

Universidade de Brasília  
Instituto de Ciências Exatas  
Departamento de Matemática

Os problemas da conjugação e da ordem  
para grupos gerados por  
autômatos de crescimento limitado

por  
Flávia Ferreira Ramos Zapata<sup>1</sup>

Brasília  
2011

---

<sup>1</sup>Trabalho não autorizado para publicação online.

*Ao Theo, meu coração... meu colaborador.*

# Agradecimentos

A minha querida mãe que durante todos esses anos se mostrou uma rocha cobrindo a mim e aos meus irmãos de carinho e proteção. Admiro-a muito pela sua força e inteligência.

Ao professor Said pelos quase 6 anos de orientação. Não posso calcular o quanto aprendi durante esse anos, nem quanto do seu tempo tomei, mas afirmo que tenho-o como espelho e me sinto honrada e privilegiada por ter sido sua orientanda no mestrado e doutorado.

Aos meus professores da UFG que despertaram meu interesse por pesquisa em matemática e que de alguma forma fizeram diferença e influenciaram as decisões que tomei desde então. Em especial à professora Edméia, que estava comigo nos meus primeiros passos dessa minha caminhada científica e por quem tenho muito carinho, respeito e gratidão.

Aos meus irmãos Jane e Valter, bem como aos meus sobrinhos Guilherme, Thales e Naiara.

Aos amigos de república, pela paciência, pelos laços de amizade que criamos e por todos os bons momentos que passamos juntos.

Ao Theo, por todo amor, companheirismo, apoio e ajuda. Não posso estimar o quanto se dedicou a mim quando precisei, mas sei que os sentimentos que me levam a fazer essa dedicação são – além do amor – a profunda admiração e respeito que o tenho.

*“A pessoa que nunca cometeu um erro  
é aquela que nunca tentou algo novo.”*

Albert Einstein

# Resumo

Neste trabalho, estudamos os problemas da conjugação e da ordem no grupo dos automorfismos  $\mathcal{A}$  da árvore regular enraizada  $\mathcal{T}$  e no seu subgrupo  $\mathcal{A}_f$  dos automorfismos de finitos estados. Mostramos que estes dois problemas são decidíveis sob as condições de contração e de finitude sobre o que chamamos de sinalizadores de órbita, e em particular, eles são decidíveis no grupo dos autômatos limitados. Para o problema da ordem um procedimento é desenvolvido em termos de um grafo finito o qual é construtível. Dois procedimentos diferentes foram desenvolvidos para a conjugação no grupo dos autômatos limitados e estes produzem um conjugador quando os automorfismos são conjugados.

**Palavras chaves:** autômatos, problema da conjugação, problema da ordem, fechado por estados, automorfismo de árvores, crescimento limitado.

# Abstract

In the present work, we study the order and conjugacy problems in the automorphism group  $\mathcal{A}$  of the regular rooted tree  $\mathcal{T}$  and in its subgroup  $\mathcal{A}_f$  of finite-state automorphisms. We show that both problems are decidable under the contracting condition and the finiteness of what we call the orbit-signalizer and in particular they are decidable in the group of bounded automata. For the order problem a procedure is developed in terms of a finite graph which is constructible. Two different procedures for conjugation in the group of bounded automata were developed and they produce a conjugator when the automorphisms are conjugate.

**Key words:** automata, conjugacy problem, order problem, state-closed, tree automorphism, bounded growth.

# Sumário

<b>Notação</b>	<b>1</b>
<b>Introdução</b>	<b>4</b>
<b>1 Preliminares</b>	<b>11</b>
1.1 Árvores enraizadas . . . . .	11
1.2 O grupo $\mathcal{A}$ . . . . .	12
1.2.1 A estrutura de $\mathcal{A}$ como produto entrelaçado . . . . .	14
1.2.2 Grupos fechados por estados . . . . .	16
1.2.3 Automorfismos funcionalmente recursivos . . . . .	18
1.2.4 Autômatos . . . . .	19
1.2.5 Automorfismos de finitos estados . . . . .	20
1.3 Crescimento de autômatos: o grupo $Pol(0)$ . . . . .	22
1.3.1 A função $\theta$ de crescimento de autômatos . . . . .	22
1.3.2 O grupo $Pol(-1)$ dos automorfismos finitários . . . . .	24
<b>2 Circuitos</b>	<b>29</b>
2.1 Automorfismos circuitos . . . . .	29
2.1.1 Produtos de circuitos . . . . .	35
2.1.2 A finitude do conjunto $\mathcal{N}(G)$ de circuitos . . . . .	38
2.1.3 Um algoritmo para calcular $\mathcal{N}(G)$ . . . . .	39
<b>3 Problemas algorítmicos para <math>\mathcal{A}</math></b>	<b>41</b>
3.1 O problema da conjugação . . . . .	42
3.1.1 Classes de conjugação em $\mathcal{A}$ . . . . .	43
3.1.2 O problema da conjugação em $\mathcal{A}$ . . . . .	45
3.2 O problema da ordem em $\mathcal{A}$ . . . . .	48

3.2.1	O grafo da ordem . . . . .	50
3.3	O problema da conjugação para automorfismos de finitos estados . . .	52
3.3.1	O grafo conjugador . . . . .	52
3.3.2	Problema da conjugação simultâneo . . . . .	58
3.3.3	Conjugação de automorfismos contráteis . . . . .	58
3.4	Conjugação de automorfismos de crescimento limitado . . . . .	64
3.5	Conjugação de automorfismos limitados por automorfismos finitários .	65
3.5.1	Decidindo conjugação entre automorfismos não finitários por automorfismos finitários . . . . .	67
3.5.2	O problema da conjugação no grupo dos autômatos limitados	71
3.5.3	Procedimento para decidir conjugação em $Pol(0)$ . . . . .	73
3.5.4	Resolvendo conjugação para autômatos limitados através do cálculo dos estados ativos . . . . .	74
3.6	Exemplos . . . . .	79
<b>Referências Bibliográficas</b>		<b>91</b>



# Notação

$Q(\alpha)$	conjunto dos estados do automorfismo $\alpha$
$x^y$	$y^{-1}xy$
$v^f; f(v); (v)f$	imagem de $v$ por $f$
$m \mid n$	$m$ divide $n$
$Y$	alfabeto finito $\{0, 1, \dots, d-1\}$
$M = Y^*$	monoide livre gerado por $Y$
$Y^k$	subconjunto de $Y^*$ formado pelas palavras de comprimento igual a $k$
$\mathcal{T} = \mathcal{T}_d$	árvore $d$ -ária regular uni-raiz
$\mathcal{T}_Y$	árvore regular uni-raiz definida sobre o alfabeto $Y$
$\mathcal{A} = \text{Aut}(\mathcal{T}_d)$	grupo de todos os automorfismos de $\mathcal{T}_d$
$\mathcal{A}_{fr}$	grupo dos automorfismos funcionalmente recursivos de $\mathcal{T}_d$
$\mathcal{A}_f$	grupo dos automorfismos de finitos estados de $\mathcal{T}_d$
$\alpha _v$	estado de $\alpha$ em $v$ , onde $v \in \mathcal{T}_d$
$\pi_\alpha$	permutação induzida por $\alpha$ nos vértices de comprimento 1 de $\mathcal{T}_d$
$\pi_\alpha^{(k-1)}$	permutação induzida por $\alpha$ nos vértices de comprimento $\leq k$ de $\mathcal{T}_d$
$\text{Stab}_{\mathcal{A}}(k)$	automorfismos de $\mathcal{A}$ que fixam vértices de comprimento $\leq k$ de $\mathcal{T}_d$
$f^{(k)}(\alpha)$	decomposição de $\alpha = f^{(k)}(\alpha)\pi_\alpha^{(k-1)}$ onde $f^{(k)}(\alpha) \in \text{Stab}_{\mathcal{A}}(k)$

$D(\alpha)$	autômato associado ao automorfismo $\alpha$
$Star(v)$	conjunto composto pelo vértice $v$ e todas as arestas chegando e saindo deste
$D(\alpha)'$	autômato de $\alpha$ removendo $Star(e)$ , ou seja, $D(\alpha) \setminus Star(e)$
$p(\alpha)$	profundidade do automorfismo $\alpha$
$u_j * \delta_j$	o automorfismo tal que $(u_j * \delta_j) _{u_j} = \delta_j$ e $(u_j * \delta_j) _u = e$ para $u \in Y^{ u_j } \setminus u_j$
$\partial(\alpha)$	grau do automorfismo de crescimento polinomial $\alpha$
$ \alpha _m =  \alpha $	comprimento $m$ – silábico de $\alpha$
$\mathcal{N}(\alpha)$	conjunto de todos os estados de $\alpha$ que são automorfismos circuitos
$\mathcal{P}(\alpha)$	conjunto de todos os estados de $\alpha$ que são automorfismos finitários
$\theta(\alpha, k)$	função de crescimento do autômato de $\alpha$
$A \setminus B$	elementos de $A$ que não pertencem a $B$
$Pol(-1)$	grupo dos automorfismo finitários de $\mathcal{A}$
$Pol(m)$	grupo dos automorfismo de crescimento polinomial no máximo $m$
$Pol(\infty)$	união de todos os subgrupos $Pol(m)$
$G_1 \cong G_2$	$G_1$ é isomorfo a $G_2$
$\langle x_1, x_2, \dots, x_n \rangle$	grupo gerado por $x_1, x_2, \dots, x_n$
$G'$	subgrupo comutador de $G$
$l(h)$	ver Seção 3.5.2
$P_k$	grupo dos automorfismos finitários com profundidade $\leq k$
$\mathcal{T}_d^{[k]}$	subárvore finita de $\mathcal{T}_d$ contendo apenas vértices de comprimento $\leq k$
$\Phi(\alpha)$	grafo da ordem de $\alpha$

$\phi$	sequencia vazia ou raiz
$\Psi(\alpha, \beta)$	grafo conjugador do par $(\alpha, \beta)$
$\mathcal{O}_v$	órbita com representante $v$
$Orb_\alpha(v)$	$\{v, v^\alpha, v^{\alpha^2}, \dots, v^{\alpha^{m-1}}\}$ órbita com representante $v$
$OS(\alpha)$	$\{\alpha^m _v \mid v \in Y^*, m =  Orb_\alpha(v) \}$
$C\Pi(\alpha, \beta)$	$\{\pi \in Sym(Y) : \pi^{-1}\pi_\alpha\pi = \pi_\beta\}$
$\alpha \sim_\gamma \beta$	$\gamma^{-1}\alpha\gamma = \beta$
$\alpha \sim_H \beta$	existe $h \in H$ tal que $\alpha \sim_h \beta$
$C_G(x)$	centralizador do elemento $x$ em $G$
$ G  = \#G$	cardinalidade do conjunto $G$
$o(\alpha)$	ordem do elemento $\alpha$
$Sym(Y)$	grupo das permutações do conjunto $Y$
$Star(v)$	conjunto formado pelo vértice $v$ e todas as arestas chegando e saindo deste
$\mathcal{C}$	configuração de órbita. Ver Seção 3.5.1
$DP_{\mathcal{C}}$	ver Seção 3.5.1
$u_{\mathcal{C}}$	ver Seção 3.5.4
$\theta_{\mathcal{C}, \pi}$	ver Seção 3.5.4
$C\Pi_{\mathcal{C}}$	ver Seção 3.5.4
$\theta_\pi$	ver Seção 3.5.4
$A_\pi$	ver Seção 3.5.4

# Introdução

A possibilidade de gerar grupos por autômatos de entrada e saída foi sugerida no início dos anos 60 por V.M. Glushkov [Glu61], [GW00] mas levou mais de uma década até que tais grupos realmente despertassem o interesse devido às suas propriedades exóticas e, ao mesmo tempo, sua complexidade. Somente com a construção feita por Aleshin [Ale72] é que foi percebido a sua importância – ele deu um exemplo de um grupo de Burnside gerado por autômatos de finitos estados sobre o alfabeto binário, contribuindo assim para um dos mais famosos problemas em álgebra: O Problema Geral de Burnside. No início da década de 80 outras construções elegantes surgiram, como os  $p$ -grupos de Grigorchuck e Gupta-Sidki [Gri80, GS83], os quais ainda hoje são estudados.

Um outro indicativo da importância desses grupos veio quando demonstrou-se que alguns deles constituíam os primeiros exemplos de grupos de crescimento intermediário [Gri83, Gri84, Gri85], respondendo positivamente à questão de J. Milnor [Mil68] sobre a existência de tais grupos, assim como à uma série de outras questões em teoria de grupos e em teoria de Probabilidades, incluindo o problema de Day [Day57] sobre a existência de grupos amenos (amenable) mas não amenos-elementares. Basicamente, até hoje, todos os exemplos conhecidos de grupos de crescimento intermediário bem como não-amenos elementares, são baseados em grupos de autômatos.

A facilidade no manejo desses grupos resultou no descobrimento de outros novos fenômenos nas últimas duas décadas [Sid87, BG00, Nek05, Sid00, GNS00] dentre eles podemos citar a quase-finitude, quase solubilidade em grupos livres de torção, separabilidade sob conjugação, ausência da propriedade de congruência [Per07] (relativo a tópicos em grupos profinitos) e por fim a existência de subgrupo galhado (branching) (ou seja, sugrupo que contém o produto cartesiano de duas cópias isomorfas ao próprio). Contudo, a principal ferramenta introduzida no início da década de 80 foi

a linguagem de ações sobre árvores sugerida por Gupta e Sidki em [GS83]: grupos gerados por autômatos podem ser interpretados como grupos de automorfismos de uma árvore regular uni-raiz  $\mathcal{T}$ . Tal interpretação ajudou muito a trazer uma visão geométrica para o assunto, já que a característica chave desses grupos está no fato de que esta ação canônica é fechada por estados (ou auto similar), no sentido de que cada estado de cada automorfismo é um automorfismo de uma subárvore de  $\mathcal{T}$ , a qual é isomorfa à própria  $\mathcal{T}$ . Segue desse isomorfismo entre árvores que cada estado pode ser identificado com um automorfismo de  $\mathcal{T}$ , dando ao grupo  $\mathcal{A}$ , de todos os automorfismos da árvore, o que chamamos de estrutura galhada – reflexo da estrutura recursiva da árvore em si. Outra característica que tais grupos herdam da árvore sobre a qual agem é a topologia natural dela: a árvore regular uni-raiz – junto com sua fronteira – é árvore profinita. O grupo  $\mathcal{A}$  possui uma topologia compatível com a da árvore e com relação a qual ele é grupo profinito.

Um desenvolvimento recente é a forte ligação desta área com sistemas dinâmicos, o que fez destes grupos uma ferramenta importante na dinâmica holomorfa e análises sobre fractais.

Uma questão muito importante discutida pela primeira vez por S. Sidki, foi analisar como a estrutura do autômato, visto como grafo orientado, reflete em propriedades algébricas do grupo por ele gerado. Analisando o crescimento da atividade dos autômatos de finitos estados ele demonstrou em [Sid00] que tal crescimento é polinomial ou exponencial e que os autômatos de crescimento polinomial no máximo  $m$ , formam um grupo, chamado  $Pol(m)$ . Mais tarde, em [Sid04], demonstrou que o grupo gerado por dois automorfismos de crescimento polinomial não possui subgrupos livres de posto 2.

Formalmente, a conexão entre os grupos de automorfismos e autômatos ocorre através de uma correspondência natural entre autômatos inversíveis de entrada e saída sobre o alfabeto  $Y = \{0, 1, 2, \dots, d-1\}$  e automorfismos da árvore regular  $d$ -ária uni-raiz  $\mathcal{T}$ . Para apresentar esta correspondência fazemos uma indexação dos vértices da árvore  $\mathcal{T}$  por elementos do monóide  $Y^*$ , livremente gerado pelo conjunto  $Y$ . Desta forma, grupo  $\mathcal{A}$  se decompõe como produto entrelaçado permutacional  $\mathcal{A} \cong \mathcal{A} \wr Sym(Y)$ , onde  $Sym(Y)$  é o grupo de todas as permutações de  $Y$ . Esta decomposição nos permite representar um automorfismo da seguinte maneira  $g = (g|_0, g|_1, g|_2, \dots, g|_{d-1})\pi_g$ , onde  $\pi_g \in Sym(Y)$  é a permutação induzida por  $g$  sobre os vértices de comprimento 1 de  $\mathcal{T}$ . Iterativamente, podemos definir o

automorfismo  $g|_v = (((g|_{y_1})|_{y_2}) \dots)|_{y_n}$  para todo vértice  $v = y_1 y_2 \dots y_n$  de  $\mathcal{T}$ . Então cada automorfismo  $g \in \mathcal{A}$  corresponde a um autômato de entrada e saída  $D(g)$  sobre o alfabeto  $Y$  e cujo conjunto de estados é  $Q(g) = \{g|_v \mid v \in Y^*\}$ .

Usando essa correspondência entre automorfismos e autômatos podemos definir várias classes de subgrupos especiais do grupo  $\mathcal{A}$ . Um subgrupo  $G < \mathcal{A}$  é chamado de *fechado por estados* ou *auto-similar* se os estados de cada elemento de  $G$  ainda pertencem a  $G$ . A união de todos os subgrupos finitamente gerados fechados por estados de  $\mathcal{A}$  é um subgrupo contável de  $\mathcal{A}$  denotado por  $\mathcal{A}_{fr}$  e chamado de *grupo dos automorfismos funcionalmente recursivos* [BS97]. Automorfismos de  $\mathcal{T}$  que correspondem a autômatos finitos são chamados de *automorfismos de finitos estados*. Mais precisamente, um automorfismo  $g \in \mathcal{A}$  é de finitos estados se o conjunto  $Q(g)$  é finito. O conjunto de todos automorfismo de finitos estados formam um grupo contável denotado por  $\mathcal{A}_f$ . Cada automorfismo de finitos estados é funcionalmente recursivo e, portanto, o grupo  $\mathcal{A}_f$  é um subgrupo de  $\mathcal{A}_{fr}$ . Conforme já observamos,  $Pol(m)$  é o grupo dos autômatos de crescimento polinomial de grau no máximo  $m$ . Um automorfismo  $g$  é chamado finitário se existe  $k$  tal que  $g|_v = e$  para todo  $v \in Y^*, |v| \geq k$ . O conjunto de todos os automorfismos finitários é um subgrupo de  $Pol(0)$  que chamamos de  $Pol(-1)$ . Denotamos a união, para  $m \geq -1$  por  $Pol(\infty) = \cup_{n=-1}^{\infty} Pol(m)$ .

Nesse trabalho vamos tratar de alguns problemas algorítmicos clássicos para alguns subgrupos de  $\mathcal{A}$  incluindo os subgrupos  $Pol(m)$  dos autômatos de crescimento polinomial no máximo  $m$ . Mais especificamente vamos tratar do problema da conjugação e da ordem para os grupos  $\mathcal{A}, \mathcal{A}_{fr}, \mathcal{A}_f, Pol(0)$ .

No início do século vinte Max Dehn formulou três problemas algorítmicos clássicos em teoria de grupos os quais vem sendo extensivamente estudados nos dias de hoje. O problema da palavra é o primeiro dos três problemas fundamentais colocados por Dehn em 1912. Dado um grupo  $G$  com um conjunto gerador  $X$ , dizemos que o *problema da palavra* é decidível (ou solúvel) se *existe* um algoritmo tal que para todo par  $(a, b)$  de palavras em  $X \cup X^{-1}$  nos responde se elas representam o mesmo elemento em  $G$ . É claro que isto é equivalente a decidir se uma palavra arbitrária  $g = ab^{-1}$  em  $X \cup X^{-1}$  representa o elemento trivial em  $G$ . Um algoritmo aceitável é um que responda ‘sim’ ou ‘não’. Se um tal algoritmo *não existe*, então dizemos que o problema da palavra é *indecidível* (ou insolúvel) para tal grupo.

O segundo dos problemas de Dehn é o chamado problema da conjugação, que

pergunta se existe algoritmo que para dados  $a, b \in G$  decide se estes são conjugados ou não em  $G$ . Tal como no caso anterior, dizemos que o problema é decidível (resp. indecidível) se um tal algoritmo existe (resp. não existe). O terceiro, e mais árduo, dos problemas propostos por Dehn é o problema do isomorfismo que pergunta se existe algoritmo que decide se dois grupos dados são isomorfos ou não.

É claro que se o problema da conjugação for decidível para um certo grupo  $G$ , também o é o problema da palavra. Também é intuitivo e plausível que o problema da conjugação seja intrinsecamente mais difícil do que o problema da palavra, pois, este contém uma variável ‘existencial’ extra, já que perguntamos sobre a existência de um elemento  $h$  tal que  $h^{-1}ahb^{-1}$  represente o elemento trivial em  $G$ . Esta intuição está correta, pois existem grupos finitamente apresentados com problema da palavra decidível mas com problema da conjugação indecidível conforme Fridman [Fri60], Collins [CM69], Miller [Mil71].

Quando  $G$  é finitamente gerado e  $H$  é um subgrupo (finitamente gerado) de  $G$ , então é bem sabido que se  $G$  tiver problema da palavra decidível,  $H$  também o tem. O inverso é falso em geral, mas é verdade quando  $H$  é de índice finito em  $G$ . Entretanto Collins e Miller mostraram em [CM77] que as respectivas afirmações são falsas se “problema palavra” for substituído por “problema da conjugação”, mesmo sob a hipótese de que  $H$  é de índice finito (igual 2) em  $G$ . Ou seja, a propriedade de ter problema da conjugação decidível nem sempre pode ser estendida do subgrupo para o grupo (como era de se esperar) e nem tampouco é preservada por imersão, o que é um pouco surpreendente. Como consequência, ao tratar o problema da conjugação para a sequência  $Pol(-1) < Pol(0) < Pol(1) < \dots < Pol(m) < \dots < Pol(\infty) < \mathcal{A}_f < \mathcal{A}_{fr} < \mathcal{A}$  teremos que utilizar fortemente a estrutura particular de cada um desses subgrupos, já que a decidibilidade do problema da conjugação não é preservada por imersão.

A decidibilidade do problema da palavra para  $\mathcal{A}_f$  segue da seguinte observação: dado um automorfismo, basta analisar a ação de cada um de seus estados sobre as sequências de comprimento 1 de  $Y$ . Também é imediato que este é decidível para todo subgrupo de  $\mathcal{A}_f$ . Já o problema da conjugação vem sendo tratado para certos subgrupos bem conhecidos de  $Pol(0)$ , como os  $p$ -grupos de Grigorchuk e Gupta-Sidki, bem como para os livre-de-torção Brunner-Sidki-Vieira e Basílica, e foi generalizado em [Ale83, GW00] para certas classes de grupos galhados e seus subgrupos de índice finito. Recentemente foi apresentado em [SV] um exemplo

de um subgrupo finitamente gerado, fechado por estados de  $\mathcal{A}_f$  com problema da conjugação indecidível. Contudo o problema continua em aberto para  $\mathcal{A}_f$ , bem como para  $Pol(m)$ ,  $m > 0$ .

Neste trabalho mostramos que o problema da conjugação é decidível para  $Pol(0)$ . Mais que isso, apresentamos algoritmos que não só decidem se dois elementos são conjugados, mas que em caso afirmativo também exhibe um conjugador.

A abordagem geral pode ser sumarizada da seguinte forma: ao lidarmos com o problema da conjugação para certo par de automorfismos de  $Pol(0)$ , nos restringimos às permutações induzidas por estes sobre as palavras de comprimento 1 em  $Y$ , ou seja, neste primeiro momento estamos lidando com um problema da conjugação em  $Sym(Y)$ , onde  $Y$  é um conjunto finito. Como consequência, o problema inicial é reduzido para certos subproblemas da conjugação, porém sobre os estados destes automorfismos. Utilizando o fato de que cada estado é novamente um automorfismo de  $\mathcal{T}$  e de que estamos trabalhando em grupos fechados por estados, recaímos novamente em certos problemas da conjugação em  $Pol(0)$ , os quais podem ser tratados da mesma forma que o problema inicial. A solução do problema da conjugação para o par inicial é uma consequência do fato de que os automorfismos em questão têm crescimento limitado.

Mais precisamente, os problemas da ordem e da conjugação nos levam à seguinte definição: Para um automorfismo  $a \in \mathcal{A}$  consideremos as órbitas  $Orb_a(v)$  da sua ação sobre os vértices  $v$  da árvore e defina o conjunto

$$OS(a) = \{a^m|_v \mid v \in Y^*, m = |Orb_a(v)|\} \quad (1)$$

que chamamos de *senalizador de órbita* de  $a$ . Em nosso trabalho demonstramos que o problema da ordem é decidível para automorfismos de finitos estados com sinalizadores de órbita finitos. É um resultado de Nekrashevych [Nek05], para o qual apresentamos uma demonstração alternativa, que automorfismos de crescimento limitado têm sinalizadores de órbita finitos, de onde segue a decidibilidade do problema da ordem para  $Pol(0)$ .

Já o problema da conjugação, nós o tratamos primeiramente no grupo  $\mathcal{A}$ . Apresentamos um procedimento que para dados dois automorfismos  $a, b \in \mathcal{A}$ , constrói um *grafo conjugador*  $\Psi(a, b)$ , a partir dos conjuntos  $OS(a), OS(b)$ , que retrata a inter-dependência entre os diferentes subproblemas da conjugação encontrados quando buscamos um conjugador para o par  $a, b$ . A construção de um conjugador



(no caso em eles são conjugados) é uma consequência do fato de que, embora existam infinitos conjugadores para o par  $a, b$ , o grafo  $\Psi(a, b)$  é finito. Formalmente, obtemos o seguinte resultado.

**Teorema 0.0.1** *Dois automorfismos de finitos estados  $a, b$  com sinalizadores de órbita finitos são conjugados em  $\mathcal{A}$  se, e somente se, são conjugados em  $\mathcal{A}_{fr}$  se, e somente se, o grafo conjugador  $\Psi(a, b)$  é não vazio.*

Uma classe importante de grupos fechados por estados são os grupos contráteis. Um grupo de automorfismo  $G$  é chamado contrátil se existe um conjunto finito  $\mathcal{N} \subset G$  tal que para todo  $\alpha \in G$  existe um inteiro positivo  $k$  para o qual vale que  $\alpha|_u \in \mathcal{N}$  para todo  $u \in Y^*$  com  $|u| > k$ . Um automorfismo de finitos estados é chamado contrátil se o grupo fechado por estados gerado por seus estados for contrátil. Tal propriedade é essencial no processo de obtenção de cotas superiores para a função de crescimento de palavras dos grupos gerados por autômatos e como consequência temos exemplos clássicos de grupos de crescimento intermediário. É um resultado de [BN03], fortemente usado em nosso trabalho, que automorfismos de crescimento limitado são contráteis.

**Teorema 0.0.2** *Dois automorfismos contráteis com sinalizadores de órbita finitos são conjugados em  $\mathcal{A}$  se, e somente se, são conjugados em  $\mathcal{A}_{fr}$ .*

Provamos ainda uma série de resultados para o problema da conjugação de automorfismos de crescimento limitado os quais resumizamos no seguinte teorema.

**Teorema 0.0.3** *1. O problema da conjugação (simultâneo) para automorfismos de crescimento limitado é decidível em  $\mathcal{A}$ .*

*2. Dois automorfismos de crescimento limitado são conjugados em  $\mathcal{A}$  se, e somente se, são conjugados em  $\mathcal{A}_{fr}$ .*

*3. O problema da conjugação (simultâneo) em  $Pol(0)$  é decidível.*

*4. Dois automorfismos de crescimento limitado são conjugados no grupo  $Pol(\infty)$  se, e somente se, são conjugados em  $Pol(0)$ .*

Porfim, apresentamos alguns exemplos que ilustram como executar os algoritmos a fim de obter solução do problema de conjugação, e descrevem a conexão existente entre a propriedade de ter sinalizador de órbita finito e outras propriedades notáveis de automorfismos.

Os resultados apresentados no terceiro capítulo podem ser encontrados em [BBSZ].

# Capítulo 1

## Preliminares

Os resultados deste capítulo podem ser encontrados em [Sid98], [Nek05], [Gri80], [GS83], [BSV99] e [Sid00].

### 1.1 Árvores enraizadas

Um *grafo* (não dirigido) é um par  $\Gamma = (V, E)$  onde  $V$  é um conjunto não vazio de objetos denominados vértices e  $E$  é uma coleção de pares não ordenados de elementos de  $V$ , denominados arestas.

Um *grafo simplicial*  $\Gamma$  é definido por um conjunto de vértices  $V$  e um conjunto de arestas  $E$ , onde cada aresta é um par  $\{v_1, v_2\}$  de dois vértices distintos. Dois vértices  $v_1$  e  $v_2$  do grafo simplicial  $\Gamma$ , são ditos adjacentes se o conjunto  $\{v_1, v_2\}$  for uma aresta deste grafo.

Um *morfismo* entre dois grafos simpliciais  $\Gamma_1$  e  $\Gamma_2$  é uma aplicação  $\alpha : V(\Gamma_1) \rightarrow V(\Gamma_2)$  tal que, para toda aresta  $\{v_1, v_2\}$  de  $\Gamma_1$  o conjunto  $\{\alpha(v_1), \alpha(v_2)\}$  é uma aresta do grafo  $\Gamma_2$ . No caso em que o morfismo  $\alpha$  é uma bijeção cuja inversa também é um morfismo, dizemos que  $\alpha$  é um isomorfismo. Se além disso,  $\Gamma_1 = \Gamma_2$  dizemos que  $\alpha$  é um automorfismo.

**Definição 1.1.1** *Uma árvore uni-raiz (ou enraizada)  $\mathcal{T}$  é um grafo simplicial conexo*

sem caminhos fechados (circuitos) com um vértice distinguindo  $v_\phi$ , chamado raiz. Um isomorfismo entre duas árvores uni-raiz é um isomorfismo entre os grafos simpliciais que leva raiz em raiz.

Toda árvore enraizada  $\mathcal{T}$  pode ser definida por uma sequência de conjuntos disjuntos e aplicações

$$M_0 \xleftarrow{f_1} M_1 \xleftarrow{f_2} M_2 \dots,$$

onde  $M_0 = \{v_\phi\}$  contém apenas a raiz,  $\cup_{n \geq 0} M_n = V$  é o conjunto dos vértices e todo  $v \in M_n$  é ligado por uma aresta ao vértice  $f_n(v) \in M_{n-1}$ . O conjunto  $M_n$  é chamado  $n$ -ésimo nível da árvore  $\mathcal{T}$  e é definido como o conjunto dos vértices que estão a uma distância  $n$  da raiz.

Uma árvore enraizada  $\mathcal{T}$  é dita  $d$ -regular se todo ponto  $v \in M_n$  tem exatamente  $d$  preimagens pela aplicação  $f_{n+1}$ , para todo  $n$ .

## 1.2 O grupo $\mathcal{A}$

Iniciamos nossa construção tomando um conjunto não vazio  $Y$ , chamado alfabeto e  $M = Y^*$  o conjunto de todas as palavras finitas em  $Y$ . Considerando em  $M$  a operação justaposição de elementos, denotada por  $\cdot$ , é imediata a verificação de que a operação  $\cdot$  é associativa e de que seu elemento neutro é a sequência vazia representada por  $\phi$ . Desta forma,  $(M, \cdot)$  é o monoide livre gerado por  $Y$ . Observemos que  $M$  possui uma estrutura natural de árvore, uma vez que cada palavra  $u \in M$  pode ser conectada à palavra  $uy$  para todo  $y \in Y$ . Tal árvore, denotada por  $\mathcal{T} = \mathcal{T}_Y$ , é definida pela sequência

$$M_0 \xleftarrow{f_1} M_1 \xleftarrow{f_2} M_2 \xleftarrow{f_3} \dots,$$

onde  $f_n(y_1 y_2 \dots y_n) = y_1 y_2 \dots y_{n-1}$  e  $M_t$  é o conjunto de todas as palavras em  $Y$  de comprimento  $t$ .

