ESTA TESE FOI JULGADA ADEQUADA PARA A OBTENÇÃO DO TITULO DE

" MESTRE EM CIÊNCIAS "

ESPECIALIDADE EM MATEMÁTICA, E APROVADA EM SUA FORMA FINAL PELO CURSO DE POS-GRADUAÇÃO EM MATEMÁTICA DA UNIVERSIDADE FEDERAL DE SANTA CATARINA.

Italo J. Dejter

PROF. ÍTALO JOSE DEJTER

- COORDENADOR DO CURSO -

BANCA EXAMINADORA:

Donald Morison Silberger

PROF. DONALD MORISON SILBERGER, PhD.

- O r i e n t a d o r -

Italo J. Dejter

PROF. ITALO JOSE DEJTER, PhD.

William G. Whitley

PROF. WILLIANM GLENN WHITLEY, PhD.

UNIVERSIDADE FEDERAL DE SANTA CATARINA

SOBRE A SYM-UNIVERSALIDADE DE PALAVRAS PRIMITIVAS

jurema maria costa arante

maio - 1981

a meus filhos Marcos Tadeu

e Fábio Luiz.

AGRADECIMENTOS

Ao Professor Donald Morison Silberger pela orientação segura e precisa, por sua disponibilidade e paciência e pelo entusiasmo que sempre procurou transmitir.

Ao Professor Milton Luiz Valente, amigo e cunhado, um agradecimento especial pelo valioso auxílio prestado.

Ao José Tadeu, meu esposo, pelo incentivo, compreensão e colaboração principalmente nos momentos mais difíceis.

A meus pais a quem muito devo.

A Universidade Federal de Santa Catarina, em particular ao Departamento de Matemática, que possibilitou a realização do presente trabalho.

Esta dissertação estabelece para cada par m *e* n *de inteiros com* $mn\neq 0$ *que para todo grupo simétrico infinito* S_x *e para todo* $f\in S_x$ *a equação* $f=x^n y^m$ *tem solução* $\langle x,y\rangle\in S_x \times S_x$.

This dissertation establishes, for every pair m and n of integers with $mn \neq 0$, that for every infinite symmetric group S_x and for every $f \in S_x$ the equation $f = x^n y^m$ has a solution $\langle x, y \rangle \in S_x \times S_x$.

INDICE

INTRODUÇÃO

Nos últimos cinquenta anos cresceu muito o interesse na definição de grupos e, consequentemente, de semigrupos e de outras estruturas mais gerais do que de um grupo G, por sistemas de equações. Tais equações são determinadas por palavras que dão as formas das equações, no sentido que, se $W(L_1,\ldots,L_p)$ for uma palavra nas letras $L_1,\ldots,L_p$ (soletrada usando somente as letras no alfabeto $\{L_1,L_2,\ldots L_p\}$), e se $y\in G$, então $y=W(x_1,\ldots,x_p)$ é a equação determinada por W e y; os x_i são considerados "variáveis em G", com $L_i\longrightarrow x_i$ uma função, e uma p-upla $(a_1,\ldots,a_p)\in G^p$ tal que $y=W(a_1,\ldots,a_p)$ é solução desta equação quando a justaposição dos símbolos a_i indica "multiplicação" em G.

Segundo Jan Mycielski perguntamos, para certas famílias C naturais e importantes de monóides: Para quais palavras $W(L_1,\ldots,L_p)$ acontece que, para todo $H\in C$ e para todo $y\in H$ a equação $y=W(x_1,\ldots,x_p)$ tem solução $(x_1,\ldots,x_p)=(a_1,\ldots,a_p)\in H^p$?

Definimos os termos fundamentais e apresentamos os lemas básicos no capítulo I. No capítulo II revisamos a história da pergunta de Mycielski e formulamos algumas perguntas relacionadas ao assunto. No capítulo III estudamos, através de um exemplo amplo e geral, o teorema principal de D.M.Silberger e M.L.Valente em [5], este trabalho é um dos principais pontos de partida para nosso capítulo IV, no qual provamos um resultado novo que amplia o alcance do referido teorema.

No capítulo V provamos nosso principal teorema que é a primeira contribuição não trivial, na história do assunto, no estudo das palavras que são ISym-universais, onde ISym denota a família de todos os grupos simétricos infinitos. Neste teorema provamos que, para todo grupo simétrico infinito G, e para todo $y \in G$, as equações $z=y^n x^n$ e $z=x^k y^n x^m$ sempre tem solução $<x,y>=<b,a> \in G^2$, sempre que k,n e m são inteiros positivos.

CAPÍTULO 1 - OBSERVAÇÕES

As notações e definições utilizadas nos capítulos subsequentes são listadas neste capítulo. Além disto alguns resultados que interessam no desenvolvimento do trabalho são aqui apresentados com exemplos para facilitar o entendimento.

Como é usual, Z denota o conjunto dos inteiros; o inteiro 0 também denota o conjunto vazio, ϕ; ω denota o conjunto $\{n \in Z: n \geqslant 0\}$; se $0 < n \in \omega$ então n também denota $\{0, 1, \ldots, n-1\}$.

Exemplo: $4 = \{0, 1, 2, 3\}$, observemos que $|4| = 4$ e, desta forma, $|n|$ indica o número de elementos do conjunto n.

Se X é um conjunto arbitrário seu número cardinal é denotado por $|X|$. Se X e Y são conjuntos então $Y \setminus X$ denota $\{x: x \in Y$ e $x \notin X\}$. Em particular $\omega \setminus n$ denota $\{n, n+1, \ldots\}$. Naturalmente se $\{p, q\} \subseteq \omega$ com $p \leqslant q$ então $|q \setminus p| = |q-p| = q-p$.

Seja $p \in \omega \setminus 2$. Então $M(p)$ denota o menor múltiplo comum de $\{2, 3, \ldots, p\}$; $S(p)$ denota o menor fator primo de p. Se além de p, tivermos $q \in \omega$ então $p|q$ denota que existe $n \in \omega$ com $np = q$, $p \nmid q$ nega a afirmação anterior e $p||q$ indica que $p^i|q$ mas $p^{i+1} \nmid q$ com $i \in \omega$.

Sejam X conjunto arbitrário e $f \subseteq X \times X$. Então $Dom(f)$ denota $\{x: \exists y \ \langle x, y \rangle \in f\}$; $Im(f)$ denota $Dom(f^{-1})$; para um conjunto A, $f[A]$ denota $\{y: \exists x \ (x \in A \wedge \langle x, y \rangle \in f\}$; e $f \upharpoonright A$ denota $(A \times X) \cap f$. A expressão $Wrld(f)$ denota $Dom(f) \cup Im(f)$.

A expressão $Prt(X)$ *denota o conjunto de todas as funções* f *com* $Wrld(f)\subseteq X$. *A expressão* ${}^X X$ *indica* $\{f: f\in Prt(X)$ *e* $Dom(f)\subseteq X\}$. *Além disso* $Sym(X)$ *denota o conjunto de todas as permutações em* X. *Certamente* $Sym(X)$ *é um subgrupo de* ${}^X X$, *e* ${}^X X$ *é um submonóide de* $Prt(X)$. *Por* $id\restriction X$ *indicaremos* $\{x\in X: f(x)=x\}$. *O conjunto* $\{f: f\in Sym(X)$ *e* f *é par*$\}$ *denota-se* $Alt(X)$.

Lema 1.1. Seja X *conjunto finito. Seja* $f\in {}^X X$. *Então as seguintes três afirmações são equivalentes:*

1. f *é injetiva;*
2. f *é sobrejetiva (sobre* X*);*
3. $f\in Sym(X)$.

Demonstração: Seja 1 verdadeira. Então $|f[X]|=|X|$ *e portanto* $X=f[X]$ *já que* X *é finito. Portanto 2 segue.*

Seja 1 falsa. Então existe $\{x,y\}\subseteq X$ *com* $x\neq y$ *mas com* $f(x)=f(y)$. *Segue que* $f[X]=f[X\setminus\{y\}]$, *e portanto que* $|f[X]|=|f[X\setminus\{y\}]|\leq|X\setminus\{y\}|<|X|$ *pois* X *é finito, e então que* $f[X]\neq X$. *Portanto 1 é falsa implica em 2 falsa também. Segue que 1 é equivalente a 2. Agora temos, obviamente, que 1 e 3 são equivalentes.*

Observação: A finidade de X *é essencial em 1.1. Note que* $Z\to Z$ *definida por* $z\to 2z$ *é injetiva sem ser sobrejetiva (sobre* Z*). Também* $Z\to Z$ *definida por* $2z+1\to z$ *e por* $2z\to z$ *é sobrejetiva sem ser injetiva.*

Seja $f\subsetneq X\times X$. *Também chamamos grafo direto, onde* f *é um digrafo, cujo conjunto de "vértices" é* $Wrld(f)$

e cujas arestas diretas, ou "arestas", é o conjunto f. Chamamos $g\subseteq X\times X$ de subdigrafo de f se, e somente se, $g\subseteq f$.

Consideremos f e g relações binárias, diremos que f é isomórfica bigraficamente com g, e representamos por $f\approx g$ se, e somente se, existem um conjunto Y e $h\in Sym(Y)$ tais que $f=\{\langle h(x),h(y)\rangle:\langle x,y\rangle\in g\}$. Temos que $\approx$ é uma relação de equivalência.

Lema 1.2. Seja $\{f,g\}\subseteq X\times X$. Então as seguintes afirmações são equivalentes:

1. $f\approx g$
2. *Existe $h\in Sym(X)$ tal que $g=hfh^{-1}$*
3. *Existe $h\in Sym(X)$ tal que $gh=hf$.*

Demonstração: [9, *Corollary of Theorem*].

Seja $F\subseteq Sym(X)$ para X conjunto arbitrário, Diremos que F é disjunta como permutação, e anotamos dcp, se e somente se, para cada par f e g de elementos distintos de F, temos que para todo $x\in X$ que $x=f(x)$ ou que $x=g(x)$.

Lema 1.3. Seja F dcp com $F\subseteq Sym(X)$ e $\{f,g\}\subseteq F$. Então $fg=gf$.

Demonstração: [10, *Lema 1.3*].

Seja $f\subseteq X\times X$. Diremos que f é conexo como digrafo se, e somente se, para cada $\{x,y\}\subseteq Wrld(f)$, se $x\neq y$ então existe uma sequência finita $x=z_0,z_1,\ldots,z_j=y$ tal que para todo $i\in j$ $\{\langle z_i,z_{i+1}\rangle,\langle z_{i+1},z_i\rangle\}\cap f\neq\phi$.

A expressão $id\restriction X$ chamaremos ciclo trivial em x, ou ciclo de comprimento 1 em X.

Seja $id\restriction X\neq f\in Sym(X)$. Diremos que f é um ciclo não trivial em X se, e somente se, existir $g\subseteq f$ tal que $|g|>1$, tal que g é conexo e tal que se $g\subseteq h\subseteq f$ e se h é conexo então $g=h$.

Seja f um ciclo não trivial cujo subdigrafo maximal conexo é g. Então f é chamado um $|g|$-ciclo em X ou um ciclo de comprimento $|g|$ em X.

Observação: Se $|g|=_{o}$ dizemos que f é um ciclo infinito em X, ou ω-ciclo em X. De outra forma f é dito ciclo finito em X.

Seja $f\in Sym(X)$. Chamamos f de permutação cíclica de X se, e somente se, f é conexo.

Quando $F\subseteq Sym(X)$, e F é dcp, então πF denota $\{<x,y>: \exists\, f\in F(y=f(x))\}$. É claro que $\pi F\in Sym(X)$.

Lema 1.4. Seja $f\in Sym(X)$. Então existe exatamente uma família F dos ciclos não triviais em X tal que F é dcp e tal que $f=\pi F$.

Demonstração: [5, Lema 1.4].

Observação: $\pi\phi=id\restriction X$, quando se estipula que estamos pensando em $\phi\subseteq Sym(X)$.

Seja f um ciclo não trivial em X, e consideremos o único sub-conjunto g de f tal que $|g|>0$, que g é conexo e que $g\subseteq h\subseteq f$ então $h=g$.

Quando $|g|=k\in\omega$, então existe uma injeção $i\to x_i$ de k em X, e g tem a forma $x_0\to x_1\to x_2\to\ldots\to x_{k-1}\to x_0$; escrevemos $f=(x_0\ x_1\ x_2\ \ldots\ x_{k-1})$. A permutação cíclica $(0\ 1\ \ldots\ k-1)$ de

k denominamos de C_k. Quando não falta entendimento, a expressão C_k denota a permutação $C_k \cup id\restriction(X\setminus k)$ quando $k\subseteq X$.

Por outro lado, quando $|g|=\aleph_0$, então existe uma injeção $i\to x_i$ de Z em X e g tem a forma $x_i \to x_{i+1}$ para todo $i\in Z$. Escrevemos $f=(\ldots\ x_{-1}\ x_0\ x_1\ x_2\ \ldots)$. A permutação cíclica $i\to i+1$ de Z denominamos de s.

Finalmente, para cada $x\in X$ a expressão (x) denota $id\restriction X$.

