Subgrupos finitamente gerados de grupos singelos

Maria Ana Barbosa
Mestrado em Matemática
Departamento de Matemática
Faculdade de Ciências da Universidade do Porto
2025

Subgrupos finitamente gerados de grupos singelos

Maria Ana Barbosa

Dissertação realizada no âmbito do Mestrado em Matemática

Departamento de Matemática

2025

Orientador
Pedro Ventura Alves da Silva, Professor Catedrático,
Faculdade de Ciências da Universidade do Porto

Agradecimentos

Em primeiro lugar, quero expressar o meu profundo agradecimento ao Professor Pedro Silva. Foi muito mais do que um orientador: foi (e continua a ser) um verdadeiro amigo ao longo de todo este percurso. A sua forma de explicar, sempre clara, natural e elegante, tornou tudo mais acessível e inspirador. Agradeço-lhe especialmente por me ter dado liberdade para ser criativa, para explorar o meu próprio caminho, mas sempre com a segurança de saber que estava atento e disponível caso eu precisasse. Também não posso deixar de mencionar a maneira como fala de Matemática: sempre com um brilho nos olhos!

Agradeço também à empresa onde trabalhei durante este último ano, Tlantic, pela compreensão e pela flexibilidade ao permitir-me trabalhar num regime mais leve, o que tornou possível a conciliação do dever laboral com a redação da dissertação.

À minha família e aos meus amigos, o meu muito obrigado por estarem sempre presentes. Alguns deles foram absolutamente essenciais neste caminho: Miguel Avides, Pedro Sottomayor, Mafalda Pereira, Eduardo Magalhães, Tristão Reis, Maria Salvador e Sónia Pereira. O vosso apoio, incentivo e companhia fizeram toda a diferença.

Resumo

Os grupos singelos, isto é, produtos livres finitários de grupos finitos e cópias de $\mathbb{Z}$, e os seus subgrupos finitamente gerados têm despertado crescente interesse ao longo dos últimos anos [1, 8, 9, 21–23]. Neste trabalho, investigamos extensões dos autómatos de Stallings, originalmente definidos para grupos livres, para a classe dos grupos singelos.

Com base nesta construção, provamos a decidibilidade de diversos problemas computacionais nesta classe de grupos, incluindo o problema da palavra generalizado e o problema da conjugação generalizado. Dado um subgrupo finitamente gerado H de um grupo singelo G, $H \leq_{f.g.} G$, mostramos que o seu normalizador $N(H)$ é finitamente gerado, é computável, e que o índice $[N(H) : H]$ é finito e computável.

Mostramos ainda que é possível deduzir propriedades de H diretamente do autómato correspondente: se é normal, se tem índice finito (e, neste caso, como o computar), se coincide com o seu normalizador ou se possui elementos de torção não triviais. Apresentamos uma prova combinatória de que H é livre se, e somente se, não contém elementos de torção não triviais, o que nos vai permitir decidir se H é livre e calcular uma base, quando for o caso. Também demonstramos que a cadeia de normalizadores gerada por H, isto é, $H \leq N(H) \leq N(N(H)) \leq \ldots$, estabiliza. Por fim, provamos que os grupos singelos satisfazem a propriedade de Howson, usando o produto de autómatos, e apresentamos versões generalizadas dos teoremas de Newman e Gunning enunciados em [23].

Palavras-chave: grupo livre, produto livre, grupos singelos, autómatos de Stallings, problemas de decisão

Abstract

Plain groups, that is, finite free products of finite groups and copies of $\mathbb{Z}$, and their finitely generated subgroups have received increasing attention in recent years [1, 8, 9, 21–23]. In this work, we investigate extensions of Stallings automata, originally defined for free groups, to the class of plain groups.

Using this framework, we prove the decidability of several algorithmic problems in this class of groups, including the generalized word problem and the generalized conjugacy problem. Given a finitely generated subgroup $H \leq_{f.g.} G$ of a plain group G, we show that its normalizer $N(H)$ is finitely generated, computable, and that the index $[N(H) : H]$ is finite and computable.

We further show that properties of H can be inferred directly from its associated automaton: whether H is normal, has a finite index (and, if that is the case, how to compute it), is self-normalizing, or contains nontrivial torsion elements. A combinatorial proof is given that H is free if and only if it contains no nontrivial torsion elements. This allows us to decide whether H is free and, if so, compute a basis. We also show that the normalizer chain generated by H, namely $H \leq N(H) \leq N(N(H)) \leq \ldots$, stabilizes. Finally, we prove that plain groups satisfy the Howson property using the product of automata and present generalized versions of Newman's and Gunning's theorems stated in [23].

Keywords: free group, free product, plain groups, Stallings automata, decision problems

Índice

1. Introdução 1
2. Monóides e semigrupos 4
   2.1. Terminologia básica 4
   2.2. Semigrupos e monóides livres 7
3. Linguagens e autómatos 10
   3.1. Linguagens 10
   3.2. Autómatos 11
   3.3. Linguagens racionais 14
   3.4. Sistemas de reescrita 18
4. Grupos Livres 21
   4.1. Apresentações de grupos 21
   4.2. Construção do grupo livre 23
5. Produto livre 28
   5.1. Existência do produto livre 29
6. Decidibilidade 34
   6.1. Alguns problemas de decidibilidade 34
   6.2. Autómatos de Stallings 38
7. Generalização dos autómatos de Stallings 44
   7.1. Construção dos autómatos 44
8. Algumas aplicações 63
   8.1. Estudo da torção 63
   8.2. Problema da conjugação 73
   8.3. Problema da conjugação generalizado 76
   8.4. O normalizador 84
9. Conclusão 101

Bibliografia 101
Índice Remissivo 105
Notação 108

1. Introdução

A Teoria de Grupos teve origem no século XIX, a partir do estudo de equações polinomiais, e rapidamente se consolidou como um dos pilares da Matemática moderna, com aplicações profundas em diversas áreas científicas. Em particular, os grupos finitamente gerados desempenham um papel central na teoria algébrica e combinatória, onde questões computacionais e estruturais frequentemente se entrelaçam.

Um exemplo de grupos finitamente gerados são os *grupos singelos*, definidos como produtos livres finitários de grupos finitos e de cópias de $\mathbb{Z}$. Na língua inglesa, esses grupos são conhecidos como *plain groups* - nome atribuído por constituírem uma subclasse mais simples dos grupos fundamentais de grafos de grupos. Por essa razão, adotamos aqui a tradução grupos singelos.

Ora, os grupos singelos têm despertado interesse ao longo dos anos, sendo a conjetura de Madlener e Otto [1], apresentada em 1986, uma das razões desse interesse crescente, e, desde então, vários progressos foram feitos [8].

Conjetura 1.0.1 (Madlener e Otto, 1986)**.** *Os grupos singelos são exatamente os grupos que admitem uma apresentação finita $\langle A|\mathcal{R}\rangle$ para algum sistema de reescrita $\mathcal{R}$ redutor e confluente.*

Outro exemplo que demonstra a importância do estudo destes grupos é o grupo modular $\mathbb{Z}_2 * \mathbb{Z}_3$ pois, embora seja um dos exemplos mais simples de um grupo singelo, o estudo deste grupo e dos seus subgrupos finitamente gerados tem desempenhado um papel central na álgebra, na teoria dos números e na geometria desde o final do século XIX. Em particular, Klein destacou em [14] a enumeração e a classificação de subgrupos de índice finito no grupo modular como um problema na teoria dos grupos de importância fundamental, situado na intersecção de vários ramos da Matemática.

Ora, é sabido que a ferramenta mais poderosa para estudar subgrupos finitamente gerados de grupos livres são os chamados autómatos de Stallings: uma subclasse de autómatos finitos, cuja construção se baseia numa reformulação combinatória e sistemática das ideias pioneiras de Stallings nos anos 1980 [28], apresentada por Kapovich e Myasnikov em [12]. Estes autómatos não só contribuem para dar resposta a vários problemas

de decisão de forma altamente eficiente, como também fornecem informações sobre o subgrupo apenas a partir da sua estrutura. Veja-se, por exemplo, [2, 6, 20, 29].

É natural que tenha surgido o interesse em generalizar esta poderosa ferramenta para outras classes de grupos. Em [13], Kapovich, Weidmann e Miasnikov estendem a técnica das dobragens de Stallings para algumas subclasses de grupos fundamentais de grafos de grupos, sendo os grupos virtualmente livres uma delas. Esta abordagem permitiu tratar estruturas mais complexas como produtos livres com amalgamação e extensões HNN, mantendo uma abordagem combinatória eficaz para problemas algorítmicos como o da palavra generalizado.

Em [17] e [19], Markus-Epstein generaliza os autómatos de Stallings a amalgamações de dois grupos finitos e responde a vários problemas de decisão nessa classe. Mais tarde, em [18], Markus-Epstein considera o produto livre arbitrário de grupos finitos, com o objetivo de obter decomposições de Kurosh de subgrupos finitamente gerados a partir dos respetivos autómatos. Já em [26], Silva, Soler-Escrivà e Ventura discutem qual a generalização mais adequada da construção de Stallings, introduzindo as chamadas secções de Stallings. Demonstram, então, que os grupos que admitem tal generalização são precisamente os grupos virtualmente livres finitamente gerados, fornecendo assim mais uma solução para o problema da palavra generalizado nessa classe.

Contudo, é expectável que, num contexto tão geral, nem todos os resultados e propriedades algorítmicas obtidos no caso dos grupos livres possam ser estendidos. O objetivo deste trabalho é explorar qual a versão mais adequada dos autómatos de Stallings para a classe dos grupos singelos e, a partir dela, estender muitos dos resultados conhecidos para grupos livres. No caso particular em que se considera apenas o produto livre de grupos finitos, os autómatos obtidos coincidem com os apresentados no trabalho de Markus-Epstein em [18]. Importa sublinhar, contudo, que a metodologia desenvolvida neste trabalho é distinta da seguida nesse artigo, tendo resultado de um percurso independente. Por exemplo, em [18], não é considerada a questão da correspondência bijetiva entre os subgrupos finitamente gerados e as classes de isomorfismo de uma dada classe de autómatos finitos, ao contrário do caso clássico de Stallings para grupos livres e do presente trabalho, que cobre tanto o produto livre de grupos finitos como os grupos singelos.

Assim sendo, os primeiros capítulos têm como função fornecer as ferramentas necessárias para a construção destes autómatos, bem como enquadrar as questões que serão abordadas. O trabalho de investigação original inicia-se no Capítulo 7, onde apresentamos um algoritmo que constrói um autómato inverso, a partir de um conjunto gerador de um subgrupo finitamente gerado de um grupo singelo G. Demonstra-se que a construção é independente do conjunto gerador escolhido, permitindo assim resolver o problema da palavra generalizado para grupos singelos. Observa-se ainda que todos os autómatos obtidos por este algoritmo satisfazem um conjunto de propriedades específicas, isto é, pertencem a uma determinada classe de autómatos finitos. Prova-se também que existe uma correspondência bijetiva entre as classes de isomorfismo desta classe de autómatos e os subgrupos finitamente gerados de G.

No Capítulo 8, apresentam-se respostas a diversos problemas de decisão baseadas nas propriedades destes autómatos, tais como: o problema da conjugação e o problema da conjugação generalizado. Demonstra-se que, a partir da estrutura do autómato associado a um subgrupo finitamente gerado $H \leq_{f.g.} G$, é possível decidir se H possui torção não trivial, se é normal, se tem índice finito (e, neste caso, como calculá-lo). Apresenta-se ainda uma prova combinatória de que H é livre de torção não trivial se, e só se, for livre, e, em caso afirmativo, como computar uma base de H. É dada uma prova alternativa de que os grupos singelos satisfazem a propriedade de Howson, utilizando o produto de autómatos.

Realiza-se também um estudo do normalizador de H, $N(H)$, concluindo que $N(H)$ é finitamente gerado e computável. Isto permite-nos deduzir que a cadeia de normalizadores gerada por H, isto é, $H \leq N(H) \leq N(N(H)) \leq \ldots$ estabiliza e que $[N(H) : H]$ é finito e computável. Como consequência deste resultado, resulta que se H é normal, então tem índice finito. Também vai ser possível decidir quando é que $H = N(H)$ ou quando é que $N(H)$ é um fator de G. Concluímos também que, se $N(H)$ é livre, $dim(N(H)) \leq dim(H)$.

Como aplicação de alguns destes resultados, generalizamos dois teoremas conhecidos relativos aos subgrupos de índice finito do grupo modular.

2. Monóides e semigrupos

Começamos este trabalho relembrando algumas definições e resultados básicos relativos a monóides e a semigrupos, assumindo que estes conceitos são já familiares no contexto dos grupos.

2.1. Terminologia básica

Um *semigrupo* é um conjunto S munido de uma operação binária que é associativa. Note-se que estamos a permitir que o semigrupo possa ser vazio munido da operação vazia. Se um semigrupo S tiver um elemento $y \in S$ tal que para todo o $x \in S$, $yx = xy = x$, este tem de ser único, e dizemos que y é o *elemento identidade* do semigrupo S. Normalmente, se existir, denotamos o elemento identidade de S por 1_S ou simplesmente 1 quando não há risco de ambiguidade. Um semigrupo com elemento identidade diz-se um *monóide*. Num monóide S, um elemento y diz-se invertível se existe um $x \in S$ tal que $yx = xy = 1$. Um monóide onde todos os seus elementos são invertíveis diz-se um *grupo*. Quando a operação do grupo é também comutativa dizemos que é um *grupo abeliano*.

Um *subsemigrupo* T de um semigrupo S é um subconjunto de S que é também um semigrupo, considerando-se em T a operação induzida por S. No caso de S ser um monóide, com elemento identidade 1, um *submonóide* de S é um subsemigrupo T tal que $1 \in T$. Se X é um subconjunto de um semigrupo S, o *subsemigrupo gerado por* X é o menor subsemigrupo de S que contém X, e denotamo-lo por $\langle X \rangle$. Se existe um subconjunto finito $X \subseteq S$ tal que $S = \langle X \rangle$, então dizemos que S é um *semigrupo finitamente gerado*. De forma análoga, definem-se os conceitos de *submonóide gerado por* X e de *monóide finitamente gerado*.

Um *homomorfismo de semigrupos* (ou *morfismo* de semigrupos) é uma função $\phi : S \to T$ entre semigrupos tal que, para todos $x, y \in S$, $(xy)\phi = x\phi y\phi$. No caso em que S, T são monóides e, adicionalmente, $1_S\phi = 1_T$, dizemos que ϕ é um *homomorfismo de monóides*. Definimos como *núcleo* de ϕ a relação $ker(\phi) = \{(x, y) \in S \times S : x\phi = y\phi\}$. Um homomorfismo injetivo, ou seja, um homomorfismo em que o núcleo é a relação diagonal $\triangle_S = \{(x, x) : x \in S\}$, diz-se um *mergulho*.

Um *isomorfismo* de semigrupos é um homomorfismo de semigrupos $\phi : S \to T$ bijetivo. Neste caso, dizemos que S, T são *isomorfos* e escrevemos $S \simeq T$. De forma análoga definimos *isomorfismo de monóides*.

Uma *congruência num semigrupo* S é uma relação de equivalência σ em S tal que, para todos $x, x', y, y' \in S$,

$$(x\sigma x' \wedge y\sigma y') \Rightarrow (xy)\sigma(x'y').$$

Por outras palavras, σ é uma relação de equivalência que é compatível com a operação em S. Esta compatibilidade permite-nos dar ao conjunto quociente ${}^{S}\!/_{\sigma}$, que consiste no conjunto formado pelas σ-classes de equivalência

$${}^{x}\!/_{\sigma} = \{y \in S : x\sigma y\} \quad (x \in S),$$

uma estrutura de semigrupo onde a operação binária $\circ$ em ${}^{S}\!/_{\sigma}$ é a operação induzida por S nas classes que equivalência, ou seja,

$${}^{x}\!/_{\sigma} \circ {}^{y}\!/_{\sigma} = {}^{(xy)}\!/_{\sigma}.$$

Note-se que a função natural $\pi : S \to {}^{S}\!/_{\sigma}$ que envia x em ${}^{x}\!/_{\sigma}$ é um homomorfismo de semigrupos e $ker(\pi) = \sigma$. Portanto, qualquer congruência em S é o núcleo de algum homomorfismo com domínio S. Por outro lado, dado um homomorfismo de semigrupos $\phi : S \to T$, é fácil de ver que $ker(\phi)$ é uma congruência em S. Assim sendo, outra maneira de definir congruência em S é como sendo o núcleo de algum homomorfismo de semigrupos de domínio S. Analogamente definimos uma *congruência num monóide* S e construimos o *monóide quociente* ${}^{S}\!/_{\sigma}$, sendo ${}^{1_S}\!/_{\sigma}$ o elemento identidade.

Exemplo 2.1.1. *Seja $T(X)$ o conjunto de todas as transformações de X, isto é, funções $X \to X$. Note-se que $T(X)$ é um monóide para a composição. Seja $X = \{0, \ldots, 4\}$, $f \in T(X)$ dada por*

$$f = \begin{pmatrix} 0\,1\,2\,3\,4 \\ 1\,2\,3\,4\,1 \end{pmatrix}.$$

e $S = \langle f \rangle$ o submonóide de $T(X)$ gerado por f. Ora, facilmente se verifica que $f^5 = f$ e que $S = \{1, f, \ldots, f^4\}$. Além disso, a partição $P = \{\{1\}, \{f, f^3\}, \{f^2, f^4\}\}$ define uma congruência σ em S. Isto pode ser visto reparando que para todo $C \in P$, $fC = Cf \subseteq C'$ para algum $C' \in P$. Portanto o monóide quociente ${}^{S}\!/_{\sigma}$ tem três elementos e é gerado por ${}^{f}\!/_{\sigma}$.

No caso em que S é um grupo, sabemos que $1/\sigma$ é um subgrupo normal de S, e as classes de equivalência de σ são as classes laterais de $1/\sigma$. Por este motivo, quando S é um grupo, por vezes representamos σ apenas por $1/\sigma$. O Exemplo 2.1.1 mostra que, congruências em monóides não são necessariamente determinadas pela classe de equivalência que contém o elemento identidade.

Teorema 2.1.2 (Teorema do homomorfismo de semigrupos/monóides)**.** *Se $\phi : S \to T$ é um homomorfismo de semigrupos/monóides, σ uma congruência em S e $\pi : S \to S/\sigma$ o homomorfismo natural então, existe um único homomorfismo $\phi' : S/\sigma \to T$ tal que o seguinte diagrama comuta*

$$\begin{array}{ccc} S & \xrightarrow{\phi} & T \\ {\scriptstyle\pi}\downarrow & \nearrow_{\phi'} & \\ S/\sigma & & \end{array}$$

se e só se $\sigma \subseteq ker(\phi)$. Além disso, ϕ' é injetiva se e só se $\sigma = ker(\phi)$.

Demonstração. Suponhamos primeiro que um tal homomorfismo $\phi' : S/\sigma \to T$ existe. Então se $(x, y) \in \sigma$, isto é, $x\sigma y$, tem-se que $x/\sigma = y/\sigma$ em S/σ. Logo, $(x/\sigma)\phi' = (y/\sigma)\phi'$ e, pela comutatividade do diagrama,

$$x\phi = x\pi\phi' = (x/\sigma)\phi' = (y/\sigma)\phi' = y\pi\phi' = y\phi.$$

Logo, $(x, y) \in ker(\phi)$ e $\sigma \subseteq ker(\phi)$. Reciprocamente, suponhamos que $\sigma \subseteq ker(\phi)$ e considere-se a seguinte função,

$$\begin{aligned} \phi' \colon S/\sigma &\longrightarrow T \ . \\ x/\sigma &\longmapsto x\phi \end{aligned}$$

Uma vez que, para todos $x, y \in S$,

$$x\sigma y \Rightarrow (x, y) \in ker(\phi) \Leftrightarrow x\phi = y\phi,$$

e ϕ é um homomorfismo, podemos concluir que, de facto, ϕ' está bem definido e é um homomorfismo. Como, para todo $x \in S$, $x\pi\phi' = (x/\sigma)\phi' = x\phi$, temos que $\phi = \pi\phi'$. Para mostrar a unicidade, basta notar que se $\varphi : S/\sigma \to T$ é outro homomorfismo nestas condições, como a igualdade $\phi = \pi\varphi$ tem se ser satisfeita, temos que, para todo o $x \in S$,

$$(x/\sigma)\varphi = x\pi\varphi = x\phi = (x/\sigma)\phi'$$

e $\varphi = \phi'$. Resta então mostrar que ϕ' é injetiva se e só se $\sigma = ker(\phi)$. Ora, ϕ' ser injetiva significa que, para todos $x, y \in S$, $(x/\sigma)\phi' = (y/\sigma)\phi'$ se e só se $x\sigma y$. Como, para todo o $x \in S$, $(x/\sigma)\phi' = x\pi\phi' = x\phi$, temos que ϕ' é injetiva se e só se $\ker(\phi) = \sigma$. □

2.2. Semigrupos e monóides livres

Assim como os semigrupos e os monóides, os grupos, anéis, corpos, espaços vetoriais sobre um dado corpo são também exemplos de estruturas algébricas, isto é, conjuntos equipados com uma ou mais operações que obedecem a certas propriedades. Com base no estudo individual de cada uma delas, podemos observar que estas estruturas partilham vários conceitos que são definidos de forma análoga tais como os que foram acima relembrados: sub-estrutura, homomorfismo, isomorfismo e congruência. Para além de conceitos partilhados, existem muitos resultados do mesmo teor que são válidos para cada uma das classes indicadas como, por exemplo, os teoremas do homomorfismo e do isomorfismo. Assim sendo, a álgebra universal surgiu como uma resposta à necessidade de unificar e generalizar o estudo de diferentes estruturas algébricas, promovendo não só uma apresentação mais económica, como também permitiu dar origem à aplicação de certos conceitos em contextos inteiramente novos. Um exemplo disso, que será o foco desta secção, é o conceito de base em monóides, sendo este bem conhecido no caso dos espaços vetoriais.

Começamos por definir um *alfabeto* como um conjunto A. Neste contexto, os elementos do alfabeto chamam-se *letras*. Uma *palavra* em A é uma sequência finita de letras. Isto inclui a *palavra vazia*, que convencionamos representar pelo símbolo 1. As palavras não vazias (no alfabeto A) são geralmente representadas na forma $a_1 \dots a_n$ para algum $n \geq 1$ e $a_1, \dots, a_n \in A$. O *comprimento* da palavra $a_1 \dots a_n$ é n e o da palavra vazia é 0. Denotamos o comprimento da palavra u por $|u|$.

Representamos por A^* o conjunto de todas as palavras em A e por A^+ o conjunto de todas as palavras em A não vazias, ou seja, $A^+ = A^* \backslash \{1\}$. Consideramos $A \subseteq A^*$ identificando cada letra $a \in A$ com a palavra $a \in A^*$, através da função injetiva $\iota : A \to A^*$.

Podemos definir uma operação binária e associativa em A^*, dita *concatenação*, do seguinte modo:

$$1u = u = u1$$

$$(a_1 \dots a_n)(b_1 \dots b_m) = a_1 \dots a_n b_1 \dots b_m,$$

onde $m, n \geq 1$, $a_i, b_j \in A$ e $u \in A^*$. Com esta operação, damos a A^* uma estrutura de monóide, sendo a palavra vazia a sua identidade. De facto, A^* é um monóide especial, no sentido em que satisfaz a seguinte propriedade:

Proposição 2.2.1 (Propriedade universal de A^*)**.** *Seja A um alfabeto e $\varphi : A \to M$ uma função de A num monóide M. Então, existe um e um só homomorfismo de monóides $\Phi : A^* \to M$ tal que $\Phi|_A = \varphi$.*

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & M \\ {\scriptstyle \iota}\downarrow & \nearrow_{\Phi} & \\ A^* & & \end{array}$$

Demonstração. Definimos $\Phi : A^* \to M$ tomando $1\Phi = 1$ e $(a_1 \dots a_n)\Phi = a_1\varphi \dots a_n\varphi$ para $n \geq 1$ e $a_i \in A$. É imediato que Φ é um homomorfismo de monóides que estende φ e que, qualquer outro homomorfismo nas mesmas condições tem de ser assim definido. □

Por A^* satisfazer esta propriedade universal, diz-se um *monóide livre de base A*. De facto, assim como os espaços vetoriais têm uma base, esta propriedade permite-nos pensar em A como uma espécie de base do monóide A^*. No entanto, uma vez que se tratam de estruturas diferentes, é natural que hajam algumas diferenças. Uma delas é que nem todo o monóide tem uma base. Na verdade, a menos de isomorfismo, existe apenas um monóide que satisfaz a propriedade acima, como podemos ver no seguinte corolário:

Corolário 2.2.2. *Seja A um conjunto e F um monóide com $A \subseteq F$ tal que, para toda a função $\varphi : A \to M$ de A num monóide M, existe um único homomorfismo de monóides $\Phi : F \to M$ que estende φ. Então $F \simeq A^*$.*

Demonstração. Sejam $\iota : A \to A^*$, $\iota' : A \to F$ as inclusões de A em, respetivamente, A^* e F. Uma vez que A^* satisfaz a propriedade universal com respeito a A, existe um único homomorfismo $\Phi : A^* \to F$ tal que o seguinte diagrama comuta,

$$\begin{array}{ccc} A & \xhookrightarrow{\iota'} & F \\ {\scriptstyle \iota}\downarrow & \nearrow_{\Phi} & \\ A^* & & \end{array},$$

ou seja, $\iota\Phi = \iota'$. Como F também satisfaz a propriedade universal com respeito a A, existe um único homomorfismo $\Phi' : F \to A^*$ tal que o seguinte diagrama comuta:

$$\begin{array}{ccc} A & \xrightarrow{\iota'} & F \\ {\scriptstyle\iota}\downarrow & \swarrow_{\Phi'} & \\ A^* & & \end{array} \quad ,$$

ou seja, $\iota'\Phi' = \iota$. Logo, $\iota\Phi\Phi' = \iota'\Phi' = \iota$ e, portanto, $\Phi\Phi' : A^* \to A^*$ e id_{A^*} estendem ambos ι. Pela unicidade da propriedade universal relativamente a A^*, podemos concluir que $\Phi\Phi' = id_{A^*}$. Analogamente se mostra que $\Phi'\Phi = id_F$. Logo, Φ, Φ' são isomorfismos mutuamente inversos e $F \simeq A^*$. $\square$

Por este motivo, dizemos que A^* é o monóide livre de base A. De forma análoga, A^+ é o *semigrupo livre* de base A no sentido em que, a menos de isomorfismo, é o único que respeita a propriedade universal, dada na Proposição 2.2.1, para a categoria dos semigrupos. Podemos então questionar se, na categoria dos grupos, existe algum objeto livre de base A? De facto, existe e uma construção deste será feita na Secção 4.2.

3. Linguagens e autómatos

A teoria dos autómatos desempenha um papel central na ciência da computação, ao estudar modelos matemáticos capazes de representar, de forma abstrata, processos de decisão e computação. Para além destes modelos serem essenciais no desenvolvimento de diversas tecnologias, estes são também uma ótima ferramenta no estudo de certas estruturas matemáticas (tais como os grupos) por meio de métodos combinatórios, como veremos mais adiante.

Já a teoria das linguagens formais surgiu do esforço para compreender as regularidades sintáticas presentes na comunicação humana. Destaca-se, nesse contexto, o trabalho do linguista Noam Chomsky, que formalizou matematicamente o conceito de gramática [4]. Desde então, esta teoria tornou-se essencial para desenvolvimento de linguagens de programação e na construção de compiladores. Neste trabalho, será destacada a classe das linguagens racionais, que está profundamente relacionada com os autómatos finitos.

3.1. Linguagens

Dado em alfabeto A, podemos querer estudar um conjunto específico de palavras em A. Surge então o conceito de *A-linguagem*, que entendemos como um subconjunto L de palavras em A, isto é, $L \subseteq A^*$. Quando o alfabeto está implícito ou é irrelevante dizemos apenas linguagem. Podemos, a partir de A-linguagens, criar outras utilizando *operadores de linguagens*, tais como:

• *Operadores booleanos*: Dadas $L_1, L_2 \subseteq A^*$, podemos tomar a sua união $L_1 \cup L_2$, a sua interseção $L_1 \cap L_2$ e o seu complemento $L_1^c = \{u \in A^* : u \notin L_1\}$;

• *Produto*: Dadas $L_1, L_2 \subseteq A^*$, podemos tomar o seu produto $L_1L_2 = \{u_1u_2 \in A^* : u_1 \in L_1, u_2 \in L_2\}$. Definimos indutivamente $L_1^0 = \{1\}$ e $L_1^n = L_1^{n-1}L_1$, para $n \geq 1$;

• *Estrela*: Dada $L \subseteq A^*$, podemos tomar a união de todas as A-linguagens obtidas aplicando um número finito de vezes o operador produto à linguagem L, isto é, $L^* = \bigcup_{n\geq 0} L^n$. Note-se que L^* é o submonóide de A^* gerado por L;

• *Morfismos*: Sejam A e B dois alfabetos e $\Phi : A^* \to B^*$ um homomorfismo de monóides. Se L é uma A-linguagem, então a imagem homomorfa $L\phi = \{u\phi \in B^* : u \in L\}$ é uma B-linguagem;

• *Morfismos inversos*: Sejam A e B alfabetos, $\phi : A^* \to B^*$ um homomorfismo de monóides e $L \subseteq B^*$. Então a imagem inversa $L\phi^{-1} = \{u \in A^* : u\phi \in L\}$ é uma A-linguagem.

É importante notar que há aqui um abuso de notação, uma vez que $*$ tem dois significados (monóide livre e submonóide gerado por). Mas em geral, o submonóide gerado por uma linguagem L não é um monóide livre sobre L. Por exemplo, se $A = \{a\}$ e $L = \{a, a^2\} \subseteq A^*$, então L^* não é um monóide livre de base L. No entanto, no caso em que $L \subseteq A$, L^* é de facto o monóide livre sobre L e, por este motivo, não há confusão quando escrevemos A^*.

Finalizamos esta pequena secção apresentando algumas relações entre palavras que vão ser importantes ao longo deste trabalho. Dadas $u, v \in A^*$, dizemos que:

• u é um *prefixo* de v se $v = uw$ para alguma $w \in A^*$;

• u é um *sufixo* de v se $v = wu$ para alguma $w \in A^*$;

• u é um *fator* de v se $v = w_1uw_2$ para algumas $w_1, w_2 \in A^*$.

3.2. Autómatos

Seja A um alfabeto. Um A-*autómato* é um quadruplo $\mathcal{A} = (Q, I, T, E)$ onde,

• Q é um conjunto não vazio, cujos elementos são chamados de *vértices*;

• I é um subconjunto de Q, cujos elementos são chamados de *vértices iniciais*;

• T é um subconjunto de Q, cujos elementos são chamados de *vértices terminais*;

• E é um subconjunto de $Q \times A \times Q$, cujos elementos são chamados de *arestas*. Dada $(p, a, q) \in E$, dizemos que a aresta (p, a, q) tem *rótulo* a.

Por vezes, usamos a notação $Q(\mathcal{A})$ e $E(\mathcal{A})$ para representar os vértices e as arestas de um autómato $\mathcal{A}$, respetivamente. Se não designarmos vértices iniciais nem terminais, temos a estrutura simplificada (Q, E), que se diz um A-*grafo*. Dado um autómato $\mathcal{A}$,

definimos como $\Gamma_{\mathcal{A}} = (Q(\mathcal{A}), E(\mathcal{A}))$ o A-grafo subjacente a $\mathcal{A}$. Reciprocamente, podemos ver um dado A-grafo (Q, E) como um A-autómato $(Q, \emptyset, \emptyset, E)$. Assim sendo, os conceitos que vão ser definidos para A-autómatos aplicam-se também para A-grafos.

> Um autómato diz-se *finito* se Q e E forem finitos. Neste trabalho, consideraremos apenas autómatos finitos. Portanto, quando nos referimos a um autómato, supomos sempre que este é finito, a menos que seja dito o contrário.

Dois autómatos $\mathcal{A} = (Q, I, T, E)$ e $\mathcal{A}' = (Q', I', T', E')$ dizem-se *isomorfos* se existir uma bijeção $\varphi : Q \to Q'$ tal que $I\varphi = I'$, $T\varphi = T'$ e

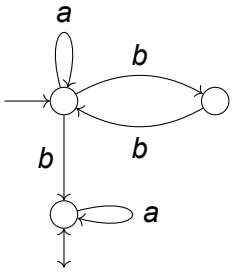
$$(p, a, q) \in E \Leftrightarrow (p\varphi, a, q\varphi) \in E'$$

para todos os $p, q \in Q$ e $a \in A$, isto é, $\mathcal{A}$ e $\mathcal{A}'$ são isomorfos se têm a mesma estrutura a menos da designação dos vértices, e escrevemos $\mathcal{A} \simeq \mathcal{A}'$. Dizemos então que φ é um *isomorfismo* de autómatos e, no caso em que $\mathcal{A}' = \mathcal{A}$, dizemos que φ é um *automorfismo* de $\mathcal{A}$. Denotamos por $Aut(\mathcal{A})$ o conjunto de todos os automorfismos de $\mathcal{A}$, isto é,

$$Aut(\mathcal{A}) = \{\varphi : \mathcal{A} \to \mathcal{A} \ : \ \varphi \text{ é um isomorfismo}\}.$$

É habitual descrever um autómato geometricamente utilizando o símbolo ◯ para representar os vértices e setas para representar as arestas. No caso de um vértice ser inicial (respetivamente final) este é identificado por uma seta que entra (respetivamente sai) sem rótulo.

Exemplo 3.2.1. *Exemplo de autómato no alfabeto* $A = \{a, b\}$*:*



Se q for o único vértice inicial e o único vértice final de um dado autómato, então q é designado por *ponto base*. Note-se que, no autómato representado no Exemplo 3.2.1, os vértices não estão identificados. Neste trabalho, sempre que a identificação dos vértices não for relevante, consideramos A-autómatos isomorfos como sendo a mesma estrutura.

Dado um A-autómato $\mathcal{A} = (Q, I, T, E)$, dizemos que $\mathcal{A}' = (Q', I', T', E')$ é um *subautómato* de $\mathcal{A}$ se $\mathcal{A}'$ é um autómato tal que $Q' \subseteq Q$, $I' \subseteq I$, $T' \subseteq T$ e $E' \subseteq E$. Se $\sim$ é uma relação de equivalência em Q, o *autómato quociente* $\overline{\mathcal{A}} = (\overline{Q}, \overline{I}, \overline{T}, \overline{E})$ com respeito a $\sim$ é o A-autómato dado por

$$\begin{aligned}
\overline{Q} &= {}^{Q}\!/\!_{\sim} = \{[q] : q \in Q\};\\
\overline{I} &= {}^{I}\!/\!_{\sim} = \{[q] : q \in I\};\\
\overline{T} &= {}^{T}\!/\!_{\sim} = \{[q] : q \in T\};\\
\overline{E} &= \{([p], a, [q]) \ : \ (p, a, q) \in E\}.
\end{aligned}$$

onde $[q]$ representa a classe de equivalência de $q \in Q$. Um exemplo de relação de equivalência em Q é a relação induzida pelos automorfismos de $\Gamma_{\mathcal{A}}$, isto é, dados $p, q \in Q$, estes estão relacionados se e só se existe $\varphi \in Aut(\Gamma_{\mathcal{A}})$ tal que $p\varphi = q$. Nesta relação, usamos a notação $Orb(q)$ para representar a classe de equivalência $[q]$. Usamos também a notação $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$ para representar o autómato quociente com respeito a esta relação. Se $Orb(q) = Q$, então $\mathcal{A}$ diz-se *transitivo nos vértices*, isto é, é sempre possível enviar um vértice noutro vértice qualquer através de um automorfismo de $\Gamma_{\mathcal{A}}$. Se $Orb(q) = \{q\}$, então dizemos que $\mathcal{A}$ é *totalmente assimétrico*. Uma vez que $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$ é novamente um autómato, podemos tomar o autómato quociente com respeito à relação induzida pelos automorfismos de $\Gamma_{\mathcal{A}/Aut(\Gamma_{\mathcal{A}})}$. Usamos então a notação $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})^2$ para o representar, isto é,

$$\mathcal{A}/Aut(\Gamma_{\mathcal{A}})^2 = (\mathcal{A}/Aut(\Gamma_{\mathcal{A}}))/Aut(\Gamma_{\mathcal{A}/Aut(\Gamma_{\mathcal{A}})}).$$

De forma a simplificar a notação, definimos

$$\mathcal{A}/Aut(\Gamma_{\mathcal{A}})^{n+1} = (\mathcal{A}/Aut(\Gamma_{\mathcal{A}})^n)/Aut(\Gamma_{\mathcal{A}/Aut(\Gamma_{\mathcal{A}})^n})$$

para todo o $n \geq 0$, sendo $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})^0 = \mathcal{A}$. Dizemos que $\mathcal{A}$ é *totalmente simétrico* se, existe $n \in \mathbb{N}$, tal que $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})^n$ é transitivo nos vértices.

Note-se que todos estes conceitos definidos relativamente ao autómato $\mathcal{A}$ - transitivo nos vértices, totalmente simétrico e totalmente assimétrico - são avaliados em relação a $Aut(\Gamma_{\mathcal{A}})$ e não a $Aut(\mathcal{A})$. Assim, para estes conceitos, os vértices iniciais e terminais não desempenham qualquer papel.

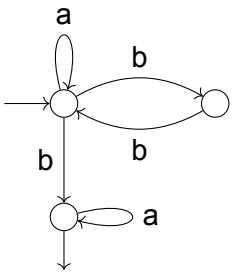
Uma das grande utilidades de um A-autómato é que ele permite definir uma A-linguagem do seguinte modo: Um *caminho não trivial* em $\mathcal{A} = (Q, I, T, E)$ é uma sequência da forma

$$q_0 \xrightarrow{a_1} \dots \xrightarrow{a_n} q_n$$

com $n \geq 1$ e $(q_{i-1}, a_i, q_i) \in E$ para $i \in \{1, \dots, n\}$. O seu *rótulo* é a palavra $a_1 \dots a_n \in A^*$ e diz-se um caminho *bem sucedido* se $q_0 \in I$ e $q_n \in T$. Consideramos também o *caminho trivial* $q \xrightarrow{1} q$ para cada $q \in Q$, cujo rótulo é a palavra vazia $1 \in A^*$ e diz-se bem sucedido se $q \in I \cap T$. Representamos por $q \xrightarrow{u} p$ qualquer caminho de rótulo u que se inicia em q e termina em p. Se $q = p$, dizemos que é um *caminho fechado*. Um caminho em que os vértices são todos distintos diz-se um *atalho*. Um A-autómato diz-se *aparado* se todo o vértice ocorre num caminho bem sucedido.

3.3. Linguagens racionais

A *linguagem reconhecida por um A-autómato $\mathcal{A}$* é o conjunto dos rótulos dos caminhos bem sucedidos em $\mathcal{A}$ e denotamos por $L(\mathcal{A})$. Dizemos também que $L(\mathcal{A})$ é o conjunto das palavras aceites (ou reconhecidas) por $\mathcal{A}$. Por exemplo, se $\mathcal{A}$ for o autómato dado por



então $L(\mathcal{A}) = \{a, bb\}^* ba^*$. Note-se que, neste exemplo, embora a palavra ab seja aceite por $\mathcal{A}$, existe em $\mathcal{A}$ um outro caminho, também com rótulo ab, que começa num vértice inicial mas que não acaba num vértice terminal. Portanto, para testar se uma palavra u é reconhecida por um determinado autómato, pode ser necessário considerar mais do que um caminho. Uma propriedade que elimina este tipo de situações é a seguinte: Um A-autómato $\mathcal{A} = (Q, I, T, E)$ diz-se *determinístico* se $|I| \leq 1$ e

$$(p, a, q), (p, a, r) \in E \Rightarrow q = r$$

para todos os $p, q, r \in Q$ e $a \in A$. Normalmente, na definição de autómato determinístico, exige-se que $|I| = 1$. No entanto, neste trabalho permitimos que $|I| \leq 1$, de forma a

abranger também a noção de grafo determinístico. Quando $I = \{q\}$ (respetivamente, $T = \{q\}$) para algum $q \in Q$, por vezes adotamos a notação (Q, q, T, E) (respetivamente, (Q, I, q, E)). Dado $X \subseteq A$, dizemos que $\mathcal{A}$ é *X-completo* se, para todos $q \in Q$ e $a \in X$, existe alguma aresta da forma (q, a, p) para algum $p \in Q$. Quando $X = A$, omitimos o índice X escrevendo apenas completo.

Uma A-linguagem L diz-se *racional* se $L = L(\mathcal{A})$ para algum A-autómato $\mathcal{A}$ e dois A-autómatos dizem-se *equivalentes* se reconhecem a mesma linguagem. Logo, autómatos isomorfos são equivalentes. Por vezes, no estudo de A-linguagens racionais, é útil permitir que os autómatos tenham arestas de rótulo $1 \in A^*$ e, a esta versão mais geral de autómato, damos o nome de *autómato com transições-*1. Uma vez que o determinismo pode facilitar o estudo da linguagem de um autómato, isto é, de linguagens racionais, seria interessante saber se, dado um A-autómato, existe sempre algum equivalente a este que seja e determinístico.

Teorema 3.3.1. *Seja L uma A-linguagem. As condições seguintes são equivalentes:*

(i) L é racional;

(ii) $L = L(\mathcal{A})$ para algum A-autómato determinístico e completo $\mathcal{A}$;

(iii) $L = L(\mathcal{A})$ para algum A-autómato com transições-1 $\mathcal{A}$;

(iv) existe um homomorfismo de monóides $\varphi : A^* \to M$ com M finito tal que $L = L\varphi\varphi^{-1}$.

Demonstração. $[(ii) \Rightarrow (i) \Rightarrow (iii)]$ Imediato.

$[(iii) \Rightarrow (iv)]$ Seja $\mathcal{A}$ um A-autómato com transições-1 tal que $L = L(\mathcal{A})$. Seja $M = 2^{Q \times Q}$ o conjunto de todas as relações binárias no conjunto Q. Dadas $R, S \in M$, a sua composição é definida por

$$R \circ S = \{(q, p) \in Q \times Q : (q, r) \in R, (r, p) \in S \text{ para algum } r \in Q\}.$$

Esta operação é associativa e a relação identidade 1_Q funciona como elemento neutro, logo M é de facto um monóide finito.

Definimos uma função $\varphi : A^* \to M$ do seguinte modo: Seja $1\varphi = 1_Q$. Para toda a palavra $u \in A^+$, fazemos

$$u\varphi = \{(q, p) \in Q \times Q : \text{ existe um caminho } \ q \xrightarrow{u} p \ \text{ em } \mathcal{A}\}.$$

Como $(uv)\varphi = (u\varphi) \circ (v\varphi)$ para todas as $u, v \in A^*$, podemos concluir que φ é um homomorfismo de monóides.

Claro que $L \subseteq L\varphi\varphi^{-1}$. Reciprocamente, suponhamos que $u\varphi = v\varphi$ para $u, v \in A^*$ e $u \in L$. Então, como $u \in L$, existe em $\mathcal{A}$ um caminho $i \xrightarrow{u} t$ tal que $i \in I$ e $t \in T$. Portanto, $(i,t) \in u\varphi = v\varphi$. Logo, existe em $\mathcal{A}$ um caminho $i \xrightarrow{v} t$. Logo, $v \in L$. Assim se conclui que $L = L\varphi\varphi^{-1}$.

$[(iv) \Rightarrow (ii)]$ Seja $\mathcal{A} = (M, 1_M, L\varphi, E)$ com

$$E = \{(x, a, y) \in M \times A \times M : y = x(a\varphi)\}.$$

É claro que $\mathcal{A}$ é um A-autómato determinístico e completo. Além disso, $q \xrightarrow{u} p$ é um caminho em $\mathcal{A}$ se e só se $p = q(u\varphi)$. Logo

$$L(\mathcal{A}) = \{u \in A^* : 1_M(u\varphi) \in L\varphi\} = L\varphi\varphi^{-1} = L$$

e a demonstração está completa. □

Proposição 3.3.2. *Sejam $L_1, L_2 \subseteq A^*$ linguagens racionais. Então, $L_1 \cup L_2$, $L_1 \cap L_2$ e L_1^c são também linguagens racionais.*

Demonstração. Uma vez que $L_1 \cap L_2 = (L_1^c \cup L_2^c)^c$, basta mostrar o resultado para a união e para o complemento. Sejam $\mathcal{A}_1 = (Q_1, I_1, T_1, E_1)$, $\mathcal{A}_2 = (Q_2, I_2, T_2, E_2)$ A-autómatos que reconhecem L_1 e L_2 respetivamente. Sem perda de generalidade, podemos supor que $Q_1 \cap Q_2 = \emptyset$. Pelo Teorema 3.3.1, podemos também supor que $\mathcal{A}_1$ é determinístico e completo. Note-se que, num A-autómato completo, se $u \in A^*$ e q é um vértice do autómato então conseguimos sempre ler a palavra u partindo de q, ou seja, existe sempre algum caminho com rótulo u que se inicia no vértice q. No caso de o autómato ser também determinístico, este caminho é único. Então,

$$L_1 \cup L_2 = L((Q_1 \cup Q_2, I_1 \cup I_2, T_1 \cup T_2, E_1 \cup E_2)),$$

$$L_1^c = L((Q_1, I_1, Q_1 \setminus T_1, E_1)). \quad \square$$

Proposição 3.3.3. *Sejam L_1 e L_2 A-linguagens racionais. Então as linguagens L_1L_2 e L_1^* são racionais.*

Demonstração. Sejam $\mathcal{A}_1 = (Q_1, I_1, T_1, E_1)$ e $\mathcal{A}_2 = (Q_2, I_2, T_2, E_2)$ os A-autómatos que reconhecem L_1 e L_2, respetivamente. Sem perda de generalidade, podemos supor que

$Q_1 \cap Q_2 = \emptyset$. Seja $\mathcal{A}$ o seguinte A-autómato com transições-1

$$\mathcal{A} = (Q_1 \cup Q_2, I_1, T_2, E_1 \cup E_2 \cup (T_1 \times \{1\} \times I_2)).$$

Note-se que os caminhos bem sucedidos em $\mathcal{A}$ são da forma

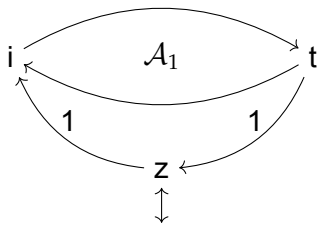
$$i_1 \xrightarrow{u} t_1 \xrightarrow{1} i_2 \xrightarrow{v} t_2$$

onde $i_1 \in I_1$, $t_1 \in T_1$, $i_2 \in I_2$, $t_2 \in T_2$, $u \in L_1$ e $v \in L_2$. Logo,

$$L(\mathcal{A}) = \{uv : u \in L_1, v \in L_2\} = L_1 L_2.$$

Considere-se agora um novo vértice $z \notin Q_1$ e seja $\mathcal{A}'$ o seguinte A-autómato com transições-1

$$\mathcal{A}' = (Q_1 \cup \{z\}, \{z\}, \{z\}, E_1 \cup (\{z\} \times \{1\} \times I_1) \cup (T_1 \times \{1\} \times \{z\})).$$



É fácil de ver que $L_1^* = L(\mathcal{A}')$. Então, pelo Teorema 3.3.1, concluímos que $L_1 L_2$ e L_1^* são racionais. □

Na Proposição 3.3.2, vimos que a interseção de duas linguagem racionais é racional. Para finalizar esta secção, deixamos aqui uma outra prova deste resultado que nos será útil mais tarde. Para tal, definimos o *autómato produto* de dois A-autómatos $\mathcal{A}_1 = (Q_1, I_1, T_1, E_1)$ e $\mathcal{A}_2 = (Q_2, I_2, T_2, E_2)$, como sendo o autómato dado por

$$\mathcal{A}_1 \times \mathcal{A}_2 = (Q_1 \times Q_2, I_1 \times I_2, T_1 \times T_2, E)$$

onde E é tal que

$$((p_1, p_2), a, (q_1, q_2)) \in E \Leftrightarrow \Big((p_1, a, q_1) \in E_1 \wedge (p_2, a, q_2) \in E_2\Big)$$

para todos os $p_1, q_1 \in Q_1$, $p_2, q_2 \in Q_2$ e $a \in A$.