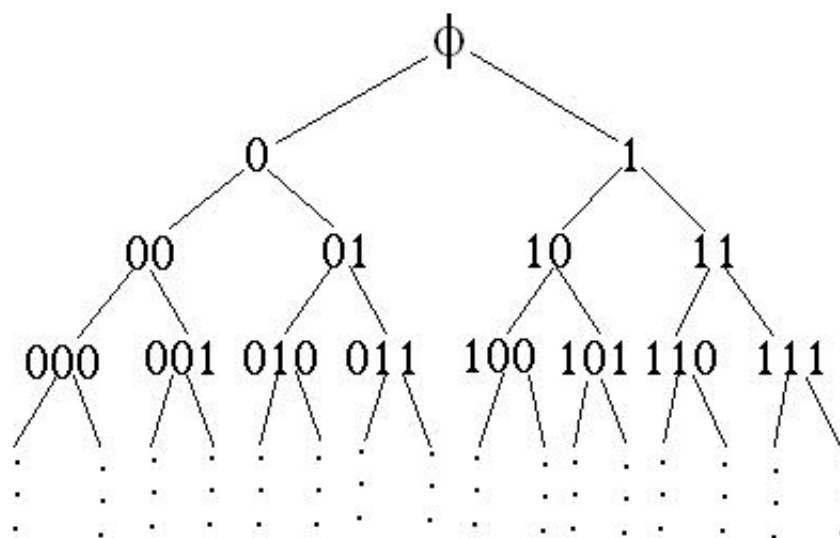


Figura 1.1: A árvore regular binária uni-raiz  $\mathcal{T}_2$

Quando  $|Y| = d$ ,  $\mathcal{T}$  é  $d$ -regular, mais ainda, toda árvore  $d$ -regular é isomorfa a  $\mathcal{T}$ . Neste caso por simplicidade tomamos  $Y = \{0, 1, \dots, d-1\}$ , denotamos o grafo de  $(M, \cdot)$  por  $\mathcal{T}_d$  e chamamos de *árvore regular  $d$ -ária uni-raiz*.

Observemos ainda que  $M$  admite uma ordenação parcial definida da seguinte forma: dados  $u, v \in M$ ,

$$v \leq u \text{ se, e somente se, } u \text{ é prefixo de } v.$$

Notemos que  $\mathcal{T}$  é precisamente o grafo de  $(M, \leq)$ .

Denotando por  $|u|$  o comprimento de um elemento  $u \in M$ , podemos definir uma métrica por

$$d(u, v) = |u| + |v| - 2|w|,$$

onde  $u, v \in M$  e  $w$  é o maior prefixo comum entre  $u$  e  $v$ . Desta forma,  $(M, d)$  é um espaço métrico.

Quando consideramos o conjunto de todos os automorfismos da árvore uni-raiz  $\mathcal{T}$ , este forma um grupo com a operação de composição de funções, denotado por  $\mathcal{A} = \text{Aut}(\mathcal{T})$  e chamado de *grupo dos automorfismos da árvore regular uni-raiz  $\mathcal{T}$* .

Contudo, podemos dar uma outra interpretação para  $\mathcal{A}$ : ele pode ser visto como o grupo das isometrias do espaço métrico  $(M, d)$ , já que:

**Lema 1.2.1** *Uma bijeção  $\alpha : M \rightarrow M$  é um automorfismo da árvore  $\mathcal{T}$  se, e somente se, para todo  $n \geq 0$ ,  $(M_n)^\alpha = M_n$  e*

$$(f_n(v))^\alpha = f_n(v^\alpha), \forall v \in M_n.$$

**Lema 1.2.2** *Dado  $n$  inteiro positivo fixo, o conjunto  $\text{Stab}_{\mathcal{A}}(n) = \{\alpha \in \mathcal{A} \mid v^\alpha = v, \forall v \in M_n\}$  de todos os automorfismos que fixam as palavras de comprimento  $n$ , é um subgrupo de  $\mathcal{A}$  e chamado de estabilizador do  $n$ -ésimo nível de  $\mathcal{A}$ .*

Os exemplos mais simples de automorfismos de  $\mathcal{T}$  são oriundos de permutações do conjunto  $Y$ . De fato, dada uma permutação  $\sigma$  de  $Y$ , ela pode ser estendida rigidamente para um automorfismo da árvore  $\mathcal{T}$  da seguinte maneira:

$$(y.v)^\sigma = (y)^\sigma.v, \forall y \in Y, \forall v \in M.$$

Desta forma, conseguimos uma imersão de  $\text{Sym}(Y)$ , o grupo de todas as permutações do conjunto  $Y$ , em  $\mathcal{A}$ .

### 1.2.1 A estrutura de $\mathcal{A}$ como produto entrelaçado

**Definição 1.2.3** *Sejam  $H$  um grupo agindo por permutação sobre um conjunto  $Y$  e  $G$  um grupo arbitrário. O produto entrelaçado permutacional de  $G$  por  $H$ ,  $G \text{wr}_Y H$ , é o produto semi-direto  $G^Y \rtimes H$ , onde  $H$  age sobre o produto direto  $G^Y$  permutando os fatores segundo a ação de  $H$  sobre  $Y$ .*

O Lema (1.2.1) assegurou que uma bijeção  $\alpha : \mathcal{T} \rightarrow \mathcal{T}$  é um automorfismo se, e somente se, preserva o comprimento das palavras e para todo  $y_1 y_2 \dots y_n \in M_n$  existe  $y \in Y$  tal que  $(y_1 y_2 \dots y_n)^\alpha = (y_1 y_2 \dots y_{n-1})^\alpha y$ . Isso implica que para todo  $v \in \mathcal{T}$  e

$u \in M_n$ , existe  $w \in M_n$  tal que  $(vu)^\alpha = v^\alpha w$ . Mais ainda, temos do Lema (1.2.1) que a aplicação  $u \mapsto w$  é também um automorfismo da árvore  $\mathcal{T}$ . Denotamos este automorfismo por  $\alpha|_v$  e chamamos de estado de  $\alpha$  em  $v$  ou ainda, dizemos que  $\alpha|_v$  é um estado de  $\alpha$ .

Por outro lado, cada automorfismo  $\alpha \in \mathcal{A}$  induz uma permutação  $\pi_\alpha$  sobre  $Y$ , a qual podemos identificar como um automorfismo de  $\mathcal{A}$  pela imersão de  $Sym(Y)$  em  $\mathcal{A}$ . Podemos então escrever  $\alpha = \alpha' \pi_\alpha$ , onde  $\alpha'$  é um automorfismo que fixa  $Y$  pontualmente. Observemos agora que para cada  $y \in Y$ ,  $\alpha'$  induz o automorfismo  $\alpha|_y$  sobre a subárvore  $y\mathcal{T}_d$ . Considerando o isomorfismo natural de  $\mathcal{T}_d$  em  $y\mathcal{T}_d$  podemos identificar  $\alpha|_y$  com um elemento de  $\mathcal{A}$ , de onde segue o seguinte resultado:

**Proposição 1.2.4** *O grupo  $\mathcal{A}$ , de todos os automorfismos de  $\mathcal{T}_Y$ , é isomorfo ao produto entrelaçado permutacional  $\text{Awr}_Y \text{Sym}(Y)$ . Mais precisamente,*

$$\begin{aligned} \mathcal{A} &\xrightarrow{\sim} (\mathcal{A} \times \dots \times \mathcal{A}) \rtimes \text{Sym}(Y) \\ \alpha &\mapsto (\alpha|_0, \alpha|_1, \dots, \alpha|_{d-1}) \pi_\alpha \end{aligned} \quad (1.1)$$

onde  $\pi_\alpha$  é a permutação induzida por  $\alpha$  sobre  $Y$  e  $\alpha|_y$  é o automorfismo induzido por  $\alpha'$  sobre a subárvore  $y\mathcal{T}_d$ .

Segue deste isomorfismo que o produto de dois automorfismos  $\alpha = (\alpha|_0, \alpha|_1, \dots, \alpha|_{d-1}) \pi_\alpha$  e  $\beta = (\beta|_0, \beta|_1, \dots, \beta|_{d-1}) \pi_\beta$  de  $\mathcal{T}_d$  é descrito por

$$\alpha\beta = (\alpha|_0\beta|_{0^{\pi_\alpha}}, \alpha|_1\beta|_{1^{\pi_\alpha}}, \dots, \alpha|_{d-1}\beta|_{(d-1)^{\pi_\alpha}}) \pi_\alpha \pi_\beta.$$

O automorfismo inverso de  $\alpha = (\alpha|_0, \alpha|_1, \dots, \alpha|_{d-1}) \pi_\alpha$  em  $\mathcal{T}_d$  é dado por

$$\alpha^{-1} = ((\alpha|_{0^{\pi_\alpha^{-1}}})^{-1}, (\alpha|_{1^{\pi_\alpha^{-1}}})^{-1}, \dots, (\alpha|_{(d-1)^{\pi_\alpha^{-1}}})^{-1}) \pi_\alpha^{-1}.$$

**Notação 1.2.5** *Dado  $\alpha = \alpha' \pi_\alpha$ , onde  $\pi_\alpha$  é a permutação induzida por  $\alpha$  em  $Y$  e  $\alpha'$  está no estabilizador do primeiro nível, então chamaremos  $\alpha'$  de  $f^{(1)}(\alpha)$  e  $\pi_\alpha$  de  $\pi_\alpha^{(0)}$ . De modo geral escrevemos  $\alpha = f^{(k)}(\alpha) \pi_\alpha^{(k-1)}$ , quando  $\pi_\alpha^{(k-1)}$  for a permutação induzida por  $\alpha$  nas palavras de comprimento menor ou igual a  $k$ , e  $f^{(k)}(\alpha)$  estiver no estabilizador  $k$ -ésimo nível de  $\mathcal{T}_d$ ,  $\text{Stab}_{\mathcal{A}}(k)$ .*

**Definição 1.2.6** *Se  $G \leq \mathcal{A}$  é tal que  $G \cong \text{GwrySym}(Y)$ , dizemos que  $G$  é estratificado.*

Em particular, uma consequência do isomorfismo (1.1) é que  $\mathcal{A}$  é estratificado.

Observemos que segue das observações feitas acima que a ação de um automorfismo  $\alpha$  em  $\mathcal{T}_d$  é dada por

$$(yu)^\alpha = (y)^{\pi_\alpha}(u)^{\alpha|_y}, \forall y \in Y, \forall u \in M,$$

onde  $\pi_\alpha$  é a permutação induzida por  $\alpha$  sobre  $Y$  e  $\alpha|_y$  é o automorfismo induzido por  $f^{(1)}(\alpha) \in \text{Stab}_{\mathcal{A}}(1)$  sobre a subárvore  $y\mathcal{T}_d$ .

**Definição 1.2.7** *Dado  $\alpha \in \mathcal{A}$ , o conjunto  $Q(\alpha) = \{\alpha|_u; u \in M\}$  é denominado o conjunto dos estados de  $\alpha$ .*

Quaisquer que sejam os automorfismos  $\alpha, \beta$  é facilmente verificável que seus estados satisfazem

$$Q(\alpha^{-1}) = Q(\alpha)^{-1}, Q(\alpha\beta) \subseteq Q(\alpha)Q(\beta) \quad (1.2)$$

Mais precisamente, com relação a  $\alpha, \beta$  e seus estados, as seguintes propriedades se verificam:

$$\begin{aligned} (vu)^\alpha &= v^\alpha u^{\alpha|_v} \\ \alpha|_{(vu)} &= (\alpha|_v)|_u \\ (\alpha\beta)|_v &= (\alpha|_v)(\beta|_{v^\alpha}) \\ (\alpha^{-1})|_v &= (\alpha|_{v^{\alpha^{-1}}})^{-1}. \end{aligned}$$

## 1.2.2 Grupos fechados por estados

Ao calcular o produto de dois automorfismos da árvore regular  $d$ -ária uni-raiz  $\mathcal{T}_d$ , certamente temos de calcular o produto de seus estados, os quais são automorfismos



que não estão necessariamente dentro do grupo gerado pelos dois primeiros. Dizemos que  $G$ , um grupo de automorfismo de  $\mathcal{T}_d$ , é fechado por estados se os estados dos seus elementos ainda permanecem em  $G$ . Veremos abaixo que qualquer grupo de automorfismos  $G$ , fechado por estados, pode ser visto como subgrupo do produto entrelaçado permutacional de  $G$  por  $Sym(Y)$ .

Generalizamos esse conceito na seguinte definição.

**Definição 1.2.8** *Uma ação de um grupo  $G$  sobre a árvore  $\mathcal{T}$  é dita fechada por estados se para todo  $\alpha \in G$  e  $y_1 \in Y$  existe  $\beta \in G$  e  $y_2 \in Y$  tais que*

$$(y_1 w)^\alpha = y_2 (w^\beta), \forall w \in \mathcal{T}.$$

Um grupo de automorfismos da árvore  $\mathcal{T}$  é dito fechado por estados se, e somente se, para todo  $g \in G$  o estado  $g|_y$  está em  $G$  para todo  $y \in Y$ .

Para todo  $G \leq \mathcal{A}$ , fechado por estados podemos definir de maneira natural um homomorfismo  $\phi : G \rightarrow Gwr_Y Sym(Y)$  pela fórmula  $\phi(\alpha) = \alpha' \pi_\alpha$ , onde  $\pi_\alpha$  é a permutação induzida por  $\alpha$  sobre  $Y$ , e  $\alpha' = (\alpha|_y)_{y \in Y} \in Stab_{\mathcal{A}}(1)$ , induz o automorfismo  $\alpha|_y$  sobre a subárvore  $y\mathcal{T}_d$ . Segue então que

$$\phi(\alpha) = (\alpha|_0, \alpha|_1, \dots, \alpha|_{d-1}) \pi_\alpha. \quad (1.3)$$

Observe que o homomorfismo  $\phi$  é injetivo e em particular, temos o isomorfismo (1.1) como consequência:

$$\begin{aligned} \phi : \mathcal{A} &\xrightarrow{\sim} (\mathcal{A} \times \dots \times \mathcal{A}) \rtimes Sym(Y) \\ \alpha &\longmapsto (\alpha|_0, \alpha|_1, \dots, \alpha|_{d-1}) \pi_\alpha \end{aligned} \quad (1.4)$$

onde  $\alpha|_y$  é o automorfismo induzido por  $\alpha'$  sobre a subárvore  $y\mathcal{T}_d$ .

Em outra direção, se temos um homomorfismo  $\phi : G \rightarrow Gwr_Y Sym(Y)$ , então este define uma ação fechada por estados do grupo  $G$  na árvore  $\mathcal{T}$  pela fórmula

$$(yv)^\alpha = y^{\pi_\alpha} v^{\alpha|_y}, \text{ onde, } \phi(\alpha) = (\alpha|_0, \alpha|_1, \dots, \alpha|_{d-1}) \pi_\alpha.$$

Observemos que esta ação, em geral, não é fiel.

Se um grupo não é fechado por estados, podemos tomar seu fecho por estados, embora propriedades tais como “ser finitamente gerado” possam não ser preservadas. Grupos finitamente gerados fechados por estados, são subgrupos de um importante grupo enumerável o qual apresentaremos na próxima seção: *o grupo dos automorfismos funcionalmente recursivos*,  $\mathcal{A}_{fr}$ .

### 1.2.3 Automorfismos funcionalmente recursivos

**Definição 1.2.9** *Seja  $S = \{\alpha, \beta, \dots\}$  um subconjunto de  $\mathcal{A}$ .*

- *Dizemos que  $S$  é funcionalmente recursivo se cada estado de cada elemento de  $S$  pode ser escrito como uma palavra nos elementos de  $S$ .*
- *Um grupo  $G$  é dito funcionalmente recursivo se existe um subconjunto finito funcionalmente recursivo que o gera.*
- *Um automorfismo  $g$  é dito funcionalmente recursivo se o grupo gerado por todos os seus estados for funcionalmente recursivo.*

Em particular, se um conjunto finito de automorfismo  $g_1, g_2, \dots, g_m$  for *funcionalmente recursivo* então existem palavras  $w_{ij}$  em  $\{g_1^{\pm 1}, g_2^{\pm 1}, \dots, g_m^{\pm 1}\}$  e permutações  $\pi_i \in \text{Sym}(Y)$  tais que

$$\begin{aligned} g_1 &= (w_{11}, w_{12}, \dots, w_{1d})\pi_1 \\ g_2 &= (w_{21}, w_{22}, \dots, w_{2d})\pi_2 \\ &\vdots \\ g_m &= (w_{m1}, w_{m2}, \dots, w_{md})\pi_m. \end{aligned}$$

Esse sistema tem uma solução única no grupo  $\mathcal{A}$ , onde a ação de cada elemento  $g_i$  sobre o primeiro nível da árvore  $\mathcal{T}$  é dada pela permutação  $\pi_i$ , e a ação dos estados  $(g_i)|_j$  é unicamente definido pelas palavras  $w_{ij}$ .

---

**Proposição 1.2.10** *Seja  $G$  um subgrupo de  $\mathcal{A}$  gerado por um conjunto finito  $S$ . Então,  $G$  é fechado por estados se, e somente se,  $S$  for funcionalmente recursivo.*

**Demonstração:** Seja  $S = \{\alpha, \beta, \dots, \gamma\}$ . Suponhamos que  $G$  seja fechado por estados. Seja  $\alpha|_i$  um estado de  $\alpha$ . Como todos os estados de  $\alpha$  são elementos de  $G$ , temos que  $\alpha|_i \in G$  e pode ser escrito como uma palavra no conjunto gerador  $S$ . Por outro lado, suponhamos  $S$  funcionalmente recursivo. Para mostrar que cada estado de cada elemento de  $G$  ainda está em  $G$ , basta mostrar, que cada estado de um elemento arbitrário do conjunto gerador  $S$  está em  $G$ . De fato, se  $\delta$  é um estado de um elemento de  $S$ , pela definição de conjunto funcionalmente recursivo,  $\delta$  é uma palavra em  $S$ , estando portanto em  $G$ . ■

É uma consequência das equações (1.2) e (1.3) o seguinte resultado.

**Teorema 1.2.11** *O conjunto de todos os automorfismos funcionalmente recursivos, denotado por  $\mathcal{A}_{fr}$ , é um subgrupo estratificado de  $\mathcal{A}$ .*

## 1.2.4 Autômatos

Autômatos são modelos matemáticos abstratos de máquinas que executam cálculos em uma entrada movendo-se através de uma série de estados e funções de transição. Tais estruturas aparecem naturalmente no processo de solução de vários problemas práticos. Diferentes tipos de autômatos (autômatos determinísticos, à pilha, de Mealy e máquinas de Turing) foram desenvolvidos em conexão com computabilidade, complexidade computacional, linguagens formais etc.

**Definição 1.2.12** *Um autômato de Mealy é uma máquina de Turing definida sobre a sextupla  $(Q, L, \Gamma, f, l, q_0)$ , onde  $Q$  é o conjunto de estados,  $L$  é o alfabeto de entrada,  $\Gamma$  é o alfabeto de saída,  $f : Q \times L \rightarrow Q$  é a função de transição dos estados,  $l : Q \times L \rightarrow \Gamma$  é a função de saída e  $q_0$  é o estado inicial.*

## Interpretação de automorfismos como autômatos

Um automorfismo  $\alpha$  da árvore  $\mathcal{T}_d$  pode ser interpretado de uma maneira simples como um autômato de Mealy. A sextupla será  $(Q(\alpha), Y, Y, f, l, \alpha)$ , ou seja, o conjunto de estados é o já definido  $Q(\alpha)$ ; o conjunto  $Y$  representa tanto o alfabeto de entrada quanto o de saída;  $\alpha$  é o estado inicial e as funções de transição e de saída são definidas através da igualdade  $(y_1 y_2 \dots y_t)^\beta = y_1^\beta (y_2 \dots y_t)^{\beta|_{y_1}}$  onde  $\beta \in \mathcal{A}$ ,  $y_i \in Y$  e  $t > 0$ , conforme descrito abaixo.

A função de transição dos estados é definida por

$$\begin{aligned} f : Q(\alpha) \times Y &\longrightarrow Q(\alpha) \\ (\beta, y) &\longmapsto \beta|_y \end{aligned}$$

e a função de saída por

$$\begin{aligned} l : Q(\alpha) \times Y &\longrightarrow Y \\ (\beta, y) &\longmapsto (y)^\beta \end{aligned}$$

### 1.2.5 Automorfismos de finitos estados

**Definição 1.2.13** *Um automorfismo  $\alpha \in \mathcal{A}$  é dito **automorfismo de finitos estados** se o conjunto  $Q(\alpha)$  contém um número finito de elementos.*

É uma consequência das equações (1.2) e (1.3), o seguinte resultado.

**Teorema 1.2.14** *O conjunto dos automorfismos de finitos estados, denotado por  $\mathcal{A}_f$ , é um subgrupo estratificado de  $\mathcal{A}$ .*

Um importante exemplo de automorfismo de finitos estados é o chamado máquina de adição binária.

**Exemplo 1.2.15 (Máquina de adição binária)** *Tomando  $Y$  binário, ou seja,  $Y = \{0, 1\}$  e  $\tau$  o automorfismo de  $\mathcal{T}_2$  definido por  $\tau = (e, \tau)\sigma$ , onde  $\sigma$  é a extensão da permutação  $(0, 1)$  para um automorfismo de  $\mathcal{T}_2$ , podemos observar que*

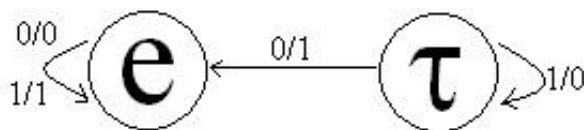


Figura 1.2: máquina de adição binária

$(0u)^\tau = 1(u^e)$  e  $(1u)^\tau = 0(u^\tau)$ , isto é, a ação de  $\tau$  é equivalente a somar 1 (pela esquerda) módulo 2.

Os estados de  $\tau$  são  $Q(\tau) = \{\tau, e\}$ , ou seja,  $\tau$  é um automorfismo de finitos estados.

**Observação 1.2.16** Observemos que  $\tau$  é funcionalmente recursivo. De modo geral, todo automorfismo de  $\mathcal{A}_f$  é funcionalmente recursivo, donde temos que  $\mathcal{A}_f < \mathcal{A}_{fr}$ . Contudo, tal inclusão é estrita, como mostra o exemplo a seguir.

**Exemplo 1.2.17** O automorfismo  $\alpha = (\alpha, \alpha^2)\sigma$  é funcionalmente recursivo mas não é de finitos estados, conforme mostra a figura 1.3.

### Automorfismos contráteis

**Definição 1.2.18** Consideremos um grupo de automorfismos  $G$  fechado por estados. Dizemos que  $G$  é contrátil se existe um conjunto finito  $\mathcal{N} \subset G$  tal que para todo  $\alpha \in G$  existe um inteiro positivo  $k$  tal que,  $\alpha|_u \in \mathcal{N}$  para todo  $u \in Y^*$  com  $|u| > k$ .

O conjunto  $\mathcal{N}$  minimal com essa propriedade é chamado *núcleo* de  $G$ .

**Definição 1.2.19** Um automorfismo de finitos estados é chamado *contrátil* se o grupo fechado por estados gerado por seus estados for contrátil.

**Observação 1.2.20** É uma consequência da definição acima que grupos contráteis possuem finitos estados.

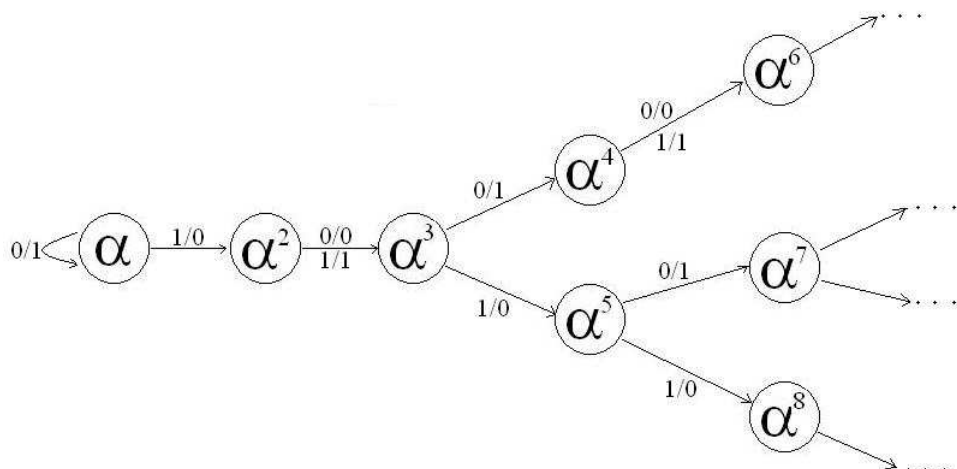


Figura 1.3:  $\alpha \in \mathcal{A}_{fr} \setminus \mathcal{A}_f$

### 1.3 Crescimento de autômatos: o grupo $Pol(0)$

Um problema central da teoria de grupos gerados por autômatos é a conexão existente entre a estrutura de um autômato como grafo orientado e as propriedades algébricas do grupo que ele gera. Considerando a estrutura cíclica dos autômatos, Sidki em [Sid00], introduziu várias classes de autômatos finitos e, em particular,  $Pol(0)$  os chamados autômatos de crescimento limitado. Embora  $Pol(0)$  seja um grupo muito menor do que o grupo de todos os automorfismos de finitos estados, ele é suficientemente grande, no sentido de que contém a maioria dos grupos gerados por autômatos estudados nos últimos anos, como os grupos de Gupta-Sidki [GS83], Grigorchuk [Gri80], Brunner-Sidki-Vieira [BSV99], Basílca [GZ02] dentre outros.

#### 1.3.1 A função $\theta$ de crescimento de autômatos

Seja  $D(\alpha)$  autômato associado a certo automorfismo  $\alpha$  de finitos estados. Se o automorfismo identidade for um estado de  $\alpha$ , removamos este de  $D(\alpha)$  junto com todas as arestas que incidem neste, produzindo um novo grafo  $D(\alpha)'$ . Para tais  $\alpha$  podemos definir a função  $\theta(\alpha, k)$ , em  $k$ , que conta o número de caminhos direcionados em  $D(\alpha)'$  começando em  $\alpha$  e tendo comprimento  $k$ . Alternativamente esta pode ser

definida como o número de palavras  $v \in M$  de comprimento  $k$  para as quais  $\alpha|_v \neq e$ .

A matriz de adjacência  $[\alpha]$  de  $\alpha$  é definida por  $[\alpha]_{\gamma\delta} = \#\{y \in Y \mid \delta = \gamma|_y\}$  para todo  $\gamma, \delta \in Q(\alpha) \setminus \{e\}$ ; ao ordenar  $Q(\alpha) \setminus \{e\}$ , escolhemos  $\alpha$  como o primeiro elemento.  $\theta(\alpha, k)$  é precisamente a primeira entrada do vetor  $[\alpha]^k \cdot \epsilon$ , onde  $\epsilon$  é o vetor  $(1, 1, \dots, 1)$  transposto. A importância geométrica do crescimento de autômatos finitos provém do seguinte fato que pode ser encontrado em [Ufn91]:

**Proposição 1.3.1** *Sejam  $D$  um grafo direcionado finito e  $v$  um vértice de  $D$  através do qual todos os outros vértices de  $D$  podem ser alcançados através de caminhos direcionados partindo de  $v$ . Então o crescimento dos caminhos direcionados de  $D$  começando em  $v$  é ou polinomial ou exponencial. O crescimento é exponencial se, e somente se, existem dois circuitos direcionados distintos com um vértice comum. O crescimento é polinomial de grau  $m$ , se este não for exponencial, o número de circuitos minimais distintos em qualquer caminho for no máximo  $m + 1$  e existir pelo menos um caminho com este número de circuitos.*

Como consequência temos o seguinte resultado.

**Corolário 1.3.2** *Seja  $\alpha$  um automorfismo de finitos estados. Então  $\theta(\alpha, k)$  como função de  $k$ , cresce polinomialmente ou exponencialmente.*

**Observação 1.3.3** *Dado um automorfismo  $\alpha$ , se seu autômato tem crescimento polinomial de grau  $m$ , então denotaremos tal grau por  $\partial(\alpha) = m$  e diremos que  $\alpha$  tem crescimento polinomial de grau  $m$ .*

**Proposição 1.3.4** *Para todo  $m \geq 0$ , o conjunto  $Pol(m)$  de todos os automorfismos de crescimento polinomial de grau  $m$  é um grupo estratificado, ou seja,*

$$Pol(m) \cong (Pol(m) \times Pol(m) \times \dots \times Pol(m)) \rtimes Sym(Y).$$

**Demonstração:** Sejam  $\alpha, \beta \in Pol(m)$ . Então, existem  $c_1, c_2 > 0$  tais que  $\theta(\alpha, k) \leq c_1 k^m$  e  $\theta(\beta, k) \leq c_2 k^m$ , para todo  $k$ .

Recordemos que  $f^{(k)}(\alpha)$  foi definido na Notação 1.2.5. Já que  $(f^{(k)}(\alpha^{-1})) = (f^{(k)}(\alpha)^{-1})^{\pi^{(k-1)}\alpha}$  e  $f^{(k)}(\alpha\beta) = f^{(k)}(\alpha)(f^{(k)}(\beta))^{\pi^{(k-1)}\alpha^{-1}}$ . Segue que  $\theta(\alpha^{-1}, k) = \theta(\alpha, k) \leq c_1 k^m$  e  $\theta(\alpha\beta, k) \leq (c_1 + c_2)k^m$ . E portanto,  $Pol(m)$  é um grupo.

Seja  $\alpha \in Pol(m)$ . Utilizando o homorfismo injetivo  $\phi$ , apresentado em 1.4, restrito a  $Pol(m)$ , temos que  $\phi(\alpha) = (\alpha|_0, \alpha|_1, \dots, \alpha|_{d-1})\pi_\alpha$ , onde  $\alpha|_y$  é a restrição de  $\alpha(\pi_\alpha)^{-1}$  à árvore  $y\mathcal{T}$ . Como  $\alpha(\pi_\alpha)^{-1}$  pertence a  $Pol(m)$  – pois cada fator pertence – segue que  $\alpha|_y$  também está em  $Pol(m)$ . A sobrejetividade segue do fato de que qualquer que seja  $\alpha \in Pol(m)$ , então  $(e, \dots, e, \alpha, e, \dots, e)\pi \in Pol(m)$  para toda  $\pi \in Sym(Y)$ . ■

**Observação 1.3.5** *Como o grupo  $Pol(m)$  é um produto entrelaçado infinitamente iterado segue que este não satisfaz nenhuma lei de grupo não trivial.*

### 1.3.2 O grupo $Pol(-1)$ dos automorfismos finitários

**Definição 1.3.6** *Um automorfismo  $g$  é chamado finitário se existe  $k$  tal que  $g|_v = e$  para todo  $v \in Y^*, |v| > k$ . O menor  $k$  para o qual a propriedade acima se verifica é chamado profundidade de  $g$  e denotado por  $p(g)$ .*

**Observação 1.3.7** *Se um automorfismo  $g$  for finitário então ele tem claramente crescimento limitado, mas neste caso denotamos seu grau por  $\partial(g) = -1$ .*

Para ilustrar as noções acima, é interessante considerar o seguinte.