Para cada $f\in Sym(X)$ a expressão $\vee'(f)$ denota ϕ se $f=id\restriction X$. Por outro lado se $f\neq id\restriction X$, $\vee'(f)$ denota a unicamente determinada família F, vista no lema 1.4. Os elementos de $\vee'(f)$ são denominados componentes não triviais de f.

O conjunto $\vee'(f)\cup\{x\colon f(x)=x\}$ será denotado por tac

$\vee(f)$. Em $\vee(f)$ pretendemos "contar" a identidade , $id\restriction f$, exatamente uma vez para cada $x\in X$ que será "fixado" por f.

Exemplo: Seja $f=(3\ 4)(5\ 6\ 7)$. Se $X=8$ então $\vee(f)=\vee'(f)\cup\{(0),(1),(2)\}$ ou $\vee(f)=\{(3\ 4),(5\ 6\ 7)\}\ \{(0),(1),(2)\}$ e $|\vee(f)|=5$. Mas se $X=9$ então $\vee(f)=\{(3\ 4),(5\ 6\ 7)\}\cup\{(0).(1),(2),(8)\}$ e $|\vee(f)|=6$.

Seja $f\in Sym(X)$. Então $\Lambda(f)$ denota $\{|g|:g\in\vee(f)\}\cup T$, com $T=\phi$ se $x\neq f(x)$ para cada $x\in X$, mas com $T=\{1\}$ se existe $x\in X$ tal que $x=f(x)$.

Quando $f^n\neq f$ para todo inteiro $n\neq 0$, então diremos que f tem ordem infinita, ou que $ord(f)=\infty$. De outra forma *ord(f) denota* $min\{n : n\in\omega\setminus 1$ *e* $f^n = id\restriction X\}$.

Chamamos f de involução de X se, e somente se, $f\in Sym(X)$ *e* $ord(f)\in\{1,2\}$.

Estudo das palavras. *Consideremos* $\Sigma=\{A,B,C,\dots\}$ *um alfabeto fixo, finito e arbitrário.* Σ^* *denota o monóide gerado pelo alfabeto* Σ. *Os elementos de* Σ^*, *são denominados palavras de semigrupo e serão denotadas por letras gregas minúsculas. Seja* $\{\alpha,\beta\}\subseteq\Sigma^*$, *a palavra* $\alpha\beta$ *será construída pela concatenação de* α *e* β. *O símbolo* ϕ *representa a palavra vazia. É claro que* $\alpha\phi=\phi\alpha=\alpha$.

Exemplo. *Se* $\alpha=BABA$ *e* $\beta=AB$ *então* $\alpha\beta=BABAAB$ *e* $\beta\alpha=ABBABA$.

Seja $\{\alpha,\beta,\gamma\}\subseteq\Sigma^*$. *Então, certamente temos que* $(\alpha\beta)\gamma=\alpha(\beta\gamma)$. *Porém* $\alpha\beta=\beta\alpha$ *nem sempre é válido. Ver o exemplo acima.*

Sejam $\beta\in\Sigma^*$ *e* $n\in\omega\setminus 1$. *Definimos* $\beta^n=\beta^{n-1}\beta$ *e* $\beta^0=\phi$. *Por comprimento de uma palavra* β, *e anotamos* $|\beta|$; *entendemos intuitivamente:* $|\phi|=0$; $|L|=1$ *para todo* $L\in\Sigma$ *e para todo* $\{\alpha,\beta\}\subseteq\Sigma^*$ *temos* $|\alpha\beta|=|\alpha|+|\beta|$.

Exemplo: Seja $\alpha=ABABBAA=ABAB^2A^2$ *então* $|\alpha|=7$. *Se* $\beta=L^n$ *para* $L\in\Sigma$ *e* $n\in\omega$, *então* $|\beta|=n$.

Seja $\alpha\in\Sigma^*$, *então* $\overline{\alpha}$ *denota a palavra formada pelos mesmos elementos que compõe* α, *concatenados em ordem inversa. Porem podemos observar que, se* $\alpha=L^n$, *então* $\overline{\alpha}=\alpha$, *sempre que* $L\in\Sigma$ *e que* $n\in\omega$. *Além disso, para todo* $\alpha\in\Sigma^*$ *temos que* $|\overline{\alpha}|=|\alpha|$.

Exemplo. Seja $\alpha=B^3ABAB^2A^3$ então $\bar{\alpha}=A^3B^2ABAB^3$.

Seja $\alpha\in\Sigma^*$ uma palavra não vazia. Diremos que uma palavra não vazia β é raiz de α se, e somente se, $\alpha=\beta^n$ para algum inteiro positivo n. Podemos observar que toda $\alpha\neq\phi$ admite exatamente uma raiz de menor comprimento que anotamos por $\pi(\alpha)$.

Uma palavra $\alpha\neq\phi$ chama-se primitiva se, e somente se, $\alpha=\pi(\alpha)$; $\alpha\neq\pi(\alpha)$ diremos que α é não primitiva. Observemos que $\pi(\pi(\alpha))=\pi(\alpha)$ para toda $\alpha\in\Sigma^*\setminus\{\phi\}$; isto é, $\pi(\alpha)$ é primitiva.

Exemplo. Se $\alpha=BA^2B^2A^2B^2A^2B^2A^2B=(BA^2B)^4$ então as palavras BA^2B e $(BA^2B)^2$ são raízes de α, e $\pi(\alpha)=BA^2B$. Se $\alpha=L^n$ então $\pi(\alpha)=L$ para todo $L\in\Sigma$. A palavra $\beta=B^3ABA^2$ é primitiva pois $\pi(\beta)=B^3ABA^2$.

Para cada $L\in\Sigma$ a expressão $Mult(L,\alpha)$ denota o conjunto de todas as posições nas quais a letra L ocorre para a formação, isto é, "soletração" da palavra α. Uma palavra α é dita não trivial se, e somente se, $|Mult(L,\alpha)|\neq 1$ para todo $L\in\Sigma$.

A expressão $gcd(\alpha)$ denota o maior fator comum de $\{|Mult(L,\alpha)|:L\in\Sigma\}$.

Exemplo. Se $\alpha=B^4A^2BA$ então $Mult(B,\alpha)=\{1,2,3,4,7\}$ e $Mult(A,\alpha)=\{5,6,8\}$. Já que $|Mult(A,\alpha)|=3$ e que $|Mult(B,\alpha)|=5$, logo α é não trivial e $gcd(\alpha)=1$.

Lema 1.5. *Seja* $\{\alpha,\beta\}\subseteq\Sigma^*\setminus\{\phi\}$. *Então* $\alpha\beta=\beta\alpha$ *se, e somente se,* $\pi(\alpha)=\pi(\alpha\beta)$.

Demonstração. [10, *Apêndice, página 50*].

Seja $\alpha\in\Sigma^*$. *Diremos que* $\beta\neq\phi$ *é segmento de* α *se e somente se* $\alpha=\tau\sigma$ *para algum* $\{\tau,\sigma\}\subseteq\Sigma^*$. *Denominamos* β *segmento à esquerda (respectivamente à direita) de* α *se e somente se* $\alpha=\beta\lambda$ $(\alpha=\lambda\beta)$ *para algum* $\lambda\in\Sigma^*$.

Seja $\{\alpha,\beta\}\subseteq\Sigma^*$. *Seja* $L\in\Sigma$ *e seja* $n\in\omega\setminus 1$. *Ao par* $\langle\lambda,L^n\rangle$ *denominamos L-fila de tamanho n de* α *se, e somente se,*

i) λL^n *é segmento à esquerda de* α;

ii) λL^{n+1} *não é segmento a esquerda de* α;

iii) L *não é segmento a direita de* λ.

Denominamos complexidade de uma palavra $\alpha\in\Sigma^*$, *e anotamos por* $cmplx(\alpha)$, *ao número de filas distintas de* α.

Exemplo: *Se* $\alpha=B^2A^2B^3A^2$ *então suas filas são* $\langle\phi,B^2\rangle,\langle B^2,A^2\rangle$, $\langle B^2A^2,B^3\rangle$ *e* $\langle B^2A^2B^3,A^2\rangle$. *Assim* $cmplx(\alpha)=4$. *Se* $L\in\Sigma$ *e* $n>1$, *então* $cmplx(L^n)=1$. *Para* $\{A,B\}\subseteq\Sigma^*$ *e para* $\{n,p,m\}\subseteq\omega\setminus 1$ *temos que* $cmplx(A^nB^m)=2$ *e* $cmplx(A^nB^pA^m)=3$.

Seja $\{\alpha,\beta\}\subseteq\Sigma^*$. *Diremos que* α *é ciclicamente equivalente a* β *e anotamos* $\alpha\sim\beta$ *se, e somente se, existe* $\{\mu,\lambda\}\subseteq\Sigma^*$ *tal que* $\alpha=\mu\lambda$, *enquanto que* $\beta=\lambda\mu$.

Exemplo: $A^2B^4A\sim A^3B^4\sim B^2A^3B^2\sim AB^4A^2\sim BA^3B^3$.

Proposição 1.6. *A relação $\sim$ é uma relação de equivalência em Σ^*.*

Demonstração: [10, Proposição 1.18].

Lema 1.7. *Seja $\{\alpha,\beta\}\subseteq\Sigma^*\setminus\{\phi\}$. Então $\alpha\sim\beta$ se, e somente se, ambos $|\alpha|=|\beta|$ e $|\pi(\alpha)|\sim|\pi(\beta)|$.*

Demonstração: [7, Lema 3.2].

Definição 1.8. Seja $W\subseteq\Sigma^*$. Seja $.W.\in\Sigma^*\times\Sigma^*$ definida como segue: $\alpha.W.\beta$ se, e somente se, existe uma sequência $\alpha=\gamma_0,\gamma_1,\ldots,\gamma_j=\beta$ tal que, para todo $i\in j$ se tenha:

i) $\gamma_i\sim\gamma_{i+1}$ ou

ii) existe $\psi\in W$ tal que $\gamma_{i+1}=\gamma_i\psi$, ou

iii) existe $\psi\in W$ tal que $\gamma_i=\gamma_{i+1}\psi$.

Diremos que a sequência $\alpha=\gamma_0,\gamma_1,\ldots,\gamma_j=\beta$ leva α em β por W. O símbolo α/W vai denotar $\{\beta:\beta.W.\alpha\}$.

Lema 1.9. *A relação $.W.$ é relação de equivalência em Σ^**

Demonstração [10, Lema 1.22].

Consideremos Σ^* como definido anteriormente. Dado Σ, escolhamos Σ' com $\Sigma\cap\Sigma'=\phi$ e com $|\Sigma|=|\Sigma'|$. Seja $':\Sigma\to\Sigma'$ uma bijeção $L\to L'$. Então $F(\Sigma)$ e $(\Sigma\cup\Sigma')^*$ junto com a relação de equivalência $\stackrel{\sim}{\sim}$ definida assim: $\alpha\stackrel{\sim}{\sim}\beta$ se, e somente se, existe uma sequência finita $\sigma=\sigma_0,\sigma_1,\ldots,\sigma_k=\beta$ tal que para cada $i\in k$ ou $\sigma_i=\sigma_{i+1}$ ou existe $L\in\Sigma$ tal que $\sigma_i=\lambda\tau$ enquanto que $\sigma_{i+1}\in\{\lambda LL'\tau,\lambda L'L\tau\}$ ou $\sigma_{i+1}=\lambda\tau$ enquanto que $\sigma_i\in\{\lambda LL'\tau,\lambda L'L\tau\}$, é o grupo livre gerado por Σ.

Cada homomorfismo $f: F(\Sigma) \to G$, *onde* G *é grupo, é unicamente determinado por* $f \upharpoonright \Sigma$ *no seguinte sentido: Para todo* $L \in \Sigma$ *temos que* $f(L') = f(L)^{-1}$.

Seja $\alpha \in F(\Sigma)$. *Através de* [4, §2], *diremos que* α *é ciclicamente reduzida se, e somente se, qualquer* β *e qualquer* γ $\gamma \sim \beta \approx \alpha$ *então* $|\alpha| \leq |\gamma|$.

Observação. Se α *é ciclicamente reduzida e* $\beta \sim \alpha$ *então* β *é ciclicamente reduzida.*

Universalidade de uma palavra para um grupo. Seja $\alpha \in F(\Sigma) \setminus \{\phi\}$. *Seja* G *um grupo e seja* $x \in G$. *Diremos que* α *representa* x *em* G, *e anotamos* $(\alpha \downarrow x)G$, *se existe um homomorfismo* $H: F(\Sigma) \to G$ *tal que* $H(\alpha) = x$. *Denominamos* α *universal para* G *se, e somente se,* $(\alpha \downarrow x)G$ *para todo* $x \in G$. *Quando* α *é universal para* G *escrevemos* $(\alpha \downarrow\downarrow G)$ *ou que* α *é* G*-universal.*

Seja M *uma família de grupos. Diremos que* α *é* M*-universal se, e somente se,* α *é* X*-universal para todo* $X \in M$. *Diremos que* α *é finitamente* M*-universal, e anotamos* FM*-universal se, e somente se,* α *é* X*-universal para todo* X *finito pertencente a* M, *e* α *é infinitamente* M*-universal, anotamos* IM*-universal se, e somente se,* α *é* X*-universal para todo* X *infinito, pertencente a* M.