Proposição 3.3.4. *Sejam* $\mathcal{A}_1 = (Q_1, I_1, T_1, E_1)$ *e* $\mathcal{A}_2 = (Q_2, I_2, T_2, E_2)$ *dois* A*-autómatos tais que* $L(\mathcal{A}_1) = L_1$ *e* $L(\mathcal{A}_2) = L_2$*. Então,* $L(\mathcal{A}_1 \times \mathcal{A}_2) = L_1 \cap L_2$.

Demonstração. Basta observar que $(p_1, p_2) \xrightarrow{u} (q_1, q_2)$ é um caminho bem sucedido em $\mathcal{A}_1 \times \mathcal{A}_2$ se e só se $p_1 \xrightarrow{u} q_1$ e $p_2 \xrightarrow{u} q_2$ são, respetivamente, caminhos bem sucedidos em $\mathcal{A}_1$ e em $\mathcal{A}_2$. □

3.4. Sistemas de reescrita

Um *sistema de reescrita* sobre um alfabeto A é um conjunto $\mathcal{R} \subseteq A^* \times A^*$. Dadas $u, v \in A^*$, escrevemos $u \to_{\mathcal{R}} v$ se existem $w_1, w_2 \in A^*$ e $(r, s) \in \mathcal{R}$ tais que $u = w_1 r w_2$, $v = w_1 s w_2$. Dizemos que $u \to_{\mathcal{R}} v$ é uma *redução elementar em* $\mathcal{R}$. Note-se que $\to_{\mathcal{R}}$ é uma relação binária em A^* que não é necessariamente reflexiva, simétrica ou transitiva.

Exemplo 3.4.1. *Seja* $A = \{a, b\}$ *e* $\mathcal{R} = \{(ab, b), (b, 1)\}$*. Então* $bab \to_{\mathcal{R}} bb$ *e* $bb \to_{\mathcal{R}} b$ *mas* $b \not\to_{\mathcal{R}} b$, $b \not\to_{\mathcal{R}} bb$ *e* $bab \not\to_{\mathcal{R}} b$.

Escrevemos, $u \xrightarrow{*}_{\mathcal{R}} v$ se existem $w_0, \ldots, w_n \in A^*$, tais que

$$u = w_0 \to_{\mathcal{R}} \ldots \to_{\mathcal{R}} w_n = v$$

para algum $n \geq 0$. Note-se que $\xrightarrow{*}_{\mathcal{R}}$ é o *fecho* reflexivo e transitivo de $\to_{\mathcal{R}}$, isto é, a menor relação reflexiva e transitiva em A^* que contem $\to_{\mathcal{R}}$. Dizemos que $u \in A^*$ é $\mathcal{R}$*-irredutível*, ou que se encontra na sua forma $\mathcal{R}$*-reduzida*, se não existir $v \in A^*$ tal que $u \to_{\mathcal{R}} v$ e designamos por *Irr($\mathcal{R}$)* o conjunto de todas as palavras $\mathcal{R}$-irredutíveis de A^*. Quando o sistema de reescrita for claro, omitimos o índice $\mathcal{R}$. Um sistema de reescrita $\mathcal{R} \subseteq A^* \times A^*$ diz-se:

- *finito*, se $\mathcal{R}$ for finito;
- *redutor*, se $|r| > |s|$ para todo o $(r, s) \in \mathcal{R}$;
- *noetheriano*, se não existir nenhuma cadeia infinita de reduções elementares

$$w_0 \to w_1 \to w_2 \to \cdots ;$$

• *confluente*, se sempre que $u \xrightarrow{*} v$ e $u \xrightarrow{*} w$, para $u, v, w \in A^*$, existir alguma $z \in A^*$ tal que $v \xrightarrow{*} z$ e $w \xrightarrow{*} z$;

$$\begin{array}{ccc} u & \xrightarrow{*} & v \\ {\scriptstyle *}\downarrow & & \downarrow{\scriptstyle *} \\ w & \xrightarrow{*} & z \end{array}$$

• *localmente confluente*, se sempre que $u \to v$ e $u \to w$, para $u, v, w \in A^*$, existir alguma $z \in A^*$ tal que $v \xrightarrow{*} z$ e $w \xrightarrow{*} z$.

$$\begin{array}{ccc} u & \longrightarrow & v \\ \downarrow & & \downarrow{\scriptstyle *} \\ w & \xrightarrow{*} & z \end{array}$$

Note-se que todo o sistema de reescrita confluente é localmente confluente. No entanto, o recíproco não se verifica.

Exemplo 3.4.2. *Seja* $A = \{a_n \mid n \geq 1\} \cup \{b, c\}$ *e*

$$\mathcal{R} = \{(a_n, a_{n+1}) : n \geq 1\} \cup \{(a_{2n}, b) : n \geq 1\} \cup \{(a_{2n-1}, c) : n \geq 1\}.$$

Vejamos primeiro que $\mathcal{R}$ *é localmente confluente. Seja* $u = xvy = x'v'y'$ *onde* $x, x', y, y' \in A^*$, $(v, w), (v', w') \in \mathcal{R}$ *e*

$$\begin{array}{ccc} u & \longrightarrow & xwy \\ \downarrow & & \\ x'w'y' & & \end{array}$$

Se as ocorrências de v *e* v' *em* u *forem disjuntas, podemos reproduzir a redução de tipo alternativo em cada uma das palavras* xwy *e* $x'w'y'$*. Portanto, para estudar a confluência local basta estudar os casos em que* v *e* v' *se sobrepõem. Temos então de avaliar dois casos:*

$$\begin{array}{ccc} xa_ny & \longrightarrow & xa_{n+1}y \\ \downarrow & & \\ xby & & \end{array}$$

quando n é par e,

$$\begin{array}{ccc} xa_ny & \longrightarrow & xa_{n+1}y \\ \downarrow & & \\ xcy & & \end{array}$$

quando n é ímpar. Ora, no primeiro caso, como n *é par, temos* $a_{n+1} \to a_{n+2} \to b$*. Logo,*

$$\begin{array}{ccc} xa_ny & \longrightarrow & xa_{n+1}y \\ \downarrow & & \downarrow{\scriptstyle *} \\ xby & \xrightarrow{*} & xby \end{array}$$

O segundo caso é análogo. Para mostrar que $\mathcal{R}$ não é confluente, observe-se que $a_2 \to a_3 \to c$ e $a_2 \to b$. Portanto,

$$\begin{array}{ccc} a_2 & \xrightarrow{*} & c \\ {\scriptstyle *}\downarrow & & \\ b & & \end{array}$$

mas, nesta situação, não conseguimos fazer mais nada.

No entanto se adicionarmos a $\mathcal{R}$ a propriedade de ser noetheriano, a implicação reciproca verifica-se.

Lema 3.4.3. *Seja $\mathcal{R} \subseteq A^* \times A^*$ um sistema de reescrita noetheriano e localmente confluente. Então $\mathcal{R}$ é confluente.*

Este resultado é conhecido como Lema de Newman e uma demonstração deste pode ser vista em [11].

É claro que todo o sistema de reescrita redutor é noetheriano. Também facilmente se observa o seguinte:

Proposição 3.4.4. *Seja $\mathcal{R} \subseteq A^* \times A^*$ um sistema de reescrita noetheriano e confluente. Para toda a palavra $u \in A^*$, existe uma e só uma $v \in Irr(\mathcal{R})$ tal que $u \xrightarrow{*} v$.*

Demonstração. A existência resulta de $\mathcal{R}$ ser noetheriano e a unicidade de $\mathcal{R}$ ser confluente. □

Se $\mathcal{R}$ é um sistema de reescrita noetheriano e confluente então, dada $u \in A^*$, representamos por $\overline{u}^{\mathcal{R}}$ a única $\overline{u}^{\mathcal{R}} \in Irr(\mathcal{R})$ tal que $u \xrightarrow{*} \overline{u}^{\mathcal{R}}$. Note-se que, pela Proposição 3.4.4 , $\overline{u}^{\mathcal{R}}$ está bem definida. Quando não houver risco de confusão relativamente ao sistema de reescrita considerado, usamos a notação $\overline{u}$.

4. Grupos Livres

Tendo estabelecido a existência de objetos livres nas categorias dos monóides e dos semigrupos, surge naturalmente a questão de saber se algo análogo pode ser construído no contexto dos grupos. Como já foi mencionado, a resposta é sim: também na categoria dos grupos existe um objeto livre gerado por um conjunto A, conhecido como grupo livre de base A. Neste capítulo será apresentada uma construção explícita do grupo livre.

4.1. Apresentações de grupos

Seja A um alfabeto. Designamos por $A^{-1} = \{a^{-1} \mid a \in A\}$ um conjunto de inversos formais dos elementos de A. Escrevemos $\widetilde{A} = A \cup A^{-1}$ e, de forma a não haver ambiguidade, $A \cap A^{-1} = \emptyset$. Seja $^{-1}$ a seguinte permutação de $\widetilde{A}^*$:

$$\begin{aligned} {}^{-1}\colon \widetilde{A}^* &\to \widetilde{A}^* \\ 1 &\mapsto 1 \\ a_1 \dots a_n &\mapsto a_n^{-1} \dots a_1^{-1} \end{aligned}$$

onde $a_1, \dots, a_n \in \widetilde{A}$ e $(a^{-1})^{-1} = a$ para todo $a \in A$. Definimos o seguinte sistema de reescrita em $\widetilde{A}$,

$$\mathcal{R}_A = \{(aa^{-1}, 1) : a \in \widetilde{A}\}.$$

Um sistema de reescrita $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$ diz-se *involutivo* se

$$1 \in Irr(\mathcal{R}) \text{ e } \mathcal{R}_A \subseteq \mathcal{R}.$$

Note-se que, se $\mathcal{R}$ é involutivo então, para toda a palavra $u \in \tilde{A}^*$, $uu^{-1} \xrightarrow{*} 1$. Se $\mathcal{R}$ é também confluente e noetheriano então, $\overline{uu^{-1}} = 1$. Estas propriedades permitem-nos construir um grupo $F_A^{\mathcal{R}}$ a partir de um sistema de reescrita noetheriano, confluente e involutivo (NCI) $\mathcal{R}$ da seguinte forma:

Definimos uma relação $\sigma_{\mathcal{R}}$ no monóide $\widetilde{A}^*$ dada por $u\sigma_{\mathcal{R}}v$ se e só se $\overline{u} = \overline{v}$. É claro que $\sigma_{\mathcal{R}}$ é uma relação de equivalência. Além disso, se $u_1\sigma_{\mathcal{R}}u_2$ e $v_1\sigma_{\mathcal{R}}v_2$, então $\overline{u_1} = \overline{u_2}$ e $\overline{v_1} = \overline{v_2}$. Logo, pela unicidade na Proposição 3.4.4, $\overline{u_1v_1} = \overline{\overline{u_1}\,\overline{v_1}} = \overline{\overline{u_2}\,\overline{v_2}} = \overline{u_2v_2}$ e, portanto, $u_1v_1\sigma_{\mathcal{R}}u_2v_2$. Então $\sigma_{\mathcal{R}}$ é uma congruência em $\widetilde{A}^*$. Seja $F_A^{\mathcal{R}} = \{u/\sigma_{\mathcal{R}} : u \in \widetilde{A}^*\}$

o monóide quociente. De facto, $F_A^{\mathcal{R}}$ é um grupo uma vez que,

$$\left(u/\sigma_{\mathcal{R}}\right)\left(u^{-1}/\sigma_{\mathcal{R}}\right) = (uu^{-1})/\sigma_{\mathcal{R}} = 1/\sigma_{\mathcal{R}}$$

para todo $u \in \widetilde{A}^*$. Note-se também que $(Irr(\mathcal{R}), \star)$ com $u \star v = \overline{uv}$ é um grupo e $F_A^{\mathcal{R}} \simeq (Irr(\mathcal{R}), \star)$ através do isomorfismo

$$\varphi \colon F_A^{\mathcal{R}} \to Irr(\mathcal{R})$$
$$u/\sigma_{\mathcal{R}} \mapsto \overline{u}$$

Portanto, é comum identificar o grupo $F_A^{\mathcal{R}}$ com o conjunto das palavras irredutíveis $Irr(\mathcal{R})$.

> Neste trabalho, quando for conveniente, utilizaremos essa identificação. Além disso, de forma a simplificar a notação, vamos denotar cada elemento de $F_A^{\mathcal{R}}$ por uma palavra de $\widetilde{A}^*$ que esteja na sua classe de equivalência.

A congruência $\sigma_{\mathcal{R}}$ utilizada para a construção de $F_A^{\mathcal{R}}$ tem uma propriedade que a caracteriza: $\mathcal{R} \subseteq \sigma_{\mathcal{R}}$ e se σ for uma outra congruência em $\widetilde{A}^*$ que contém $\mathcal{R}$ então $\sigma_{\mathcal{R}} \subseteq \sigma$, ou seja, $\sigma_{\mathcal{R}}$ é a menor congruência em $\widetilde{A}^*$ que contém $\mathcal{R}$. Podemos generalizar este conceito para qualquer sistema de reescrita.

Proposição 4.1.1. *Seja A um alfabeto, $\mathcal{R} \subseteq A^* \times A^*$ um sistema de reescrita. A interseção de todas as congruências em A^* que contêm $\mathcal{R}$ é uma congruência que denotamos por $\sigma_{\mathcal{R}}$. Dizemos que $\sigma_{\mathcal{R}}$ é a* congruência gerada por $\mathcal{R}$.

Demonstração. Existe pelo menos uma congruência que contém $\mathcal{R}$, nomeadamente $A^* \times A^*$. Como a interseção de relações de equivalência é ainda uma relação de equivalência, $\sigma_{\mathcal{R}}$ é uma relação de equivalência que contém $\mathcal{R}$. Suponhamos que $x\sigma_{\mathcal{R}}y$. Então, para cada palavra $z \in A^*$ e para cada congruência σ que contém $\mathcal{R}$, sabemos que $x\sigma y$ e, portanto, $(xz)\sigma(yz)$ e $(zx)\sigma(zy)$. Logo, $(xz)\sigma_{\mathcal{R}}(yz)$ e $(zx)\sigma_{\mathcal{R}}(zy)$. Concluímos assim que $\sigma_{\mathcal{R}}$ é uma congruência. □

Seja A um alfabeto e $\mathcal{R} \subseteq A^* \times A^*$. Denotamos por $Mon\langle A \mid \mathcal{R}\rangle$ o monóide quociente $A^*/\sigma_{\mathcal{R}}$, onde $\sigma_{\mathcal{R}}$ é a congruência gerada por $\mathcal{R}$. Se $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$ denotamos por $Grp\langle A \mid \mathcal{R}\rangle$ o monóide $Mon\langle \widetilde{A} \mid \mathcal{R} \cup \mathcal{R}_A\rangle$, que é um grupo. Note-se que, quando $\mathcal{R} \cup \mathcal{R}_A$ é um sistema de reescrita NCI, então $F_A^{\mathcal{R}\cup\mathcal{R}_A} = Grp\langle A \mid \mathcal{R}\rangle$. Dado um grupo G tal que $G \simeq Grp\langle A \mid \mathcal{R}\rangle$, dizemos que $\langle A \mid \mathcal{R}\rangle$ é uma *apresentação* de G. A apresentação diz-se *finita* se A e $\mathcal{R}$ forem ambos finitos e dizemos que G é *finitamente apresentável* se G admite uma apresentação finita.

4.2. Construção do grupo livre

Nesta secção vamos usar a construção de $F_A^{\mathcal{R}}$ para construir um grupo livre de base A, no sentido em que respeita a propriedade universal, dada na Proposição 2.2.1, na classe dos grupos. Para tal precisamos de um sistema de reescrita $\mathcal{R} \subset \widetilde{A}^* \times \widetilde{A}^*$ que seja NCI. Como queremos que A seja de alguma forma uma base, não convém que tal sistema $\mathcal{R}$ relacione as letras de $\widetilde{A}$ se essas relações não forem já trivialmente esperadas pelas que existem num grupo, tais como, $(aa^{-1}, 1)$ ou $(abb^{-1}a^{-1}c, c)$ no caso em que $A = \{a, b, c\}$.

Lema 4.2.1. *O sistema de reescrita $\mathcal{R}_A$ é NCI.*

Demonstração. Pela definição de $\mathcal{R}_A$, é claro que $\mathcal{R}_A$ é involutivo. Como para toda $(u, v) \in \mathcal{R}_A$, $|v| < |u|$, temos que $\mathcal{R}_A$ é redutor e, portanto, noetheriano. Pelo Lema 3.4.3, para mostrar a confluência basta mostrar a confluência local. Para tal, temos só de considerar o seguinte caso: Sejam $a_1, a_2 \in \widetilde{A}$ tais que

$$x_1 a_1 a_1^{-1} y_1 = u = x_2 a_2 a_2^{-1} y_2,$$

com $x_1, y_1, x_2, y_2 \in A^*$ e

$$\begin{array}{ccc} u & \longrightarrow & x_1 y_1 \\ \downarrow & & \\ x_2 y_2 & & \end{array}$$

Se as ocorrências $a_1 a_1^{-1}$ e $a_2 a_2^{-1}$ forem disjuntas, podemos reproduzir a redução de tipo alternativo em cada uma das palavras $x_1 y_1$ e $x_2 y_2$. Caso as ocorrências se sobreponham, resulta imediatamente $x_1 y_1 = x_2 y_2$. □

Uma vez que $\mathcal{R}_A$ é um sistema de reescrita NCI, podemos construir o grupo $F_A^{\mathcal{R}_A}$ e este vai ser um grupo livre de base A:

Proposição 4.2.2 (Propriedade universal de $F_A^{\mathcal{R}_A}$)**.** *Seja A um alfabeto e $\varphi : A \to G$ uma função de A num grupo G. Seja*

$$\begin{aligned} \iota \colon A &\to F_A^{\mathcal{R}_A} \\ a &\mapsto a/\sigma_{\mathcal{R}_A}. \end{aligned}$$

Então ι é injetiva e existe um único homomorfismo de grupos $\Phi : F_A^{\mathcal{R}_A} \to G$ tal que $\iota\Phi = \varphi$,

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & G \\ {\scriptstyle \iota}\downarrow & \nearrow_{\Phi} & \\ F_A^{\mathcal{R}_A} & & \end{array}$$

Demonstração. Como todas as letras são palavras irredutíveis relativamente a $\mathcal{R}_A$, resulta da Proposição 3.4.4 que ι é injetiva. Seja $\tilde{\varphi} : \widetilde{A} \to G$ a função que estende φ tal que $a^{-1}\tilde{\varphi} = (a\varphi)^{-1}$ para toda a letra $a \in A$. Pela propriedade universal de $\tilde{A}^*$, existe um único homomorfismo $\tilde{\Phi} : \widetilde{A}^* \to G$ que estende $\tilde{\varphi}$. Note-se que $u^{-1}\tilde{\Phi} = (u\tilde{\Phi})^{-1}$ para toda $u \in \widetilde{A}^*$. Portanto, dada $u \in \widetilde{A}^*$, temos que $u\tilde{\Phi} = \overline{u}\tilde{\Phi}$. Logo, dadas $u, v \in \widetilde{A}^*$, $u\sigma_{\mathcal{R}_A}v$ implica que $u\tilde{\Phi} = v\tilde{\Phi}$. Logo $\sigma_{\mathcal{R}_A} \subseteq ker(\tilde{\Phi})$. Pelo Teorema 2.1.2, existe um único homomorfismo de monóides $\Phi : F_A^{\mathcal{R}_A} \to G$ dado por

$$\begin{aligned} \Phi\colon F_A^{\mathcal{R}_A} &\to G \\ u/_{\sigma_{\mathcal{R}_A}} &\mapsto u\tilde{\Phi} \end{aligned}$$

De facto, Φ é um homomorfismo de grupos. Além disso, para $a \in A$, temos que $(a/_{\sigma_{\mathcal{R}_A}})\Phi = a\tilde{\Phi} = a\tilde{\varphi} = a\varphi$. Logo, $\iota\Phi = \varphi$. □

Um dos motivos pelos quais os grupos livres são tão importantes é dado pelo seguinte resultado:

Proposição 4.2.3. *Todo o grupo é isomorfo a algum quociente de um grupo livre.*

Demonstração. Seja G um grupo e $A \subseteq G$ um subconjunto de geradores de G. Seja φ a inclusão $\varphi : A \to G$. Então, pela propriedade universal de $F_A^{\mathcal{R}_A}$, φ induz um homomorfismo de grupos $\Phi : F_A^{\mathcal{R}_A} \to G$ tal que $\Phi|_A = \varphi$. Ora, como A gera G, Φ é sobrejetiva. Logo, $G \simeq F_A^{\mathcal{R}_A}/_{ker(\Phi)}$. □

Com uma prova análoga à do Corolário 2.2.2, usando a propriedade universal de $F_A^{\mathcal{R}_A}$ conseguimos mostrar que, a menos de isomorfismo, existe um único grupo livre de base A. Por este motivo, dizemos que $F_A^{\mathcal{R}_A}$ é *o grupo livre de base A*. Podemos então averiguar quando é que dois grupos livres são isomorfos.

Teorema 4.2.4. *Sejam A, B alfabetos. Então,*

$$F_A^{\mathcal{R}_A} \simeq F_B^{\mathcal{R}_B} \Leftrightarrow |A| = |B|.$$

Uma demonstração deste resultado pode ser vista em [25].

Outra pergunta que naturalmente se levanta é a seguinte: Se G é um grupo e $B \subseteq G$ um subconjunto de G, quando é que G é livre de base B? Ora, se considerarmos o grupo livre $F_B^{\mathcal{R}_B}$, resulta da propriedade universal a existência de um homomorfismo $\Phi : F_B^{\mathcal{R}_B} \to G$ que será sobrejetivo se $G = \langle B \rangle$. Assumindo que B gera G, o que está em causa é

saber se Φ é injetiva. Isto equivale a ter $ker(\Phi) = \{1\}$, isto é, a única palavra $b_1^{\epsilon_1} \dots b_n^{\epsilon_n}$ irredutível, com $b_i \in B$, $\epsilon_i \in \{-1, 1\}$ e $n \in \mathbb{N}$, tal que $b_1^{\epsilon_1} \dots b_n^{\epsilon_n} = 1$ em G é a palavra vazia. Caso estas condições se verifiquem, dizemos que B é uma *base* de G. Além disso, pelo Teorema 4.2.4, sabemos que todas as bases de um mesmo grupo livre G possuem a mesma cardinalidade, à qual damos o nome de *dimensão* de G e denotamos por $dim(G)$. Surge então a questão recíproca. Ou seja, se $B' \subseteq F_B^{\mathcal{R}_B}$ é tal que $\langle B' \rangle = F_B^{\mathcal{R}_B}$ e $|B'| = |B|$, podemos concluir que B' é uma base de $F_B^{\mathcal{R}_B}$? Ora no caso em que B é finito, a resposta a esta pergunta é sim e resulta do facto de, nesse caso, $F_B^{\mathcal{R}_B}$ ser *hopfiano*: Dizemos que um grupo G é hopfiano se todo o homomorfismo sobrejetivo $\varphi : G \to G$ for injetivo. Uma prova deste resultado pode ser vista em [16]. Se B não for finito, não podemos dizer o mesmo. Por exemplo, $F_{\mathbb{N}}^{\mathcal{R}_{\mathbb{N}}} = \langle \{00\} \cup \mathbb{N} \rangle$ e $|\mathbb{N}| = |\{00\} \cup \mathbb{N}|$ mas $\{00\} \cup \mathbb{N}$ não é uma base de $F_{\mathbb{N}}^{\mathcal{R}_{\mathbb{N}}}$.

No inicio deste capítulo, foi visto que, no caso em que $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$ é um sistema de reescrita NCI, então $F_A^{\mathcal{R}}$ é um grupo. Temos também o seguinte:

Proposição 4.2.5. *Seja G um grupo. Então existe um alfabeto A e um sistema de reescrita NCI, $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$, tal que $G \simeq F_A^{\mathcal{R}}$. Se G for finito, podemos assumir que A e $\mathcal{R}$ também o são. Além disso, para todo $a \in \widetilde{A}$, $\overline{a}^{\mathcal{R}} \neq 1$.*

Demonstração. Construa-se o alfabeto $A = \{a_g \mid g \in G \backslash \{1_G\}\}$. Seja $\mathcal{R} = C_1 \cup C_2 \cup C_3 \cup C_4$ um sistema de reescrita em $\widetilde{A}^* \times \widetilde{A}^*$ onde,

$$
\begin{aligned}
C_1 &= \{(a_{g_1} a_{g_2}, a_{g_1 g_2}) \mid a_{g_1}, a_{g_2} \in A \text{ e } g_1 g_2 \neq 1_G\},\\
C_2 &= \{(a_g a_{g^{-1}}, 1) \mid a_g \in A\},\\
C_3 &= \{(a_g^{-1}, a_{g^{-1}}) \mid a_g \in A\},\\
C_4 &= \{(a_g a_g^{-1}, 1) \mid a_g \in \widetilde{A}\}.
\end{aligned}
$$

Pela definição de $\mathcal{R}$, temos que $\mathcal{R}$ é involutivo. Embora as reduções do tipo C_4 sejam deduzidas a partir das outras, estas são necessárias para que $\mathcal{R}$ seja involutivo. Note-se que, dada uma palavra $u \in \widetilde{A}^*$, apenas um número finito de reduções do tipo C_3 se pode aplicar a u e mantêm sempre o comprimento da palavra u. Além disso, se $(u, v) \in C_1 \cup C_2 \cup C_4$, então $|u| > |v|$. Logo o sistema de reescrita $\mathcal{R}$ é noetheriano. Basta provar a confluência para $\mathcal{R}$ ser NCI. Note-se que A é um alfabeto indexado por $G \backslash \{1_G\}$ e o sistema $\mathcal{R}$ opera as palavras em $\widetilde{A}^*$ com regras que modelam:

• A operação de G (C_1 e C_2);

• A identificação de inversos formais com os elementos inversos de G (C_3);

• A redução de elementos com os seus inversos à identidade (C_4).

Assim sendo, $\mathcal{R}$ define uma reescrita que implementa a multiplicação e simplificação no grupo G via palavras. Como cada palavra em $\widetilde{A}^*$ representa uma sequência de multiplicações e inversos no grupo G, a aplicação sucessiva das regras de $\mathcal{R}$ transforma qualquer palavra $u \in \widetilde{A}^*$ numa palavra reduzida correspondente a um único elemento $g \in G$, representado por a_g, se $g \neq 1$, ou 1, se $g = 1_G$. Ou seja, dados $g_1, g_2, g_3 \in G\backslash\{1_G\}$, a palavra $a_{g_1}a_{g_2}^{-1}a_{g_3}$ de $\widetilde{A}^*$, na sua forma $\mathcal{R}$-reduzida é, $a_{g_1g_2^{-1}g_3}$ se $g_1g_2^{-1}1g_3 \neq 1_G$, ou 1 caso contrário.

Logo, $\mathcal{R}$ é confluente. Veja-se um exemplo concreto, através da seguinte situação

$$\begin{array}{ccc} xa_ga_g^{-1}y & \longrightarrow & xa_ga_{g^{-1}}y \\ \downarrow & & \\ xy & & \end{array}$$

para algum $a_g \in A$, $x, y \in \widetilde{A}^*$. Aplicando a redução $(a_ga_{g^{-1}}, 1)$ na palavra $xa_ga_{g^{-1}}y$ obtemos $x1y = xy$. Seja $\varphi : G \to F_A^{\mathcal{R}}$ tal que

$$g\varphi = \begin{cases} a_g/_{\sigma_{\mathcal{R}'}} & \text{se } g \neq 1_G \\ 1/_{\sigma_{\mathcal{R}'}} & \text{se } g = 1_G \end{cases}$$

Ora, φ é um homomorfismo de grupos e $a_g/_{\sigma_{\mathcal{R}}} \neq 1/_{\sigma_{\mathcal{R}}}$ para todo $g \neq 1_G$, logo φ é injetiva. Seja $u/_{\sigma_{\mathcal{R}}} \in F_A^{\mathcal{R}}$ não trivial. Então $\overline{u} = a_g$ para algum $g \in G\backslash\{1_G\}$. Logo $g\varphi = u/_{\sigma_{\mathcal{R}}}$ e φ é sobrejetiva. Portanto, $G \simeq F_A^{\mathcal{R}}$. Agora basta notar que no caso em que G é finito, o alfabeto A é finito e, portanto, $\mathcal{R}$ também é finito. □

Dado um grupo G, a demonstração da Proposição 4.2.5 dá-nos uma 'receita' para obter um alfabeto A e um sistema de reescrita $\mathcal{R}$ para o qual $G \simeq F_A^{\mathcal{R}}$. No entanto, estes não são únicos nem são necessariamente os mais simples de se trabalhar. Por exemplo, se $G = \{1, g, \ldots, g^{n-1}\}$ for o grupo cíclico de ordem n para algum $n \geq 1$, o alfabeto A, obtido seguindo os passos dados na demonstração, seria $A = \{a_g, \ldots, a_{g^{n-1}}\}$ composto por $n-1$ letras. Portanto $|\mathcal{R}| = |C_1| + |C_2| + |C_3| + |C_4| = (n-1)(n-2) + (n-1) + (n-1) + 2(n-1)$. Na próxima proposição vemos um exemplo de outro alfabeto A e sistema de reescrita NCI $\mathcal{R}$ que têm, respetivamente, cardinalidades 1 e 4 e tais que $F_A^{\mathcal{R}}$

é também o grupo cíclico de ordem n. Dadas $u \in \widetilde{A}^*$ e $a \in \widetilde{A}$, definimos $N_a(u)$ como o número de ocorrências da letra a em u.

Proposição 4.2.6. *Seja $\mathbb{Z}_n$ o grupo cíclico de ordem n para algum $n \geq 1$, $A = \{a\}$ um alfabeto e $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$ um sistema de reescrita dado por, $\mathcal{R} = \mathcal{R}_A \cup \{(a^n, 1), (a^{-1}, a^{n-1})\}$. Então $\mathcal{R}$ é NCI e $\mathbb{Z}_n \simeq F_A^{\mathcal{R}}$.*

Demonstração. Seja $u \in \widetilde{A}^*$. Então as letras que compõem u são a e a^{-1}. Seja $R(u) = N_a(u) - N_{a^{-1}}(u) \pmod n$. Por definição, $\mathcal{R}$ é involutivo. Além disso, a redução (a^{-1}, a^{n-1}) pode ser aplicada apenas um número finito de vezes a u e se $(v, w) \in \mathcal{R}$ é uma outra redução então $|v| > |w|$. Logo $\mathcal{R}$ é noetheriano. Logo, existe $z \in Irr(\mathcal{R})$ tal que $u \xrightarrow{*} z$. Note-se que, se $(v, w) \in \mathcal{R}$ então $R(v) = R(w)$ e isto implica que $R(u) = R(z)$. Também é fácil de ver que $Irr(\mathcal{R}) = \{1, a, \ldots, a^{n-1}\}$. Resulta destas duas observações que $\mathcal{R}$ é também confluente. Logo $F_A^{\mathcal{R}}$ é um grupo isomorfo a $Irr(\mathcal{R})$ e este é claramente o grupo cíclico de ordem n. □

5. Produto livre

Na Matemática, um dos temas centrais é entender como estruturas algébricas podem ser combinadas ou construídas a partir de outras. Uma das operações mais fundamentais em teoria de grupos nesse contexto é o produto direto, que combina dois grupos G_1 e G_2 impondo que os elementos de um comutem com os do outro. Portanto, embora preserve as operações internas de cada grupo, o produto direto introduz relações de comutatividade entre os fatores. No entanto, em muitas situações matemáticas - especialmente na topologia, teoria de apresentações e álgebra combinatória - surge a necessidade de combinar grupos sem impor relações adicionais entre eles além das que já existem internamente.

É justamente aqui que entra o conceito de produto livre de grupos. Ao contrário do produto direto, o produto livre permite "colar" grupos de forma mais flexível, sem interferência mútua entre as respetivas estruturas internas. De modo informal, o produto livre de dois grupos G_1 e G_2 é o grupo "mais geral possível" que contém cópias de G_1 e G_2 e nada mais.

Definição 5.0.1. *Dizemos que o grupo G é* produto livre *dos grupos G_1 e G_2 se existirem homomorfismos $\iota_i : G_i \to G$ $(i \in \{1,2\})$ tais que: para todo o grupo H e homomorfismos $\varphi_i : G_i \to H$ $(i \in \{1,2\})$, existe um único homomorfismo $\Phi : G \to H$ tal que o seguinte diagrama comuta,*

$$\begin{array}{ccccc} G_1 & \xrightarrow{\iota_1} & G & \xleftarrow{\iota_2} & G_2 \\ & \searrow^{\varphi_1} & \downarrow{\scriptstyle \Phi} & \swarrow_{\varphi_2} & \\ & & H & & \end{array}$$

O próximo resultado afirma que se um produto livre de dois grupos existir, este é único a menos de isomorfismo.

Proposição 5.0.2. *Sejam G_1 e G_2 grupos e G, G' produtos livres de G_1 e G_2 para os homomorfismos $\iota_i : G_i \longrightarrow G$ e $\iota_i' : G_i \longrightarrow G'$ $(i \in \{1,2\})$, respetivamente. Então $G \simeq G'$.*

Demonstração. Sejam $\Phi : G \to G'$ e $\Phi' : G' \to G$ homomorfismos tais que $\iota_i\Phi = \iota'_i$ e $\iota'_i\Phi' = \iota_i$ $(i \in \{1,2\})$. Então temos o seguinte diagrama comutativo,

$$\begin{array}{ccccc} G_1 & \xrightarrow{\iota_1} & G & \xleftarrow{\iota_2} & G_2 \\ & \searrow^{\iota_1} & \circlearrowleft^{\Phi\Phi'} \quad \circlearrowright_{1_G} & \swarrow_{\iota_2} & \\ & & G & & \end{array}$$

Como G é produto livre de G_1 e G_2, pela definição, sabemos que $\Phi\Phi' = 1_G$. Analogamente se mostra que $\Phi'\Phi = 1_{G'}$. Logo Φ e Φ' são isomorfismos e $G \simeq G'$. □

Usamos a notação $G_1 * G_2$ para representar o produto livre de G_1 e G_2 (caso exista).

Corolário 5.0.3. *Sejam G_1, G_2, G'_1, G'_2 grupos tais que $G_1 \simeq G'_1$ e $G_2 \simeq G'_2$. Se o produto livre de G_1 e de G_2 existir, então também existe o de G'_1 e de G'_2 e temos $G_1 * G_2 \simeq G'_1 * G'_2$.*

Demonstração. Ora, por hipótese, o produto livre $G_1 * G_2$ existe para determinados homomorfismos $\iota_i : G_i \to G_1 * G_2$ $(i \in \{1,2\})$. Sejam $\varphi_i : G_i \to G'_i$ isomorfismos de grupos $(i \in \{1,2\})$. Pela Proposição 5.0.2, basta mostrar que $G_1 * G_2$ é um produto livre de G'_1 e G'_2. Seja então H um grupo e $\phi_i : G'_i \to H$ homomorfismos de grupo $(i \in \{1,2\})$. Então $\varphi_i\phi_i : G_i \to H$ $(i \in \{1,2\})$ são homomorfismos de grupos. Logo existe um único homomorfismo $\Phi : G_1 * G_2 \to H$ tal que $\iota_i\Phi = \varphi_i\phi_i$ $(i \in \{1,2\})$. Sejam $\iota'_i = (\varphi_i)^{-1}\iota_i$ $(i \in \{1,2\})$. Então $\iota'_i\Phi = (\varphi_i)^{-1}\iota_i\Phi = (\varphi_i)^{-1}\varphi_i\phi_i = \phi_i$. Logo temos o seguinte diagrama comutativo:

$$\begin{array}{ccccc} G_1 & \xrightarrow{\iota_1} & G_1 * G_2 & \xleftarrow{\iota_2} & G_2 \\ {\scriptstyle\varphi_1}\downarrow & & \downarrow{\scriptstyle\Phi} & & \downarrow{\scriptstyle\varphi_2} \\ G'_1 & \xrightarrow[\phi_1]{} & H & \xleftarrow[\phi_2]{} & G'_2 \end{array}$$

Suponhamos agora que existe $\Phi' : G_1 * G_2 \to H$ tal que

$$\begin{array}{ccccc} G_1 & \xrightarrow{\iota_1} & G_1 * G_2 & \xleftarrow{\iota_2} & G_2 \\ {\scriptstyle\varphi_1}\downarrow & & \downarrow{\scriptstyle\Phi'} & & \downarrow{\scriptstyle\varphi_2} \\ G'_1 & \xrightarrow[\phi_1]{} & H & \xleftarrow[\phi_2]{} & G'_2 \end{array}$$

é também um diagrama comutativo. Então, $\iota_i\Phi' = \varphi_i\phi_i$. Logo, pela unicidade de Φ da propriedade universal de $G_1 * G_2$ resulta que $\Phi' = \Phi$. □

5.1. Existência do produto livre

Nesta secção, vamos mostrar que o produto livre existe sempre.

Definição 5.1.1. *Seja $P = \{A_i\}_{i\in\{1,\dots,n\}}$, $n \geq 1$, uma partição de um alfabeto A e $u \in \widetilde{A}^*$. Então u é a palavra vazia ou*

$$u = u_1 \dots u_m$$

para algum $m \geq 1$, $u_j \in \cup_{i=1}^{n} \widetilde{A_i}^+$, $j \in \{1, \dots, m\}$, e tal que

$$u_j \in \widetilde{A_i}^+ \Rightarrow u_{j+1} \notin \widetilde{A_i}^+$$

para todo o $j \in \{1, \dots, m-1\}$.

Quando estamos no segundo caso, aos $u_j's$ damos o nome de componentes homogéneas relativas a P *e dizemos que $u_1 \dots u_m$ é a fatorização de u em componentes homogéneas relativamente a P. Note-se que esta fatorização é única e definimos $H_P[u] = m$. No caso em que u não tem componentes homogéneas, ou seja $u = 1$, definimos também $H_P[1] = 0$. Quando não houver risco de confusão relativamente à partição em causa, omitimos o índice P ficando apenas $H[u]$ e $H[1]$.*

Lema 5.1.2. *Sejam A_1 e A_2 dois alfabetos disjuntos. Se, para $i \in \{1,2\}$, $\mathcal{R}_i \subseteq \widetilde{A_i}^* \times \widetilde{A_i}^*$ for um sistema de reescrita NCI, então, escrevendo $A = A_1 \cup A_2$ e $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$, resulta que $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$ é um sistema de reescrita NCI sobre $\widetilde{A}$.*

Demonstração. Seja $P = \{A_1, A_2\}$. Então P é uma partição de A. Dada $a \in \widetilde{A}$, então $a \in \widetilde{A_i}$ para algum $i \in \{1,2\}$. Logo, $(aa^{-1}, 1) \in \mathcal{R}_i \subseteq \mathcal{R}$. Além disso $1 \in \widetilde{A}^*$ é também $\mathcal{R}$-irredutível. Portanto, $\mathcal{R}$ é involutivo. Seja $u \in \widetilde{A}^*$. Vamos mostrar que o número de reduções elementares aplicadas consecutivamente a u é finito. Para tal, vamos usar indução sobre $H[u]$. Se $H[u] = 0$, então $u = 1$ e não admite reduções. Suponhamos o resultado válido para palavras v tais que $H[v] \leq k$, para um dado $k \in \mathbb{N}$, e suponhamos que $H[u] = k+1$. Note-se que, como $\mathcal{R}_1$, $\mathcal{R}_2$ são noetherianos e $\mathcal{R}_1 \cap \mathcal{R}_2 = \emptyset$, o número de reduções elementares consecutivas aplicadas a u que preservam o número de componentes homogéneas tem de ser finito. Por outro lado, se numa dada redução, o número de componentes homogéneas diminui, aplicamos a hipótese de indução. Logo $\mathcal{R}$ é noetheriano. Portanto, pelo Lema 3.4.3, para mostrar a confluência basta mostrar a confluência local. Como $\mathcal{R}_1$ e $\mathcal{R}_2$ são confluentes e $A_1 \cap A_2 = \emptyset$, a confluência local de $\mathcal{R}$ resulta da confluência local em $\mathcal{R}_1$ e $\mathcal{R}_2$. □

Proposição 5.1.3. *Sejam A_1 e A_2 alfabetos disjuntos e $\mathcal{R}_1 \subseteq \widetilde{A_1}^* \times \widetilde{A_1}^*$, $\mathcal{R}_2 \subseteq \widetilde{A_2}^* \times \widetilde{A_2}^*$ sistemas de reescrita NCI. Seja $A = A_1 \cup A_2$ e $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2 \subseteq \widetilde{A}^* \times \widetilde{A}^*$. Então $F_A^{\mathcal{R}}$ é o produto livre de $F_{A_1}^{\mathcal{R}_1}$ com $F_{A_2}^{\mathcal{R}_2}$, isto é, $F_{A_1}^{\mathcal{R}_1} * F_{A_2}^{\mathcal{R}_2}$.*

Demonstração. Observe-se primeiro que, pela Proposição 5.1.2, $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$ é um sistema de reescrita NCI. Logo, o grupo $F_A^{\mathcal{R}}$ está bem definido.

Como $(Irr(\mathcal{R}_i), \star) \simeq F_A^{\mathcal{R}_i}$ ($i \in \{1,2\}$) e $(Irr(\mathcal{R}), \star) \simeq F_A^{\mathcal{R}}$, pelo Corolário 5.0.3, basta mostrar que $(Irr(\mathcal{R}), \star)$ é o produto livre dos grupos $(Irr(\mathcal{R}_1), \star)$ e $(Irr(\mathcal{R}_2), \star)$. Note-se que $Irr(\mathcal{R}_1), Irr(\mathcal{R}_2) \subseteq Irr(\mathcal{R})$. Para $i \in \{1,2\}$, seja ι_i a inclusão $\iota_i : Irr(\mathcal{R}_i) \longrightarrow Irr(\mathcal{R})$. Sejam H um grupo e $\varphi_i : Irr(\mathcal{R}_i) \to H$ homomorfismos de grupos, $i \in \{1,2\}$.