**Exemplo 1.3.8** *Seja  $\mathcal{T}$  a árvore regular uni-raiz gerada por  $Y = \{0, 1\}$  e considere os automorfismos:  $\sigma$ , a extensão da permutação  $(0, 1)$  para um automorfismo de  $\mathcal{T}$ ,  $\sigma_1 = (e, \sigma)$ ,  $\tau = (e, \tau)\sigma$ ,  $\gamma = (\gamma, \tau)$  e  $\delta = (\delta, \delta)\sigma$ . As matrizes de adjacência para os respectivos subgrafos dirigidos  $D(\alpha)'$  associados a estes automorfismos são:*



$$[\sigma] = ( 0 ), [\sigma_1] = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, [\tau] = ( 1 ), [\gamma] = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, [\delta] = ( 2 )$$

*Todos estes automorfismos com exceção de  $\delta$  tem crescimento polinomial:*

$$\partial(\sigma) = \partial(\sigma_1) = -1, \partial(\tau) = 0 \text{ e } \partial(\gamma) = 1.$$

*As profundidades dos automorfismos finitários  $\sigma$  e  $\sigma_1$  são  $p(\sigma) = 0$  e  $p(\sigma_1) = 1$ .*

É uma consequência imediata das propriedades (1.3) que o inverso de um automorfismo finitário também é finitário, assim como o é, o produto de dois automorfismos finitários. De onde segue que os automorfismos finitários formam um subgrupo. Utilizado este fato e seguindo a segunda parte da demonstração da Proposição 1.3.4, concluímos que:

**Proposição 1.3.9** *O conjunto  $Pol(-1)$  de todos os automorfismos finitários é um subgrupo estratificado de  $Pol(0)$ .*

**Proposição 1.3.10** *Um automorfismo  $\alpha$  é finitário se, e somente se, existe um inteiro positivo  $k$ , tal que, todo caminho direcionado (no grafo do autômato de  $\alpha$ ) partindo do estado  $\alpha$  de comprimento  $k$ , tem como vértice final o estado  $e$ .*

As classes de conjugação do grupo  $Pol(-1)$  foram determinadas para o caso binário em [BS97] e para o caso geral na tese de doutorado [Rib08].

Um subgrupo finitamente gerado  $P$  de  $Pol(-1)$  tem uma estrutura bastante tratável, já que basta tomar o máximo das profundidades dos geradores, digamos  $k$ , que  $G$  poderá ser visto como um grupo de permutações do conjunto  $Y^k$ .

Os primeiros exemplos de grupos de automorfismos de crescimento polinomial que não podem ser imersos em um grupo de permutação de um conjunto  $Y^k$ , com  $Y$  finito e  $k$  inteiro positivo, estão no grupos  $Pol(0)$ . Contudo este grupo guarda uma propriedade que o torna tratável e ao mesmo tempo fonte da maioria dos exemplos importantes estudados: a contração.

**Teorema 1.3.11** ([BN03, Teorema 5.3]) *Todo subgrupo finitamente gerado e fechado por estados de  $Pol(0)$  é contrátil.*

### Exemplo 1.3.12

- Considerando o automorfismo  $\alpha = (\gamma, \rho)\sigma$  da árvore binária, onde  $\gamma = (e, \tau)$ ,  $\rho = (\rho, \tau)$ ,  $\tau = (e, \tau)\sigma$ , então  $\alpha, \rho \in Pol(1) \setminus Pol(0)$  e  $\tau, \gamma \in Pol(0) \setminus Pol(-1)$ ;
- O automorfismo  $b = (b, b^{-2})\sigma$  é contrátil e o núcleo do grupo fechado por estados  $\langle b \rangle$  é o conjunto  $\mathcal{N} = \{e, b^{\pm 1}, b^{\pm 2}, b^{\pm 3}\}$ . Ao mesmo tempo, o grupo  $\langle \tau, b \rangle$  não é contrátil: caso fosse, as potências  $(b\tau)^n = (b\tau, b^{-2})^n$ , estariam todas no núcleo para  $n$  suficientemente grande. Contudo os  $(b\tau)^n$  são todos distintos. Em particular, concluimos que  $b\tau = (b\tau, b^{-2})$  não é contrátil. Ou seja, o conjunto dos automorfismos contráteis não formam um grupo.
- O automorfismo  $b$  dado por  $b = (\tau, b)$  está em  $Pol(1) \setminus Pol(0)$ , contudo  $b$  não é contrátil, pois, caso fosse todos os elementos  $b^n = (\tau^n, b^n)$  estariam no núcleo para  $n$  suficientemente grande. Entretanto, os  $b^n$  são todos distintos para  $n > 1$ , o que nos daria um núcleo infinito.
- $b = (b, b)\sigma$  tem crescimento exponencial e é contrátil.

Vamos apresentar a seguir, exemplos clássicos de grupos que são de crescimento limitado.

### O grupo de Grigorchuk [Gri80]

O grupo de Grigorchuk age sobre  $\mathcal{T}_2$  e é gerado pelos automorfismos:

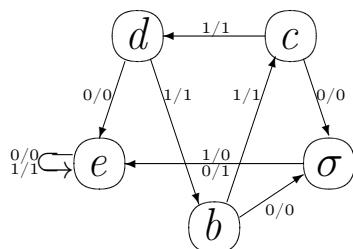
$$a = \sigma = (0, 1)$$

$$b = (a, c)$$

$$c = (a, d)$$

$$d = (e, b).$$

Trata-se de um 2-grupo infinito de crescimento intermediário. O autômato que representa a ação dos geradores é:



### O grupo de Gupta-Sidki [GS83]

Nos anos 80 Gupta e Sidki apresentaram uma construção simples de um grupo de Burnside, ou seja, um grupo de torção finitamente gerado infinito. Considerando  $p \geq 3$  primo, definimos o automorfismo  $\gamma$  de  $\mathcal{T}_p$  por  $\gamma = (\sigma, \sigma^{-1}, 1, 1, \dots, 1, \gamma)$ , onde  $\sigma$  é a extensão da permutação  $(0, 1, 2, \dots, p-1)$  para um automorfismo de  $\mathcal{T}_p$ .

### O grupo de Brunner-Sidki-Vieira [BSV99]

O grupo  $\mathcal{H}$  de Brunner-Sidki-Vieira é um grupo de automorfismos da árvore binária gerado pela chamada máquina de adição binária  $\tau$  e seu conjugado  $\mu$  onde,

$$\tau = (e, \tau)\sigma$$

$$\mu = (e, \mu^{-1})\sigma.$$

O grupo  $\mathcal{G}$  de Gupta-Sidki é tal que  $\mathcal{G} = \langle \gamma, \sigma \rangle$ . Este foi o primeiro exemplo de grupo finitamente gerado livre-de-torção quase-solúvel.  $\mathcal{H}$  tem aspectos interessantes:

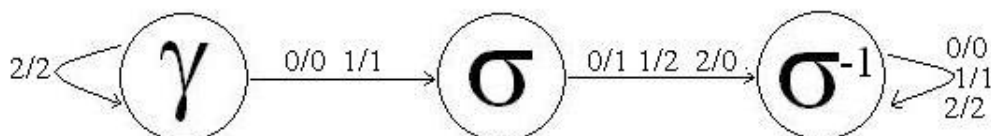


Figura 1.4: Autômato de  $\gamma$

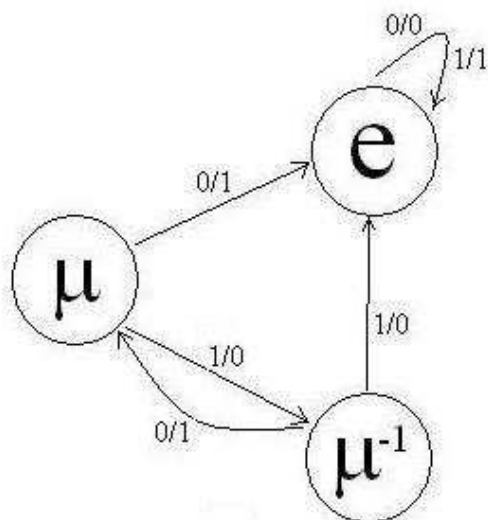


Figura 1.5: Autômato de  $\mu$

por um lado é residualmente (abeliano por 2-grupo finito e livre de torção) e por outro é residualmente (poli-cíclico infinito).

# Capítulo 2

## Circuitos

Ao considerarmos um automorfismo  $\alpha \in \mathcal{A}_f$  de crescimento polinomial, certamente este induz uma permutação sobre o conjunto  $Y^k$  para cada  $k$ . Contudo, quando tal automorfismo não é finitário, o grupo cíclico  $\langle \alpha \rangle$  não pode ser imerso no grupo das permutações do conjunto  $Y^k$  para nenhum  $k$ . Como consequência, o autômato de  $\alpha$  possuirá, necessariamente, uma estrutura cíclica, mais precisamente, alguns de seus estados terão a propriedade especial de estarem em um circuito de seus próprios autômatos.

### 2.1 Automorfismos circuitos

**Definição 2.1.1** *Seja  $g \in \text{Pol}(m)$ ,  $m \geq 0$ . Então  $g$  é dito automorfismo circuito, se quando consideramos o autômato  $D(g)$ , o estado  $g$  está em um circuito de seu próprio grafo. Quando no contexto estiver claro, chamaremos um tal  $g$  simplesmente de circuito.*

Mais precisamente, quando um certo  $\alpha$  de finitos estados não é finitário, isso significa que para todo inteiro positivo  $k$  existe  $u \in Y^*$  de comprimento  $k$  tal que  $\alpha|_u \neq e$ . Sendo  $\alpha$  de finitos estados, necessariamente existem  $u, w \in Y^* \setminus \phi$  tais que  $\alpha|_u = \alpha|_{uw}$ , onde  $\phi$  é a palavra vazia. Ou seja, chamando  $\alpha|_u = g$ , então,  $g = g|_w = g|_{ww} = \dots = g|_{w^t}$ , para todo  $t$ . Tal automorfismo  $g$  tem a propriedade

especial de que quando consideramos seu autômato, ele está em um circuito deste grafo. Notemos que existe uma palavra  $w$  minimal não trivial tal que  $g = g|_w$ . Mais ainda, se  $\alpha \in Pol(m)$ ,  $m \geq 0$ , existe um primeiro nível  $k$  da árvore tal que cada entrada de  $f^{(k)}(\alpha)$  é um circuito ou tem grau menor que  $m$ . Este fato nos permite introduzir uma função comprimento silábico que desempenha um papel importante em nossas análises futuras.

Suponha que para este  $\alpha$  as entradas de  $f^{(k)}(\alpha)$  as quais são circuitos, sejam  $\delta_1, \delta_2, \dots, \delta_l$  e que eles ocorram respectivamente nos índices  $u_1, u_2, \dots, u_l$ . Denotamos por  $\beta_j = u_j * \delta_j$  o vetor tal que  $(\beta_j)|_{u_j} = \delta_j$  e  $(\beta_j)|_u = e$  se  $u \in Y^{|u_j|}$  for diferente de  $u_j$ . Então  $\alpha = \beta_1 \beta_2 \dots \beta_l h$  onde  $\beta_j = u_j * \delta_j$   $1 \leq j \leq m$  e  $h \in Pol(m-1)$ . Esse  $l$  é canônico no seguinte sentido: se  $\alpha = c \rho_1 c' \rho_2 \dots c'' \rho_t c'''$ , onde  $\rho_1, \rho_2, \dots, \rho_t$  são tais que existem índices  $w_j$  onde  $\rho_j = w_j * g_j$ , para  $g_j$  circuitos de  $\alpha$  e  $c, c', c'', c''' \in Pol(m-1)$ , então  $l \leq t$ . Isso porque podemos supor que cada  $\rho_j$  pertence ao estabilizador do  $k$ -ésimo nível, contribuindo com um único circuito para a entrada de  $f^{(k)}(\alpha)$ .

Chamamos  $l$  de comprimento  $m$ -silábico de  $\alpha$  e denotamos por  $|\alpha|_m = l$ .

É uma consequência das observações feitas acima que  $\sum_{i \in Y} |\alpha_i|_m \leq |\alpha|_m$  (mais adiante em 2.3, daremos uma demonstração deste fato). Como  $|\alpha|_m = |f(\alpha)|_m$  e  $|y * \alpha|_m = |\alpha|_m$ , segue que  $|\alpha|_m = |f(\alpha)|_m = |(\alpha|_0, \alpha|_1, \dots, \alpha|_{|Y|-1})|_m \leq \sum_{i \in Y} |\alpha|_i|_m$  e portanto temos a fórmula:

$$|\alpha|_m = \sum_{i \in Y} |\alpha|_i|_m.$$

Quando no contexto estiver claro, vamos omitir os índices. Se estivermos trabalhando com elementos de  $Pol(m)$  para um  $m$  fixo, vamos escrever  $|\alpha|$  ao invés de  $|\alpha|_m$ . Neste caso,  $|\alpha| = 0$  significa que  $\alpha$  está em  $Pol(m-1)$ .

**Definição 2.1.2** *Se  $\alpha \in Pol(m)$ ,  $m \geq 0$ , o menor  $k$  tal que cada entrada de  $f^{(k)}(\alpha)$  é um circuito ou tem grau menor que  $m$  é chamado profundidade de  $\alpha$  e denotado por  $p(\alpha) = k$ .*

**Exemplo 2.1.3** Consideremos os automorfismos  $\mu = (e, \mu^{-1})\sigma$ ,  $\alpha = (\gamma, \zeta)\sigma$  da árvore binária, onde  $\gamma = (e, \tau)$ ,  $\zeta = (\zeta, \tau)$ ,  $\tau = (e, \tau)\sigma$ . Então, indo para o segundo nível, produzimos  $f^{(2)}(\alpha) = (e, \tau, \zeta, \tau)$  e portanto  $\alpha = \beta h$  onde  $\beta = (e, e, \zeta, e)$  e  $h = (e, \tau, e, \tau)\sigma$ .

- $\tau$  e  $\mu$  são circuitos de  $Pol(0)$ , pois, seus autômatos possuem um caminho com um único ciclo;
- $\zeta$  é um circuito de  $Pol(1)$ , pois, seu autômato possui um caminho com dois ciclos distintos;
- $\alpha \in Pol(1)$  não é um circuito. Segue da decomposição  $f^{(2)}(\alpha) = (e, \tau, \mu, \tau)$  que  $|\alpha|_1 = 1$ ;
- $\beta \in Pol(1)$  mas não é um circuito. Segue de  $\beta = (e, e, \mu, e)$  que  $|\beta|_1 = 1$ .
- $h = (e, \tau, e, \tau)\sigma \in Pol(0)$  mas não é um circuito. Observemos que  $|h|_0 = 2$ .
- $\gamma \in Pol(0)$  mas não é um circuito e  $|\gamma|_0 = 1$ .

**Observação 2.1.4** Consideremos um grupo de automorfismos  $G$  fechado por estados. São equivalentes as seguintes afirmações:

- $G$  é contrátil;
- Existem constantes positivas  $\lambda < 1$ ,  $C$  e  $k$  tais que para todo  $\alpha \in G$ , temos que  $|\alpha|_u \leq \lambda|\alpha| + C$  para todo  $u \in Y^*$  com  $|u| > k$ ;

**Lema 2.1.5** Seja  $\alpha \in Pol(m)$  onde  $m \geq 0$ .

- (1) Se  $|Q(\alpha|_u)| = |Q(\alpha)|$  para um índice  $u \neq \phi$  então  $\alpha$  é um circuito.
- (2) Se  $p(\alpha)$  é a profundidade de  $\alpha$ , então,  $p(\alpha) \leq |Q(\alpha)|$ .

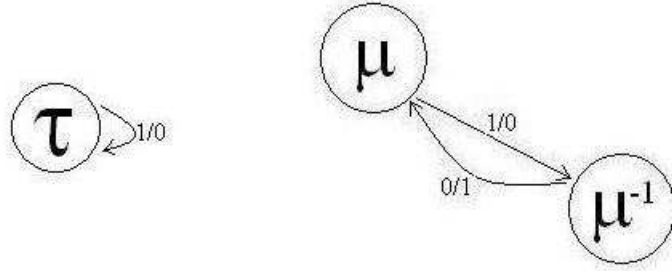


Figura 2.1:  $D(\tau)' = D(\tau) \setminus \{Star(e)\}$  e  $D(\mu)' = D(\mu) \setminus \{Star(e)\}$

**Demonstração:** (1) Já que  $Q(\alpha|_u)$  é um subconjunto finito de  $Q(\alpha)$ , segue que  $\alpha \in Q(\alpha|_u)$ . Ou seja, existe  $w$  tal que  $\alpha|_u|_w = \alpha$ , e portanto  $\alpha$  é um circuito.

(2) Se  $\alpha$  é um circuito então vale que a profundidade  $p(\alpha) = 1$  e a desigualdade se verifica. Vamos proceder por indução sobre  $|Q(\alpha)|$ . Suponhamos que  $\alpha$  não seja um circuito e escrevamos  $\alpha = (\alpha|_i) \pi_\alpha$ . Então

$$\begin{aligned} |Q(\alpha|_i)| &< |Q(\alpha)|, \text{ e} \\ p(\alpha) &\leq 1 + \max_{0 \leq i \leq n-1} \{p(\alpha|_i)\}, \\ &\leq 1 + \max_{0 \leq i \leq n-1} \{|Q(\alpha|_i)|\} \leq |Q(\alpha)|. \end{aligned}$$

■

**Observação 2.1.6** Dado um automorfismo  $\alpha$ , denotaremos por  $\mathcal{N}(\alpha)$  o conjunto de todos os estados de  $\alpha$  que são automorfismos circuitos, e por  $\mathcal{P}(\alpha)$  o conjunto de todos os estados de  $\alpha$  que são automorfismos finitários.

Existem duas maneiras de representar um elemento  $\alpha$  de  $Pol(m)$  para  $m \geq 0$ . A primeira é como uma *palavra* na forma  $\alpha = \kappa_1 \beta_1 \kappa_2 \dots \beta_l \kappa_{l+1}$  onde  $\kappa_1, \kappa_2, \dots, \kappa_{l+1} \in Pol(m-1)$  e  $\beta_1, \dots, \beta_l$  são circuitos. A segunda, é uma representação por *profundidade*, neste caso escrevemos  $\alpha = \alpha' \kappa$ ,  $\alpha' \in Stab_{Pol(0)}(k)$ ,  $\kappa \in P_{k-1}$  e onde cada entrada de  $\alpha'$  é um elemento de  $Pol(m-1)$  ou um circuito.



Se  $\alpha$  é uma palavra da forma  $\alpha = \kappa_1 \beta_1 \kappa_2 \dots \beta_l \kappa_{l+1}$  então uma estimativa elementar para sua profundidade é

$$\begin{aligned} p(\alpha) &\leq |Q(\alpha)| \\ &\leq \prod_{1 \leq i \leq l+1} |Q(\kappa_i)| \prod_{1 \leq i \leq l} |Q(\beta_i)|. \end{aligned}$$

Por outro lado, começando por uma representação por profundidade de  $\alpha$ , a próxima proposição nos dá uma representação de  $\alpha$  como palavra de comprimento silábico mínimo  $|\alpha|_m$ .

**Proposição 2.1.7** *Seja  $\alpha \in \text{Pol}(m)$  dada por sua representação por profundidade  $\alpha = (\alpha|_u)_{|u|=k} \cdot \kappa$  onde cada  $\alpha|_u$  é um circuito ou um elemento de  $\text{Pol}(m-1)$  e  $\kappa \in P_{k-1}$ . Seja  $\alpha_1, \dots, \alpha_l$  o conjunto de circuitos de  $\{\alpha|_u \mid |u| = k\}$ . Então  $\alpha$  pode ser escrito como  $\kappa_1 \beta_1 \kappa_2 \dots \kappa_l \beta_l \kappa_{l+1}$  onde  $\beta_i \in \mathcal{N}(\alpha_i)$ ,  $\kappa_i \in \text{Pol}(m-1)$  para todo  $i$  e  $l = |\alpha|_m$ .*

**Demonstração:** Começamos considerando  $\beta$  um circuito. Então para algum vértice  $u$  de comprimento  $c(\beta)$  temos que  $\beta = \beta|_{ui}$  para algum  $i \in Y$ . Então  $\beta|_u$  é um circuito e  $\beta|_{uj} \in \text{Pol}(m-1)$  para todo  $j \neq i$ . Suponhamos  $i = d-1$ . Então,

$$\begin{aligned} \beta|_u &= (\beta|_{u0}, \dots, \beta) \pi = (e, \dots, e, \beta) \kappa, \\ \kappa &= (\beta|_{u0}, \beta|_{u1}, \dots, \beta|_{u(d-2)}, e) \pi \in \text{Pol}(m-1). \end{aligned}$$

Portanto,

$$\begin{aligned} (e, \dots, e, \beta) &= \beta|_u \kappa^{-1}, \\ (\beta, e, \dots, e) &= \rho \beta|_u (\kappa^{-1} \rho^{-1}) \end{aligned}$$

para algum  $\rho \in \text{Sym}(Y)$ . Suponha que  $u'$  é um índice tal que  $\beta|_{u'} = (\beta|_{u'0}, \dots, \beta|_{u'd-1}) \pi_{i'}$ . Então, procedendo tal como acima obtemos

$$(e, \dots, e, \beta|_u) = \beta|_{u'} (\kappa')^{-1} \tag{2.1}$$

e

$$\begin{aligned}(e, \dots, e, (e, \dots, e, \beta) \kappa) &= \beta|_{u'} (\kappa')^{-1}, \\ (e, \dots, e, (e, \dots, e, \beta)) &= \beta|_{u'} (\kappa')^{-1} (e, \dots, e, \kappa)^{-1}.\end{aligned}$$

Continuando, obtemos uma expressão para  $(e, e, \dots, \beta)$  de profundidade  $k \geq 1$  como

$$(e, e, \dots, \beta) = \zeta \beta|_v \kappa \quad (2.2)$$

para  $\beta|_v$  no circuito de  $\beta$ ,  $\zeta \in P_{k-1}$  e  $\kappa$  em  $Pol(m-1)$ .

Segue de  $\alpha = (\alpha|_u)_{|u|=k} \cdot \kappa$ , que cada  $(e, \dots, \alpha_i, \dots, e)$ , onde  $\alpha_i$  é um circuito, se levanta para um  $\beta_i$ , tal como mostrado acima e portanto, obtemos uma palavra para  $\alpha$  tal como desejado. Finalmente se  $\alpha$  pode ser escrita como palavra de comprimento menor que  $l$  então esta terá menos que  $l$  circuitos no nível  $k$ . ■

Como consequência, temos o resultado.

**Corolário 2.1.8** *Seja  $G$  um subgrupo finitamente gerado de  $Pol(m)$ . Então o fecho por estados de  $G$  é gerado por um número finito de circuitos e um número finito de elementos de  $Pol(m-1)$ .*

Ambos as representações de  $\alpha$  – por profundidade ou como palavra nos circuitos e em  $Pol(m-1)$  – produzem representações do mesmo tipo para cada estado  $\alpha|_i$  onde  $i \in Y$ . De fato, seja  $\alpha = (\alpha|_i)_{i \in Y} \pi$  e  $\alpha = \kappa_1 \beta_1 \kappa_2 \dots \kappa_l \beta_l \kappa_{l+1}$  como acima, e

$$\begin{aligned}\mathcal{N} &= \cup_{1 \leq i \leq l} \mathcal{N}(\beta_i), \\ \mathcal{K} &= \langle Q(\beta_i) \cap Pol(m-1), Q(\kappa_j) \mid 1 \leq i \leq l, 1 \leq j \leq l+1 \rangle.\end{aligned}$$

Então  $\alpha|_i$  é uma palavra nos estados do primeiro nível dos  $\kappa_j$  e  $\beta_j$  e mais ainda, os estados do primeiro nível dos  $\beta_j$  que são circuitos, são particionados entre os  $\alpha|_i$ , para os diferentes  $i$ . Em particular, temos que  $\sum_{i \in Y} |(\alpha|_i)|_m \leq |\alpha|_m$ .

### 2.1.1 Produtos de circuitos

**Lema 2.1.9** *Sejam  $\alpha, \beta$  circuitos de  $Pol(0)$ ,  $u, w \in Y^* \setminus \{\phi\}$  palavras de comprimento minimal tais que  $\alpha = \alpha|_u$  e  $\beta = \beta|_w$ . Então*

1.  $\alpha^{-1}$  é um circuito;
2.  $\alpha\beta$  é um circuito se, e somente se,

$$(u^i)^\alpha = w^j,$$

$$\text{onde } i = \frac{mmc(|u|, |w|)}{|u|} \text{ e } j = \frac{mmc(|u|, |w|)}{|w|}.$$

**Demonstração:**

1. Como  $\alpha$  é um circuito e  $\alpha = \alpha|_u$ , então  $\alpha^{-1} = \alpha|_u^{-1}$ , mas pelas fórmulas (1.3),  $\alpha|_u^{-1} = (\alpha^{-1})|_{u^{\alpha^{-1}}}$ . Portanto  $\alpha^{-1}$  é um circuito;
2. Suponhamos que  $\alpha\beta$  seja um circuito e seja  $v \in Y^* \setminus \{\phi\}$ , de comprimento minimal tal que  $(\alpha\beta)|_v = \alpha\beta$ . Segue de  $(\alpha\beta)|_v = \alpha|_v\beta|_v^\alpha$ , que  $(\alpha\beta) = \alpha|_v\beta|_v^\alpha = \alpha|_{vv}\beta|_{(vv)^\alpha} = \dots = \alpha|_{vv\dots v}\beta|_{(vv\dots v)^\alpha}$ . Como existe um nível  $k$  a partir do qual cada estado de  $\alpha\beta$  é um circuito ou uma permutação, então existe  $t$  tal que  $\alpha|_{v^t}$  e  $\beta|_{(v^t)^\alpha}$  são circuitos ou permutações. Como  $\alpha\beta$  é um circuito, nem  $\alpha|_{v^t}$  nem  $\beta|_{(v^t)^\alpha}$  podem ser permutações (de fato, se ambos forem permutações o produto não é um circuito e o mesmo ocorre no caso em que temos o produto de uma permutação por um circuito). Caso  $v$  não fosse uma potência de  $u$ , percorrendo  $\alpha|_v, \alpha|_{vv}, \dots, \alpha|_{v^t}$ , encontramos  $t$  tal que  $\alpha|_{v^t} = \alpha$ . Ou seja,  $v^t$  é uma potência de  $u$ , digamos,  $v^t = u^r$  e utilizando um argumento análogo concluímos que existe  $l$  tal que  $(v^l)^\alpha = w^s$  para  $s$  inteiro positivo. Segue que existe uma potência de  $u$  que é igual a uma potência de  $w$ . Sem perda de generalidade, podemos supor que  $|u^r| = |w^s|$ , então  $m = r|u| = s|w|$  é um múltiplo comum entre

$|u|$  e  $|w|$ . Suponha que  $m$  não seja o  $mmc(|u|, |w|)$ , ou seja, existe  $k > 1$  tal que  $m = k \cdot mmc(|u|, |w|)$ . Tomando  $i = \frac{mmc(|u|, |w|)}{|u|}$  e  $j = \frac{mmc(|u|, |w|)}{|w|}$ , observe que  $(u^i)^\alpha$  é um prefixo de  $w^s$ , e que  $|(u^i)^\alpha|$  é um múltiplo de  $|w|$ . Portanto,  $(u^i)^\alpha = w^t$  e portanto  $\beta|_{(w^t)^\alpha} = \beta$ . ou seja,  $(\alpha\beta)|_{(u^i)} = \alpha|_{(u^i)}\beta|_{(w^t)^\alpha} = \alpha\beta$ . Isso contradiz a minimalidade de  $v$ .

Por outro lado, suponhamos que

$$(u^i)^\alpha = w^j.$$

Então,  $(\alpha\beta)|_{(u^i)} = \alpha|_{(u^i)}\beta|_{(u^i)^\alpha} = \alpha|_{(u^i)}\beta|_{w^j} = \alpha\beta$ . Ou seja,  $\alpha\beta$  é um circuito. ■

**Lema 2.1.10** *Suponhamos que  $\alpha, \beta$  sejam circuitos de  $Pol(0)$  tais que  $\alpha\beta$  é um circuito.*

1. *Se  $\beta\alpha$  também for um circuito então  $\alpha\beta$  tem ordem finita.*
2. *Se  $\beta^{-1}\alpha$  for um circuito então  $\alpha$  tem ordem finita.*

**Demonstração:**

1. Sejam  $\alpha, \beta$  circuitos de  $Pol(0)$  e sejam  $u, w, v \in Y^*$  palavras de comprimento minimal tais que  $|u|, |w|, |v| > 1$ ,  $\alpha = \alpha|_u$ ,  $\beta = \beta|_w$  e  $(\alpha\beta)|_v = \alpha\beta$ .

Sejam  $i = \frac{mmc(|u|, |w|)}{|u|}$  e  $j = \frac{mmc(|u|, |w|)}{|w|}$ . Segue do resultado anterior que

$$(u^i)^\alpha = w^j.$$

Se  $\beta\alpha$  é também um circuito então

$$(w^j)^\beta = u^i.$$

Agora observe que para todo  $k$ ,  $(\alpha\beta)^k|_{(u^i)} = (\alpha\beta)^k$ . Basta escolher um  $k$  tal que  $(\alpha\beta)^k|_v$  seja inativo para todos os  $v$  de comprimento menor que  $|u^i|$ .