Observação. Neste trabalho Sym *denota o conjunto* $\{Sym(X) : X$ *é conjunto*$\}$, Prt *denota o conjunto* $\{Prt(X) : X$ *é conjunto*$\}$, Myc *denota o conjunto* $\{{}^X X : X$ *é conjunto*$\}$ *e* Alt *denota o conjunto* $\{Alt(k) : k \in \omega\}$.

Seja $\phi \neq A \subseteq Z \setminus 1$. *A expressão* $mdc(A)$ *denota max* $\{d: d|a$ *para todo* $a\ A\}$.

Quando for conveniente a expressão $mdc(\{x,y\})$ *é escrita* (x,y).

CAPÍTULO II - A REPRESENTAÇÃO DE GRUPOS SIMÉTRICOS

Introdução: Em recente trabalho [5] estendem-se as técnicas usadas em [2] e em [10] a fim de ser estabelecido o

Teorema 2.1. Seja α qualquer palavra primitiva de complexidade menor que seis. Então $(\alpha\downarrow s)Sym(Z)$.

Encontramos em [1] a

Proposição 2.2. A palavra B^2A^2 é $Sym(X)$-universal para todo X infinito.

O artigo [1], não apresenta uma demonstração para a proposição 2.2, mas indica um esboço e um diagrama, muito uteis no desenvolvimento de nossas idéias, neste trabalho, dando-nos um caminho para a demonstração exigida.

Em nosso Capítulo III, apresentamos um exemplo, amplo e detalhado, para exemplificarmos todas as técnicas usadas por D.M.Silberger e M.L.Valente na demonstração do Teorema 2.1. Então, em nosso Capítulo IV, estendemos um pouco os resultados alcançados pelo Teorema 2.1, em conjunto com os resultados relacionados em [10].

No Capítulo V aproveitamos as técnicas sugeridas em [1] para demonstrar nosso principal teorema, que $cmplx(\pi(\alpha))<4$ implica em $\pi(\alpha)$ é $ISym$-universal.

No presente capítulo, apresentamos um breve histórico do estudo das palavras que são FSym-universais ou I-Sym-universais.

Em 1966, J.R.Isbell publicou o primeiro artigo [3] sobre a questão, introduzida por J. Mycielski, sobre termos universais. Neste artigo encontra-se o

Teorema 2.3. *Se* $\alpha \neq \phi$ *não é da forma* $\alpha=\beta\gamma\beta$ *para* $\beta \neq \phi$, *então* α *é* ${}^{X}X$*-universal para todo conjunto* X *infinito.*

Mas, as técnicas usadas por J.R.Isbell na demonstração do Teorema 2.3, aparentemente não permitem uma resposta a seguinte pergunta natural: Se $\alpha \neq \phi$ *não é da forma* $\alpha=\beta\gamma\beta$ *para* $\beta \neq \phi$, *então* α *é ISym-universal?*

Este problema continua em aberto e é nossa principal consideração, neste trabalho.

Também em [3] encontra-se um resultado que é aplicado na área de termos FSym-universais. Este resultado de J.R.Isbell é

Teorema 2.4. *Seja* n *potência de primo. Seja* $k \in \omega \setminus 1$, *e seja* $f \in {}^{k}k$. *Então existem* $g \in {}^{k}k$ *e uma involução* $h \in {}^{k}k$ *tais que* $f=g^{n}h$.

Isto, junto com o Teorema 2.3, imediatamente implica que, se n *é potência de primo, e se* m *é inteiro ímpar, então as palavras* $B^{n}A^{m}$ *e* $A^{m}B^{n}$ *são Myc-universais.*

Além disso, sendo $h \in Sym(k)$ *com* $k \in \omega \setminus 1$, *e sendo* $f=g^{n}h$ *com* $\{f,g\} \subseteq {}^{k}k$, *temos pelo Lema 1.1 que* $f \in Sym(k)$ *se, e somente se,* $g \in Sym(k)$. *Desta forma obtivemos o*

Corolário 2.5. Seja n potência de inteiro primo, e seja m inteiro ímpar. Então as palavras B^nA^m e A^mB^n são FSym universais.

Empregando técnicas desenvolvidas por J.R. Isbell na demonstração do Teorema 2.4, A.Ehrenfeucht e D.M. Silberger publicam um melhoramento do Teorema 2.4:

Teorema 2.6. Seja $2^i||n$ com $n>2^i$. Então as seguintes condições são equivalentes:

1. $2^{i+1}< S(n/2^i)$;

2. Para todo $k\in\omega\setminus 1$ e para toda $f\in {}^kk$, existem $g\in {}^kk$ e h involução de k tal que $f=g^nh$.

Deixaremos de mencionar os corolários do Teorema 2.6, pois são análogos aos do Teorema 2.4.

Os mesmos autores publicam [2], em que encontramos o seguinte resultado análogo aos Teoremas 2.4 e 2.6, mas mais forte. Este é

Teorema 2.7. Sejam $n>1<m$ inteiros. Então as seguintes condições são equivalentes:

1. $M(S(n))$ não é fator de m e $M(S(m))$ não é fator de n.

2. As palavras B^nA^m e A^mB^n são Myc-universais.

3. As palavras B^nA^m e A^mB^n são FSym-universais.

Também em [2] encontramos um resultado muito importante no desenvolvimento dos trabalhos [10] e [5] e, para esta dissertação.

Teorema 2.8. Sejam $m\neq 0\neq n$ inteiros quaisquer. Então $(B^nA^m \dashv s)Sym(Z)$.

De fato, melhorando as técnicas empregadas na demonstração em [2] do Teorema 2.8, fica estabelecido em [5] o

Teorema 2.9. Sejam $p>n>0$ e $q>m>0$ inteiros quaisquer. Então existe $\{f,g\}\subseteq Sym(Z)$ tal que $s=g^nf^m$ enquanto que $g^p=id\restriction Z=f^q$.

O principal teorema de D.M.Silberger em [8] permite uma vasta exemplificação das técnicas usadas na demonstração do Teorema 2.7, e resulta em [6] no seguinte:

Teorema 2.10. Sejam $n>1<m$ inteiros. Então as seguintes condições são equivalentes:

1. $M(S(n))$ não é fator de m, e $M(S(m))$ não é fator de n.
2. As palavras B^nA^m e A^mB^n são Myc-universais.
3. As palavras B^nA^m e A^mB^n são FSym-universais.
4. As palavras B^nA^m e A^mB^n são Prt-universais.

No capítulo V deste trabalho, apresentamos um resultado obtido que representa um melhoramento bastante forte, porque afirma que B^nA^m é FSym-universal não só sob as condições que $M(S(n))\nmid m$ e $M(S(m))\nmid n$, mas também que B^nA^m é $Sym(X)$-universal para todo X infinito e para todo $n\neq 0\neq m$ inteiros quaisquer.

Colocamos agora as seguintes perguntas:

Pergunta 2.11. *Se* $\pi(\alpha)=B^nA^mB^pA^q$ *então* $\pi(\alpha)$ *é ISym-universal?*

Mais geralmente

Pergunta 2.12. $\pi(\alpha)$ *é ISym-universal para qualquer* $\pi(\alpha)$?

Pergunta 2.13. *Dado* α *uma palavra de grupo que é ciclicamente reduzida e tal que* α *não é da forma* β^n *para* $|n|>1$, *então* α *é ISym-universal?*

CAPÍTULO III - PALAVRAS DE COMPLEXIDADE MENOR QUE SEIS

O principal ponto de partida para os resultados originais que apresentamos no Capítulo IV, é [5] , que pode ser escrito como segue:

Teorema 3.1. Seja $\pi(\alpha)$ de complexidade menos que seis. Então $(\pi(\alpha)\downarrow s)Sym(Z)$.

O espírito, de nossas contribuições, aparece no exemplo característico abaixo apresentado. Escolhemos a palavra primitiva

(3.1) $\pi(\alpha)= A^4B^{27}A^9B^{19}A^{11}$ de comprimento 70 e de complexidade 5. Para esta $\pi(\alpha)$ construímos explicitamente duas permutações, a e b de Z tais que

(3.2) $s=a^4b^{27}a^9b^{19}a^{11}$, $\Lambda(a)=\{1,15\}$ e $\Lambda(b)=\{1,12\}$.

As condições $\Lambda(a)=\{1,15\}$ e $\Lambda(b)=\{1,12\}$ que implicam $ord(a)=15$ e $ord(b)=12$, respectivamente, não são necessárias neste exemplo; ficamos com estas condições a fim de que as etapas da demonstração, em [5], do teorema acima, sejam fielmente exibidas.

O diagrama I indica o jeito de conseguirmos $\{b_1,a_1\}$ subconjunto de $Sym(Z)$ tal que

(3.3) $s=b_1a_1$, $\Lambda(a_1)=\{1,5\}$ e $\Lambda(b_1)=\{1,6\}$

sem tentar generalizar, escrevemos componentes cíclicas das permutações a_1 e b_1 obtidas no diagrama I.

Assim temos do diagrama I que:

(3.4) $b_1=(0\ 1\ 2\ 3\ 4\ -1)(8\ 9\ 10\ 11\ 12\ -2)(16\ 17\ 18\ 19\ 20\ -3)(24\ 25\ 26\ 27\ 28\ -4)(32\ 33\ 34\ 35\ 36\ -5)(40\ 41\ 42\ 43\ 44\ -6)\ldots$

(3.5) $a_1=(-1\ 5\ 6\ 7\ 8)(-2\ 13\ 14\ 15\ 16)(-3\ 21\ 22\ 23\ 24)(-4\ 29\ 30\ 31\ 32)(-5\ 37\ 38\ 39\ 40)\ldots$

A próxima etapa é procurar $\{b_3,a_3\}\subset Sym(Z)$ *tal que*

(3.6) $b_3^{10}=b_1$, $\Lambda(b_3)=\{1,12\}$

$a_3^{9}=a_1$ *e* $\Lambda(a_3)=\{1,15\}$

Este processo exige duas etapas para conseguirmos b_3 *de* b_1 *e* a_3 *de* a_1. *Iniciemos o processo com* b_1. *Temos, de (3.4), que* $\Lambda(b_1)=\{1,6\}$. *Também* $(ord(b_1),10)=(6,10)=2$. *Mas queremos* $b_3^{10}=b_1$ *enquanto* $\Lambda(b_3)=\{1,12\}$. *Nossa primeira subetapa para* b_1 *é buscar uma permutação* b_2 *tal que* $b_2^5=b_1$ *enquanto que* $\Lambda(b_2)=\Lambda(b_1)=\{1,6\}$. *Já que* $(ord(b_1),5)=(6,5)=1=6.1+5.(-1)$, *temos que* $b_1=b_1^6(b_1^{-1})^5=(b_1^{-1})^5$. *Seja* $b_2=b_1^{-1}$. *Por* [5] *temos que* $\Lambda(b_2)=\{1,6\}$. *Obviamente também* $b_2^5=b_1$. *De fato, da expressão (3.4), obtemos*

(3.7) $b_2=(0\ -1\ 4\ 3\ 2\ 1)(8\ -2\ 12\ 11\ 10\ 9)(16\ -3\ 20\ 19\ 18\ 17)(24\ -4\ 28\ 27\ 26\ 25)(32\ -5\ 36\ 35\ 34\ 33)(40\ -6\ 44\ 43\ 42\ 41)\ \ldots$

Nossa segunda subetapa é intercalar aos pares as componentes 6-cíclicas de b_2, *seguindo técnica empregada na demonstração do Teorema 3.1 em* [5], *a fim de obtermos uma permutação* b_3 *de* Z *tal que* $(b_3)=\{1,12\}$ *enquanto* $b_3^2=b_2$. *De fato, da expressão (3.7), obtemos*

(3.8) $b_3=(0\ 8\ -1\ -2\ 4\ 12\ 3\ 11\ 2\ 10\ 1\ 9)(16\ 24\ -3\ -4\ 20\ 28\ 19\ 27\ 18\ 26\ 17\ 25)(32\ 40\ -5\ -6\ 36\ 44\ 35\ 43\ 34\ 42\ 33\ 41)\ldots$

Segue que $(b_3)^{10}=(b_3^3)^5=b_2^5=b_1$, *com desejávamos.*

Terminemos o processo com a_1. *Temos de (3.5) que* $\Lambda(a_1)=\{1,5\}$. *Também* $(ord(a_1),3)=(5,3)=1=2.5+(-3).3$. *Portanto* $a_1=(a_1^5)^2(a_1^{-3})^3=(a_1^{-3})^3$. *Seja* $a_2=a_1^{-3}$. *Então de (3.5) obtemos*

(3.9) $a_2=(-1\ 6\ 8\ 5\ 7)(-2\ 14\ 16\ 13\ 15)(-3\ 22\ 24\ 21\ 23)(-4\ 30\ 32\ 29\ 31)(-5\ 38\ 40\ 37\ 39)(-6\ 46\ 48\ 45\ 47)\ldots$

