



UFSC

A EQUAÇÃO

$$x^m y^n x^p y^q = f$$

NUM GRUPO SIMÉTRICO

MÍLTON PROCÓPIO DE BORBA

MAIO — 1982

UNIVERSIDADE FEDERAL DE SANTA CATARINA

CAMPUS UNIVERSITÁRIO — CAIXA POSTAL 476 — TRINDADE — FLORIANÓPOLIS — S. C.

A EQUAÇÃO $x^m y^n x^p y^q = f$ NUM GRUPO SIMÉTRICO

por

Milton Procópio de Borba.

Esta dissertação foi julgada adequada para a obtenção do título de

" M E S T R E E M C I Ê N C I A S "

Especialidade em MATEMÁTICA, e aprovada em sua forma final pelo

Curso de Pós-Graduação em Matemática da

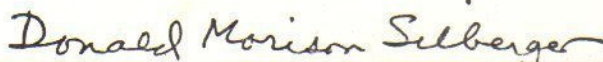
UNIVERSIDADE FEDERAL DE SANTA CATARINA



Prof. INDER JEET TANEJA

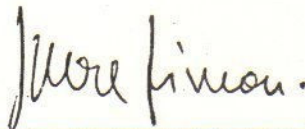
Coordenador

Banca Examinadora:



Prof. Donald Morison Silberger, Ph.D.

Orientador



Prof. Imre Simon, Ph.D.



Prof. Milton Luiz Valente, MSc.

A Equação $x^m y^n x^p y^q = 1$ Num Grupo Simétrico

A meus filhos :

Hilton e Karina

AGRADECIMENTOS :

Ao professor Donald, pela sua orientação, disponibilidade, e paciência, que merecem os melhores adjetivos;

À Rosa, pelas horas e dias que nos separamos para que pudesse realizar esta dissertação;

À Faculdade de Engenharia de Joinville e também à Universidade Federal de Santa Catarina, que possibilitaram a realização deste trabalho;

Aos responsáveis pela minha formação, meus pais, meus professores da primeira série do Primeiro Grau até a última disciplina do curso de Pós-Graduação;

O meu sincero

Muito Obrigado .

RESUMO :

O resultado principal desta dissertação é que a permutação cíclica $i \rightarrow i+1$ de $Z = \{\dots, -1, 0, 1, 2, \dots\}$ pode ser expressa na forma $f^m g^n f^p g^q$ por permutações f e g de Z , sempre que $m \neq p$ ou $n \neq q$.

ABSTRACT :

The main result of this dissertation is that the cyclic permutation $i \rightarrow i+1$ of $Z = \{\dots, -1, 0, 1, 2, \dots\}$ can be expressed in the form $f^m g^n f^p g^q$ for permutations f and g of Z , whenever either $m \neq p$ or $n \neq q$.

ÍNDICE :

Introdução	8
Capítulo I - Preliminares	10
Capítulo II - Histórico	25
Capítulo III - $A^m B^n A^p B^q$ representa δ se e somente se $m \neq p$ ou $n \neq q$	30
Capítulo IV - Comentários gerais e Perguntas	60
Apêndice	64
Referências	81

INTRODUÇÃO :

O nosso principal resultado, Teorema 3.10 que está no Capítulo III , é o seguinte : Se m, n, p e q são inteiros não nulos tais que $m \neq p$ ou $n \neq q$, então existem permutações ϕ e g do conjunto $\mathbb{Z}$ de todos os inteiros tais que $g^m \phi^n g^p \phi^q(x) = x+1$ para todo inteiro x . Isto generaliza o resultado principal de [14] , e aplica-se ao problema de caracterizar as palavras que são universais para grupos simétricos infinitos. Veja [1 , 3 , 5 , 14 , 15] .

A referida generalização é fácil para o caso em que $m+p \neq 0 \neq n+q$ mas aparentemente difícil para o caso $m+p = 0$. Assim a nossa real contribuição é o TEOREMA 3.8, em especial seu LEMA 3.7, que demonstramos exaustivamente no Capítulo III e para o qual oferecemos uma idéia nos Diagramas 4.5 do Apêndice, de uma possível demonstração, diferente daquela dada ao TEOREMA 3.8 .

Também estudamos em geral o problema de solucionar, para toda permutação ϕ dos inteiros, a equação do tipo $y^m x^n y^p x^q = \phi$ no grupo simétrico de $\mathbb{Z}$. Em [1] encontra-se a resposta do problema análogo de solucionar equações do tipo $y^m x^n = \phi$, cujas técnicas procuramos empregar .