2. Suponhamos que  $\alpha|_u = \alpha, \beta^{-1}|_w = \beta^{-1}$  e estas sejam as palavras minimais não triviais tais que isso ocorra. Então  $\beta|_{w^{\beta^{-1}}} = \beta$  e como  $\beta^{-1}\alpha$  é um circuito, então  $(w^j)^{\beta^{-1}} = u^i$ . E como  $\alpha\beta$  é um circuito, então  $(u^i)^\alpha = (w^{\beta^{-1}})^j$ . Como  $(w^j)^{\beta^{-1}} = w^{\beta^{-1}}w^{\beta^{-1}|_w}w^{\beta^{-1}|_w} \dots w^{\beta^{-1}|_{w^{j-1}}} = (w^{\beta^{-1}})^j$ , então,  $(u^i)^\alpha = (w^{\beta^{-1}})^j = (w^j)^{\beta^{-1}} = u^i$ . Basta tomar  $k$  tal que a permutação induzida por  $\alpha$  sobre  $Y^{|u^i|}$  seja trivial, ou seja,  $(\sigma^{(|u^i|)}(\alpha))^k = e$ . Segue que  $(\alpha^k)|_{u^i} = (\alpha|_{u^i})^k = \alpha^k$ , donde concluímos que  $\alpha^k$  é trivial. ■

**Lema 2.1.11** *Suponhamos que  $\gamma = \kappa_1\alpha_1\kappa_2 \dots \kappa_l\alpha_l\kappa_{l+1} \in Pol(0)$  seja um circuito escrito não trivialmente como uma palavra nos circuitos  $\alpha_i$  e nas permutações  $\kappa_i$ , minimizando o comprimento  $l$ . Então  $\gamma$  é um produto de circuitos; de fato,  $\gamma = \beta_1 \dots \beta_l$  onde cada  $\beta_i$  é um circuito que é um estado de  $\alpha_i$ .*

**Demonstração:** Já que  $l$  é minimal, os estados de  $\gamma$  que são circuitos tem a forma  $\gamma' = \kappa'_1\alpha'_1\kappa'_2 \dots \kappa'_l\alpha'_l\kappa'_{l+1}$  com comprimento silábico minimal  $l$ , onde  $\alpha'_i$  são estados de  $\alpha_i$  que são circuitos e onde as permutações  $\kappa'_i$  são estados de  $\kappa_i$ . Existe uma profundidade onde os  $\kappa'_i$  são todos iguais ao elemento trivial. Portanto, concluímos que  $\gamma = \beta_{j_1} \dots \beta_{j_l}$ . ■

Damos a seguir uma descrição dos circuitos  $\alpha \in Pol(0)$  que têm ordem finita

**Proposição 2.1.12** *Seja  $\alpha = (\alpha|_i)_{i \in Y} \cdot \pi_\alpha \in Pol(0)$  um circuito e seja  $\mathcal{N}_0(\alpha)$  o conjunto dos elementos de torção de  $\mathcal{N}(\alpha)$ .*

1. *Suponhamos que existam  $l \geq 1$  e  $\kappa_1, \kappa_2, \dots, \kappa_l, \kappa_{l+1} \in Pol(-1)$  tais que  $\gamma = \kappa_1\alpha\kappa_2 \dots \kappa_l\alpha\kappa_{l+1} = e$ . Então  $\mathcal{N}_0(\alpha)$  é não vazio.*
2. *Suponhamos que  $\mathcal{N}_0(\alpha)$  seja não vazio e seja  $t = \min\{o(\beta) \mid \beta \in \mathcal{N}_0(\alpha)\}$ . Então  $\mathcal{N}(\alpha) = \mathcal{N}_0(\alpha)$  e  $o(\gamma) = t$  para todo  $\gamma \in \mathcal{N}(\alpha)$ . Mais ainda, se  $\alpha|_j \in \mathcal{N}(\alpha)$  então  $j$  é um ponto fixo de  $\pi_\alpha$ .*

3. O circuito  $\alpha$  têm ordem infinita se, e somente se, existe  $\beta = (\beta|_i)_{i \in Y} \cdot \pi_\beta \in \mathcal{N}(\alpha)$  tal que para  $\beta|_j \in \mathcal{N}(\alpha)$ , o índice  $j$  não é um ponto fixo de  $\pi_\beta$ .

**Demonstração:**

1. Os estados  $\gamma$  tem a forma  $\gamma' = \kappa'_1 \beta \kappa'_2 \dots \kappa'_t \beta \kappa'_{t+1} = e$  onde  $\beta \in \mathcal{N}(\alpha)$ , ou seja, este é um estado de  $\alpha$  que é um circuito. Podemos supor que  $t$  seja mínimo. Então, existe uma profundidade onde os  $\kappa'_i$  são todos iguais ao elemento trivial, donde a asserção segue.
2. Seja  $\beta \in \mathcal{N}_0(\alpha)$  de ordem finita mínima  $t$ . Escrevamos  $\beta = (\beta|_i)_{i \in Y} \cdot \pi_\beta$  e seja  $\gamma = \beta|_j \in \mathcal{N}(\alpha)$ . Suponhamos que a órbita de  $j$  pela ação de  $\pi_\beta$  tenha tamanho  $r$ . Então  $r|t$ , e  $\beta^r$  é conjugado a  $\kappa\gamma\kappa'$  e  $(\beta^l)^{\frac{t}{r}} (= e)$  é conjugado a  $(\kappa\gamma\kappa')^{\frac{t}{r}} = e$ . Pela primeira parte, existem  $\eta \in \mathcal{N}_0(\alpha)$  tais que  $\eta^i = e$  onde  $1 \leq i \leq \frac{t}{r}$ . Portanto,  $r = 1$ .

Então  $\beta^t (= e)$  é conjugado a  $\gamma^t = e$  e o resto da asserção segue do fato de que  $\mathcal{N}(\alpha) = \mathcal{N}(\beta)$ .

Suponhamos que  $\alpha|_j$  seja um circuito. Como  $e = \alpha^t|_j = \alpha|_j \alpha|_{j^\alpha} \dots \alpha|_{j^{\alpha^{t-1}}}$ , se  $t < |\text{Orb}_\alpha(j)|$ , então, teríamos de  $\alpha|_j = \alpha|_{j^\alpha}^{-1} \dots \alpha|_{j^{\alpha^{t-1}}}^{-1}$  que  $\alpha|_j$  seria uma permutação. Se  $1 < |\text{Orb}_\alpha(j)| \leq t$  encontraríamos um estado circuito de  $\alpha$  com ordem positiva menor que  $t$ . Segue que  $|\text{Orb}_\alpha(j)| = 1$ .

3. É um consequência direta do item anterior.

■

### 2.1.2 A finitude do conjunto $\mathcal{N}(G)$ de circuitos

Foi demonstrado em [Nek05] Seção 2.11, que  $\mathcal{N}(G)$  é finito quando  $G$  é um subgrupo finitamente gerado de  $\text{Pol}(0)$ .

Apresentamos aqui uma demonstração alternativa deste resultado.

**Teorema 2.1.13** *Seja  $G$  um subgrupo finitamente gerado de  $Pol(0)$ . Então o conjunto  $\mathcal{N}(G)$  dos circuitos de  $G$  é finito.*

**Demonstração:** Podemos supor  $G$  fechado por estados. Caso não fosse, basta tomar seu fecho por estados, que este ainda é finitamente gerado. Seja  $G$  gerado por  $X = \mathcal{N} \cup \mathcal{P}$  onde  $\mathcal{N}$  é um conjunto finito de circuitos e  $\mathcal{P}$  é um conjunto finito de permutações. Podemos supor que  $X$  é um conjunto fechado por estados e que  $X = X^{-1}$ . Particionando  $\mathcal{N} = \mathcal{N}_0 \cup \mathcal{N}_\infty$  onde  $\mathcal{N}_0$  é formado por elementos de ordem finita e  $\mathcal{N}_\infty$  por elementos de ordem infinita. Podemos supor  $|\mathcal{N}_\infty| = n$ . Agora particionando  $\mathcal{N}_0$  em subconjuntos  $\mathcal{N}_{0\nu}$  com a propriedade de que para cada dois  $\alpha, \beta$  distintos em  $\mathcal{N}_{0\nu}$  então  $\alpha\beta$  e  $\beta\alpha$  são circuitos. Segue do primeiro item do Lema 2.1.10 que cada  $\mathcal{N}_{0\nu}$  gera um subgrupo finito  $H_\nu$ , digamos de ordem  $n_\nu$ .

Suponha que  $\gamma$  seja um circuito em  $G$ . Então podemos supor  $\gamma = \beta_1 \dots \beta_l$  onde  $\beta_i \in \mathcal{N}$  e  $l$  é minimal. Segue que toda subpalavra de  $\beta_1 \dots \beta_l$  é também um circuito. Observe que fatores adjacentes que são circuitos de ordem finita satisfazem o segundo item do Lema 2.1.9 e portanto seu produto é um elemento de  $H_\nu$ . Seguindo esta divisão, obtemos  $\gamma = v_1 w_1 v_2 \dots v_t w_t$  onde  $v_i$  são elementos de ordem finita e os  $w_i$  são subpalavras que são produtos de consecutivos  $\gamma_i$  de ordem infinita. Cada subpalavra dos  $w_i$  é um circuito e não contém subpalavras da forma  $\alpha_i \dots \alpha_j$  onde  $\alpha_j = \alpha_i^{\pm 1}$ . Portanto o comprimento de cada  $w_i$  é no máximo  $n$ . ■

### 2.1.3 Um algoritmo para calcular $\mathcal{N}(G)$

Uma consequência dessa demonstração alternativa do Teorema 2.1.13 é que se  $G$  for um subgrupo finitamente gerado de  $Pol(0)$  então cada circuito de  $G$  pode ser escrito como um produto de no máximo  $n$  estados-circuitos dos geradores, para um certo  $n$ , inteiro positivo. Tal fato nos permite calcular todos os circuitos de  $G$  da seguinte maneira:

Suponhamos que  $G = \langle g_1, g_2, \dots, g_t \rangle$ .

- Consideremos o conjunto  $S = \{\alpha \mid \alpha \in Q(g_i), \text{ para algum } i \text{ e } \alpha \text{ é circuito}\}$ .
- Calculemos  $S_1$ , o conjunto obtido pela união de  $S$  com o conjunto de todas as palavras em  $S \cup S^{-1}$  de comprimento 1 que são circuitos. Verifiquemos se  $S_1 = S$ . Se for,  $\mathcal{N}(G) = S$ , caso contrário, calculemos  $S_2$ , o conjunto obtido pela união de  $S_1$  com o conjunto de todas as palavras em  $S \cup S^{-1}$  de comprimento 2 que são circuitos. Recordemos que o Lema 2.1.9 nos dá uma condição necessária e suficiente para que o produto de dois circuitos seja um circuito.
- De modo geral, o processo consiste em calcular  $S_{n+1}$ , o conjunto obtido pela união de  $S_n$  com o conjunto de todas as palavras em  $S \cup S^{-1}$  de comprimento  $n+1$  as quais são circuitos. Se  $S_{n+1} = S_n$  então  $\mathcal{N}(G) = S_n$  e o processo pára. Um tal  $n$  existe porque pelo Teorema anterior, os circuitos tem comprimento no máximo  $n$ , para algum  $n$ .

**Exemplo 2.1.14** Consideremos  $\mathcal{H} = \langle \tau, \mu \rangle$ , o grupo de Brunner-Sidki-Vieira.

Como  $\tau = (e, \tau)\sigma$  e  $\mu = (e, \mu^{-1})\sigma$ , então, seguindo a notação anterior,

$$S = \{e, \tau, \mu, \mu^{-1}\} \text{ e } S_1 = \{e, \tau, \tau^{-1}, \mu, \mu^{-1}\}.$$

Como  $S_1 \neq S$ , devemos calcular  $S_2$ . Pelo Lema 2.1.9,  $\alpha\beta$  é um circuito se, e somente se,  $(u^i)^\alpha = w^j$ , onde,  $\alpha = \alpha|_u$  e  $\beta = \beta|_w$  e  $i = \frac{mmc(|u|, |w|)}{|u|}$  e  $j = \frac{mmc(|u|, |w|)}{|w|}$ . Fazendo  $\alpha = \tau$  e  $\beta = \mu$  então  $u = 1$  e  $w = 10$  já que  $\tau|_1 = \tau$  e  $\mu|_{10} = \mu$ . Nesse caso  $i = 2$ ,  $j = 1$  e como  $(11)^\tau = 00 \neq 10$  temos que  $\tau\mu$  não é um circuito.

Fazendo uma análise análoga, concluímos que nenhuma palavra de comprimento 2 é circuito, donde,  $\mathcal{N}(\mathcal{H}) = S_1 = S_2$ .



## Capítulo 3

# Problemas algorítmicos para $\mathcal{A}$

Os resultados fundamentais de Novikov [Nov55] e Boone [Boo59] mostraram que até mesmo uma apresentação finita pode não fornecer muita informação sobre um grupo. Um dos problemas algorítmicos mais primitivos em teoria de grupos – saber se duas palavras nos geradores de um grupo  $G$  representam o mesmo elemento em  $G$  – se mostrou indecível mesmo na classe dos grupos finitamente apresentados. É de se esperar que no caso em que o grupo não é finitamente apresentado o problema se torne muito mais intratável, como de fato é. No entanto, a interpretação de  $\mathcal{A}$  como grupo de autômatos fornece uma maneira simples de resolver o problema da palavra em  $\mathcal{A}_f$ . Ainda mais, sob as hipóteses de contração e fechamento por estados existem algoritmos galhantes muito efetivos [Gri84, Sav03]. Com o problema da conjugação, não ocorre o mesmo, já que o problema está em aberto para  $\mathcal{A}_f$  mas pôde ser resolvido para uma certa quantidade de subgrupos de  $\mathcal{A}_f$  graças à sua estrutura galhada [Ale83, Roz98, Leo98, GW00], embora [SV] tenha dado recentemente um exemplo de grupo gerado por autômatos com problema da conjugação indecível.

A seguir, vamos mostrar que tanto o problema da ordem como o da conjugação simultâneo são decíveis em  $Pol(0)$ .

Os resultados apresentados neste capítulo foram obtidos em colaboração com I. Bondarenko e N. Bondarenko.

### 3.1 O problema da conjugação

Dado um grupo  $G$ , dizemos que o problema da conjugação é decidível para este grupo se existe um algoritmo que para quaisquer  $a, b \in G$  decide se eles são conjugados ou não em  $G$ . Quando um tal algoritmo não existe, dizemos que o problema da conjugação é indecidível para  $G$ .

- Dados  $a, b, h \in G$ , dizemos que um elemento  $h$  é um *conjugador para o par*  $(a, b)$ , se  $h^{-1}ah = b$  e usamos a notação  $a \sim_h b$  (alternativamente, dizemos que  $h$  *conjuga a por b*).
- Dados  $a, b \in G$ , se  $H$  e  $G$  são ambos subgrupos de um certo grupo  $K$  e existe algum elemento de  $H$  que conjuga  $a$  por  $b$ , então dizemos que o par  $(a, b)$  é conjugado em  $H$  e escrevemos  $a \sim_H b$ . Se  $h \in H$  é tal que  $h^{-1}ah = b$ , então dizemos que  $h$  é um *conjugador para o par*  $(a, b)$  em  $H$  e escrevemos  $a \sim_h b$ . Ou, dito de outra forma,  $h$  *conjuga a por b em H*.
- No caso em que  $a, b \in \mathcal{A} = \text{Aut}(\mathcal{T}_Y)$ , se  $a$  e  $b$  forem conjugados, então também o são as permutações  $\pi_a, \pi_b \in \text{Sym}(Y)$  induzidas pela ação de  $a$  e  $b$  sobre  $Y$ . Se  $\pi \in \text{Sym}(Y)$  é tal que  $\pi^{-1}\pi_a\pi = \pi_b$ , dizemos que  $\pi$  é um *conjugador permutacional* para o par  $(\pi_a, \pi_b)$ . O conjunto de todos os conjugadores permutacionais do par  $(\pi_a, \pi_b)$  é denotado por

$$C\Pi(a, b) = \{\pi \in \text{Sym}(Y) : \pi^{-1}\pi_a\pi = \pi_b\}. \quad (3.1)$$

- O conjunto  $C\Pi(a, b)$  pode ser vazio no caso em que  $a, b \in \mathcal{A}$  não são conjugados. Mas podemos observar que este conjunto ser não vazio não implica em  $a$  e  $b$  serem conjugados.
- Se  $a, b \in G$  são conjugados em um certo grupo  $H$ , onde  $G, H \leq K$ , então dois conjugadores  $\gamma, \gamma' \in H$  se relacionam da seguinte forma:  $\gamma' = c\gamma$  para algum

$c \in C_H(a)$ . Segue então que se  $\gamma$  conjuga o par  $(a, b)$  em  $H$ , então  $C_H(a)\gamma$  é o conjunto de todos os conjugadores do par  $(a, b)$  em  $H$ .

### 3.1.1 Classes de conjugação em $\mathcal{A}$

Iniciamos nossas considerações tomando  $\rho$ , um automorfismo da árvore binária  $\mathcal{T}_2$  o qual induz uma permutação transitiva sobre o  $k$ -ésimo nível, para cada  $k$ . Vamos ilustrar como um processo infinito define um conjugador  $\gamma$  tal que  $\rho \sim_\gamma \tau$ , onde  $\tau = (e, \tau)\sigma$  é a máquina de adição binária, mesmo no caso em  $\rho$  tenha um número infinito de estados.

Podemos observar primeiramente, que  $\rho = (\rho|_0, \rho|_1)\sigma$ , pois este induz a permutação  $\sigma$  no primeiro nível. Conjugando  $\rho$  pelo automorfismo  $\beta = (\rho|_0, e)$  obtemos

$$\rho^\beta = \rho' = (e, \rho|_1\rho|_0)\sigma.$$

Agora,  $\rho'|_1 = \rho|_1\rho|_0$  é novamente um automorfismo que induz uma permutação transitiva sobre cada nível de  $\mathcal{T}_2$ , e portanto,  $\rho'|_1 = (\rho'|_{10}, \rho'|_{11})\sigma$ . Conjugando  $\rho^\beta$  por  $\delta = (\delta|_0, \delta|_1)$ , onde  $\delta|_0 = (\rho'|_{10}, e)$ , obtemos

$$\rho^{\beta\delta} = ((e, e), (e, \rho'|_{11}\rho'|_{10})\sigma)\sigma.$$

Produzimos dessa forma, uma sequência infinita de conjugadores  $\beta, \delta, \dots$  cujo produto (que pode ser infinito) é bem definido, já que em um determinado nível  $k$ , existem finitos destes que agem não trivialmente sobre tal nível. Chamando tal produto infinito de  $\gamma$ , então  $\rho^\gamma = \alpha$ , onde  $\alpha|_u = (e, \alpha|_{1u})\sigma$ , se o índice  $u = \phi$  ou  $11\dots 1$ , e  $\alpha|_u = e$  para outras escolhas de  $u$ . Mas esta definição de  $\alpha$  coincide exatamente com a definição de  $\tau$ .

O processo apresentado neste exemplo contém a ideia central de [Sid98] para calcular as classes de conjugação de  $\mathcal{A}$ . Apresentamos abaixo o procedimento geral.

Primeiramente, vamos recordar que toda classe de conjugação do grupo simétrico  $Sym(Y)$  tem uma única representação (orientada à esquerda) na forma

$$(1, 2, \dots, n_1)(n_1 + 1, n_1 + 2, \dots, n_2) \dots (n_{k-1} + 1, n_{k-1} + 2, \dots, n_k), \quad (3.2)$$

onde  $1 \leq n_1 \leq n_2 - n_1 \leq \dots \leq n_k - n_1 - \dots - n_{k-1}$  e  $n_k = d = |Y|$ . Esta observação pode ser generalizada para o grupo  $\mathcal{A}$  conforme descrito na Seção 4.1 de [Sid98] e em [GNS01]. Dado um automorfismo  $a = (a|_1, a|_2, \dots, a|_d)\pi_a$  em  $\mathcal{A}$  podemos conjugar este à um único representante (orientado à esquerda) de sua classe de conjugação seguindo os seguintes passos:

1. Conjugamos a permutação  $\pi_a \in Sym(Y)$ , induzida pela ação de  $a$  sobre  $Y$ , ao seu único representante (orientado à esquerda) de classe de conjugação (3.2).
2. Consideramos cada ciclo  $\beta|_{i+1} = (n_i + 1, n_i + 2, \dots, n_{i+1})$  nos representantes (3.2) de  $\pi_a$  e definimos

$$h|_{i+1} = (a|_{n_i+1}, e, (a|_{n_i+2})^{-1}, (a|_{n_i+2}a|_{n_i+3})^{-1}, \dots, (a|_{n_i+2}a|_{n_i+3} \dots a|_{n_{i+1}-1})^{-1}). \quad (3.3)$$

Conjugamos  $a$  pelo automorfismo  $h = (h|_1, h|_2, \dots, h|_k)$  para obter  $h^{-1}ah = (a|_1, a|_2, \dots, a|_k)$ , onde

$$a_i = (e, \dots, e, a|_{n_i+2} \dots a|_{n_{i+1}} a|_{n_i+1}) \beta_i. \quad (3.4)$$

3. Aplicamos os passos 1 e 2 ao automorfismo  $a|_{n_i+2} \dots a|_{n_{i+1}} a|_{n_i+1}$ .

Podemos observar que uma iteração infinita desse procedimento produz um automorfismo bem definido da árvore que conjuga  $a$  em um representante e que dois representantes diferentes não são conjugados em  $\mathcal{A}$ . É importante notar que tal processo não decide conjugação entre dois automorfismos, já que a iteração pode ser infinita, e pode não nos responder em tempo finito ‘sim, eles são conjugados’ ou ‘não, eles não são conjugados’.

Uma outra abordagem é baseada no fato de que duas permutações são conjugadas se, e somente se, elas tem a mesma estrutura cíclica. O tipo de órbita de um automorfismo  $a \in \mathcal{A}$  é o grafo indexado, cujos vértices são as órbitas dos automorfismos  $a$  sobre  $Y^*$ , cada órbita é indexada por sua cardinalidade, e conectamos duas órbitas,  $\mathcal{O}_1$  e  $\mathcal{O}_2$  por uma aresta se existem vértices  $v_1 \in \mathcal{O}_1$  e  $v_2 \in \mathcal{O}_2$ , que são adjacentes na árvore  $T$ . Então, dois automorfismos da árvore  $T$  são conjugados se e somente se seus tipos de órbita são isomorfos como grafos indexados (veja [GNS01, Teorema 3.1]). Em particular, segue que o grupo  $\mathcal{A}$  é ambivalente (isto é, cada elemento é conjugado com seu inverso). Mais geralmente, a cada automorfismo  $a \in \mathcal{A}$  é conjugado a  $a^\xi$  para toda unidade  $\xi$  do anel  $\mathbb{Z}_m$  dos inteiros  $m$ -ádicos, onde  $m$  é o expoente do grupo  $Sym(Y)$ .

### 3.1.2 O problema da conjugação em $\mathcal{A}$

O estudo do problema da conjugação entre dois automorfismos da árvore  $\mathcal{T}$  inicia-se através da seguinte análise elementar:

Observemos que a equação  $\beta = \gamma^{-1}\alpha\gamma$  pode ser reescrita como  $\gamma\beta = \alpha\gamma$ . Decompondo  $\alpha = (\alpha|_i)_{i=0,\dots,d-1} \pi_\alpha$ ,  $\beta = (\beta|_i)_{i=0,\dots,d-1} \pi_\beta$ ,  $\gamma = (\gamma|_i)_{i=0,\dots,d-1} \pi_\gamma$ , onde  $\pi_\alpha$ ,  $\pi_\beta$  e  $\pi_\gamma$  são as permutações que  $\alpha$ ,  $\beta$  e  $\gamma$  respectivamente, induzem sobre o conjunto  $Y$ . Suponhamos ainda que  $|Orv_\alpha(i)| = m$  ou seja,  $i^{\alpha^m} = i$ . Então temos que

$$(\gamma|_i) \pi_\gamma \cdot (\beta|_i) \pi_\beta = (\alpha|_i) \pi_\alpha \cdot (\gamma|_i) \pi_\gamma,$$

$$(\gamma|_i \beta|_{i^{\pi_\gamma}}) \pi_\gamma \pi_\beta = (\alpha|_i \gamma|_{i^{\pi_\alpha}}) \pi_\alpha \pi_\gamma,$$

$$\text{Ou seja, } \pi_\gamma^{-1} \pi_\alpha \pi_\gamma = \pi_\beta \text{ e}$$

$$\gamma|_i = \alpha|_i \gamma|_{i^{\pi_\alpha}} (\beta|_{i^{\pi_\gamma}})^{-1} \quad (0 \leq i \leq d-1).$$

Portanto,

$$\gamma|_{i^{\pi_\alpha}} = \alpha|_i^{-1} \gamma|_i \beta|_{i^{\pi_\gamma}},$$

$$\gamma|_{i^{(\pi_\alpha)^2}} = \alpha|_{i^{\pi_\alpha}}^{-1} \gamma|_{i^{\pi_\alpha}} \beta|_{i^{\pi_\alpha \pi_\gamma}}$$

$$\begin{aligned} &= (\alpha|_{i^{\pi\alpha}}^{-1} \alpha|_i^{-1}) \gamma|_i (\beta|_{i^{\pi\gamma}} \beta|_{i^{\pi\alpha\pi\gamma}}), \\ \gamma|_{i^{(\pi\alpha)^j}} &= (\alpha|_{i^{(\pi\alpha)^{j-1}}}^{-1} \dots \alpha|_{i^{\pi\alpha}}^{-1} \alpha|_i^{-1}) \gamma|_i (\beta|_{i^{\pi\gamma}} \beta|_{i^{\pi\alpha\pi\gamma}} \dots \beta|_{i^{(\pi\alpha)^{j-1}\pi\gamma}}) \end{aligned}$$

onde  $1 \leq j \leq m$ . Para  $j = m$ , obtemos

$$\gamma|_i = (\alpha|_{i^{(\pi\alpha)^{m-1}(\alpha)}}^{-1} \dots \alpha|_{i^{\pi\alpha}}^{-1} \alpha|_i^{-1}) \gamma|_i (\beta|_{i^{\pi\gamma}} \beta|_{i^{\pi\alpha\pi\gamma}} \dots \beta|_{i^{(\pi\alpha)^{m-1}\pi\gamma}});$$

ou seja,

$$\alpha|_i \alpha|_{i^{\pi\alpha}} \dots \alpha|_{i^{(\pi\alpha)^{m-1}}} \sim_{\gamma|_i} \beta|_{i^{\pi\gamma}} \beta|_{i^{\pi\alpha\pi\gamma}} \dots \beta|_{i^{(\pi\alpha)^{m-1}\pi\gamma}} \left( = \beta|_{i^{\pi\gamma}} \beta|_{i^{\pi\gamma\pi\beta}} \dots \beta|_{i^{\pi\gamma(\pi\beta)^{m-1}}} \right). \quad (3.5)$$

Mostramos que o problema da conjugação entre  $\alpha$  e  $\beta$  em  $\mathcal{A}$  – primeiramente recai em decidir conjugação em  $Sym(Y)$ , para  $Y$  finito – e se reduz a subproblemas da conjugação nos níveis inferiores. De modo geral:

**Proposição 3.1.1 (Conjugação)** *Sejam  $\alpha, \beta, \gamma \in \mathcal{A}$ .*

1. Se  $\gamma^{-1}\alpha\gamma = \beta$ , então  $|Orb_\alpha(v)| = |Orb_\beta(v^\gamma)|$  para todo  $v \in Y^*$  e

$$\alpha^m|_v \sim_{\gamma|_v} \beta^m|_{v^\gamma} \quad (3.6)$$

onde  $m = |Orb_\alpha(v)|$ .

Alternativamente (3.6) pode ser reescrita como

$$\alpha|_v \alpha|_{v^\alpha} \dots \alpha|_{v^{\alpha^{m-1}}} \sim_{\gamma|_v} \beta|_{v^\gamma} \beta|_{v^\gamma\beta} \dots \beta|_{v^\gamma\beta^{m-1}} \left( = \beta|_{v^\gamma} \beta|_{v^\alpha\gamma} \dots \beta|_{v^{\alpha^{m-1}\gamma}} \right).$$

2. Sejam  $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_k$  as órbitas da ação de  $\alpha$  sobre  $Y$ . Se existe  $\pi \in C\Pi(\alpha, \beta)$  tal que  $\alpha|_{\mathcal{O}_i}|_v$  e  $\beta|_{\mathcal{O}_i}|_{v^\pi}$  sejam conjugados em  $\mathcal{A}$  para todo  $i = 1, 2, \dots, k$ , onde  $v \in \mathcal{O}_i$  é um vértice arbitrário, então  $\alpha \sim_{\mathcal{A}} \beta$ .

**Demonstração:**

1. Seja  $Orb_\alpha(v) = \{v_0 = v, v_1, \dots, v_{m-1}\}$ , onde  $v_i = (v)^{\alpha^i}$  e  $(v)^{\alpha^m} = v$ .

A igualdade  $\gamma^{-1}\alpha^m\gamma = \beta^m$  implica que  $\beta^m|_{v^\gamma} = (\gamma^{-1}\alpha^m\gamma)|_{v^\gamma} = (\gamma^{-1})|_{v^\gamma}\alpha^m|_{v^\gamma\gamma^{-1}\gamma}|_{v^{\alpha^m}} = (\gamma|_v)^{-1}\alpha^m|_v\gamma|_v$ . Ou seja, mostramos que  $\alpha^m|_v \sim_{(\gamma|_v)} \beta^m|_{v^\gamma}$ .

Segue imediatamente das equações (1.3) que

$$\alpha^m|_v = \alpha|_v\alpha|_{v^\alpha}\dots\alpha|_{v^{\alpha^{m-1}}} \text{ e que } \beta^m|_{v^\gamma} = \beta|_{v^\gamma}\beta|_{v^\gamma\beta}\dots\beta|_{v^\gamma\beta^{m-1}}.$$

2. Seja  $u = v^\gamma$ , então  $Orb_\beta(u) = \{u_0 = u, u_1, \dots, u_{m-1}\}$ , onde  $u_i = (u)^{\beta^i}$  e  $u_i = v_i^\gamma$ . Então

$$\begin{aligned} \beta|_{u_0} &= (\gamma^{-1}\alpha\gamma)|_{u_0} = (\gamma|_{v_0})^{-1}\alpha|_{v_0}\gamma|_{v_1} \\ \beta|_{u_1} &= (\gamma^{-1}\alpha\gamma)|_{u_1} = (\gamma|_{v_1})^{-1}\alpha|_{v_1}\gamma|_{v_2} \\ &\dots \quad \dots \\ \beta|_{u_{m-1}} &= (\gamma^{-1}\alpha\gamma)|_{u_{m-1}} = (\gamma|_{v_{m-1}})^{-1}\alpha|_{v_{m-1}}\gamma|_{v_0} \end{aligned}$$

Multiplicando estas equações, obtemos

$$\begin{aligned} (\gamma|_v)^{-1}\alpha^m|_v\gamma|_v &= (\gamma|_{v_0})^{-1}(\alpha|_{v_0}\alpha|_{v_1}\dots\alpha|_{v_{m-1}})\gamma|_{v_0} = \\ &= \beta|_{u_0}\beta|_{u_1}\dots\beta|_{u_{m-1}} = \beta^m|_u. \end{aligned}$$

Em particular

$$\begin{aligned} (\gamma|_{v_i})^{-1}\alpha^m|_{v_i}\gamma|_{v_i} &= (\gamma|_{v_i})^{-1}(\alpha|_{v_i}\alpha|_{v_{i+1}}\dots\alpha|_{v_{i-1}})\gamma|_{v_i} = \\ &= \beta|_{u_i}\beta|_{u_{i+1}}\dots\beta|_{u_{i-1}} = \beta^m|_{u_i}, \end{aligned} \tag{3.7}$$

$$\gamma|_{v_i} = (\alpha|_{v_0}\dots\alpha|_{v_{i-2}}\alpha|_{v_{i-1}})^{-1}\gamma|_{v_0}(\beta|_{u_0}\dots\beta|_{u_{i-2}}\beta|_{u_{i-1}}) = (\alpha^i|_v)^{-1}\gamma|_v\beta^i|_u. \tag{3.8}$$

Observemos agora, que isso define completamente um conjugador em  $\mathcal{A}$  para o par  $(\alpha, \beta)$ .

De fato, se existe  $\pi \in C\Pi(\alpha, \beta)$  tal que  $\alpha^{|\mathcal{O}_i|}|_v$  e  $\beta^{|\mathcal{O}_i|}|_{v\pi}$  são conjugados em  $\mathcal{A}$ , seja  $\gamma|_v (= \gamma|_{v_0})$  esse conjugador. Pelas equações 3.7 e 3.8 temos que

$$(\gamma|_{v_i})^{-1} \alpha^{|\mathcal{O}_i|}|_{v_i} \gamma|_{v_i} = \beta^{|\mathcal{O}_i|}|_{u_i},$$

e

$$\gamma|_{v_i} = (\alpha|_{v_0} \cdots \alpha|_{v_{i-2}} \alpha|_{v_{i-1}})^{-1} \gamma|_{v_0} (\beta|_{u_0} \cdots \beta|_{u_{i-2}} \beta|_{u_{i-1}}) = (\alpha^i|_v)^{-1} \gamma|_v \beta^i|_u.$$

onde nesse caso,  $v_i = v^{\alpha^i}$  e  $u_i = (v^\pi)^{\beta^i}$ . Ou seja, para cada órbita  $\mathcal{O}_i$  com um representante  $v = v_0$ , os estados  $\gamma|_{v_i}$  são determinados completamente em termos do estado  $\gamma|_{v_0}$  e dos estados de  $\alpha$  e  $\beta$ . Segue que  $\gamma = (\gamma|_{v_i})\pi$  (onde os  $v_i$  variam nas órbitas  $\mathcal{O}_i, i = 1, \dots, k$ ), é o conjugador para o par  $(\alpha, \beta)$ . ■

## 3.2 O problema da ordem em $\mathcal{A}$

O problema de encontrar a ordem de um dado elemento pode ser tratada usando a estrutura gahada dos automorfismos de  $\mathcal{A}$ . A próxima observação nos dá uma condição frequentemente utilizada para provar que um automorfismo dado tem ordem infinita.