Observemos que $a_2^3=a_1$ *enquanto que* $\Lambda(a_2)=\Lambda(a_1)=\{1,5\}$. *Até aqui temos a subetapa um. A subetapa dois consiste em intercalar de forma tríplice as componentes 5-cíclicas de* a_2 *a fim de obter uma* a_3 *tal que* $a_3^2=a_2$ *enquanto* $\Lambda(a_3)=\{1,15\}$. *Desta maneira, de (3.9), obtemos*

(3.10) $a_3=(-1\ -2\ -3\ 6\ 14\ 22\ 8\ 16\ 24\ 5\ 13\ 21\ 7\ 15\ 23)(-4\ -5\ -6\ 30\ 38\ 46\ 32\ 40\ 48\ 29\ 37\ 45\ 31\ 39\ 47)\ldots$

Notemos que as permutações b_3 *e* a_3 *assim obtidas satisfazem as condições (3.6) exigidas. Notemos também de (3.3) e (3.6) que temos satisfeitas as condições*

(3.11) $s=a_3^9b_3^{10}$ e $a_3=id\restriction Z=b_3^{12}$

Nossa próxima observação é que

$$b^3sb^{-3}=b_3^3a_3^9b_3^{10}b_3^{-3}=b_3^3a_3^9b_3^7.$$

Seja

(3.12) $$s_1=b_3^3sb_3^{-3}$$

Acontece, por [2, Teorema 4.3] que $s'\simeq s$. Mas não precisamos utilizar este fato no presente argumento. Consideremos o homomorfismo $H:F(\{A,B\})\to Sym(Z)$ gerado por $A\to a_3$ e $B\to b_3$. Com $\beta=B^3A^9B^7$ temos que $H(\beta)=s_1$. De fato, $H(\eta)=s_1$, paraqualquer η obtida de β por uma sequência de "inserções" em qualquer posição dentro de β, ou dentro de palavras assim conseguidas de β, das palavras B^{12} e/ou A^{15}.

Exemplos de tais palavras η, expansões de β, são $B^{15}A^9B^7$, $B^{15}A^9B^7A^{15}$, $B^2A^{15}B^{13}A^9B^7A^{15}$, $B^2A^{15}B^{13}AB^{25}A^8B^7A^{15}$, e a palavra que nos interessa no presente

(3.13) $$\delta=A^{15}B^{27}A^9B^{19}$$

Como mencionamos

(3.14) $$s_1=a_3^{15}b_3^{27}a_3^9b_3^{19}$$

Seja

(3.15) $$s_2=a_3^{11}s_1a_3^{-11}$$

Segue, de (3.14), que $s_2=a_3^{-11}a_3^{15}b_3^{27}a_3^9b_3^{19}a_3^{11}$, e portanto que

(3.16) $$s_2=a_3^4b_3^{27}a_3^9b_3^{19}a_3^{11}$$

Assim vimos que $(\pi(\alpha)\downarrow s_2)Sym(Z)$. *Agora seja*

(3.17) $$f=b_3^{-3}a_3^{11}$$

Então, de (3.12) e (3.15) temos que $s=b_3^{-3}s_1b_3^3=b_3^{-3}a_3^{11}s_2a_3^{-11}b_3^3=(b_3^{-3}a_3^{11})s_2(b_3^{-3}b_3^{11})$, *e portanto, por (3.17)* *que*

(3.18) $$s=fs_2f^{-1}$$

Notemos, para $g\in Sym(Z)$ *e* $z\in Z$ *quaisquer, que* $(fgf^{-1})^z=(fgf^{-1})(fgf^{-1})\ldots(fgf^{-1})=fg^zf^{-1}$. *Desta forma, segue por (3.16) juntamente com (3.18), que* $s=fa_3^4b_3^{27}a_3^9a_3^{11}f^{-1}=fa_3^4f^{-1}b_3^{27}f^{-1}fa_3^9f^{-1}fb_3^{19}f^{-1}fa_3^{11}f^{-1}=(fa_3f^{-1})^4(fb_3f^{-1})^{27}(fa_3f^{-1})^9(fb_3f^{-1})^{19}(fa_3f^{-1})^{11}$.

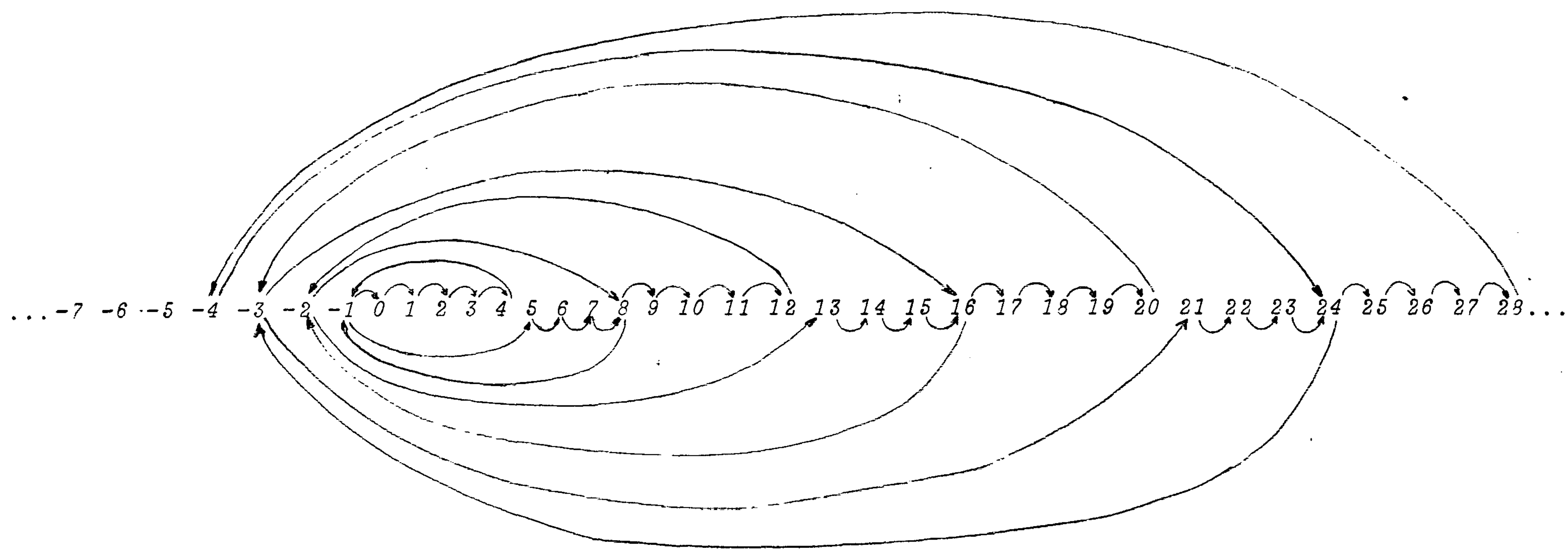
Assim, com a estipulação

(3.19) $$b=fb_3f^{-1}$$
$$a=fa_3f^{-1}$$

temos que $s=a^4b^{27}a^9b^{19}a^{11}$. *Segue que* $(\pi(\alpha)\downarrow s)Sym(Z)$. *Também de* [9] *temos que* $\Lambda(a)=\Lambda(a_3)=\{1,15\}$ *e que* $\Lambda(b)=\Lambda(b_3)=\{1,12\}$. *Isto é, as permutações a e b de Z satisfazem as condições (3.2). Formalmente, nossos cálculos para este exemplo poderiam terminar agora. Mas, tendo comprometido as permutações a e b explícitas, calcularemos umas poucas componentes cíclicas de a e b, e com elas mostraremos que a equação de (3.2), que é* $s=a^4b^{27}a^9b^{19}a^{11}$, *realmente é satisfeita pelo menos no subconjunto* $\{x:-6<x<14\}$ *do domínio Z das funções a, b e s.*

TÁBUAS E GRÁFICOS

Diagrama II



Consideramos agora: a_1 - acima

b_1 - abaixo

Tábua 1

Considere a_1 e b_1 como em (3.3) e (3.4)

$\vdots$	$\xrightarrow{b_1}$	$\vdots$	$\xrightarrow{a_1}$	$\vdots$
-14		104		-13
-13		96		-12
-12		88		-11
-11		80		-10
-10		72		-9
-9		64		-8
-8		56		-7
-7		48		-6
-6		40		-5
-5		32		-4
-4		24		-3
-3		16		-2
-2		8		-1
-1		0		0
0		1		1
1		2		2
2		3		3
3		4		4
4		-1		5
5		5		6
6		6		7
7		7		8
8		9		9
9		10		10
10		11		11
11		12		12
12		-2		13
13		13		14
14		14		15
15		15		16
16		17		17
$\vdots$		$\vdots$		$\vdots$

Tábua 2

Considere a_3 e b_3 como em (3.10) e (3.8)

b_3^{10}		a_3^9
⋮	⋮	⋮
-18	136	-17
-17	128	-16
-16	120	-15
-15	112	-14
-14	104	-13
-13	96	-12
-12	88	-11
-11	80	-10
-10	72	- 9
- 9	64	- 8
- 8	56	- 7
- 7	48	- 6
- 6	40	- 5
- 5	32	- 4
- 4	24	- 3
- 3	16	- 2
- 2	8	- 1
- 1	0	0
0	1	1
1	2	2
2	3	3
3	4	4
4	- 1	5
5	5	6
6	6	7
7	7	8
8	9	9
9	10	10
10	11	11
11	12	12
12	- 3	13
13	13	14
⋮	⋮	⋮

$s=b_3^{10}a_3^9$

Tábua 3

Temos que $a=b_3^{-3}a_3^{11}b_3^{-11}b_3^{3}$

		$\xrightarrow{b_3^3}$	$\xrightarrow{a_3^{-11}}$	$\xrightarrow{b_3}$	$\xrightarrow{a_3^{11}}$	$\xrightarrow{b_3^{-3}}$
	⋮	⋮	⋮	⋮	⋮	⋮
	0	-2	22	22	-2	0
um 12-ciclo de a	1	8	13	13	8	1
	2	9	9	0	0	10
	10	0	0	8	-3	25
	25	-3	8	-1	21	21
	21	21	-1	-2	7	7
	7	7	-2	4	1	-1
	-1	12	12	3	3	-2
	-2	3	3	11	11	4
	4	11	11	2	2	12
	12	2	2	10	10	3
	3	10	10	1	1	11
	11	1	1	9	9	2
	5	5	15	15	5	5
um 12-ciclo de a	6	6	17	24	14	14
	14	14	24	-3	15	15
	15	15	-3	-4	45	45
	45	45	-4	20	20	24
	24	20	20	28	28	-3
	-3	28	28	19	19	-4
	-4	19	19	27	27	20
	20	27	27	18	18	28
	28	18	18	26	26	19
	19	26	26	17	17	27
	27	17	17	25	25	18
	18	25	25	16	6	6
	7	7	-2	4	4	8
	⋮	⋮	⋮	⋮	⋮	⋮

Tábua 4

$s=a^4b^{27}a^9b^{19}a^{11}$, onde a e b são as permutações obtidas conforme (3.19)

	$\xrightarrow{a^{11}}$	$\xrightarrow{b^{19}}$	$\xrightarrow{a^{9}}$	$\xrightarrow{b^{27}}$	$\xrightarrow{a^{4}}$
⋮	⋮	⋮	⋮	⋮	⋮
-6	-6	30	31	-5	-5
-5	-5	32	45	-4	-4
-4	-4	14	15	-3	-3
-3	-3	6	7	-2	-2
-2	-2	25	21	-1	-1
0	7	11	11	25	1
1	25	12	12	2	2
2	2	-2	-2	3	3
3	3	8	8	4	4
4	4	21	22	22	5
5	22	22	23	23	6
6	23	23	17	17	7
7	17	17	25	8	8
8	8	2	2	21	9
9	21	3	3	10	10
10	10	4	4	11	11
11	11	-1	-1	12	12
12	12	7	1	1	13
13	1	1	9	9	14
14	9	9	5	5	15
⋮	⋮	⋮	⋮	⋮	⋮

CAPÍTULO IV - PALAVRAS VULNERÁVEIS

Com o objetivo de resolvermos a representação de s *em* $Sym(Z)$ *através de palavras do grupo livre* $F(\Sigma)$, *fizemos um estudo que resultou em algumas conclusões, aumentando as condições suficientes para aplicar as técnicas contidas em* [5].

Definição 4.1. *Seja* $p \in \omega \setminus 2$. *Seja* $n(0), n(1), \ldots, n(p-1)$ *uma sequência de números inteiros. Chamaremos esta sequência fatoramente vulnerável se, e somente se, existe* $\in i$ p *tal que* $mdc\{n(j) : j \in p\} \neq mdc\{n(j) : i \neq j \in p\}$.