Definimos o homomorfismo de monóides $\varphi : \widetilde{A}^* \to H$ dado por $a\varphi = \overline{a}^{\mathcal{R}_i}\varphi_i$ se $a \in A_i$, $i \in \{1,2\}$. Seja $\Phi = \varphi|_{Irr(\mathcal{R})}$. Para todo $u \in Irr(\mathcal{R}_1)$, $u\iota_1\Phi = u\varphi_1$ e portanto $\iota_1\Phi = \varphi_1$. Analogamente, $\iota_2\Phi = \varphi_2$. Para mostrar que Φ é um homomorfismo de grupos, temos de provar que $(u \star v)\Phi = (u\Phi)(v\Phi)$ para todos $u, v \in Irr(\mathcal{R})$. Como

$$(u\Phi)(v\Phi) = (u\varphi)(v\varphi) = (uv)\varphi,$$

basta verificar que $r\varphi = s\varphi$ sempre que $(r,s) \in \mathcal{R}$. Se $(r,s) \in \mathcal{R}$ então $(r,s) \in \mathcal{R}_i$ para algum $i \in \{1,2\}$. Mas então

$$r\varphi = \overline{r}^{\mathcal{R}_i}\varphi_i = \overline{s}^{\mathcal{R}_i}\varphi_i = s\varphi$$

uma vez que $\overline{r}^{\mathcal{R}_i} = \overline{s}^{\mathcal{R}_i}$. Logo Φ é um homomorfismo. Finalmente, a unicidade resulta do facto de $X = Irr(\mathcal{R}_1) \cup Irr(\mathcal{R}_2)$ gerar $Irr(\mathcal{R})$ e $\Phi|_X$ estar univocamente determinado. □

Exemplo 5.1.4. *Um dos exemplos mais simples de produto livre é $\mathbb{Z}_2 * \mathbb{Z}_2$. Ora, pela Proposição 4.2.6, para $i \in \{1,2\}$, temos que*

$$\mathcal{R}_i = \{(a_i a_i^{-1}, 1), (a_i^{-1} a_i, 1), (a_i^2, 1), (a_i^{-1}, a_i)\}$$

é um sistema de reescrita NCI, no alfabeto $\{a_i, a_i^{-1}\}$. Além disso, temos ainda $F_{\{a_i\}}^{R_i} \simeq \mathbb{Z}_2$. Portanto, pelo Corolário 5.0.3 e pela Proposição 5.1.3, $\mathbb{Z}_2 * \mathbb{Z}_2$ é isomorfo a

$$Grp\langle a_1, a_2 | \mathcal{R}_1 \cup \mathcal{R}_2 \rangle = F_{\{a_1,a_2\}}^{\mathcal{R}_1 \cup \mathcal{R}_2}.$$

que, por sua vez, é isomorfo ao grupo diedral infinito, $D_\infty = \langle r, t \mid (r^2,1), (rtrt,1) \rangle$. Seja $\phi : F_{\{a_1,a_2\}}^{\mathcal{R}_{\{a_1,a_2\}}} \to D_\infty$ tal que $a_1\phi = r$, $a_2\phi = tr$. Então, $(a_i a_i^{-1})\phi = (a_i^{-1}a_i)\phi = (1)\phi = 1$, $(a_1^2)\phi = r^2 = 1$, e $(a_2^2)\phi = trtr = t(rtrt)t^{-1} = 1$. Logo, $\mathcal{R}_1 \cup \mathcal{R}_2 \subseteq ker(\phi)$ e, pela Proposição 4.1.1, $\sigma_{\mathcal{R}_1 \cup \mathcal{R}_2} \subseteq ker(\phi)$. Logo, pelo teorema do homomorfismo, existe um homomorfismo de grupos $\phi' : F_{\{a_1,a_2\}}^{\mathcal{R}_1 \cup \mathcal{R}_2} \to D_\infty$ tal que $a_1\phi' = r$ e $a_2\phi' = tr$. Seja agora $\varphi : F_{\{r,t\}}^{\mathcal{R}_{\{r,t\}}} \to F_{\{a_1,a_2\}}^{\mathcal{R}_1 \cup \mathcal{R}_2}$ tal que $r\varphi = a_1$ e $t\varphi = a_2 a_1$. Como $(r^2)\varphi = a_1^2 = 1$ e $(rtrt)\varphi = (a_1 a_2 a_1)(a_1 a_2 a_1) = 1$, podemos concluir que $\mathcal{R} = \{(r^1,1), (rtrt,1)\} \subseteq ker(\varphi)$. Logo

$\sigma_{\mathcal{R}} \subseteq ker(\varphi)$ *e existe um homomorfismo* $\varphi' : D_\infty \to F^{\mathcal{R}_1 \cup \mathcal{R}_2}_{\{a_1,a_2\}}$ *tal que* $r\varphi' = a_1$ *e* $t\varphi' = a_1a_2$. *Agora, basta notar que* ϕ' *e* φ' *são mutuamente inversas e, portanto, são isomorfismos.*

Pela Proposição 4.2.5, sabemos que todo o grupo é isomorfo a um $F^{\mathcal{R}}_A$ para algum alfabeto A e sistema de reescrita NCI, $\mathcal{R}$. Juntamente com o Corolário 5.0.3 e a Proposição 5.1.3, podemos concluir que, dados dois grupos G_1 e G_2, existe sempre o produto livre $G_1 * G_2$. Além disso, se H é um grupo gerado por $G_1 \cup G_2$, então H é imagem homomorfa de $G_1 * G_2$. Portanto, faz sentido dizer que $G_1 * G_2$ é o maior grupo gerado por $G_1 \cup G_2$.

Sejam $G_1, \ldots, G_n$ grupos para um dado $n \geq 3$. Definimos o respetivo produto livre recursivamente, isto é,

$$G_1 * \ldots * G_n = (G_1 * \ldots * G_{n-1}) * G_n$$

É fácil de ver que a definição recursiva de $G_1 * \ldots * G_n$ é coerente com a extensão da Definição 5.0.1 aplicada a mais de dois grupos, isto é,

Definição 5.1.5. *O produto livre de uma família de grupos* $\{G_i\}$, *onde* $i \in \{1, \ldots, n\}$ *para algum* $n \geq 1$, *é um grupo* G *para o qual existem homomorfismos* $\iota_i : G_i \to G$ *com a seguinte propriedade: para qualquer grupo* H *e qualquer família de homomorfismos* $\varphi_i : G_i \to H$, *existe um único homomorfismo* $\Phi : G \to H$ *tal que* $\iota_i\Phi = \varphi_i$.

Exemplo 5.1.6. *Seja* $A = \{a_1, \ldots, a_n\}$, $n \geq 1$. *Então, pela Proposição 5.1.3,*

$$F^{\mathcal{R}_A}_A = F^{\mathcal{R}_{\{a_1\}}}_{\{a_1\}} * \ldots * F^{\mathcal{R}_{\{a_n\}}}_{\{a_n\}}.$$

Uma vez que $F^{\mathcal{R}_{\{a_i\}}}_{\{a_i\}} \simeq \mathbb{Z}$, *para todo* $i \in \{1, \ldots, n\}$, *temos que* $F^{\mathcal{R}_A}_A \simeq *^n_{i=1}\mathbb{Z}$, *ou seja, um grupo livre é o produto livre de* $\mathbb{Z}'s$.

Quando um grupo é descrito como o produto livre de dois ou mais grupos, faz sentido tentar responder a certas questões em função dos respetivos fatores que o compõem. Um exemplo é o seguinte Teorema de Kurosh.

Teorema 5.1.7 (Alexander Kurosh, 1934)**.** *Seja* $G = K * N$ *o produto livre dos grupos* K *e* N *e seja* H *um subgrupo finitamente gerado de* G. *Então, existe uma família finita* $(K_i)_{i\in I}$ *de subgrupos* $K_i \leq K$, *uma família finita* $(N_j)_{j\in J}$ *de subgrupos* $N_j \leq N$, *famílias* $(g_i)_{i\in I}$ *e* $(f_j)_{j\in J}$ *de elementos de* G, *e um subconjunto finito* $X \subseteq G$ *tais que*

$$H = F^{\mathcal{R}_X}_X * (*_{i\in I}\, g_iK_ig_i^{-1}) * (*_{j\in J}\, f_jN_jf_j^{-1}),$$

onde $F^{\mathcal{R}_X}_X$ *é o grupo livre gerado por X.*

Uma demonstração deste resultado pode ser vista em [24]. Note-se que, do Teorema 5.1.7 e do Exemplo 5.1.6, resulta que os subgrupos finitamente gerados de um grupo livre finitamente gerado são também grupos livres: os únicos subgrupos de $\mathbb{Z}$ não triviais são isomorfos a $\mathbb{Z}$ e subgrupos conjugados são isomorfos, isto é, se $K_1, K_2 \leq G$ e $K_2 = gK_1g^{-1}$ para algum $g \in G$ então $K_1 \simeq K_2$. Na verdade, este resultado era já conhecido e foi descoberto por Nielsen em 1921.

Corolário 5.1.8 (Nielsen)**.** *Todo o subgrupo finitamente gerado de um grupo livre é também livre.*

Mais tarde, em 1926, Schreier provou a sua versão mais geral.

Corolário 5.1.9 (Nielsen-Schreier)**.** *Todo o subgrupo de um grupo livre é também livre.*

Uma demonstração do Teorema de Nielsen-Schreier pode ser encontrada também em [24].

6. Decidibilidade

Uma das maneiras mais comuns de especificar um grupo G é através de uma apresentação $\langle A \mid \mathcal{R} \rangle$ onde A é um alfabeto e $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$. Quando um grupo é definido como um quociente de $\widetilde{A}^*$, é importante estudar o *problema da palavra*: podemos decidir quando é que uma dada palavra em $\widetilde{A}^*$ representa a identidade em $Grp\langle A \mid \mathcal{R} \rangle$?

No caso em que $\mathcal{R}$ é NCI, dada $u \in \widetilde{A}^*$ sabemos, pela Proposição 3.4.4, que $u = 1$ em $F_A^{\mathcal{R}}$ se e só se $\overline{u} = 1$. Como $\mathcal{R}$ é um sistema de reescrita NCI sabemos que, independentemente das reduções aplicadas sucessivamente a u, obtemos $\overline{u}$ num número finito de passos. No entanto, há que saber que reduções podemos aplicar a u. Para isso, convém que, dado um fator x de u, tenhamos acesso, num número finito de passos, às reduções do tipo (x, y) que existem em $\mathcal{R}$. Por exemplo, se $\mathcal{R}$ for finito, sabemos sempre que reduções podemos aplicar a uma determinada palavra $u \in \widetilde{A}^*$.

> De agora em diante consideramos apenas alfabetos e sistemas de reescrita $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$ finitos. Consequentemente, as apresentações de grupo também serão finitas.

Assim sendo, quando nos referimos a um grupo $F_A^{\mathcal{R}}$, o alfabeto A é finito, assim como $\mathcal{R}$. Logo, conseguimos resolver o problema da palavra em $F_A^{\mathcal{R}}$.

6.1. Alguns problemas de decidibilidade

Historicamente, há duas questões centrais que podemos perguntar relativamente a apresentações (finitas), tendo estas sido apresentadas em conjunto pela primeira vez em 1911 por Max Dehn [5].

• *problema da palavra*: Seja $\langle A \mid \mathcal{R} \rangle$ uma apresentação de um grupo. Podemos decidir quando é que uma palavra $u \in \widetilde{A}^*$ representa a identidade em $Grp\langle A \mid \mathcal{R} \rangle$?

• *problema da conjugação*: Seja $\langle A \mid \mathcal{R} \rangle$ uma apresentação de um grupo. Podemos decidir quando é que duas palavras $u, v \in \widetilde{A}^*$ são conjugadas em $Grp\langle A \mid \mathcal{R} \rangle$, isto é, se existe $w \in \widetilde{A}^*$ tal que $u = wvw^{-1}$ em $Grp\langle A \mid \mathcal{R} \rangle$?

Estes problemas são exemplo daquilo que chamamos de problema de decisão, essencialmente uma pergunta de sim/não que pode (ou não) ser decidida por um algoritmo. Por algoritmo queremos dizer um procedimento bem definido que termina qualquer que seja o input. Dizemos que uma apresentação $\langle A \mid \mathcal{R} \rangle$ de um grupo tem o problema da palavra *decidível* se existir algum algoritmo que determine se um elemento arbitrário de $\widetilde{A}^*$ é a identidade em $Grp\langle A \mid \mathcal{R} \rangle$. Caso um tal algoritmo não exista, dizemos que $\langle A \mid \mathcal{R} \rangle$ tem o problema da palavra *indecidível*. Analogamente estendemos esta definição para o problema da conjugação e para outros possíveis problemas de decisão.

Como no problema da palavra e no problema da conjugação o input são palavras sobre os geradores de um determinado grupo que está fixo, faz sentido perguntar se a decidibilidade depende ou não da apresentação considerada para o grupo.

Proposição 6.1.1. *Sejam $\langle A \mid \mathcal{R} \rangle$ e $\langle A' \mid \mathcal{R}' \rangle$ apresentações de um grupo G. Então $\langle A \mid \mathcal{R} \rangle$ tem o problema da palavra (respetivamente problema da conjugação) decidível se e só se $\langle A' \mid \mathcal{R}' \rangle$ tem o problema da palavra (respetivamente problema da conjugação) decidível.*

Demonstração. Suponhamos que $\langle A \mid \mathcal{R} \rangle$ tem o problema da palavra ou o problema da conjugação decidível. Sejam $\varphi : F_A^{\mathcal{R}_A} \to G$ e $\varphi' : F_{A'}^{\mathcal{R}_{A'}} \to G$ os homomorfismos sobrejetivos resultantes, respetivamente, das inclusões $\iota : A \to G$ e $\iota' : A' \to G$. Então $ker(\varphi) = \sigma_{\mathcal{R}}$ e $ker(\varphi') = \sigma_{\mathcal{R}'}$. Note-se que podemos definir um homomorfismo $\alpha : F_{A'}^{\mathcal{R}_{A'}} \to F_A^{\mathcal{R}_A}$ tal que o seguinte diagrama comuta,

$$\begin{array}{ccc} F_A^{\mathcal{R}_A} & \xrightarrow{\varphi} & G \\ {\scriptstyle\alpha}\uparrow & \nearrow_{\varphi'} & \\ F_{A'}^{\mathcal{R}_{A'}} & & \end{array}$$

Para tal, escolhemos $a\alpha \in a\varphi'(\varphi)^{-1}$ para todo o $a \in A'$ e usamos a propriedade universal. Dado $u \in F_{A'}^{\mathcal{R}_{A'}}$, temos

$$u \in \sigma_{\mathcal{R}'} \Leftrightarrow u\varphi' = 1 \Leftrightarrow u\alpha\varphi = 1 \Leftrightarrow u\alpha \in \sigma_{\mathcal{R}}.$$

Uma vez que podemos decidir se $u\alpha \in \sigma_{\mathcal{R}}$, concluímos que $\langle A' \mid \mathcal{R}' \rangle$ tem o problema da palavra decidível. Além disso, dados $u, v \in F_{A'}^{\mathcal{R}_{A'}}$, temos que $u\varphi'$, $v\varphi'$ são conjugados em G se e só se $u\varphi' = x(v\varphi')x^{-1}$ para algum $x \in G$. Isto equivale a dizer que $u\alpha\varphi = x(v\alpha\varphi)x^{-1}$ para algum $x \in G$, ou seja, $u\alpha$ e $v\alpha$ são conjugados em G. Como $\langle A \mid \mathcal{R} \rangle$ tem

o problema da conjugação decidível, concluímos que $\langle A' \mid \mathcal{R}' \rangle$ também tem. Por simetria obtemos o resultado. □

A Proposição 6.1.1 permite-nos estudar o problema da palavra e o da conjugação de um determinado grupo finitamente apresentável G sem especificarmos a apresentação. Vejamos agora que, no caso dos grupos livres finitamente gerados, a decidibilidade do problema da conjugação também se mantém.

Dada $u \in \widetilde{A}^*$, dizemos que u é *ciclicamente $\mathcal{R}_A$-reduzida* se uu é uma palavra $\mathcal{R}_A$-reduzida ou, equivalentemente, se $u \in Irr(\mathcal{R}_A)$ e não for da forma ava^{-1} para algumas $a \in \widetilde{A}$ e $v \in \widetilde{A}^*$. De forma a simplificar a notação, omitimos $\mathcal{R}_A$. É fácil de ver que toda a palavra $u \in Irr(\mathcal{R}_A)$ pode ser escrita, de forma única, como $u = vwv^{-1}$ para algumas $v, w \in \widetilde{A}^*$ com w ciclicamente reduzida. Dizemos então que w é o *núcleo cíclico* de u e escrevemos $c(u) = w$. Note-se também que se $u = vw$ é ciclicamente reduzida, então wv também é. Nesta situação, dizemos que wv é *conjugada cíclica* de u. De facto, $u = \overline{w^{-1}(wv)w}^{\mathcal{R}_A}$ e, portanto, os conjugados cíclicos são conjugados no grupo livre $F_A^{\mathcal{R}_A}$. Além disso, assim como a relação "ser conjugado de", a relação "ser conjugado cíclico de" é uma relação de equivalência.

Lema 6.1.2. *Sejam $g, h \in \widetilde{A}^*$. Então, g, h são conjugados em $F_A^{\mathcal{R}_A}$ se e só se $c(\overline{g})$ e $c(\overline{h})$ são conjugados cíclicos.*

Demonstração. Suponhamos primeiro que $c(\overline{g})$ e $c(\overline{h})$ são conjugados cíclicos. Temos que, em $F_A^{\mathcal{R}_A}$, g (respetivamente, h) é conjugado de $c(\overline{g})$ (respetivamente, $c(\overline{h})$). Além disso ser conjugado cíclico implica ser conjugado em $F_A^{\mathcal{R}_A}$. Da transitividade da relação de conjugação resulta que g e h são conjugados.

Suponhamos agora que g, h são conjugados em $F_A^{\mathcal{R}_A}$. Se $\overline{g} = 1$, então $\overline{h} = 1$ e nada mais há a mostrar. Suponhamos então que $\overline{g} \neq 1$ e $\overline{g} = xux^{-1}$ com u ciclicamente reduzida não trivial e $x \in Irr(\mathcal{R}_A)$. Uma vez que ser conjugado cíclico é uma relação de equivalência, basta mostrar que, para todo o $a \in \widetilde{A}$, $v = c(\overline{aga^{-1}})$ e $u = c(\overline{g})$ são conjugados cíclicos. Seja então $a \in \widetilde{A}$. Se $aua^{-1} \in Irr(\mathcal{R}_A)$ ou $x \neq 1$, temos que

$$v = c(\overline{aga^{-1}}) = c(\overline{axux^{-1}a^{-1}}) = u$$

e nada mais há a mostrar. Supomos então que $x = 1$ e aua^{-1} não é reduzida. Uma vez que $u \neq 1$, podemos assumir que au não é reduzida (o outro caso é análogo). Então

$u = a^{-1}w$ para alguma $w \in \widetilde{A}^*$ e

$$\overline{aga^{-1}} = \overline{aua^{-1}} = \overline{wa^{-1}}.$$

Como u é ciclicamente reduzida, não pode terminar em a e, portanto, $wa^{-1} \in Irr(\mathcal{R}_A)$. Logo, $\overline{aga^{-1}} = wa^{-1}$. Além disso, como $u = a^{-1}w$ é reduzida, w não pode começar pela letra a. Logo $wa^{-1} = v$ e u e v são conjugados cíclicos. □

Corolário 6.1.3. *$F_A^{\mathcal{R}_A}$ tem o problema da conjugação decidível.*

Demonstração. Resulta do Lema 6.1.2 e do facto dos núcleos cíclicos e dos respetivos conjugados cíclicos serem computáveis. □

Exemplo 6.1.4. *Seja $A = \{a, b\}$. Então, em $F_A^{\mathcal{R}_A}$, $aba^{-1}b^2a^{-1}$ e $b^{-1}a^{-1}b^4$ são conjugados, uma vez que, os respetivos núcleos cíclicos $ba^{-1}b^2$ e $a^{-1}b^3$ são conjugados cíclicos. No entanto, $ba^{-1}b^{-2}$ já não o é, visto que, $|c(ba^{-1}b^{-2})| = |a^{-1}b| = 2 < 3 = |a^{-1}b^3|$ e, portanto, $a^{-1}b$ não pode ser um conjugado cíclico de $a^{-1}b^3$.*

Em geral, é muito difícil concluir certas propriedades de G conhecendo apenas uma apresentação deste.

Teorema 6.1.5. *(Novikov 1955, Boone 1957) Existem grupos finitamente apresentáveis com o problema da palavra indecidível.*

Teorema 6.1.6. *(Adjan 1955, Rabin 1958) É indecidível se um grupo finitamente apresentável arbitrário é trivial, finito, livre.*

Uma demonstração destes resultados pode ser vista em [16]. No entanto, se tivermos mais informações sobre G, a resposta a um dado problema computacional pode variar. Por exemplo, foi observado no início deste capítulo que o problema da palavra é decidível no caso em que G admite uma apresentação $\langle A \mid \mathcal{R} \rangle$ para algum sistema de reescrita $\mathcal{R}$ que seja NCI. Pela Proposição 6.1.3, sabemos que, se $\mathcal{R} = \mathcal{R}_A$, então o problema da conjugação também é decidível.

Proposição 6.1.7. *Seja $\langle A \mid \mathcal{R} \rangle$ uma apresentação finita de um grupo finito G tal que $\mathcal{R}$ é um sistema de reescrita NCI, isto é, $G \simeq F_A^{\mathcal{R}}$. Então, o problema da conjugação é decidível em G.*

Demonstração. Seja $S_0 = \{\overline{a} \mid a \in \widetilde{A}\}$ e $S_i = S_{i-1} \cup \{\overline{uv} \mid (u, v) \in S_{i-1} \times S_{i-1}\}$. Note-se que estes conjuntos são computáveis, uma vez que, para todo o $i \in \mathbb{N}$, S_i é finito (pois

A é finito) e $\mathcal{R}$ é um sistema de reescrita NCI que é finito. Como também sabemos que G é finito, existe um $j \in \mathbb{N}$ tal que $\{\overline{uv} \mid (u,v) \in S_{j-1} \times S_{j-1}\} \subseteq S_{j-1}$, isto é, $S_{j-1} = S_j$. Logo, num número finito de passos, conseguimos computar todos os elementos de G e, consequentemente, o problema da conjugação é decidivel em G. □

Terminamos esta secção com mais alguns problemas clássicos de decidibilidade relativos a subgrupos finitamente gerados. Usamos a notação $H \leq_{f.g.} G$ para denotar um subgrupo finitamente gerado H de um grupo G.

• *problema da palavra generalizado*: Seja $H \leq_{f.g.} G$. Existe algum algoritmo tal que, dada $u \in G$ como input, determina se $u \in H$?

• *problema da conjugação generalizado*: Existe algum algoritmo tal que, dados $H, K \leq_{f.g.} G$, determina se H e K são subgrupos conjugados, isto é, se $H = g^{-1}Kg$ para algum $g \in G$?

• *problema do isomorfismo para subgrupos finitamente gerados*: Existe algum algoritmo tal que, dados $H, K \leq_{f.g.} G$, determina se $H \simeq K$?

Ora, o estudo destes problemas torna-se bastante mais complicado, mesmo quando G é um grupo livre $F_A^{\mathcal{R}_A}$. No entanto, no início dos anos oitenta, Stallings desenvolveu um método inovador [28], que serviu de base para a construção dos chamados autómatos de Stallings - uma classe especial de autómatos que rapidamente se tornaram uma ferramenta fundamental no estudo dos subgrupos finitamente gerados de grupos livres [12]. Essa abordagem estabelece uma correspondência precisa entre os subgrupos finitamente gerados de $F_A^{\mathcal{R}_A}$ e os $\tilde{A}$-autómatos de Stallings, permitindo, assim, responder de forma altamente eficaz a diversos problemas, incluindo os mencionados acima em $F_A^{\mathcal{R}_A}$.

6.2. Autómatos de Stallings

A existência de inversos nos grupos conduz naturalmente ao conceito de *autómato inverso*. Dado um $\widetilde{A}$-autómato $\mathcal{A}$, para algum alfabeto A, dizemos que $\mathcal{A}$ é:

• *involutivo*, se satisfaz

$$(p, a, q) \in E(\mathcal{A}) \Leftrightarrow (q, a^{-1}, p) \in E(\mathcal{A})$$

para todo o $a \in A$;

• *conexo por arcos*, se para quaisquer dois vértices p, q de $\mathcal{A}$ existe um caminho em $\mathcal{A}$ que os liga. Se permitirmos que o caminho não tenha em consideração a orientação das arestas, então dizemos que $\mathcal{A}$ é *conexo*, ou seja, $\mathcal{A}$ diz-se conexo, se para todos $p, q \in Q(\mathcal{A})$ distintos, existe uma sequência

$$p = q_0, \ldots, q_n = q$$

onde $q_i \in Q(\mathcal{A})$, $n \geq 1$ e tal que, para todo o $i \in \{1, \ldots, n\}$, existe um $a \in \tilde{A}$, tal que $(q_{i-1}, a, q_i) \in E(\mathcal{A})$ ou $(q_i, a, q_{i-1}) \in E(\mathcal{A})$. Note-se que, num autómato involutivo, ser conexo é equivalente a ser conexo por arcos;

• *inverso*, se é determinístico, involutivo e conexo. Note-se que, se $\mathcal{A}$ é inverso e tem pelo menos um vértice inicial e um vértice final, então $\mathcal{A}$ é aparado.

Num autómato inverso, definimos também o grau de um vértice $q \in Q(\mathcal{A})$, relativamente a um subconjunto X de $\widetilde{A}$, da seguinte maneira:

Definição 6.2.1. *Seja $\mathcal{A}$ um $\widetilde{A}$-autómato inverso e $q \in Q(\mathcal{A})$ para um certo alfabeto A. Seja também $X \subseteq \widetilde{A}$. Então definimos o grau de q relativamente a X como sendo*

$$deg_X(q) = |\{(q, x, p) \in E(\mathcal{A}) \, : \, x \in X, \, p \in Q(\mathcal{A})\}|.$$

Informalmente, $deg_X(q)$ é o número de arestas com rótulo em X que "saem" do vértice q. Quando $X = \widetilde{A}$, denotamos $deg_{\widetilde{A}}(q)$ simplesmente por $deg(q)$ e dizemos que é o grau *de q.*

Uma boa ilustração destes conceitos é dada pelos grafos de Cayley e pelos grafos de Schreier: seja A um alfabeto, G um grupo e $\Phi : \tilde{A} \to G$ uma função tal que $a^{-1}\Phi = (a\Phi)^{-1}$ para todo o $a \in A$. Uma função com esta propriedade diz-se *involutiva*. Dizemos que A gera G através de Φ se $\langle A\Phi \rangle = G$. Nestas condições, o *grafo de Cayley* $Cay_{A,\Phi}(G)$ é um $\widetilde{A}$-grafo que tem os elementos de G como vértices e arestas da forma

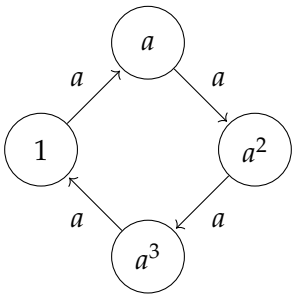
$$g \xrightarrow{a} g(a\Phi) \quad (g \in G, a \in \widetilde{A})$$

Se $N \leq G$, o *grafo de Schreier* $Sch_{A,\Phi}(G, N)$ é um $\widetilde{A}$-grafo cujo os vértices são as classes laterais direitas $(\text{de } N \text{ em } G)$ e as arestas são da forma

$$Ng \xrightarrow{a} Ng(a\Phi) \quad (g \in G, a \in \widetilde{A}).$$

De forma a simplificar a escrita, na representação geométrica de autómatos e de grafos inversos é habitual omitir as arestas com rótulo em A^{-1}.

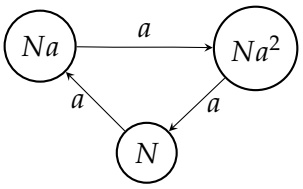
Exemplo 6.2.2. *Considere-se $A = \{a\}$ e $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$ o sistema de reescrita dado por $\mathcal{R} = \{(aa^{-1}, 1), (a^{-1}a, 1), (a^{-1}, a^3), (a^4, 1)\}$. Então, pela Proposição 4.2.5, $\mathcal{R}$ é um sistema de reescrita NCI e $F_A^{\mathcal{R}}$ é o grupo cíclico de ordem 4. Seja $\Phi : \widetilde{A} \longrightarrow F_A^{\mathcal{R}}$ a função involutiva que envia a em $a/\sigma_{\mathcal{R}}$. Note-se que $\langle a\Phi \rangle = F_A^{\mathcal{R}}$ e $Cay_{A,\Phi}(F_A^{\mathcal{R}})$ é dado por*



Exemplo 6.2.3. *Seja $N \trianglelefteq G$, A um alfabeto que gera G através de $\Phi : \widetilde{A} \to G$ e $\pi : G \to {}^{G}\!/_{N}$ o homomorfismo canónico. Então $Sch_{A,\Phi}(G, N) \simeq Cay_{A,\Phi\pi}({}^{G}\!/_{N})$.*

De modo a simplificar a notação, quando a função Φ em $Cay_{A,\Phi}(G)$ e em $Sch_{A,\Phi}(G, N)$ está subentendida, esta é omitida.

Exemplo 6.2.4. *Seja G o grupo cíclico de ordem 6 gerado por $a \in G$ e $N = \{1, a^3\}$. Então, N é um subgrupo de G e, para $A = \{a\}$, temos que $Sch_A(G, N)$ é*



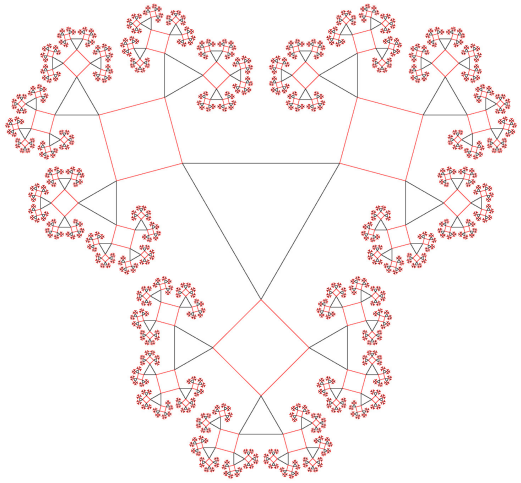
Como $N \trianglelefteq G$, $Sch_A(G, N) \simeq Cay_A({}^{G}\!/_{N})$.

Exemplo 6.2.5. *Sejam*

$$A_1 = \{a\}, \mathcal{R}_1 = \{(aa^{-1}, 1), (a^{-1}a, 1), (a^{-1}, a^3), (a^4, 1)\},$$

$$A_2 = \{b\}, \mathcal{R}_2 = \{(bb^{-1}, 1), (b^{-1}b, 1), (b^{-1}, b^2), (b^3, 1)\}.$$

Tomando $A = A_1 \cup A_2$ e $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$, pelas Proposições 5.1.3 e 5.0.3, temos que $F_A^{\mathcal{R}} \simeq \mathbb{Z}_3 * \mathbb{Z}_4$. Além disso, $Cay_A(\mathbb{Z}_3 * \mathbb{Z}_4)$ é infinito e geometricamente será algo da seguinte forma:

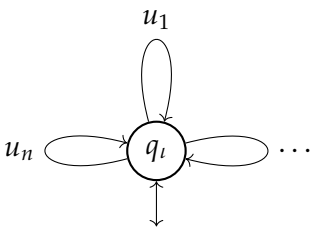


Uma observação trivial mas que vai ser usada várias vezes neste trabalho é a seguinte: num $\widetilde{A}$-autómato inverso $\mathcal{A}$, se $p \xrightarrow{uu^{-1}} q$ é um caminho em $\mathcal{A}$ para algum $u \in \widetilde{A}^*$, então necessariamente $p = q$. Vejamos agora a construção dos autómatos de Stallings que, por sua vez, são também inversos.

Seja $F_A^{\mathcal{R}_A}$ o grupo livre sobre um alfabeto A. Seja $H = \langle u_1, \ldots, u_n \rangle \leq_{f.g.} F_A^{\mathcal{R}_A}$, $n \geq 1$, onde cada gerador u_i é visto como uma palavra (não vazia) e reduzida em $\widetilde{A}^*$, isto é, $u_i \in Irr(\mathcal{R}_A) \backslash \{1\}$. Seja $X = \{u_1, \ldots, u_n\}$. Construímos um autómato involutivo $\mathcal{F}(X)$ fixando um ponto base q_ι e colando a este *pétalas* rotuladas pelas palavras reduzidas u_i da seguinte forma: se $u_i = a_1 \ldots a_k$, com $a_j \in \widetilde{A}$, a pétala consiste nos vértices e arestas do caminho fechado

$$q_\iota \xrightarrow{a_1} \cdots \xrightarrow{a_k} q_\iota$$

e as respetivas arestas inversas onde todos os vértices intermediários são distintos.



Por razões óbvias $\mathcal{F}(X)$ é chamado de *autómato flor*. Para tornar o autómato $\mathcal{F}(X)$ um

autómato inverso, precisamos que seja determinístico. Para tal, são usadas as *dobragens de Stallings*: identificamos sucessivamente pares de arestas da forma

$$p \xleftarrow{a} q \xrightarrow{a} r$$

onde $a \in \widetilde{A}$. Em particular, os vértices p e r são também identificados (caso sejam distintos). Note-se que, como o número de arestas diminui a cada dobragem, acabamos sempre por ter um autómato inverso, designado por $\mathcal{S}(X)$. O ponto chave desta construção é que a construção do autómato de Stallings é independente (no sentido que, a menos de isomorfismo, o autómato obtido é sempre o mesmo) do conjunto de geradores $X \subseteq Irr(\mathcal{R}_A)$ escolhido para H e da ordem pela qual as dobragens de Stallings são feitas. Mais adiante, será vista uma versão mais geral deste resultado.

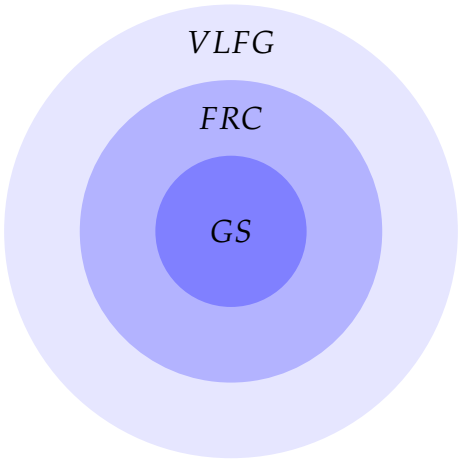
Como já foi dito anteriormente, com estes autómatos, conseguimos resolver o problema da palavra generalizado em $F_A^{\mathcal{R}_A}$. Acontece que, verificar se uma palavra $u \in \widetilde{A}^*$ está em $H \leq_{f.g.} F_A^{\mathcal{R}_A}$ equivale a verificar se $\overline{u}$ está em $L(\mathcal{S}(X))$. Mais adiante, também será apresentada a demonstração de uma versão mais geral deste resultado.

Dada a utilidade dos autómatos de Stallings, surgiram naturalmente generalizações desta abordagem para outras classes de grupos. Por exemplo, em [13], Kapovich, Weidmann e Miasnikov estendem a técnica das dobragens de Stallings para algumas subclasses de grupos fundamentais de grafos de grupos, sendo os grupos virtualmente livres uma delas. Um grupo *virtualmente livre* é um grupo que contém um subgrupo livre de índice finito - note-se que os grupos livres são uma subclasse destes. Esta abordagem permitiu tratar estruturas mais complexas como produtos livres com amalgamação e extensões HNN, mantendo uma abordagem combinatória eficaz para problemas algorítmicos como o da palavra generalizado. Em [26], Silva, Soler-Escrivà e Ventura discutem qual a generalização mais favorável possível da construção de Stallings, através das chamadas secções de Stallings, e concluíram que os grupos que admitem tal generalização são precisamente os grupos virtualmente livres finitamente gerados. No entanto, é natural que, num contexto tão geral, nem todos os resultados e propriedades algorítmicas obtidas no caso dos grupos livres possam ser estendidos.

No próximo capítulo, exploramos qual a versão mais adequada dos autómatos de Stallings para uma subclasse dos grupos virtualmente livres finitamente gerados e que têm ganhado atenção nos últimos anos: os *grupos singelos* - isto é, os grupos isomorfos a um produto livre finitário de grupos finitos e de um grupo livre finitamente gerado. Para

tal vamos usar o facto que um grupo singelo admite sempre uma apresentação $\langle A|\mathcal{R}\rangle$ finita onde $\mathcal{R}$ é um sistema de reescrita NCI.

Ora, estes grupos são uma subclasse dos grupos virtualmente livres finitamente gerados. Acontece que, de facto, os grupos singelos são isomorfos a algum $Mon\langle A|\mathcal{R}\rangle$ com $A, \mathcal{R}$ finitos e $\mathcal{R}$ um sistema de reescrita redutor e confluente e, em 1987, Diekert provou que grupos nestas condições estão estritamente contidos na família dos grupos virtualmente livres finitamente gerados [7]. Ou seja, se GS, FRC e $VLFG$ representam, respetivamente, o conjunto dos grupos singelos, o conjunto dos grupos isomorfos a um $Mon\langle A|\mathcal{R}\rangle$ com $A, \mathcal{R}$ finitos e $\mathcal{R}$ um sistema de reescrita redutor e confluente e, o conjunto dos grupos virtualmente livres finitamente gerados, temos o seguinte diagrama



Podemos então questionar-nos se o conjunto GS está estritamente contido no conjunto FRC. No entanto, até hoje, não sabemos a resposta. Esta conjetura foi apresentada por Madlener e Otto em 1986 [1]. Deste então, vários progressos foram feitos e deixamos como referência [8] para mais detalhes sobre este assunto.

Para finalizar este capítulo, apresentamos um exemplo de um grupo virtualmente livre finitamente gerado que não é um grupo singelo e de que vamos voltar a falar mais tarde: $\mathbb{Z} \times \mathbb{Z}_2$. De facto, este grupo é virtualmente livre, uma vez que $\mathbb{Z} \times \{0\}$ é livre e tem índice dois, no entanto não é isomorfo a um grupo singelo uma vez que é um grupo infinito, abeliano e não é isomorfo a $\mathbb{Z}$.

7. Generalização dos autómatos de Stallings

Seja G um grupo singelo, isto é, um produto livre finitário de grupos finitos e de um grupo livre finitamente gerado. Então, pelos resultados anteriores,

$$G \simeq F_{A_0}^{\mathcal{R}_0} * F_{A_1}^{\mathcal{R}_1} * \dots F_{A_{\mathfrak{N}}}^{\mathcal{R}_{\mathfrak{N}}}$$

para algum $\mathfrak{N} \in \mathbb{N}$ e onde as seguintes condições se verificam:

• para todo $i \in \{0, \dots, \mathfrak{N}\}$, $\mathcal{R}_i \subseteq \widetilde{A_i}^+ \times \widetilde{A_i}^*$ é um sistema de reescrita NCI e finito;

• para todo $a \in \widetilde{A}$, $\overline{a}^{\mathcal{R}} \neq 1$;

• para todo $i \in \{1, \dots, \mathfrak{N}\}$, $F_{A_i}^{\mathcal{R}_i}$ é um grupo finito;

• $\mathcal{R}_0 = \mathcal{R}_{A_0} = \{(aa^{-1}, 1) : a \in \widetilde{A_0}\}$ e, portanto, $F_{A_0}^{\mathcal{R}_0}$ é o grupo livre de base A_0.

Além disso, pela Proposição 5.1.3, se

$$A = \cup_{i=0}^{\mathfrak{N}} A_i \text{ e } \mathcal{R} = \cup_{i=0}^{\mathfrak{N}} \mathcal{R}_i,$$

então $\mathcal{R} \subseteq \widetilde{A}^* \times \widetilde{A}^*$ e $G \simeq F_A^{\mathcal{R}}$. Observe-se que, para todo o $i \in \{0, \dots, \mathfrak{N}\}$, se $u \in \widetilde{A_i}^*$ então $\overline{u}^{\mathcal{R}} = \overline{u}^{\mathcal{R}_i}$.

> De agora em diante, $\mathcal{R}$ e A serão respetivamente o sistema de reescrita e o alfabeto descritos acima.

7.1. Construção dos autómatos

Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ e $X = \{u_1 \dots, u_n\}$ um subconjunto finito de geradores de H em forma reduzida, no sentido em que $X \subseteq Irr(\mathcal{R})$. Apresentamos agora um algoritmo que vai construir um autómato inverso e, os autómatos obtidos a partir desta construção, serão denotados por autómatos $\mathcal{S}_{\mathcal{R}}(X)$:

[1] Começamos por construir o chamado autómato flor $\mathcal{F}(X)$, em que pétalas rotuladas pelas palavras não vazias e reduzidas u_i (e as arestas inversas, para que seja um autómato involutivo) são coladas a um ponto base q_ι.

[2] De seguida, para todo $i \in \{1, \dots, \mathfrak{N}\}$, se (p, a, q) for uma aresta em $\mathcal{F}(X)$ com $a \in A_i$, colamos ao vértice p o grafo $Cay_{A_i}(F_{A_i}^{\mathcal{R}_i})$ (que é finito). Denotamos este novo autómato

por $\mathcal{F}_{\mathcal{R}}(X)$. Observe-se que o grafo de Cayley de um grupo é sempre transitivo nos vértices, por isso é irrelevante qual o vértice do grafo de Cayley usado para a colagem.

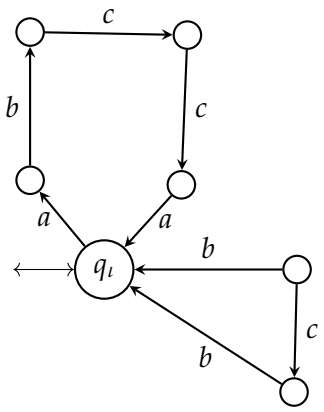
[3] Por fim, identificamos sucessivamente pares de arestas da forma $p \xleftarrow{a} q \xrightarrow{a} r$ até obtermos um autómato determinístico que, de facto, é inverso.

Exemplo 7.1.1. *Suponhamos que,*

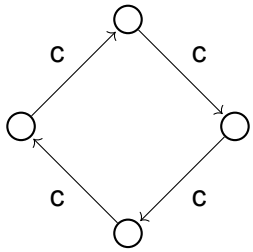
$$A_0 = \{a, b\}, \quad \textit{logo } \mathcal{R}_0 = \mathcal{R}_{A_0};$$
$$A_1 = \{c\}, \quad \mathcal{R}_1 = \{(cc^{-1}, 1),\ (c^{-1}c, 1),\ (c^{-1}, c^3),\ (c^4, 1)\}.$$

Então, sabemos que $F_A^{\mathcal{R}}$ é o produto livre do grupo livre $F_{A_0}^{\mathcal{R}_0}$ com o grupo cíclico de ordem quatro $F_{A_1}^{\mathcal{R}_1} \simeq \mathbb{Z}_4$. Seja $H =< abc^2a, b^{-1}cb >$ um subgrupo finitamente gerado de $F_A^{\mathcal{R}}$. Note-se que $abc^2a, b^{-1}cb \in Irr(\mathcal{R})$ e seja X o conjunto formado por essas duas palavras reduzidas.

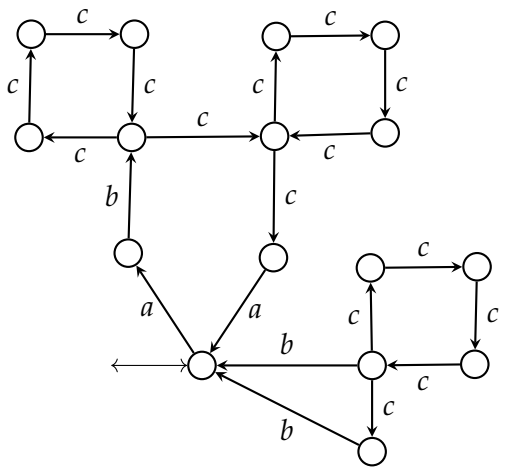
[1] *Construímos o autómato flor $\mathcal{F}(X)$*



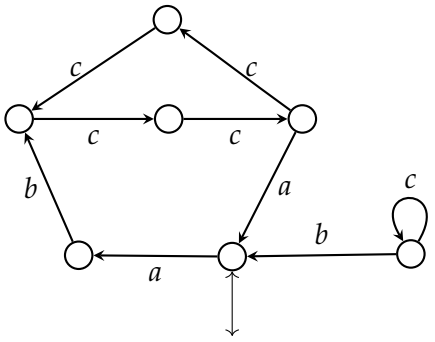
[2] *Como $Cay_{A_1}(F_{A_1}^{\mathcal{R}_1})$ é*



o autómato $\mathcal{F}_{\mathcal{R}}(X)$ é dado por



[3] *No final de todas as dobragens necessárias para o tornar determinístico, obtemos um autómato* $\mathcal{S}_{\mathcal{R}}(X)$



É natural questionarmos se a ordem pela qual as dobragens são feitas ao construir um autómato $\mathcal{S}_{\mathcal{R}}(X)$ é relevante. Mais tarde, veremos que a resposta é não. Por esse motivo, e com o intuito de simplificar a escrita, os próximos resultados serão formulados diretamente em termos de um único autómato $\mathcal{S}_{\mathcal{R}}(X)$. Note-se que, se $\mathcal{R} = \mathcal{R}_0$ e $A = A_0$ então $F_A^{\mathcal{R}}$ é o grupo livre gerado por A e $\mathcal{S}_{\mathcal{R}}(X)$ é o autómato de Stallings $\mathcal{S}(X)$.

Vamos então estudar mais propriedades destes autómatos de modo a tentar caracterizá-los da melhor forma possível. Por exemplo, o que acontece aos grafos de Cayley que são colados a $\mathcal{F}(X)$ após as possíveis dobragens?

Proposição 7.1.2. *Seja* G *um grupo gerado por* A *e* $Cay_A(G)$ *o respetivo grafo de Cayley. Seja* $\overline{Cay_A(G)}$ *um grafo quociente de* $Cay_A(G)$*. Se* $\overline{Cay_A(G)}$ *for determinístico, então* $\overline{Cay_A(G)} = Sch_A(G, N)$ *para algum* $N \leqslant G$*.*

Demonstração. Seja G um grupo gerado por A e $Cay_A(G) = (Q, E)$. Seja $(Q_i)_{i\in I}$ uma partição do conjunto Q induzindo o grafo quociente $\overline{Cay_A(G)} = (\overline{Q}, \overline{E})$ que supomos determinístico. Note-se que $\overline{Cay_A(G)}$ é completo, uma vez que $Cay_A(G)$ é completo.

Seja $(Q_i, a, Q_j) \in \overline{E}$. Então, por definição de $\overline{E}$, existem $q_i \in Q_i$ e $q_j \in Q_j$ tais que $q_i a = q_j$. Logo, $Q_i a \cap Q_j \neq \emptyset$, onde $Q_i a$ é visto como o produto em G, isto é, $Q_i a = \{qa \ : q \in Q_i\}$. Por outro lado, se $Q_i a \cap Q_k \neq \emptyset$ para algum $k \in I$, temos que $(Q_i, a, Q_k) \in \overline{E}$. Como $\overline{Cay_A(G)}$ é determinístico, $Q_j = Q_k$. Logo,

$$Q_i a = \bigcup_{k\in I} (Q_i a \cap Q_k) = Q_i a \cap Q_j \Rightarrow Q_i a \subseteq Q_j.$$

Analogamente, como $(Q_j, a^{-1}, Q_i) \in \overline{E}$, temos que

$$Q_j a^{-1} \subseteq Q_i \Rightarrow Q_j \subseteq Q_i a.$$

Logo, $Q_i a = Q_j$ e $\overline{E} = \{(Q_i, a, Q_j) \ : \ a \in \widetilde{A},\ Q_i a = Q_j\}$. Consideramos Q_1 o bloco em $\overline{Q}$ que contém 1_G. Como $\overline{Cay_A(G)}$ é conexo por arcos, para todo o $i \in I$, existe $u \in \widetilde{A}^*$, tal que $Q_i = Q_1 u$. Logo, como $\overline{Cay_A(G)}$ é também completo,

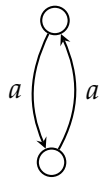
$$\overline{E} = \{(Q_1 u, a, Q_1 ua) \ : \ a \in \widetilde{A},\ u \in \widetilde{A}^*\}.$$

Como $1_G \in Q_1$, $Q_1 \neq \emptyset$. Sejam $u, v \in Q_1$. Então, como $1_G \in Q_1$, $Q_1 = Q_1 u = Q_1 v$. Logo, $Q_1 uv^{-1} = Q_1$, isto é, $uv^{-1} \in Q_1$. Portanto, $Q_1 \leqslant G$. Além disso,

$$E(Sch_A(G, Q_1)) = \{(Q_1 u, a, Q_1 ua) \,|\, u \in \widetilde{A}^*,\ a \in \widetilde{A}\} = \overline{E}.$$

Podemos então concluir que $\overline{Cay_A(G)} = Sch_A(G, Q_1)$. □

No Exemplo 6.2.2, se identificarmos o vértice 1 com o vértice a^2 e o vértice a com o vértice a^3, obtemos o grafo determinístico



que é isomorfo a $Sch_A(F_A^{\mathcal{R}}, \langle a^2 \rangle)$.