**Lema 3.2.1** *Seja  $\alpha \in \mathcal{A}$ .*

1. *Sejam  $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_k$  as órbitas da ação de  $\alpha$  sobre  $Y$ . Defina  $\alpha_i = \alpha^{m_i}|_{y_i}$  para  $i = 1, 2, \dots, k$ , onde  $m_i = |\mathcal{O}_i|$  e  $y_i \in \mathcal{O}_i$  é um vértice arbitrário. O automorfismo  $\alpha$  tem ordem finita se, e somente se, todos os estados  $\alpha_i$  tem ordem finita. Mais ainda, neste caso, a ordem de  $\alpha$  é igual a*

$$|\alpha| = \text{mmc}(m_1|\alpha_1|, m_2|\alpha_2|, \dots, m_k|\alpha_k|).$$

2. *Suponha que  $\alpha_i = \alpha$  para algum  $y_i \in \mathcal{O}_i$ . Se  $m_i > 1$  então  $\alpha$  tem ordem infinita. Se  $m_i = 1$  então  $\alpha$  tem ordem finita se, e somente se  $\alpha_j$  tem ordem*



finita para todo  $j \neq i$ , neste caso,

$$|\alpha| = \text{mmc}(m_1|\alpha_1|, \dots, m_{i-1}|\alpha_{i-1}|, m_{i+1}|\alpha_{i+1}|, \dots, m_k|\alpha_k|).$$

**Demonstração:**

1. Suponhamos que  $\alpha$  tenha ordem finita, digamos  $l$ . Então, todos os estados de  $\alpha^l$  são iguais a  $e$ , ou seja,  $e = (\alpha^{m_i l}|_{y_i}) = \alpha^{m_i}|_{y_i} \alpha^{m_i}|_{(y_i)\alpha^{m_i}} \dots \alpha^{m_i}|_{(y_i)\alpha^{m_i(l-1)}} = (\alpha^{m_i}|_{y_i})^l$ , pois,  $y_i^{\alpha^{m_i}} = y_i$ . Suponhamos que para cada  $i$ ,  $\alpha_i$  tenha ordem finita. Como  $\alpha_i = \alpha^{m_i}|_{y_i}$ , então  $\alpha^{m_i|\alpha_i}|_{y_i} = e$ . Segue que se  $l$  for um múltiplo de todos os  $m_i|\alpha_i|$ , então  $\alpha^l = e$ . Vamos mostrar agora que

$$|\alpha| = \text{mmc}(m_1|\alpha_1|, \dots, m_{i-1}|\alpha_{i-1}|, m_{i+1}|\alpha_{i+1}|, \dots, m_k|\alpha_k|). \text{ Como}$$

$$\alpha^{\text{mmc}(m_1|\alpha_1|, \dots, m_{i-1}|\alpha_{i-1}|, m_{i+1}|\alpha_{i+1}|, \dots, m_k|\alpha_k|)} = e, \text{ então, } |\alpha| \text{ divide}$$

$$\text{mmc}(m_1|\alpha_1|, \dots, m_{i-1}|\alpha_{i-1}|, m_{i+1}|\alpha_{i+1}|, \dots, m_k|\alpha_k|).$$

Por outro lado, como  $\alpha$  tem ordem finita,  $\alpha|_{y_i}$  também o tem e  $(\alpha|_{y_i})^{|\alpha|} = e$ .

Mas  $|\alpha|_{y_i} = m_i|\alpha_i|$ . Donde, para cada  $i$ ,  $m_i|\alpha_i|$  divide  $|\alpha|$ .

2. Suponhamos por contradição que  $|m_i| > 1$  e que  $\alpha$  tenha ordem finita. Pelo item anterior  $|\alpha|$  é um múltiplo de  $m_i|\alpha_i|$ . Mas  $|\alpha_i| = |\alpha|$  pois  $\alpha_i = \alpha$ .

Suponhamos agora que  $m_i = 1$  e que  $\alpha_j$  tenha ordem finita para todo  $j \neq i$ .

$$\text{Seja } l = \text{mmc}(m_1|\alpha_1|, \dots, m_{i-1}|\alpha_{i-1}|, m_{i+1}|\alpha_{i+1}|, \dots, m_k|\alpha_k|).$$

Para ver que  $\alpha^l = e$ , basta observar que  $\pi_{\alpha^l} = e = \pi_{\alpha_i^l}$  e que  $\alpha^l|_{y_j} = \alpha^{m_j|\alpha_j|R}|_{y_j} = (\alpha^{m_j}|_{y_j})^{|\alpha_j|R} = e$ , para todo  $j \neq i$ .

No caso em que supomos  $\alpha$  de ordem finita com  $m_i = 1$ , então  $\alpha_j$  tem ordem finita para todo  $j \neq i$  pelo item 1.

■

Se  $\alpha$  é um automorfismo de finitos estados, o Lema 3.2.1 sugere um procedimento galhante para encontrar a ordem de  $\alpha$ , em outras palavras, um procedimento que reduz o problema inicial a subproblemas nos níveis inferiores.

A proposição 3.1.1 e o Lema 3.2.1 nos leva a definir o chamado sinalizador de órbita de um automorfismo:

**Definição 3.2.2** *Dado  $\alpha \in \mathcal{A}$  o conjunto*

$$OS(\alpha) = \{\alpha^m|_v \mid v \in Y^*, m = |Orb_\alpha(v)|\}, \quad (3.9)$$

*é chamado sinalizador de órbita do automorfismo  $\alpha$ .*

*Podemos observar que equivalentemente,*

$$OS(\alpha) = \{\alpha|_v \alpha|_{v^\alpha} \cdots \alpha|_{v^{\alpha^{m-1}}} \mid v \in Y^*, m = |Orb_\alpha(v)|\}.$$

Este conjunto contém todos os automorfismos que podem aparecer nos procedimentos *da Ordem e da Conjugação*. Para automorfismos com sinalizadores de órbita finitos vamos modelar tais procedimentos através de certos grafos. O passo fundamental para a decidibilidade destes problemas está no fato de que, neste caso, tais grafos são finitos.

### 3.2.1 O grafo da ordem

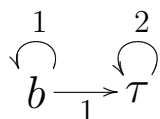
Considere um automorfismo  $\alpha \in \mathcal{A}$  o qual tem sinalizador de órbita finito. Vamos construir um grafo finito  $\Phi(\alpha)$ , chamado *grafo da ordem*, cujo conjunto de vértices é precisamente  $OS(\alpha)$ , que modela o procedimento da ordem. As arestas deste grafo são construídas como segue: Para todo  $\beta \in OS(\alpha)$  considere todas as órbitas  $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_k$  da ação de  $\beta$  sobre  $Y$  e seja  $y_i \in \mathcal{O}_i$  o menor elemento em  $\mathcal{O}_i$ . Segue da Proposição 3.1.1 que  $\beta^{m_i}|_{y_i} \in OS(\alpha)$  para  $m_i = |\mathcal{O}_i|$ , e introduzimos a aresta indexada  $\beta \xrightarrow{m_i} \beta^{m_i}|_{y_i}$  no grafo  $\Phi(\alpha)$  para todo  $i = 1, \dots, k$ . Então o Lemma 3.2.1 pode ser reformulado por:

**Proposição 3.2.3** *Suponha que  $\alpha \in \mathcal{A}$  tenha sinalizador de órbita finito. Então  $\alpha$  tem ordem finita se, e somente se, todas as arestas dos ciclos direcionados no grafo da ordem  $\Phi(\alpha)$  são indexadas por 1.*

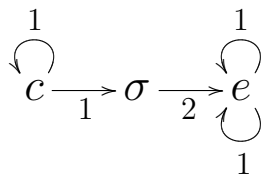
Neste caso a ordem de  $\alpha$  pode ser computada usando o grafo  $\Phi(\alpha)$ . Remova todos os ciclos direcionados em  $\Phi(a)$ . Então o único vértice morto de  $\Phi(a)$ , isto é, vértice sem arestas incidentes, é o automorfismo trivial que tem ordem 1. Então, indutivamente, para  $\beta \in \text{OS}(a)$  considere todas as arestas saindo de  $\beta$ , sejam  $m_1, m_2, \dots, m_k$  os índices de tais arestas e  $\beta_1, \beta_2, \dots, \beta_k$  os vértices finais correspondentes cujas ordens já conhecemos. Então pelo Lema 3.2.1 a ordem de  $\beta$  é o mínimo múltiplo comum dos  $m_i|\beta_i|$ . Vamos ilustrar a construção do grafo da ordem e a solução do problema da ordem no Exemplo 3.2.4 da Seção 3.6.

Nos próximos exemplos vamos ilustrar o procedimento para solução do problema da ordem.

**Exemplo 3.2.4 (Problema da ordem)** *Consideremos os automorfismos  $b = (\tau, b)$  e  $\tau = (e, \tau)\sigma$ . O grafo da ordem  $\Phi(\tau)$  é um subgrafo de  $\Phi(b)$  conforme mostrado na Figura abaixo. Como existe um ciclo indexado por 2,  $\tau$  e  $b$  tem ordem infinita.*



*O grafo da ordem  $\Phi(c)$  para o automorfismo  $c = (c, \sigma)$  é mostrado na Figura abaixo. Como não existem ciclos com índices maiores que 1, temos que  $c$  tem ordem finita. Mais precisamente,  $|c| = 2$ .*



### 3.3 O problema da conjugação para automorfismos de finitos estados

#### 3.3.1 O grafo conjugador

Sejam  $\alpha, \beta \in \mathcal{A}_f$ , automorfismos cujos sinalizadores de órbita sejam finitos. Vamos construir um grafo  $\Psi(\alpha, \beta)$ , chamado *grafo conjugador* de  $\alpha$  e  $\beta$ , onde os vértices estarão associados as novas equações de conjugação e as arestas representarão as dependências entre elas. Tal grafo conterá todos os automorfismos de  $\mathcal{A}$  que conjugam  $\alpha$  em  $\beta$ . Um tal conjugador estará associado a um subgrafo de  $\Psi(\alpha, \beta)$ . Um passo fundamental para decidir conjugação estará no fato de que, embora exista um número infinito de conjugadores para o par  $(\alpha, \beta)$ ,  $\Psi(\alpha, \beta)$  é um grafo finito.

Para cada  $\alpha, \beta \in \mathcal{A}$  denotamos

$$C\Pi(\alpha, \beta) = \{\pi \in Sym(Y) : \pi^{-1}\pi_\alpha\pi = \pi_\beta\}$$

(este conjunto pode ser vazio).

Mais formalmente, os vértices de  $\Psi(\alpha, \beta)$  são elementos do conjunto finito  $U = OS(\alpha) \times OS(\beta) \times Sym(Y)$ , onde  $(x, y, \pi)$  indica um possível conjugador  $x \sim_{\gamma|_u} y$  ( $\gamma|_u$  induz a permutação  $\pi$  sobre  $Y$ ) e  $\pi \in C\Pi(x, y)$ .

**Procedimento.** O grafo  $\Psi(\alpha, \beta)$  será construído em passos como segue:

1. **Inserir vértices iniciais** Escrevamos  $\alpha = (\alpha|_i)_{i=0, \dots, d-1}\pi_\alpha$  e  $\beta = (\beta|_i)_{i=0, \dots, d-1}\pi_\beta$ , onde  $\pi_\alpha, \pi_\beta \in Sym(Y)$ .

Calculemos  $C\Pi(\alpha, \beta)$ , isto é, encontremos todos os  $\pi_\gamma \in Sym(Y)$  tais que  $\pi_\alpha^{\pi_\gamma} = \pi_\beta$  (Isso pode ser feito utilizando a observação sobre centralizador no início da Seção 3.1). Se  $C\Pi(\alpha, \beta)$  for vazio, então não inserimos nenhum vértice inicial e o grafo  $\Psi(\alpha, \beta)$  é vazio. Caso contrario,

inserir um vértice inicial  $(\alpha, \beta, \pi_\gamma)$ , para cada  $\pi_\gamma \in C\Pi(\alpha, \beta)$ .

## 2. Analisar vértices

Conforme já observado em (3.5) e mais geralmente na Proposição 3.1.1, se  $\pi_g \sim_\pi \pi_h$  então o terno  $(g, h, \pi)$  dá origem a um conjunto finito de novas equações de conjugação.

Para um vértice  $(g, h, \pi)$  (não analisado), considere todas as órbitas  $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_k$  da ação de  $g$  (ou de  $\pi_g$ ) sobre  $Y$  e seja  $y_i \in \mathcal{O}_i$  o menor elemento em  $\mathcal{O}_i$  com respeito à ordem escolhida ( $y_i$  sempre denota o menor elemento das órbitas para o terno considerado). Se para algum vértice  $(g, h, \pi)$ , um dos conjuntos  $C\Pi(g^{m_i}|_{y_i}, h^{m_i}|_{y_i^\pi})$ , onde  $m_i = |\mathcal{O}_i|$ , é vazio, então o terno  $(g, h, \pi)$  é um vértice morto. Caso contrário, inserimos a aresta

$$(g, h, \pi) \xrightarrow{y_i} (g^{m_i}|_{y_i}, h^{m_i}|_{y_i^\pi}, \delta), \quad \text{onde } m_i = |\mathcal{O}_i|$$

para cada  $\delta \in C\Pi(g^{m_i}|_{y_i}, h^{m_i}|_{y_i^\pi})$  e  $i = 1, \dots, k$ .

Observemos que  $g^{m_i}|_{y_i} \in \text{OS}(\alpha)$  e  $h^{m_i}|_{y_i^\pi} \in \text{OS}(\beta)$ , e portanto, o terno  $(g^{m_i}|_{y_i}, h^{m_i}|_{y_i^\pi}, \delta) \in U$ .

3. Iteramos esse processo de análise repetidas vezes até que todos os vértices tenham sido analisados e não seja preciso inserir nenhum vértice. Observemos que esse processo termina, pois,  $U$  é finito.

Realizemos agora certas reduções:

4. **Remoção de componentes sem vértices iniciais:** Removamos todas as componentes conexas que não contenham nenhum vértice inicial.
5. **Remoção de vértices mortos:** Removamos todos os vértices mortos juntamente com suas arestas incidentes.
6. **Remoção de vértices:** Removamos todos os vértices  $(g, h, \pi)$  tais que para algum índice  $i = 1, 2, \dots, k$  não exista uma aresta indexada associada à órbita

deste índice. Ou seja, não existe  $(g, h, \pi) \xrightarrow{y_i} (g^{m_i}|_{y_i}, h^{m_i}|_{y_i^\pi}, \delta)$  onde  $m_i = |\mathcal{O}_i|$ , com  $y_i \in \mathcal{O}_i$ , e  $\delta \in C\Pi(g, h)$ .

**7. Iteração dos passos de remoção:** Repetimos tais reduções quantas vezes forem possíveis. Eventualmente podemos obter o grafo vazio. Tal processo termina pela finitude de  $U$ .

Acabamos de mostrar que

**Proposição 3.3.1** *Dados  $\alpha, \beta \in \mathcal{A}_f$  automorfismos cujos sinalizadores de órbita sejam finitos:*

- *O grafo  $\Psi(\alpha, \beta)$  é finito;*
- *$\alpha \sim_{\mathcal{A}} \beta$  se, e somente se,  $\Psi(\alpha, \beta)$  é não vazio.*

**Corolário 3.3.2** *Nas condições acima, se  $\alpha \sim_{\mathcal{A}} \beta$  então existe um algoritmo que exhibe  $\gamma \in \mathcal{A}$ , um conjugador.*

**Demonstração:** Basta construir o grafo  $\Psi(\alpha, \beta)$ . Se ao término da construção algum dos vértices iniciais tiverem permanecido no grafo, então  $\alpha$  e  $\beta$  são conjugados em  $\mathcal{A}$ .

A primeira parte segue do algoritmo para construção do grafo conjugador.

Caso  $\Psi(\alpha, \beta)$  seja não vazio, eles são conjugados e todo conjugador  $\gamma$  tal que  $\alpha \sim_{\gamma} \beta$  pode ser construído nível por nível como segue. Escolha algum vértice inicial da construção de  $\Psi(\alpha, \beta)$ , isto é,  $(\alpha, \beta, \pi)$  para algum  $\pi$ , e defina a ação de  $\gamma$  sobre  $Y$  por  $\pi_\gamma = \pi$ , ou seja,  $y^\gamma = y^\pi$  para  $y \in Y$ .

Sejam  $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_k$  as órbitas da ação de  $\alpha$  (ou  $\pi_\alpha$ ) sobre  $Y$  e sejam  $y_i$  os representantes (minimais) de órbitas. Pela construção de  $\Psi(\alpha, \beta)$ , para cada  $i = 1, \dots, k$  existe uma aresta saindo de  $(\alpha, \beta, \pi)$  para um vértice  $(g_i, h_i, \pi_i)$  associado a

essa órbita. Para cada órbita, isto é, cada  $i$ , escolha uma tal aresta saindo de  $(\alpha, \beta, \pi)$  juntamente com seu vértice  $(g_i, h_i, \pi_i)$  correspondente. Considere  $\gamma|_{y_i}$  o estado de  $\gamma$  em  $y_i$ . Definimos a ação de  $\gamma|_{y_i}$  sobre  $Y$  por  $\pi_{\gamma|_{y_i}} = \pi_i$  ou seja,  $y^{\gamma|_{y_i}} = y^{\pi_i} \forall y \in Y$ . Agora se  $\bar{y} \in \mathcal{O}_i$  então a ação de  $\gamma|_{\bar{y}}$  sobre  $Y$  é definida unicamente em termos de  $\gamma|_{y_i}$  pela fórmula (3.6).

Procedemos de maneira similar para definir a ação de  $\gamma$  nos níveis seguintes. Como  $\Psi(\alpha, \beta)$  é finito, em algum estágio da construção ou poderemos escolher entre os vértices  $(e, e, \pi)$ , para todo  $\pi \in \text{Sym}(Y)$  (neste caso qualquer automorfismo de  $\mathcal{A}$  pode ser escolhido como estado de  $\gamma$  neste ponto), ou um vértice  $(g, h, \pi)$  que havia aparecido em outro estágio do processo, se repete. Suponha que  $g \sim_{\gamma|_u} h$  no primeiro estágio e  $g \sim_{\gamma|_v} h$  no segundo estágio. Então  $\gamma|_v = c\gamma|_u$ , onde  $c$  centraliza  $g$ . Isso define completamente  $\gamma$ . ■

### Conjugadores básicos

Sejam  $\alpha, \beta \in \mathcal{A}_f$  automorfismos cujos sinalizadores de órbita sejam finitos e tais que  $\Psi(\alpha, \beta)$  seja não vazio. Das considerações anteriores, sabemos que existe  $\gamma \in \mathcal{A}$ , tal que  $\alpha \sim_\gamma \beta$ . Mas não é claro se existe um conjugador que seja funcionalmente recursivo. Vamos mostrar que basta que  $\Psi(\alpha, \beta)$  seja não vazio para que construamos certos conjugadores, chamados *conjugadores básicos* para o par  $(a, b)$ , que serão automorfismos funcionalmente recursivos. A ideia central é fazer menos escolhas possíveis, no sentido de que se temos um terno  $(c, d, \pi)$  em certo estágio da construção, então vamos escolher a permutação  $\pi \in C\Pi(c, d)$  sempre que o par  $(c, d)$  aparecer novamente. Basicamente, para cada dois vértices  $(c, d, \pi_1)$  e  $(c, d, \pi_2)$  obtidos pela construção, insistimos em  $\pi_1 = \pi_2$ . O que está por detrás desta ideia é o fato de que todo automorfismo de crescimento limitado, em níveis suficientemente inferiores, todos seus estados são automorfismos finitários ou circuitos. Todo conjugador básico pode ser definido usando certos subgrafos especiais do grafo conjugador

$\Psi(a, b)$ .

Um *subgrafo definidor* é um subgrafo  $S$  de  $\Psi(a, b)$  que satisfaz as seguintes propriedades:

1.  $S$  contém um vértice inicial  $(\alpha, \beta, \pi)$  para algum  $\pi \in C\Pi(\alpha, \beta)$ .
2. Para cada vértice  $(g, h, \pi)$  de  $S$  e cada  $y_i$  (representante minimal de órbita pela ação de  $g$  sobre  $Y$ ), existe uma, e somente uma, aresta saindo de  $(g, h, \pi)$  para o vértice associado à respectiva órbita.
3. Se  $a = (g, h, \pi) \in S$  então  $\bar{a} = (g, h, \bar{\pi}) \notin S$  se  $\pi \neq \bar{\pi}$ , ou seja, para cada  $g \in OS(\alpha)$  e  $h \in OS(\beta)$  existe no máximo um vértice do tipo  $(g, h, *)$  no grafo  $S$ .
4. Se  $(e, e, \pi) \in S$  então  $\pi = e$ .

Observe que se  $\Psi(\alpha, \beta)$  é não vazio, sempre existe pelo menos um subgrafo satisfazendo, as propriedades 1 – 4, e por outro lado, existem finitos tais subgrafos. Para cada grafo definidor, vamos construir um conjugador  $\gamma = \gamma(S)$  associado a este, chamado *conjugador básico*:

Vamos construir um sistema funcionalmente recursivo envolvendo cada conjugador  $\gamma_{(g,h)}$  tal que  $g \sim \gamma_{(g,h)}h$ , onde  $(g, h, \pi)$  é um vértice de  $S$  e em particular, construímos  $\gamma_{(\alpha,\beta)}$  tal que  $\alpha \sim \gamma_{(\alpha,\beta)}\beta$ .

Definamos a ação de  $\gamma_{(\alpha,\beta)}$  sobre  $Y$  por  $\pi_{\gamma_{(\alpha,\beta)}} = \pi$ , ou seja,  $(y)^{\gamma_{(\alpha,\beta)}} = (y)^\pi$  para  $y \in Y$ . Aqui a permutação  $\pi \in C\Pi(\alpha, \beta)$  é unicamente determinada pelo terno  $(\alpha, \beta, \pi)$  pertencente a  $S$ . Agora definimos o conjugador  $\gamma_{(\alpha,\beta)}$  nível por nível, da seguinte maneira: Para toda aresta  $(g, h, \pi) \xrightarrow{y} (c, d, \delta)$  em  $S$ , definimos os estados do conjugador  $\gamma_{(g,h)}$  através do representante da órbita  $\mathcal{O} = \{y, (y)g, (y)g^2, \dots, (y)g^{m-1}\}$  de  $y$  sobre  $g$  recursivamente pela regra

$$\gamma_{(g,h)}|_y = \gamma_{(c,d)} \quad \text{e} \quad \gamma_{(g,h)}|_{yg^i} = (g^i|_y)^{-1} \cdot \gamma_{(c,d)} \cdot h^i|_{y^\pi}, \quad (3.10)$$



para  $i = 1, \dots, m - 1$ . Estas regras definem completamente os automorfismos  $\gamma_{(g,h)}$ . Pela Proposição 3.1.1 cada automorfismo  $\gamma_{(g,h)}$  é de fato um conjugador para o par  $(g, h)$ . Ou seja,  $\gamma_{(\alpha,\beta)}$  é um conjugador para o par  $(\alpha, \beta)$ .

Suponhamos que um vértice  $(g, h, \pi)$  que havia aparecido em certo estágio do processo, se repita. Mais precisamente  $g \sim_{\gamma|_u} h$  no primeiro estágio e  $g \sim_{\gamma|_v} h$  no segundo estágio, e portanto  $\gamma|_v = (\gamma|_u)|_w$  para certos  $w, u, v$  de comprimentos minimais tal que isso ocorra. Então, conforme observado,  $\gamma|_v = c\gamma|_u$ , onde  $c$  centraliza  $g$ , e como  $\gamma|_v$  é um estado de  $\gamma|_u$ , chegamos que  $c\gamma|_u$  é um estado de  $\gamma|_u$ . Da propriedade (3) do grafo definidor temos que  $c = e$ . Já que o grafo  $S$  é finito e os automorfismos  $\alpha$  e  $\beta$  são de finitos estados, obtemos um sistema funcionalmente recursivo que define unicamente o conjugador básico  $\gamma = \gamma_{(\alpha,\beta)}$  dado pelo subgrafo  $S$ .

Provamos os seguintes resultados:

**Lema 3.3.3** *Sejam  $\alpha, \beta \in \mathcal{A}_f$  automorfismos cujos sinalizadores de órbita sejam finitos. Se o grafo conjugador  $\Psi(\alpha, \beta)$  é não vazio, então existe pelo menos um conjugador básico para o par  $(\alpha, \beta)$  e todo conjugador básico é um automorfismo funcionalmente recursivo.*

**Teorema 3.3.4** *Sejam  $\alpha, \beta \in \mathcal{A}_f$  automorfismos cujos sinalizadores de órbita sejam finitos. Então  $\alpha \sim_{\mathcal{A}} \beta$ , se, e somente se,  $\alpha \sim_{\mathcal{A}_{fr}} \beta$  se, e somente se, o grafo conjugador  $\Psi(\alpha, \beta)$  é não vazio.*

Em particular, provamos que:

**Teorema 3.3.5** *O problema da conjugação para automorfismos de finitos estados com sinalizadores de órbita finitos é decidível nos grupos  $\mathcal{A}$  e  $\mathcal{A}_{fr}$ .*

### 3.3.2 Problema da conjugação simultâneo

Dado um grupo  $G$ , dizemos que o problema da conjugação simultâneo é decidível para este grupo se existe um algoritmo que para todo  $k$  (inteiro positivo) e dadas sequencias  $a_1, a_2, \dots, a_k$  e  $b_1, b_2, \dots, b_k$  em  $G$ , decide se existe um elemento  $h \in G$  tal que  $h^{-1}a_i h = b_i$  para todo  $i$ .

O conceito de  $a_1, a_2, \dots, a_k$  e  $b_1, b_2, \dots, b_k$  em  $G$  simultaneamente conjugados em um grupo  $H$  é completamente análogo ao já definido.

O mesmo método funciona para o problema da conjugação simultâneo, o qual, dados automorfismos  $a_1, a_2, \dots, a_k$  e  $b_1, b_2, \dots, b_k$  pergunta se existe um automorfismo  $h$  tal que  $h^{-1}a_i h = b_i$  para todo  $i$ . Nesse caso, nós novamente consideramos as permutações  $\pi$  tais que  $\pi^{-1}a_i \pi = b_i$  para todo  $i$ , tomando a órbita  $\mathcal{O}_i$  da ação  $a_i$  sobre  $Y$ , e  $y_i \in \mathcal{O}_i$  o menor elemento da órbita e  $m_i = |\mathcal{O}_i|$ . Então o problema se reduz ao problema da conjugação simultâneo para  $a^{m_1}|_{y_1}, a^{m_2}|_{y_2}, \dots, a^{m_k}|_{y_k}$  e  $b^{m_1}|_{y_1}, b^{m_2}|_{y_2}, \dots, b^{m_k}|_{y_k}$ . Se os automorfismos  $a_i$  e  $b_i$  são de finitos estados e tem sinalizadores de órbitas finitos, então podemos similarmente construir o grafo conjugador associado e portanto, nesse caso, o Teorema 3.3.4 vale.

### 3.3.3 Conjugação de automorfismos contráteis

Vimos no Lema 3.3.3 que se  $a, b \in \mathcal{A}_f$  tiverem sinalizadores de órbita finitos e forem conjugados em  $\mathcal{A}$  então eles são conjugados por algum automorfismo funcionalmente recursivo. A pergunta geral é: se dois automorfismos forem conjugados por um automorfismo funcionalmente recursivo, como decidir se existe um automorfismo de finitos estados que os conjuga? Essa pergunta em geral está em aberto, mas conseguimos respondê-la sob hipóteses de contração e finitude dos sinalizadores de órbitas. Mais especificamente, obtemos o seguinte resultado:

**Teorema 3.3.6** *Dois automorfismos contráteis  $\alpha, \beta \in \mathcal{A}$  cujos sinalizadores de órbita sejam finitos, são conjugados em  $\mathcal{A}$  se, e somente se, são conjugados em  $\mathcal{A}_f$ .*

**Demonstração:** Para isso, vamos provar que nestas condições, todos os conjugadores básicos para o par  $(\alpha, \beta)$  são de finitos estados.

■

**Observação 3.3.7** *Seja  $S$  um subconjunto finito de  $\mathcal{A}_f$ . Então o fecho por estados  $\tilde{S}$  de  $S$  (ou seja  $\tilde{S}$  é o menor conjunto que contém  $S$  e que é fechado por estados) é de finitos estados.*

O exemplo abaixo ilustra a dificuldade em se mostrar a finitude de um automorfismo funcionalmente recursivo.

**Exemplo 3.3.8** *Sejam*

$$\begin{aligned} a &= (a|_0, a|_1), a|_0 = (a|_{00}, a|_{01}), \sigma, a|_1 = (a|_{10}, a|_{11}), \\ b &= (b|_0, b|_1), b|_0 = (b|_{00}, b|_{01}), b|_1 = (b|_{10}, b|_{11}). \end{aligned}$$

$\gamma = a(\gamma, \gamma)b$  é o conjugador para o par  $(a, b)$ . Então, ao tentarmos checar se  $\gamma$  é de finitos estados, temos de calcular

$$\begin{aligned} \gamma &= (a|_0\gamma b|_0, a|_1\gamma b|_1), \\ a|_0\gamma b|_0 &= a|_0(a|_0\gamma b|_0, a|_1\gamma b|_1)b|_0 \\ &= (a|_{00}, a|_{01})\sigma(a|_0\gamma b|_0, a|_1\gamma b|_1)(b|_{00}, b|_{01}) \\ &= (a|_{00}a|_1\gamma b|_1b|_{01}, a|_{01}a|_0\gamma b|_0b|_{00})\sigma, \\ a|_1\gamma b|_1 &= (a|_{10}, a|_{11})(a|_0\gamma b|_0, a|_1\gamma b|_1)(b|_{10}, b|_{11}) \\ &= (a|_{10}a|_0\gamma b|_0b|_{10}, a|_{11}a|_1\gamma b|_1b|_{11}). \end{aligned}$$

Portanto,  $\gamma$  tem como estados a seguinte sequência de conjuntos com estados de cada nível:

$$\begin{aligned} Q(\gamma)_0 &= \{\gamma\}, \\ Q(\gamma)_1 &= \{a|_0\gamma b|_0, a|_1\gamma b|_1\}, \end{aligned}$$

$$Q(\gamma)_2 = \begin{cases} a|_{00}a|_{1\gamma}b|_{1b}|_{01}, & a|_{01}a|_{0\gamma}b|_{0b}|_{00}, \\ a|_{10}a|_{0\gamma}b|_{0b}|_{10}, & a|_{11}a|_{1\gamma}b|_{1b}|_{11} \end{cases}$$

$$\vdots$$

Tais cálculos motivam o seguinte Lema – o qual é uma reformulação da Proposição 2.11.5 de [Nek05].