Exemplo. *Seja a sequência* $2,3,4,8$. *Temos* $mdc\{2,4,8\}=2$, *enquanto que* $mdc\{2,3,4,8\}=1$. *Portanto a sequência* $2,3,4,8$ *é fatoramente vulnerável.*

Definição 4.2. *Chamamos uma palavra* α *vulnerável se, e somente se, existem* $\beta \sim \alpha$ *e uma letra* L *em* β *tais que a sequência dos comprimentos dos blocos de* L *em* β *é fatoramente vulnerável.*

Terminologia. *O conjunto de todas as palavras vulneráveis será representado por* V.

Teorema 4.3. *Seja* $\alpha \in V$. *Então* $(\alpha \downarrow s) Sym(Z)$.

Demonstração: *Por hipótese existem* L *em* α *e* $\beta \sim \alpha$ *tais que a sequência* $n(0), n(1), \ldots, n(p-1)$ *dos comprimentos dos blocos de* L *em* β *é fatoramente vulnerável. Então existe* i p *tal que* $mdc\{n(j): j \; p\} \neq mdc\{n(j): i \neq j \; p\}$. *Sejam* $d = mdc\{n(j): i \neq j \; p\}$ *e* x *o resto sob a divisão de* $n(i)$ *por* d. *Observe* que $0<x<d$ pois $d \nmid n(i)$. Podemos supor que a letra L é diferente da letra A. Seja γ a palavra obtida pela substituição em β da letra A para toda ocorrência em β das letras diferentes de L. Sejam $t=|\beta|-\sum_{j=0}^{p-1} n(j)$ e $W=\{L^d, A^{t+1}\}$. Desde que, obviamente, $\gamma.W.L^x A^t$ para $t>1$, temos por [5, lema 3], que $(\gamma+s)Sym(Z)$. Segue que $(\beta+s)Sym(Z)$, e portanto, por [2, Teorema 4.3], $(\alpha+s)Sym(Z)$.

Lema 4.4. Seja $F(\{A,B\})$ com complexidade par, isto é, $d=B^{n(1)}A^{m(1)}B^{n(2)}A^{m(2)},,,B^{n(j)}A^{m(j)}$, com $\{n(i),m(i)\}\ \omega\setminus 1$ para todo $i\in\{1,2,\ldots,j\}$ tal que ou $n(1),n(2),\ldots,n(i-1)$, $n'(i),n''(i),n(i+1),\ldots,n(j)$ é fatoramente vulnerável para algum $\{n'(i),n''(i)\}\subseteq\omega$, com $n'(i)+n''(i)=n(i)$, ou condição análoga é satisfeita pelos $m(t)$, com $t\in\{1,2,\ldots,j\}$.

Demonstração: Suponha que $\alpha\in V$. Então existe $\beta\sim\alpha$ tal que ou os comprimentos dos blocos de B em β ou os de A em β é fatoramente vulnerável. Sem perda de generalidade, podemos escrever $\beta=B^{n''(i)}A^{m(i)}B^{n(i+1)}A^{m(i+1)}\ldots B^{n(j)}A^{m(j)}B^{n(1)}$ $A^{m(1)}B^{n(2)}A^{m(2)}\ldots B^{n(i-1)}A^{m(i-1)}B^{n''(i)}$ e podemos supor que ou $n''(i),n(i+1),\ldots n(j),\ldots n(2),\ldots,n(i-1),n'(i)$ é fatoramente vulnerável, com $n'(i)>0<n''(i)$ e com $n'(i)+n''(i)=n(i)$, como queríamos. A recíproca é óbvia.

Consideremos $\alpha\in F(\Sigma)$. Diremos que α é fracamente primitiva, representaremos $\alpha\in\mathrm{F}$, se ambas $\alpha=\pi(\alpha)$ e $gcd(\alpha)>1$ acontecem. Por outro lado se $\alpha=\pi(\alpha)$ e $gcd(\alpha)=2i+1$ com $i\in\omega\setminus 1$, diremos que α é muito fracamente primitiva e representaremos $\alpha\in\mathrm{MF}$.

Observação. Consideremos agora s em $Sym(Z)$, bem como todos seus conjugados cíclicos. Podemos observar que estas três palavras representam todas as classes de $\sim$-equivalência geradas pelas sequências $3,3,2$ e $2,1,1$ (sendo β um segmento a esquerda de α).

Observação. Seja $\alpha \in \{B^3A^2B^2ABA,\ B^3AB^2A^2BA\}$. Vê-se facilmente que as sequências $3,2,1$ e $2,1,1$ são relativamente primas aos pares, mas $gcd(\alpha)=2$ e portanto $\alpha \in F$. Estas duas palavras, cada uma de comprimento 10, são as mais curtas que ainda não tem estabelecidas suas capacidades, em relação a representação de s em $Sym(Z)$.

Observação. Seja $\alpha=B^{n(1)}A^{m(1)}\ldots B^{n(j)}A^{m(j)}$ de complexidade de par, com $j>2$. Então há uma relação natural de equivalência, $\underset{-}{J}$, tal que $\beta \underset{-}{J}$ se, e somente se, existe permutações f e g dos inteiros $\{1,2,\ldots,j\}$ tais que $\beta=B^{n(f(1))}A^{m(g(1))}\ldots B^{n(f(j))}A^{m(g(j))}$.

Pergunta 4.6. Dado $j>2$, qual é o número cardinal $J(\alpha,j)$ do conjunto $\{\beta: \exists\, \gamma \underset{-}{J}\ B^{n(1)}A^{m(1)}\ldots B^{n(j)}A^{m(j)}$ e $\beta\sim\gamma\}$, e qual é o número cardinal $P(\alpha,j)$ de $\{(f,g): f$ e g são permutações de $\{1,2,\ldots,j\}\}$ para atingir $J(\alpha,j)$.

Naturalmente, ambos $J(\alpha,j)$ e $P(\alpha,j)$, espera-se, sejam máximo e mínimo respectivamente, para todo j, se $|\{n(i): i=1,2,\ldots,j\}|=|\{m(i): i=1,2,\ldots,j\}|=j$.

Corolário 4.7. Seja $\alpha=A^{n(1)}B^{m(1)}A^{n(2)}B^{m(2)}A^{n(3)}B^{m(3)}$ tal que $n(3)$ não é múltiplo de $mdc\{n(1),n(2)\}$. Então $(\alpha \nmid s)Sym(Z)$.

Demonstração: Já que $mdc\{n(1),n(2),n(3)\}<mdc\{n(1),n(2)\}$, temos que $\alpha\in V$. O corolário segue do Teorema 4.3.

Podemos observar que cada homomorfismo $f:F(\Sigma)\to F(\Sigma)$ é perfeitamente determinado por $f\restriction\Sigma$; isto é $f\restriction\Sigma=g\restriction\Sigma$ se, e somente se, $f=g$.

Proposição 4.8. Seja M um monóide qualquer. Seja $x\in M$. Se $(\beta\downarrow x)M$ e $(\alpha\downarrow\beta)F(\Sigma)$, então $(\alpha\downarrow x)M$.

Demonstração: Temos $(\beta\downarrow x)M$ se, e somente se, existe um homomorfismo $h:F(\Sigma)\to M$ com $h:\beta\to x$, e $(\alpha\downarrow\beta)F(\Sigma)$ se, e somente se, existe $f:F(\Sigma)\to F(\Sigma)$ tal que $f:\alpha\to\beta$. Então observemos que $hf:F(\Sigma)\to M$ é homomorfismo tal que $hf:\alpha\to x$. Assim segue a proposição.

Proposição 4.9. Seja $f:F(\Sigma)\to F(\Sigma)$ um homomorfismo e $\alpha\in F(\Sigma)$ tal que $f(\alpha)\neq\phi$. Então $gcd(\alpha)|gcd(f(\alpha))$.

Demonstração: Já que $f(\alpha)\neq\phi$ temos que $\alpha\neq\phi$. Para cada letra $A\in f(\alpha)$ temos que $Mlt(A,f(\alpha))=\{Mlt(L,\alpha).\ Mlt(A,f(L)):$ L é letra em $\alpha\}$. Portanto, já que $gcd(\alpha)|Mlt(L,\alpha)$ para cada L, temos que $gcd(\alpha)|Mlt(A,f(\alpha))$ para cada A em $f(\alpha)$. Segue que $gcd(\alpha)|gcd(f(\alpha))$.

Corolário 4.10. Sejam $\alpha\in F(\Sigma)$ e $f:F(\Sigma)\to F(\Sigma)$ homomorfismo tal que $f(\alpha)\neq\phi$. Então $\alpha\in\mathrm{F}$ implica que $f(\alpha)\in\mathrm{F}$, e $\alpha\in\mathrm{MF}$ implica que $f(\alpha)\in\mathrm{MF}$.

Demonstração. É óbvio da proposição 4.9.

Pergunta 4.11. O recíproco do Corolário 4.9 é verdade? O que acontece se crescermos a complexidade de α?

CAPÍTULO V - REPRESENTAÇÃO EM SYM(Z)

Em [1] A.Ehrenfeucht, S.Fajtlowicz, J.Malitz e J.Mycielski afirmam, sem apresentarem demonstração, que A^2B^2 é ISym-universal. Neste capítulo, estabeleceremos o nosso principal teorema cuja parte mais importante é que A^mB^n é ISym-universal para todo $\{m,n\}\subseteq\omega\setminus 1$.

Lema 5.1. Sejam X um conjunto e $\{k,p\}\subseteq\omega\setminus 1$. Para cada $i\in p$, seja $g_i\in Sym(X)$ tal que g_i tem uma única componente não trivial, sendo $\Lambda(g_i)\subseteq\{1,k\}$. Seja $\{g_i\colon i\in p\}$ conjunto dcp contendo exatamente p elementos. Então existe $f\in Sym(X)$ tal que f tem uma única componente não trivial, que $\Lambda(f)\subseteq\{1,pk\}$ e que $f^p=g_0\, g_1\, \cdots\, g_{p-1}$.

Demonstração. Para cada $i\in p$ escrevemos $g_i=({}_ix_0\ {}_ix_1\ \cdots\ {}_ix_{k-1})$. Seja f a permutação de X, cuja única componente não trivial é o pk-ciclo $({}_0x_0\ {}_1x_0\cdots{}_{p-1}x_0\ {}_0x_1\ {}_1x_1\ \cdots{}_{p-1}x_1\ \cdots{}_0x_{k-1}\ {}_1x_{k-1}\ {}_1x_{k-1}\cdots{}_{p-1}x_{k-1})$. É claro que f satisfaz todas as condições para a conclusão do Lema.

Terminologia. O processo usado na demonstração do Lema 5.1, afim de obtermos f do p-bloco $g_0g_1\cdots g_{p-1}$ de k-ciclos, chamaremos de intercalação do bloco $g_0g_1\cdots g_{p-1}$.

Corolário 5.2. Seja $k\in\omega\setminus 2$, e seja X um conjunto infinito. Seja $g_0, g_1,\ldots$ uma sequência infinita e injetiva de k-ciclos em Sym(X) tal que $\{g_i\colon i\in\omega\}$ é dcp. Seja g a permutação de X, cujo conjunto das componentes é $\{g_i\colon i\in\omega\}$. Então existe $f\in Sym(X)$ tal que $\Lambda(f)\subseteq\{1,p^k\}$ e que $f^p=g$.

Demonstração. Escrevendo $g=g_0g_1\dots g_{p-1}g_p\dots g_{2p-1}g_{2p}\dots$, intercalemos cada p-bloco de componentes k-cíclicas de g, como indicado pelos parênteses na seguinte expressão:

$$g=(g_0\ g_1\dots g_{p-1})(g_p\ g_{p+1}\ \dots g_{2p-1})\dots$$

Assim, obtemos $f=f_0f_1\dots f_i\dots$, onde cada f_i é da intercalação do p-bloco $g_{ip}g_{ip+1}\dots g_{(i+1)p-1}$ como na demonstração do Lema 5.1. Esta f satisfaz os requerimentos do corolário.

De 5.3 abaixo até 5.11, inclusive, suponhamos que f seja elemento em $Sym(Z)$. Suponhamos também, até o final do presente capítulo, que $\{m,n\}\subseteq\omega\setminus 2$.

Lema 5.3. Seja $f=(0\ 1\ 2\ \dots\ k-1)\in Sym(Z)$. Então existe $\{a,b\}\subseteq Sym(Z)$ tal que $f=b^na^m$.

Demonstração. Definamos $g=g_0g_1\dots$ onde o conjunto $\{g_i: i\in\omega\}$ das componentes k-cíclicas de g tem número cardinal $\aleph_0$, e tal que $g(x)=x$ para todo $x\in Z$ com $f(x)\neq x$. Então $fg=fg$; isto é, $fg_0g_1\dots=fg_0g_1g_2\dots$. Nos dois lados da igualdade, associemos os blocos das componentes fg da seguinte maneira:

$$f(g_0\ g_1\ \dots g_{m-1})(g_m\ g_{m+1}\dots g_{2m-1})\dots=$$
$$(f\ g_0\ g_1\ \dots\ g_{n-2})(g_{n-1}\ g_n\ \dots\ g_{2n-2})\ \dots$$

Por intercalação dos blocos assim indicados, obtemos $fh_0^mh_1^m\dots h_j^m\dots=d_0^nd_1^n\dots d_j^n\dots$, onde cada h_i é um mk-ciclo em $Sym(Z)$ tal que $d_i^n=g_{in-1}g_{in}\dots g_{(i+1)n-2}$ com $i>0$, mas tal que $d_0^n=$

$fg_0g_2\ldots g_{n-2}$. Definamos as permutações $b=d_0d_1\ldots d_j\ldots$ e $a^{-1}=h_0h_1\ldots h_j\ldots$ de Z, e observamos que $f(a^{-1})^m=b^n$. Portanto $f=b^na^m$.