Definição 7.1.3. *Seja $\mathcal{A}$ um $\widetilde{A}$-autómato e $\mathcal{G}$ um $\widetilde{A}$-grafo. Denotamos por $[\mathcal{G}]_{\mathcal{A}}$ o conjunto de todos os subgrafos do grafo $\Gamma_{\mathcal{A}}$ que são isomorfos a $\mathcal{G}$. Definimos também os*

seguintes conjuntos:

$$Cay(\mathcal{A}) = \bigcup_{i=1}^{\mathfrak{N}} [Cay_{A_i}(F_{A_i}^{\mathcal{R}_i})]_{\mathcal{A}}$$

$$Sch(\mathcal{A}) = \bigcup_{i=1}^{\mathfrak{N}} Sch_i(\mathcal{A}).$$

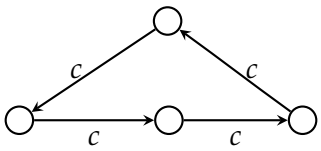
onde $Sch_i(\mathcal{A}) = \bigcup_{N \leq F_{A_i}^{\mathcal{R}_i}} [Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, N)]_{\mathcal{A}}$. *Note-se que* $Cay(\mathcal{A}) \subseteq Sch(\mathcal{A})$. *Dado* $q \in Q(\mathcal{A})$, *definimos também o seguinte conjunto*

$$Cay_q(\mathcal{A}) = \{C \in Cay(\mathcal{A}) \,:\, q \in Q(C)\}.$$

Lema 7.1.4. *Seja* (p, a, q) *uma aresta em* $\mathcal{S}_{\mathcal{R}}(X)$ *tal que* $a \in \widetilde{A_i}$ *para algum* $i \in \{1, \ldots, \mathfrak{N}\}$. *Então os vértices* p *e* q *estão contidos em algum* $K \in Sch_i(\mathcal{S}_{\mathcal{R}}(X))$.

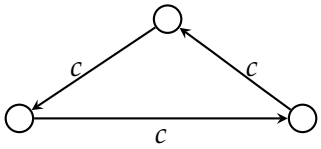
Demonstração. Uma vez que $\mathcal{S}_{\mathcal{R}}(X)$ é involutivo, podemos supor que $a \in A_i$. Ora, o vértice p resulta de um vértice p' de $\mathcal{F}_{\mathcal{R}}(X)$ onde (p', a, q') é uma aresta em $\mathcal{F}_{\mathcal{R}}(X)$ para algum vértice q'. Dada a construção de $\mathcal{F}_{\mathcal{R}}(X)$, o vértice p' está contido em algum $K' \in \left[Cay_{A_i}(F_{A_i}^{\mathcal{R}_i})\right]_{\mathcal{F}_{\mathcal{R}}(X)}$. Na passagem do autómato $\mathcal{F}_{\mathcal{R}}(X)$ para o autómato $\mathcal{S}_{\mathcal{R}}(X)$ alguns vértices de K' são identificados. Como $\mathcal{S}_{\mathcal{R}}(X)$ é determinístico, pela Proposição 7.1.2, podemos concluir que o vértice p em $\mathcal{S}_{\mathcal{R}}(X)$ está contido em algum $K \in \left[Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, N)\right]_{\mathcal{S}_{\mathcal{R}}(X)}$ para algum $N \leqslant F_{A_i}^{\mathcal{R}_i}$, isto é, $K \in Sch_i(\mathcal{S}_{\mathcal{R}}(X))$. Como $\mathcal{S}_{\mathcal{R}}(X)$ é determinístico e $Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, N)$ é completo, o vértice q também está contido em K. □

No autómato $\mathcal{S}_{\mathcal{R}}(X)$ dado no Exemplo 7.1.1, toda a aresta rotulada por c está contida num dos seguintes subgrafos de $\Gamma_{\mathcal{S}_{\mathcal{R}}(X)}$,





que pertencem, respetivamente, a $\left[Sch_{A_1}(F_{A_1}^{\mathcal{R}_1}, \langle 1 \rangle)\right]_{\mathcal{S}_{\mathcal{R}}(X)}$ e a $\left[Sch_{A_1}(F_{A_1}^{\mathcal{R}_1}, F_{A_1}^{\mathcal{R}_1})\right]_{\mathcal{S}_{\mathcal{R}}(X)}$ (ambos contidos em $Sch_1(\mathcal{S}_{\mathcal{R}}(X))$). Ainda relativamente ao Exemplo 7.1.1, o Lema 7.1.4 também nos permite concluir que, para qualquer subconjunto finito X' de $Irr(\mathcal{R})$, $\Gamma_{S_{\mathcal{R}}(X')}$ nunca vai ter um subgrafo da seguinte forma



De facto, se tal fosse possível, significava que este grafo era isomorfo a um $Sch_{A_1}(F_{A_1}^{\mathcal{R}_1}, N)$ para algum $N \leq F_{A_1}^{\mathcal{R}_1}$. Logo, $[F_{A_1}^{\mathcal{R}_1} : N] = 3$. Mas como $|F_{A_1}^{\mathcal{R}_1}| = 4$, que não é divisível por três, isto não pode acontecer.

Definição 7.1.5. *Seja $\mathcal{A} = (Q, I, T, E)$ um $\widetilde{A}$-autómato e $\mathcal{G}$ um subgrafo de $\Gamma_{\mathcal{A}}$. Dizemos que $\mathcal{G}$ é útil em $\mathcal{A}$ relativamente a $\mathcal{R}$ se existe uma aresta (p, a, q) de $\mathcal{G}$ e um caminho em $\mathcal{A}$*

$$i \xrightarrow{u} p \xrightarrow{a} q \xrightarrow{v} f$$

com $u, v \in \widetilde{A}^*$, $i \in I$, $f \in T$ e tal que $uav \in Irr(\mathcal{R})$. Por outras palavras, $\mathcal{G}$ é útil em $\mathcal{A}$ relativamente a $\mathcal{R}$ se existe alguma palavra $\mathcal{R}$-irredutível que é lida no autómato $\mathcal{A}$ e que passa pelo menos numa aresta de $\mathcal{G}$.

Lema 7.1.6. *Se $K \in Sch(\mathcal{S}_{\mathcal{R}}(X))$, então K é útil em $\mathcal{S}_{\mathcal{R}}(X)$ relativamente a $\mathcal{R}$.*

Demonstração. Note-se que K tem de conter uma aresta que foi identificada a alguma aresta de $\mathcal{F}(X)$. Como $X \subseteq Irr(\mathcal{R})$, obtemos o pretendido. □

Definição 7.1.7. *Dizemos que um $\widetilde{A}$-autómato $\mathcal{A}$ é um $\mathcal{R}$-*autómato *se satisfaz as seguintes condições:*

I. *$\mathcal{A}$ é inverso;*

II. *$\mathcal{A}$ tem um ponto base;*

III. *todo o vértice de $\mathcal{A}$ ocorre nalgum caminho bem sucedido de rótulo em $Irr(\mathcal{R}_A)$. Note-se que $Irr(\mathcal{R}_A)$ não é necessariamente um subconjunto de $Irr(\mathcal{R})$;*

IV. *Seja (p, a, q) uma aresta de $\mathcal{A}$ tal que $a \in A_i$, para algum $i \in \{1, \ldots, n\}$. Então o vértice p está contido em algum $K \in Sch_i(\mathcal{A})$.*

Dizemos que $\mathcal{A}$ é um *$\mathcal{R}$-autómato trivial* se $\mathcal{A}$ é um $\mathcal{R}$-autómato e $E(\mathcal{A}) = \emptyset$. Logo $\mathcal{A}$ é um autómato que é formado apenas por um único vértice, sendo este o seu ponto base.

Definição 7.1.8. *Um $\widetilde{A}$-autómato $\mathcal{A}$ diz-se um $\mathcal{R}$-SFG se é um $\mathcal{R}$-autómato tal que todo o $K \in Sch(\mathcal{A})$ é útil em $\mathcal{A}$ relativamente a $\mathcal{R}$.*

Portanto, o $\mathcal{R}$-autómato trivial é também o $\mathcal{R}$-SFG trivial. Note-se que, se $\mathcal{A}$ é um $\mathcal{R}$-autómato e $u = a_1 \dots a_n$ é uma palavra em $\widetilde{A_i}^+$ para algum $i \in \{1, \dots, \mathfrak{N}\}$ ($a_j \in \widetilde{A_i}$) e se

$$q_0 \xrightarrow{a_1} \dots \xrightarrow{a_n} q_n$$

é um caminho em $\mathcal{A}$, então, como $\mathcal{A}$ é um $\mathcal{R}$-autómato, toda a aresta $q_{j-1} \xrightarrow{a_j} q_j$ ($j \in \{1 \dots, n\}$) está contida em algum $K_j \in \left[Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, N_j)\right]_{\mathcal{A}}$ para algum $N_j \leqslant F_{A_i}^{\mathcal{R}_i}$. Uma vez que $\mathcal{A}$ é determinístico e K_j é um $\widetilde{A_i}$-grafo completo, temos que $K_1 = \dots = K_n$. Logo, o caminho $q_0 \xrightarrow{u} q_n$ está todo contido em algum $K \in Sch_i(\mathcal{A})$. Esta observação vai ser usada várias vezes ao longo deste trabalho. O próximo resultado facilita a verificação da condição III da definição de $\mathcal{R}$-autómato (Definição 7.1.7).

Lema 7.1.9. *Seja $\mathcal{A}$ um $\widetilde{A}$-autómato inverso com um ponto base q_ι. Então, verificar se todo o vértice de $\mathcal{A}$ ocorre nalgum caminho bem sucedido de rótulo em $Irr(\mathcal{R}_A)$ equivale a verificar se todo o vértice em $\mathcal{A}$ que é distinto de q_ι tem grau superior a um.*

Demonstração. De facto, se q_0 for um vértice distinto de q_ι, então este não é inicial nem final e, se $deg(q_0) = 1$, qualquer caminho bem sucedido que passe por q_0 vai ter um fator da forma aa^{-1} para algum $a \in \widetilde{A}$ ($\mathcal{A}$ é involutivo). Por outro lado, suponhamos que todo o vértice distinto de q_ι tem grau superior a um e seja q_0 um vértice de $\mathcal{A}$. Então, ou $q_0 = q_\iota$ e a palavra $1 \in Irr(\mathcal{R}_A)$ é rótulo do caminho trivial

$$q_\iota \xrightarrow{1} q_\iota$$

ou existe um atalho em $\mathcal{A}$ que liga q_ι a q_0. De facto, como $\mathcal{A}$ é conexo por arcos, existe um caminho em $\mathcal{A}$ que liga q_ι a q_0. Ora, se esse caminho passar por um vértice p mais do que uma vez,

$$q_\iota \xrightarrow{v} p \xrightarrow{w} p \xrightarrow{z} q_0$$

com $v, w, z \in \widetilde{A}^*$, então consideramos o caminho

$$q_\iota \xrightarrow{v} p \xrightarrow{z} q_0 \ .$$

e, ao fim de um número finito de passos, obtemos um atalho

$$q_\iota \xrightarrow{u} q_0 \ .$$

para algum $u \in \widetilde{A}^*$. Note-se que, num $\widetilde{A}$-autómato inverso, todo o rótulo de um atalho é uma palavra em $Irr(\mathcal{R}_A)$. Logo, $u \in Irr(\mathcal{R}_A)$. Como $deg(q_0) \geq 2$ e $\mathcal{A}$ é inverso, existe $a_1 \in \widetilde{A}$ e q_1 um vértice de $\mathcal{A}$ tal que $q_\iota \xrightarrow{u} q_0 \xrightarrow{a_1} q_1$ ocorre em $\mathcal{A}$ com $ua_1 \in$

$Irr(\mathcal{R}_A)$. Ora, se o vértice q_1 ocorre no atalho $q_\iota \xrightarrow{u} q_0$, então temos a seguinte situação

$$q_\iota \xrightarrow{u_1} q_1 \underset{a_1}{\overset{u_2}{\rightleftarrows}} q_0$$

onde $u = u_1u_2$ para alguns $u_1, u_2 \in \widetilde{A}^*$. Como $\mathcal{A}$ é inverso e q_0 não é vértice intermediário em $q_\iota \xrightarrow{u_1} q_1$, temos que a_1^{-1} não é prefixo de u_1^{-1} e, consequentemente, $ua_1u_1^{-1} \in Irr(\mathcal{R}_A)$. Logo, q_0 ocorre num caminho bem sucedido de rótulo em $Irr(\mathcal{R}_A)$. Caso

$$q_\iota \xrightarrow{u} q_0 \xrightarrow{a_1} q_1$$

ainda seja um atalho então, novamente, existe $a_2 \in \widetilde{A}$ e q_2 um vértice de $\mathcal{A}$ tal que

$$q_\iota \xrightarrow{u} q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2$$

ocorre em $\mathcal{A}$ com $ua_1a_2 \in Irr(\mathcal{R}_A)$. Ora, se $q_\iota \xrightarrow{ua_1a_2} q_2$ ainda for um atalho, repetimos o argumento até eventualmente alcançarmos um vértice que se repete. Note-se que isso necessariamente tem de acontecer uma vez que o autómato é finito. Portanto, ao fim de um número finito de passos voltamos ao caso anterior. □

Exemplo 7.1.10. *Sejam,*

$A_0 = \{a\}, \quad A_1 = \{b, c\},$

$\mathcal{R}_0 = \{(aa^{-1}, 1),\ (a^{-1}a, 1)\},$

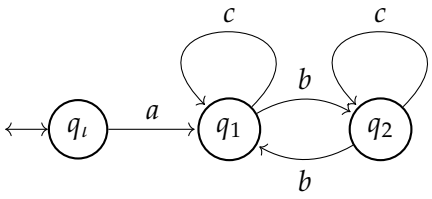
$\mathcal{R}_1 = \{(bb^{-1}, 1),\ (b^{-1}b, 1),\ (cc^{-1}, 1),\ (c^{-1}c, 1),\ (b^2, 1),\ (c^2, 1),\ (b^{-1}, b),\ (c^{-1}, c),\ (cb, bc)\}.$

Pela Proposição 4.2.6 e pelo Lema 5.1.2, sabemos que $\mathcal{R}_1 \setminus \{(cb, bc)\}$ é um sistema de reescrita NCI. Note-se que, ao final de um número finito de vezes em que a redução (cb, bc) é aplicada a uma determinada palavra $u \in \widetilde{A_1}^*$, o número de letras $b's$ em u que estão à direita de algum c diminui e as únicas reduções de $\mathcal{R}_1$ que fazem este número aumentar são as reduções (b^{-1}, b) e (c^{-1}, c) que podem ser aplicadas apenas um número finito de vezes. Logo, $\mathcal{R}_1$ é noetheriano. Seja $u \in \widetilde{A_1}^*$. Então, como $\mathcal{R}_1$ é noetheriano, existe alguma $v \in Irr(\mathcal{R}_1)$ tal que $u \xrightarrow{*} v$. Para cada $x \in A_1$, seja $R_x(u) = N_x(u) - N_{x^{-1}}(u) \pmod 2$. Uma vez que

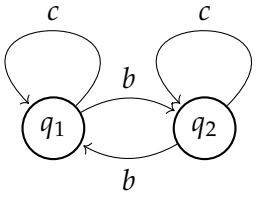
$$(w, z) \in \mathcal{R}_1 \Rightarrow (R_b(w) = R_b(z) \wedge R_c(w) = R_c(z)),$$

podemos concluir que $R_b(u) = R_b(v)$ e $R_c(u) = R_c(v)$. Além disso, facilmente se verifica que $Irr(\mathcal{R}_1) = \{1, c, b, bc\}$. Logo, $\mathcal{R}_1$ é de facto confluente, e $F_{A_1}^{\mathcal{R}_1}$ é isomorfo ao grupo de

Klein, $\mathbb{Z}_2 \times \mathbb{Z}_2$. Pela Proposição 5.1.3, concluímos que $F_A^{\mathcal{R}}$ é o produto livre de $\mathbb{Z}$ e de $\mathbb{Z}_2 \times \mathbb{Z}_2$. Considere-se o seguinte $\widetilde{A}$-autómato inverso $\mathcal{A}$,



Vejamos que $\mathcal{A}$ é um $\mathcal{R}$-SFG: Como $\mathcal{A}$ é inverso, a condição I da definição de $\mathcal{R}$-autómato (Definição 7.1.7) é satisfeita. É claro que II também é satisfeita. Uma vez que todo o vértice distinto de q_ι tem grau superior a um, pelo Lema 7.1.9, facilmente concluímos III. Note-se que toda a aresta com rótulo em A_1 está contida no seguinte subgrafo de $\Gamma_{\mathcal{A}}$,



que, por sua vez, pertence a $\left[Sch_{A_1}(F_{A_1}^{\mathcal{R}_1}, \langle c \rangle)\right]_{\mathcal{A}}$. Logo, a condição IV é satisfeita e $\mathcal{A}$ é um $\mathcal{R}$-autómato. Por último, para verificar que $\mathcal{A}$ é um $\mathcal{R}$-SFG, basta mostrar que o subgrafo dado acima é útil em $\mathcal{A}$ relativamente a $\mathcal{R}$. Por exemplo, $aca^{-1} \in Irr(\mathcal{R})$ e é rótulo de um caminho bem sucedido em $\mathcal{A}$ que passa por uma aresta do subgrafo dado acima. Concluímos então que $\mathcal{A}$ é um $\mathcal{R}$-SFG.

O Exemplo 7.1.10 mostra que num $\mathcal{R}$-SFG podem existir vértices que não ocorrem em nenhum caminho bem sucedido com rótulo em $Irr(\mathcal{R})$. De facto, nesse exemplo, qualquer caminho bem sucedido em $\mathcal{A}$ que passa pelo vértice q_2, nunca vai ter rótulo em $Irr(\mathcal{R})$.

Proposição 7.1.11. *Seja $X \subseteq Irr(\mathcal{R})$. Então, $\mathcal{S}_{\mathcal{R}}(X)$ é um $\mathcal{R}$-SFG.*

Demonstração. Resulta diretamente da construção de $\mathcal{S}_{\mathcal{R}}(X)$ que este autómato é inverso e tem um ponto base. Seja p um vértice em $\mathcal{F}_{\mathcal{R}}(X)$ distinto do ponto base. Se p é um vértice em $\mathcal{F}(X)$ então, como $X \subseteq Irr(\mathcal{R}) \subseteq Irr(\mathcal{R}_A)$ e $\mathcal{F}(X)$ é involutivo, existem $(p, a, q_1), (p, b, q_2) \in E(\mathcal{F}_{\mathcal{R}}(X))$ tais que $a \neq b$. Se p não é um vértice em $\mathcal{F}(X)$, então está contido num grafo de Cayley de algum grupo finito não trivial. Logo também existem $(p, a, q_1), (p, b, q_2) \in E(\mathcal{F}_{\mathcal{R}}(X))$ tais que $a \neq b$. Podemos então concluir que, todo o vértice p em $\mathcal{F}_{\mathcal{R}}(X)$, distinto do ponto base, tem pelo menos duas arestas com rótulos

distintos que "saem" de p. Portanto, o mesmo acontece em $\mathcal{S}_{\mathcal{R}}(X)$ (arestas com rótulos distintos não são identificadas). Logo, pelo que foi visto no Lema 7.1.9, em $\mathcal{S}_{\mathcal{R}}(X)$ todo o vértice ocorre nalgum caminho bem sucedido de rótulo em $Irr(\mathcal{R}_A)$. Os Lemas 7.1.4 e 7.1.6 garantem as duas últimas condições. □

Assim como o Lema 7.1.9 facilita a verificação da condição III na definição de $\mathcal{R}$-autómato, seria útil algo do género para verificar quando é que um $\mathcal{R}$-autómato é um $\mathcal{R}$-SFG. Vamos então apresentar alguns resultados que nos vão permitir visualizar de uma forma mais clara, na representação geométrica de um dado $\mathcal{R}$-autómato, a condição de ser um $\mathcal{R}$-SFG.

Lema 7.1.12. *Seja $\mathcal{A}$ um $\mathcal{R}$-autómato. Seja (p,a,q) uma aresta de $\mathcal{A}$ com $a \in \widetilde{A_i}$ para algum $i \in \{1,\ldots,\mathfrak{N}\}$ e u uma palavra em $\widetilde{A_i}^*$ tal que $\overline{u}^{\mathcal{R}} = 1$. Então o caminho $p \xrightarrow{u} p \xrightarrow{a} q$ ocorre em $\mathcal{A}$.*

Demonstração. Como $\mathcal{A}$ é um $\mathcal{R}$-autómato, $\mathcal{A}$ satisfaz IV da Definição 7.1.7. Logo, o vértice p pertence a algum $K \in \left[Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, N)\right]_{\mathcal{A}}$ para algum $N \leqslant F_{A_i}^{\mathcal{R}_i}$. Ora, se $u \in \widetilde{A_i}^*$ é tal que $\overline{u}^{\mathcal{R}} = 1$, então $u = 1$ em $F_{A_i}^{\mathcal{R}_i}$ e, consequentemente, $Nv = Nvu$ para todo $v \in F_{A_i}^{\mathcal{R}_i}$. Logo, como p pertence a $K \simeq Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, N)$, concluímos que $p \xrightarrow{u} p \xrightarrow{a} q$ é um caminho em $\mathcal{A}$. □

Lema 7.1.13. *Seja $\mathcal{A}$ um $\mathcal{R}$-autómato e seja $p \xrightarrow{x} q$ um caminho em $\mathcal{A}$ com $x \in \widetilde{A_i}^+$ para algum $i \in \{1,\ldots,\mathfrak{N}\}$. Se $y \in \widetilde{A_i}^*$ é tal que $\overline{x}^{\mathcal{R}} = \overline{y}^{\mathcal{R}}$, então $\mathcal{A}$ admite um caminho da forma $p \xrightarrow{y} q$.*

Demonstração. Seja $y \in \widetilde{A_i}^*$ tal que $\overline{x}^{\mathcal{R}} = \overline{y}^{\mathcal{R}}$. Então $yx^{-1} \in \widetilde{A_i}^*$ e $\overline{yx^{-1}}^{\mathcal{R}} = 1$. Por hipótese, o caminho $p \xrightarrow{x} q$ ocorre em $\mathcal{A}$. Uma vez que x não é a palavra vazia, p é vértice de uma aresta etiquetada por uma letra de $\widetilde{A_i}$. Como $\mathcal{A}$ está nas condições do Lema 7.1.12, o caminho

$$p \xrightarrow{yx^{-1}} p \xrightarrow{x} q$$

ocorre em $\mathcal{A}$. Mas $\mathcal{A}$ é inverso, logo o caminho $p \xrightarrow{y} q$ ocorre em $\mathcal{A}$. □

Lema 7.1.14. *Seja $\mathcal{A}$ um $\mathcal{R}$-autómato. Se $p \xrightarrow{u} q$ é um caminho em $\mathcal{A}$, então $p \xrightarrow{\overline{u}^{\mathcal{R}}} q$ também é um caminho em $\mathcal{A}$.*

Demonstração. Seja $p \xrightarrow{u} q$ um caminho em $\mathcal{A}$. Se $u = \overline{u}^{\mathcal{R}}$, nada mais há a mostrar. Caso contrário, existem $u_1, u_2 \in \widetilde{A}^*$ e $(x,y) \in \mathcal{R}$ tais que $u = u_1 x u_2$. Note-se que,

como $1 \in Irr(\mathcal{R})$ e $\mathcal{R}$ é noetheriano, $x \neq 1$. Sejam p' e q' os vértices de $\mathcal{A}$ para os quais o caminho

$$p \xrightarrow{u_1} p' \xrightarrow{x} q' \xrightarrow{u_2} q$$

ocorre em $\mathcal{A}$. Como $\mathcal{R} = \cup_{i=0}^{\mathfrak{N}} \mathcal{R}_i$, sabemos que $(x, y) \in \mathcal{R}_i$ para algum $i \in \{0, \ldots, \mathfrak{N}\}$. Se $i = 0$, então $(x, y) = (aa^{-1}, 1)$ para algum $a \in \widetilde{A_0}$ e, como $\mathcal{A}$ é inverso, $p' = q'$. Logo, o caminho

$$p \xrightarrow{u_1} p' \xrightarrow{u_2} q$$

ocorre em $\mathcal{A}$. Se $i > 0$, então $x \in \widetilde{A_i}^+$, $y \in \widetilde{A_i}^*$, $\overline{x}^{\mathcal{R}} = \overline{y}^{\mathcal{R}}$ e, pelo Lema 7.1.13,

$$p \xrightarrow{u_1} p' \xrightarrow{y} q' \xrightarrow{u_2} q$$

é um caminho em $\mathcal{A}$. Como $\mathcal{R}$ é noetheriano, podemos concluir que

$$p \xrightarrow{\overline{u}^{\mathcal{R}}} q$$

é um caminho em $\mathcal{A}$. □

Corolário 7.1.15. *Seja $\mathcal{A}$ um $\mathcal{R}$-autómato. Se $u \in L(\mathcal{A})$, então $\overline{u}^{\mathcal{R}} \in L(\mathcal{A})$.* □

Note-se que, se $\mathcal{A}$ for um $\mathcal{R}$-autómato e $p \xrightarrow{u} q$ for um caminho em $\mathcal{A}$, então o Lema 7.1.14 garante-nos que o caminho $q \xrightarrow{\overline{u^{-1}}^{\mathcal{R}}} p$ também ocorre em $\mathcal{A}$.

Definição 7.1.16. *Seja $\mathcal{A}$ um $\mathcal{R}$-autómato. Dizemos que um dado vértice q de $\mathcal{A}$ é um* vértice partilhado *se q for o ponto base ou existirem $i, j \in \{0, \ldots, \mathfrak{N}\}$ distintos e $a_i \in \widetilde{A_i}$, $a_j \in \widetilde{A_j}$ tais que*

$$q_1 \xleftarrow{a_i} q \xrightarrow{a_j} q_2$$

ocorre em $\mathcal{A}$ para determinados vértices q_1, q_2 de $\mathcal{A}$.

Dada $u \in \widetilde{A}^+$ denotamos por $[\mathbf{u})$ a primeira letra de u e por $(\mathbf{u}]$ a última letra de u. No caso em que $u = 1$, $[u) = (u] = 1$.

Lema 7.1.17. *Seja $\mathcal{A}$ é um $\mathcal{R}$-autómato. Então $\mathcal{A}$ é um $\mathcal{R}$-SFG se e só se para todo $K \in Cay(\mathcal{A})$, K contém pelo menos dois vértices partilhados.*

Demonstração. Suponhamos primeiro que $\mathcal{A}$ é um $\mathcal{R}$-SFG e seja $K \in [Cay_{A_i}(F_{A_i}^{R_i})]_{\mathcal{A}}$ para algum $i \in \{1, \ldots, \mathfrak{N}\}$. Como $\mathcal{A}$ é um $\mathcal{R}$-SFG, temos que K é útil em $\mathcal{A}$ relativamente a $\mathcal{R}$. Suponhamos, por absurdo, que K tem menos que dois vértices partilhados. Como $\mathcal{A}$

é conexo por arcos, seja

$$q_\iota \xrightarrow{u} q$$

um caminho em $\mathcal{A}$ onde $q \in K$ e q_ι é o ponto base de $\mathcal{A}$. Podemos supor que q é o único vértice de K que ocorre nesse caminho. Ora, se $u = 1$, então $q_\iota = q$ e, por definição de vértice partilhado, K contém pelo menos um vértice partilhado. Suponhamos agora que $u \neq 1$. Como q é o único vértice de K que ocorre em $q_\iota \xrightarrow{u} q$, temos que $(u] \notin \widetilde{A_i}$. Logo, o vértice q é partilhado. Podemos então supor que K tem exatamente um vértice partilhado q. Mas então, qualquer caminho bem sucedido em $\mathcal{A}$ que passe por alguma aresta de K tem de ser da seguinte forma,

$$q_\iota \xrightarrow{u} q \xrightarrow{x} q \xrightarrow{v} q_\iota$$

com $x \in \widetilde{A_i}^+$. Além disso $q \xrightarrow{x} q$ é um caminho fechado em K e, uma vez que $K \simeq Cay_{A_i}(F_{A_i}^{\mathcal{R}_i})$, isto implica que $x = 1$ em $F_{A_i}^{\mathcal{R}_i}$. Logo $\overline{x}^{\mathcal{R}} = 1$. Logo, se $uxv \in Irr(\mathcal{R})$ então $x = 1$, o que é um absurdo pois $x \in \widetilde{A_i}^+$.

Reciprocamente, seja $K \in Cay(\mathcal{A})$. Então, por hipótese, K tem pelo menos dois vértices partilhados p e q que são distintos. Logo K é útil em $\mathcal{A}$ relativamente a $\mathcal{R}$. Basta observar que, pelo facto de $\mathcal{A}$ ser conexo por arcos, tem de existir em $\mathcal{A}$ um caminho da seguinte forma

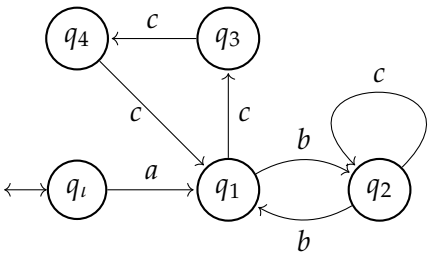
$$q_\iota \xrightarrow{u} p \xrightarrow{x} q \xrightarrow{v} q_\iota$$

e podemos supor que p e q são os únicos vértices em K que ocorrem, respetivamente, em $q_\iota \xrightarrow{u} p$ e em $q \xrightarrow{v} q_\iota$ e que $p \xrightarrow{x} q$ é um caminho em K. Logo, $\overline{u}^{\mathcal{R}}\overline{x}^{\mathcal{R}}\overline{v}^{\mathcal{R}} \in Irr(\mathcal{R})$ e, pelo Lema 7.1.14, é rótulo de um caminho bem sucedido em $\mathcal{A}$. Como p e q são distintos, necessariamente $\overline{x}^{\mathcal{R}} \neq 1$ pois, caso contrário, pelo Lema 7.1.14 tínhamos $p = q$. Logo este caminho bem sucedido percorre pelo menos uma aresta de K. □

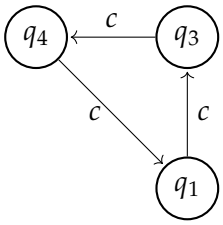
Exemplo 7.1.18. *Considere-se os seguintes alfabetos e os respetivos sistemas de reescrita*

$$\begin{aligned}
&A_0 = \{a\}, \quad A_1 = \{b\}, \quad A_2 = \{c\},\\
&\mathcal{R}_0 = \{(aa^{-1}, 1),\ (a^{-1}a, 1)\},\\
&\mathcal{R}_1 = \{(bb^{-1}, 1),\ (b^{-1}b, 1),\ (b^2, 1),\ (b^{-1}, b)\},\\
&\mathcal{R}_2 = \{(cc^{-1}, 1),\ (c^{-1}c, 1),\ (c^3, 1),\ (c^{-1}, c^2)\}.
\end{aligned}$$

Pelas Proposições 4.2.6 e 5.1.3 sabemos que $F_A^{\mathcal{R}} \simeq \mathbb{Z} * \mathbb{Z}_2 * \mathbb{Z}_3$. *Seja* $\mathcal{A}$ *o* $\widetilde{A}$*-autómato dado por*



Ora, facilmente se verifica que $\mathcal{A}$ *é um* $\mathcal{R}$*-autómato. No entanto, como existe* $K \in [Cay_{A_2}(F_{A_2}^{R_2})]_{\mathcal{A}}$



que tem apenas um vértice partilhado, q_1*, podemos concluir pelo Lema 7.1.17 que* $\mathcal{A}$ *não é um* $\mathcal{R}$*-*SFG. *Pela Proposição 7.1.11 concluímos ainda que* $\mathcal{A}$ *nunca vai ser um* $\mathcal{S}_{\mathcal{R}}(X)$ *para qualquer subconjunto* $X \subseteq Irr(\mathcal{R})$.

Vejamos agora que, através dos autómatos $\mathcal{S}_{\mathcal{R}}(X)$, podemos responder ao problema da palavra generalizado em $F_A^{\mathcal{R}}$.

Lema 7.1.19. *Seja* $\mathcal{A}$ *um* $\widetilde{A}$*-autómato involutivo. Seja* $\mathcal{B}$ *o autómato obtido a partir de* $\mathcal{A}$ *identificando sucessivamente pares de arestas da forma* $p \xleftarrow{a} q \xrightarrow{a} r \quad (a \in \widetilde{A})$ *até obtermos um autómato determinístico. Então,*

$$\overline{L(\mathcal{A})}^{\mathcal{R}} = \overline{L(\mathcal{B})}^{\mathcal{R}}.$$

Demonstração. Uma vez que $\mathcal{B}$ é obtido a partir de $\mathcal{A}$ através da identificação de arestas (e respetivamente vértices) da forma $p \xleftarrow{a} q \xrightarrow{a} r$, é fácil de ver que $L(\mathcal{A}) \subseteq L(\mathcal{B})$. Logo $\overline{L(\mathcal{A})}^{\mathcal{R}_A} \subseteq \overline{L(B)}^{\mathcal{R}_A}$. Dada $u \in L(\mathcal{B})$, e acrescentando se necessário fatores a u da forma aa^{-1} com $a \in \widetilde{A}$, também podemos concluir que existe $v \in L(\mathcal{A})$ tal que $\overline{u}^{\mathcal{R}_A} = \overline{v}^{\mathcal{R}_A}$. Logo,

$$\overline{L(\mathcal{A})}^{\mathcal{R}_A} = \overline{L(\mathcal{B})}^{\mathcal{R}_A}.$$

Como $\mathcal{R}_A \subseteq \mathcal{R}$, podemos concluir a igualdade enunciada. □

Proposição 7.1.20. *Seja H um subgrupo de $F_A^{\mathcal{R}}$ finitamente gerado por $X \subseteq Irr(\mathcal{R})$. Então,*

$$L(\mathcal{S}_{\mathcal{R}}(X)) \cap Irr(\mathcal{R}) = \overline{L(\mathcal{S}_{\mathcal{R}}(X))}^{\mathcal{R}} = \overline{H}^{\mathcal{R}}.$$

Demonstração. Primeiro, vamos mostrar que

$$\overline{L(\mathcal{S}_{\mathcal{R}}(X))}^{\mathcal{R}} = \overline{H}^{\mathcal{R}}.$$

É claro que $\overline{L(\mathcal{F}(X))}^{\mathcal{R}} = \overline{\langle X \rangle}^{\mathcal{R}}$. Como $\mathcal{F}_{\mathcal{R}}(X)$ é o autómato obtido a partir de $\mathcal{F}(X)$ acrescentando a alguns vértices grafos de Cayley de subgrupos finitos de $F_A^{\mathcal{R}}$, resulta que

$$\overline{L(\mathcal{F}_{\mathcal{R}}(X))}^{\mathcal{R}} = \overline{L(\mathcal{F}(X))}^{\mathcal{R}} = \overline{\langle X \rangle}^{\mathcal{R}}.$$

Pelo Lema 7.1.19, sabemos que $\overline{L(\mathcal{S}_{\mathcal{R}}(X))}^{\mathcal{R}} = \overline{L(\mathcal{F}_{\mathcal{R}}(X))}^{\mathcal{R}}$. Logo, $\overline{L(\mathcal{S}_{\mathcal{R}}(X))}^{\mathcal{R}} = \overline{\langle X \rangle}^{\mathcal{R}} = \overline{H}^{\mathcal{R}}$. Note-se que, consequentemente, temos que

$$L(\mathcal{S}_{\mathcal{R}}(X)) \cap Irr(\mathcal{R}) \subseteq \overline{L(\mathcal{S}_{\mathcal{R}}(X))}^{\mathcal{R}} = \overline{H}^{\mathcal{R}}.$$

Portanto, para concluir a demonstração, temos de mostrar que $L(\mathcal{S}_{\mathcal{R}}(X)) \cap Irr(\mathcal{R}) \supseteq \overline{H}^{\mathcal{R}}$. Seja $u \in \overline{H}^{\mathcal{R}} = \overline{\langle X \rangle}^{\mathcal{R}}$ não trivial (se $u = 1$, é claro que $u \in L(\mathcal{S}_{\mathcal{R}}(X)) \cap Irr(\mathcal{R})$). Então, existe $v = b_1^{\epsilon_1} \dots b_n^{\epsilon_n}$ para $n \geq 1$, $b_j \in X$ e $\epsilon_j \in \{1, -1\}$, tal que $\overline{v}^{\mathcal{R}} = u$. Por construção de $\mathcal{F}(X)$, temos que $v \in L(\mathcal{F}(X))$. Além disso, como $L(\mathcal{F}(X)) \subseteq L(\mathcal{F}_{\mathcal{R}}(X)) \subseteq L(\mathcal{S}_{\mathcal{R}}(X))$, temos que $v \in L(\mathcal{S}_{\mathcal{R}}(X))$. Pela Proposição 7.1.11, $\mathcal{S}_{\mathcal{R}}(X)$ é um $\mathcal{R}$-SFG e, portanto, pelo Lema 7.1.14 podemos concluir que $\overline{v}^{\mathcal{R}} = u \in L(\mathcal{S}_{\mathcal{R}}(X))$. Fica assim mostrada a inclusão $L(\mathcal{S}_{\mathcal{R}}(X)) \cap Irr(\mathcal{R}) \supseteq \overline{H}^{\mathcal{R}}$. □

Corolário 7.1.21. [*Problema da palavra generalizado*] *Dados $u \in F_A^{\mathcal{R}}$ e $H \leq_{f.g.} F_A^{\mathcal{R}}$, é decidível se $u \in H$.*

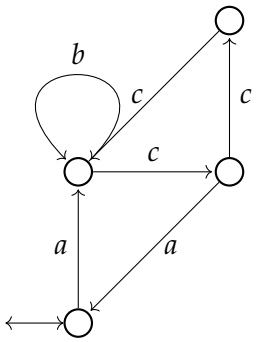
Demonstração. Seja X um subconjunto finito de $Irr(\mathcal{R})$ e $H = \langle X \rangle \leq_{f.g.} F_A^{\mathcal{R}}$. Ora, $u \in H$ se e só se $\overline{u}^{\mathcal{R}} \in \overline{H}^{\mathcal{R}}$. Pela Proposição 7.1.20, $\overline{u}^{\mathcal{R}} \in \overline{H}^{\mathcal{R}}$ se e só se $\overline{u}^{\mathcal{R}} \in L(\mathcal{S}_{\mathcal{R}}(X))$. □

De facto, um dos resultados que se conseguiu estender a grupos virtualmente livres finitamente gerados, com base nas generalizações da construção de Stallings apresentadas em [13] e [26], foi a decidibilidade do problema da palavra generalizado.

Exemplo 7.1.22. *Sejam,*

$$A_0 = \{a, b\}, \quad A_1 = \{c\},$$
$$\mathcal{R}_0 = \{(aa^{-1}, 1),\ (a^{-1}a, 1),\ (bb^{-1}, 1),\ (b^{-1}b, 1)\},$$
$$\mathcal{R}_1 = \{(cc^{-1}, 1),\ (c^{-1}c, 1),\ (c^3, 1),\ (c^{-1}, c^2)\}.$$

e $X = \{abca, a^{-1}c^2a^{-1}\} \subseteq Irr(\mathcal{R})$. *Seja* $H = \langle X \rangle$ *e suponhamos que queremos decidir se os elementos* $a^{-1}c^3aab^{-6}ca$ *e* $ab^5c^4a^2$ *de* $F_A^{\mathcal{R}}$ *estão em* H *ou não. Pelo Corolário 7.1.21, basta construir* $\mathcal{S}_{\mathcal{R}}(X)$ *e verificar se* $\overline{a^{-1}c^3aab^{-6}ca}^{\mathcal{R}} = ab^{-6}ca$, $\overline{ab^5c^4a^2}^{\mathcal{R}} = ab^5ca^2$ *são palavras em* $L(\mathcal{S}_{\mathcal{R}}(X))$. *Seguindo os passos da construção de* $\mathcal{S}_{\mathcal{R}}(X)$, *obtemos o seguinte autómato*



Logo, podemos concluir que $ab^{-6}ca \in H$ *e* $ab^5ca^2 \notin H$.

Lema 7.1.23. *Sejam* $\mathcal{A}_1$ *e* $\mathcal{A}_2$ $\widetilde{A}$*-autómatos inversos com um ponto base. Se* $L(\mathcal{A}_1) = L(\mathcal{A}_2)$, *então* $\mathcal{A}_1 \simeq \mathcal{A}_2$.

Demonstração. Sejam $\mathcal{A}_1 = (Q_1, q_\iota, q_\iota, E_1)$ e $\mathcal{A}_2 = (Q_2, q'_\iota, q'_\iota, E_2)$ e $\varphi_1 : Q_1 \to Q_2$ a função definida do seguinte modo: seja $q_1 \in Q_1$ e $u \in \widetilde{A}^*$ o rótulo de um caminho de q_ι a q_1,

$$q_\iota \xrightarrow{u} q_1 \ .$$

Note-se que tal caminho existe uma vez que $\mathcal{A}_1$ é inverso. Além disso $uu^{-1} \in L(\mathcal{A}_1)$. Como, $L(\mathcal{A}_1) = L(\mathcal{A}_2)$, temos que $uu^{-1} \in L(\mathcal{A}_2)$. Logo, em $\mathcal{A}_2$, existe um caminho da seguinte forma,

$$q'_\iota \xrightarrow{u} q_2 \xrightarrow{u^{-1}} q'_\iota$$

e este é único uma vez que $\mathcal{A}_2$ é determinístico. Definimos $q_1\varphi_1 = q_2$. Vejamos que, de facto, φ_1 está bem definida. Suponhamos que $q_\iota \xrightarrow{v} q_1$ é outro caminho em $\mathcal{A}_1$ e que $q'_\iota \xrightarrow{v} p_2 \xrightarrow{v^{-1}} q'_\iota$ é um caminho em $\mathcal{A}_2$. Queremos mostrar que $q_2 = p_2$. Ora, como $uv^{-1} \in L(\mathcal{A}_1) = L(\mathcal{A}_2)$, temos que $uv^{-1} \in L(\mathcal{A}_2)$. Logo, como $\mathcal{A}_2$ é determinístico, $q_2 \xrightarrow{v^{-1}} q'_\iota$ ocorre em $\mathcal{A}_2$. Temos então $q'_\iota \xrightarrow{v} q_2$ e $q'_\iota \xrightarrow{v} p_2$ ocorrem em

$\mathcal{A}_2$. Novamente, usando e determínismo de $\mathcal{A}_2$, resulta que $q_2 = p_2$. Note-se que, considerando $u = 1$, temos que $q_\iota\varphi_1 = q'_\iota$.

Seja $\varphi_2 : Q_2 \to Q_1$ definida de forma análoga. Então, $\varphi_1\varphi_2 = id_{Q_1}$ e $\varphi_2\varphi_1 = id_{Q_2}$. Logo φ_1 é bijetiva.

Agora basta observar que, se $(q_1, a, p_1) \in E_1$ então o seguinte o caminho

$$q_\iota \xrightarrow{u} q_1 \xrightarrow{a} p_1$$

ocorre em $\mathcal{A}_1$ e, portanto, pela definição de φ_1, temos que

$$q'_\iota \xrightarrow{u} q_1\varphi_1 \xrightarrow{a} p_1\varphi_1$$

ocorre em $\mathcal{A}_2$. Logo $(q_1\varphi_1, a, p_1\varphi_1) \in E_2$. Utilizando agora φ_2, se $(q_1\varphi_1, a, p_1\varphi_1) \in E_2$ então $(q_1\varphi_1\varphi_2, a, p_1\varphi_1\varphi_2) = (q_1, a, p_1) \in E_1$. Logo, φ_1 é um isomorfismo de autómatos. □

Se dois autómatos inversos satisfazem III na Definição 7.1.7, temos uma variação mais forte do lema anterior:

Proposição 7.1.24. *Sejam $\mathcal{A}_1$ e $\mathcal{A}_2$ A-autómatos inversos com um ponto base e tais que, todo o vértice pertence a um caminho bem-sucedido com rótulo em $Irr(\mathcal{R}_A)$. Se $L(\mathcal{A}_1) \cap Irr(\mathcal{R}_A) = L(\mathcal{A}_2) \cap Irr(\mathcal{R}_A)$, então $\mathcal{A}_1 \simeq \mathcal{A}_2$.*

Uma demonstração deste resultado pode ser vista em [25].