**Lema 3.3.9** *Seja  $G$  um grupo contrátil fechado por estados e  $S$  um subconjunto finito de  $G$ . Então o conjunto de todos os elementos da forma*

$$(((h_1|_{y_1} \cdot h_2)|_{y_2} \cdot h_3)|_{y_3} \cdot \dots \cdot h_n|_{y_n}, \quad (h_n \cdot \dots \cdot (h_n \cdot (h_2 \cdot h_1|_{y_1})|_{y_2})|_{y_3} \cdot \dots)|_{y_n},$$

onde  $h_i \in S$  e  $y_i \in Y$ , é finito.

**Demonstração:**

Pela observação 3.3.7 podemos supor que  $S$  seja um conjunto fechado por estados contendo  $\mathcal{N}$ . Existe um inteiro positivo  $k$  tal que  $S^2|_v \subset \mathcal{N} \subset S$  para todas as palavras  $v$ ,  $|v| \geq k$ . Então  $S^{2t}|_v \subset S^t$  para todo  $v \in Y^k$  e  $t \geq 1$ . É suficiente provar que existem finitos elementos da forma

$$(((h_1|_{v_1} \cdot h_2)|_{v_2} \cdot h_3)|_{v_3} \cdot \dots \cdot h_t)|_{v_t}$$

para  $h_i \in S^k$  e  $v_i \in Y^k$ . Então  $h_1|_{v_1} \in S^k$  e  $(h_1|_{v_1} \cdot h_2)|_{v_2} \in S^{2k}|_{v_2} \subset H^k$ . Indutivamente concluímos que todos os elementos da forma acima estão em  $S^k$ , o qual é um conjunto finito. ■

O próximo Lema é similar ao Corolário 2.11.7 de [Nek05].

**Lema 3.3.10** *Seja  $G$  um grupo contrátil fechado por estados. Então para toda coleção  $H = \{h_y, h'_y\}_{y \in Y} \subset G$ , e uma permutação  $\pi \in \text{Sym}(Y)$  o automorfismo definido recursivamente por*

$$g = (h_{y_1}gh'_{y_1}, h_{y_2}gh'_{y_2}, \dots, h_{y_d}gh'_{y_d})\pi$$

é de finitos estados.

**Demonstração:** Vamos mostrar primeiramente, por indução sobre  $t$  que para toda palavra  $y_0y_1y_2 \dots y_t \in Y^*$ , vale que

$$\begin{aligned} g|_{y_0y_1y_2 \dots y_t} &= \\ &= (((((h_1|_{y_1} \cdot h_2)|_{y_2} \cdot h_3)|_{y_3} \cdot \dots \cdot h_t)|_{y_t} h_{t+1}) \cdot g \cdot (h'_{t+1}(h'_t \cdot \dots \cdot (h'_3 \cdot (h'_2 \cdot h'_1|_{y_1})|_{y_2})|_{y_3} \cdot \dots)|_{y_t})), \end{aligned} \quad (3.11)$$

onde  $h_i, h'_i$  são elementos de  $H$ , e  $y_i \in Y$ .

Observemos que  $g|_{y_0} = h_1gh'_1$  para certos  $h_1, h'_1 \in H$ .

Suponhamos que

$$\begin{aligned} g|_{y_0y_1y_2 \dots y_{t-1}} &= \\ &= (((((h_1|_{y_1} \cdot h_2)|_{y_2} \cdot h_3)|_{y_3} \cdot \dots \cdot h_{t-1})|_{y_{t-1}} h_t) \cdot g \cdot (h_t \cdot (h'_{t-1} \cdot \dots \cdot (h'_3 \cdot (h'_2 \cdot h'_1|_{y_1})|_{y_2})|_{y_3} \cdot \dots)|_{y_{t-1}})). \end{aligned}$$

Então

$$\begin{aligned} g|_{y_0y_1y_2 \dots y_t} &= \\ &= (((((h_1|_{y_1} \cdot h_2)|_{y_2} \cdot \dots \cdot h_{t-1})|_{y_{t-1}} \cdot h_t)|_{y_t} \cdot g|_{(y_t)\bar{h}} \cdot (h_t \cdot (h'_{t-1} \cdot \dots \cdot (h'_2 \cdot h'_1|_{y_1})|_{y_2} \cdot \dots)|_{y_{t-1}})|_{(y_t)g\bar{h}} \\ &= (((((h_1|_{y_1} \cdot h_2)|_{y_2} \cdot \dots \cdot h_{t-1})|_{y_{t-1}} \cdot h_t)|_{y_t} \cdot h_{t+1} \cdot g \cdot h'_{t+1} \cdot (h'_t \cdot (h'_{t-1} \cdot \dots \cdot (h'_2 \cdot h'_1|_{y_1})|_{y_2} \cdot \dots)|_{y_{t-1}})|_{y_t}, \end{aligned}$$

onde  $g|_{(y_t)\bar{h}} = h_{t+1} \cdot g \cdot h'_{t+1}$ , para certos  $h_{t+1}, h'_{t+1} \in H$ , e  $(y_t)g\bar{h} = y_t$ .

Pelo Lema 3.3.9, o conjunto de todos os elementos da forma (3.11) é finito. Portanto,  $g$  é de finitos estados. ■

**Lema 3.3.11** *Seja  $\Gamma \subset \mathcal{A}$  um subconjunto finito de automorfismos. Suponha que existam dois grupos  $G_1, G_2$ , contráteis fechados por estados e dois subconjuntos finitos  $A \subset G_1, B \subset G_2$  satisfazendo a condição de que para todo  $g \in \Gamma$  e todo  $y \in Y$  existem  $a \in A, b \in B$  e  $g' \in \Gamma$  tais que  $g_y = ag'b$ . Sob estas condições, todos os automorfismos de  $\Gamma$  são de finitos estados.*

**Demonstração:** A demonstração é essencialmente a mesma do Lema 3.3.10. A única diferença é que no lado direito da equação (3.11) ao invés de  $g$ , pode aparecer qualquer elemento do conjunto finito  $\Gamma$ . ■

**Corolário 3.3.12** *Sejam  $\alpha, \beta \in \mathcal{A}$  dois automorfismos conjugados em  $\mathcal{A}$ , contráteis e cujos sinalizadores de órbita sejam finitos. Então todos os conjugadores básicos para o par  $(\alpha, \beta)$  são de finitos estados.*

**Demonstração:** Considere o grafo  $\Psi(\alpha, \beta)$  e seja  $\gamma$  um conjugador básico de  $\alpha, \beta$ . Seja  $\Gamma$  o conjunto dos conjugadores, cada um deles resolvendo as equações que surgem ao longo de  $\gamma$ . Existem finitos deles. Sejam  $A$  o conjunto dos coeficientes a esquerda de  $\Gamma$  e  $B$  o conjunto dos coeficientes a direita de  $\Gamma$ . Seja  $G_1$  o grupo fechado por estados gerado por  $A$  e  $G_2$  o grupo fechado por estados gerado por  $B$ . Estamos nas hipóteses do Lema 3.3.11 portanto,  $\gamma$  é de finitos estados. ■

**Demonstração do Teorema 3.3.6:** O resultado segue imediatamente do fato de que os conjugadores básicos são de finitos estados. ■

**Proposição 3.3.13** *Sejam  $\alpha, \beta \in \mathcal{A}$  conjugados  $\mathcal{A}_f$ . Então  $\alpha$  tem sinalizador de órbita finito se, e somente se,  $\beta$  também o tem.*

**Demonstração:** Suponha  $\gamma^{-1}\alpha\gamma = \beta$  para algum  $\gamma$ , automorfismo de finitos estados, e  $\alpha$  com sinalizador de órbita finito. Então  $m = |\text{Orb}_\alpha(v)| = |\text{Orb}_\beta(v^\gamma)|$  para todo  $v \in Y^*$  e

$$(\beta^m)|_{v^\gamma} = \gamma|_v^{-1}\alpha^m|_v\gamma|_v \in \gamma|_v^{-1}OS(\alpha)\gamma|_v \subset Q(\gamma)^{-1}OS(\alpha)Q(\gamma),$$

o qual é finito, pois  $Q(\gamma)$ , o conjunto de estados de  $\gamma$ , é um conjunto finito. ■

**Exemplo 3.3.14** *Nos próximos exemplos, vamos investigar quais interações possíveis entre as propriedades de contração, finitude do sinalizador de órbita, crescimento de autômato e finitude do conjunto de estados.*

1. A máquina de adição binária  $\tau$  é de crescimento limitado, e conforme já observamos, é contrátil e tem sinalizador de órbita finito. Observe que  $OS(\tau) = \{\tau\}$ .

### **Sobre contração e crescimento**

2. Sabemos que todo subgrupo fechado por estados e finitamente gerado de  $Pol(0)$  é contrátil, contudo, é de esperar que o conjunto dos automorfismos contráteis seja estritamente maior que  $Pol(0)$ . De fato, os automorfismos  $b = (\tau, c)\sigma$ ,  $c = (\tau, b)$  estão em  $Pol(1) \setminus Pol(0)$ . Ao mesmo tempo  $b$  e  $c$  são contráteis, para o grupo fechado por estados gerado por  $\tau, b, c$  tem núcleo  $\mathcal{N} = \{e, \tau^{\pm 1}, b^{\pm 1}, c^{\pm 1}, (\tau^{-1}b)^{\pm 1}, (\tau^{-1}c)^{\pm 1}, (b^{-1}c)^{\pm 1}\}$ .

Este exemplo mostra também que a hipótese de finitude do sinalizador de órbita no Teorema 3.3.6 e no Corolário 3.3.12 são necessárias, já que  $b$  e  $c$  são contráteis mas tem sinalizadores de órbita infinitos: Todos os elementos  $\tau^{2n}b$  para  $n \geq 0$  são distintos e estão nos conjuntos  $OS(b)$  e  $OS(c)$ .

3. Observamos no Capítulo 1 que o automorfismo  $b = (b, b)\sigma$  tem crescimento exponencial e é contrátil. Mais que isso, ele tem sinalizador de órbita finito. Observe que  $OS(b) = \{e, b\}$ .
4. É natural perguntar se a classe dos automorfismos contráteis contém  $Pol(m)$  para algum  $m > 0$ . A resposta é negativa e contra-exemplo é o automorfismo  $b$  dado por  $b = (\tau, b)$ .  $Q(b) = \{e, \tau, b\}$ ,  $b$  está em  $Pol(1) \setminus Pol(0)$ , e  $OS(b) = \{\tau, b\}$ . Contudo  $b$  não é contrátil, pois, caso fosse todos os elementos  $b^n = (\tau^n, b^n)$  estariam no núcleo para  $n$  suficientemente grande. Contudo, os  $b^n$  são todos distintos para  $n > 1$ , o que nos daria um núcleo infinito.
5. Observamos no Capítulo 1 que o automorfismo  $\alpha = (\alpha, \alpha^2)\sigma$  é funcionalmente recursivo mas não é de finitos estados. Portanto, o automorfismo  $c = (\alpha, \alpha^{-1})\sigma$  é funcionalmente recursivo, de infinitos estados mas tem sinalizador de órbita finito. Observemos que  $OS(c) = \{e, c\}$ .

### 3.4 Conjugação de automorfismos de crescimento limitado

Na seção anterior vimos alguns resultados para automorfismos de finitos estados que tem sinalizador de órbita finito. Contudo, checar que um dado automorfismo de finitos estados tem sinalizador de órbita finito, pode não ser um problema fácil. Vamos mostrar que algumas importantes classes de automorfismos satisfazem esta condição.

**Observação 3.4.1** *Todo automorfismo  $\alpha$ , de ordem finita, tem sinalizador de órbita finito.*

Basta observar que o conjunto  $OS(\alpha)$  é uma limitação para o número de todos os estados de todas as potências de  $\alpha$  o qual é finito. Em particular, se um automorfismo de finitos estados tem sinalizador de órbita infinito, então ele tem ordem infinita.

**Proposição 3.4.2** *Todo automorfismo de crescimento limitado tem sinalizador de órbita finito.*

**Demonstração:** Seja  $\alpha$  automorfismo de crescimento limitado e escolha uma constante  $C$  tal que o número de estados  $e \neq \alpha|_v$ ,  $v \in Y^n$ , não seja maior que  $C$  para todo  $n \geq 0$ . Então, para todo  $v \in Y^*$  o estado  $\alpha^m|_v$  onde  $m = |Orb_\alpha(v)|$ , é um produto de não mais que  $C$  estados de  $\alpha$  temos então que  $OS(\alpha)$  é finito. ■

Em particular, o procedimento *da Conjugação* decide se dois automorfismos de crescimento limitado são conjugados em  $\mathcal{A}$  e o procedimento *da Ordem* encontra a ordem de um automorfismo de crescimento limitado.

Acabamos de mostrar que

**Corolário 3.4.3** *1. O problema da ordem para automorfismos de crescimento limitado é decidível.*



2. *Problema da conjugação (simultâneo) para automorfismos de crescimento limitado é decidível em  $\mathcal{A}$ .*

**Teorema 3.4.4** *Dois automorfismos de crescimento limitado são conjugados no grupo  $\mathcal{A}$  se, e somente se, são conjugados no grupo  $\mathcal{A}_f$ .*

**Demonstração:** Cada um destes dois automorfismos de  $Pol(0)$  são contráteis por [BN03] e tem sinalizadores de órbita finitos pela Proposição 3.4.2. Portanto, podemos aplicar o Teorema 3.3.6. ■

**Corolário 3.4.5** *Seja  $\alpha$  um automorfismo de crescimento limitado. Então  $\alpha$  e  $\alpha^{-1}$  são conjugados em  $\mathcal{A}_f$ .*

**Demonstração:** Basta observar que uma permutação de  $Sym(Y)$  e sua inversa são conjugadas em  $Sym(Y)$ , de onde temos que  $\Psi(\alpha, \alpha^{-1})$  é não vazio, isto é,  $\alpha$  e  $\alpha^{-1}$  são conjugados em  $\mathcal{A}$ . Pelo Teorema 3.4.4 segue o resultado. ■

**Corolário 3.4.6** *Sejam  $\alpha$  um automorfismo de crescimento limitado,  $\beta$  um automorfismo contrátil, ambos conjugados em  $\mathcal{A}$ . Então  $\alpha$  e  $\beta$  são conjugados em  $\mathcal{A}_f$  se, e somente se,  $\beta$  tem sinalizador de órbita finito.*

**Demonstração:** Segue do resultado [BN03], de que automorfismos de crescimento limitado são contráteis, e das Proposições 3.4.2 e 3.3.13. ■

## 3.5 Conjugação de automorfismos limitados por automorfismos finitários

Recordemos que  $P_k$  é grupo de automorfismos da subárvore finita  $\mathcal{T}_d^{[k]} \subset \mathcal{T}_d$  truncada no nível  $k$ , ou seja,  $\mathcal{T}_d^{[k]}$  contém apenas vértices de comprimento menor ou igual a  $k$  e  $P_k < Pol(-1) < \mathcal{A}_f$ .

Começamos mostrando que conjugação em  $Pol(-1)$  é localmente controlada.

**Proposição 3.5.1** *Sejam  $\alpha, \beta \in P_k \leq Pol(-1)$ . Se  $\alpha \sim_{\mathcal{A}} \beta$  então,  $\alpha \sim_{P_k} \beta$ .*

**Demonstração:** Como  $\alpha \sim_{\mathcal{A}} \beta$  então  $\pi_{\alpha} \sim_{Sym(Y)} \pi_{\beta}$ . Vamos proceder por indução sobre  $k$ . Se  $k = 0$ , então  $\alpha, \beta \in P_0 = Sym(Y)$ , ou seja,  $\pi_{\alpha} = \alpha$  e  $\pi_{\beta} = \beta$ , donde eles são conjugados em  $P_k$ .

Suponhamos  $k \geq 1$  e escrevamos  $\alpha = (\alpha|_i) \pi_{\alpha}, \beta = (\beta|_i) \pi_{\beta}$ .

Seja  $\gamma \in \mathcal{A}$  tal que  $\alpha \sim_{\gamma} \beta$  e escrevamos

$$\gamma = (\gamma|_i) \pi_{\gamma} \quad (3.12)$$

Para cada  $i = 0, \dots, d-1$ , recordemos da equação (3.5) que se  $m = |Orb_{\alpha}(i)|$ , então,

$$\gamma|_i = \left( \alpha|_{i(\pi_{\alpha})^{m-1}(\alpha)}^{-1} \dots \alpha|_{i\pi_{\alpha}}^{-1} \alpha|_i^{-1} \right) \gamma|_i \left( \beta|_{i\pi_{\gamma}} \beta|_{i\pi_{\alpha}\pi_{\gamma}} \dots \beta|_{i(\pi_{\alpha})^{m-1}\pi_{\gamma}} \right),$$

ou seja,

$$\alpha|_i \alpha|_{i\pi_{\alpha}} \dots \alpha|_{i(\pi_{\alpha})^{m-1}} \sim_{\gamma|_i} \beta|_{i\pi_{\gamma}} \beta|_{i\pi_{\alpha}\pi_{\gamma}} \dots \beta|_{i(\pi_{\alpha})^{m-1}\pi_{\gamma}} \left( = \beta|_{i\pi_{\gamma}} \beta|_{i\pi_{\gamma}\pi_{\beta}} \dots \beta|_{i\pi_{\gamma}(\pi_{\beta})^{m-1}} \right). \quad (3.13)$$

Como  $\alpha \in P_k$ , então cada fator de  $\alpha|_i \alpha|_{i\pi_{\alpha}} \dots \alpha|_{i(\pi_{\alpha})^{m-1}}$  está em  $P_{k-1}$  e então  $\alpha|_i \alpha|_{i\pi_{\alpha}} \dots \alpha|_{i(\pi_{\alpha})^{m-1}} \in P_{k-1}$ . Analogamente concluímos que  $\beta|_{i\pi_{\gamma}} \beta|_{i\pi_{\alpha}\pi_{\gamma}} \dots \beta|_{i(\pi_{\alpha})^{m-1}\pi_{\gamma}} \in P_{k-1}$ . Como eles são conjugados em  $\mathcal{A}$  por  $\gamma|_i$ , pela hipótese de indução existe  $h|_i \in P_{k-1}$  que os conjuga.

A existência de um conjugador  $h \in P_k$  para o par  $(\alpha, \beta)$ , segue do fato de que  $\pi_{\alpha} \sim_{Sym(Y)} \pi_{\beta}$ .

■

### 3.5.1 Decidindo conjugação entre automorfismos não finitários por automorfismos finitários

Consideremos agora o problema de decidir se dois automorfismos de crescimento limitado, não ambos finitários, são conjugados em  $Pol(-1)$ . Uma abordagem, é fazer uma restrição sobre a profundidade de um possível conjugador finitoário.

Sejam  $a, b$  dois automorfismos de crescimento limitado e suponhamos que eles sejam conjugados em  $Pol(-1)$ . Escolhamos um conjugador finitoário  $h$  para o par  $(a, b)$  de menor profundidade possível. Todo estado  $h|_y$ , onde  $y \in Y$ , é um conjugador finitoário para o par  $(a^m|_y, b^m|_{y^h})$ , onde  $m = |Orb_a(y)|$ , e tem profundidade menor que a de  $h$ . Contudo, é possível que todo par  $(a^m|_y, b^m|_{y^h})$ , para  $y \in Y$  e  $m = |Orb_a(y)|$ , seja conjugado por um automorfismo finitoário de profundidade, digamos, menor ou igual a  $d$ , enquanto  $(a, b)$  não sejam conjugados por um automorfismo finitoário de profundidade menor ou igual a  $d+1$ . Assim continuamos sem obter uma limitação na profundidade de  $h$ , mesmo tendo uma limitação para a profundidade do conjugador finitoário de cada par  $(a^m|_y, b^m|_{y^h})$ . O problema é que precisamos encontrar um conjugador finitoário  $h|_y$  para o par  $(a^m|_y, b^m|_{y^h})$  de tal forma que todos os estados em dependência deste (isto é, com índices na mesma órbita),  $h|_{(y)a^i} = (a^i|_y)^{-1} \cdot h|_y \cdot b^i|_{y^h}$  para  $i = 0, \dots, m-1$  sejam finitários. Para descrever tais dependências vamos introduzir o que chamamos de *configurações de órbitas*.

#### Configurações de Órbitas

Fixemos um conjugador  $h$  tal que  $a \sim_h b$  e para toda órbita  $\mathcal{O}$  da ação de  $a$  sobre  $Y^*$ , seja  $v$  o menor elemento da órbita e seja  $m = |\mathcal{O}|$ . A *configuração da órbita*  $\mathcal{O}_v$  (com relação ao conjugador  $h$ ) é o conjunto  $\mathcal{C} = \{(a^m|_v, b^m|_{v^h}), DP_{\mathcal{C}}\}$ , onde  $(a^m|_v, b^m|_{v^h})$  é chamado *par principal* de  $\mathcal{C}$  e o conjunto  $DP_{\mathcal{C}}$  se refere às dependências envolvendo a órbita  $\mathcal{O}$  e os estados de  $h$ :

$$DP_{\mathcal{C}} = \{(a^i|_v, b^i|_{v^h}), \text{ para } i = 0, \dots, m-1\}. \quad (3.14)$$

**Definição 3.5.2** *Se  $(c, d) \in DP_{\mathcal{C}}$  e  $h|_{(y)a^i} = c^{-1}h|_y d$ , então dizemos que  $h|_{(y)a^i}$  é um estado associado ao par  $(c, d)$ .*

Observe que o par  $(a, b)$  aparece como par principal da configuração  $\mathcal{C} = \{(a, b), DP_{\mathcal{C}} = \{(e, e)\}\}$  associada à órbita da palavra vazia  $\phi$ . De fato,  $1 = |Orb_a(\phi)|$ ,  $a|_{\phi} = a$  e  $b|_{\phi} = b$ . Como  $a^0|_{\phi} = e$  e  $b^0|_{\phi} = e$  temos que  $DP_{\mathcal{C}} = \{(e, e)\}$ .

Para um automorfismo de crescimento limitado  $a$  o número de conjuntos  $\{a^i|_v, \text{ para } 0 \leq i < |Orb_a(v)|\}$ ,  $v \in Y^*$  distintos, é finitos e este fato pode ser demonstrado usando a ideia central da Proposição 3.4.2). Portanto o número de configurações para um par de automorfismos de crescimento limitado é finito.

Em particular, não precisamos nos referir a um conjugador  $h$  na definição de configuração.

### O problema da existência de um conjugador finitário

**Definição 3.5.3** *Dizemos que um automorfismo finitário  $\gamma$  satisfaz a configuração  $\mathcal{C}$  se  $\gamma$  for um conjugador para o par principal de  $\mathcal{C}$  e se todos os elementos  $c^{-1}\gamma d$ , para  $(c, d) \in DP_{\mathcal{C}}$ , forem finitários.*

Em particular, os automorfismos  $a, b$  são conjugados em  $\text{Pol}(-1)$  se, e somente se, a configuração  $\mathcal{C} = \{(a, b), DP_{\mathcal{C}} = \{(e, e)\}\}$  for satisfeita por algum automorfismo finitário. Observe ainda, que se  $a, b$  são conjugados por um automorfismo finitário de profundidade  $k > 0$ , e não existir automorfismo de profundidade menor que  $k$  que conjugue  $a, b$ , então se considerarmos todas as configurações do par  $a, b$ , existe pelo menos uma que é satisfeita por um automorfismo de profundidade 0 (e esta não é  $\mathcal{C}$ ), pelo menos uma que é satisfeita por um automorfismo de profundidade 1

(e esta não é  $\mathcal{C}$ ), etc. E porfim existe pelo menos uma (incluindo  $\mathcal{C}$ ) que é satisfeita por um automorfismo de profundidade  $k$ .

Vamos mostrar que é decidível se uma determinada configuração  $\mathcal{C}$  pode ser satisfeita por um automorfismo finitário.

Temos  $h$  tal que  $a \sim_h b$ , e  $\mathcal{O}_v$  a órbita da ação de  $a$  sobre  $Y^*$ , seja  $v$  o menor elemento da órbita e seja  $r = |\mathcal{O}_v|$ . A *configuração da órbita*  $\mathcal{O}$  (com relação ao conjugador  $h$ ) é o conjunto  $\mathcal{C} = \{(a^m|_v, b^m|_{v^h}), DP_{\mathcal{C}}\}$ , onde

$$DP_{\mathcal{C}} = \{(a^i|_v, b^i|_{v^h}), \text{ para } i = 0, \dots, m-1\}. \quad (3.15)$$

Suponha que exista um automorfismo finitário  $h$  satisfazendo  $\mathcal{C}$  e escolhemos  $h$  de modo que a profundidade máxima dentre os  $c^{-1}hd$  para  $(c, d) \in DP_{\mathcal{C}}$  seja a menor possível. Chamamos este número de *profundidade da configuração*  $\mathcal{C}$ .

Seja  $(a^m|_v, b^m|_{v^h}) = (\alpha, \beta)$  o par principal de  $\mathcal{C}$ , e  $\gamma$  um conjugador para  $(\alpha, \beta)$ . Considere a órbita  $\mathcal{O}$  da ação de  $\alpha$  sobre  $Y^*$ , e seja  $y$  o menor elemento em  $\mathcal{O}$  e  $m = |\mathcal{O}|$ . Então  $(\gamma|_y)^{-1}\alpha^m|_y\gamma|_y = \beta^m|_{y^\gamma}$  e as próximas fórmulas mostram como os outros estados de  $c^{-1}\gamma d$ , onde  $(c, d) \in DP_{\mathcal{C}}$ , dependem do estado  $\gamma|_y$ :

$$\begin{aligned} (c^{-1}\gamma d)|_x &= (c|_{(x)^{c^{-1}}})^{-1}\gamma|_{(x)^{c^{-1}}}\gamma d|_{(x)^{c^{-1}}\gamma} \\ &= (c|_{(y)^{\alpha^i}})^{-1}\gamma|_{(y)^{\alpha^i}}\gamma d|_{(y)^{\alpha^i}\gamma} \\ &= (c|_{(y)^{\alpha^i}})^{-1}(\alpha^i|_y)^{-1} \cdot (\alpha^i|_y\gamma|_{(y)^{\alpha^i}}) \cdot d|_{(y)^{\alpha^i}\gamma} \\ &= (\alpha^i|_y c|_{(y)^{\alpha^i}})^{-1} \cdot (\gamma|_y \beta^i|_{(y)^\gamma}) \cdot d|_{(y)^{\alpha^i}\gamma} \\ &= (\alpha^i|_y c|_{(y)^{\alpha^i}})^{-1} \cdot \gamma|_y \cdot \beta^i|_{(y)^\gamma} d|_{(y)^{h\beta^i}} \\ &= ((\alpha^i c)|_y)^{-1} \cdot \gamma|_y \cdot (\beta^i d)|_{(y)^\gamma} \end{aligned} \quad (3.16)$$

para  $(c, d) \in DP_{\mathcal{C}}$ , onde  $x = (y)\alpha^i c$  e  $i = 0, 1, \dots, m-1$ .

O conjunto associado  $\mathcal{C}' = \{(\alpha^m|_y, \beta^m|_{y^\gamma}), DP_{\mathcal{C}'}\}$ , onde

$$DP_{\mathcal{C}'} = \{((\alpha^i c)|_y, (\beta^i d)|_{y^\gamma}), \text{ para } (c, d) \in DP_{\mathcal{C}} \text{ e } i = 0, \dots, m-1\}, \quad (3.17)$$

é uma configuração para o par  $(a, b)$ . Mais precisamente, se  $\mathcal{C}$  é a configuração correspondente à órbita do vértice  $v$ , então  $\mathcal{C}'$  é a configuração correspondente à órbita do vértice  $vy$ . De fato,

$$\begin{aligned}
\alpha^m|_y &= (a^r|_v)^m|_y = (a_v a_{(v)a} a_{(v)a^2} a_{(v)a^{r-1}})^m|_y = \\
&= \left( (a_v a_{(v)a} a_{(v)a^2} a_{(v)a^{r-1}}) \cdot (a_v a_{(v)a} a_{(v)a^2} a_{(v)a^{r-1}}) \cdots (a_v a_{(v)a} a_{(v)a^2} a_{(v)a^{r-1}}) \right)|_y = \\
&= \left( (a_v a_{(v)a} a_{(v)a^2} \cdots a_{(v)a^{r-1}}) \cdot (a_{(v)a^r} a_{(v)a^{r+1}} a_{(v)a^{r+2}} \cdots a_{(v)a^{2r-1}}) \cdots \right. \\
&\quad \left. \cdots (a_{(v)a^{(m-1)r}} a_{(v)a^{(m-1)r+1}} a_{(v)a^{(m-1)r+2}} \cdots a_{(v)a^{mr-1}}) \right)|_y = \\
&= \left( (a_v)_x (a_{(v)a})_{(x)a_v} (a_{(v)a^2})_{(x)a_v a_{(v)a}} \cdots a_{(v)a^{r-1}} \right) \cdot (a_{(v)a^r} a_{(v)a^{r+1}} a_{(v)a^{r+2}} \cdots a_{(v)a^{2r-1}}) \cdots \\
&\quad \cdots (a|_{(v)a^{(m-1)r}} a|_{(v)a^{(m-1)r+1}} a|_{(v)a^{(m-1)r+2}} \cdots a|_{(v)a^{mr-1}})|_y = \\
&= a|_{vy} \cdot a|_{(v)a \cdot (y)a|_v} \cdot a|_{(v)a^2 \cdot (y)a|_v \cdot a|_{(v)a}} \cdots a|_{(v)a^{mr-1} \cdot (y)a|_v \cdot a|_{(v)a} \cdots a|_{(v)a^{mr-2}}} = \\
&= a|_{vy} \cdot a|_{(vy)a} \cdot a|_{(vy)a^2} \cdots a|_{(vy)a^{mr-1}} = a^{rm}|_{vy}
\end{aligned}$$

Analogamente mostramos que  $\beta^m|_{y\gamma} = b^{rm}|_{v^{h \cdot y\gamma}} = b^{rm}|_{(vy)^h}$ , pois,  $h|_v = \gamma$ . Ou seja, o estado  $h|_{vy}$  satisfaz a configuração  $\mathcal{C}'$ , e como ele tem profundidade menor que a de  $h$  as configurações  $\mathcal{C}'$  para toda órbita de  $c$  sobre  $Y$  tem profundidade menor que  $\mathcal{C}$ . Analogamente se todas as configurações  $\mathcal{C}'$  tiverem profundidade menor ou igual a um certo  $d$ , então a configuração  $\mathcal{C}$  terá profundidade menor ou igual a  $d + 1$ . Já que o número de configurações é finito, obtemos uma limitação para a profundidade de um possível conjugador (conjugador este, satisfazendo  $\mathcal{C}$ ), o que torna o problema decidível.

Acabamos de mostrar o seguinte resultado.