O Capítulo I contém as definições, lemas e outros preliminares percorrendo o resto da dissertação, cujo resumo aparece na Tabela 4.7 do Apêndice. O Capítulo II apresenta uma visão histórica do assunto. O Capítulo IV resume o trabalho e propõe problemas relacionados ainda em aberto.

Apresentamos ainda, no Apêndice, a Tabela 4.6 , onde aparece um índice dos lemas, corolários, proposições e teoremas desta dissertação, juntamente com sua numeração total, que pode auxiliar o trabalho de leitura, por ocasião de referências aos mesmos.

Capítulo I :

PRELIMINARES

Neste capítulo aparecem as definições, notações e lemas básicos referentes ao assunto pesquisado nos demais capítulos desta dissertação.

Para conjuntos arbitrários A e B , a expressão $A-B$ denota o conjunto $\{x : x \in A \text{ e } x \notin B\}$. A cardinalidade do conjunto A será denotada por $|A|$.

Como de costume, ω denota o conjunto $\{0, 1, 2, 3, \dots\}$ dos inteiros não negativos; e $\mathbb{Z}$ denota o conjunto de todos os inteiros, ou seja $\mathbb{Z} = \omega \cup \{-n : n \in \omega\}$. Para $k \in \omega$ o símbolo $\underline{k}$ denota o conjunto $\{n : k > n \in \omega\}$. É claro que $|\underline{k}| = k$. Usaremos o símbolo $\aleph_0$ para representar a cardinalidade de ω e o símbolo $\aleph_1$ para representar a cardinalidade dos reais.

Seja $n \in \omega - \underline{1}$. Escreveremos $n|m$ para significar que $m/n \in \mathbb{Z}$; caso contrário escreveremos $n \nmid m$. Quando $n|m$, diremos que n é divisor de m , ou que n é fator de m , ou ainda que m é múltiplo de n .

Seja $x \in \mathbb{Z}$ e seja $t \in \omega - \underline{1}$. Por $(x)_t$ expressamos o único elemento do conjunto $\{x + kt : k \in \mathbb{Z}\} \cap \underline{t}$. É claro que $t \mid (x)_t - x$.

Seja $j \in \omega - \underline{2}$ e seja $D = \{n_i : i \in j\}$ um subconjunto de $\mathbb{Z}$ com pelo menos um n_i não nulo. Então a expressão $(n_0, n_1, \dots, n_j)$ ou a expressão $\text{mdc } D$ denota o máximo divisor

comum entre os elementos de D ; e se $n_i \neq 0$ para todo $i \in j$ então a expressão $[n_0, n_1, \dots, n_j]$ ou a expressão mmc D denota o mínimo múltiplo comum positivo entre os elementos de D . Desta forma, $(n_i, n_j) = 1$ significa que n_i e n_j são relativamente primos entre si. Quando $n \in \omega - 2$, a expressão $S(n)$ denota o menor fator primo de n e a expressão $M(n)$ denota o inteiro positivo $[2, 3, \dots, n]$.

Seja X um conjunto arbitrário e seja $f \subseteq X \times X$. Utilizaremos a expressão $Dom(f)$ e $Im(f)$ para denotar respectivamente o domínio $\{x : \exists y \in X \text{ e } \langle x, y \rangle \in f\}$ de f e a imagem $\{y : \exists x \in X \text{ e } \langle x, y \rangle \in f\}$ de f . Por $Mnd(f)$, expressamos $Dom(f) \cup Im(f)$. Quando A é um conjunto, a restrição de f ao conjunto A é denotada por $f \upharpoonright A$ e significa $(A \times X) \cap f$. Por $f[A]$, expressamos o conjunto $\{y : \langle x, y \rangle \in f \text{ para algum } x \in A\}$. É claro que $f[A] \subseteq Im(f)$ para todo conjunto A .

Seja $f \subseteq X \times X$. Então f é dita conexa se e somente se para cada par de elementos distintos x e y de $Mnd(f)$, existe uma sequência finita $x = z_0, z_1, \dots, z_j = y$ tal que para todo $i \in j$, temos que $\{\langle z_i, z_{i+1} \rangle, \langle z_{i+1}, z_i \rangle\} \cap f \neq \emptyset$.