Definição 7.1.25. *Seja $u \in \widetilde{A}^*$ e, caso $u \neq 1$, seja $u = u_1 \dots u_n$, $n \geq 1$, a sua fatorização em componentes homogéneas relativamente à partição $\{A_i\}_{i\in\{0,\dots,\mathfrak{N}\}}$. Definimos*

$$\mathcal{E}[u] = \begin{cases} |\{u_j \ : \ \overline{u_j}^{\mathcal{R}} = 1, j \in \{1, \dots, n\}\}| & \text{se } u \neq 1 \\ 0 & \text{se } u = 1 \end{cases}$$

Exemplo 7.1.26. *Considere-se no Exemplo 7.1.22 as seguintes palavras em $\widetilde{A}^*$: $u = aaa^{-1}bc^6b^{-1}c^4b$, $v = c^3bc^4aa^{-1}$ e $w = abc^7a$. Então $\mathcal{E}[u] = 1$, $\mathcal{E}[v] = 2$ e $\mathcal{E}[w] = 0$.*

Proposição 7.1.27. *Sejam $\mathcal{A}_1$ e $\mathcal{A}_2$ autómatos $\mathcal{R}$-SFG tais que $L(\mathcal{A}_1) \cap Irr(\mathcal{R}) = L(\mathcal{A}_2) \cap Irr(\mathcal{R})$. Então, $L(\mathcal{A}_1) \cap Irr(\mathcal{R}_A) = L(\mathcal{A}_2) \cap Irr(\mathcal{R}_A)$.*

Demonstração. Vamos mostrar que se $u \in L(\mathcal{A}_1) \cap Irr(\mathcal{R}_A)$ então $u \in L(\mathcal{A}_2) \cap Irr(\mathcal{R}_A)$. Para tal, vamos usar indução sobre $\mathcal{E}[u]$. Se $\mathcal{E}[u] = 0$ e $u = 1$, como $1 \in Irr(\mathcal{R})$,

temos que $u \in L(\mathcal{A}_1) \cap Irr(\mathcal{R})$. Como por hipótese, $L(\mathcal{A}_1) \cap Irr(\mathcal{R}) = L(\mathcal{A}_2) \cap Irr(\mathcal{R})$, resulta que $u \in L(\mathcal{A}_2) \cap Irr(\mathcal{R}_A)$. Suponhamos então que $\mathcal{E}[u] = 0$ e $u \neq 1$ e seja $u = u_1 \dots u_n$ a sua fatorização em componentes homogéneas relativamente à partição $\{A_i\}_{i\in\{0,\dots,\mathfrak{N}\}}$. Então, $\overline{u}^{\mathcal{R}} = \overline{u_1}^{\mathcal{R}} \dots \overline{u_n}^{\mathcal{R}}$ e, se existe $j \in \{1,\dots,n\}$ tal que $u_j \in \widetilde{A_0}^+$, então $\overline{u_j}^{\mathcal{R}} = u_j$ pois $u \in Irr(\mathcal{R}_A)$. Pelo Corolário 7.1.15, $\overline{u}^{\mathcal{R}} \in L(\mathcal{A}_1) \cap Irr(\mathcal{R}) = L(\mathcal{A}_2) \cap Irr(\mathcal{R})$. Como $\mathcal{E}[u] = 0$, para todo $j \in \{1,\dots,n\}$, $\overline{u_j}^{\mathcal{R}} \neq 1$. Logo, pelo Lema 7.1.13, $u \in L(\mathcal{A}_2) \cap Irr(\mathcal{R}_A)$.

Suponhamos agora que $\mathcal{E}[u] = d + 1$, para algum $d \in \mathbb{N}$ e que a hipótese é válida para palavras u' em $L(\mathcal{A}_1) \cap Irr(\mathcal{R}_A)$ com $\mathcal{E}[u'] \leq d$. Como $\mathcal{E}[u] \geq 1$ e $u \in Irr(\mathcal{R}_A)$, temos que $u = x_1 u_i x_2$ com $u_i \in \widetilde{A_i}^+$ para algum $i \in \{1,\dots,\mathfrak{N}\}$ e $\overline{u_i}^{\mathcal{R}} = 1$. Além disso, $(x_1], [x_2) \notin \widetilde{A_i}$ e $\mathcal{E}[x_1], \mathcal{E}[x_2] \leq d$. Como $x_1 u_i x_2 \in L(\mathcal{A}_1)$, o seguinte caminho ocorre em $\mathcal{A}_1$,

$$q_\iota \xrightarrow{x_1} p \xrightarrow{u_i} p' \xrightarrow{x_2} q_\iota \ .$$

Sabemos também, pelo facto de $\mathcal{A}_1$ ser um $\mathcal{R}$-SFG e $u_i \neq 1$, que o caminho $p \xrightarrow{u_i} p'$ está contido em algum $K \in Sch_i(\mathcal{A}_1)$. Como $\overline{u_i}^{\mathcal{R}} = 1$, temos que $u_i = 1$ em $F_{A_i}^{\mathcal{R}_i}$. Logo, $p = p'$ e o caminho

$$q_\iota \xrightarrow{x_1} p \xrightarrow{x_2} q_\iota$$

ocorre em $\mathcal{A}_1$, onde p é um vértice de K. Como $\mathcal{A}_1$ é um $\mathcal{R}$-SFG, K é útil em $\mathcal{A}_1$ relativamente ao sistema de reescrita $\mathcal{R}$. Logo, existe $y_1 v_i y_2 \in Irr(\mathcal{R})$ com $(y_1], [y_2) \notin \widetilde{A_i}$ e $v_i \in \widetilde{A_i}^+$, tal que o caminho

$$q_\iota \xrightarrow{y_1} q \xrightarrow{v_i} q' \xrightarrow{y_2} q_\iota$$

ocorre em $\mathcal{A}_1$ e $q \xrightarrow{v_i} q'$ é um caminho em K. Logo, tal como o vértice p, os vértices q e q' são vértices de K. Existem apenas dois cenários possíveis:

Caso 1: Se o vértice p coincide com q', então $x_1 v_i^{-1} y_1^{-1}, y_1 v_i x_2 \in L(\mathcal{A}_1)$. Como $\mathcal{A}_1$ é um $\mathcal{R}$-SFG,

$$x_1 \overline{\overline{v_i^{-1}}^{\mathcal{R}} \overline{y_1^{-1}}^{\mathcal{R}}} \in L(\mathcal{A}_1).$$

Note-se que, como $y_1 \in Irr(\mathcal{R})$ e $(y_1] \notin \widetilde{A_i}$, então $[\overline{y_1^{-1}}^{\mathcal{R}}) \notin \widetilde{A_i}$ pois, caso contrário,

$$\overline{y_1 \overline{y_1^{-1}}^{\mathcal{R}}}^{\mathcal{R}} = \overline{y_1 \overline{y_1^{-1}}^{\mathcal{R}}}^{\mathcal{R}} \neq 1.$$

Além disso, como $v_i \in \widetilde{A_i}^+$, então $\overline{v_i^{-1}}^{\mathcal{R}} \in \widetilde{A_i}^+$ pois, caso contrário,

$$\overline{v_i v_i^{-1}}^{\mathcal{R}} = \overline{v_i \overline{v_i^{-1}}^{\mathcal{R}}}^{\mathcal{R}} \neq 1.$$

Portanto, $\overline{v_i^{-1}}^{\mathcal{R}} \overline{y_1^{-1}}^{\mathcal{R}}$ (respetivamente, $y_1 v_i$) é uma palavra irredutível com a primeira letra (respetivamente última letra) em $\widetilde{A_i}$. Logo, como $(x_1], [x_2) \notin \widetilde{A_i}$, $\mathcal{E}[x_1 \overline{v_i^{-1}}^{\mathcal{R}} \overline{y_1^{-1}}^{\mathcal{R}}] = \mathcal{E}[x_1] \leq d$ e $\mathcal{E}[y_1 v_i x_2] = \mathcal{E}[x_2] \leq d$. Note-se também que $x_1 \overline{v_i^{-1}}^{\mathcal{R}} \overline{y_1^{-1}}^{\mathcal{R}}$, $y_1 v_i x_2 \in Irr(\mathcal{R}_A)$. Logo, por hipótese de indução,

$$x_1 \overline{v_i^{-1}}^{\mathcal{R}} \overline{y_1^{-1}}^{\mathcal{R}}, \ y_1 v_i x_2 \in L(\mathcal{A}_2) \cap Irr(\mathcal{R}_A).$$

Como $\mathcal{A}_2$ tem um ponto base,

$$x_1 \overline{v_i^{-1}}^{\mathcal{R}} \overline{y_1^{-1}}^{\mathcal{R}} y_1 v_i x_2 \in L(\mathcal{A}_2).$$

e como $\mathcal{A}_2$ é $\mathcal{R}$-SFG, $x_1 \overline{v_i^{-1}}^{\mathcal{R}} v_i x_2 \in L(\mathcal{A}_2)$. Agora basta notar que $\overline{v_i^{-1}}^{\mathcal{R}} v_i$ é uma palavra em $\widetilde{A_i}^+$ e $\overline{v_i^{-1} \overline{v_i^{-1}}^{\mathcal{R}} v_i}^{\mathcal{R}} = 1 = \overline{u_i}^{\mathcal{R}}$ logo, pelo Lema 7.1.13, $u = x_1 u_i x_2 \in L(\mathcal{A}_2)$.

Caso 2: Se o vértice p não coincidir com q', existe em K um caminho de p para q' que tem como rótulo uma palavra $w \in Irr(\mathcal{R}_i) \subseteq Irr(\mathcal{R})$ com $w \neq 1$. Mas então,

$$x_1 w y_2, \ y_2^{-1} w^{-1} x_2 \in L(\mathcal{A}_1).$$

Como $\mathcal{A}_1$ é um $\mathcal{R}$-SFG,

$$\overline{y_2^{-1}}^{\mathcal{R}} \overline{w^{-1}}^{\mathcal{R}} x_2 \in L(\mathcal{A}_1)$$

Além disso, como $w \in \widetilde{A_i}^+$ e $[y_2) \notin \widetilde{A_i}$, temos que $\overline{y_2^{-1}}^{\mathcal{R}} \overline{w^{-1}}^{\mathcal{R}}$ (respetivamente $w y_2$) é uma palavra irredutível com a última letra (respetivamente primeira letra) em $\widetilde{A_i}$. Logo, como $(x_1], [x_2) \notin \widetilde{A_i}$, temos que $\mathcal{E}[x_1 w y_2] = \mathcal{E}[x_1] \leq d$ e $\mathcal{E}[\overline{y_2^{-1}}^{\mathcal{R}} \overline{w^{-1}}^{\mathcal{R}} x_2] = \mathcal{E}[x_2] \leq d$, podemos usar novamente a hipótese de indução para concluir que

$$x_1 w y_2, \ \overline{y_2^{-1}}^{\mathcal{R}} \overline{w^{-1}}^{\mathcal{R}} x_2 \in L(\mathcal{A}_2) \cap Irr(\mathcal{R}_A).$$

Como $\mathcal{A}_2$ tem um ponto base,

$$x_1 w y_2 \overline{y_2^{-1}}^{\mathcal{R}} \overline{w^{-1}}^{\mathcal{R}} x_2 \in L(\mathcal{A}_2)$$

e, como também é um $\mathcal{R}$-SFG, $x_1 w \overline{w^{-1}}^{\mathcal{R}} x_2 \in L(\mathcal{A}_2)$. Agora, como $\overline{w \overline{w^{-1}}^{\mathcal{R}}}^{\mathcal{R}} = 1 = \overline{u_i}^{\mathcal{R}}$ e $w \overline{w^{-1}}^{\mathcal{R}} \in \widetilde{A_i}^+$, usamos novamente o Lema 7.1.13 para concluir que $u = x_1 u_i x_2 \in$

$L(\mathcal{A}_2) \cap Irr(\mathcal{R}_A)$. Concluímos assim que $L(\mathcal{A}_1) \cap Irr(\mathcal{R}_A) \subseteq L(\mathcal{A}_2) \cap Irr(\mathcal{R}_A)$ e a inclusão oposta é completamente análoga. □

Corolário 7.1.28. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ e $X \subseteq Irr(\mathcal{R})$ um subconjunto finito tal que $\langle X \rangle = H$. Então $\mathcal{S}_{\mathcal{R}}(X)$ não depende do subconjunto finito X de geradores de H escolhido e da ordem pela qual as dobragens são feitas.*

Demonstração. Pela Proposição 7.1.11, sabemos que $\mathcal{S}_{\mathcal{R}}(X)$ é um $\mathcal{R}$-SFG. Sabemos também, pela Proposição 7.1.20, que $L(\mathcal{S}_{\mathcal{R}}(X)) \cap Irr(\mathcal{R}) = \overline{H}^{\mathcal{R}}$. Logo, $L(\mathcal{S}_{\mathcal{R}}(X)) \cap Irr(\mathcal{R})$ é independente do subconjunto finito de geradores X e da ordem pela qual as dobragens são feitas. Pela Proposição 7.1.27, isto implica que $L(\mathcal{S}_{\mathcal{R}}(X)) \cap Irr(\mathcal{R}_A)$ também o é. Basta agora aplicar a Proposição 7.1.24. □

Note-se que, dado $H \leqslant_{f.g.} F_A^{\mathcal{R}}$, o Corolário 7.1.28 permite-nos usar a notação $\mathcal{S}_{\mathcal{R}}H$ sem termos de especificar um conjunto finito de geradores X de H. Além disso, pela Proposição 7.1.20, sabemos que a função

$$\begin{aligned} \Lambda \colon \{H \ : \ H \leq_{f.g.} F_A^{\mathcal{R}}\} &\to \{ \text{ classes de isomorfismo de autómatos } \mathcal{R}\text{-}SFG \ \} \\ H &\mapsto \mathcal{S}_{\mathcal{R}}H \end{aligned}$$

é injetiva. A resposta à pergunta relativa à sobrejetividade é dada no próximo capítulo.

8. Algumas aplicações

Vimos já no capítulo anterior um exemplo da utilidade dos autómatos $\mathcal{S}_{\mathcal{R}}H$, para um dado $H \leq_{f.g.} F_A^{\mathcal{R}}$: a decidibilidade do problema da palavra generalizado em $F_A^{\mathcal{R}}$. Este capítulo tem como principal objetivo reforçar a ideia de que, de facto, estes autómatos são uma excelente ferramenta para trabalhar com subgrupos finitamente gerados de $F_A^{\mathcal{R}}$.

8.1. Estudo da torção

Nesta secção, vamos estudar o problema da torção, isto é, dado $H \leq_{f.g.} F_A^{\mathcal{R}}$, será que conseguimos decidir se H tem ou não torção? Note-se que, o facto dos elementos da base escolhida para H serem livres de torção, não implica que H o seja.

Exemplo 8.1.1. *Sejam,*

$$\begin{aligned} &A_0 = \{a\}, \quad A_1 = \{b\}, \\ &\mathcal{R}_0 = \{(aa^{-1}, 1),\ (a^{-1}a, 1)\}, \\ &\mathcal{R}_1 = \{(bb^{-1}, 1),\ (b^{-1}b, 1),\ (b^3, 1),\ (b^{-1}, b^2)\}. \end{aligned}$$

e $X = \{ab, a\} \subseteq Irr(\mathcal{R})$. *Seja* $H = \langle X \rangle$. *É fácil de ver que, para todo o* $n \geq 1$, a^n, $(ab)^n \in Irr(\mathcal{R})$ *e, portanto,* a *e* ab *não têm torção. No entanto,* $b = a^{-1}ab \in H$ *e* $b^3 = 1$.

Se queremos estudar a torção em subgrupos finitamente gerados de $F_A^{\mathcal{R}}$, convém perceber que características têm os elementos com torção. Para tal, será útil generalizar a definição de uma palavra ciclicamente $\mathcal{R}_A$-reduzida, já apresentada na Secção 6.1.

Definição 8.1.2. *Uma palavra* $u \in Irr(\mathcal{R})$ *diz-se ciclicamente* $\mathcal{R}$*-reduzida se não for da forma* $wv\overline{w^{-1}}^{\mathcal{R}}$ *com* $w, v \in \widetilde{A}^+$.

Lema 8.1.3. *Toda a palavra* $u \in Irr(\mathcal{R})$ *se fatoriza, em* $\widetilde{A}^*$*, como um produto da forma* $wv\overline{w^{-1}}^{\mathcal{R}}$ *com* v *ciclicamente* $\mathcal{R}$*-reduzida e* $w \in Irr(\mathcal{R})$.

Demonstração. Usamos indução sobre $|u|$. Se $|u| = 0$, então $u = 1$ que é ciclicamente $\mathcal{R}$-reduzida. Suponhamos agora que $|u| = n + 1$ com $n \in \mathbb{N}$ e que a existência da fatorização é válida para palavras de comprimento menor que $n + 1$. Se u for ciclicamente $\mathcal{R}$-reduzida então nada há a mostrar. Caso contrário, $u = wv\overline{w^{-1}}^{\mathcal{R}}$ com $w \in \widetilde{A}^+$. Mas então, $|v| < n + 1$ e, portanto, usando a hipótese de indução, v fatoriza-se como um produto da forma $w'v'\overline{w'^{-1}}^{\mathcal{R}}$ com v' ciclicamente $\mathcal{R}$-reduzida. Logo, $u = ww'v'\overline{w'^{-1}}^{\mathcal{R}}\overline{w^{-1}}^{\mathcal{R}}$.

Ora, como $u \in Irr(\mathcal{R})$, temos que $\overline{\overline{w'^{-1}}^{\mathcal{R}}\overline{w^{-1}}^{\mathcal{R}}} = \overline{\overline{w'^{-1}}w^{-1}}^{\mathcal{R}} = \overline{(ww')^{-1}}^{\mathcal{R}}$ e v' é ciclicamente $\mathcal{R}$-reduzida. □

No caso em que $\mathcal{R} = \mathcal{R}_A$, esta fatorização é única. No entanto, a unicidade não é garantida em geral. Considere-se novamente o Exemplo 8.1.1 e seja $u = b^2ab^2 \in Irr(\mathcal{R})$. Então, tanto para $w = b^2, v = ab$ como para $w = b, v = ba$, obtemos duas fatorizações nas condições do Lema 8.1.3.

Lema 8.1.4. *Seja $u \in Irr(\mathcal{R})$ uma palavra ciclicamente $\mathcal{R}$-reduzida. Se u tem ordem finita em $F_A^{\mathcal{R}}$, então $u \in \widetilde{A_i}^*$ para algum $i \in \{1, \dots, \mathfrak{N}\}$.*

Demonstração. O caso em que $u = 1$ é trivial. Suponhamos então que $u \neq 1$ e considere-se a fatorização de u em componentes homogéneas, $u = u_1 \dots u_n$ para algum $n \geq 1$. Como u tem ordem finita, existe um $k \in \mathbb{N}$ tal que $\overline{u^k}^{\mathcal{R}} = 1$. Portanto, como $u \in Irr(\mathcal{R})$, necessariamente u_1 e u_n são componentes do mesmo tipo, isto é, $u_1, u_n \in \widetilde{A_i}^+$ para algum $i \in \{0, \dots, \mathfrak{N}\}$. Portanto $n \neq 2$. Suponhamos que $n > 2$. Então, como $u \in Irr(\mathcal{R})$ é ciclicamente $\mathcal{R}$-reduzida, $u_n \neq \overline{u_1^{-1}}^{\mathcal{R}}$, logo $u_n u_1 \neq 1$ em $F_A^{\mathcal{R}}$. Mas isto não pode acontecer, caso contrário, u_2 não desaparece em $\overline{(u_1 \dots u_n) \dots (u_1 \dots u_n)}^{\mathcal{R}}$. Portanto $n = 1$. Logo, $u = u_1 \in \widetilde{A_i}^+$. Basta agora observar que $u \notin \widetilde{A_0}^+$, uma vez que $F_{A_0}^{\mathcal{R}_0}$ é o grupo livre gerado por A_0 e, portanto, não pode ter torção não trivial. □

Proposição 8.1.5. *Seja $H \leqslant_{f.g.} F_A^{\mathcal{R}}$. Então, H tem torção não trivial se e só se*

$$Sch(\mathcal{S}_{\mathcal{R}}H) \backslash Cay(\mathcal{S}_{\mathcal{R}}H) \neq \emptyset.$$

Demonstração. O caso em que H é trivial é claro. Suponhamos então que H não é trivial. [⇐] Seja $K \in \left[Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, N)\right]_{\mathcal{S}_{\mathcal{R}}H}$, para alguns $i \in \{1, \dots, \mathfrak{N}\}$ e $N \leq F_{A_i}^{\mathcal{R}_i}$ não trivial. Seja q um vértice de K tal que

$$q_\iota \xrightarrow{u} q$$

é um caminho em $\mathcal{S}_{\mathcal{R}}H$ em que $(u] \notin \widetilde{A_i}$, $u \in Irr(\mathcal{R})$ e q_ι é o ponto base de $\mathcal{S}_{\mathcal{R}}H$. Note-se que tal caminho existe uma vez que K é útil relativamente a $\mathcal{R}$. Como N é não trivial e $K \simeq Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, N)$, existe $v \in \overline{F_{A_i}^{R_i}}^{\mathcal{R}}$, com $v \neq 1$, tal que

$$q_\iota \xrightarrow{u} q \xrightarrow{v} q \xrightarrow{u^{-1}} q_\iota$$

ocorre em $\mathcal{S}_{\mathcal{R}}H$. Portanto, $uvu^{-1} \in L(\mathcal{S}_{\mathcal{R}}H)$ e, como $\mathcal{S}_{\mathcal{R}}H$ é um $\mathcal{R}$-SFG, $\overline{uvu^{-1}}^{\mathcal{R}} \in L(\mathcal{S}_{\mathcal{R}}H)$. Logo, pela Proposição 7.1.20, $\overline{uvu^{-1}}^{\mathcal{R}} \in \overline{H}^{\mathcal{R}}$ e $\overline{uvu^{-1}}^{R} = \overline{u}^R v \overline{u^{-1}}^R \neq 1$.

Como $F_{A_i}^{\mathcal{R}_i}$ é um grupo finito e $v \in F_{A_i}^{\mathcal{R}_i}$, existe um $k \geq 1$ tal que $v^k = 1$ em $F_A^{\mathcal{R}}$. Logo, $(\overline{u}^R v \overline{u^{-1}}^R)^k = \overline{u}^R v^k \overline{u^{-1}}^R = 1$ em $F_A^{\mathcal{R}}$.

$[\Rightarrow]$ Seja $u \in \overline{H}^{\mathcal{R}}$ um elemento de torção não trivial. Então, pela Proposição 7.1.20, $u \in L(\mathcal{S}_{\mathcal{R}}H) \cap Irr(\mathcal{R})$. Seja $u = wv\overline{w^{-1}}^{\mathcal{R}}$ uma fatorização de u em $\widetilde{A}^*$, com v ciclicamente $\mathcal{R}$-reduzida, e

$$q_\iota \xrightarrow{w} q \xrightarrow{v} q' \xrightarrow{\overline{w^{-1}}^{\mathcal{R}}} q_\iota$$

o respetivo caminho em $\mathcal{S}_{\mathcal{R}}H$. Então, existe um $k \geq 1$ tal que $\overline{u^k}^{\mathcal{R}} = \overline{wv^k\overline{w^{-1}}^{\mathcal{R}}}^{\mathcal{R}} = 1$. Logo $\overline{v^k}^{\mathcal{R}} = 1$. Como v é ciclicamente $\mathcal{R}$-reduzida e não é a palavra vazia (u é não trivial), pelo Lema 8.1.4, $v \in \widetilde{A_i}^+$ para algum $i \in \{1, \ldots, \mathfrak{N}\}$. Além disso, como $\mathcal{S}_{\mathcal{R}}H$ é um $\mathcal{R}$-SFG, $q \xrightarrow{\overline{w^{-1}}^{\mathcal{R}}} q_\iota$ ocorre em $\mathcal{S}_{\mathcal{R}}H$. Logo, como $\mathcal{S}_{\mathcal{R}}H$ é determinístico, $q = q'$. Portanto, como $v \in Irr(\mathcal{R}_i)$ e não é a palavra vazia, o vértice q pertence a algum $K \in \left[Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, N)\right]_{\mathcal{S}_{\mathcal{R}}H}$ para algum $N \leqslant F_{A_i}^{\mathcal{R}_i}$ não trivial. Note-se que se N for trivial, $Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, N) = Sch_{A_i}(F_{A_i}^{\mathcal{R}_i}, \{1\}) \simeq Cay_{A_i}(F_{A_i}^{\mathcal{R}_i})$ e qualquer rótulo de um caminho fechado em $Cay_{A_i}(F_{A_i}^{\mathcal{R}_i})$ é, como elemento de $F_{A_i}^{\mathcal{R}_i}$, a identidade do grupo. □

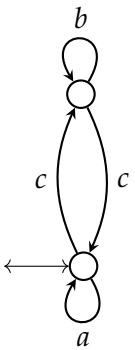
Portanto, a partir da estrutura de $\mathcal{S}_{\mathcal{R}}H$ para um dado $H \leq_{f.g.} F_A^{\mathcal{R}}$, conseguimos analisar se H tem ou não torção não trivial. Resulta então o seguinte corolário:

Corolário 8.1.6. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$. Então é decidível determinar se H tem elementos de torção não triviais.*

Exemplo 8.1.7. *Suponhamos que,*

$$A_0 = \{a, b\}, \quad \mathcal{R}_0 = \{(aa^{-1}, 1), (a^{-1}a, 1), (bb^{-1}, 1), (b^{-1}b, 1)\},$$
$$A_1 = \{c\}, \quad \mathcal{R}_1 = \{(cc^{-1}, 1), (c^{-1}c, 1), (c^4, 1), (c^{-1}, c^3)\}.$$

Então $F_A^{\mathcal{R}}$ é o produto livre do grupo livre de dimensão 2 com o grupo cíclico de ordem 4. Seja $H = \langle ac^2, acbc, cb^{-1}c\rangle$. Facilmente se verifica que $\mathcal{S}_{\mathcal{R}}H$ é dado por



Como $\{1, c^2\} \leq F_{A_1}^{\mathcal{R}_1}$ *e* $\left[Sch_{A_1}(F_{A_1}^{\mathcal{R}_1}, \{1, c^2\})\right]_{\mathcal{S}_{\mathcal{R}}H} \neq \emptyset$, H *tem elementos de torção não triviais. De facto,*

$$(acb)c^2(acb)^{-1} = (acbc)(cb^{-1}c)(c^2a^{-1}) \in H$$

é um elemento não trivial e $(acbc^2(acb)^{-1})^2 = 1$ *em* $F_A^{\mathcal{R}}$.

Podemos então questionar-nos sobre quando é que um dado $H \leq_{f.g.} F_A^{\mathcal{R}}$ é um grupo livre. Em [27], Stallings provou que um grupo finitamente gerado, livre de torção que contém um subgrupo livre de índice finito é livre, isto é, um grupo virtualmente livre, finitamente gerado e livre de torção é livre. Sabemos também, pelo Teorema de Kurosh (Teorema 5.1.7), que $H \leq_{f.g.} F_A^{\mathcal{R}}$ é novamente um grupo singelo (logo, virtualmente livre). Logo conseguimos deduzir que H é livre se e só se é livre de torção. De seguida, veremos uma prova alternativa para este resultado, usando apenas as propriedades de $\mathcal{S}_{\mathcal{R}}H$. Além disso, mostraremos também, caso H seja livre, como computar uma base a partir de $\mathcal{S}_{\mathcal{R}}H$ e calcular a sua cardinalidade.

Seja $\mathcal{A}$ um $\widetilde{A}$-autómato inverso com m vértices. Uma *árvore geradora* $\mathcal{T}$ de $\mathcal{A}$ é um subgrafo de $\Gamma_{\mathcal{A}}$ que é involutivo, conexo, contém todos os vértices de $\mathcal{A}$ e tem a seguinte propriedade: Se $(p, a, q) \in E(\mathcal{T})$ e $\mathcal{T}'$ é o grafo obtido a partir de $\mathcal{T}$ eliminando as arestas $(p, a, q), (q, a^{-1}, p)$, então $\mathcal{T}'$ é desconexo. Usando indução sobre $|Q(\mathcal{A})|$, facilmente se mostra que $|E(\mathcal{T})| = 2(|Q(\mathcal{A})| - 1)$, onde exatamente $|Q(\mathcal{A})| - 1$ arestas têm rótulo em A. Note-se que se a $\mathcal{A}$ retirarmos o número maximal de arestas (e as respetivas inversas) de forma a manter a conexidade, então o autómato resultante é necessariamente uma árvore geradora. No caso em que $\mathcal{A}$ tem um ponto base q_ι e $p \in Q(\mathcal{A})$, designamos por w_p a $\mathcal{T}$*-geodésica* que conecta o ponto base q_ι a p, isto é, o rótulo do caminho mais curto em $\mathcal{T}$ que liga q_ι a p, $q_\iota \xrightarrow{w_p} p$. Note-se que, uma vez que $\mathcal{T}$ é uma árvore geradora, esta $\mathcal{T}$-geodésica existe e é única. Além disso, se $(p, a, q) \in E(\mathcal{T})$, então $w_q = w_p a$ ou $w_p = w_q a^{-1}$.

Proposição 8.1.8. *Seja* $H \leqslant_{f.g.} F_A^{\mathcal{R}}$. *Então* H *é um grupo livre se e só se* H *é livre de torção. Além disso, caso* H *seja livre, conseguimos computar uma base* $\mathcal{B}$ *de* H *a partir de um conjunto de geradores de* H *e*

$$|\mathcal{B}| = \left(\sum_{q \in Q(\mathcal{S}_{\mathcal{R}}H)} deg_{A_0}(q) - 1 + |Cay_q(\mathcal{S}_{\mathcal{R}}H)| \right) - |Cay(\mathcal{S}_{\mathcal{R}}H)| + 1.$$

Demonstração. Primeiro vamos mostrar que H é um grupo livre se e só se H é livre de torção: $[\Rightarrow]$ É clara.

$[\Leftarrow]$ Para mostrar esta implicação vamos apresentar um algoritmo que, a partir de $\mathcal{S}_{\mathcal{R}}H$ onde $H \leq_{f.g.} F_A^{\mathcal{R}}$ é livre de torção, fornece-nos uma base do grupo H concluindo que este é livre. Como H é livre de torção, pela Proposição 8.1.5, toda a aresta $p \xrightarrow{a} q$ de $\mathcal{S}_{\mathcal{R}}H$ onde $a \in \widetilde{A_i}$ para algum $i \in \{1,\dots,\mathfrak{N}\}$, está contida em algum $K \in Cay(\mathcal{S}_{\mathcal{R}}H)$. Considere-se o seguinte procedimento:

$[1]$ Para todo o $K \in Cay(\mathcal{S}_{\mathcal{R}}H)$ retire-se o número maximal de arestas (e as respetivas inversas) de forma a manter a conexidade de K. Seja $\mathcal{T}^+$ este novo autómato. Note-se que $\mathcal{T}^+$ é conexo, involutivo e tem um ponto base q_ι. Vamos mostrar que $\overline{L(\mathcal{T}^+)}^{\mathcal{R}} = \overline{L(\mathcal{S}_{\mathcal{R}}H)}^{\mathcal{R}}$. É claro que a palavra vazia está em ambos os conjuntos da igualdade. Ora, como $L(\mathcal{T}^+) \subseteq L(\mathcal{S}_{\mathcal{R}}H)$. temos que $\overline{L(\mathcal{T}^+)}^{\mathcal{R}} \subseteq \overline{L(\mathcal{S}_{\mathcal{R}}H)}^{\mathcal{R}}$. Suponhamos então que $u \in \overline{L(\mathcal{S}_{\mathcal{R}}H)}^{\mathcal{R}} = L(\mathcal{S}_{\mathcal{R}}H) \cap Irr(\mathcal{R})$ é uma palavra não vazia. Seja $u = a_1 \dots a_n$, $n \geq 1$ e $a_j \in \widetilde{A}$ para todo o $j \in \{1,\dots,n\}$. Então, como $u \in L(\mathcal{S}_{\mathcal{R}}H)$, existe um caminho em $\mathcal{S}_{\mathcal{R}}H$ da seguinte forma:

$$q_\iota = q_0 \xrightarrow{a_1} \dots \xrightarrow{a_n} q_n = q_\iota$$

Suponhamos que existe $j \in \{1,\dots,n\}$ tal que a aresta $q_{j-1} \xrightarrow{a_j} q_j$ não está em $\mathcal{T}^+$. Então, existe $r_j \in \{1,\dots,\mathfrak{N}\}$ tal que $a_j \in \widetilde{A_{r_j}}$ e, pelo Lema 7.1.4, q_{j-1} e q_j são vértices de algum $K \in \left[Cay_{A_{r_j}}(F_{A_{r_j}}^{\mathcal{R}_{r_j}})\right]_{\mathcal{S}_{\mathcal{R}}H}$. Como na construção de $\mathcal{T}^+$ foi exigida a conexidade do subgrafo resultante de K, existe em $\mathcal{T}^+$ um caminho da seguinte forma:

$$q_{j-1} \xrightarrow{v_j} q_j$$

onde $v_j \in \widetilde{A_{r_j}}^*$. Como K é isomorfo a $Cay_{A_{r_j}}(F_{A_{r_j}}^{\mathcal{R}_{r_j}})$, temos que $\overline{a_j}^{\mathcal{R}} = \overline{v_j}^{\mathcal{R}}$. Logo, existe $v \in L(\mathcal{T}^+)$ tal que $\overline{v}^{\mathcal{R}} = u$. Portanto, $u = \overline{v}^{\mathcal{R}} \in \overline{L(\mathcal{T}^+)}^{\mathcal{R}}$. Concluímos assim que $\overline{L(\mathcal{T}^+)}^{\mathcal{R}} = \overline{L(\mathcal{S}_{\mathcal{R}}H)}^{\mathcal{R}}$. Seja $\Phi : \widetilde{A}^* \to F_A^{\mathcal{R}}$ o homomorfismo canónico. Pela Proposição 7.1.20, sabemos que $\overline{L(\mathcal{S}_{\mathcal{R}}H)}^{\mathcal{R}} = \overline{H}^{\mathcal{R}}$. Logo, $(L(\mathcal{T}^+))\Phi = (L(\mathcal{S}_{\mathcal{R}}H))\Phi = H$.

$[2]$ Seja $\mathcal{T}$ uma árvore geradora de $\mathcal{T}^+ = (Q, q_\iota, q_\iota, E)$. Seja $E_A = E \cap (Q \times A \times Q)$. Considere-se

$$\mathcal{B} = \{w_p a w_q^{-1} \mid (p,a,q) \in E_A \setminus \mathcal{T}\}$$

onde w_p, w_q são as $\mathcal{T}$-geodésicas de $p, q \in Q(\mathcal{T})$, respetivamente. Vamos mostrar que $\mathcal{B}\Phi$ é uma base de $(L(\mathcal{T}^+))\Phi = H$. Para começar note-se que $\mathcal{B} \subseteq Irr(\mathcal{R}_A)$. Como $\mathcal{B} \subseteq L(\mathcal{T}^+)$, temos que $\langle \mathcal{B}\Phi \rangle \subseteq \langle (L(\mathcal{T}^+))\Phi \rangle = \langle H \rangle = H$. Seja $u \in L(\mathcal{T}^+)$ não trivial e suponhamos que $u = a_1 \dots a_n$ para algum $n \geq 1$ e $a_i \in \widetilde{A}$ para todo o $i \in \{1,\dots,n\}$.

Uma vez que $u \in L(\mathcal{T}^+)$, existe um caminho em $\mathcal{T}^+$ da seguinte forma,

$$q_\iota = q_0 \xrightarrow{a_1} \dots \xrightarrow{a_n} q_n = q_\iota \ .$$

Note-se que, para todo o $i \in \{1, \dots, n\}$, temos que $w_{q_{i-1}} a_i w_{q_i}^{-1} \in \mathcal{B} \cup \mathcal{B}^{-1}$ ou $(q_{i-1}, a_i, q_i) \in \mathcal{T}$. Mas, se $(q_{i-1}, a_i, q_i) \in \mathcal{T}$, então $w_{q_i} = w_{q_{i-1}} a_i$ ou $w_{q_{i-1}} = w_{q_i} a_i^{-1}$ e $\overline{w_{q_{i-1}} a_i w_{q_i}^{-1}}^{\mathcal{R}} = 1$. Logo,

$$u\Phi = (a_1 \dots a_n)\Phi = (w_{q_0} a_1 w_{q_1}^{-1} w_{q_1} a_2 w_{q_2}^{-1} \dots w_{q_{n-1}} a_n w_{q_0}^{-1})\Phi \in \langle \mathcal{B}\Phi \rangle.$$

Logo $(L(\mathcal{T}^+))\Phi \subseteq \langle \mathcal{B}\Phi \rangle$ e, portanto, $\langle (L(\mathcal{T}^+))\Phi \rangle \subseteq \langle \mathcal{B}\Phi \rangle$. Concluímos assim que $\langle \mathcal{B}\Phi \rangle = \langle (L(\mathcal{T}^+))\Phi \rangle = \langle H \rangle = H$.

Sejam $b_1, \dots, b_n \in \mathcal{B} \cup \mathcal{B}^{-1}$ com $n \geq 1$ e $b_i \neq b_{i-1}^{-1}$ para todo $i \in \{2, \dots, n\}$. Note-se que se $u \in L(\mathcal{T}^+)$, então $\mathcal{E}[\overline{u}^{\mathcal{R}_A}] = 0$. Então, como $b_1 \dots b_n \in L(\mathcal{T}^+)$, $\mathcal{E}[\overline{b_1 \dots b_n}^{\mathcal{R}_A}] = 0$. Logo, se $\overline{b_1 \dots b_n}^{\mathcal{R}_A} \neq 1$, temos que $\overline{b_1 \dots b_n}^{\mathcal{R}} \neq 1$, o que implica que $(b_1 \dots b_n)\Phi = b_1\Phi \dots b_n\Phi \neq 1$, e concluímos que $\mathcal{B}\Phi$ é uma base de $H \leq_{f.g.} F_A^{\mathcal{R}}$. Basta então mostrar que $\overline{b_1 \dots b_n}^{\mathcal{R}_A} \neq 1$. Seja $b_i = w_{p_i} a_i w_{q_i}^{-1}$ onde $a_i \in \widetilde{A}$ é o rótulo de uma aresta que não pertence a $\mathcal{T}$. Resulta facilmente de $b_i \neq b_{i-1}^{-1}$ e da definição de árvore geradora que

$$\overline{b_1 \dots b_n}^{\mathcal{R}_A} = w_{p_1} a_1 \overline{w_{q_1}^{-1} w_{p_2}}^{\mathcal{R}_A} a_2 \dots a_{n-1} \overline{w_{q_{n-1}}^{-1} w_{p_n}}^{\mathcal{R}_A} a_n w_{q_n}^{-1},$$

é uma palavra $\mathcal{R}_A$-reduzida e não vazia e concluímos a primeira parte da prova.

Vamos agora estudar a cardinalidade da base $\mathcal{B}$. Como $\mathcal{B} = \{w_p a w_q^{-1} \mid (p, a, q) \in E_A \setminus \mathcal{T}\}$, $|\mathcal{B}|$ é igual ao número de arestas de $\mathcal{T}^+$ com rótulo em A menos o número de arestas de $\mathcal{T}$ com rótulo em A. Ora, se $C \in Cay(\mathcal{S}_{\mathcal{R}} H)$ então, apenas $2(|Q(C)| - 1)$ de C vão continuar em $\mathcal{T}^+$ onde destas, apenas $|Q(C)| - 1$ têm rótulo em A. Portanto, o número de arestas de $\mathcal{T}^+$ com rótulo em A é igual a

$$|\{(p, a, q) \in E(\mathcal{S}_{\mathcal{R}} H) \mid a \in A_0\}| + \sum_{C \in Cay(\mathcal{S}_{\mathcal{R}} H)} (|Q(C)| - 1)$$

onde $|\{(p, a, q) \in E(\mathcal{S}_{\mathcal{R}} H) \mid a \in A_0\}|$ é o número de arestas de $\mathcal{S}_{\mathcal{R}} H$ com rótulo em A que não fazem parte de nenhum $C \in Cay(\mathcal{S}_{\mathcal{R}} H)$, isto é, o número de arestas de $\mathcal{S}_{\mathcal{R}} H$ com rótulo em A_0. Como contar uma aresta $(p, a, q) \in E(\mathcal{S}_{\mathcal{R}} H)$, onde $a \in A_0$, corresponde a contar um grau de $deg_{A_0}(p)$, temos que $|\{(p, a, q) \in E(\mathcal{S}_{\mathcal{R}} H) \mid a \in A_0\}| = \sum_{v \in Q(\mathcal{S}_{\mathcal{R}} H)} deg_{A_0}(v)$. Como $\mathcal{T}$ é uma árvore de $\mathcal{S}_{\mathcal{R}} H$, o número de arestas de $\mathcal{T}$ com

rótulo em A é igual a $|Q(\mathcal{S}_{\mathcal{R}}H)|-1$. Logo,

$$\begin{aligned}|\mathcal{B}| &= \left(\sum_{v\in Q(\mathcal{S}_{\mathcal{R}}H)} deg_{A_0}(v)\right)+\left(\sum_{C\in Cay(\mathcal{S}_{\mathcal{R}}H)}(|Q(C)|-1)\right)-|Q(\mathcal{S}_{\mathcal{R}}H)|+1\\ &= \left(\sum_{v\in Q(\mathcal{S}_{\mathcal{R}}H)} deg_{A_0}(v)-1\right)+\left(\sum_{C\in Cay(\mathcal{S}_{\mathcal{R}}H)}(|Q(C)|-1)\right)+1\\ &= \left(\sum_{v\in Q(\mathcal{S}_{\mathcal{R}}H)} deg_{A_0}(v)-1\right)+\left(\sum_{C\in Cay(\mathcal{S}_{\mathcal{R}}H)}|Q(C)|\right)-|Cay(\mathcal{S}_{\mathcal{R}}H)|+1.\end{aligned}$$

Agora basta observar que $\sum_{C\in Cay(\mathcal{S}_{\mathcal{R}}H)}|Q(C)|=\sum_{v\in Q(\mathcal{S}_{\mathcal{R}}H)}|Cay_v(\mathcal{S}_{\mathcal{R}}H)|$. Logo,

$$|\mathcal{B}|=\left(\sum_{v\in Q(\mathcal{S}_{\mathcal{R}}H)} deg_{A_0}(v)-1+|Cay_v(\mathcal{S}_{\mathcal{R}}H)|\right)-|Cay(\mathcal{S}_{\mathcal{R}}H)|+1$$

e concluímos a prova. □

Portanto, embora já se saiba que, para um dado $H\leq_{f.g.} F_A^{\mathcal{R}}$, H é livre se e só se é livre de torção, com os autómatos $\mathcal{S}_{\mathcal{R}}H$ conseguimos algo mais:

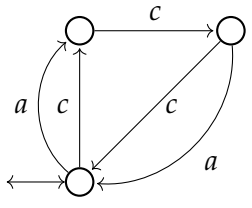
Corolário 8.1.9. *Seja $H\leq_{f.g.} F_A^{\mathcal{R}}$. Então é decidível se H é um grupo livre e, no caso em que é, conseguimos computar uma base de H.*

Demonstração. Resulta da Proposição 8.1.8 e do Corolário 8.1.6. □

Exemplo 8.1.10. *Suponhamos que,*

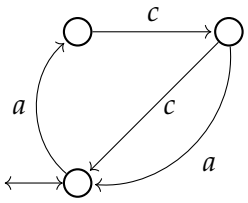
$$A_0=\{a,b\},\quad \mathcal{R}_0=\{(aa^{-1},1),(a^{-1}a,1),(bb^{-1},1),(b^{-1}b,1)\},$$
$$A_1=\{c\},\quad \mathcal{R}_1=\{(cc^{-1},1),(c^{-1}c,1),(c^3,1),(c^{-1},c^2)\}.$$

Então $F_A^{\mathcal{R}}$ é o produto livre do grupo livre de dimensão 2 com o grupo cíclico de ordem 3. Seja $H=\langle ac^2,aca,a^{-1}c\rangle$. Facilmente se verifica que $\mathcal{S}_{\mathcal{R}}H$ é dado por

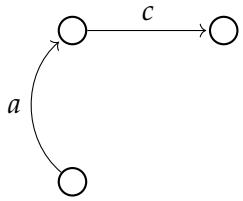


Então, pelas Proposições 8.1.5 e 8.1.8, sabemos que H é um grupo livre de dimensão

$2-3+3-1+1=2$. *Além disso, conseguimos computar uma base. Seguindo a demonstração da Proposição 8.1.8, um possível* $\mathcal{T}^+$ *é dado por*



e uma possível árvore geradora de $\mathcal{T}^+$ *é dada por*



Logo, uma possível base de H *é* $\{ac^2, aca\}$.

Definição 8.1.11. *Seja* $\mathcal{A}$ *um* $\mathcal{R}$*-SFG. Dizemos que* $\mathcal{A}$ *é* $\mathcal{R}$-livre *se* $Sch(\mathcal{A})\backslash Cay(\mathcal{A})=\emptyset$.

Note-se que, na demonstração da Proposição 8.1.8, mostramos mais do que aquilo que foi enunciado. Mostrou-se que se $\mathcal{A}$ é $\mathcal{R}$-livre, então existe um subconjunto finito $\mathcal{B}\subseteq\widetilde{A}^*$ tal que $\langle(L(\mathcal{A}))\Phi\rangle=\langle\mathcal{B}\Phi\rangle$ é o grupo livre de base $\mathcal{B}\Phi$, onde $\Phi:\widetilde{A}^*\to F_A^{\mathcal{R}}$ é o homomorfismo canónico. Note-se também que dado $S\subseteq\widetilde{A}^*$, $\overline{S\Phi}^{\mathcal{R}}=\overline{S}^{\mathcal{R}}$. Resulta então o seguinte corolário.

Corolário 8.1.12. *Seja* $\mathcal{A}$ $\mathcal{R}$*-livre. Então, existe* $H\leq_{f.g.}F_A^{\mathcal{R}}$ *tal que* $\mathcal{A}\simeq\mathcal{S}_{\mathcal{R}}H$.

Demonstração. Como $\mathcal{A}$ é $\mathcal{R}$-livre, existe $H\leq_{f.g.}F_A^{\mathcal{R}}$ tal que $\langle(L(\mathcal{A}))\Phi\rangle=H$. Ora, se $u,v\in L(\mathcal{A})$ então, como $L(\mathcal{A})$ é involutivo e tem um ponto base, $u^{-1},v^{-1},uv\in L(\mathcal{A})$. Logo, como Φ é um homomorfismo, $\langle(L(\mathcal{A}))\Phi\rangle=(L(\mathcal{A}))\Phi$. Portanto, $\overline{H}^{\mathcal{R}}=\overline{\langle(L(\mathcal{A}))\Phi\rangle}^{\mathcal{R}}=\overline{(L(\mathcal{A}))\Phi}^{\mathcal{R}}=\overline{L(\mathcal{A})}^{\mathcal{R}}$. Além disso, como $\mathcal{A}$ é um $\mathcal{R}$-SFG, $\overline{L(\mathcal{A})}^{\mathcal{R}}=L(\mathcal{A})\cap Irr(\mathcal{R})$. Logo,

$$L(\mathcal{A})\cap Irr(\mathcal{R})=\overline{H}^{\mathcal{R}}=L(\mathcal{S}_{\mathcal{R}}H)\cap Irr(\mathcal{R}).$$

Das Proposições 7.1.24 e 7.1.27, resulta que $\mathcal{A}\simeq\mathcal{S}_{\mathcal{R}}H$. □

Proposição 8.1.13. *Seja* $\mathcal{A}$ *um* $\mathcal{R}$*-SFG. Então* $\mathcal{A}\simeq\mathcal{S}_{\mathcal{R}}H$ *para algum* $H\leq_{f.g.}F_A^{\mathcal{R}}$.