Notemos que o Lema 5.3 depende do fato que Z é infinito. De fato, nós observamos que A^2B^2 não representa c_k em $Sym(k)$ sempre que k é par.

Lema 5.4. Seja $\{m,n,t\}\subseteq\omega\setminus 2$, e seja $k_i\in\omega\setminus 2$ para cada $i\in t$. Seja f_i um k_i-ciclo no conjunto Z, para cada $i\in t$, seja $\{f_i:i\in t\}$ dcp. Seja $f=f_0f_1\ldots f_{t-1}\in Sym(Z)$. Então existe $\{a,b\}\subseteq Sym(Z)$ tal que $f=b^na^m$.

Demonstração. Seja $h=g_0^{(0)}g_0^{(1)}\ldots g_0^{(t-1)}g_1^{(0)}g_1^{(1)}\ldots g_1^{(t-1)}\ldots$ onde os comprimentos dos ciclos $g_i^{(j)}$ é k_j, para todos $\langle j,i\rangle\in t\times\omega$. Já que $\{x:f(x)=x\}$ é infinito, podemos construir os $g_i^{(j)}$ de tal maneira que o conjunto $\{f_j:\ j\in t\}\cup\{g_i^{(j)}:\ \langle j,i\rangle\in t\times\omega\}$ é dcp. Então observemos que $f_0g_0^{(0)}g_1^{(0)}\ldots g_i^{(0)}\ldots f_1 g_0^{(1)}g_1^{(1)}\ldots g_i^{(1)}\ldots f_jg_0^{(j)}g_1^{(j)}\ldots g_i^{(j)}\ldots f_{t-1}g_0^{(t-1)}g_1^{(t-1)}\ldots g_i^{(t-1)}\ldots$, e portanto que nós podemos associar, em blocos indicados por parênteses, os dois lados da igualdade consequentemente, como aparece a seguir:

$$(f_0g_0^{(0)}g_1^{(1)}\ldots g_{n-2}^{(1)})(g_{n-1}^{(0)}\ g_n^{(0)}\ldots g_{2n-2}^{(0)})\ldots$$
$$(g_{in-1}^{(0)}\ g_{in}^{(0)}\ \ldots g_{(i+1)n-2}^{(0)})\ldots(f_1g_0^{(1)}\ g_1^{(1)}\ \ldots g_{n-2}^{(1)})$$
$$(g_{n-1}^{(1)}\ \ g_n^{(1)}\ldots g_{2n-2}^{(1)})\ldots(g_{in-1}^{(1)}\ g_{in}^{(1)}\ldots g_{(i+1)n-2}^{(1)})$$
$$\ldots(f_{t-1}\ g_0^{(t-1)}\ \ g_1^{(t-1)}\ \ldots g_{n-2}^{(t-1)})(g_{n-1}^{(t-1)}\ \ g_n^{(t-1)}$$
$$\ldots g_{2n-2}^{(t-1)})\ldots(g_{in-1}^{(t-1)}\ g_{in}^{(t-1)}\ \ldots g_{(i+1)n-2}^{(t-1)})\ldots\ =$$
$$f(g_0^{(0)}\ g_1^{(0)}\ \ldots g_{m-1}^{(0)})(g_m^{(0)}\ g_{m+1}^{(0)}\ \ldots g_{2m-1}^{(0)})\ldots$$

$$(g_{im}^{(0)}\ g_{im+1}^{(0)} \ldots g_{(i+1)m-1}^{(0)}) \ldots (g_0^{(1)}\ g_1^{(1)} \ldots g_{m-1}^{(1)})\ (g_m^{(1)} g_{m+1}^{(1)} \ldots g_{2m-1}^{(1)}) \ldots (g_{im}^{(1)} \ldots g_{(i+1)m-1}^{(1)}) \ldots (g_0^{(t-1)}\ g_1^{(t-1)} \ldots g_{m-1}^{(t-1)})(g_m^{(t-1)}\ g_{m+1}^{(t-1)} \ldots g_{2m-1}^{(t-1)}) \ldots (g_{im}^{(t-1)}\ g_{im+1}^{(t-1)} \ldots g_{(i+1)m-1}^{(t-1)}) \ldots$$

Então, intercalemos ciclos e assim obtemos a igualdade

$$(G_0^{(0)})^n (G_1^{(0)})^n \ldots (G_i^{(0)})^n \ldots (G_0^{(1)})^n (G_1^{(1)})^n \ldots (G_i^{(1)})^n \ldots (G_o^{(t-1)})^n (g_1^{(t-1)})^n \ldots (G_i^{(t-1)})^n \ldots =$$

$$f(H_0^{(0)})^m (H_1^{(0)})^m \ldots (H_i^{(0)})^m \ldots (H_0^{(1)})^m (H_1^{(1)})^m \ldots (H_i^{(1)})^m \ldots (H_0^{(t-1)})^m (H_1^{(t-1)})^m \ldots (H_i^{(t-1)})^m \ldots$$

onde $G_0^{(j)}$ *é o* nk_j*-ciclo obtido pela intercalação do n-bloco* $f_j g_0^{(j)} \ldots g_{n-2}^{(j)}$ *para todo* $j \in t$*, e onde* $G_i^{(j)}$ *é o* nk_j*-ciclo obtido pela intercalação do n-bloco* $g_{in-1}^{(j)} g_{in}^{(j)} \ldots g_{(i+1)n-2}^{(j)}$ *para todo* $\langle j,i\rangle \in t\times(\omega\setminus 1)$*; enquanto que* $H_i^{(j)}$ *é o* mk_j*-ciclo obtido pela intercalação do m-bloco* $g_{im}^{(j)}\ g_{im+1}^{(j)} \ldots g_{(i+1)m-1}^{(j)}$ *para todo* $\langle j,i\rangle \in t\times\omega$.

Seja $b = G_0^{(0)} G_1^{(0)} \ldots G_i^{(0)} \ldots G_0^{(1)} G_1^{(1)} \ldots G_i^{(1)} \ldots G_0^{(t-1)} G_1^{(t-1)} \ldots G_i^{(t-1)} \ldots$, *e seja* $a^{-1} = H_0^{(0)} H_1^{(0)} \ldots H_i^{(0)} \ldots H_0^{(1)} \ldots H_1^{(1)} \ldots H_i^{(1)} \ldots H_0^{(t-1)} H_1^{(t-1)} \ldots H_i^{(t-1)} \ldots$. *Temos então* $b^n = f(a^{-1})^m$*, e consequentemente que* $f = b^n a^m$.

Corolário 5.5. Seja $\{m,n\} \subseteq \omega\setminus 2$*. Seja* $k_o, k_1, \ldots$ *uma sequência infinita em* $\omega\setminus 2$*. Para cada* $i \in \omega$ *seja* f_i *um* k_i*-ciclo em* Z*, e sejam a sequência* $f_o, f_1, \ldots$ *injetiva e o conjunto*

$\{f_i: i\in\omega\}$ dcp. Seja f a permutação cujo conjunto das componentes cíclicas não triviais é $\{f_i: i\in\omega\}$ tal que o conjunto $\{x: f(x)=x\}$ é infinito. Então existe $\{a,b\}\subseteq Sym(Z)$ tal que $f=b^n a^m$.

Demonstração. Seja $F=\{x: f(x)=x\}$. Então já que F é infinito, temos que $|F|=|F\times\omega|$. Portanto existe $r:F\to F\times\omega$ bijeção, e a família $\{F_i: i\in\omega\}$ é uma partição de F em classes infinitas, onde F_i denota $r^{-1}[F\times\{i\}]$ para cada $i\in\omega$.

Agora, para cada $i\in\omega$ seja $F_i'=F_i\cup\{x: f_i(x)\neq x\}$. Usando a técnica do Lema 5.3 encontramos $\{a_i,b_i\}\subseteq Sym(F_i')$ tal que $f_i\restriction F_i'=b_i^n a_i^m$. Sejam $a=\bigcup\{a_i: i\in\omega\}$ e $b=\bigcup\{b_i: i\in\omega\}$. Observe que $f=\bigcup\{f_i|F_i': i\in\omega\}=\bigcup\{b_i^n a_i^m: i\in\omega\}$. Afirmamos que $\{b_i^n a_i^m: i\in\omega\}=b^n a^m$. Seja $<x,y>\in\bigcup\{b_i^n a_i^m: i\in\omega\}$. Então $<x,y>\in b_j^n a_j^m$ para algum $j\in\omega$. Então, $<x,y>\in b^n a^m$ pois $b_j\subseteq b$ e $a_j\subseteq a$. Segue que $\{b_i^n a_i^m: i\in\omega\}\subseteq b^n a^m$. Por outro lado, suponha que $<p,q>\in b^n a^m$. Então existe componente cíclica d de $b^n a^m$ tal que $<p,q>\in d$. Mas, já que $\{F_i': i\in\omega\}$é uma partição de Z, temos que existe $t\in\omega$ tal que $p\in F_t'$. Então $q=b^n a^m(p)=b^n a_t^m(p)=b^n(a_t^m(p))=b_t^n(a_t^m(p))=b_t^n a_t^m(p)$, e portanto $<p,q>\in b_t^n a_t^m\subseteq\bigcup\{b_i^n a_i^m: i\in\omega\}$. Segue que $b^n a^m\subseteq\bigcup\{b_i^n a_i^m: i\in\omega\}$. A afirmação segue. O corolário fica provado.

Lema 5.6. Sejam $\{m,n,k\}\subseteq\omega\setminus 2$, e $f\in Sym(Z)$ tal que $f=c_k s'$ onde $s'\sim s$. Então existe $\{a,b\}\subseteq Sym(Z)$ tal que $f=b^n a^m$.

Demonstração. Como $s'\approx s$, temos por [2, Theorem 4.3] que $s'=uv$, com $\{u,v\}\subseteq Sym(Z)$. De fato, podemos escolher $\{u,v\}\subseteq Sym(Z)$ tal que $\Lambda(u)\subseteq\{1,k\}$ e $\Lambda(v)\subseteq\{1,q\}$, onde $q\in\omega\setminus 2$ é ar-

bitrário, e tal que ambos, u *e* v*, tenham um conjunto infinito de componentes cíclicas não triviais. Podemos também supor que o conjunto* $\{c_k, u, v\}$ *é dcp. Desta forma existem sequências infinitas e injetivas* $u_0, u_1, \ldots$ *e* $v_0, v_1, \ldots$ *com* u_i *um k-ciclo para todo* $i \in \omega$ *e com* v_j *um q-ciclo para todo* $j \in \omega$ *(ver diagrama I). Seja* $u = u_0\, u_1 \ldots$ *e seja* $v = v_0 v_1 \ldots$ *Então* $f = (0\ 1\ \ldots\ k-1)\ u_0\ u_1 \ldots v_0\ v_1\ \ldots$ *. Associemos, em blocos, cada lado da igualdade, da seguinte maneira:*

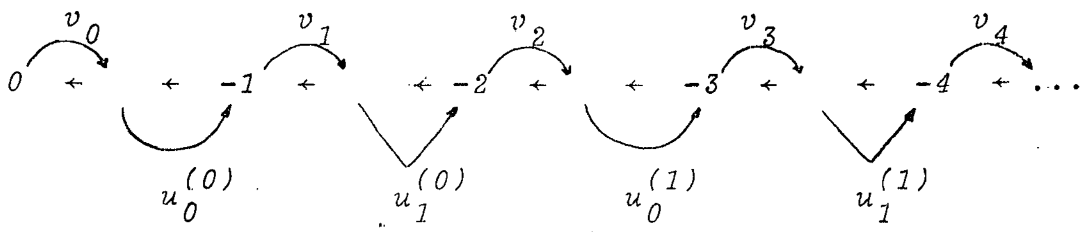
$$f = ((0\ 1\ \ldots\ k-1)\ u_0\ u_1 \ldots u_{n-2})(u_{n-1}\ u_n \ldots u_{2n-2})$$
$$\ldots (v_0\ v_1 \ldots v_{m-1})(v_m\ v_{m-1} \ldots v_{2m-1}) \ldots$$

Assim obtemos $f = (G_0^n\ G_1^n \ldots G_j^n \ldots)(H_0^m\ H_1^m \ldots H_j^m \ldots)$ *onde* G_0 *é o nk-ciclo obtido pela intercalação do n bloco* $(0\ 1\ \ldots\ k-1)\ u_0\ u_1 \ldots u_{n-2}$*, e* G_j *é o nk-ciclo obtido pela intercalação do n-bloco* $u_{(j-1)n-1} \ldots u_{jn-2}$ *para todo* $j \in \omega \setminus 1$*, enquanto que* H_j *é o mq-ciclo obtido pela intercalação do m-bloco* $v_{jm}\ v_{jm+1} \ldots v_{(j+1)m-1}$ *para todo* $j \in \omega$*. Sejam* $b = G_0 G_1 \ldots G_j \ldots$ *e* $a = H_0 H_1 \ldots H_j \ldots$ *. Observamos que* $b^n = G_0^n\ G_1^n \ldots G_j^n \ldots$ *e que* $a^m = H_0^m\ H_1^m \ldots H_j^m\ \ldots$ *. Assim* $f = b^n a^m$.