Quando X é um conjunto qualquer representamos por $Prt(X)$ o conjunto $\{f : f \text{ é função com } Mnd(f) \subseteq X\}$; por ${}^X X$ o conjunto $\{f : f \in Prt(X) \text{ e } Dom(f) = X\}$; e por $Sym(X)$ o conjunto de todas as permutações de X , isto é $Sym(X)$ significa $\{f : f \in {}^X X \text{ e } f \text{ é bijeção}\}$. Notemos que $Prt(X)$ é um monoide, que ${}^X X$ é um submonoide de $Prt(X)$ e que $Sym(X)$ é um subgrupo de ${}^X X$, com respeito à composição de funções. Dizemos ainda que $Sym(X)$ é o grupo simétrico do conjunto X e costuma-

remos , quando possível, expressá-lo tão somente por S_X . O grupo simétrico de real interesse nesta dissertação é o S_Z de todas as permutações dos inteiros .

Também utilizaremos os símbolos Prt , Myc , e Sym para representar respectivamente as classes $\{Prt(X) : X \text{ é conjunto}\}$, $\{^X X : X \text{ é conjunto}\}$ e $\{S_X : X \text{ é conjunto}\}$.

Quando X é um conjunto arbitrário e quando $f \subseteq X \times X$ e $g \subseteq X \times X$, denotaremos simplesmente por fg a composição da relação binária f com a relação binária g . Assim, temos que $fg = \{ \langle x, y \rangle : \exists z \in X \text{ com } \langle x, z \rangle \in g \text{ e com } \langle z, y \rangle \in f \}$. Além disso, se f e g são funções, então $fg(x) = f(g(x))$ sempre que $x \in Dom(g)$ enquanto que $g(x) \in Dom(f)$. Também a composição da relação binária f com ela própria será denotada por f^2 , enquanto que f^n denotará a composição n vezes consecutivas desta relação binária, sempre que $n \in \omega - 1$. Finalmente utilizaremos o símbolo f^0 para denotar $id \upharpoonright X = \{ \langle x, x \rangle : x \in X \}$, também chamado de *ciclo trivial* em X ou *1-ciclo* em X . Se $f \subseteq X \times X$ então f^{-1} denota a relação inversa de f , isto é $f^{-1} = \{ \langle x, y \rangle : \langle y, x \rangle \in f \}$. Claramente, quando $f \in S_X$, temos que $ff^{-1} = id \upharpoonright X = f^{-1}f$.

Definição 1.1 : Sejam $f \subseteq X \times X$ e $g \subseteq X \times X$. Diremos que f é isomórfica bigraficamente com g e anotamos $f \approx g$ se e somente se existe $h \in S_X$ tal que $f = \{ \langle h(x), h(y) \rangle : \langle x, y \rangle \in g \}$.

Facilmente se vê que $\approx$ é uma relação de equivalência de $X \times X$ e também que $f \approx f^{-1}$ sempre que f é uma permutação.

Lema 1.2 : Sejam $f \subseteq X \times X$ e $g \subseteq X \times X$. Então as seguintes afirmações são equivalentes :

1. $f \approx g$,
2. Existe $h \in S_X$ tal que $g = hfh^{-1}$,
3. Existe $h \in S_X$ tal que $gh = hg$.

Demonstração : [13 , corollary of theorem] .

Definição 1.3 : Seja X um conjunto qualquer e seja $H \subseteq S_X$. Diremos que H é disjuncto como permutação, ou simplesmente que H é dcp , se e somente se para cada $\{f, g\} \subseteq H$ tivermos que, para todo $x \in X$, $f(x) = x$ ou $g(x) = x$ sempre que $f \neq g$.

Lema 1.4 : Seja H dcp , e sejam f e g elementos de H . Então $fg = gf$.

Demonstração : [15 , lema 1.3] .

Quando X é um conjunto e $f \in S_X$, dizemos que f é um ciclo não trivial em X se e somente se existe $x \in X$ tal que $f(x) \neq x$ enquanto que $f(y) = y$ sempre que $y \in X - \{f^i(x) : i \in \mathbb{Z}\}$. Neste caso, a expressão $\|f\|$ denota o comprimento deste ciclo, significando $|\{f^i(x) : i \in \mathbb{Z}\}|$. Claramente, $\|f\| > 1$.