Demonstração. Seja $F_A^{\mathcal{R}_A}$ o grupo livre gerado por A e π o seguinte homomorfismo de grupos sobrejetivo,

$$\pi\colon F_A^{\mathcal{R}_A} \longrightarrow F_A^{\mathcal{R}}$$
$$u/\sigma_{\mathcal{R}_A} \mapsto u/\sigma_{\mathcal{R}}$$

que está bem definido uma vez que $\mathcal{R}_A \subseteq \mathcal{R}$. Como $\mathcal{A}$ é um $\mathcal{R}$-SFG, $\mathcal{A}$ é um $\mathcal{R}_A$-SFG. Logo $\mathcal{A}$ é $\mathcal{R}_A$-livre e, pelo Corolário 8.1.12, é isomorfo a um $\mathcal{S}_{\mathcal{R}_A}H$ para algum $H \leq_{f.g.} F_A^{\mathcal{R}_A}$. Logo, $L(\mathcal{A}) \cap Irr(\mathcal{R}_A) = \overline{H}^{\mathcal{R}_A}$. Como $\mathcal{R}_A \subseteq \mathcal{R}$,

$$\overline{L(\mathcal{A}) \cap Irr(\mathcal{R}_A)}^{\mathcal{R}} = \overline{H}^{\mathcal{R}}.$$

Uma vez que $\mathcal{A}$ é $\mathcal{R}$-SFG,

$$\overline{L(\mathcal{A}) \cap Irr(\mathcal{R}_A)}^{\mathcal{R}} = L(\mathcal{A}) \cap Irr(\mathcal{R}).$$

Como $H \leq_{f.g.} F_A^{\mathcal{R}_A}$, temos que $H\pi \leq_{f.g.} F_A^{\mathcal{R}}$ e

$$L(\mathcal{S}_{\mathcal{R}}(H\pi)) \cap Irr(\mathcal{R}) = \overline{H\pi}^{\mathcal{R}} = \overline{H}^{\mathcal{R}}.$$

Logo, como $\mathcal{S}_{\mathcal{R}}(H\pi)$ e $\mathcal{A}$ são autómatos $\mathcal{R}$-SFG e $L(\mathcal{S}_{\mathcal{R}}(H\pi)) \cap Irr(\mathcal{R}) = L(\mathcal{A}) \cap Irr(\mathcal{R})$, pelas Proposições 7.1.24 e 7.1.27 resulta que $\mathcal{A} \simeq \mathcal{S}_{\mathcal{R}}(H\pi)$. □

A Proposição 8.1.13, diz-nos que a função Λ, apresentada no final do capítulo anterior, é também sobrejetiva, ou seja, existe uma correspondência bijetiva entre as classes de isomorfismo de autómatos $\mathcal{R}$-SFG e subgrupos finitamente gerados de $F_A^{\mathcal{R}}$.

Finalizamos esta secção mostrando que $F_A^{\mathcal{R}}$ satisfaz a *propriedade de Howson*: Um grupo G satisfaz a propriedade de Howson se a interseção de quaisquer dois subgrupos finitamente gerados de G é também um subgrupo finitamente gerado. É sabido que os grupos livres satisfazem esta propriedade tendo este resultado sido provado por Howson em 1954 [10]. Mais tarde, em 1966, Baumslag generalizou este resultado para o produto livre de grupos que satisfazem a propriedade de Howson [3] onde a demonstração teve por base a demonstração feita por Howson em [10]. Note-se que estes grupos estudados por Baumslag incluem os grupos singelos. Mais tarde, em 2002, com a aparecimento dos autómatos de Stallings, Kapovich provou propriedade de Howson para grupos livres através de uma abordagem combinatória e bastante mais simples [12] utilizando o produto direto de autómatos. Uma vez que neste trabalho conseguimos estabelecer uma correspondência entre os subgrupos finitamente gerados de um grupo singelo e as classes de

isomorfismo de autómatos $\mathcal{R}$-SFG, naturalmente surge a ideia de provar a propriedade de Howson pare estes grupos através do produto direto de autómatos.

Lema 8.1.14. *Seja G um grupo finito, $H_1, H_2 \leq G$ e X um conjunto gerador de G. Então, cada componente conexa de $Sch_X(G,H_1) \times Sch_X(G,H_2)$ é isomorfa a um $Sch_X(G,H_3)$ para algum $H_3 \leq G$.*

Demonstração. Seja $i \in \{1,2\}$, $g \in G$ e $\varphi_i : Q(Sch_X(G,H_i)) \to Q(Sch_X(G,g^{-1}H_ig))$ tal que $\varphi_i(H_iu) = (g^{-1}H_ig)g^{-1}u$ para todo o $u \in G$. Então φ_i é sobrejetiva e, se $(g^{-1}H_ig)g^{-1}u = (g^{-1}H_ig)g^{-1}v$ para alguns $u,v \in G$, então $g^{-1}uv^{-1}g \in g^{-1}H_ig$. Logo, $uv^{-1} \in H_i$, isto é, $H_iu = H_iv$. Logo, φ_i é injetiva. Além disso, dados $x \in \widetilde{X}$, $u,v \in G$, $(H_iu, x, H_iv) \in E(Sch_X(G,H_i)) \Leftrightarrow H_iv = H_iux \Leftrightarrow (g^{-1}H_ig)g^{-1}v = (g^{-1}H_ig)g^{-1}ux \Leftrightarrow (\varphi_i(H_iu), x, \varphi_i(H_iv)) \in E(Sch_X(G,g^{-1}H_ig))$. Logo φ_i induz um isomorfismo de grafos.

Seja $(p,q) \in Q(Sch_X(G,H_1) \times Sch_X(G,H_2))$ e considere-se a componente conexa K que o contém. Pela observação feita anteriormente, podemos supor que $(p,q) = (H_1,H_2)$. Vamos mostrar que $K \simeq Sch_X(G, H_1 \cap H_2)$. Note-se que, se $(H_1u, H_2v) \in Q(K)$ para alguns $u,v \in G$, então $(H_1u, H_2v) = (H_1w, H_2w)$ para algum $w \in G$ pois, como K é conexo por arcos, existe um caminho em K de (H_1,H_2) a (H_1u, H_2v) e $E(K) \subseteq E(Sch_X(G,H_1) \times Sch_X(G,H_2))$. Seja $\varphi : Q(K) \to Q(Sch_X(G, H_1 \cap H_2))$ tal que $\varphi((H_1u, H_2u)) = (H_1 \cap H_2)u$. Então, é fácil de ver que φ induz um isomorfismo de grafos. □

Proposição 8.1.15. *Sejam $H_1, H_2 \leq_{f.g.} F_A^{\mathcal{R}}$. Então $H_1 \cap H_2$ é finitamente gerado.*

Demonstração. Consideremos o autómato produto $\mathcal{S}_{\mathcal{R}}H_1 \times \mathcal{S}_{\mathcal{R}}H_2$. Seja $\mathcal{A}_0$ a componente conexa de $\mathcal{S}_{\mathcal{R}}H_1 \times \mathcal{S}_{\mathcal{R}}H_2$ que contém o ponto base e $\mathcal{A}$ o autómato obtido a partir de $\mathcal{A}_0$ apagando sucessivamente as arestas dos $K \in [Cay_{A_i}(F_{A_i}^{\mathcal{R}_i})]_{\mathcal{A}_0}$ que não são úteis relativamente a $\mathcal{R}$, onde $i \in \{1,\dots,\mathfrak{N}\}$, como também os vértices de grau inferior a dois distintos do ponto base. Então, juntamente com o Lema 8.1.14, podemos concluir que $\mathcal{A}$ é um $\mathcal{R}$-SFG. Logo, pela Proposição 8.1.13, $\mathcal{A} \simeq S_{\mathcal{R}}H$ para algum $H \leq_{f,g} F_A^{\mathcal{R}}$. Além disso,

$$L(\mathcal{S}_{\mathcal{R}}H_1 \times \mathcal{S}_{\mathcal{R}}H_2) \cap Irr(\mathcal{R}) = L(\mathcal{A}_0) \cap Irr(\mathcal{R}) = L(\mathcal{A}) \cap Irr(\mathcal{R}).$$

e, pela Proposição 3.3.4,

$$L(\mathcal{A}) \cap Irr(\mathcal{R}) = L(\mathcal{S}_{\mathcal{R}}H_1) \cap L(\mathcal{S}_{\mathcal{R}}H_2) \cap Irr(\mathcal{R}) = \overline{H_1}^{\mathcal{R}} \cap \overline{H_2}^{\mathcal{R}} = \overline{H_1 \cap H_2}^{\mathcal{R}}.$$

Logo, pela Proposição 7.1.20, podemos concluir que $\overline{H}^{\mathcal{R}} = \overline{H_1 \cap H_2}^{\mathcal{R}}$ e, portanto, $H_1 \cap H_2 = H \leq_{f.g.} F_A^{\mathcal{R}}$. □

8.2. Problema da conjugação

Nesta secção, vamos estudar o problema da conjugação em $F_A^{\mathcal{R}}$ e mostrar que é decidível. Embora os autómatos $\mathcal{R}$-SFG não sejam utilizados na resolução deste problema, esta parte do trabalho foi importante, não só para desenvolver intuição, como também ferramentas relativas ao problema que iremos abordar na próxima secção: o problema da conjugação generalizado.

Definição 8.2.1. *Seja $u \in Irr(\mathcal{R})$ e, caso $u \neq 1$, seja $u = u_1 \dots u_n$, $n \geq 1$, a sua decomposição em componentes homogéneas relativamente à partição $P = \{A_i\}_{i\in\{0,\dots,\mathfrak{N}\}}$. Dizemos que u é uma palavra* minimal por conjugação, *se $H[u] \leq 1$ ou se $H[u] \geq 2$ e u_1, u_n são palavras em alfabetos da partição P distintos, ou seja, se $u_1 \in \widetilde{A}_i^*$ para algum i, então $u_n \notin \widetilde{A}_i^*$.*

Definição 8.2.2. *Seja $u \in Irr(\mathcal{R})$ e, caso $u \neq 1$, seja $u = u_1 \dots u_n$, $n \geq 1$, a sua fatorização em componentes homogéneas relativamente à partição $\{A_i\}_{i\in\{0,\dots,\mathfrak{N}\}}$. Seja $^c : Irr(\mathcal{R}) \to Irr(\mathcal{R})$ o operador definido da seguinte forma*

$$u^c = \begin{cases} \overline{u_n u u_n^{-1}}^{\mathcal{R}}, & \text{se } u \neq 1 \\ 1, & \text{se } u = 1 \end{cases}$$

Dado $k \in \mathbb{N}$, usamos a notação u^{c^k} para representar a aplicação do operador ^{c}, k vezes à palavra u. Então, $u^{c^0} = u$.

No Exemplo 7.1.22, aplicando sucessivamente o operador ^{c} a $c^2babc \in Irr(\mathcal{R})$ obtemos o seguinte,

$$c^2babc \xrightarrow{c} bab \xrightarrow{c} b^2a \xrightarrow{c} ab^2 \xrightarrow{c} b^2a \xrightarrow{c} \dots$$

Note-se que c^2babc e bab não são minimais por conjugação mas b^2a e ab^2 são. Escrevemos agora algumas notas que, embora simples, serão usadas bastantes vezes nos próximos resultados.

Notas 8.2.3. *Seja $u \in Irr(\mathcal{R})$. Então,*

1. *u^c e u são conjugados em $F_A^{\mathcal{R}}$;*
2. *$u = 1$ se e só se $u^c = 1$;*
3. *Se u é minimal por conjugação, então também o é u^c;*

4. *Existe* $k \in \mathbb{N}$*, tal que* u^{c^k} *é minimal por conjugação;*

5. *Se* u *é minimal por conjugação,* $H[u] = H[u^{c^k}]$ *para todo* $k \in \mathbb{N}$*;*

6. *Se* u *é minimal por conjugação e* $H[u] = l$*,* $u^{c^l} = u$*.*

Lema 8.2.4. *Sejam* $u, v \in Irr(\mathcal{R})$ *conjugados em* $F_A^{\mathcal{R}}$ *tais que ambas as palavras* u *e* v *são minimais por conjugação e* $H[u] \geq 2$*. Então, existe* $k \leq H[u] - 1$ *tal que* $v = u^{c^k}$*.*

Demonstração. Ora, como u e v são conjugados, existe $w \in Irr(\mathcal{R})$ tal que $v = \overline{wuw^{-1}}^{\mathcal{R}}$. Vamos usar indução sobre $H[w]$. Se $H[w] = 0$, então $w = 1$ e $v = \overline{wuw^{-1}}^{\mathcal{R}} = \overline{u}^{\mathcal{R}} = u = u^{c^0}$. Suponhamos que o lema é válido quando $H[w] \leq n$, para um dado $n \in \mathbb{N}$ e suponhamos agora que $H[w] = n + 1$. Uma vez que $u \neq 1$ e $w \neq 1$, sejam $u_1 \dots u_m$ e $w_1 \dots w_{n+1}$ as fatorizações em componentes homogéneas de, respetivamente, u e w, onde $m \geq 1$.

Note-se que, se $\overline{w_{n+1}u_1}^{\mathcal{R}} \neq 1$ e $\overline{u_m w_{n+1}^{-1}}^{\mathcal{R}} \neq 1$ então, como $u, w \in Irr(\mathcal{R})$ e $H[u] \geq 2$, $\overline{wuw^{-1}}^{\mathcal{R}} = \overline{w_1 \dots w_{n+1}u_1 \dots u_m w_{n+1}^{-1} \dots w_1^{-1}}^{\mathcal{R}} = w_1 \dots \overline{w_{n+1}u_1}^{\mathcal{R}} \dots \overline{u_m w_{n+1}^{-1}}^{\mathcal{R}} \dots \overline{w_1^{-1}}^{\mathcal{R}}$ e $v = \overline{wuw^{-1}}^{\mathcal{R}}$ não seria minimal por conjugação. Logo, $\overline{w_{n+1}u_1}^{\mathcal{R}} = 1$ ou $\overline{u_m w_{n+1}^{-1}}^{\mathcal{R}} = 1$.

Suponhamos primeiro que $\overline{w_{n+1}u_1}^{\mathcal{R}} = 1$, ou seja, $w_{n+1} = \overline{u_1^{-1}}^{\mathcal{R}}$. Então $\overline{w_{n+1}uw_{n+1}^{-1}}^{\mathcal{R}} = \overline{u_1^{-1}uu_1}^{\mathcal{R}} = u^{c^{m-1}}$. Seja $w' = \overline{ww_{n+1}^{-1}}^{\mathcal{R}} \in Irr(\mathcal{R})$. Então $H[w'] = n < n + 1$. Além disso, temos que $\overline{w'w_{n+1}uw_{n+1}^{-1}(w')^{-1}}^{\mathcal{R}} = \overline{wuw^{-1}}^{\mathcal{R}}$ é minimal por conjugação, $H[\overline{w_{n+1}uw_{n+1}^{-1}}^{\mathcal{R}}] = H[u^{c^{m-1}}] = H[u] \geq 2$ e $\overline{w_{n+1}uw_{n+1}^{-1}}^{\mathcal{R}} = u^{c^{m-1}}$ é minimal por conjugação (Notas 8.2.3). Logo, por hipótese de indução, $\overline{wuw^{-1}}^{\mathcal{R}} = (\overline{w_{n+1}uw_{n+1}^{-1}}^{\mathcal{R}})^{c^k}$ para algum $k \in \mathbb{N}$. Como $\overline{w_{n+1}uw_{n+1}^{-1}}^{\mathcal{R}} = u^{c^{m-1}}$, resulta que $\overline{wuw^{-1}}^{\mathcal{R}} = (u^{c^{m-1}})^{c^k} = u^{c^{m-1+k}}$.

Suponhamos agora que $\overline{u_m w_{n+1}^{-1}}^{\mathcal{R}} = 1$. Então, $w_{n+1} = u_m$. Logo, $\overline{w_{n+1}uw_{n+1}^{-1}}^{\mathcal{R}} = u^c$. De forma análoga ao que foi feito anteriormente, usando a hipótese de indução, concluímos que $\overline{wuw^{-1}}^{\mathcal{R}} = (\overline{w_{n+1}uw_{n+1}^{-1}}^{\mathcal{R}})^{c^k}$ para algum $k \in \mathbb{N}$. Logo, $\overline{wuw^{-1}}^{\mathcal{R}} = (u^c)^{c^k} = u^{c^{k+1}}$.

Para terminar a demonstração, basta mostrar que, dada $s \in Irr(\mathcal{R})$ que é minimal por conjugação e tal que $H[s] \geq 2$, $|\{s^{c^k} : k \in \mathbb{N} \text{ e } s^{c^k} \neq s\}| \leq H[s] - 1$. Mas isso é claro. □

No Exemplo 7.1.22, $a^2c = \overline{ac^2(cacac^2)ca^{-1}}^{\mathcal{R}}$ e $cacac^2$ são conjugados mas $cacac^2 \neq (a^2c)^{c^k}$ para todo $k \in \mathbb{N}$. Portanto, no Lema 8.2.4, é necessário que u e v sejam minimais por conjugação.

Lema 8.2.5. *Sejam $u, v \in Irr(\mathcal{R})$ palavras minimais por conjugação. Então é decidível verificar se u e v são conjugadas em $F_A^{\mathcal{R}}$.*

Demonstração. Ora, se u e v são conjugadas, então uma das seguintes situações acontece:

1. $H[u] \geq 2$ e, pelo Lema 8.2.4, $v = u^{c^k}$, para algum $k \in \mathbb{N}$;
2. $H[v] \geq 2$ e, pelo Lema 8.2.4, $u = v^{c^k}$, para algum $k \in \mathbb{N}$;
3. $H[u] = H[v] = 1$ e u, v são conjugados em algum $F_{A_i}^{\mathcal{R}_i}$, para algum $i \in \{0, \ldots, \mathfrak{N}\}$;
4. $H[u] = H[v] = 0$ e $u = 1 = v$.

Note-se que é decidível verificar se as condições 1. ou 2. são ou não satisfeitas num número finito de passos. Ora, para todo o $i \in \{0, \ldots, \mathfrak{N}\}$, temos que $F_{A_i}^{\mathcal{R}_i}$ é um grupo finito ou um grupo livre. Pelo Corolário 6.1.3 e pela Proposição 6.1.7, sabemos que o problema da conjugação é decidível nestes grupos. Portanto, verificar 3. é também decidível. □

Exemplo 8.2.6. *Sejam,*

$$\begin{aligned} &A_1 = \{b\}, \quad A_2 = \{c\}, \\ &\mathcal{R}_1 = \{(bb^{-1}, 1),\ (b^{-1}b, 1),\ (b^2, 1),\ (b^{-1}, b)\}, \\ &\mathcal{R}_2 = \{(cc^{-1}, 1),\ (c^{-1}c, 1),\ (c^4, 1),\ (c^{-1}, c^3)\} \end{aligned}$$

e considere-se as seguintes palavras minimais por conjugação:

$$u_1 = bc^2bcbc^3,\ u_2 = bc^3bc^2bc,\ u_3 = bc^3bc^3bc,\ u_4 = bc^3bc^2bcbc.$$

Então, como $u_2 = (u_1)^{c^2}$, temos que u_1 e u_2 são conjugadas em $F_A^{\mathcal{R}}$. Como $H[u_4] > H[u_i]$ para todo o $i \in \{1, 2, 3\}$, u_4 não é conjugada de nenhuma das restantes palavras. Note-se que u_3 não tem nenhum fator da forma c^2. Logo u_3 também não é conjugada de nenhuma das restantes palavras.

Proposição 8.2.7. *O problema da conjugação é decidível em $F_A^{\mathcal{R}}$.*

Demonstração. Sejam $u, v \in F_A^{\mathcal{R}}$. Então, u e v são conjugados se e só se $\overline{u}^{\mathcal{R}}$ e $\overline{v}^{\mathcal{R}}$ são conjugados. Podemos então supor que $u, v \in Irr(\mathcal{R})$. Então, existem $k_u, k_v \in \mathbb{N}$ tais que $u^{c^{k_u}}, v^{c^{k_v}}$ são palavras minimais por conjugação (Notas 8.2.3). Além disso, u e $u^{c^{k_u}}$

são conjugados e v e $v^{c^{k_v}}$ são conjugados (Notas 8.2.3). Logo u e v são conjugados se e só se $u^{c^{k_u}}$ e $v^{c^{k_v}}$ o são. Basta agora aplicar o Lema 8.2.5. □

Exemplo 8.2.8. *Revisitando novamente o Exemplo 8.2.6, considerem-se $u, v \in F_A^{\mathcal{R}}$ tais que,*

$$u = bc^5bc^5bb^{-1}b^3cc^{-1},\ v = bc^2b^2.$$

Então $\overline{u}^{\mathcal{R}} = bcbcb$ e $\overline{v}^{\mathcal{R}} = bc^2$. Ora, $(\overline{u}^{\mathcal{R}})^{c^2} = (bcbcb)^{c^2} = (cbc)^c = c^2b$ e $\overline{v}^{\mathcal{R}} = bc^2$ são minimais por conjugação. Como $c^2b = (bc^2)^c$, podemos concluir que u e v são conjugados em $F_A^{\mathcal{R}}$.

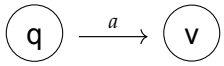
Observe-se que, para a demonstração da Proposição 8.2.7, as únicas propriedades de $F_A^{\mathcal{R}}$ usadas foram o facto de $F_A^{\mathcal{R}}$ ser um produto livre de grupos onde o problema da conjugação é decidível e que admitem uma *forma normalizada*, isto é, um conjunto de representantes canônicos para os elementos do grupo, escolhido de forma que qualquer elemento possa ser expresso de maneira única, sem ambiguidades. Logo, podemos concluir o seguinte:

Proposição 8.2.9. *Sejam $\{G_i\}_{\{i\in I\}}$ uma família finita de grupos onde o problema da conjugação é decidível e admitem uma forma normalizada. Então o problema da conjugação é decidível em $*_{\{i\in I\}}G_i$.*

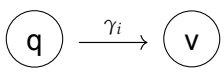
Podemos então questionar-nos se o problema da conjugação generalizado é decidível em $F_A^{\mathcal{R}}$, isto é, dados $H, G \leq_{f.g.} F_A^{\mathcal{R}}$, conseguimos decidir se H e G são conjugados em $F_A^{\mathcal{R}}$.

8.3. Problema da conjugação generalizado

Seja $\mathcal{A}$ um $\mathcal{R}$-autómato. Assim como usamos



para representar uma determinada aresta (q, a, v) de $\mathcal{A}$, usaremos



para representar um determinado $K \in [Cay_{A_i}(F_{A_i}^{\mathcal{R}_i})]_{\mathcal{A}}$, onde $i \in \{1, \ldots, \mathfrak{N}\}$, que tem exatamente dois vértices partilhados, sendo eles q e v. Note-se que a orientação da seta

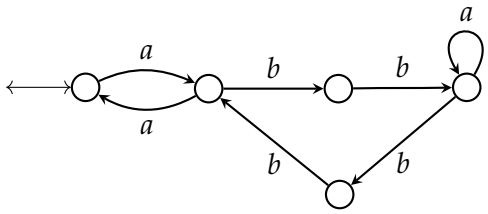
não tem qualquer importância nesta notação. No entanto, esta será útil na simplificação da escrita em algumas provas.

Embora a representação gráfica de $\mathcal{A}$ desta forma seja mais compacta, podemos perder informação da sua estrutura.

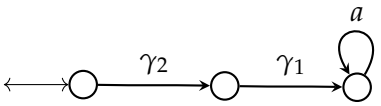
Exemplo 8.3.1. *Suponhamos que,*

$$A_1 = \{b\}, \quad \mathcal{R}_1 = \{(bb^{-1},1),\ (b^{-1}b,1),\ (b^4,1),\ (b^{-1},b^3)\},$$
$$A_2 = \{a\}, \quad \mathcal{R}_2 = \{(aa^{-1},1),\ (a^{-1}a,1),\ (a^2,1),\ (a^{-1},a)\}.$$

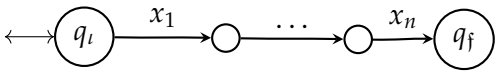
Considere-se o seguinte autómato $\mathcal{R}$-SFG:



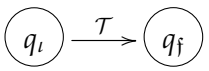
Então ficamos com a seguinte representação



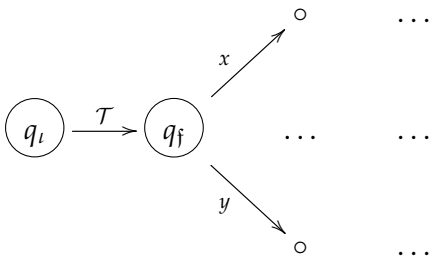
Dizemos que um $\mathcal{R}$-autómato da seguinte forma



onde $n \geq 1$, $x_i \in \{\gamma_1, \ldots, \gamma_\mathfrak{N}\} \cup \widetilde{A_0}$ para todo $i \in \{1, \ldots, n\}$ é uma *$\mathcal{R}$-cauda não trivial*. Note-se que, como é um autómato inverso, se $x_i, x_{i+1} \in \{\gamma_1, \ldots, \gamma_\mathfrak{N}\}$, então $x_i \neq x_{i+1}$ para todo $i \in \{1, \ldots, n-1\}$. A q_ι e a $q_\mathfrak{f}$ damos o nome de *ponto inicial* e *ponto final* da $\mathcal{R}$-cauda, respetivamente. A *$\mathcal{R}$-cauda trivial* é o $\mathcal{R}$-autómato trivial com um único vértice $q_\iota = q_\mathfrak{f}$, designado simultaneamente como ponto inicial e ponto final da cauda. Uma *$\mathcal{R}$-cauda* é uma $\mathcal{R}$-cauda não trivial ou trivial e representamos por



onde q_ι e $q_\mathfrak{f}$ são, respetivamente, o ponto inicial e o ponto final. Observe-se que, se $\mathcal{A}$ for um $\mathcal{R}$-SFG não trivial com ponto base q_ι, então $\mathcal{A}$ apresenta a seguinte forma

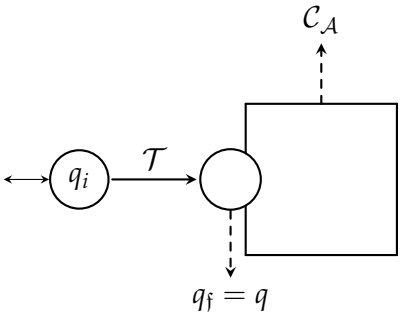


onde $x, y \in \widetilde{A}$ são letras distintas cujas respetivas arestas não estão contidas num mesmo $K \in Cay(\mathcal{A})$ com menos do que três vértices partilhados. Além disso, nenhuma dessas arestas faz parte da $\mathcal{R}$-cauda $q_\iota \xrightarrow{\mathcal{T}} q_\mathfrak{f}$. Dizemos também que $q_\iota \xrightarrow{\mathcal{T}} q_\mathfrak{f}$ é a *cauda* de $\mathcal{A}$. No caso em que $\mathcal{A}$ é o $\mathcal{R}$-SFG trivial, a sua cauda é a cauda trivial. Denominamos o grafo obtido a partir de $\Gamma_\mathcal{A}$ retirando a sua cauda, à exceção do vértice final $q_\mathfrak{f}$, por *cerne* de $\mathcal{A}$ e denotamos por $\mathcal{C}_\mathcal{A}$. Note-se que, se $\mathcal{A}$ tem cauda trivial, então $\mathcal{C}_\mathcal{A} = \Gamma_\mathcal{A}$. Note-se também que todo o vértice em $\mathcal{C}_\mathcal{A}$ tem grau superior a um, exceto no caso trivial. Se $\mathcal{C}_\mathcal{A} = (Q, E)$ e $q \in Q$, dizemos que o autómato $\mathfrak{R}_q(\mathcal{A}) = (Q, q, q, E)$ é a ***redução*** de $\mathcal{A}$ em q. Caso não se mencione qual o ponto base q, escrevemos apenas $\mathfrak{R}(\mathcal{A})$ e dizemos que é uma redução de $\mathcal{A}$. Se o autómato $\mathcal{A}$ estiver subentendido escrevemos apenas $\mathfrak{R}_q$ e $\mathfrak{R}$.

Seja $\mathcal{A}$ um $\mathcal{R}$-SFG não trivial, $\mathcal{C}_\mathcal{A} = (Q, E)$, $q \in Q$ e $\mathcal{T} = (Q', q_\iota, q_\iota, E')$ uma $\mathcal{R}$-cauda com vértice final $q_\mathfrak{f}$. Seja $\mathfrak{E}_{q,\mathcal{T}}(\mathcal{A})$ o autómato obtido a partir de $\mathcal{C}_\mathcal{A}$ e de $\mathcal{T}$ identificando $q_\mathfrak{f}$ com o vértice q de $\mathcal{C}_\mathcal{A}$, isto é, $\mathfrak{E}_{q,\mathcal{T}}(\mathcal{A}) = (Q'', q_\iota, q_\iota, E'')$ onde

$$Q'' = Q' \cup Q \backslash \{q\},$$

$$E'' = E' \cup \Big(E \cap (Q\backslash\{q\} \times \widetilde{A} \times Q\backslash\{q\})\Big) \cup \{(q_\mathfrak{f}, a, p), (p, a^{-1}, q_\mathfrak{f}) \mid a \in \widetilde{A} \text{ e } (q, a, p) \in E\}$$

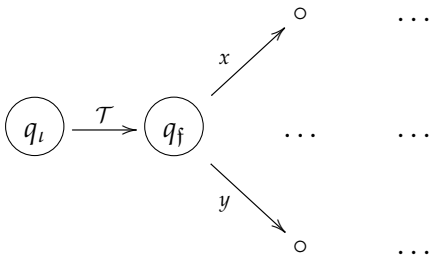


Se $\mathfrak{E}_{q,\mathcal{T}}(\mathcal{A})$ for determinístico, então dizemos que $\mathfrak{E}_{q,\mathcal{T}}(\mathcal{A})$ é a *extensão* de $\mathcal{A}$ em q por $\mathcal{T}$.

Caso não se mencione qual o ponto q e a cauda $\mathcal{T}$, escrevemos apenas $\mathfrak{E}(\mathcal{A})$ e dizemos que é uma extensão de $\mathcal{A}$. Se o autómato $\mathcal{A}$ estiver subentendido, escrevemos apenas $\mathfrak{E}_{q,\mathcal{T}}$ e $\mathfrak{E}$.

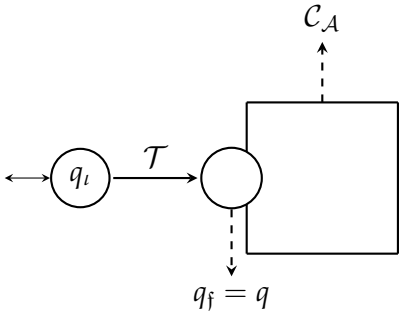
Proposição 8.3.2. *Seja $\mathcal{A}$ um $\mathcal{R}$-SFG não trivial. Qualquer redução ou extensão de $\mathcal{A}$ é também um $\mathcal{R}$-SFG.*

Demonstração. Seja $\mathfrak{R}_q$ uma redução de $\mathcal{A}$ para algum $q \in Q(\mathcal{C}_\mathcal{A})$. É claro que $\mathfrak{R}_q$ é inverso e tem um ponto base. Além disso, como $\mathcal{A}$ é um $\mathcal{R}$-SFG não trivial, todo o vértice em $\mathcal{C}_\mathcal{A}$ tem grau superior a um. Então, pelo Lema 7.1.9, podemos concluir que todo o vértice de $\mathfrak{R}_q$ ocorre num caminho bem sucedido com rótulo em $Irr(\mathcal{R}_A)$, isto é, $\mathfrak{R}_q$ satisfaz III da definição de $\mathcal{R}$-autómato. Ora, se uma dada aresta de $\mathcal{A}$ com rótulo em A_i, com $i \in \{1,\ldots,\mathfrak{N}\}$, não está em $\mathcal{C}_\mathcal{A}$ é porque está na cauda de $\mathcal{A}$. Mas então o respetivo $K \in Sch(\mathcal{A})$ onde ela está contida, está também na cauda de $\mathcal{A}$. Logo, como $\mathcal{A}$ é um $\mathcal{R}$-SFG, podemos concluir que $\mathcal{B}$ satisfaz IV da definição de $\mathcal{R}$-autómato, isto é, se $(p,a,p') \in E(\mathfrak{R}_q)$ é tal que $a \in A_i$, para algum $i \in \{1,\ldots,\mathfrak{N}\}$, então o vértice p está contido em algum $K \in Sch_i(\mathfrak{R}_\mathfrak{q})$. Logo, $\mathfrak{R}_q$ é um $\mathcal{R}$-autómato. Sabemos que $\mathcal{A}$ é da seguinte forma



onde $x,y \in \widetilde{A}$ são letras distintas cujas respetivas arestas não estão contidas num mesmo $K \in Cay(\mathcal{A})$ com menos do que três vértices partilhados e nenhuma delas faz parte da $\mathcal{R}$-cauda $q_\iota \xrightarrow{\mathcal{T}} q_\mathfrak{f}$. Pelo Lema 7.1.17, sabemos que todo o $K \in Cay(\mathcal{A})$ contém pelo menos dois vértices partilhados. Se $\mathcal{A}$ tiver cauda trivial, esta condição continua-se a verificar em $\mathfrak{R}_q$ uma vez que nenhuma aresta é eliminada. Caso contrário, o único caso que temos de estudar é se $K \in Cay(\mathfrak{R}_q)$ é tal que contém o ponto final da cauda de $\mathcal{A}$, $q_\mathfrak{f}$, uma vez que, $q_\mathfrak{f}$ é o único vértice de $\mathcal{A}$ que pode deixar de ser partilhado em $\mathfrak{R}_q$ (porque "baixa um grau de partilha"). Como x e y são letras distintas cujas respetivas arestas não estão contidas num mesmo $K' \in Cay(\mathcal{A})$ com menos do que três vértices partilhados, podemos concluir que K contém pelo menos dois vértices partilhados. Logo, este caso também não é um problema. Novamente pelo Lema 7.1.17, podemos finalmente concluir que $\mathfrak{R}_q$ é um $\mathcal{R}$-SFG.

Suponhamos agora que $\mathfrak{E}_{q,\mathcal{T}}$ é uma extensão de $\mathcal{A}$ para algum $q \in Q(\mathcal{C}_{\mathcal{A}})$ e alguma $\mathcal{R}$-cauda $q_\iota \xrightarrow{\mathcal{T}} q_\mathfrak{f}$ não trivial (se for trivial, estamos nos caso anterior). Por definição de extensão, $\mathfrak{E}_{q,\mathcal{T}}$ é determinístico e tem a seguinte forma



É claro que $\mathfrak{E}_{q,\mathcal{T}}$ é também involutivo e conexo, logo inverso, e tem um ponto base. Como $\mathcal{A}$ é um $\mathcal{R}$-SFG não trivial, todo o vértice em $\mathcal{C}_{\mathcal{A}}$ tem grau superior a um. Além disso, os únicos vértices que podem ter grau inferior a dois em $q_\iota \xrightarrow{\mathcal{T}} q_\mathfrak{f}$ são q_ι e $q_\mathfrak{f}$. Ora, como $q_\mathfrak{f}$ é identificado ao vértice q, o grau deste passará a ser superior a um e q_ι vai ser o ponto base de $\mathfrak{E}_{q,\mathcal{T}}$. Portanto, todo o vértice em $\mathfrak{E}_{q,\mathcal{T}}$ distinto do ponto base, q_ι, tem grau superior a um. Como a redução de $\mathcal{A}$, $\mathfrak{R}_q$, é um $\mathcal{R}$-SFG, sabemos que $\mathfrak{R}_q$ satisfaz IV da definição de $\mathcal{R}$-autómato. Note-se que esta condição também é satisfeita em $q_\iota \xrightarrow{\mathcal{T}} q_\mathfrak{f}$, logo $\mathfrak{E}_{q,\mathcal{T}}$ é um $\mathcal{R}$-autómato. Sabemos também que todo o $K \in Cay(\mathfrak{R}_q)$ contém pelo menos dois vértices partilhados. Note-se que a única maneira de existir um $K \in Cay(\mathcal{T})$ que não tem pelo menos dois vértices partilhados, é se este contém o vértice $q_\mathfrak{f}$. Neste caso, como $\mathfrak{E}_{q,\mathcal{T}}$ é determinístico e $\mathcal{C}_{\mathcal{A}}$ é não trivial, o vértice $q_\mathfrak{f}$ passa a ser partilhado em $\mathfrak{E}_{q,\mathcal{T}}$. Logo, podemos concluir que $\mathfrak{E}_{q,\mathcal{T}}$ é um $\mathcal{R}$-SFG. □

Vamos agora mostrar que as reduções e extensões de um determinado $\mathcal{S}_{\mathcal{R}}H$ não trivial, onde $H \leq_{f.g.} F_A^{\mathcal{R}}$ não é trivial, representam subgrupos conjugados de H.

Lema 8.3.3. *Sejam $H \leq_{f.g.} F_A^{\mathcal{R}}$, $q \in Q(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})$ e $\mathfrak{R}_q$ a redução de $\mathcal{S}_{\mathcal{R}}H$ em q. Se q_ι é o ponto base de $\mathcal{S}_{\mathcal{R}}H$ e $q_\iota \xrightarrow{w} q$ é um caminho em $\mathcal{S}_{\mathcal{R}}H$ para algum $w \in \widetilde{A}^*$, então $\mathfrak{R}_q \simeq \mathcal{S}_{\mathcal{R}}(w^{-1}Hw)$.*

Demonstração. O caso em que H é o subgrupo trivial é claro. Suponhamos então que H é não trivial. Temos que

$$u \in L(\mathfrak{R}_q) \Leftrightarrow wuw^{-1} \in L(\mathcal{S}_{\mathcal{R}}H). \tag{8.1}$$

Logo, como $\mathfrak{R}_q$ é também um $\mathcal{R}$-SFG (Proposição 8.3.2), $w^{-1}uw \in L(\mathfrak{R}_q) \Rightarrow u \in L(\mathcal{S}_{\mathcal{R}}H)$. Além disso, como $ww^{-1} \in L(\mathcal{S}_{\mathcal{R}}H)$, temos que, dada $u \in L(\mathcal{S}_{\mathcal{R}}H)$, $ww^{-1}uww^{-1} \in L(\mathcal{S}_{\mathcal{R}}H)$. Logo, por 8.1, $w^{-1}uw \in L(\mathfrak{R}_q)$ e

$$w^{-1}uw \in L(\mathfrak{R}_q) \Leftrightarrow u \in L(\mathcal{S}_{\mathcal{R}}H). \tag{8.2}$$

Portanto, usando 8.1 (para $\Rightarrow$) e 8.2 (para $\Leftarrow$),

$$\overline{w^{-1}uw}^{\mathcal{R}} \in L(\mathfrak{R}_q) \cap Irr(\mathcal{R}) \Leftrightarrow \overline{u}^{\mathcal{R}} \in L(\mathcal{S}_{\mathcal{R}}H) \cap Irr(\mathcal{R}). \tag{8.3}$$

Seja $H' = w^{-1}Hw$. Pela Proposição 7.1.20, sabemos que $L(\mathcal{S}_{\mathcal{R}}H') \cap Irr(\mathcal{R}) = \overline{H'}^{\mathcal{R}}$. Então,

$$\overline{H'}^{\mathcal{R}} = \{\overline{w^{-1}uw}^{\mathcal{R}} \mid u \in H\} = \{\overline{w^{-1}\overline{u}^{\mathcal{R}}w}^{\mathcal{R}} \mid \overline{u}^{\mathcal{R}} \in \overline{H}^{\mathcal{R}}\} =$$

$$= \{\overline{w^{-1}\overline{u}^{\mathcal{R}}w}^{\mathcal{R}} \mid \overline{u}^{\mathcal{R}} \in L(\mathcal{S}_{\mathcal{R}}H) \cap Irr(\mathcal{R})\} = L(\mathfrak{R}_q) \cap Irr(\mathcal{R})$$

onde na última igualdade foi usado 8.3. Como $L(\mathcal{S}_{\mathcal{R}}H') \cap Irr(\mathcal{R}) = L(\mathfrak{R}_q) \cap Irr(\mathcal{R})$, pelas Proposições 7.1.24 e 7.1.27, podemos concluir que $\mathfrak{R}_q \simeq \mathcal{S}_{\mathcal{R}}H'$. □

Lema 8.3.4. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ não trivial. Se $\mathfrak{E}$ é uma extensão de $\mathcal{S}_{\mathcal{R}}H$, então existe $w \in F_A^{\mathcal{R}}$ tal que $\mathfrak{E} \simeq \mathcal{S}_{\mathcal{R}}(w^{-1}Hw)$.*

Demonstração. Como $\mathfrak{E}$ é um $\mathcal{R}$-SFG (Proposição 8.3.2), pela Proposição 8.1.13, sabemos que existe um $K \leq_{f.g.} F_A^{\mathcal{R}}$ tal que $\mathfrak{E} \simeq \mathcal{S}_{\mathcal{R}}K$. Pelo Lema 8.3.3, se $q_{\mathfrak{f}}$ for o ponto final da cauda de $\mathfrak{E}$ e $\mathfrak{R}_{q_{\mathfrak{f}}}$ a redução de $\mathfrak{E}$ em $q_{\mathfrak{f}}$, sabemos que $\mathfrak{R}_{q_{\mathfrak{f}}} \simeq \mathcal{S}_{\mathcal{R}}(u^{-1}Ku)$ para algum $u \in F_A^{\mathcal{R}}$. Mas $\mathfrak{R}_{q_{\mathfrak{f}}}$ é também uma redução de $\mathcal{S}_{\mathcal{R}}H$, logo, pelo Lema 8.3.3, $\mathfrak{R}_{q_{\mathfrak{f}}} \simeq \mathcal{S}_{\mathcal{R}}(v^{-1}Hv)$ para algum $v \in F_A^{\mathcal{R}}$ e $\mathcal{S}_{\mathcal{R}}(u^{-1}Ku) \simeq \mathcal{S}_{\mathcal{R}}(v^{-1}Hv)$, isto é, $\overline{u^{-1}Ku}^{\mathcal{R}} = \overline{v^{-1}Hv}^{\mathcal{R}}$. Logo $\mathfrak{E} \simeq \mathcal{S}_{\mathcal{R}}(uv^{-1}Hvu^{-1})$. Tomamos $w = vu^{-1}$. □

Proposição 8.3.5. *Sejam H, K subgrupos finitamente gerados de $F_A^{\mathcal{R}}$. Então H e K são conjugados se e só se $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H} \simeq \mathcal{C}_{\mathcal{S}_{\mathcal{R}}K}$.*

Demonstração. O caso em que H ou K é trivial é claro. Suponhamos então que H e K não são triviais. Pelo Lema 8.3.3, conseguimos sempre através de uma conjugação de H, obter um grupo H' cujo respetivo $\mathcal{S}_{\mathcal{R}}H'$ é uma redução $\mathfrak{R}_q$ de $\mathcal{S}_{\mathcal{R}}H$ para algum $q \in Q(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})$. Note-se também que $\mathcal{S}_{\mathcal{R}}H'$ tem de ter cauda trivial, caso contrário, o vértice q ou não teria grau superior a um em $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$, ou estaria contido num $K \in Cay(\mathcal{S}_{\mathcal{R}}H)$ que não é útil relativamente a $\mathcal{R}$. Além disso, $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H} \simeq \mathcal{C}_{\mathcal{S}_{\mathcal{R}}H'}$.

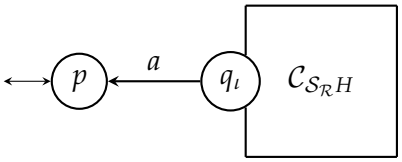
Vamos agora mostrar que H e K são conjugados se e só se $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H} \simeq \mathcal{C}_{\mathcal{S}_{\mathcal{R}}K}$.

$[\Leftarrow]$ Suponhamos que $\varphi : Q(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}) \to Q(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}K})$ induz um isomorfismo de grafos e seja $q \in Q(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})$. Então φ induz também um isomorfismo entre $\mathfrak{R}_q(\mathcal{S}_{\mathcal{R}}H))$ e $\mathfrak{R}_{\varphi(q)}(\mathcal{S}_{\mathcal{R}}K)$. Uma vez que a relação "ser conjugado" é uma relação de equivalência, pelo Lema 8.3.3, podemos concluir que H e K são conjugados.

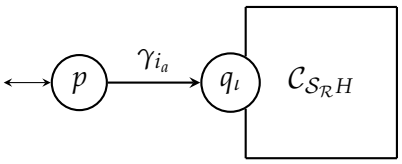
$[\Rightarrow]$ Para mostrar a implicação reciproca, basta mostrar para o caso em que K é a conjugação de H por uma letra. Seja então $a \in \widetilde{A_{i_a}}$ para algum $i_a \in \{0, \ldots, \mathfrak{N}\}$ tal que $K = a^{-1}Ha$. Pela observação feita anteriormente, podemos reduzir o estudo ao caso em que $\mathcal{S}_{\mathcal{R}}H$ tem cauda trivial. Seja q_ι o ponto base de $\mathcal{S}_{\mathcal{R}}H$. Então, como $\mathcal{S}_{\mathcal{R}}H$ tem cauda trivial e H não é trivial, $deg(q_\iota) \geq 2$.

Suponhamos que existe um vértice q de $\mathcal{S}_{\mathcal{R}}H$ tal que $q_\iota \xrightarrow{a} q$ é uma aresta de $\mathcal{S}_{\mathcal{R}}H$. Seja $\mathfrak{R}_q$ a redução de $\mathcal{S}_{\mathcal{R}}H$ em q. Então $\mathfrak{R}_q$ é um $\mathcal{R}$-SFG e, pelo Lema 8.3.3, $\mathfrak{R}_q \simeq \mathcal{S}_{\mathcal{R}}(a^{-1}Ha)$. Logo, $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}K} \simeq \mathcal{C}_{\mathfrak{R}_q} \simeq \mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$.