**Teorema 3.5.4** *O problema da conjugação para automorfismos de crescimento limitado é decidível em  $Pol(-1)$ , o grupo dos automorfismos finitários.*

### O procedimento de decisão em $Pol(-1)$

Pelo que acabamos de demonstrar, um procedimento possível seria checar dentre todos os automorfismos finitários com uma certa limitação sobre a profundidade,

se existe algum conjugador. Contudo, o algoritmo pode ser executado da seguinte forma:

- Encontramos primeiramente todas as configurações do par  $(a, b)$  da seguinte maneira: Calculamos a configuração  $\mathcal{C}$ , associada a  $\mathcal{O}_\phi$ , a órbita da palavra vazia. Esta induz as configurações associadas às órbitas do primeiro nível pela fórmula (3.17). Estas configurações obtidas induzem as configurações do nível seguinte, etc. Encontramos todas quando nenhuma configuração é acrescentada fazendo este processo.
- Construa  $D_0$  o conjunto das configurações satisfeitas por um automorfismo de profundidade 0, que são precisamente as configurações  $\mathcal{C} = \{(\alpha, \beta), DP_{\mathcal{C}}\}$  tais que  $\alpha = \beta$  e  $c = d$  para todo  $(c, d) \in DP_{\mathcal{C}}$ . Indutivamente construímos  $D_k$ , o conjunto das configurações não pertencentes a  $D_t$ , para  $t < k$ , e que são satisfeitas por um automorfismo de profundidade  $k$ .
- O procedimento pára quando:
  - Concluimos que a configuração  $\mathcal{C}$ , associada a  $\mathcal{O}_\phi$ , está em um certo  $D_k$ . Neste caso existe um automorfismo de profundidade  $k$  que conjuga o par  $(a, b)$ .
  - Não existe nenhuma configuração para uma certa profundidade e a configuração  $\mathcal{C}$  não pertence a nenhum dos  $D_i$  construídos. Isso significa que as outras configurações não podem ser satisfeitas por automorfismos finitários. Em particular, não existe conjugador finito para o par  $(a, b)$ .

### 3.5.2 O problema da conjugação no grupo dos autômatos limitados

Nesta subseção, provaremos que o problema da conjugação no grupo dos automorfismos de crescimento limitado é decidível. Mais precisamente, vamos exibir um

algoritmo que dados dois automorfismos de crescimento limitado, decide se existe algum automorfismo de crescimento limitado que os conjuga. Vamos abordar este problema de duas maneiras diferentes.

### Resolvendo conjugação através da estrutura cíclica dos autômatos limitados

Sejam  $a$  e  $b$  dois automorfismos de crescimento limitado conjugados em  $Pol(0) \setminus Pol(-1)$ . Para  $h$  um certo automorfismo de crescimento limitado podemos considerar todas as palavras  $u \in Y^*$  tais que  $e \neq h|_u$  seja um circuito, mas que  $h|_v$  não seja circuito, para todo  $v$  prefixo de  $u$ . Denotemos por  $l(h)$ , a soma de todos os comprimentos de tais palavras  $u$  e chamemos de *comprimento do autômato  $h$* . Seja  $h$  um conjugador de crescimento limitado para o par  $(a, b)$  com menor  $l(h)$  possível. Se  $h$  não for um circuito, então todos os estados  $h|_u$  para  $|u| \geq 1$  é um conjugador para algum par  $(c, d)$ , onde  $c \in OS(a)$  e  $d \in OS(b)$ , diferente de  $(a, b)$ . Caso contrário — ou seja, se para algum  $|u| \geq 1$ ,  $a \sim_{h|_u} b$  —  $h|_u$  seria um conjugador para o par  $(a, b)$  com  $l(h|_u) < l(h)$ , o que não pode ocorrer. Como os conjuntos  $OS(a)$  e  $OS(b)$  são finitos, obtemos uma limitação para o número  $l(h)$ .

Portanto, podemos supor que existe um conjugador de crescimento limitado  $h$  que seja um circuito, e escolhemos  $h$  com o menor circuito possível, ou seja, este é um com  $h|_u = h$ , onde  $|u| \geq 1$  é o menor possível dentre todos tais conjugadores. Consideremos tal palavra  $u$  de comprimento minimal que é lida ao longo do circuito. Consideremos dois casos.

Se  $u^a = u$  então  $\mathcal{O}_u = \{u\}$  e o mesmo ocorre com todas as órbitas dos prefixos de  $u$ . Então, os estados de  $h$  que aparecem ao longo do circuito (do autômato de  $h$ ), não tem dependências com outros estados, e temos então liberdade pra fazer mudanças nesses estados sem ter que mudar os outros estados do mesmo nível. Agora suponhamos que uma mesma equação se repita em diferentes estágios ao longo do circuito. Mais precisamente, suponhamos que existam dois estados  $h|_{v_1}$



e  $h|_{v_2}$  ao longo do circuito, isto é,  $v_1$  é um prefixo de  $v_2$  e  $|v_1| < |v_2|$ , os quais são conjugadores associados à mesma equação:  $(a|_{v_1}, b|_{(v_1)h|_{v_1}}) = (a|_{v_2}, b|_{(v_2)h|_{v_2}})$ . Definamos o automorfismo  $g$  pelas regras  $g|_{v_1} = h|_{v_2}$ ,  $g|_v = h|_v$  para  $v \in Y^{|v_1|}$ ,  $v \neq v_1$ . Assim,  $g$  age sobre  $Y^{|v_1|}$  igual  $h$  age (ou seja, as ações são iguais em  $Y^{|v_1|}$ ). Então  $g$  é tal que  $a \sim_g b$ , este é um circuito, tem crescimento limitado e o circuito de seu autômato tem comprimento menor que o de  $h$ ; uma contradição. Portanto, os estados de  $h$  ao longo do circuito resolvem distintos problemas da conjugação. Desta forma, encontramos uma limitação sobre o comprimento de um circuito, o que torna o problema decidível.

Se  $u^a = v \neq u$  então  $v$  pertence a  $\mathcal{O}_u$ , donde  $h|_v$  e  $h|_u$  estão em dependência um com outro. Mais precisamente,  $h|_v = (a|_u)^{-1}h|_u b|_{u^h}$  é um conjugador finitário para o par  $(a^m|_v, b^m|_{v^h})$ , pois  $h$  é um circuito (assim como  $h|_u$ ), e portanto os estados de  $h$  no  $|u|$ -ésimo nível são finitários. Analogamente, se  $h|_v$  é finitário, então  $a|_u h|_v (b|_{u^h})^{-1}$  é um conjugador de crescimento limitado para  $(a, b)$ . Já que o problema da conjugação é decidível em  $Pol(-1)$ , podemos decidir conjugação em  $Pol(0)$ . Mostramos que:

**Teorema 3.5.5** *O problema da conjugação no grupo gerado pelos autômatos limitados é decidível.*

### 3.5.3 Procedimento para decidir conjugação em $Pol(0)$

Um procedimento possível seria checar dentre todos os automorfismos finitários com uma certa limitação, se existe algum conjugador. Contudo, o algoritmo pode ser executado da seguinte forma:

- Calculemos primeiramente todas as configurações associadas ao par  $(a, b)$ .
- Verifiquemos quais configurações podem ser satisfeitas por um automorfismo finitário.

- Dentre as configurações restantes, podemos identificar os pares de  $OS(a) \times OS(b)$  que são conjugados por um automorfismo de crescimento limitado usando o primeiro caso acima, e então usando o primeiro caso. Alguns destes possivelmente irão recair em outros problemas (distintos).
- Tratamos tais problemas novos.

Tal processo termina pelas considerações iniciais.

### 3.5.4 Resolvendo conjugação para autômatos limitados através do cálculo dos estados ativos

Todo conjugador para o par  $(a, b)$  pode ser construído a cada nível, conforme descrito na Seção 3.1.1, através da escolha de uma permutação conjugadora associada a cada órbita da ação de  $a$ . O número de órbitas pode crescer a medida em que descemos nos níveis, e conseqüentemente o número de escolhas aumenta. No entanto, o número de configurações de órbitas é finito, o que indica que possivelmente mais de uma órbita está associada à uma mesma configuração. Mais precisamente, se  $a$  e  $b$  são conjugados em  $Pol(0)$ , então existe um conjugador de crescimento limitado tal que, para todas as órbitas de um mesmo nível correspondendo a uma mesma configuração, os estados correspondentes de  $h$  são iguais. Tal fato é uma consequência do método anterior. De fato, se  $\mathcal{O}_{v_1}, \mathcal{O}_{v_2}, \dots, \mathcal{O}_{v_k}$  são órbitas distintas de um mesmo nível, todas com uma mesma configuração de órbita  $\mathcal{C}$ , então, conforme observado anteriormente temos liberdade na escolha dos  $h|_{v_i}, i = 1, \dots, k$  (pelo fato de serem de órbitas distintas e portanto, um não depender do outro). Como todos eles são solução de um mesmo par de equação ( $h|_{v_i}$  é solução de  $(a^{m_i}|_{v_i}, b^{m_i}|_{v_i\pi})$ , onde, para todo  $i, (a^{m_i}|_{v_i}, b^{m_i}|_{v_i\pi}) = (\alpha, \beta)$ , o par principal de  $\mathcal{C}$ ), donde podemos escolher os  $h|_{v_i}$  todos iguais. Como  $h|_{(v_i)a^i} = c^{-1}h|_{v_i}d$ , segue da configuração de órbita ser a mesma que os outros estados correspondentes de  $h$  também são iguais. Portanto, é suficiente escolher permutações conjugadoras apenas para as configurações. (Mais

precisamente, apenas para o par principal de cada configuração.) A seguir, vamos mostrar como contar o número de estados ativos do conjugador  $h$ , dependendo de nossa escolha das permutações conjugadoras. A importância disso está no fato de que  $h$  é de crescimento limitado se existe uma constante que limita o número de estados ativos de cada nível.

Suponha que o conjugador  $h$  foi construído até o  $(n-1)$ -ésimo nível. Isso significa que a ação de  $h$  está definida em  $Y^{n-1}$  mas não está definida em  $Y^n$ , ou analogamente, se  $v \in Y^n$  então a ação de  $h|_v$  sobre  $Y$  não está definida. Considere então a órbita  $\mathcal{O}_v$  da ação de  $a$  sobre  $Y^n$  (onde  $v$  é o menor elemento da órbita) e seja  $\mathcal{C} = \{(\alpha, \beta); DP_{\mathcal{C}}\}$  a configuração de  $\mathcal{O}_v$ . Recorde que o conjunto  $DP_{\mathcal{C}}$  consiste dos pares  $(c, d)$  que aparecem na fórmula  $h|_{(v)a^i} = c^{-1}h|_v d$ , onde aqui  $c = a^i|_v$  e  $d = b^i|_{v^h}$  para  $i = 0, \dots, |\mathcal{O}_v| - 1$ ; contudo pode acontecer que dois dos índices  $i$  distintos podem estar associados ao mesmo par  $(c, d)$ . Tendo em mãos apenas o conjunto  $DP_{\mathcal{C}}$ , sabemos que existe um estado associado a  $(c, d)$ , mas o número de estados associados ao mesmo  $(c, d)$  é perdido. Para preservar esta informação introduzimos o vetor coluna  $u_{\mathcal{C}}$  de dimensão  $|DP_{\mathcal{C}}|$ , cujas entradas são inteiros não negativos e tal que a  $(c, d)$ -ésima coordenada  $u_{\mathcal{C}}(c, d)$ , para  $(c, d) \in DP_{\mathcal{C}}$ , é igual ao número de  $i$ 's tais que  $c = a^i|_v$  e  $d = b^i|_{v^h}$ .

Para definir a ação de  $h$  sobre  $Y^n$ , escolha uma permutação  $\pi \in C\Pi(\alpha, \beta)$  e defina  $y^{h|_v} = y^{\pi}$  para  $y \in Y$ . Então checamos quais estados de  $h$  nos vértices da órbita  $\mathcal{O}_v$ , são ativos ou não: o estado  $h|_{(v)a^i}$  do "tipo"  $(c, d)$  (isto é,  $h|_{(v)a^i} = c^{-1}h|_v d$ ) é ativo se a permutação  $\pi_{c^{-1}\pi\pi_d}$  é não trivial (ou seja, se  $\pi_{h|_{(v)a^i}} = \pi_{c^{-1}h|_v d} = \pi_{c^{-1}\pi h|_v \pi_d} = \pi_{c^{-1}\pi\pi_d}$  for não trivial). Então guardamos esta informação no vetor coluna  $\theta_{\mathcal{C}, \pi}$  de dimensão  $|DP_{\mathcal{C}}|$  e tal que a  $(c, d)$ -ésima coordenada  $\theta_{\mathcal{C}, \pi}(c, d) = 1$  se  $\pi_{c^{-1}\pi\pi_d} \neq 1$  e  $\theta_{\mathcal{C}, \pi}(c, d) = 0$  caso contrário. Assim, quando escolhemos a permutação  $\pi$  temos que o número de estados ativos de  $h$  (sobre os vértices da órbita  $\mathcal{O}_v$ ) é igual a  $\theta_{\mathcal{C}, \pi} \cdot u_{\mathcal{C}} = \sum \theta_{\mathcal{C}, \pi}(c, d)u_{\mathcal{C}}(c, d)$ .

Seja  $\Lambda$  o conjunto de todas as configurações para o par  $(a, b)$ . Seja  $\Pi = \prod_{\mathcal{C} \in \Lambda} C\Pi_{\mathcal{C}}$ ,

onde  $C\Pi_{\mathcal{C}} = C\Pi(\alpha, \beta)$  e  $(\alpha, \beta)$  é o par principal de  $\mathcal{C}$ . Podemos pensar em  $\Pi$  como um conjunto de escolhas, tal que quando tomamos  $\pi \in \Pi$  foi escolhida uma permutação conjugadora para cada configuração. Os conjuntos  $\Lambda$  e  $\Pi$  são finitos. Para  $\pi = (\pi_{\mathcal{C}})_{\mathcal{C} \in \Lambda}$  defina  $\theta_{\pi} = (\theta_{\mathcal{C}, \pi_{\mathcal{C}}})_{\mathcal{C} \in \Lambda}$ . Quando escolhemos  $\pi \in \Pi$  toda configuração  $\mathcal{C} \in \Lambda$  induz certas configurações  $\mathcal{C}'$  sobre o nível seguinte através da Equação (3.17), e cada par  $(c, d) \in DP_{\mathcal{C}}$  induz certos pares  $(c', d')$  através da Equação (3.16). Guardamos esta informação na matriz quadrada com coeficientes inteiros não negativos  $A_{\pi}$  de dimensão  $\sum_{\mathcal{C} \in \Lambda} |DP_{\mathcal{C}}|$ , onde a entrada  $A_{\pi}$  correspondente aos pares  $(c, d)$ ,  $(c', d')$  e às configurações  $\mathcal{C}, \mathcal{C}'$  é igual ao número de todos os pares  $(c', d')$  induzidos pelo par  $(c, d)$ . Então, se temos o vetor coluna  $u = (u_{\mathcal{C}})$ , onde  $u_{\mathcal{C}}(c, d)$  é o número de estados associados ao par  $(c, d)$  que temos em certo nível, e escolhemos  $\pi \in \Pi$ , então o número de estados associados a cada par de cada configuração do nível seguinte é dada pelo vetor  $A_{\pi}u$ . Chame  $\mathcal{M} = \{A_{\pi} : \pi \in \Pi\}$ .

Agora, considere todas órbitas de  $a$  sobre  $Y^n$ , considere as configurações de tais órbitas e defina o vetor coluna  $u = (u_{\mathcal{C}})_{\mathcal{C} \in \Lambda}$ , onde  $u_{\mathcal{C}}(c, d)$  para  $(c, d) \in DP_{\mathcal{C}}$  é igual ao número de todos os estados “tipo”  $(c, d)$  sobre todas as órbitas com configuração  $\mathcal{C}$ . Para definir a ação de  $h$  sobre o  $(n+1)$ -ésimo nível, escolha  $\pi = (\pi_{\mathcal{C}})_{\mathcal{C} \in \Lambda} \in \Pi$  e para toda órbita com configuração  $\mathcal{C}$  definimos a ação de  $h$  ao longo desta órbita usando a permutação  $\pi_{\mathcal{C}}$  conforme descrito acima (escolhemos uma permutação para cada configuração mesmo se nem todas as configurações aparecem no  $n$ -ésimo nível). Desta forma, o conjugador  $h$  está definido até o  $n$ -ésimo nível, e o número de estados ativos de  $h$  no  $n$ -ésimo nível é  $\theta_{\pi} \cdot u$ . O vetor  $v = (v_{\mathcal{C}})_{\mathcal{C} \in \Lambda}$ , onde  $v_{\mathcal{C}}(c, d)$  é igual ao número de estados do “tipo”  $(c, d)$  sobre as órbitas de  $a$  sobre  $Y^{n+1}$  com configuração  $\mathcal{C}$ , é igual a  $v = A_{\pi}u$ .

O processo começa no 0-ésimo nível, isto é, da raiz, onde temos o vetor  $u_0 = (u_{\mathcal{C}})$  (associado às configurações do 0-ésimo nível) tal que  $u_{\mathcal{C}}(e, e) = 1$  para a configuração  $\mathcal{C} = \{(a, b); DP_{\mathcal{C}} = \{(e, e)\}\}$ , que corresponde ao par  $(a, b)$ , e  $u_{\mathcal{C}'}(c, d) = 0$  para todos os outros pares e configurações. Então fazemos escolhas  $\pi_0, \pi_1, \dots, \pi_n, \dots$

do conjunto  $\Pi$  e construímos o conjugador  $h$ . Segue da discussão acima que as atividades dos estados de  $h$  podem ser calculadas pelas seguintes regras:

$$\theta_n(h) = \theta_{\pi_n} u_n \quad \text{e} \quad u_{n+1} = A_{\pi_n} u_n \quad (3.18)$$

para todo  $n \geq 0$ . Se existe uma escolha tal que a sequência  $\theta_n(h)$  é limitada, então existirá (possivelmente) uma escolha periódica e portanto o conjugador  $h$  associado a essa escolha será de finitos estados e de crescimento limitado.

Se a sequência  $\theta_n(h)$  não é limitada, qualquer que seja a escolha, então não existe conjugador  $h$  de crescimento limitado tal que  $a \sim_h b$ .

Portanto, os automorfismos  $a$  e  $b$  são conjugados no grupo  $Pol(0)$  se, e somente se, existe uma sequência  $A_n \in \mathcal{M}$  tal que a sequência correspondente  $\theta_{A_n} u_n$  seja limitada.

Com este método, não precisamos (possivelmente) resolver problemas da conjugação em  $Pol(-1)$ , tal como no método anterior, contudo, o problema se reduz para certos problemas envolvendo matrizes, os quais também podem ser resolvidos, enquanto o anterior é direto. Ambas abordagens foram feitas nos Exemplos 3.6.3 e 3.6.4 da Seção 3.6.

Observemos que ambas as abordagens resolvem também o problema da conjugação simultâneo. Basta fazer uma observação análoga á feita na Seção 3.3.2.

**Teorema 3.5.6** *O problema da conjugação (simultâneo) no grupo dos autômatos limitados é decidível.*

Os procedimentos anteriores não apenas decidem se dois automorfismos de  $Pol(0)$  são conjugados ou não em  $Pol(0)$ , mas em caso afirmativo exhibe um conjugador neste grupo.

Da mesma forma, pode-se resolver o problema da conjugação para automorfismos de crescimento limitado em cada grupo  $Pol(m)$ . No entanto, temos uma afirmação mais forte.

**Proposição 3.5.7** *Dois automorfismos de crescimento limitado são conjugados no grupo  $Pol(\infty)$  se, e somente se, eles são conjugados no grupo  $Pol(0)$ .*

**Demonstração:** Sejam  $a$  e  $b$  dois automorfismos conjugados em  $Pol(m)$  para  $m \geq 1$ . Vamos proceder tal como no primeiro método. Novamente o problema se reduz ao caso em que o conjugador  $h \in Pol(m)$  é um circuito. Seja  $u$  a palavra não trivial de menor comprimento que é lida ao longo do circuito, ou seja,  $h|_u = h$ . Considere os mesmos dois casos considerados acima:

Se  $u^a = v \neq u$  então o estado  $h|_v$  deve estar em  $Pol(m-1)$ . Mas então,  $h = h|_u = a|_u h|_v (b|_{u^h})^{-1} \in Pol(m-1)$ . Portanto,  $a$  e  $b$  são conjugados em  $Pol(m-1)$ . Utilizamos o mesmo argumento para o caso em que  $w^a \neq w$  para alguma palavra  $w$  da forma  $uu \dots u$ .

Suponha  $w^a = w$  para toda palavra  $w$  da forma  $uu \dots u$ . Então  $h^{-1}a|_w h = b|_{w^h}$ . Se  $a|_w = 1$  (e portanto  $b|_{w^h} = 1$ ) então defina o automorfismo  $g$  pelas regras  $g|_w = 1$ ,  $g|_v = h|_v$  para todo  $v \in Y^{|w|}$ ,  $v \neq w$ , e a ação de  $g$  on  $Y^{|w|}$  é igual a de  $h$ . Então  $g$  está em  $Pol(m-1)$  e é um conjugador para  $(a, b)$ .

Se  $a|_w \neq 1$  para toda palavra  $w = uu \dots u$ , então algum estado  $a|_w$  é um automorfismo circuito e  $(a|_w)|_v = a|_w$  para alguma palavra  $v$  da forma  $uu \dots u$ . Sem perda de generalidade podemos supor que  $a|_u = a$  e  $b|_{u^h} = b$ . Então os estados  $a|_v$  e  $b|_{v^h}$  são finitários para todo  $v \in Y^{|u|}$ ,  $v \neq u$ . Considere todas as órbitas  $\mathcal{O}$  da ação de  $a$  sobre  $Y^{|u|} \setminus u$ , seja  $v \in \mathcal{O}$  o menor elemento de  $\mathcal{O}$  e  $m = |\mathcal{O}|$ . Então os automorfismos finitários  $a^m|_v$  e  $b^m|_{v^h}$  são conjugados em  $\mathcal{A}$ , e portanto são conjugados em  $Pol(-1)$ . Defina o automorfismo  $g$  pelas regras: a ação de  $g$  sobre  $Y^{|u|}$  é igual a de  $h$ ,  $g|_u = g$ ,  $g|_v$  é um conjugador finitário para o par  $(a^m|_v, b^m|_{v^h})$ , e  $g|_{(v)^{a^i}} = (a^i|_v)^{-1} g|_v b^i|_{v^h}$  (também é finitário) para todo  $i = 1, \dots, m-1$  e para toda órbita  $\mathcal{O}$ . Então  $g$  é um conjugador de crescimento limitado para o par  $(a, b)$ .

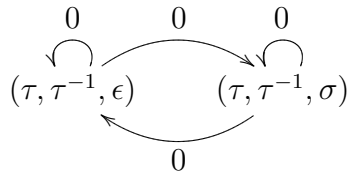
Indutivamente concluímos que  $a$  e  $b$  são conjugados em  $Pol(0)$ . ■

### 3.6 Exemplos

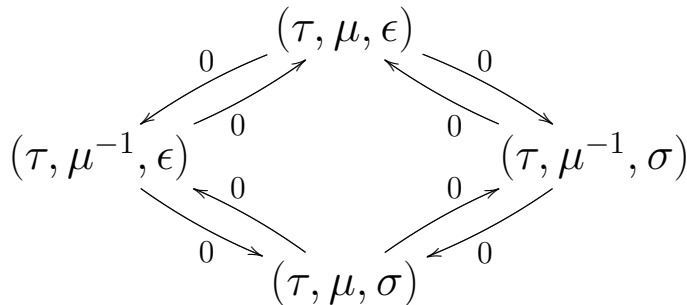
**Exemplo 3.6.1 (Grafo conjugador e conjugadores básicos)** 1. Considere o

problema da conjugação para o par  $(e, e)$ , onde  $e$  é o automorfismo identidade da árvore binária. Aqui,  $OS(e) = \{e\}$  e  $C\Pi(e, e) = \text{Sym}(Y) = \{\varepsilon, \sigma\}$ . Existem dois subgrafos definidores do grafo  $\Psi(e, e)$ , e os conjugadores básicos correspondentes a cada um desses subgrafos são  $h_1 = (h_1, h_1) = e$  e  $h_2 = (h_2, h_2)\sigma$ .

2. Considere o problema da conjugação para a máquina de adição binária  $\tau = (e, \tau)\sigma$  e seu inverso  $\tau^{-1} = (\tau^{-1}, e)\sigma$ . Observe que  $OS(\tau) = \{\tau\}$ ,  $OS(\tau^{-1}) = \{\tau^{-1}\}$ , e  $C\Pi(\tau, \tau^{-1}) = \{\varepsilon, \sigma\}$ . Existe uma órbita da ação de  $\tau$  sobre  $\{0, 1\}$ ,  $\tau^2|_0 = \tau$  e  $\tau^{-2}|_{0\pi} = \tau^{-1}$  para todo  $\pi \in \{\varepsilon, \sigma\}$ . O grafo conjugador  $\Psi(\tau, \tau^{-1})$  é mostrado na Figura abaixo. Existem dois subgrafos definidores do grafo  $\Psi(\tau, \tau^{-1})$ , e os conjugadores básicos correspondentes a cada um desses subgrafos são  $h_1 = (h_1, h_1\tau^{-1})$  e  $h_2 = (h_2, h_2)\sigma$ .



3. Considere o problema da conjugação para a máquina de adição binária  $\tau = (e, \tau)\sigma$  e o automorfismo  $\mu = (e, \mu^{-1})\sigma$ . Aqui  $OS(\tau) = \{\tau\}$ ,  $OS(\mu) = \{\mu, \mu^{-1}\}$ , e  $C\Pi(\tau, \mu) = C\Pi(\tau, \mu^{-1}) = \{\varepsilon, \sigma\}$ . Existe uma órbita da ação de  $\tau$  sobre  $\{0, 1\}$ ,  $\tau^2|_0 = \tau$ ,  $\mu^2|_{0\pi} = \mu^{-1}$ , e  $\mu^{-2}|_{0\pi} = \mu$  para todo  $\pi \in \{\varepsilon, \sigma\}$ . O grafo conjugador  $\Psi(\tau, \mu)$  é mostrado na Figura abaixo.



Existem quatro subgrafos definidores do grafo  $\Psi(\tau, \mu)$ , cada um deles consiste dos dois vértices  $(\tau, \mu, \pi_1)$  e  $(\tau, \mu^{-1}, \pi_2)$  junto com as arestas induzidas para  $\pi_1, \pi_2 \in \{\varepsilon, \sigma\}$ . Os conjugadores básicos correspondentes a cada um dos grafos definidores são  $h_1, h_2, h_3, h_4$ , os quais são definidos da seguinte maneira

$$\begin{aligned} h_1 &= (g_1, g_1) & h_2 &= (g_2, g_2) & h_3 &= (g_3, \tau g_3)\sigma & h_4 &= (g_4, \tau g_4)\sigma \\ g_1 &= (h_1, h_1\mu) & g_2 &= (h_2, h_2)\sigma & g_3 &= (h_3, h_3\mu) & g_4 &= (h_4, h_4)\sigma, \end{aligned} \quad (3.19)$$

onde  $g_1, g_2, g_3, g_4$  são os conjugadores básicos do par  $(\tau, \mu^{-1})$ .

O próximo exemplo mostra que a condição de finitude sobre os sinalizadores de órbita não pode ser omitida no Teorema 3.3.6, e que o Teorema 3.4.4 não vale para automorfismos de crescimento polinomial de grau maior ou igual a 1.

**Exemplo 3.6.2** Considere os automorfismos  $b = (\tau, c)\sigma$ ,  $c = (\tau, b)$  definidos no Exemplo 3.3.14. Indutivamente podemos provar que o estado  $b^{2^n}|_{0^n}$  é ativo para todo  $n$ , e portanto o automorfismo  $b$  age transitivamente sobre  $Y^n$  para todo  $n$ . Portanto  $b$  é conjugado a  $a$  no grupo  $\mathcal{A}$ .  $a$  e  $b$  são ambos contráteis, contudo,  $b$  tem sinalizadore de órbita infinito e portanto, este não é conjugado a  $a$  no grupo  $\mathcal{A}_f$ , pela Proposição 3.3.13.

Finalmente, vamos ilustrar como resolver o problema da conjugação no grupo dos autômatos de crescimento limitado utilizando os dois últimos métodos.

**Exemplo 3.6.3** Considere o problema da conjugação para a máquina de adição binária  $\tau = (e, \tau)\sigma$  e seu inverso  $\tau^{-1} = (\tau^{-1}, e)\sigma$  no grupo dos autômatos limitados.

A configuração associada a órbita da palavra vazia  $\phi$  é dada por  $\mathcal{C}_1 = \{(\tau, \tau^{-1}), DP_1 = \{(e, e)\}\}$ .

$\mathcal{C}_1$ , por sua vez, induz certas configurações de órbitas do primeiro nível:

Tomamos o par principal de  $\mathcal{C}_1$ ,  $(\tau, \tau^{-1})$  e olhamos para a ação de  $\tau$  sobre  $Y$ .  $Orb_\tau(0) = \{0, 1\}$ ,  $|Orb_\tau(0)| = 2$  e  $C\Pi(\tau, \tau^{-1}) = \{\varepsilon, \sigma\}$ .



- Escolhendo a permutação conjugadora  $\varepsilon$ ,  $\mathcal{C}_1$  induz  $\mathcal{C}_2$ .

De fato, o par principal da configuração da órbita  $Orb_\tau(0)$  (com permutação conjugadora  $\varepsilon$ ) é  $(\tau^2|_0, \tau^{-2}|_{0^\varepsilon}) = (\tau, \tau^{-1})$ . O conjunto  $DP$  desta configuração induzida é

$$\{((\tau^i c)|_0, (\tau^{-1^i} d)|_{0^\varepsilon}), \text{ para } (c, d) \in DP_{\mathcal{C}_1} \text{ e } i = 0, 1\} = \{(e, e), (e, \tau^{-1})\}. \quad (3.20)$$

Portanto,  $\mathcal{C}_2$  é a configuração induzida por  $\mathcal{C}_1$  quando escolhermos a permutação  $\varepsilon$ .

Observe que o par  $(c, d) = (e, e) \in DP_{\mathcal{C}_1}$  induz o par  $(e, e)_{\mathcal{C}_2}$  (isto é, induz o par  $(e, e)$  da configuração  $\mathcal{C}_2$ ) com multiplicidade 1 (quando  $i = 0$ ). O par  $(c, d) = (e, e) \in DP_{\mathcal{C}_1}$  induz também o par  $(e, \tau^{-1})_{\mathcal{C}_2}$  com multiplicidade 1 (quando  $i = 1$ ).

- Escolhendo a permutação conjugadora  $\sigma$ ,  $\mathcal{C}_1$  induz  $\mathcal{C}_1$ .

O par principal da configuração da órbita  $Orb_\tau(0)$  (com permutação conjugadora  $\sigma$ ) é  $(\tau^2|_0, \tau^{-2}|_{0^\sigma}) = (\tau, \tau^{-1})$ . O conjunto  $DP$  desta configuração induzida é

$$\{((\tau^i c)|_0, (\tau^{-1^i} d)|_{0^\sigma}), \text{ para } (c, d) \in DP_{\mathcal{C}_1} \text{ e } i = 0, 1\} = \{(e, e)\}.$$

Portanto,  $\mathcal{C}_1$  é a configuração induzida por  $\mathcal{C}_1$  quando escolhermos a permutação  $\sigma$ .

Observe que o par  $(c, d) = (e, e) \in DP_{\mathcal{C}_1}$  induz o par  $(e, e)_{\mathcal{C}_1}$  com multiplicidade 2 (quando  $i = 0, 1$ ).

**$\mathcal{C}_2$ , por sua vez, induz certas configurações associadas às órbitas nível seguinte (segundo):**

Tomamos o par principal de  $\mathcal{C}_2$ ,  $(\tau, \tau^{-1})$  e olhamos para a ação de  $\tau$  sobre  $Y$ .  $Orb_\tau(0) = \{0, 1\}$ ,  $|Orb_\tau(0)| = 2$  e  $C\Pi(\tau, \tau^{-1}) = \{\varepsilon, \sigma\}$ .