Lema 5.7. Sejam $\{k_0, k_1, m, n\} \subseteq \omega \setminus 2$ *e* $f \in Sym(Z)$ *com três componentes não triviais, um* k_0*-ciclo* f_0*, um* k_1*-ciclo* f_1 *e um ciclo infinito* s'*. Então existe* $\{a, b\} \subseteq Sym(Z)$ *tal que* $f = b^n a^m$.

Demonstração. Temos por [2, Theorem 4.3] que $s' = uv$ *para* $\{u, v\} \subseteq Sym(Z)$ *tal que* $\Lambda(u) = \{1, k_0, k_1\}$*, tal que* $\Lambda(v) \subseteq \{1, q\}$ *para algum* $q \in \omega \setminus 2$*, tal que o conjunto das componentes cíclicas não triviais de* v *e de* u *são ambos infinitos sendo* $\{u_i^{(0)} : i \in \omega\}$ *conjunto de componentes* k_0*-cíclicas,* $\{u_i^{(1)} : i \in \omega\}$ *de com* ponentes k_1-cíclicas, e tal que o conjunto $\{f_0,f_1\}\cup\{u_i^{(0)}: i\in\omega\}\cup\{u_i^{(1)}: i\in\omega\}$ é dep. De fato podemos supor que a função $2\times\omega\to Sym(Z)$ definida por $\langle j,i\rangle\mapsto u_i^{(j)}$ é injetiva, que $u=u_0^{(0)}u_0^{(1)}u_1^{(0)}u_1^{(1)}u_2^{(0)}u_2^{(1)}\ldots u_j^{(0)}u_j^{(1)}\ldots$. Semelhantemente podemos supor que a sequência infinita $v_0,v_1,\ldots v_j\ldots$ é injetiva e que $v=v_0v_1\ldots v_j\ldots$. Conseguimos estas componentes cíclicas e u e v, da maneira indicada no diagrama seguinte (lembrando o diagrama I).

Diagrama 5.7.1



Agora $f=f_0f_1u_0^{(0)}u_0^{(1)}u_1^{(0)}u_1^{(1)}\ldots u_j^{(0)}u_j^{(1)}\ldots v_0 v_1\ldots v_j\ldots$

$=f_0u_0^{(0)}u_1^{(0)}\ldots u_j^{(0)}\ldots f_1u_0^{(1)}u_1^{(1)}\ldots u_j^{(1)}\ldots v_0v_1\ldots v_j\ldots$

Agrupemos o n-bloco $f_0u_0^{(0)}\ldots u_{n-2}^{(0)}$ de k_0-ciclos e intercalemos para obtermos um nk_0-ciclo ${}_{(0)}G_0^n=f_0u_0^{(0)}u_1^{(0)}\ldots u_{n-2}^{(0)}$. Para cada $i>0$, agrupemos o n-bloco $u_{in-1}^{(0)}u_{in}^{(0)}\ldots u_{(i+1)n-2}^{(0)}$ de k_0-ciclos e por intercalação obtemos o nk_0-ciclo ${}_{(0)}G_i$ tal que ${}_{(0)}G_i^n=u_{in-1}^{(0)}u_{in}^{(0)}\ldots u_{(i+1)n-2}^{(0)}$. Da mesma forma, agrupemos o n-bloco $f_1u_0^{(1)}\ldots u_{n-2}^{(1)}$ de k_1-ci - clos, e obtemos por intercalação um nk_1-ciclo ${}_{(1)}G_0$ tal que ${}_{(1)}G_0^n=f_1u_0^{(1)}u_1^{(1)}\ldots u_{n-2}^{(0)}$; e, para cada $i>0$, agrupemos o n-bloco $u_{in-1}^{(1)}u_{in}^{(1)}\ldots u_{(i+1)n-2}^{(1)}$ de k_1-ciclos para obter mos, por intercalação, um nk_1-ciclo ${}_{(1)}G_i$ tal que ${}_{(1)}G_i = u^{(1)}_{in-1}u^{(1)}_{in}\ldots u^{(1)}_{(i+1)n-2}$. Por último, para cada $j\in\omega$, agrupemos o m-bloco $v_{jm}v_{jm+1}\ldots v_{jm-1}$, e intercalemos obtendo assim o mq-ciclo H_j tal que $H^m_j = v_{jm}v_{jm+1}\ldots v_{jm-1}$. Seja $b = {}_{(0)}G_0\ {}_{(0)}G_1 \ldots {}_{(1)}G_0\ {}_{(1)}G_1 \ldots$ e $a = H_0H_1\ldots$ Então $f = b^na^m$.

Corolário 5.8. Sejam $\{m,n,t\}\subseteq\omega\smallsetminus 2$ e $k_i\in\omega\smallsetminus 2$ para cada $i\in t$. Seja f_i um k_i-ciclo no conjunto Z. Seja $f = f_0f_1\ldots f_{t-1}s'$ Sym(Z) tal que s' é um ciclo infinito, e tal que a sequência $f_0, f_1, \ldots, f_{t-1}$ é injetiva e que o conjunto $\{f_0, f_1, \ldots, f_{t-1}, s'\}$ é dcp. Então $f = b^na^m$.

Demonstração. Como nas demonstrações de 5.5 e de 5.7, podemos escrever $s' = uv$, com u e v sujeitas as seguintes estipulações: Existe $q\in\omega\smallsetminus 2$ e sequência infinita injetiva v_0, $v_1, \ldots$ de q-ciclos tal que $\{v_i : i\in\omega\}$ é o conjunto de componentes cíclicas de v. Para cada $j\in t$ há uma sequência infinita $u^{(j)}_0, u^{(j)}_1, \ldots,$ de k_j-ciclos, tal que a função $t\times\omega \to Sym(Z)$ definita por $\langle j,i\rangle \mapsto u^{(j)}_i$ é injetiva e tal que $\{u^{(j)}_i : \langle j,i\rangle\in t\times\omega\}$ é o conjunto de componentes cíclicas de u. Finalmente, podemos também estipular que o conjunto $\{f_j : j\in t\}$ $\cup\{u^{(j)}_i : \langle j,i\rangle\in t\times\omega\}$ é dcp.

O modo de conseguir as $u^{(j)}_i$ mencionadas no parágrafo anterior é uma generalização óbvia do caso $t=2$ tratado em detalhes na demonstração do Lema 5.7. Evitaremos uma repetição dos detalhes na presente redação.

Adotemos uma convenção útil: denominemos f_i de $u^{(j)}_{-1}$ para cada $j\in t$. Assim $f = f_0f_1\ldots f_{t-1}uv = u^{(0)}_{-1}u^{(1)}_{-1}\ldots u^{(t-1)}_{-1}$ $u^{(0)}_0u^{(1)}_0\ldots u^{(t-1)}_0u^{(0)}_1u^{(1)}_1\ldots u^{(t-1)}_1\ldots u^{(0)}_ju^{(1)}_j\ldots u^{(t-1)}_j\ldots$ $v_0v_1\ldots v_i\ldots$, ou ainda $f = u^{(0)}_{-1}u^{(0)}_0u^{(0)}_1u^{(0)}_2\ldots u^{(0)}_i\ldots u^{(1)}_{-1}$

$u_0^{(1)}u_1^{(1)}\ldots u_i^{(1)}\ldots u_{-1}^{(t-1)}u_0^{(t-1)}\ldots u_i^{(t-1)}\ldots v_0v_1\ldots v_i\ldots$. *Agora agrupemos o n-bloco* $u_{in-1}^{(j)}u_{in}^{(j)}\ldots u_{(i+1)n-2}^{(j)}\ldots$ *de* k_j*-ciclos, e intercalemos para obtermos um* nk_j*-ciclo* ${}_{(j)}G_i$ *tal que* ${}_{(j)}G_i^{\;}=u_{in-1}^{(j)}u_{in}^{(j)}\ldots u_{(i+1)n-2}^{(j)}$, *para todo* $\langle j,i\rangle\in t\times\omega$. *Desta mesma forma, agrupemos o m-bloco* $v_{im}v_{im+1}\ldots v_{(i+1)m-1}$ *de q-ciclos, e obtemos por intercalação o mq-ciclo* H_i *tal que* $H_i^m=v_{im}v_{im+1}\ldots v_{(i+1)m-1}$, *para todo* $i\in\omega$. *Seja* $b={}_{(0)}G_0\,{}_{(0)}G_1\ldots{}_{(0)}G_i\ldots{}_{(1)}G_0\ldots{}_{(1)}G_i\ldots{}_{(j)}G_0\,{}_{(j)}G_1\ldots{}_{(j)}G_i\ldots$ *e* $a=H_0H_1\ldots H_i\ldots$. *Então* $f=b^na^m$.

Lema 5.9. Seja $\{m,n\}\subseteq\omega\setminus 2$. *Seja* $k_0,k_1,\ldots$ *uma sequência infinita em* $\omega\setminus 2$. *Seja* $f_0,f_1,\ldots$ *uma sequência finita e injetiva tal que* f_j *é um* k_j*-ciclo para cada* $j\in\omega$. *Seja* $s'\approx s$ *tal que o conjunto* $\{s'\}\cup\{f_j\colon j\in\omega\}$ *é dcp. Finalmente seja f a permutação tendo este conjunto como seu conjunto das componentes cíclicas não triviais. Então existe* $\{a,b\}\subseteq Sym(Z)$ *tal que* $f=b^na^m$.

Demonstração. Seja $q\in\omega\setminus 2$. *Como* $s'\approx s$, *então por* [2, *Theorem* 4.3] $s'=uv$ *para algum* $\{u,v\}\subseteq Sym(Z)$. *Podemos estipular que se* $u(x)\neq x$ *ou* $v(x)\neq x$, *então* $s'(x)\neq x$, *sempre que* $x\in Z$.

Estipulemos agora o conjunto de todas as componentes cíclicas de u de tal maneira que, para todo $j\in\omega$, *existem um número infinito de tais componentes que são de comprimento* k_j. *A estipulação comprometida segue essa tabela triangular:*

$$
\begin{array}{cccccc}
u_0^{(0)} & & & & & \\
u_1^{(0)} & u_0^{(1)} & & & & \\
u_2^{(0)} & u_1^{(1)} & u_0^{(2)} & & & \\
u_3^{(0)} & u_2^{(1)} & u_1^{(2)} & u_0^{(3)} & & \\
\vdots & \vdots & \vdots & \vdots & \ddots & \\
u_i^{(0)} & u_{i-1}^{(1)} & u_{i-2}^{(2)} & u_{i-3}^{(3)} & \cdots & u_0^{(i)} \\
 & & & & & \\
k_0\text{-ciclos} & k_1\text{-ciclos} & k_2\text{-ciclos} & k_3\text{-ciclos} & & k_i\text{-ciclos}
\end{array}
$$

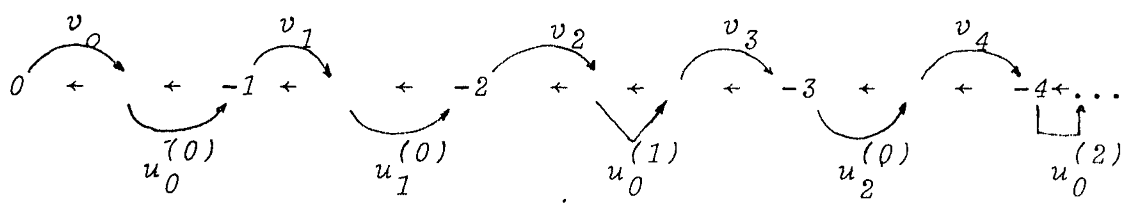
Também estipulemos que a função $\omega\times\omega\to Sym(Z)$ *definida por* $\langle j,i\rangle\mapsto u_i^{(j)}$ *é injetiva. Finalmente, mencionamos que a sequência injetiva* $g_0, g_1, \ldots$ *de componentes cíclicas de* u *é idêntica a sequência obtida pela listagem, na ordem dada no diagrama triangular, das linhas; isto é,*

$$g_0\, g_1 \ldots = u_0^{(0)} u_1^{(0)} u_0^{(1)} u_2^{(0)} u_1^{(1)} u_0^{(2)} \ldots u_0^{(i-1)} u_i^{(0)}$$

$$\ldots u_{i-1}^{(1)} \ldots u_0^{(i)} u_{i+1}^{(0)} \ldots$$

Ver o diagrama abaixo

Diagrama 5.9.1.