Suponhamos então que não existe um vértice q de $\mathcal{S}_{\mathcal{R}}H$ tal que $q_\iota \xrightarrow{a} q$ é uma aresta de $\mathcal{S}_{\mathcal{R}}H$. No caso em que $i_a = 0$, seja $\mathfrak{E}$ a seguinte extensão de $\mathcal{S}_{\mathcal{R}}H$



Note-se que $\mathfrak{E}$ é, de facto, determinístico e, portanto, uma extensão. Logo, $\mathfrak{E}$ é um $\mathcal{R}$-SFG. Note-se que, se $i_a \in \{1, \ldots, \mathfrak{N}\}$, então não pode existir $x \in \widetilde{A_{i_a}}$ e um vértice q de $\mathcal{S}_{\mathcal{R}}H$ tal que $q_\iota \xrightarrow{x} q$ é uma aresta de $\mathcal{S}_{\mathcal{R}}H$. Caso contrário, como $\mathcal{S}_{\mathcal{R}}H$ é um $\mathcal{R}$-SFG, o vértice q_ι teria que pertencer a algum $K \in Sch_{i_a}(\mathcal{S}_{\mathcal{R}}H)$. Logo, como $a \in \widetilde{A_{i_a}}$ e K é $\widetilde{A_{i_a}}$-completo, isto implicaria a existência de uma aresta $q_\iota \xrightarrow{a} q'$ em $\mathcal{S}_{\mathcal{R}}H$ para algum vértice q'. No caso em que $i_a \in \{1, \ldots, \mathfrak{N}\}$, seja $\mathfrak{E}$ a extensão de $\mathcal{S}_{\mathcal{R}}H$ obtida colando ao vértice q_ι o grafo $Cay_{A_{i_a}}(F_{A_{i_a}}^{\mathcal{R}_{i_a}})$ e tomando como ponto base o vértice p de $Cay_{A_{i_a}}(F_{A_{i_a}}^{\mathcal{R}_{i_a}})$ tal que $p \xrightarrow{a^{-1}} q_\iota$ é uma aresta de $\mathfrak{E}$,



Portanto, neste caso, $\mathfrak{E}$ é também uma extensão de $\mathcal{S}_{\mathcal{R}}H$ e, consequentemente, um $\mathcal{R}$-SFG. Ora, em ambos os casos temos as seguintes igualdades

$$L(\mathfrak{E}) \cap Irr(\mathcal{R}) = \overline{L(\mathfrak{E})}^{\mathcal{R}} = \overline{a^{-1}Ha}^{\mathcal{R}} = L(\mathcal{S}_{\mathcal{R}}(a^{-1}Ha)) \cap Irr(\mathcal{R})$$

onde na primeira e na última igualdade foi usada a Proposição 7.1.20. Vamos então explicar a igualdade do meio: No primeiro caso ($i_a = 0$), em que $p \xleftarrow[a]{} q_\iota$ é a cauda de $\mathfrak{E}$, é claro. No segundo caso ($i_a \geq 1$), em que a cauda de $\mathfrak{E}$ é $p \xrightarrow{\gamma_{i_a}} q_\iota$, a inclusão $\overline{L(\mathfrak{E})}^{\mathcal{R}} \supseteq \overline{a^{-1}Ha}^{\mathcal{R}}$ é também clara. Para a inclusão oposta, basta observar que se $p \xrightarrow{u} p$ é um caminho bem sucedido em $\mathfrak{E}$, $u = vwz$ com $v, z \in \widetilde{A_{i_a}}^*$ e $w \in L(\mathcal{S}_{\mathcal{R}}H)$

$$p \xrightarrow{v} q_\iota \xrightarrow{w} q_\iota \xrightarrow{z} p \ .$$

Como $p \xrightarrow{a^{-1}} q_\iota$ e $p \xrightarrow{v} q_\iota$ são caminhos em $Cay_{A_{i_a}}(F^{\mathcal{R}_{i_a}}_{A_{i_a}})$, podemos concluir que $\overline{v}^{\mathcal{R}} = \overline{a^{-1}}^{\mathrm{R}}$. Analogamente, como $q_\iota \xrightarrow{a} p$ e $q_\iota \xrightarrow{z} p$ são caminhos em $Cay_{A_{i_a}}(F^{\mathcal{R}_{i_a}}_{A_{i_a}})$, podemos concluir que $\overline{z}^{\mathcal{R}} = \overline{a}^{\mathcal{R}}$. Logo $\overline{u}^{\mathcal{R}} = \overline{a^{-1}wa}^{\mathcal{R}} \in \overline{a^{-1}Ha}^{\mathcal{R}}$ e concluímos a igualdade.

Logo, como $L(\mathfrak{E}) \cap Irr(\mathcal{R}) = L(\mathcal{S}_{\mathcal{R}}(a^{-1}Ha)) \cap Irr(\mathcal{R})$, podemos concluir que $\mathfrak{E} \simeq \mathcal{S}_{\mathcal{R}}(a^{-1}Ha)$. Então, $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}K} \simeq \mathcal{C}_{\mathfrak{E}} \simeq \mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$. □

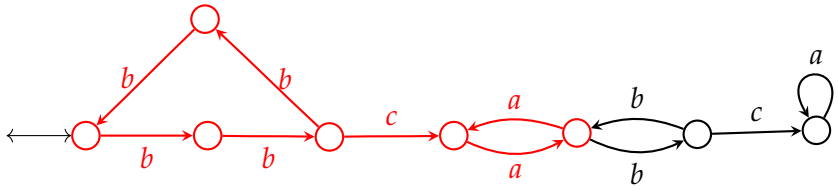
Corolário 8.3.6. *Existe um algoritmo que decide se dois subgrupos finitamente gerados de $F^{\mathcal{R}}_A$ são conjugados.*

Este resultado já era conhecido. Isto deriva do facto de a decidibilidade deste problema ter sido já provada para grupos virtualmente livres finitamente gerados (veja-se por exemplo [15]). No entanto, para o caso dos grupos singelos, a Proposição 8.3.5 diz-nos como responder a este problema de uma forma altamente eficaz e elegante usando a apenas a estrutura dos autómatos $\mathcal{R}$-SFG.

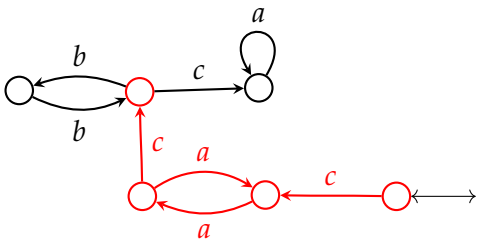
Exemplo 8.3.7. *Suponhamos que,*

$$\begin{aligned}
A_0 &= \{c\}, \quad \mathcal{R}_0 = \{(cc^{-1}, 1),\ (c^{-1}c, 1)\},\\
A_1 &= \{a\}, \quad \mathcal{R}_1 = \{(aa^{-1}, 1),\ (a^{-1}a, 1),\ (a^2, 1),\ (a^{-1}, a)\},\\
A_2 &= \{b\}, \quad \mathcal{R}_2 = \{(bb^{-1}, 1),\ (b^{-1}b, 1),\ (b^4, 1),\ (b^{-1}, b^3)\}.
\end{aligned}$$

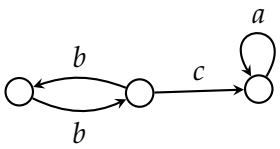
Sejam H, K subgrupos finitamente gerados de $F^{\mathcal{R}}_A$. Sejam $\mathcal{S}_{\mathcal{R}}H$ e $\mathcal{S}_{\mathcal{R}}K$, respetivamente, dados por



e



onde as respetivas caudas estão pintadas a vermelho. Como os respetivos $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ *e* $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}K}$ *são isomorfos a*



podemos concluir que H *e* K *são conjugados.*

8.4. O normalizador

Na demonstração da Proposição 8.3.5 vimos que qualquer autómato $\mathcal{S}_{\mathcal{R}}K$, onde K é um conjugado de $H \leqslant_{f.g.} F_A^{\mathcal{R}}$, é uma redução ou uma extensão de $\mathcal{S}_{\mathcal{R}}H$. Uma vez que os subgrupos normais são aqueles que são invariantes por conjugação, faz sentido questionar se somos capazes de, através da estrutura de $\mathcal{S}_{\mathcal{R}}H$, decidir se H é um subgrupo normal ou não.

Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ não trivial. Note- se que, como numa extensão a colagem da cauda tem de manter o autómato determinístico, as extensões só podem ser realizadas se $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ não for um $\widetilde{A}$-grafo completo. Portanto, se $\mathcal{S}_{\mathcal{R}}H$ é um autómato $\widetilde{A}$-completo, então $\mathcal{S}_{\mathcal{R}}H$ tem cauda trivial.

Proposição 8.4.1. *Seja* $H \leq_{f.g.} F_A^{\mathcal{R}}$ *não trivial. Então* H *é normal se e só se* $\mathcal{S}_{\mathcal{R}}H$ *é um* $\widetilde{A}$*-autómato completo e transitivo nos vértices.*

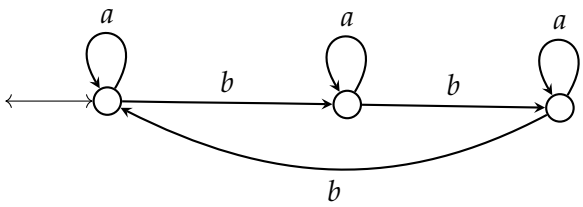
Demonstração. Se $H \trianglelefteq F_A^{\mathcal{R}}$, $aHa^{-1} = H$, em $F_A^{\mathcal{R}}$, para todo o $a \in \widetilde{A}$, isto é, $\mathcal{S}_{\mathcal{R}}H \simeq \mathcal{S}_{\mathcal{R}}(aHa^{-1})$. Logo, qualquer redução ou extensão de $\mathcal{S}_{\mathcal{R}}H$ é isomorfa a $\mathcal{S}_{\mathcal{R}}H$. Portanto, $\mathcal{S}_{\mathcal{R}}H$ tem de ter cauda trivial e não pode existir a possibilidade de deixar de ser trivial. Então tem de ser $\widetilde{A}$-completo. Então, a condição de ter cauda trivial e de não existir a possibilidade de deixar de ser trivial equivale a dizer que $\mathcal{S}_{\mathcal{R}}H$ tem de ser $\widetilde{A}$-completo. Além disso, é necessário que a escolha do ponto base não altere o autómato. Logo $\mathcal{S}_{\mathcal{R}}H$ tem de ser transitivo nos vértices. Reciprocamente, se $\mathcal{S}_{\mathcal{R}}H$ estiver nestas condições, H é normal. □

Exemplo 8.4.2. *Suponhamos que,*

$$A_1 = \{a\}, \mathcal{R}_1 = \{(aa^{-1}, 1), (a^{-1}a, 1), (a^2, 1), (a^{-1}, a)\},$$

$$A_2 = \{b\}, \mathcal{R}_2 = \{(bb^{-1}, 1), (b^{-1}b, 1), (b^3, 1), (b^{-1}, b^2)\}.$$

Se $H \leq_{f.g.} F_{A_1}^{\mathcal{R}_1} * F_{A_2}^{\mathcal{R}_2} \simeq \mathbb{Z}_2 * \mathbb{Z}_3$ *é tal que* $\mathcal{S}_{\mathcal{R}}H$ *é dado por*



então, como $\mathcal{S}_{\mathcal{R}}H$ *é completo e transitivo nos vértices, podemos concluir que* $H \trianglelefteq F_{A_1}^{\mathcal{R}_1} * F_{A_2}^{\mathcal{R}_2}$.

Na Proposição 8.4.1, vimos uma correspondência bijetiva entre os subgrupos finitamente gerados, não triviais, de $F_A^{\mathcal{R}}$ que são normais e as classes de isomorfismo dos autómatos $\mathcal{S}_{\mathcal{R}}H$ que são completos e transitivos nos vértices. E se relaxarmos uma das condições dos $\mathcal{S}_{\mathcal{R}}H$? Ou seja, será que conseguimos classificar algebricamente os subgrupos $H \leq_{f.g.} F_A^{\mathcal{R}}$ para os quais $\mathcal{S}_{\mathcal{R}}H$ é apenas completo, ou apenas transitivo nos vértices? Os próximos resultados respondem afirmativamente aos dois casos.

Proposição 8.4.3. *Seja* $H \leq_{f.g.} F_A^{\mathcal{R}}$ *não trivial. Então* $[F_A^{\mathcal{R}} : H] < \infty$ *se e só se* $\mathcal{S}_{\mathcal{R}}H$ *é um autómato completo.*

Demonstração. $[\Rightarrow]$ Suponhamos que $\mathcal{S}_{\mathcal{R}}H$ não é completo. Então, através de uma redução ou uma extensão de $\mathcal{S}_{\mathcal{R}}H$, sabemos que existe um subgrupo H' conjugado de H, tal que $\mathcal{S}_{\mathcal{R}}H'$ não é completo no seu ponto base q_ι, no sentido em que existe $a \in \widetilde{A}$

tal que $q_\iota \xrightarrow{a} \circ$ não ocorre em $\mathcal{S}_\mathcal{R}H'$. Suponhamos que $a \in \widetilde{A_0}$ e $n, m \in \mathbb{N}$ são tais que $n \leq m$. Então,

$$H'a^m = H'a^n \Leftrightarrow a^{m-n} \in H' \Leftrightarrow \overline{a^{m-n}}^R = a^{m-n} \in L(\mathcal{S}_\mathcal{R}H').$$

Logo $H'a^m = H'a^n$ se e só se $m = n$. Se $a \in \widetilde{A_i}$ para algum $i \in \{1, \ldots, \mathfrak{N}\}$, então q_ι não é vértice de nenhum $K \in Sch_i(\mathcal{S}_\mathcal{R}H')$. Note-se que, dada a definição de $\mathcal{R}$, $\overline{a}^\mathcal{R} \neq 1$. Como H' é não trivial e $\mathcal{S}_\mathcal{R}H'$ é um $\mathcal{R}$-autómato, existe um $u \in Irr(\mathcal{R})\backslash\{1\}$ tal que $[u), (u] \notin \widetilde{A_i}$ e $q_\iota \xrightarrow{u} q_\iota$ ocorre em $\mathcal{S}_\mathcal{R}H'$. Mas então, $\overline{(au)^m}^\mathcal{R} = (\overline{a}^\mathcal{R}u)^m$ para todo o $m \in \mathbb{N}$. Logo, $H'(au)^m \neq H'(au)^n$ sempre que $n, m \in \mathbb{N}$ são distintos. Logo, em qualquer um dos casos, $[F_A^\mathcal{R} : H']$ é infinito. Portanto, como H e H' são conjugados, $[F_A^\mathcal{R} : H]$ também é infinito.

$[\Leftarrow]$ Suponhamos que $\mathcal{S}_\mathcal{R}H$ é completo com ponto base q_ι. Para cada $q \in Q(\mathcal{S}_\mathcal{R}H)$, seja $q_\iota \xrightarrow{u_q} q$ um caminho em $\mathcal{S}_\mathcal{R}H$ com $u_q \in Irr(\mathcal{R})$. Vamos ver que $F_A^\mathcal{R} = \cup_{q \in Q(\mathcal{S}_\mathcal{R}H)} Hu_q$. Seja $u \in \widetilde{A}^*$. Como $\mathcal{S}_\mathcal{R}H$ é completo, existe em $\mathcal{S}_\mathcal{R}H$ um caminho da forma $q_\iota \xrightarrow{u} q$ para algum $q \in Q$. Logo $uu_q^{-1} \in L(\mathcal{S}_\mathcal{R}H)$. Mas então, $uu_q^{-1} \in H$ e $u \in Hu_q$. □

Corolário 8.4.4. *Todo o subgrupo, não trivial, finitamente gerado e normal de um grupo singelo tem índice finito.*

Demonstração. Resulta das Proposições 8.4.1 e 8.4.3. □

Note-se que este resultado, em geral, não é verdade para grupos virtualmente livres finitamente gerados. Voltando ao exemplo $\mathbb{Z} \times \mathbb{Z}_2$, temos que $\{0\} \times \mathbb{Z}_2$ é normal ($\mathbb{Z} \times \mathbb{Z}_2$ é abeliano) e é finitamente gerado mas não tem índice finito.

Corolário 8.4.5. *Seja $H \leq_{f.g.} F_A^\mathcal{R}$ não trivial. Se $[F_A^\mathcal{R} : H] < \infty$, então é igual ao número de vértices de $\mathcal{S}_\mathcal{R}H$.*

Demonstração. Suponhamos que q_ι é o ponto base de $\mathcal{S}_\mathcal{R}H$. Na demonstração da Proposição 8.4.3 vimos que $F_A^\mathcal{R} = \cup_{q \in Q(\mathcal{S}_\mathcal{R}H)} Hu_q$. Basta então mostrar que, dados $p, q \in Q(\mathcal{S}_\mathcal{R}H)$, $p \neq q \Rightarrow Hu_p \neq Hu_q$. Suponhamos que $Hu_p = Hu_q$. Então $Hu_pu_q^{-1} = H$ e $u_pu_q^{-1} \in H$. Logo $\overline{u_pu_q^{-1}}^\mathcal{R} \in L(\mathcal{S}_\mathcal{R}H)$. Logo, o caminho $q_\iota \xrightarrow{\overline{u_pu_q^{-1}}^\mathcal{R} u_q} q$ ocorre em $\mathcal{S}_\mathcal{R}H$. Mas então $q_\iota \xrightarrow{\overline{\overline{u_pu_q^{-1}}^\mathcal{R} u_q}^\mathcal{R}} q$ também ocorre em $\mathcal{S}_\mathcal{R}H$. Como $\overline{\overline{u_pu_q^{-1}}^\mathcal{R} u_q}^\mathcal{R} = u_p$ e $\mathcal{S}_\mathcal{R}H$ é determinístico, $p = q$. □

O grupo apresentado no Exemplo 8.4.2, $\mathbb{Z}_2 * \mathbb{Z}_3$, conhecido como grupo modular, desempenha um papel fundamental em várias áreas da Matemática, incluindo a geometria e a teoria dos números. O interesse pelos seus subgrupos, especialmente os de índice finito, remonta ao século XIX, e a investigação sobre estas estruturas mantém-se bastante ativa na matemática contemporânea. Normalmente, na literatura é usada a notação Γ para o grupo modular e Γ^n para o subgrupo de Γ gerado por $\{g^n : g \in \Gamma\}$. Em 1962, M. Newman mostrou que Γ^2 é o produto livre de dois grupos cíclicos de ordem três (de índice dois) e que Γ^3 é o produto livre de três grupos cíclicos de ordem dois (de índice três) [22]. Pouco tempo depois, M. Newman conclui em [23] o seguinte teorema:

Teorema 8.4.6. *Seja H um subgrupo não trivial normal de Γ distinto de Γ, Γ^2 e Γ^3. Então H é livre.*

Neste mesmo artigo, é dada uma prova alternativa do seguinte teorema provado por R. C. Gunning em [9].

Teorema 8.4.7. *Seja H um subgrupo não trivial normal de Γ distinto de Γ, Γ^2 e Γ^3. Se H tem índice finito, então $[\Gamma : H]$ é divisível por seis.*

Mais tarde, em 2004, Müller e Schlage-Puchta mostraram que, se p_1 e p_2 são números primos, e $H \leq \mathbb{Z}_{p_1} * \mathbb{Z}_{p_2}$ é normal, tem índice finito e não é livre, então $[\mathbb{Z}_{p_1} * \mathbb{Z}_{p_2} : H] \in \{1, p_1, p_2\}$ [21]. Vejamos agora que, através dos autómatos $\mathcal{R}$-SFG, conseguimos generalizar estes resultados de uma forma bastante simples.

Proposição 8.4.8. *Sejam p_1, p_2 números primos. Então $\mathbb{Z}_{p_1} * \mathbb{Z}_{p_2}$ tem exatamente três subgrupos finitamente gerados não triviais que são normais e não são livres: um com índice 1, outro com índice p_1 e outro com índice p_2. Além disso, estes subgrupos são computáveis.*

Demonstração. Sejam

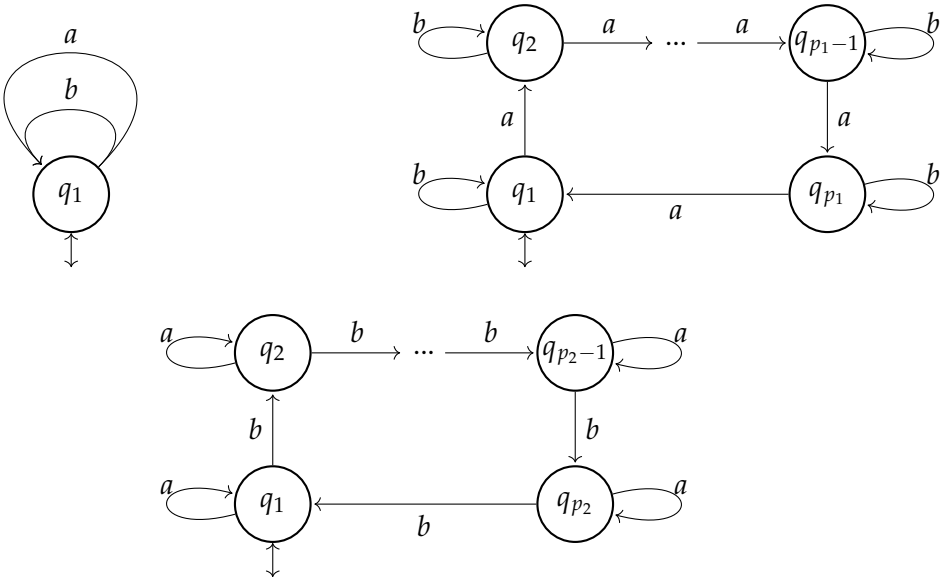
$$A_1 = \{a\}, \mathcal{R}_1 = \{(aa^{-1}, 1), (a^{-1}a, 1), (a^{p_1}, 1), (a^{-1}, a^{p_1-1})\},$$

$$A_2 = \{b\}, \mathcal{R}_2 = \{(bb^{-1}, 1), (b^{-1}b, 1), (b^{p_2}, 1), (b^{-1}, b^{p_2-1})\}.$$

Então $\mathbb{Z}_{p_1} * \mathbb{Z}_{p_2} \simeq F_A^{\mathcal{R}}$. Suponhamos que $H \leq_{f.g.} F_A^{\mathcal{R}}$ é um subgrupo não trivial, normal e que não é livre. Então pela Proposição 8.1.8, H tem torção não trivial e, pela Proposição 8.1.5, $Sch(\mathcal{S}_{\mathcal{R}}H) \backslash Cay(\mathcal{S}_{\mathcal{R}}H) \neq \emptyset$. Além disso, como p_1 e p_2 são primos, se $K \in Sch(\mathcal{S}_{\mathcal{R}}H) \backslash Cay(\mathcal{S}_{\mathcal{R}}H)$, K é isomorfo a um dos seguintes grafos:



Como H é normal, pela Proposição 8.4.1, $\mathcal{S}_{\mathcal{R}}H$ tem de ser transitivo nos vértices e tem de ser completo. Logo, como $\mathcal{S}_{\mathcal{R}}H$ é um $\mathcal{R}$-SFG, facilmente se conclui que $\mathcal{S}_{\mathcal{R}}H$, tem de ser isomorfo a um dos seguintes autómatos:



Agora, basta notar que, pelos Corolários 8.4.4 e 8.4.5, os subgrupos que estes $\mathcal{R}$-$SFG's$ representam têm, respetivamente, índices 1, p_1 e p_2. □

Proposição 8.4.9. *Sejam $n \geq 1$ e G_i, $i \in \{1,\ldots,n\}$, grupos finitos. Suponhamos que $H \leq_{f.g.} *_{i=1}^{n} G_i$ é um subgrupo livre de índice finito. Então,*

$$[*_{i=1}^{n} G_i : H] \equiv 0 \pmod{mmc(|G_1|,\ldots,|G_n|)}$$

onde $mmc(|G_1|,\ldots,|G_n|)$ é o mínimo múltiplo comum de $|G_1|,\ldots,|G_n|$.

Demonstração. Para cada $i \in \{1,\ldots,n\}$ sejam A_i um alfabeto finito e $\mathcal{R}_i$ um sistema de reescrita finito NCI para os quais $G_i \simeq F_{A_i}^{\mathcal{R}_i}$. Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ um subgrupo livre e de índice finito. Se H é trivial, como tem índice finito, necessariamente $n = 1$ e $[G_1 : H] = |G_1|$. Suponhamos então que H é não trivial. Como H tem índice finito, pela Proposição 8.4.3 e pelo Corolário 8.4.5, $[F_A^{\mathcal{R}} : H] = |Q(\mathcal{S}_{\mathcal{R}}H)|$ e $\mathcal{S}_{\mathcal{R}}H$ é completo. Além disso, pelas Proposições 8.1.5 e 8.1.8, como H é livre, $Sch(\mathcal{S}_{\mathcal{R}}H)\backslash Cay(\mathcal{S}_{\mathcal{R}}H) = \emptyset$. Uma vez que $\mathcal{S}_{\mathcal{R}}H$ é determinístico e completo, podemos concluir que, para todo o $i \in \{1,\ldots,n\}$, todo o vértice tem de estar contido em exatamente um $K_i \in Cay_i(\mathcal{S}_{\mathcal{R}}H)$ com $|Q(K_i)| = |G_i|$. Logo, para todo o $i \in \{1,\ldots,n\}$, $[F_A^{\mathcal{R}} : H] = |Q(\mathcal{S}_{\mathcal{R}}H)|$ é divisível por $|G_i|$. □

Seja G um grupo qualquer. Dado $H \leq_{f.g.} G$. Denotamos por $N(H)$ o seu *normalizador*, isto é,

$$N(H) = \{u \in G \ : \ u^{-1}Hu = H\}.$$

Relembre-se que $N(H)$ é o maior subgrupo de G onde H é normal e que, se $H = u^{-1}Ku$, para algum $u \in G$ e $K \leq G$, então $N(H) = u^{-1}N(K)u$. De forma a simplificar a notação, definimos, para todo o $i \geq 1$, $N^i(H) = N(N^{i-1}(H))$ sendo $N^0(H) = H$. Temos então a seguinte *cadeia de normalizadores* gerada por H,

$$H \trianglelefteq N^1(H) \trianglelefteq N^2(H) \trianglelefteq ...$$

e dizemos que esta cadeia *estabiliza* se existir $i \in \mathbb{N}$ tal que $N^i(H) = N^j(H)$ para todo o $j \geq i$. Nesta situação, dizemos que $N^i(H)$ é o *estabilizador* da cadeia e representamos por $N^*(H)$.

Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$. Se $H = \langle A' \rangle$ onde $A' = \left(\cup_{i \in \mathcal{I}} A_i \right) \cup A'_0$, para alguns $\mathcal{I} \subseteq \{1, \ldots, \mathfrak{N}\}$ e $A'_0 \subseteq A_0$, então dizemos que H é um *fator* de $F_A^{\mathcal{R}}$.

Proposição 8.4.10. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$. Então $\mathcal{S}_{\mathcal{R}}H$ é transitivo nos vértices se e só se $N(H)$ é um fator de $F_A^{\mathcal{R}}$.*

Demonstração. O caso em que H é trivial é claro. Suponhamos então que H não é trivial.

[$\Leftarrow$] Suponhamos que existem $\mathcal{I} \subseteq \{1, \ldots, \mathfrak{N}\}$ e $A'_0 \subseteq A_0$ tal que $N(H) = \langle A' \rangle \leq F_A^{\mathcal{R}}$ onde $A' = \left(\cup_{i \in \mathcal{I}} A_i \right) \cup A'_0$. Seja $\mathcal{R}' = \bigcup_{i \in \mathcal{I}} \mathcal{R}_i \cup \mathcal{R}_{A'_0}$. Através das identificações usuais $\langle A' \rangle \simeq \overline{\langle A' \rangle}^{\mathcal{R}} = \overline{\langle A' \rangle}^{\mathcal{R}'} \simeq F_{A'}^{\mathcal{R}'}$, podemos pensar em H como um subgrupo normal de $F_{A'}^{\mathcal{R}'}$, isto é, $H \trianglelefteq_{f.g.} F_{A'}^{\mathcal{R}'}$ e, pela Proposição 5.1.3, sabemos que $F_{A'}^{\mathcal{R}'}$ é o produto livre $*_{i \in \mathcal{I}} F_{A_i}^{\mathcal{R}_i} * F_{A'_0}^{\mathcal{R}_{A'_0}}$. Como $H \leq_{f.g.} F_A^{\mathcal{R}}$, temos que $H \leq_{f.g.} F_{A'}^{\mathcal{R}'}$ e, portanto, podemos construir $\mathcal{S}_{\mathcal{R}'}H$ que é um $\mathcal{R}'$-SFG. Como H é subgrupo normal de $F_{A'}^{\mathcal{R}'}$, pela Proposição 8.4.1, sabemos que $\mathcal{S}_{\mathcal{R}'}H$ é um autómato $\widetilde{A'}$-completo e transitivo nos vértices. Ora, de facto, $\mathcal{S}_{\mathcal{R}'}H$ é também um $\mathcal{R}$-SFG: como $\mathcal{S}_{\mathcal{R}'}H$ é um $\mathcal{R}'$-SFG e não contém nenhuma aresta com rótulo em $A \backslash A'$, podemos concluir que é um $\mathcal{R}$-autómato, isto é, satisfaz I, II, III e IV da Definição 7.1.7. Basta agora observar que $Irr(\mathcal{R}') \subseteq Irr(\mathcal{R})$ e, portanto, todo o $K \in Cay(\mathcal{S}_{\mathcal{R}'}H)$ que é $\mathcal{R}'$-útil, é também útil relativamente a $\mathcal{R}$. Logo, $\mathcal{S}_{\mathcal{R}'}H$ é um $\mathcal{R}$-SFG. Como $L(\mathcal{S}_{\mathcal{R}'}H) \cap Irr(\mathcal{R}) = L(\mathcal{S}_{\mathcal{R}'}H) \cap Irr(\mathcal{R}') = \overline{H}^{\mathcal{R}'} = \overline{H}^{\mathcal{R}} = L(\mathcal{S}_{\mathcal{R}}H) \cap Irr(\mathcal{R})$ e $\mathcal{S}_{\mathcal{R}'}H$ é um $\mathcal{R}$-SFG, podemos concluir que $\mathcal{S}_{\mathcal{R}'}H \simeq \mathcal{S}_{\mathcal{R}}H$. Logo, $\mathcal{S}_{\mathcal{R}}H$ é transitivo nos vértices.

$[\Rightarrow]$ Suponhamos que $\mathcal{S}_{\mathcal{R}}H$ é transitivo nos vértices. Então se $a \in A$ é rótulo de uma aresta em $\mathcal{S}_{\mathcal{R}}H$, podemos concluir que para todo o $q \in Q(\mathcal{S}_{\mathcal{R}}H)$, existe $q_a \in Q(\mathcal{S}_{\mathcal{R}}H)$ tal que $(q, a, q_a) \in E(\mathcal{S}_{\mathcal{R}}H)$. Seja $A' = \{a \in A \mid \text{existem } p, q \in Q(\mathcal{S}_{\mathcal{R}}H) \text{ tais que } (p, a, q) \in E(\mathcal{S}_{\mathcal{R}}H)\}$. Seja $i \in \{1, \ldots, \mathfrak{N}\}$ e $a \in A_i \cap A'$. Então, existem $q, q_a \in Q(\mathcal{S}_{\mathcal{R}}H)$ tais que $(q, a, q_a) \in E(\mathcal{S}_{\mathcal{R}}H)$ e, uma vez que $\mathcal{S}_{\mathcal{R}}H$ é um $\mathcal{R}$-SFG, o vértice q está contido em algum $K \in Sch_i(\mathcal{S}_{\mathcal{R}}H)$. Como K é um grafo $\widetilde{A_i}$-completo, podemos concluir que $A_i \subseteq A'$. Logo, existe $\mathcal{I} \subseteq \{1, \ldots, \mathfrak{N}\}$ e $A'_0 \subseteq A_0$ tal que $A' = \bigcup_{i \in \mathcal{I}} A_i \cup A'_0$. Ora, como $\overline{H}^{\mathcal{R}} = L(\mathcal{S}_{\mathcal{R}}H) \cap Irr(\mathcal{R})$ e $L(\mathcal{S}_{\mathcal{R}}H) \subseteq \widetilde{A'}^*$, temos que $H \leq \langle A' \rangle$. Como já observado, podemos identificar $\langle A' \rangle$ com $F_{A'}^{\mathcal{R}'}$ onde $\mathcal{R}' = \left(\cup_{i \in \mathcal{I}} \mathcal{R}_i \right) \cup \mathcal{R}_{A'_0}$. Como $\mathcal{R}' \subseteq \mathcal{R}$ e $\mathcal{S}_{\mathcal{R}}H$ é um $\mathcal{R}$-SFG em $\widetilde{A'}$, temos que $\mathcal{S}_{\mathcal{R}}H$ é um $\mathcal{R}'$-SFG. Além disso $\mathcal{S}_{\mathcal{R}}H$ é $\widetilde{A'}$-completo e transitivo nos vértices. Logo, pela Proposição 8.4.1, $H \trianglelefteq F_{A'}^{\mathcal{R}'} = \langle A' \rangle$. Podemos então concluir que $\langle A' \rangle \subseteq N(H)$. Se $\overline{\widetilde{A}^*}^{\mathcal{R}} \setminus \overline{\widetilde{A'}^*}^{\mathcal{R}} = \emptyset$, então $\langle A \rangle = \langle A' \rangle$ e $H \trianglelefteq F_A^{\mathcal{R}}$. Caso contrário, seja $u \in \overline{\widetilde{A}^*}^{\mathcal{R}} \setminus \overline{\widetilde{A'}^*}^{\mathcal{R}}$. Note-se que $u \neq 1$ pois $1 \in \overline{\widetilde{A'}^*}^{\mathcal{R}}$. Seja $w \in \overline{H}^{\mathcal{R}}$ tal que $\overline{w}^{\mathcal{R}} \neq 1$ (note-se que w existe porque H não é trivial). Então, $\overline{uwu^{-1}}^{\mathcal{R}} = uw\overline{u^{-1}}^{\mathcal{R}} \notin \overline{H}^{\mathcal{R}} \subseteq \widetilde{A'}^*$. Logo $\langle A' \rangle = N(H)$. □

Corolário 8.4.11. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$. Se $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ é transitivo nos vértices, então $N(H)$ é conjugado de um fator de $F_A^{\mathcal{R}}$.*

Demonstração. O caso em que H é trivial é claro. Suponhamos então que H é não trivial e seja $q \in Q(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})$. Seja $\mathfrak{R}_q$ a redução de $\mathcal{S}_{\mathcal{R}}H$ em q. Pelo Lema 8.3.3, sabemos que existe $M \leq_{f.g.} F_A^{\mathcal{R}}$ que é um subgrupo conjugado de H e $\mathcal{S}_{\mathcal{R}}M \simeq \mathfrak{R}_q$. Então, se $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ é transitivo nos vértices, $\mathfrak{R}_q$ e $\mathcal{S}_{\mathcal{R}}M$ também são. Logo, pela Proposição 8.4.10, sabemos que $N(M)$ é um fator de $F_A^{\mathcal{R}}$ e, portanto, $N(H)$ é conjugado de um fator de $F_A^{\mathcal{R}}$. □

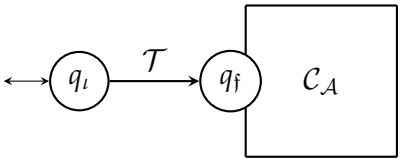
Seja $\mathcal{A}$ um $\mathcal{R}$-SFG. Relembre-se o autómato quociente $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$ apresentado na Secção 3.2. Note-se que $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$ continua a ser um $\widetilde{A}$-autómato com um ponto base, involutivo e conexo. Na verdade, temos o seguinte resultado:

Proposição 8.4.12. *Seja $\mathcal{A}$ um autómato $\mathcal{R}$-SFG. Então $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$ é um autómato $\mathcal{R}$-SFG.*

Demonstração. Para verificar que $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$ é inverso, falta só verificar o determinismo. Sejam $Orb(q)$, $Orb(p)$ e $Orb(d)$ vértices de $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$ e $a \in \widetilde{A}$ tais que que $(Orb(q), a, Orb(p))$ e $(Orb(q), a, Orb(d))$ são arestas de $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$. Sejam $q_1, q_2, p', d' \in Q(\mathcal{A})$ tais que $q_1, q_2 \in Orb(q)$, $p' \in Orb(p)$, $d' \in Orb(d)$ e $(q_1, a, p'), (q_2, a, d') \in E(\mathcal{A})$. Seja $\varphi \in Aut(\Gamma_{\mathcal{A}})$ tal que $q_1\varphi = q_2$. Então, $(q_2, a, p'\varphi) = (q_1\varphi, a, p'\varphi) \in E(\mathcal{A})$. Pelo determinismo de $\mathcal{A}$, concluímos que $p'\varphi = d'$, isto é, $Orb(p) = Orb(d)$. Logo $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$ é

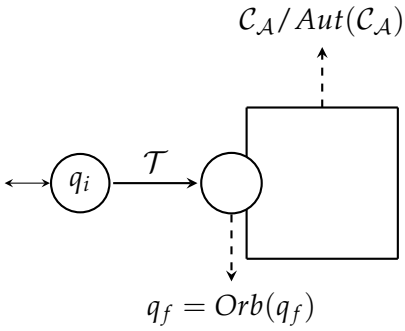
determinístico e as condições I e II da definição de $\mathcal{R}$-autómato são satisfeitas. Como na passagem ao quociente, o grau dos vértices pode, quanto muito, aumentar, pelo Lema 7.1.9, podemos concluir que III também se verifica. Seja $(Orb(q), a, Orb(p))$ uma aresta de $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$ onde $a \in A_i$ para algum $i \in \{1, \ldots, \mathfrak{N}\}$. Então, existem $q' \in Orb(q)$ e $p' \in Orb(p)$ tais que $(q, a, p) \in E(\mathcal{A})$. Como $\mathcal{A}$ é um $\mathcal{R}$-SFG, existe $K \in Sch_i(\mathcal{A})$ tal que (q', a, p') é uma aresta de K. Como na passagem ao quociente alguns vértices de K são identificados e K é, por sua vez, um quociente de um grafo em $[Cay_{A_i}(F_{A_i}^{\mathcal{R}_i})]_{\mathcal{F}_{\mathcal{R}}X}$ para algum subconjunto gerador X de $\overline{H}^{\mathcal{R}}$, pela Proposição 7.1.2, podemos concluir que IV é também satisfeita em $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$. Logo, $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$ é um $\mathcal{R}$-autómato. Para terminar, falta verificar que todo o $K \in Cay(\mathcal{A}/Aut(\Gamma_{\mathcal{A}}))$ é útil relativamente a $\mathcal{R}$. Pela Proposição 7.1.17, isto também é claro uma vez que, na passagem para o quociente, o número de vértices partilhados em cada $K \in Cay(\mathcal{A}/Aut(\Gamma_{\mathcal{A}}))$, quanto muito aumenta. □

Seja $\mathcal{A}$ um $\mathcal{R}$-SFG não trivial com cauda $\mathcal{T}$ e onde q_ι, q_f são, respetivamente, o ponto inicial e o ponto final de $\mathcal{T}$.



Definimos o *autómato normalizador* de $\mathcal{A}$, $N(\mathcal{A})$, como sendo

$$N(\mathcal{A}) = \mathfrak{E}_{Orb(q_\mathfrak{f}),\mathcal{T}}\left(\mathfrak{R}_{q_\mathfrak{f}}(\mathcal{A})/Aut(\Gamma_{\mathfrak{R}_{q_\mathfrak{f}}(\mathcal{A})})\right)$$

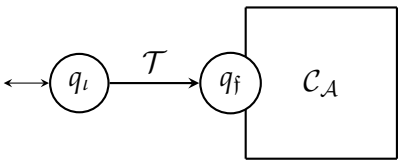


Note-se que, pela Proposição 8.3.2, $\mathfrak{R}_{q_\mathfrak{f}}(\mathcal{A})$ é um $\mathcal{R}$-SFG e, pela Proposição 8.4.12, $\mathfrak{R}_{q_\mathfrak{f}}(\mathcal{A})/Aut(\Gamma_{\mathfrak{R}_{q_\mathfrak{f}}(\mathcal{A})})$ é também um $\mathcal{R}$-SFG. Portanto, para vermos que $N(\mathcal{A})$ é uma extensão de $\mathfrak{R}_{q_\mathfrak{f}}(\mathcal{A})/Aut(\Gamma_{\mathfrak{R}_{q_\mathfrak{f}}(\mathcal{A})})$, temos só de ver que $N(\mathcal{A})$ é determinístico. Para tal, vamos usar o seguinte lema:

Lema 8.4.13. *Seja $\mathcal{A} = (Q, E)$ um $\widetilde{A}$-grafo e $(Orb(p), a, Orb(q))$ uma aresta de $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$. Então, existe um $t \in Orb(q)$ tal que $(p, a, t) \in E$.*

Demonstração. Como $(Orb(p), a, Orb(q))$ é uma aresta de $\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$, existem $p' \in Orb(p), q' \in Orb(q)$ tais que (p', a, q') é uma aresta de $\mathcal{A}$. Suponhamos que φ é o automorfismo que envia p' em p. Então temos que $(p, a, q'\varphi) \in E(\mathcal{A})$ e $q'\varphi \in Orb(q)$. Basta tomar $t = q'\varphi$. □

Ora, se a cauda $\mathcal{T}$ for trivial, então é claro que $N(\mathcal{A})$ é determinístico. Caso contrário, como $\mathcal{T}$ e $\mathfrak{R}_{q_f}(\mathcal{A})/Aut(\Gamma_{\mathfrak{R}_{q_f}(\mathcal{A})})$ são determinísticos, temos só de verificar o determinismo de $N(\mathcal{A})$ em $Orb(q_f)$. Pelo Lema 8.4.13, se $(Orb(q_f), a, Orb(q))$ é uma aresta de $\mathcal{C}_{\mathcal{A}}/Aut(\mathcal{C}_{\mathcal{A}})$, existe um vértice de $\mathcal{C}_{\mathcal{A}}$, q', tal que (q_f, a, q') é uma aresta em $\mathcal{C}_{\mathcal{A}}$. Então, uma vez que $\mathcal{A}$ é determinístico e da seguinte forma



podemos concluir que o autómato $N(\mathcal{A})$ também é determinístico. Portanto, $N(\mathcal{A})$ é uma extensão. Resulta então o seguinte:

Corolário 8.4.14. *Seja $\mathcal{A}$ um $\mathcal{R}$-SFG não trivial. Então $N(\mathcal{A})$ é um $\mathcal{R}$-SFG.*

Proposição 8.4.15. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ não trivial. Então $N(H)$ é finitamente gerado e $\mathcal{S}_{\mathcal{R}}N(H) \simeq N(\mathcal{S}_{\mathcal{R}}H)$.*

Demonstração. Como H é não trivial, o vértice base de $\mathcal{S}_{\mathcal{R}}H$ tem pelo menos grau um. Se, adicionalmente, $\mathcal{S}_{\mathcal{R}}H$ tiver cauda trivial, então o vértice base tem pelo menos grau dois. Suponhamos primeiro que $\mathcal{S}_{\mathcal{R}}H$ tem cauda trivial. Vamos mostrar que

$$L(\mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})) \cap Irr(\mathcal{R}) = \overline{N(H)}^{\mathcal{R}}.$$

$[\subseteq]$ Seja $u = a_1 \dots a_n \in L(\mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})) \cap Irr(\mathcal{R})$ onde $a_i \in \widetilde{A}$ e q_ι é o ponto base de $\mathcal{S}_{\mathcal{R}}H$. Então,

$$Orb(q_\iota) \xrightarrow{u} Orb(q_\iota)$$

ocorre em $\mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})$. Logo, existem $n+1$ vértices de $\mathcal{S}_{\mathcal{R}}H$, $q_i \in Q(\mathcal{S}_{\mathcal{R}}H)$ com $i \in \{0, \dots, n\}$ tais que

$$Orb(q_\iota) = Orb(q_0) \xrightarrow{a_1} Orb(q_1) \xrightarrow{\cdots} Orb(q_{n-1}) \xrightarrow{a_n} Orb(q_n) = Orb(q_\iota)$$

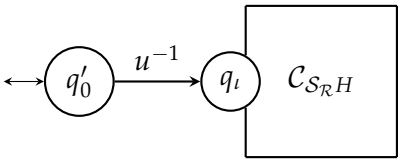
ocorre em $\mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})$. Logo, para todo $i \in \{1,\dots,n\}$, existem $q'_{i-1} \in Orb(q_{i-1})$ e $q'_i \in Orb(q_i)$ tais que $(q'_{i-1}, a_i, q'_i) \in E(\mathcal{S}_{\mathcal{R}}H)$. Então, pelo Lema 8.4.13, para todo o $i \in \{1,\dots,n\}$ e $p \in Orb(q_{i-1})$, existe $q \in Orb(q_i)$ tal que $(p, a_i, q) \in E$. Logo, existe um caminho

$$q_\iota \xrightarrow{u} q$$

em $\mathcal{S}_{\mathcal{R}}H$ para algum $q \in Orb(q_\iota)$.

Seja $\mathfrak{R}_q$ a redução de $\mathcal{S}_{\mathcal{R}}H$ em q. Então, pelo Lema 8.3.3, podemos concluir que $\mathfrak{R}_q$ é um $\mathcal{R}$-SFG e $\mathcal{S}_{\mathcal{R}}(u^{-1}Hu) \simeq \mathfrak{R}_q$. Além disso, $q \in Orb(q_\iota)$, logo $L(\mathfrak{R}_q) = L(\mathcal{S}_{\mathcal{R}}H)$. Portanto, $\overline{H}^{\mathcal{R}} = \overline{\overline{u^{-1}Hu}^{\mathcal{R}}}$, isto é $u \in \overline{N(H)}^{\mathcal{R}}$.