- Escolhendo a permutação conjugadora  $\varepsilon$ ,  $\mathcal{C}_2$  induz  $\mathcal{C}_2$ .

O par principal da configuração da órbita  $\text{Orb}_\tau(0)$  (com permutação conjugadora  $\varepsilon$ ) é  $(\tau^2|_0, \tau^{-2}|_{0^\varepsilon}) = (\tau, \tau^{-1})$ .

O conjunto  $DP$  desta configuração é

$$\{((\tau^i c)|_0, (\tau^{-1^i} d)|_{0^\varepsilon}), \text{ para } (c, d) \in DP_{\mathcal{C}_2} \text{ e } i = 0, 1\} = \{(e, e), (e, \tau^{-1})\}. \quad (3.21)$$

Portanto,  $\mathcal{C}_2$  é a configuração induzida por  $\mathcal{C}_2$  quando escolhermos a permutação  $\varepsilon$ .

Observe que o par  $(c, d) = (e, e) \in DP_{\mathcal{C}_2}$  induz o par  $(e, e)$  com multiplicidade 1 (quando  $i = 0$ ) e o par  $(e, \tau^{-1})$  com multiplicidade 1 (quando  $i = 1$ ). O par  $(c, d) = (e, \tau^{-1}) \in DP_{\mathcal{C}_2}$  induz o par  $(e, \tau^{-1})$  com multiplicidade 2 (quando  $i = 0, 1$ ).

- Escolhendo a permutação conjugadora  $\sigma$ ,  $\mathcal{C}_2$  induz  $\mathcal{C}_2$ .

O par principal da configuração da órbita  $\text{Orb}_\tau(0)$  (com permutação conjugadora  $\sigma$ ) é  $(\tau^2|_0, \tau^{-2}|_{0^\sigma}) = (\tau, \tau^{-1})$ . O conjunto  $DP$  desta configuração é

$$\{((\tau^i c)|_0, (\tau^{-1^i} d)|_{0^\sigma}), \text{ para } (c, d) \in DP_{\mathcal{C}_2} \text{ e } i = 0, 1\} = \{(e, e), (e, \tau^{-1})\}.$$

Portanto,  $\mathcal{C}_2$  é a configuração induzida por  $\mathcal{C}_2$  quando escolhermos a permutação  $\sigma$ .

Observe que o par  $(c, d) = (e, e) \in DP_{\mathcal{C}_2}$  induz o par  $(e, e)_{\mathcal{C}_2}$  com multiplicidade 2 (quando  $i = 0, 1$ ). O par  $(c, d) = (e, \tau^{-1}) \in DP_{\mathcal{C}_2}$  induz o par  $(e, e)_{\mathcal{C}_2}$  com multiplicidade 1 (quando  $i = 0$ ) e o par  $(e, \tau^{-1})_{\mathcal{C}_2}$  com multiplicidade 1 (quando  $i = 1$ ).

Portanto, existem apenas duas configurações para o par  $(\tau, \tau^{-1})$ :

$$\mathcal{C}_1 = \{(\tau, \tau^{-1}), DP_1 = \{(e, e)\}\}, \quad \mathcal{C}_2 = \{(\tau, \tau^{-1}), DP_2 = \{(e, e), (e, \tau^{-1})\}\}. \quad (3.22)$$

**Utilizando o primeiro método** Como nenhuma das duas configurações é satisfeta pelo automorfismo trivial, concluímos que  $\tau$  e  $\tau^{-1}$  não são conjugados no grupo  $Pol(-1)$ . (Ver método na Seção 3.5).

Nenhum automorfismo pode ser construído pelo segundo caso do primeiro método, conforme vimos na subseção 3.5.3, porque não existe nenhum par em  $OS(\tau) \times OS(\tau^{-1})$  que seja conjugado em  $Pol(-1)$ . Recorde que  $OS(\tau) = \{\tau\}$  e  $OS(\tau^{-1}) = \{\tau^{-1}\}$ . O primeiro caso do primeiro método não pode ser aplicado porque  $\tau$  não possui nenhum vértice fixo. Portanto,  $\tau$  e  $\tau^{-1}$  não são conjugados no grupo  $Pol(\infty)$ .

### Utilizando o segundo método

Conforme vimos na Subseção 3.5.3, analisando cada configuração induzida de outra e os pares induzidos de outros pares, obtemos o seguinte conjunto de matrizes  $A_\pi$  e vetores  $\theta_\pi$  onde  $\pi = (\pi_{C_1}, \pi_{C_2}) \in \Pi$ :

Onde a matriz  $A_{(\pi_{C_1}, \pi_{C_2})}$  é

	$(e, e)_{C_1}$	$(e, e)_{C_2}$	$(e, \tau^{-1})_{C_2}$
$(e, e)_{C_1}$	$(A_\pi)_{11}$	$(A_\pi)_{12}$	$(A_\pi)_{13}$
$(e, e)_{C_2}$	$(A_\pi)_{21}$	$(A_\pi)_{22}$	$(A_\pi)_{23}$
$(e, \tau^{-1})_{C_2}$	$(A_\pi)_{31}$	$(A_\pi)_{32}$	$(A_\pi)_{33}$

Onde se  $(c, d)_{C_k}$  estiver na  $j$ -ésima coluna e se  $(c', d')_{C_i}$  estiver na  $i$ -ésima linha então isso significa que a através da permutação  $\pi_{C_k}$  o par  $(c, d)_{C_k}$  induz o par  $(c', d')_{C_i}$  com multiplicidade (a entrada)  $(A_\pi)_{ij}$ .

Mais precisamente,

$$A_{(\varepsilon, \varepsilon)} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 2 \end{pmatrix}, \quad A_{(\varepsilon, \sigma)} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad (3.23)$$

$$A_{(\sigma, \varepsilon)} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}, \quad A_{(\sigma, \sigma)} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \quad (3.24)$$

Lembrando que

$$\theta_{(\pi_{C_1}, \pi_{C_2})} = (\theta_{C_1, \pi_{C_1}}, \theta_{C_2, \pi_{C_2}})$$

onde

$\theta_{\mathcal{C}_1, \pi_{\mathcal{C}_1}}$  tem dimensão  $|DP_{\mathcal{C}_1}| = 1$  e  $\theta_{\mathcal{C}_2, \pi_{\mathcal{C}_2}}$  tem dimensão  $|DP_{\mathcal{C}_2}| = 2$ . Vale ainda que

$$\theta_{\mathcal{C}_1, \varepsilon} = (0) \text{ pois } \pi_{e^{-1}} \varepsilon \pi_e = \varepsilon;$$

$$\theta_{\mathcal{C}_1, \sigma} = (1) \text{ pois } \pi_{e^{-1}} \sigma \pi_e = \sigma;$$

$$\theta_{\mathcal{C}_2, \varepsilon} = (0, 1) \text{ pois } \pi_{e^{-1}} \varepsilon \pi_e = \varepsilon \text{ e } \pi_{e^{-1}} \varepsilon \pi_{\tau^{-1}} = \sigma;$$

$$\theta_{\mathcal{C}_2, \sigma} = (1, 0) \text{ pois } \pi_{e^{-1}} \sigma \pi_e = \sigma \text{ e } \pi_{e^{-1}} \sigma \pi_{\tau^{-1}} = \varepsilon.$$

Portanto

$$\theta_{(\varepsilon, \varepsilon)} = (0, (0, 1)), \quad \theta_{(\varepsilon, \sigma)} = (0, (1, 0)), \quad \theta_{(\sigma, \varepsilon)} = (1, (0, 1)), \quad \theta_{(\sigma, \sigma)} = (1, (1, 0)).$$

O vetor inicial é  $u_0 = (1, 0, 0)^t$  e no  $n$ -ésimo passo obtemos  $u_{n+1} = A_{\pi_n} u_n$  e  $\theta_n = \theta_{\pi_n} u_n$  quando escolhermos  $\pi_n \in \Pi$ .

Para qualquer escolha de  $\{\pi_n\}_{n \geq 0} \subset \Pi$  a sequência  $\theta_n$  tem crescimento exponencial e portanto,  $\tau$  e  $\tau^{-1}$  não são conjugados no grupo  $\text{Pol}(\infty)$  dos autômatos de crescimento polinomial.

**Exemplo 3.6.4** Considere o problema da conjugação para os automorfismos de crescimento limitado  $b = (\sigma, b)$  e  $c = (c, \sigma)$ . Note que os pares  $(\sigma, c)$  e  $(b, \sigma)$  não são conjugados em  $\mathcal{A}$ . Portanto, não existe conjugador inativo para  $(b, c)$ , ou seja, apenas  $\sigma$  pode aparecer como ação de um possível conjugador sobre  $Y$ .

Então, tomamos  $C\Pi(b, c) = \{\sigma\}$ . Observe que  $OS(b) = \{e, \sigma, b\}$  e  $OS(c) = \{e, \sigma, c\}$ ,  $C\Pi(\sigma, \sigma) = \{\varepsilon, \sigma\}$ .

A configuração associada a órbita da palavra vazia  $\phi$  é dada por  $\mathcal{C}_1 = \{(b, c), DP_1 = \{(e, e)\}\}$ .

$\mathcal{C}_1$ , por sua vez, induz certas configurações associadas às órbitas do primeiro nível:

Tomamos o par principal de  $\mathcal{C}_1$ ,  $(b, c)$  e olhamos para a ação de  $b$  sobre  $Y$ .  $Orb_b(0) = \{0\}$  e  $Orb_b(1) = \{1\}$ , donde  $|Orb_b(0)| = 1 = |Orb_b(1)|$ .

- Escolhendo a permutação conjugadora  $\sigma$  e a órbita  $Orb_b(0) = \{0\}$  temos que  $\mathcal{C}_1$  induz  $\mathcal{C}_2$ .

De fato, o par principal da configuração da órbita  $Orb_b(0)$  (com permutação conjugadora  $\sigma$ ) é  $(b^1|_0, c^1|_{0\sigma}) = (\sigma, \sigma)$ . O conjunto  $DP$  desta configuração induzida é

$$\{((b^i c)|_0, (c^i d)|_{0\sigma}), \text{ para } (c, d) \in DP_{\mathcal{C}_1} \text{ e } i = 0\} = \{(e, e)\}.$$

Portanto,  $\mathcal{C}_2 = \{(\sigma, \sigma), DP_2 = \{(e, e)\}\}$  é a configuração induzida por  $\mathcal{C}_1$  quando escolhermos a permutação  $\sigma$  e consideramos  $Orb_b(0)$ .

Observe que o par  $(c, d) = (e, e) \in DP_{\mathcal{C}_1}$  induz o par  $(e, e)_{\mathcal{C}_2}$  (isto é, induz o par  $(e, e)$  da configuração  $\mathcal{C}_2$ ) com multiplicidade 1 (quando  $i = 0$ ).

- Escolhendo a permutação conjugadora  $\sigma$  e a órbita  $Orb_b(1) = \{1\}$  temos que  $\mathcal{C}_1$  induz  $\mathcal{C}_1$ .

De fato, o par principal da configuração da órbita  $Orb_b(1)$  (com permutação conjugadora  $\sigma$ ) é  $(b^1|_1, c^1|_{1\sigma}) = (b, c)$ . O conjunto  $DP$  desta configuração induzida é

$$\{((b^i c)|_1, (c^i d)|_{1\sigma}), \text{ para } (c, d) \in DP_{\mathcal{C}_1} \text{ e } i = 0\} = \{(e, e)\}. \quad (3.25)$$

Portanto,  $\mathcal{C}_1$  é a configuração induzida por  $\mathcal{C}_1$  quando escolhermos a permutação  $\sigma$  e consideramos  $Orb_b(1)$ .

Observe que o par  $(c, d) = (e, e) \in DP_{\mathcal{C}_1}$  induz o par  $(e, e)_{\mathcal{C}_1}$  (isto é, induz o par  $(e, e)$  da configuração  $\mathcal{C}_1$ ) com multiplicidade 1 (quando  $i = 0$ ).

$\mathcal{C}_2$  induz certas configurações associadas às órbitas do segundo nível:

Tomamos o par principal de  $\mathcal{C}_2$ ,  $(\sigma, \sigma)$  e olhamos para a ação de  $\sigma$  sobre  $Y$ .  $Orb_\sigma(0) = \{0, 1\}$  donde  $|Orb_\sigma(0)| = 1$ .

- Escolhendo a permutação conjugadora  $\varepsilon$  e a órbita  $Orb_\sigma(0) = \{0, 1\}$  temos que  $\mathcal{C}_2$  induz  $\mathcal{C}_3$ .

De fato, o par principal da configuração da órbita  $Orb_\sigma(0)$  (com permutação conjugadora  $\varepsilon$ ) é  $(\sigma^2|_0, \sigma^2|_{0^\varepsilon}) = (e, e)$ . O conjunto  $DP$  desta configuração induzida é

$$\{((\sigma^i c)|_0, (\sigma^i d)|_{0^\varepsilon}), \text{ para } (c, d) \in DP_{\mathcal{C}_2} \text{ e } i = 0, 1\} = \{(e, e)\}. \quad (3.26)$$

Portanto,  $\mathcal{C}_3 = \{(e, e), DP_3 = \{(e, e)\}\}$  é a configuração induzida por  $\mathcal{C}_2$  quando escolhemos a permutação  $\varepsilon$ .

Observe que o par  $(c, d) = (e, e) \in DP_{\mathcal{C}_2}$  induz o par  $(e, e)_{\mathcal{C}_3}$  (isto é, induz o par  $(e, e)$  da configuração  $\mathcal{C}_3$ ) com multiplicidade 2 (quando  $i = 0, 1$ ).

- Escolhendo a permutação conjugadora  $\sigma$  e a órbita  $Orb_\sigma(0) = \{0, 1\}$  temos que  $\mathcal{C}_2$  induz  $\mathcal{C}_3$ .

De fato, o par principal da configuração da órbita  $Orb_\sigma(0)$  (com permutação conjugadora  $\sigma$ ) é  $(\sigma^2|_0, \sigma^2|_{0^\sigma}) = (e, e)$ . O conjunto  $DP$  desta configuração induzida é

$$\{((\sigma^i c)|_0, (\sigma^i d)|_{0^\sigma}), \text{ para } (c, d) \in DP_{\mathcal{C}_2} \text{ e } i = 0, 1\} = \{(e, e)\}. \quad (3.27)$$

Portanto,  $\mathcal{C}_3 = \{(e, e), DP_3 = \{(e, e)\}\}$  é a configuração induzida por  $\mathcal{C}_2$  quando escolhemos a permutação  $\sigma$ .

Observe que o par  $(c, d) = (e, e) \in DP_{\mathcal{C}_2}$  induz o par  $(e, e)_{\mathcal{C}_3}$  (isto é, induz o par  $(e, e)$  da configuração  $\mathcal{C}_3$ ) com multiplicidade 2 (quando  $i = 0, 1$ ).

**$\mathcal{C}_3$  induz certas configurações associadas às órbitas do terceiro nível:**

Tomamos o par principal de  $\mathcal{C}_3$ ,  $(e, e)$  e olhamos para a ação de  $e$  sobre  $Y$ .  $Orb_e(0) = \{0\}$  e  $Orb_e(1) = \{1\}$ , donde  $|Orb_e(0)| = 1 = |Orb_e(1)|$ .

- Escolhendo a permutação conjugadora  $\varepsilon$  e a órbita  $Orb_e(0) = \{0\}$  temos que  $\mathcal{C}_3$  induz  $\mathcal{C}_3$ .

De fato, o par principal da configuração da órbita  $Orb_e(0)$  (com permutação conjugadora  $\varepsilon$ ) é  $(e^1|_0, e^1|_{0^\varepsilon}) = (e, e)$ . O conjunto  $DP$  desta configuração induzida é

$$\{((e^i c)|_0, (e^i d)|_{0^\varepsilon}), \text{ para } (c, d) \in DP_{\mathcal{C}_3} \text{ e } i = 0\} = \{(e, e)\}.$$

Portanto,  $\mathcal{C}_3 = \{(e, e), DP_2 = \{(e, e)\}\}$  é a configuração induzida por  $\mathcal{C}_3$  quando escolhermos a permutação  $\varepsilon$  e consideramos  $Orb_e(0)$ .

Observe que o par  $(c, d) = (e, e) \in DP_{\mathcal{C}_3}$  induz o par  $(e, e)_{\mathcal{C}_3}$  (isto é, induz o par  $(e, e)$  da configuração  $\mathcal{C}_3$ ) com multiplicidade 1 (quando  $i = 0$ ).

- Escolhendo a permutação conjugadora  $\sigma$  e a órbita  $Orb_e(1) = \{1\}$  temos que  $\mathcal{C}_3$  induz  $\mathcal{C}_3$ .

De fato, o par principal da configuração da órbita  $Orb_e(1)$  (com permutação conjugadora  $\sigma$ ) é  $(e^1|_1, e^1|_{1^\sigma}) = (e, e)$ . O conjunto  $DP$  desta configuração induzida é

$$\{((e^i c)|_1, (e^i d)|_{1^\sigma}), \text{ para } (c, d) \in DP_{\mathcal{C}_1} \text{ e } i = 0\} = \{(e, e)\}. \quad (3.28)$$

Portanto,  $\mathcal{C}_3$  é a configuração induzida por  $\mathcal{C}_3$  quando escolhermos a permutação  $\sigma$  e consideramos  $Orb_e(1)$ .

Observe que o par  $(c, d) = (e, e) \in DP_{\mathcal{C}_1}$  induz o par  $(e, e)_{\mathcal{C}_3}$  (isto é, induz o par  $(e, e)$  da configuração  $\mathcal{C}_3$ ) com multiplicidade 1 (quando  $i = 0$ ).

$$\mathcal{C}_1 = \{(b, c), DP_1 = \{(e, e)\}\}, \quad \mathcal{C}_2 = \{(\sigma, \sigma), DP_2 = \{(e, e)\}\}, \quad (3.29)$$

$$\mathcal{C}_3 = \{(e, e), DP_3 = \{(e, e)\}\}. \quad (3.30)$$

### Utilizando o primeiro método

As configurações  $\mathcal{C}_2$  e  $\mathcal{C}_3$  são satisfeitas pelo automorfismo trivial, enquanto  $\mathcal{C}_1$  não é satisfeita por nenhum automorfismo finitário. (Para ver isso, basta executar o procedimento descrito na subseção 3.5.3) Portanto,  $b$  e  $c$  não são conjugados em  $Pol(-1)$ . No primeiro caso do primeiro método, estamos procurando por um conjugador ativo e

Conforme observado acima, quando escolhendo a permutação conjugadora  $\sigma$  e a órbita  $Orb_e(0) = \{0\}$  temos que  $\mathcal{C}_1$  induz  $\mathcal{C}_2$  (ou seja,  $h_0$  é um conjugador que satisfaz  $\mathcal{C}_2$ , podendo ser escolhido como  $e$ ). Quando escolhendo a permutação conjugadora  $\sigma$  e a órbita  $Orb_e(1) = \{1\}$  temos que  $\mathcal{C}_1$  induz  $\mathcal{C}_1$  (ou seja,  $h_1$  é um conjugador que satisfaz  $\mathcal{C}_1$ , e como o tomamos com  $l(h)$  minimal, este é tal que  $h_1 = h$ ). Desta forma obtemos um conjugador  $h$  tal que  $h = (e, h)\sigma$ , e portanto  $b$  e  $c$  são conjugados no grupo  $Pol(0)$ .

### Utilizando o segundo método

Para o segundo método, tomamos o conjunto  $\Pi = \{(\sigma, \varepsilon, \varepsilon), (\sigma, \sigma, \varepsilon), (\sigma, \varepsilon, \sigma), (\sigma, \sigma, \sigma)\}$ , já que  $C\Pi(b, c) = \{\sigma\}$ .

Onde a matriz  $A_{(\pi_{\mathcal{C}_1}, \pi_{\mathcal{C}_2}, \pi_{\mathcal{C}_3})}$  é

	$(e, e)_{\mathcal{C}_1}$	$(e, e)_{\mathcal{C}_2}$	$(e, e)_{\mathcal{C}_3}$
$(e, e)_{\mathcal{C}_1}$	$(A_\pi)_{11}$	$(A_\pi)_{12}$	$(A_\pi)_{13}$
$(e, e)_{\mathcal{C}_2}$	$(A_\pi)_{21}$	$(A_\pi)_{22}$	$(A_\pi)_{23}$
$(e, e)_{\mathcal{C}_3}$	$(A_\pi)_{31}$	$(A_\pi)_{32}$	$(A_\pi)_{33}$

Onde se  $(c, d)_{\mathcal{C}_k}$  estiver na  $j$ -ésima coluna e se  $(c', d')_{\mathcal{C}_i}$  estiver na  $i$ -ésima linha então isso significa que a através da permutação  $\pi_{\mathcal{C}_k}$  e de uma órbita (da ação do primeiro membro do par principal de  $\mathcal{C}_k$  sobre  $Y$ ), o par  $(c, d)_{\mathcal{C}_k}$  induz o par  $(c', d')_{\mathcal{C}_i}$  com certa multiplicidade. A entrada  $(A_\pi)_{ij}$  é a soma das multiplicidades, dependendo



da órbita considerada.

Agora observe que as matrizes  $A_\pi$  são iguais para todo  $\pi \in \Pi$ .

$$A_\pi = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 2 \end{pmatrix}. \quad (3.31)$$

Uma observação importante é que escolhendo a permutação conjugadora  $\sigma$  temos que  $\mathcal{C}_1$  induz  $\mathcal{C}_1$  e  $\mathcal{C}_2$ , dependendo da órbita considerada (órbita do 0 ou órbita do 1 pela ação de  $b$ ).

No primeiro caso  $(e, e)_{\mathcal{C}_1}$  induz  $(e, e)_{\mathcal{C}_1}$  com multiplicidade 1. E no segundo caso  $(e, e)_{\mathcal{C}_1}$  induz  $(e, e)_{\mathcal{C}_2}$  com multiplicidade 1.

Da mesma forma, para independente da permutação conjugadora escolhida, temos que  $\mathcal{C}_1$  induz  $\mathcal{C}_1$  considerando a órbita do 0, e induz novamente  $\mathcal{C}_1$ , considerando a órbita do 1.

No primeiro caso  $(e, e)_{\mathcal{C}_1}$  induz  $(e, e)_{\mathcal{C}_1}$  com multiplicidade 1. E no segundo caso  $(e, e)_{\mathcal{C}_1}$  induz  $(e, e)_{\mathcal{C}_1}$  com multiplicidade 1. Então, conforme observado, a entrada  $(A_\pi)_{33} = 2$  pois é a soma destas multiplidades.

Os outros casos são análogos, com a diferença que temos apenas uma órbita pela ação sobre  $Y$  do primeiro membro do par principal (da configuração).

Calculemos os vetores  $\theta_\pi$ :

Lembrando que  $\theta_{(\pi_{\mathcal{C}_1}, \pi_{\mathcal{C}_2}, \pi_{\mathcal{C}_3})} = (\theta_{\mathcal{C}_1, \pi_{\mathcal{C}_1}}, \theta_{\mathcal{C}_2, \pi_{\mathcal{C}_2}}, \theta_{\mathcal{C}_3, \pi_{\mathcal{C}_3}})$  onde  $\theta_{\mathcal{C}_i, \pi_{\mathcal{C}_i}}$  tem dimensão  $|DP_{\mathcal{C}_i}| = 1$ , concluímos que

$$\theta_{\mathcal{C}_1, \sigma} = (1) \text{ pois } \pi_{e^{-1}} \sigma \pi_e = \sigma;$$

$$\theta_{\mathcal{C}_2, \varepsilon} = (0) \text{ pois } \pi_{e^{-1}} \varepsilon \pi_e = \varepsilon;$$

$$\theta_{\mathcal{C}_2, \sigma} = (1) \text{ pois } \pi_{e^{-1}} \sigma \pi_e = \sigma;$$

$$\theta_{\mathcal{C}_3, \varepsilon} = (0) \text{ pois } \pi_{e^{-1}} \varepsilon \pi_e = \varepsilon;$$

$$\theta_{\mathcal{C}_3, \sigma} = (1) \text{ pois } \pi_{e^{-1}} \sigma \pi_e = \sigma.$$

---

*Portanto*

$$\begin{aligned}\theta_{(\sigma,\varepsilon,\varepsilon)} &= (1, 0, 0), & \theta_{(\sigma,\sigma,\varepsilon)} &= (1, 1, 0), \\ \theta_{(\sigma,\varepsilon,\sigma)} &= (1, 0, 1), & \theta_{(\sigma,\sigma,\sigma)} &= (1, 1, 1).\end{aligned}$$

*O vetor inicial é  $u_0 = (1, 0, 0)^t$  e  $u_n = A^n u_0 = (1, 1, 2^n - 2)$  independentemente de nossa escolha. Se escolhermos  $\pi_n = (\sigma, \varepsilon, \varepsilon)$  para todo  $n \geq 0$ , então a sequência  $\theta_n = (1, 0, 0) \cdot u_n = 1$  é limitada. Portanto  $b$  e  $c$  são conjugados no grupo  $Pol(0)$ . O conjugador correspondente à nossa escolha é a máquina de adição binária  $\tau$ .*

# Referências Bibliográficas

- [Ale72] S. V. Aleshin, Finite automata and the burnsie problem for periodic groups, *Mat. Zametki* (1972), no. 11, 319–328.
- [Ale83] ———, A free group of finite automata, *Vestnik Moskov. Univ. Ser. I Mat. Mekh.* (1983), no. 4, 12–14.
- [BBSZ] I. Bondarenko, N Bondarenko, S. Sidki, and F. Zapata, On the conjugacy problem for finite-state automorphisms of regular rooted tree., *Preprint, available at <http://arxiv.org/pdf/1011.2227>*.
- [BG00] L. Bartholdi and R.I. Grigorchuk, On the spectrum of hecke type operators related to some fractal groups., *Trudy Mat. Inst. Steklov.* (2000), no. 231, 5–45.
- [BN03] I. Bondarenko and V. Nekrashevych, Post-critically finite self-similar groups., *Algebra Discrete Math.* (2003), no. 4, 21–32.
- [Boo59] W. W. Boone, The word problem, *Annals of Mathematics* **70** (2) (1959), 207–265.
- [BS97] A. Brunner and S. Sidki, On the automorphism group of one-rooted binary trees., *J. Algebra* (1997), no. 195, 465–486.
- [BSV99] A. M. Brunner, S. Sidki, and A. Vieira, A just-nonsolvable torsion-free group defined on the binary tree, *J. Algebra* **211** (1999), 99–114.
- [CM69] D. Collins and C. Miller, Word and conjugacy problems in groups with only a few defining relations, *Zeitschr.f. Math. Logik und Grundlagen d. Math* **15** (1969), 305–324.
- [CM77] ———, The conjugacy problem and subgroups of finite index, *Proc. London Math. Soc.* **3** (1977), 535–556.
- [Day57] M. Day, Amenable semigroups, *Illinois J. Math.* (1957), no. 1, 509–544.
- [Fri60] A. Fridman, On the relation between the word problem and the conjugacy problem in finitely defined groups, *Uspekhi Mat. Nauk* **91** (1960), no. 246.
- [Glu61] V. Glushkov, Abstract theory of automata., *Uspehi Mat. Nauk* **16** (1961), no. 5, 3–62.

- 
- [GNS00] R. Grigorchuk, V. Nekrashevych, and V. Sushchansky, Automata, dynamical systems, and groups., *Proc. Steklov Institute* (2000), no. 231, 128–203.
- [GNS01] P. Gawron, V. Nekrashevych, and V. Sushchansky, Conjugation in tree automorphism groups., *Int. J. Algebra Comput.* (2001), no. 5, 529–547.
- [Gri80] R.I. Grigorchuk, On the Burnside problem for periodic groups, *Functional Anal. Appl.* **14** (1980), 41–43.
- [Gri83] ———, On the milnor problem of group growth., *Dokl. Akad. Nauk SSSR* **271** (1983), 30–33.
- [Gri84] R. Grigorchuk, Degrees of growth of finitely generated groups and the theory of invariant means., *Izv. Akad. Nauk SSSR Ser. Mat.* (1984), no. 48, 939–985, *English translation: Math. USSR-Izv.* **25** (1985), no. 2, 259–300.
- [Gri85] R.I. Grigorchuk, Degrees of growth of p-groups and torsion-free groups., *Mat. Sb. (N.S.)* **126** (1985), 194–214.
- [GS83] N. Gupta and S. Sidki, On the Burnside problem for periodic groups, *Math. Z.* **182** (1983), no. 3, 385–388.
- [GW00] I. Grigorchuk and J. Wilson, The conjugacy problem for certain branch groups, *Tr. Mat. Inst. Steklova* (2000), no. 231, 215–230.
- [GZ02] R.I. Grigorchuk and A. Zuk, On a torsion-free weakly branch group defined by a three state automaton, *Int. Journal of Algebra and Comp.*, **12** (2002), 223–246.
- [Leo98] Y. Leonov, The conjugacy problem in a class of 2-groups, *Mat. Zametki* **64** (1998), no. 4, 573–583.
- [Mil68] J. Milnor, Problem 5603, *Amer. Math. Monthly* (1968), no. 75, 685–686.
- [Mil71] C. Miller, On group-theoretic decision problems and their classification, *Annals of Math. Studies* **68** (1971).
- [Nek05] V. Nekrashevych, Self-similar groups, *Mathematical Surveys and Monographs*, vol. 117, *American Mathematical Society, Providence, RI*, 2005.
- [Nov55] P. S. Novikov, On the algorithmic unsolvability of the word problem in group theory, *Trudy Mat. Inst. Steklov* **44** (1955), pp 1–143, (in Russian).
- [Per07] L. Pervova, Profinite completions of some groups acting on trees., *J. of Algebra* (2007), no. 310, 858–879.
- [Rib08] M. Ribeiro, O grupo finitario de isometrias da arvore n-ária (the finitary group of isometries of the n-ary tree), *Doctoral Thesis, Universidade de Brasília* (2008).
- [Roz98] A. Rozhkov, The conjugacy problem in an automorphism group of an infinite tree, *Mat. Zametki* **64** (1998), no. 4, 592–597.

- 
- [Sav03] D. Savchuk, On word problem in contracting automorphism groups of rooted trees., *Bull. of the Univ. of Kiev, Series: Physics and Math.*, (2003), no. 1, 51–56.
- [Sid87] S. Sidki, On a 2-generated infinite 3-group: subgroups and automorphisms, *J. of Algebra* (1987), no. 110, 24–55.
- [Sid98] ———, Regular trees and their automorphisms, *Monografias de Matemática [Mathematical Monographs]*, vol. 56, Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 1998.
- [Sid00] ———, Automorphisms of one-rooted trees: growth, circuit structure, and acyclicity, *J. Math. Sci. (New York)* **100** (2000), no. 1, 1925–1943, *Algebra*, 12. MR MR1774362 (2002g:05100)
- [Sid04] ———, Finite automata of polynomial growth do not generate a free group, *Geom. Dedicata* **108** (2004), no. 1, 193–204.
- [SV] Z. Sunic and E. Ventura, The conjugacy problem is not solvable in automaton groups., *Preprint*, available at <http://arxiv.org/abs/1010.1993>.
- [Ufn91] V. A. Ufnarovski, On the use of graphs for calculating the basis, growth and hilbert series of associative algebras, *Math. USSR-Sb* **68** (1991), 417–428.