Como nas demonstrações anteriores estipularemos que v_i é q-ciclo para todo $i\in\omega$, que a sequência $v_0,v_1,\ldots$ é injetiva, que $\{v_i: i\in\omega\}$ é o conjunto das componentes cíclicas de v e que $\{u_i^{(j)}: <j,i>\in\omega\times\omega\}$ é o conjunto das componentes cíclicas de u.

Adotemos de novo a seguinte convenção: chamemos $f_i=u_{-1}^{i}$ para cada $i\in\omega$. Assim $f=u_{-1}^{(0)}u_0^{(0)}u_1^{(0)}\ldots u_j^{(0)}$ $\ldots u_{-1}^{(1)}u_0^{(1)}u_1^{(1)}\ldots u_j^{(1)}\ldots u_{-1}^{(i)}u_0^{(i)}u_1^{(i)}\ldots u_j^{(i)}\ldots v_0v_1\ldots v_j\ldots$ Agora agrupemos o n-bloco $u_{jn-1}^{(i)}u_{jn}^{(i)}\ldots u_{(j+1)n-2}^{(i)}$ de k_i-ciclos, e intercalemos para obtermos um nk_i-ciclo ${}_{(j)}G_i$ tal que ${}_{(j)}G_i^n=u_{jn-1}^{(i)}u_{jn}^{(i)}\ldots u_{(j+1)n-2}^{(i)}$, para todo $<i,j>\in\omega\times\omega$. Analogamente, agrupemos o m-bloco $v_{jm}\ldots v_{(j+1)m-1}$ de q-ciclos e obtemos, por intercalação, o mq-ciclo H_j tal que $H_j^m=v_{jm}v_{jm+1}\ldots v_{(j+1)m-1}$ para todo $j\in\omega$.

Seja $b={}_{(0)}G_0\,{}_{(0)}G_1\ldots{}_{(0)}G_i\ldots{}_{(1)}G_0\ldots{}_{(1)}G_i\ldots$ ${}_{(j)}G_0\,{}_{(j)}G_1\ldots{}_{(j)}G_i\ldots$, e $a=H_0H_1\ldots H_j\ldots$. Então $f=b^na^m$.

Lema 5.10. Seja $k\in\omega\setminus 3$. Então existe involução $h\in Sym(Z)$ tal que $h\neq id\restriction Z$, tal que c_kh é involução e tal que $c_kh\neq$ $id\restriction Z$.

Demonstração. Seja $c_k=(0\ 1\ \ldots\ k-1)$. Consideremos o caso em que k é par e o caso em que k é ímpar.

1º caso: Seja k par, assim $k=2n>3$. Então $c_{2n}=$ $(0\ 1\ \ldots\ 2n-1)$. Seja $h=(0\ \ 2n-1)(1\ \ 2n-2)\ldots(n-1\ \ n)$. Temos que $c_{2n}h=(0\ 1\ 2\ \ldots\ 2n-1)(0\ \ 2n-1)(1\ \ 2n-2)\ldots(n-1\ \ n)=$ $(1\ \ 2n-1)(2\ \ 2n-2)\ldots(n-1\ \ n+1)$

2º caso: Seja k ímpar, assim $k=2n-1\geq 3$. Então $c_{2n-1}=(0\ 1\ \ldots\ 2n)$. Seja agora $h=(0\ 2n)(1\ 2n-1)\ldots(n-1\ n+1)$. Observemos que $c_{2n-1}h=(0\ 1\ \ldots\ 2n)(0\ 2n)(1\ 2n-1)\ldots(n-1\ n+1)=(1\ 2n)(2\ 2n-1)(3\ 2n-2)\ldots(n\ n+1)$.

Observemos que, em os casos, h e $c_k h$ são involuções tais que $h\neq id\restriction Z$ e $c_k h=id\restriction Z$. Além disso, para k par temos que h tem n componentes 2-cíclicas e que $c_k h$ tem $n-1$ componentes 2-cíclicas para todo $n\in\omega\setminus 2$. Por outro lado, para k ímpar observemos que h tem n componentes 2-cíclicas e $c_k h$ tem n componentes 2 cíclicas para todo $n\in\omega\setminus 1$.

Lema 5.11. Seja $f\in Sym(Z)$, tal que o conjunto $\{x: f(x)=x\}$ é finito e tal que todas as componentes de f são finitas. Então existe $\{a,b\}\subseteq Sym(Z)$ tal que $f=b^n a^m$.

Demonstração. Podemos observar que o conjunto, das componentes cíclicas não triviais de f, tem que ser infinito. Podemos escrever estas componentes em uma sequência $f_0, f_1, \ldots$ infinita e injetiva. Seja $D=\{i:\ f_i$ é um 2 ciclo$\}$. Existe dois casos a considerarmos:

1º caso: D é um conjunto infinito. Então escrevemos f na forma $f=F_0F_1$ onde $\{F_0,F_1\}$ é dcp, e que cada componente cíclica de F_0 é 2-cíclica, e onde nenhuma componente cíclica de F_1 é 2-cíclica. Também escrevemos $F_0=d_0d_1\ldots d_j\ldots$, onde $\{d_i:\ i\in\omega\}$ é o conjunto das componentes cíclicas de F_0; cada d_i é um 2-ciclo; e a sequência $d_0,d_1,\ldots$ infinita é injetiva. É claro que pelo Lema 5.10, que existe involução h em Z tal que $\{F_0,h\}$ é dcp, e tal que F_1h também é involução em Z. Além disso o conjunto $\{F_0, F_1h\}$ é dcp. Separemos F_0 em duas partes: $F_2=d_0d_2\ldots d_{2j}\ldots$ e $F_3=d_1d_3\ldots d_{2j+1}\ldots$. Então, ambos os conjuntos $\{F_3, F_1h\}$ e $\{F_2, h^{-1}\}$ são dcp. Segue que $f=F_0F_1=F_2F_3F_1=F_2F_3F_1hh^{-1}=F_2F_1hF_3h^{-1}$, que o conjunto de componentes 2-cíclicas de F_2F_1h é infinito, e que o conjunto de componentes 2-cíclicas de F_3h^{-1} também é infinito. Assim podemos agrupar em n blocos as componentes 2-cíclicas de F_2F_1h, e intercalá-los, obtendo desta maneira as componentes $2n$-cíclicas de uma permutação b tal que $b^n=F_2F_1h$. Semelhantemente agrupemos em m-blocos, e intercalemos as componentes de F_3h^{-1}, obtendo as componentes $2m$-cíclicas de uma permutação a tal que $a^m=F_3h^{-1}$. Agora $f=b^na^m$.

2º caso: O conjunto D é finito. De novo, escrevemos $f=F_0F_1$, como no 1º caso, com $\Lambda(F_0)\subseteq\{1,2\}$ com $2\notin\Lambda(F_1)$, e com o conjunto $\{F_0, F_1\}$ dcp. Então o conjunto das componetes não triviais de F_1 é infinito, e o comprimento de cada uma dessas componentes é maior que dois. Então escrevemos $F_1=g_0g_1\ldots g_j\ldots$, onde os g_j são as componentes cíclicas não triviais de F_1. Podemos supor também que a sequência infinita $g_0, g_1, \ldots$ é injetiva.

Para cada $j\in\omega$, decorre facilmente do Lema 5.10 que existe involução h_j de Z, com as seguintes propriedades: (1) $h_j\neq id\restriction Z$. (2) para cada $x\in Z$ temos que $g_j(x)=x$ implica que $h_j(x)=x$. (3) g_jh_j também é involução de Z. (4) $g_jh_j\neq id\restriction Z$. É claro que $\{g_i, h_j\}$ é dcp, sempre que $i\neq j$. Seja $h=h_0h_1\ldots h_j\ldots$. Então $F_1h=g_0g_1\ldots g_j\ldots h_0h_1\ldots h_j\ldots =g_0h_0g_1h_1\ldots g_jh_j\ldots$, e o conjunto $\{g_jh_j\colon j\in\omega\}$ é dcp. Assim vimos que F_1h e h são involuções de Z, já que o conjunto $\{h_i: i\in\omega\}$ é dcp. Além disso, o conjunto das componentes 2 cíclicas de F_1h é infinito, o conjunto das componentes 2-cíclicas de h é infinito e $h=h^{-1}$. Finalmente, já que $\{F_0, F_1h\}$ é obviamente dcp, temos que F_0F_1h é involução e tem conjunto infinito de componentes 2-cíclicas. Observe que $f=F_0F_1hh^{-1}$. Por agrupamento e intercalação de n-blocos dos 2 ciclos de F_0F_1h, obtemos as componentes $2n$-cíclicas de uma permutação b tal que $b^n=F_0F_1h$.

Semelhantemente, por agrupamento e intercalação de m-blocos dos 2-ciclos de h^{-1}, obtemos a permutação a tal que $a^m=h^{-1}$. Segue que $f=b^na^m$.

Corolário 5.12. B^nA^m é $Sym(Z)$-universal.

Demonstração. O corolário é imediato dos Lemas 5.3 à 5.9 inclusive, e do Lema 5.11.

Lema 5.13. Seja X infinito e Y tal que $|Y|\leqslant|X|$. Então existe uma partição χ de X tal que para todo $P\in\chi$, $|P|=|Y|$.

Demonstração. Já que $|Y|\leqslant|X|$, existe bijeção $f:X\to X\times Y$. Seja $P_x=\{f^{-1}[\{x\}\times Y]$ para cada $x\in X\}$. Então $\chi=\{P_x: x\in X\}$ claramente é uma partição do tipo desejado.

Teorema 5.14. Sejam $\{m,n\}\subseteq\omega\setminus 2$, e $\alpha=B^nA^m$. Então α é $ISym$-universal.

Demonstração. Seja X infinito, e seja $f\in Sym(X)$. Seja $C=\{f_\lambda: \lambda\in I\}$ o conjunto das componentes cíclicas e não trivi-

ais de f.

Se C for finito, então é fácil representar f na forma $f=b^n a^m$ *com* $\{a,b\}\subseteq Sym(X)$. *Portanto, suponhamos que C é infinito.*

Pelo Lema 5.13 existe uma partição $\{F_\rho : \rho\in P\}$ *de C, tal que* $|F_\rho|=\aleph_0$ *para cada* $\rho\in P$. *Para cada* $\rho\in P$ *seja* $F_\rho^{(f)}$ *o conjunto de todo* $x\in X$ *tal que existem h e* F_ρ *com* $h(x)\neq x$. *Então* $|F_\rho^{(f)}|=\aleph_0$ *já que cada componente cíclica de uma permutação, não pode mudar mais que um número enumerá - vel de pontos.*

Então, para cada $\rho\in P$, *temos pelo Corolário 5.12, que existe* $\{a_\rho, b_\rho\}\subseteq Sym(F^{(f)})$ *tal que* $f\restriction F_\rho^{(f)}=b_\rho^n a_\rho^m$. *Seja* $T=\{x:\ f(x)=x\}$, *seja* $a_T=b_T=id\restriction T$. *Então* $f=\bigcup\{f\restriction F_\rho^{(t)}:\ \rho\in P\}\cup\{f\restriction T\}=\bigcup\{b_\rho^n a_\rho^m : \rho\in P\}\cup\{b_T^n a_T^m\}=b^n a^m$.

Corolário 5.15. Seja $k\in\omega\setminus 1$. *Então a palavra* $A^kB^nA^m$ *é ISym-universal.*

Demonstração. Seja X infinito e seja $f\in Sym(X)$. *Pelo Teorema 5.13 temos que existe* $\{a,b\}\subseteq Sym(X)$ *tal que* $f=b^n a^{m+k}$. *Segue que* $a^k f a^{-k}=a^k b^n a^m$. *Mas o dígrafo* $a^k f a^{-k}$ *é isomorfo ao dígrafo de f. Portanto* $(A^kB^nA^m\downarrow a^k f a^{-k})Sym(X)$, *implica em* $(A^kB^nA^m\downarrow f)Sym(X)$. *O teorema segue.*

BIBLIOGRAFIA

[1] Ehrenfeucht, A., Fajtolowicz, S.,Malitz,J. e Mycielski, J. Some problems on the universality of words in groups, Algebra Universalis (a ser publicado).

[2] Ehrenfeucht,A.. e Silberger D.M. Universal terms of the form $B^n A^m$, Algebra Universalis X (1980).

[3] Isbell, J.R. On the problems of universal terms, Bull de L'Academie Polonaise des Sciences XIV (1966), 593-595.

[4] Lyndon, R.C. Equations in groups, Trabalho de Matemática nº 150, Universidade de Brasília, 1979.

[5] Silberger, D.M. e Valente M.L., Representing the infinite cycle with semigroup (a ser publicado)

[6] Silberger, D.M., $B^n A^m$ is universal iff point universal, Algebra Universalis (em vias de publicação).

[7] Silberger, D.M., Borders and roots of a word, Portugaliae Mathematica, 30(1971), 191-199.

[8] Silberger, D.M., When is a term point universal?, Algebra Universalis (a ser publicado).

[9] *Silberger, D.M., When is gf isomorphic to fg?, (a ser publicado).*

[10] *Valente, M.L., Sobre a universalidade de palavras para grupos simétricos, Dissertação de mestrado, Universidade Federal de Santa Catarina, 1979*