$[\supseteq]$ Seja $u \in \overline{N(H)}^{\mathcal{R}}$. Então $\overline{\overline{u^{-1}Hu}^{\mathcal{R}}} = \overline{H}^{\mathcal{R}}$ e, consequentemente, $\mathcal{S}_{\mathcal{R}}H \simeq \mathcal{S}_{\mathcal{R}}(u^{-1}Hu)$. Suponhamos que $u^{-1} = a_0 \dots a_n$ para $a_i \in \widetilde{A}$. Sejam $q'_0,\dots,q'_n \notin Q(\mathcal{S}_{\mathcal{R}}H)$ e $\mathcal{A}_0 = (Q(\mathcal{S}_{\mathcal{R}}H) \cup \{q'_0,\dots,q'_n\}, q'_0, q'_0, E')$ onde $E' = E(\mathcal{S}_{\mathcal{R}}H) \cup \{(q'_i, a_i, q'_{i+1}) \mid i \in \{0,\dots,n-1\}\} \cup \{(q'_n, a_n, q_\iota)\}$. Denotamos q_ι por q'_{n+1} quando for necessário.



Então o caminho $q'_0 \xrightarrow{u^{-1}} q_\iota$ ocorre em $\mathcal{A}_0$. Seja $\mathcal{A}_1$ o autómato obtido a partir de $\mathcal{A}_0$ adicionando as respetivas arestas inversas das arestas em $E' \backslash E$ e, caso $a_i \in \widetilde{A_j}$ para algum $j \in \{1,\dots,\mathfrak{N}\}$, colando ao vértice q'_i o grafo $Cay_{A_j}(F_{A_j}^{\mathcal{R}_j})$. Seja $\mathcal{A}_2$ o autómato obtido a partir de $\mathcal{A}_1$ aplicando sucessivamente as dobragens do tipo $p \xleftarrow{a} q \xrightarrow{a} t$ em arestas que não estão em $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$. Por fim, seja $\mathcal{A}_3$ o autómato obtido a partir do último aplicando sucessivamente as dobragens do tipo $p \xleftarrow{a} q \xrightarrow{a} t$ até obtermos um autómato determinístico.

Vamos mostrar que $\mathcal{A}_3$ é um $\mathcal{R}$-SFG: Note-se que $\mathcal{A}_3$ é inverso e tem um ponto base q'_0. Além disso, como todos os vértices de $\mathcal{S}_{\mathcal{R}}H$ têm grau superior a um, todos os vértices em $\mathcal{A}_3$ distintos do ponto base q'_0 têm grau superior a um. Note-se também que toda a aresta com rótulo em $\widetilde{A_i}$ para algum $i \in \{1,\dots,\mathfrak{N}\}$ está contida em algum $K \in Sch_i(\mathcal{A}_3)$. Logo, $\mathcal{A}_3$ é um $\mathcal{R}$-autómato. Note-se que, se em $\mathcal{A}_2$ existir algum $K \in Cay(\mathcal{A}_2)$ que não é útil relativamente a $\mathcal{R}$, então este está contido na parte "nova" que foi adicionada a $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ (uma vez que $\mathcal{S}_{\mathcal{R}}H$ é um $\mathcal{R}$-SFG). Além disso, é fácil de ver que se $a_l \dots a_m$ é uma componente homogénea de u^{-1} com $a_l \dots a_m \in \widetilde{A}^* \backslash \widetilde{A_0}^*$, $l \leq m \in \{0,\dots,n\}$, então as

arestas

$$q'_l \xrightarrow{a_l} \dots \xrightarrow{a_m} q'_{m+1}$$

estão contidas num mesmo $K \in Sch(\mathcal{A}_2)$, sendo q_l necessariamente um vértice partilhado. Logo a única hipótese de $\mathcal{A}_2$ conter um grafo $K \in Cay(\mathcal{A}_2)$ que não tem pelo menos dois vértices partilhados é se este contém q_ι e q_ι não ser partilhado, isto é, se existem $\beta \in \{1, \dots, \mathfrak{N}\}$ tal que $a_n \in \widetilde{A_\beta}$ e $K_\beta \in \left[Cay_{A_\beta}(F_{A_\beta}^{\mathcal{R}_\beta})\right]_{\mathcal{A}_2}$ tal que q_ι é um vértice de K_β e q_ι não é partilhado. Mas então, como q_ι não é um vértice partilhado, significa que as arestas em $\mathcal{C}_{\mathcal{S}_\mathcal{R}H}$ que saem de q_ι têm todas rótulo em $\widetilde{A_\beta}$. Portando o grafo K_β vai ser identificado, em $\mathcal{A}_3$, a algum $K \in Sch_\beta(\mathcal{S}_\mathcal{R}H)$ e, se este for isomorfo a $Cay_{A_\beta}(F_{A_\beta}^{\mathcal{R}_{A_\beta}})$ tem de ser útil relativamente a $\mathcal{R}$. Portanto, $\mathcal{A}_3$ é um $\mathcal{R}$-SFG.

Logo,

$$L(\mathcal{A}_3) \cap Irr(\mathcal{R}) = \overline{L(\mathcal{A}_3)}^{\mathcal{R}} = \overline{L(\mathcal{A}_1)}^{\mathcal{R}} = \overline{u^{-1}L(\mathcal{S}_\mathcal{R}H)u}^{\mathcal{R}}$$

onde a igualdade do meio se justifica com o Lema 7.1.19. Portanto, $L(\mathcal{A}_3) \cap Irr(\mathcal{R}) = \overline{u^{-1}Hu}^{\mathcal{R}} = \overline{H}^{\mathcal{R}}$. Logo $\mathcal{A}_3 \simeq \mathcal{S}_\mathcal{R}H$ e, consequentemente, $q_\iota \xrightarrow{u^{-1}} q$ ocorre em $\mathcal{S}_\mathcal{R}H$ para algum $q \in Q(\mathcal{S}_\mathcal{R}H)$. Além disso,

$$u^{-1}L(\mathcal{S}_\mathcal{R}H)u \subseteq L(\mathcal{A}_1) \subseteq L(\mathcal{A}_3) = L(\mathcal{S}_\mathcal{R}H).$$

Como $u^{-1} \in N(H)$, temos que $\overline{uHu^{-1}}^{\mathcal{R}} = \overline{H}^{\mathcal{R}}$. De forma completamente análoga concluímos que $q_\iota \xrightarrow{u} p$ ocorre em $\mathcal{S}_\mathcal{R}H$ para algum $p \in Q(\mathcal{S}_\mathcal{R}H)$ e

$$uL(\mathcal{S}_\mathcal{R}H)u^{-1} \subseteq L(\mathcal{S}_\mathcal{R}H).$$

Seja $\mathfrak{R}_p$ a redução de $\mathcal{S}_\mathcal{R}H$ em p. Note-se que $\mathfrak{R}_p$ é um $\mathcal{R}$-SFG. Ora, como $q_\iota \xrightarrow{u} p$ ocorre em $\mathcal{S}_\mathcal{R}H$, temos que $uL(\mathfrak{R}_p)u^{-1} \subseteq L(\mathcal{S}_\mathcal{R}H)$. Logo,

$$u^{-1}uL(\mathfrak{R}_p)u^{-1}u \subseteq u^{-1}L(\mathcal{S}_\mathcal{R}H)u \subseteq L(\mathcal{S}_\mathcal{R}H)$$

e, pelo Lema 7.1.14, $L(\mathfrak{R}_p) \subseteq L(\mathcal{S}_\mathcal{R}H)$. Analogamente, como $u^{-1}L(\mathcal{S}_\mathcal{R}H)u \subseteq L(\mathfrak{R}_p)$ temos,

$$u^{-1}uL(\mathcal{S}_\mathcal{R}H)u^{-1}u \subseteq u^{-1}L(\mathcal{S}_\mathcal{R}H)u \subseteq L(\mathfrak{R}_p)$$

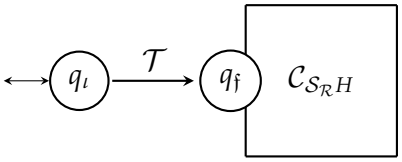
e $L(\mathcal{S}_\mathcal{R}H) \subseteq L(\mathfrak{R}_p)$. Portanto, $L(\mathcal{S}_\mathcal{R}H) = L(\mathfrak{R}_p)$ e, pelo Lema 7.1.23, temos que $\mathcal{S}_\mathcal{R}H \simeq \mathfrak{R}_p$. Portanto, $p \in Orb(q_\iota)$ e $u \in L(\mathcal{S}_\mathcal{R}H/Aut(\Gamma_{\mathcal{S}_\mathcal{R}H}))$. Concluímos assim a igualdade enunciada.

Pela Proposição 8.4.12, sabemos que $\mathcal{S}_\mathcal{R}H/Aut(\Gamma_{\mathcal{S}_\mathcal{R}H})$ é um $\mathcal{R}$-SFG. Portanto, como Λ

é sobrejetiva (Proposição 8.1.13), existe $M \leq_{f.g.} F_A^{\mathcal{R}}$ tal que $\mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H}) \simeq \mathcal{S}_{\mathcal{R}}M$. Além disso, $\overline{M}^{\mathcal{R}} = L(\mathcal{S}_{\mathcal{R}}M) \cap Irr(\mathcal{R}) = L(\mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})) \cap Irr(\mathcal{R}) = \overline{N(H)}^{\mathcal{R}}$. Logo, $N(H) = M$ é finitamente gerado e

$$\mathcal{S}_{\mathcal{R}}N(H) = \mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H}).$$

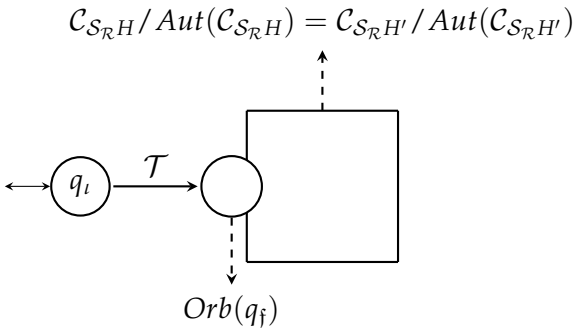
Falta ver o caso em que a cauda de $\mathcal{S}_{\mathcal{R}}H$ não é trivial. Suponhamos então que o ponto base de $\mathcal{S}_{\mathcal{R}}H$ é q_ι e $\mathcal{S}_{\mathcal{R}}H$ é da seguinte forma



onde $q_\iota \xrightarrow{\mathcal{T}} q_\mathfrak{f}$ representa a cauda de $\mathcal{S}_{\mathcal{R}}H$. Seja $\mathfrak{R}_{q_\mathfrak{f}}$ a redução de $\mathcal{S}_{\mathcal{R}}H$ em $q_\mathfrak{f}$ e u o rótulo de um caminho de q_ι até $q_\mathfrak{f}$. Então, pelo Lema 8.3.3, sabemos que $\mathfrak{R}_{q_\mathfrak{f}} \simeq \mathcal{S}_{\mathcal{R}}H'$ onde $H' = u^{-1}Hu$ é não trivial. Logo, $H = uH'u^{-1}$ e, consequentemente, $N(H) = uN(H')u^{-1}$ em $F_A^{\mathcal{R}}$, isto é, $\overline{N(H)}^{\mathcal{R}} = \overline{uN(H')u^{-1}}^{\mathcal{R}}$. Como $\mathcal{S}_{\mathcal{R}}H'$ tem cauda trivial sabemos, pelo que foi visto anteriormente, que

$$\overline{N(H')}^{\mathcal{R}} = L(\mathcal{S}_{\mathcal{R}}H'/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H'})) \cap Irr(\mathcal{R}) = \overline{L(\mathcal{S}_{\mathcal{R}}H'/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H'}))}^{\mathcal{R}}.$$

Então, $\overline{N(H)}^{\mathcal{R}} = \overline{uL(\mathcal{S}_{\mathcal{R}}H'/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H'}))u^{-1}}^{\mathcal{R}} = L(N(\mathcal{S}_{\mathcal{R}}H)) \cap Irr(\mathcal{R})$.



Além disso $N(\mathcal{S}_{\mathcal{R}}H)$ é um $\mathcal{R}$-SFG. Logo, $N(\mathcal{S}_{\mathcal{R}}H) \simeq \mathcal{S}_{\mathcal{R}}N(H)$. □

Corolário 8.4.16. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$. Então $N(H)$ é computável.*

Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ não trivial. Na Proposição 8.4.15, não só vimos que $N(H)$ é finitamente gerado, como também apresentamos uma "receita" para obter $\mathcal{S}_{\mathcal{R}}N(H)$ a partir de $\mathcal{S}_{\mathcal{R}}H$. De facto, temos que $N^i(\mathcal{S}_{\mathcal{R}}H) \simeq \mathcal{S}_{\mathcal{R}}(N^i(H))$ onde $N^i(\mathcal{S}_{\mathcal{R}}H) = N(N^{i-1}(\mathcal{S}_{\mathcal{R}}H))$ para

todo $i \geq 1$ e $N^0(\mathcal{S}_{\mathcal{R}}H) = \mathcal{S}_{\mathcal{R}}H$. Portanto, $N(H)$ é estritamente maior que H se e só se o número de vértices de $\mathcal{S}_{\mathcal{R}}N(H)$ for estritamente menor que o número de vértices de $\mathcal{S}_{\mathcal{R}}H$. Como o número de vértices de $\mathcal{S}_{\mathcal{R}}H$ é finito, resulta, portanto, o seguinte corolário.

Corolário 8.4.17. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$. A cadeia de normalizadores gerada por H estabiliza.*

Vamos agora estudar de que forma a cadeia de normalizadores gerada por um determinado subgrupo finitamente gerado H de $F_A^{\mathcal{R}}$ pode estabilizar, isto é, estudar $N^*(H)$.

Proposição 8.4.18. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ não trivial. Então $N^*(H) = H$ se e só se $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ é totalmente assimétrico.*

Demonstração. Se $N^*(H) = H$, então $N(H) = H$. Logo, pela Proposição 8.4.15, $N(\mathcal{S}_{\mathcal{R}}H) \simeq \mathcal{S}_{\mathcal{R}}H$. Logo, $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ é totalmente assimétrico. Reciprocamente, se $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ é totalmente assimétrico, então $N(\mathcal{S}_{\mathcal{R}}H) = \mathcal{S}_{\mathcal{R}}H$. Logo, novamente pela Proposição 8.4.15, $\mathcal{S}_{\mathcal{R}}N(H) \simeq \mathcal{S}_{\mathcal{R}}H$. Logo, $H = N(H)$. □

Corolário 8.4.19. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$. Então conseguimos decidir quando é que H é* autonormalizador *em $F_A^{\mathcal{R}}$, isto é, quando é que $N(H) = H$.*

Proposição 8.4.20. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$. Então, $N^*(H)$ é conjugado de um fator de $F_A^{\mathcal{R}}$ se e só se $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ é totalmente simétrico.*

Demonstração. O caso em que H é trivial é claro. Portanto, estudaremos apenas o caso em que H não é trivial. Suponhamos primeiro que $\mathcal{S}_{\mathcal{R}}H$ tem cauda trivial. Então $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H} \simeq \Gamma_{\mathcal{S}_{\mathcal{R}}H}$. Ora, $\Gamma_{\mathcal{S}_{\mathcal{R}}H}$ é totalmente simétrico se e só se $\mathcal{S}_{\mathcal{R}}H$ é totalmente simétrico se e só se existe $i \in \mathbb{N}$ tal que $\mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})^i$ é transitivo nos vértices. Como $\mathcal{S}_{\mathcal{R}}H$ tem cauda trivial, $\mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})^i \simeq N^i(\mathcal{S}_{\mathcal{R}}H) \simeq \mathcal{S}_{\mathcal{R}}N^i(H)$ e, pela Proposição 8.4.10, $\mathcal{S}_{\mathcal{R}}N^i(H)$ é transitivo nos vértices se e só se $N(N^i(H)) = N^{i+1}(H)$ é um fator de $F_A^{\mathcal{R}}$. Além disso, como $N^{i+1}(H)$ é um fator de $F_A^{\mathcal{R}}$, $N(N^{i+1}(H)) = N^{i+1}(H)$ e $N^{i+1}(H) = N^*(H)$.

Suponhamos agora que $\mathcal{S}_{\mathcal{R}}H$ não tem cauda trivial. Então, pelo Lema 8.3.3, existe um $K \leq_{f.g.} F_A^{\mathcal{R}}$ tal que $\mathcal{S}_{\mathcal{R}}K$ é uma redução de $\mathcal{S}_{\mathcal{R}}H$ e H e K são subgrupos conjugados. Então, $\mathcal{S}_{\mathcal{R}}K$ tem cauda trivial e $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}K} \simeq \mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$. Logo, pelo que vimos anteriormente, $N^*(K)$ é um fator de $F_A^{\mathcal{R}}$ se e só se $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}K} \simeq \mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ é totalmente simétrico. Logo, como H e K conjugados implica que $N(H)$ e $N(K)$ também o são, podemos concluir que $N^*(H)$ é conjugado de um fator de $F_A^{\mathcal{R}}$ se e só se $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ é totalmente simétrico. □

Corolário 8.4.21. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ não trivial. Então $N^*(H) = F_A^{\mathcal{R}}$ se e só se $\mathcal{S}_{\mathcal{R}}H$ é totalmente simétrico e completo.*

Demonstração. $[\Rightarrow]$ Se $H = F_A^{\mathcal{R}}$ então é claro. Caso contrário, existe um $i \in \mathbb{N}$ tal que $N^i(H) \leq_{f.g.} F_A^{\mathcal{R}}$ e $N^i(H)$ é um subgrupo normal. Pela Proposição 8.4.1, $N^i(H)$ é um subgrupo normal se e só se $\mathcal{S}_{\mathcal{R}}N^i(H) \simeq N^i(\mathcal{S}_{\mathcal{R}}H)$ é transitivo nos vértices e completo. Como $N^i(\mathcal{S}_{\mathcal{R}}H)$ é completo, $\mathcal{S}_{\mathcal{R}}H$ tem cauda trivial e $N^i(\mathcal{S}_{\mathcal{R}}H) \simeq \mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})^i$. Além disso, pelo Lema 8.4.13, o facto de $N^i(\mathcal{S}_{\mathcal{R}}H)$ ser completo implica que $\mathcal{S}_{\mathcal{R}}H$ também o é. Logo $\mathcal{S}_{\mathcal{R}}H$ é completo e totalmente simétrico.

$[\Leftarrow]$ Ora, se $\mathcal{S}_{\mathcal{R}}H$ é totalmente simétrico e completo, então existe $i \in \mathbb{N}$ tal que $N^i(\mathcal{S}_{\mathcal{R}}H) \simeq \mathcal{S}_{\mathcal{R}}N^i(H)$ é transitivo nos vértices e completo e isto equivale a dizer que $N^i(H)$ é normal. Logo $N^*(H) = N(N^i(H)) = F_A^{\mathcal{R}}$. $\square$

Vamos agora estudar o índice $[N(H) : H]$ para um dado $H \leq_{f.g.} F_A^{\mathcal{R}}$. Note-se que, em geral, se H é um subgrupo finitamente gerado de um grupo virtualmente livre, este índice pode não ser finito. Como exemplo, $\mathbb{Z} \times \mathbb{Z}_2$ para $H = \{0\} \times \mathbb{Z}_2$.

Proposição 8.4.22. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ não trivial. Então,*

$$[N^i(H) : N^{i-1}(H)] = |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}N^{i-1}(H)})|$$

para todo o $i \geq 1$, logo finito.

Demonstração. Como $N(H)$ é também um subgrupo finitamente gerado de $F_A^{\mathcal{R}}$, basta mostrar o caso em que $i = 1$, isto é, $[N(H) : H] = |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})|$. Suponhamos primeiro que $\mathcal{S}_{\mathcal{R}}H$ tem cauda trivial. Então $\mathcal{S}_{\mathcal{R}}N(H) \simeq N(\mathcal{S}_{\mathcal{R}}H) \simeq \mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})$. Seja q_ι o ponto base de $\mathcal{S}_{\mathcal{R}}H$. Para cada vértice $q \in Orb(q_\iota)$, seja $q_\iota \xrightarrow{w_q} q$ um caminho em $\mathcal{S}_{\mathcal{R}}H$ com $w_q \in Irr(\mathcal{R})$. Note-se que, uma vez que $q \in Orb(q_\iota)$ e $\mathcal{S}_{\mathcal{R}}N(H) \simeq \mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})$, podemos concluir que $w_q \in N(H)$. Vamos ver que $N(H) = \cup_{q \in Orb(q_\iota)} Hw_q$. Seja $u \in \overline{N(H)}^{\mathcal{R}}$. Como $\mathcal{S}_{\mathcal{R}}N(H) = N(\mathcal{S}_{\mathcal{R}}H) \simeq \mathcal{S}_{\mathcal{R}}H/Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})$, pelo Lema 8.4.13, existe em $\mathcal{S}_{\mathcal{R}}H$ um caminho da forma $q_\iota \xrightarrow{u} q$ para algum $q \in Orb(q_\iota)$. Logo $uw_q^{-1} \in L(\mathcal{S}_{\mathcal{R}}H)$. Mas então, $uw_q^{-1} \in H$ e $u \in Hw_q$.

Portanto, para concluir a igualdade, basta mostrar que se $p, q \in Orb(q_\iota)$ são distintos então $Hw_p \neq Hw_q$. Suponhamos que $Hw_p = Hw_q$. Então $Hw_pw_q^{-1} = H$ e $w_pw_q^{-1} \in H$. Logo $\overline{w_pw_q^{-1}}^{\mathcal{R}} \in L(\mathcal{S}_{\mathcal{R}}H)$. Logo, o caminho $q_\iota \xrightarrow{\overline{w_pw_q^{-1}}^{\mathcal{R}} w_q} q$ ocorre em $\mathcal{S}_{\mathcal{R}}H$. Mas então $q_\iota \xrightarrow{\overline{\overline{w_pw_q^{-1}}^{\mathcal{R}} w_q}^{\mathcal{R}}} q$ também ocorre em $\mathcal{S}_{\mathcal{R}}H$. Como $\overline{\overline{w_pw_q^{-1}}^{\mathcal{R}} w_q}^{\mathcal{R}} = w_p$ e $\mathcal{S}_{\mathcal{R}}H$ é determinístico, $p = q$. Logo, $[N(H) : H] = |Orb(q_\iota)| = |Aut(\Gamma_{\mathcal{S}_{\mathcal{R}}H})| = |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})|$. Se $\mathcal{S}_{\mathcal{R}}H$ não tem cauda trivial, então existe algum $M \leq_{f.g.} F_A^{\mathcal{R}}$ tal que H e M são conjugados em $F_A^{\mathcal{R}}$ e

$\mathcal{S}_{\mathcal{R}}M$ é uma redução de $\mathcal{S}_{\mathcal{R}}H$. Portanto, $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H} \simeq \mathcal{C}_{\mathcal{S}_{\mathcal{R}}M}$. Como, $\mathcal{S}_{\mathcal{R}}M$ tem cauda trivial, sabemos que $[N(M) : M] = |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}M})|$. Agora, basta observar que $|Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})| = |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}M})|$ e, uma vez que M e H são conjugados, $[N(H) : H] = [N(M) : M]$. □

Se $F_A^{\mathcal{R}}$ for um grupo livre, pelo Corolário 5.1.9, sabemos que todo o subgrupo é também livre. Logo, nesta situação, sabemos que o normalizador de um determinado subgrupo finitamente gerado de $F_A^{\mathcal{R}}$ é também livre. No entanto, se $F_A^{\mathcal{R}}$ não for um grupo livre, isto nem sempre se verifica.

Exemplo 8.4.23. *Sejam*

$$\begin{aligned} A_1 &= \{a\}, \quad \mathcal{R}_1 = \{(aa^{-1},1),\ (a^{-1}a,1),\ (a^2,1),\ (a^{-1},a)\},\\ A_2 &= \{b\}, \quad \mathcal{R}_2 = \{(bb^{-1},1),\ (b^{-1}b,1),\ (b^3,1),\ (b^{-1},b^2)\},\\ A_3 &= \{c\}, \quad \mathcal{R}_3 = \{(cc^{-1},1),\ (c^{-1}c,1),\ (c^6,1),\ (c^{-1},c^5)\}. \end{aligned}$$

Então, $F_{A_1}^{\mathcal{R}_1} \simeq \mathbb{Z}_2$, $F_{A_2}^{\mathcal{R}_2} \simeq \mathbb{Z}_3$ *e* $F_{A_3}^{\mathcal{R}_3} \simeq \mathbb{Z}_6$. *Considere-se o seguinte homomorfismo de grupos,*

$$\begin{aligned} \varphi :\ & F_{A_1}^{\mathcal{R}_1} * F_{A_2}^{\mathcal{R}_2} \to F_{A_3}^{\mathcal{R}_3}\\ & a \mapsto c^3\\ & b \mapsto c^2 \end{aligned}$$

Note-se que φ *é um homomorfismo de grupos sobrejetivo. Logo* $(F_{A_1}^{\mathcal{R}_1} * F_{A_2}^{\mathcal{R}_2})/ker(\varphi) \simeq \mathbb{Z}_6$. *Portanto,* $ker(\varphi)$ *tem índice finito e, consequentemente, é finitamente gerado (é subgrupo de índice finito de um grupo finitamente gerado). Além disso* $ker(\varphi)$ *não tem elementos de torção: Suponhamos por absurdo que* $ker(\varphi)$ *tem elementos de torção não triviais. Então pelo Lema 8.1.4, existem* $x \in \widetilde{A_1}^* \cup \widetilde{A_2}^*$ *e* $u \in Irr(\mathcal{R})$ *tais que* $\overline{x}^{\mathcal{R}} \neq 1$ *e* $uxu^{-1} \in ker(\varphi)$. *Mas então, como* $ker(\varphi)$ *é normal,* $x \in ker(\varphi)$. *Ora, isto implicaria que* $a \in ker(\varphi)$ *ou* $b \in ker(\varphi)$ *o que não é verdade. Logo,* $ker(\varphi)$ *é um subgrupo livre (Proposição 8.1.8), finitamente gerado e normal. Uma vez que é um subgrupo normal,* $N(ker(\varphi)) \simeq \mathbb{Z}_2 * \mathbb{Z}_3$ *que tem torção.*

Corolário 8.4.24. *Seja* $H \leq_{f.g.} F_A^{\mathcal{R}}$. *Conseguimos decidir se* $N(H)$ *é livre ou não.*

Demonstração. Pela Proposição 8.4.15, conseguimos obter $\mathcal{S}_{\mathcal{R}}N(H)$ a partir de um conjunto de geradores de H. Aplicando a Proposição 8.1.5, conseguimos decidir se $N(H)$ tem elementos de torção triviais ou não, isto é, se é livre ou não. □

Pela Proposição 8.4.15, sabemos que, dado $H \leq_{f.g.} F_A^{\mathcal{R}}$, o seu normalizador $N(H)$ é também finitamente gerado. No caso em que ambos os subgrupos são livres, estes vão ter uma dimensão (que é a cardinalidade da base). Ora, uma vez que o autómato $\mathcal{S}_{\mathcal{R}}N(H)$ é obtido a partir da identificação de alguns vértices de $\mathcal{S}_{\mathcal{R}}H$, faz sentido perguntar de que forma é que as respetivas dimensões podem estar relacionadas. Um resultado bastante conhecido é a igualdade de Nielsen–Schreier que nos diz o seguinte: dado um subgrupo de índice finito H de um grupo livre F_n ($dim(F_n) = n$) então,

$$dim(H) - 1 = (n-1)[F_n : H].$$

Portanto, se $H \leq_{f.g.} F_A^{\mathcal{R}}$ e H e $N(H)$ são livres, então $H \leq_{f.g.} N(H)$ e, pela Proposição 8.4.22, $[N(H) : H]$ é finito. Além disso, pela Proposição 8.4.15, $N(H)$ é finitamente gerado. Logo, $dim(H) - 1 = (dim(N(H)) - 1)[N(H) : H]$. Para terminar, apresentamos uma demonstração desta igualdade usando os autómatos $\mathcal{S}_{\mathcal{R}}H$.

Proposição 8.4.25. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ livre e não trivial. Se $N(H)$ é também livre, temos que*

$$dim(N(H)) = \frac{dim(H) - 1}{|Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})|} + 1.$$

Demonstração. Suponhamos que $N(H)$ é livre. Então, $\mathcal{S}_{\mathcal{R}}H$ e $\mathcal{S}_{\mathcal{R}}N(H) \simeq N(\mathcal{S}_{\mathcal{R}}H)$ são $\mathcal{R}$-livres. Suponhamos primeiro que $\mathcal{S}_{\mathcal{R}}H$ tem cauda trivial. Então, $\mathcal{S}_{\mathcal{R}}N(H) \simeq \mathcal{S}_{\mathcal{R}}H/Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})$. Pela Proposição 8.1.8, sabemos que $dim(H) - 1$ é igual a

$$\begin{aligned} & \Big(\sum_{q \in Q(\mathcal{S}_{\mathcal{R}}H)} deg_{A_0}(q) - 1 + |Cay_q(\mathcal{S}_{\mathcal{R}}H)| \Big) - |Cay(\mathcal{S}_{\mathcal{R}}H)| \\ = & \Big(\sum_{Orb(q) \in Q(\mathcal{S}_{\mathcal{R}}H/Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}))} \Big(\sum_{p \in Orb(q)} deg_{A_0}(p) - 1 - |Cay_p(\mathcal{S}_{\mathcal{R}}H)| \Big) \Big) - |Cay(\mathcal{S}_{\mathcal{R}}H)| \end{aligned}$$

Ora se $p \in Orb(q)$, então existe um automorfismo de $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}$ que envia p em q. Então $deg_{A_0}(p) = deg_{A_0}(q)$ e $|Cay_p(\mathcal{S}_{\mathcal{R}}H)| = |Cay_q(\mathcal{S}_{\mathcal{R}}H)|$. Logo,

$$\begin{aligned} & \sum_{Orb(q) \in Q(\mathcal{S}_{\mathcal{R}}H/Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}))} \Big(\sum_{p \in Orb(q)} deg_{A_0}(p) - 1 - |Cay_p(\mathcal{S}_{\mathcal{R}}H)| \Big) \\ = & \sum_{Orb(q) \in Q(\mathcal{S}_{\mathcal{R}}H/Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}))} |Orb(q)| \Big(deg_{A_0}(q) - 1 - |Cay_q(\mathcal{S}_{\mathcal{R}}H)| \Big) \\ = & \sum_{Orb(q) \in Q(\mathcal{S}_{\mathcal{R}}H/Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}))} |Orb(q)| \Big(deg_{A_0}(Orb(q)) - 1 - |Cay_{Orb(q)}(\mathcal{S}_{\mathcal{R}}H/Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H}))| \Big) \\ = & |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})| \Big(\sum_{q \in Q(\mathcal{S}_{\mathcal{R}}N(H))} deg_{A_0}(q) - 1 + |Cay_q(\mathcal{S}_{\mathcal{R}}N(H))| \Big). \end{aligned}$$

Agora, note-se que se q, p são vértices de algum $K \in Cay(\mathcal{S}_{\mathcal{R}}H)$ então estes não podem ser identificados em $\mathcal{S}_{\mathcal{R}}H/Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})$, caso contrário, pela Proposição 8.1.5, $\mathcal{S}_{\mathcal{R}}N(H)$

não seria um autómato livre e, consequentemente, $N(H)$ não seria livre de torção. Portanto, $|Cay(\mathcal{S}_{\mathcal{R}}H)| = |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})||Cay(\mathcal{S}_{\mathcal{R}}N(H))|$. Concluímos assim que

$$\begin{aligned} dim(H)-1 &= |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})|\Big(\Big(\sum_{q\in Q(\mathcal{S}_{\mathcal{R}}N(H))} deg_{A_0}(q)-1+|Cay_q(\mathcal{S}_{\mathcal{R}}N(H))|\Big)-|Cay(\mathcal{S}_{\mathcal{R}}N(H))|\Big) \\ &= |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})|(dim(N(H))-1). \end{aligned}$$

Suponhamos agora que $\mathcal{S}_{\mathcal{R}}H$ não tem cauda trivial. Então, pelo Lema 8.3.3, sabemos que existe algum $M \leq_{f.g.} F_A^{\mathcal{R}}$ tal que H e M são conjugados em $F_A^{\mathcal{R}}$ e $\mathcal{S}_{\mathcal{R}}M$ é uma redução de $\mathcal{S}_{\mathcal{R}}H$. Portanto, como $\mathcal{S}_{\mathcal{R}}M$ tem cauda trivial, sabemos que $dim(M)-1 = |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}M})|(dim(N(M))-1)$. Além disso, $\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H} \simeq \mathcal{C}_{\mathcal{S}_{\mathcal{R}}M}$. Logo,

$$dim(M)-1 = |Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})|(dim(N(M))-1).$$

Agora, basta notar que, se M e H são conjugados, então $N(M)$ e $N(H)$ também o são e $dim(M) = dim(H)$, $dim(N(M)) = dim(N(H))$. Como $|Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})| \geq 1$, podemos reescrever a igualdade obtendo a igualdade enunciada. □

Corolário 8.4.26. *Seja $H \leq_{f.g.} F_A^{\mathcal{R}}$ não trivial. Se H e $N^i(H)$ são livres, para algum $i \geq 1$, então*

$$dim(H)-1 = (dim(N^i(H))-1)[N^i(H):H].$$

Demonstração. Da Proposição 8.4.25, sabemos que $dim(H)-1 = (dim(N(H))-1)|Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})|$. Por outro lado, da Proposição 8.4.22, sabemos que $|Aut(\mathcal{C}_{\mathcal{S}_{\mathcal{R}}H})| = [N(H):H]$. Logo,

$$dim(H)-1 = (dim(N(H))-1)[N(H):H]$$

e, no caso em que $i = 1$, temos já a igualdade enunciada. Suponhamos então que $i \geq 2$. Note-se que, se $N^i(H)$ é livre, então $N^j(H)$ também o é para todo $j \leq i$. De forma análoga, podemos concluir que $dim(N(H)-1) = (dim(N^2(H))-1)[N^2(H) : N(H)]$. Logo, $dim(H)-1 = (dim(N^2(H))-1)[N^2(H):N(H)][N(H):H]$, isto é, $dim(H)-1 = (dim(N^2(H))-1)[N^2(H):H]$. Repetindo o processo $i-2$ vezes chegamos à igualdade enunciada. □

9. Conclusão

Neste trabalho comprovou-se mais uma vez o poder e a utilidade de estudar subgrupos finitamente gerados através de autómatos inversos. De facto, através desta abordagem, foi-nos possível deduzir várias propriedades algébricas que, a priori, não seriam tão fáceis de obter por métodos puramente algébricos. Dado um grupo singelo $F_A^{\mathcal{R}}$, o facto de conseguirmos computar $N(H)$ de um dado $H \leq_{f.g.} F_A^{\mathcal{R}}$ partindo apenas de um conjunto de geradores de H e de conseguirmos responder a vários problemas de decisão através de uma análise geométrica destes autómatos é um excelente exemplo de como estes autómatos são talvez a melhor ferramenta para estudar problemas computacionais em $F_A^{\mathcal{R}}$. Outro exemplo que reforça o valor destes autómatos é o facto de conseguirmos generalizar, de forma bastante simples, certos teoremas conhecidos relativos ao grupo modular. Por fim, podemos concluir que, caso a conjetura de Madlener e Otto se confirme, todos os resultados aqui obtidos aplicam-se igualmente à classe dos grupos que admitem uma apresentação finita $\langle A|\mathcal{R}\rangle$ para algum sistema de reescrita $\mathcal{R}$ redutor e confluente.

Bibliografia

[1] Jürgen Avenhaus, Klaus Madlener, and Friedrich Otto. Groups presented by finite two-monadic church-rosser thue systems. *Transactions of the American Mathematical Society*, 297(2):427–443, 1986. [Citado nas páginas ii, iii, 1 e 43.]

[2] Laurent Bartholdi and Pedro V Silva. Rational subsets of groups., 2021. [Citado na página 2.]

[3] Benjamin Baumslag. Intersections of finitely generated subgroups in free products. *Journal of the London Mathematical Society*, 1(1):673–679, 1966. [Citado na página 71.]

[4] Noam Chomsky. Three models for the description of language. *IRE Transactions on information theory*, 2(3):113–124, 1956. [Citado na página 10.]

[5] Max Dehn. Über unendliche diskontinuierliche gruppen. *Mathematische Annalen*, 71(1):116–144, 1911. [Citado na página 34.]

[6] Jordi Delgado and Pedro V Silva. On the lattice of subgroups of a free group: complements and rank. *journal of Groups, complexity, cryptology*, 12, 2020. [Citado na página 2.]

[7] Volker Diekert. Some remarks on presentations by finite church-rosser thue systems. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 272–285. Springer, 1987. [Citado na página 43.]

[8] Murray Elder and Adam Piggott. Rewriting systems, plain groups, and geodetic graphs. *Theoretical Computer Science*, 903:134–144, 2022. [Citado nas páginas ii, iii, 1 e 43.]

[9] Robert C Gunning. *Lectures on modular forms*. Number 48. Princeton University Press, 1962. [Citado nas páginas ii, iii e 87.]

[10] Albert G Howson. On the intersection of finitely generated free groups. *Journal of the London Mathematical Society*, 1(4):428–434, 1954. [Citado na página 71.]

[11] Gérard Huet. Confluent reductions: Abstract properties and applications to term rewriting systems: Abstract properties and applications to term rewriting systems. *Journal of the ACM (JACM)*, 27(4):797–821, 1980. [Citado na página 20.]

[12] Ilya Kapovich and Alexei Myasnikov. Stallings foldings and subgroups of free groups. *Journal of Algebra*, 248(2):608–668, 2002. [Citado nas páginas 1, 38 e 71.]

[13] Ilya Kapovich, Richard Weidmann, and Alexei Myasnikov. Foldings, graphs of groups and the membership problem. *International Journal of Algebra and Computation*, 15 (01):95–128, 2005. [Citado nas páginas 2, 42 e 57.]

[14] Felix Klein. *Vorlesungen über die Theorie der elliptischen Modulfunctionen: Grundlegung der Theorie*, volume 1. Teubner, 1890. [Citado na página 1.]

[15] Manuel Ladra and Pedro V Silva. The generalized conjugacy problem for virtually free groups. 2011. [Citado na página 83.]

[16] Roger C Lyndon and Paul E Schupp. *Combinatorial group theory*, volume 89. Springer, 1977. [Citado nas páginas 25 e 37.]

[17] L Markus-Epstein. Algorithmic problems in amalgams of finite groups: conjugacy and intersection properties. *arXiv preprint arXiv:0707.0165*, 2007. [Citado na página 2.]

[18] L Markus-Epstein. Reading off kurosh decompositions. *International Journal of Algebra and Computation*, 18(06):1117–1136, 2008. [Citado na página 2.]

[19] Luda Markus-Epstein. Stallings foldings and subgroups of amalgams of finite groups. *International Journal of Algebra and Computation*, 17(08):1493–1535, 2007. [Citado na página 2.]

[20] Alexei Miasnikov, Enric Ventura, and Pascal Weil. Algebraic extensions in free groups. In *Geometric Group Theory: Geneva and Barcelona Conferences*, pages 225–253. Springer, 2007. [Citado na página 2.]

[21] Thomas W Müller and Jan-Christoph Schlage-Puchta. Classification and statistics of finite index subgroups in free products. *Advances in Mathematics*, 188(1):1–50, 2004. [Citado nas páginas ii, iii e 87.]

[22] Morris Newman. The structure of some subgroups of the modular group. *Illinois Journal of Mathematics*, 6(3):480–487, 1962. [Citado na página 87.]

[23] Morris Newman. Free subgroups and normal subgroups of the modular group. *Illinois Journal of Mathematics*, 8(2):262–265, 1964. [Citado nas páginas ii, iii e 87.]

[24] Joseph J Rotman. *An introduction to the theory of groups*, volume 148. Springer Science & Business Media, 2012. [Citado na página 33.]

[25] Pedro V. Silva. Teoria geométrica de grupos. Universidade Federal da Bahia, Salvador – Curso de Pré-Doutorado em Matemática, 2014. [Citado nas páginas 24 e 59.]

[26] Pedro V Silva, Xaro Soler-Escrivà, and Enric Ventura. Finite automata for schreier graphs of virtually free groups. *Journal of Group Theory*, 19(1):25–54, 2016. [Citado nas páginas 2, 42 e 57.]

[27] John R Stallings. On torsion-free groups with infinitely many ends. *Annals of Mathematics*, 88(2):312–334, 1968. [Citado na página 66.]

[28] John R Stallings. Topology of finite graphs. *Inventiones mathematicae*, 71(3): 551–565, 1983. [Citado nas páginas 1 e 38.]

[29] Enric Ventura. On fixed subgroups of maximal rank. *Communications in Algebra*, 25 (10):3361–3375, 1997. [Citado na página 2.]

Índice Remissivo

alfabeto, 7
apresentação, 22
    finita, 22
aresta, 11
árvore geradora, 66
atalho, 14
automorfismo de autómatos, 12
autonormalizador, 96
autómato, 11
    aparado, 14
    com transições-1, 15
    completo, 15
    conexo, 39
    conexo por arcos, 39
    de Stallings, 38
    determinístico, 14
    equivalente, 15
    finito, 12
    flor, 41
    inverso, 39
    involutivo, 38
    totalmente assimétrico, 13
    totalmente simétrico, 13
    transitivo, 13

cadeia de normalizadores, 89
caminho, 14
    bem-sucedido, 14
    fechado, 14
    trivial, 14
componentes homogéneas, 30
comprimento de uma palavra, 7
congruência
    gerada por $\mathcal{R}$, 22
    num monóide, 5
    num semigrupo, 5
conjugada cíclica, 36

dimensão, 25
dobragens de Stallings, 42

fator
    de $F_A^{\mathcal{R}}$, 89
    de uma palavra, 11
função involutiva, 39

grafo, 11
    de Cayley, 39
    de Schreier, 39
    útil relativamente a $\mathcal{R}$, 49
grau de um vértice, 39
grupo, 4
    abeliano, 4
    finitamente apresentável, 22
    livre, 24
    singelo, 42
    virtualmente livre, 42

homomorfismo
    de monóides, 4
    de semigrupos, 4

isomorfismo
    de autómatos, 12
    de monóides, 5

de semigrupos, 5

letra, 7
linguagem, 10
de um autómato, 14
racional, 15

monóide, 4
finitamente gerado, 4
livre, 8

normalizador
de um grupo, 89
de um $\mathcal{R}$-SFG, 91
núcleo, 4
cíclico, 36

palavra, 7
ciclicamente $\mathcal{R}$-reduzida, 63
minimal por conjugação, 73
$\mathcal{R}$-irredutível, 18
$\mathcal{R}$-reduzida, 18
vazia, 7
pétalas, 41
ponto
base, 12
final, 77
inicial, 77
prefixo, 11
problema
da conjugação, 34
generalizado, 38
da palavra, 34
generalizado, 38
decidível, 35
do isomorfismo, 38
indecidível, 35

produto
de autómatos, 17
livre, 28
propriedade de Howson, 71

quociente
de um autómato, 13
de um monóide, 5
de um semigrupo, 5

$\mathcal{R}$-autómato, 49
trivial, 49
$\mathcal{R}$-cauda, 77
não trivial, 77
trivial, 77
$\mathcal{R}$-SFG, 49
cerne, 78
extensão, 78
livre, 70
$\mathcal{R}$-cauda, 78
redução, 78
redução elementar, 18
rótulo de um caminho, 14

semigrupo, 4
finitamente gerado, 4
livre, 9
sistema de reescrita, 18
confluente, 19
finito, 18
involutivo, 21
localmente confluente, 19
NCI, 21
noetheriano, 18
redutor, 18
sub

autómato, 13
grupo
conjugado, 33
monóide, 4
semigrupo, 4
sufixo, 11
$\mathcal{T}$-geodésica, 66
vértice, 11
inicial, 11
terminal, 11
vértice partilhado, 54

Notação

$Cay_{A,\Phi}(G)$, 39
$\mathcal{A}/Aut(\Gamma_{\mathcal{A}})^n$, 13
$\mathcal{A}_1 \times \mathcal{A}_2$, 17
$\triangle_S$, 4
$(Irr(\mathcal{R}), \star)$, 22
A^+, 7
A^*, 7
A^{-1}, 21
$Aut(\mathcal{A})$, 12
$Cay(\mathcal{A})$, 48
$Cay_q(\mathcal{A})$, 48
$E(\mathcal{A})$, 11
$F_A^{\mathcal{R}}$, 21
$G_1 * G_2$, 29
$Grp\langle A\ ,\ \mathcal{R}\rangle$22
$H \leq_{f.g.} G$, 38
$H_P[u] = m$, 30
$Irr(\mathcal{R})$, 18
$L(\mathcal{A})$, 14
L^*, 10
$Mon\langle A\ ,\ \mathcal{R}\rangle$22
$N(H)$, 89
$N(\mathcal{A})$, 91
$N^*(H)$, 89
$N_a(u)$, 27
$Orb(q)$, 13
$Q(\mathcal{A})$, 11
$Sch(\mathcal{A})$, 48
$Sch_i(\mathcal{A})$, 48
$Sch_{A,\Phi}(G, N)$, 39
$[\mathcal{G}]_{\mathcal{A}}$, 47
$\Gamma_{\mathcal{A}}$, 12
Λ, 62
γ_i, 76
$\langle A\ ,\ \mathcal{R}\rangle$22
$\langle X\rangle$, 4
$(\mathbf{u}]$, 54
$[\mathbf{u})$, 54
$\mathcal{A}/Aut(\Gamma_{\mathcal{A}})$, 13
$\mathcal{C}_{\mathcal{A}}$, 78
$\mathcal{E}[u]$, 59
$\mathcal{F}(X)$, 41
$\mathcal{F}_{\mathcal{R}}(X)$, 45
$\mathcal{R}_A$, 21
$\mathcal{S}(X)$, 42
$\mathcal{S}_{\mathcal{R}}(X)$, 44
$\mathcal{S}_{\mathcal{R}}H$, 62
$\mathfrak{E}_{q,\mathcal{T}}(\mathcal{A})$, 78
$\mathfrak{N}$, 44
$\mathfrak{R}_q(\mathcal{A})$, 78
$\overline{u}^{\mathcal{R}}$, 20
$\sigma_{\mathcal{R}}$, 22
$\widetilde{A}$, 21
$c(u)$, 36
$deg_X(q)$, 39
$dim(G)$, 25
$ker(\phi)$, 4
q_ι, 77
$q_{\mathfrak{f}}$, 77
$u \rightarrow_{\mathcal{R}} v$, 18
u^{c^k}, 73
w_p, 66
$|u|$, 7