Seja f um ciclo não trivial em X , para algum conjunto X . Se $\|f\| = k \in \omega$, dizemos que f é um k -ciclo em X e podemos expressá-lo, quando $f(x) \neq x$, por $(x \ f(x) \ f^2(x) \ \dots \ f^{k-1}(x))$, ou mais geramente por

$(f^i(x) \ f^{i+1}(x) \ \dots \ f^{k-1}(x) \ x \ f(x) \ f^2(x) \ \dots \ f^{i-1}(x))$,
 para qualquer $i \in \underline{k}$. Quando no entanto $\|f\| = \bigcup_0$, dizemos que
 f é um ciclo infinito em X ou que f é um ω -ciclo em X e
 podemos expressá-lo, quando $f(x) \neq x$, na forma
 $(\dots \ f^{-2}(x) \ f^{-1}(x) \ x \ f(x) \ f^2(x) \ \dots)$. Em particular,
 quando $0 < k \in \omega$, o símbolo c_k denota o k -ciclo em ω repre-
 sentado por $(0 \ 1 \ 2 \ \dots \ k-1)$, e o símbolo s usaremos
 para denotar o ω -ciclo em $\mathbb{Z}$ representado por
 $(\dots \ -2 \ -1 \ 0 \ 1 \ 2 \ 3 \ \dots)$, isto é $s(x) = x+1$ para
 cada $x \in \mathbb{Z}$.

Lema 1.5 : Seja X um conjunto e seja $f \in S_X$. Então
 existe um único conjunto C dep de ciclos não triviais em X
 tal que para cada $x \in X$, temos que $f(x) \neq x$ implica que exis-
 te exatamente um ciclo $g \in C$ com $f(x) = g(x)$, mas se $f(x) = x$
 então $g(x) = x$ para cada $g \in C$.

Demonstração : [15, lema 1.5].

Definição 1.6 : Seja X um conjunto e $f \in S_X$. Repre-
 sentaremos o conjunto mencionado no Lema 1.5 por $C_X(f)$ e cha-
 maremos cada ciclo $g \in C_X(f)$ de componente cíclica de f em X .
 É claro que quando $\{f, g\} \subseteq S_X$, temos que $f = g$ se e somente
 se $C_X(f) = C_X(g)$. Também se X e Y são conjuntos distintos,
 então $C_X(f) \cap C_Y(g) = \emptyset$ sempre que $f \in S_X$ e $g \in S_Y$.

Exemplo 1.7 : Seja $X = \underline{7}$ e $Y = \underline{2}$. Seja
 $f = (0 \ 1 \ 2 \ 4) (3 \ 6) \in S_{\underline{7}}$. Então temos que
 $C_{\underline{7}}(f) = \{(0 \ 1 \ 2 \ 4), (3 \ 6)\}$. Seja também
 $g = (0 \ 1 \ 2 \ 4) (3 \ 6) \in S_{\underline{2}}$. Então temos que

$C_2(g) = \{(0\ 1\ 2\ 4), (3\ 6)\}$. Apesar de $C_2(f)$ e $C_2(g)$ serem igualmente representados, temos que o ciclo

$(0\ 1\ 2\ 4) \in C_2(f)$ significa a função determinada por $\{ \langle 0,1 \rangle, \langle 1,2 \rangle, \langle 2,4 \rangle, \langle 4,0 \rangle, \langle 3,3 \rangle, \langle 5,5 \rangle, \langle 6,6 \rangle \}$, enquanto que o ciclo $(0\ 1\ 2\ 4) \in C_2(g)$ significa outra função diferente, onde aparece, por exemplo, o par $\langle 9,9 \rangle$, que não aparece no ciclo $(0\ 1\ 2\ 4) \in C_2(f)$.

Seja $f \in S_X$ para algum conjunto X . Então f é dita uma *transposição* em X se e somente se $f = (x\ y)$ para algum $\{x,y\} \subseteq X$, com $x \neq y$. Pelo teorema de Cauchy [8, pg.96] temos que se X é finito e $g \in S_X$, e se $t_1, t_2, \dots, t_n$ e $t'_1, t'_2, \dots, t'_m$ são transposições em X tais que $t_1 t_2 \dots t_n = g = t'_1 t'_2 \dots t'_m$, então $n+m$ é inteiro par. Dizemos que g é uma permutação *par* se e somente se n for inteiro par, e neste caso então também m é inteiro par. Quando g é permutação não par, dizemos que g é permutação *ímpar*.

