibilidade de  $X$ , 27  
 refinamento de uma equivalência, 27  
 $\sim$ -regular, 41  
 regularidade, 40  
 relações de Green, 40  
 relações Green-induzidas, 41  
 relações Green-induzidas pelo morfismo  $\sim$ , 41  
 representação de  $X$ , 118  
 representante de uma palavra, 118  
 saturação de  $X$  por  $\sim$ , 27  
 semigrupo de Burnside livre satisfazendo  $x^n = x^{n+m}$  gerado por  $A$ , 58  
 seqüência de ocorrências de  $\mathcal{D}$ -entradas de  $w$ , 46

- seqüência de ocorrências de transições de  $w$ , 46
- seqüência de transições de  $w$ , 46
- sistema de adequações associado a  $e$ , 52
- sistema de adequações básico associado a  $e$ , 52
- sistema de adequações básico coerente, 52
- sistema de adequações coerente, 53
- sistema de adequações completo, 52
- sobreposição de  $u$  e  $v$ , 126
- subgrafo de  $G$ , 15
- subgrafo de  $G$  induzido por  $E(T)$ , 15
- substituição por  $(t, t')$ , 26
- substituição por  $\pi$ , 26
- sufixo de  $y$ , 25
  
- término do passeio, 14
- término de uma aresta, 14
- transição, 46
- transição de  $w$ , 46
  
- vértice de  $G$ , 14