Para X finito, A_X denota o conjunto $\{f : f \text{ é permutação par de } X\}$. É possível ver que toda transposição de X é permutação ímpar; que também o ciclo c_{2n} é permutação ímpar; mas que o ciclo c_{2n-1} é permutação par sempre que $n \in \omega - 1$. Também é possível ver que para $\{f,g\} \subseteq S_X$, temos que $fg \in A_X$ se e somente se ou $\{f,g\} \subseteq A_X$ ou $\{f,g\} \subseteq S_X - A_X$.

Quando $1 < m \in \omega$, denotaremos por $C_X(f;m)$ o conjunto $\{g : g \in C_X(f) \text{ e } \|g\| = m\}$ e por $C_X(f;\omega)$, o conjunto $\{g : g \in C_X(f) \text{ e } \|g\| = \aleph_0\}$. Assim, temos que $C_X(f) = C_X(f;\omega) \cup \{C_X(f;i) : 1 < i \in \omega\}$ sempre que $f \in S_X$ para algum conjunto X .

Por X_f denotamos o suporte de f em X , significando o conjunto $\{x : f(x) \neq x \in X\}$. Claramente $X_f \subseteq X$. Quando $X_f = X$ enquanto que f é um ciclo em X , diremos que f é uma permutação cíclica de X . Quando $X_f \neq X$, diremos que x é ponto fixo de f em X se e somente se $x \in X - X_f$.

Seja X um conjunto e $f \in S_X$. Se, para todo inteiro n positivo, tivermos que $f^n \neq id_X$, diremos que f tem ordem infinita e representamos tal fato por $ord(f) = \infty$, ou por $ord(f) = \omega$; caso contrário, $ord(f)$ denota $\min\{n : 0 < n \in \omega \text{ e } f^n = id_X\}$. Em particular, quando $ord(f) \in \{1, 2\}$, diremos que f é uma involução de X .

Observação 1.8 : Quando $f \in S_X$ para algum conjunto X e $ord(f) = t \in \omega - 1$, então

1. $f^x = f^{(x)_t}$ para todo $x \in \mathbb{Z}$;
2. $f^m = f^n$ se e somente se $t \mid (m - n)$.

Lema 1.9 : Seja $(p, k) = 1$. Então existe permutação g cíclica de $\underline{k}$ tal que $g^p = c_k$.

Demonstração : [15, lema 1.7].

Também em [15, lema 1.8], vemos que c_k^m tem exatamente (m, k) ciclos em $\underline{k}$, todos de comprimento $k/(m, k)$ sempre que $0 < m \in \omega$. É fácil ver também que s^m tem exatamente m componentes ω -cíclicas em $\mathbb{Z}$, e que s^m não tem outro ciclo.

Na demonstração do Lema 1.9, Valente observou também que se f é permutação de X então $|C_X(f^m)| \geq |C_X(f)|$ para

Lema 1.10 : Seja n um inteiro com $|n| \neq 1$. Então não existe permutação h de Z tal que $h^n = s$.

Demonstração : Suponha que $h^n = s$ para algum $h \in S_Z$. Então $1 = |C_Z(s)| = |C_Z(h^n)| \geq |C_Z(h)| \geq 1$. Segue que $|C_Z(h)| = 1$, ou seja que h é permutação cíclica de Z . Mas então $C_Z(h^n) = C_Z(h^n; \omega)$ e $|C_Z(h^n; \omega)| = |n|$. Assim, $1 = |C_Z(s)| = |C_Z(h^n; \omega)| = |n|$, o que é uma contradição, já que $|n| \neq 1$. $\square$

Habitualmente denotamos por Σ um alfabeto finito mas arbitrário $\{A, B, C, \dots\}$. Nesta dissertação, designaremos por Σ^+ o semigrupo livre das palavras finitas geradas pela soletração dos elementos de Σ , enquanto que $\Sigma^{\pm}$ denotará o grupo livre das palavras finitas geradas por Σ . Assim temos que $ABAACB \in \Sigma^+$; enquanto que $AB^{-1}CA^{-1}A^{-1} \in \Sigma^{\pm} - \Sigma^+$. Claramente $\Sigma \subseteq \Sigma^+ \subseteq \Sigma^{\pm}$. Representaremos tais palavras pelas letras gregas minúsculas. Quando $\{\alpha, \beta\} \subseteq \Sigma^{\pm}$, a concatenação das palavras α e β será denotada por $\alpha\beta$ e a palavra vazia designaremos por ϕ , com a propriedade que $\alpha\phi = \alpha = \phi\alpha$ para cada $\alpha \in \Sigma^{\pm}$.

Seja $\alpha \in \Sigma^{\pm}$ e seja $n \in \omega - 1$. A concatenação n vezes consecutivas da palavra α será representada por $\alpha^n = \alpha^{n-1}\alpha = \alpha\alpha^{n-1}$, onde α^1 significa α e α^0 significa também a palavra vazia ϕ . Usaremos o símbolo α^{-1} para designar a palavra inversa de α , isto é a palavra com a propriedade que $\alpha^{-1}\alpha = \phi = \alpha\alpha^{-1}$, e o símbolo $\bar{\alpha}$ designará a palavra soletrada na ordem reversa de α . Claramente temos que $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$ e que $\phi^{-1} = \phi$ sempre que $\{\alpha, \beta\} \subseteq \Sigma^{\pm}$.

Exemplo 1.11 : Seja $\alpha = AB^3B = AB^3$ e seja $\beta = B^2A^{-3}$.
 Então $\alpha\beta = AB^5A^{-3}$ enquanto que $\beta\alpha = B^2A^{-2}B^3$; ainda
 $\bar{\alpha} = BBBA = B^3A$ e $\beta^{-1} = A^3B^{-2}$, pois $\beta\beta^{-1} = B^2A^{-3}A^3B^{-2} = \phi$ e
 $\phi = A^3B^{-2}B^2A^{-3} = \beta^{-1}\beta$.

Diremos que a palavra não vazia $\gamma \in \Sigma^+$ é segmento da palavra $\alpha \in \Sigma^+$ quando $\alpha = \mu\gamma\lambda$ para algum $\{\mu, \lambda\} \subseteq \Sigma^+$. Se $\mu = \phi$, diremos que γ é segmento à esquerda de α ; se $\lambda = \phi$ diremos que γ é segmento à direita de α .

Definição 1.12 : Seja $\{\alpha, \lambda\} \subseteq \Sigma^+$, seja $L \in \Sigma$ e seja $0 < n \in \omega$. Diremos que o par $\langle \lambda, L^n \rangle$ é um L -bloco de α ou simplesmente um bloco de α de comprimento n se e somente se são cumpridas as três seguintes afirmações :

1. λL^n é segmento à esquerda de α ,
2. λL^{n+1} não é segmento à esquerda de α ,
3. L não é segmento à direita de λ .

Intuitivamente podemos estender estas definições para palavras de grupo. Veja o seguinte

Exemplo 1.13 : Seja $\alpha = AB^2AC^3A^2B^2 \in \Sigma^+$. Vemos aqui que AB^2 é segmento simultaneamente à esquerda e à direita de α , pois podemos escrever $\alpha = AB^2AC^3AAB^2$. Temos também que $\langle \phi, A \rangle$, $\langle AB^2, A \rangle$ e $\langle AB^2AC^3, A^2 \rangle$ são A -blocos de comprimentos um, um e dois respectivamente, enquanto $\langle A, B^2 \rangle$ e $\langle AB^2AC^3A^2, B^2 \rangle$ são B -blocos de comprimento dois e $\langle AB^2A, C^3 \rangle$ é o único C -bloco, e é de comprimento três.

Seja agora $\beta = B^3A^{-2}B^{-1}A^5C^{-3}B^2$. Notemos aqui que B^3A^{-1} e B^3A^{-2} são segmentos à esquerda de β , enquanto que

B^2 é segmento simultaneamente à esquerda e à direita de β .
 Claramente estes são apenas alguns dos muitos segmentos de β que poderíamos citar, entre eles, $B^{-1}A^5$, $B^{-1}A^2$, A^5C^{-3} , C^{-2} , A^2C^{-2} , $AC^{-3}B$, etc... Os seis distintos blocos de β são $\langle \phi, B^3 \rangle$, $\langle B^3, A^{-2} \rangle$, $\langle B^3A^{-2}, B^{-1} \rangle$, $\langle B^3A^{-2}B^{-1}, A^5 \rangle$, $\langle B^3A^{-2}B^{-1}A^5, C^{-3} \rangle$ e $\langle B^3A^{-2}B^{-1}A^5C^{-3}, B^2 \rangle$, respectivamente de comprimentos *três*, *dois*, *um*, *cinco*, *três* e *dois*.

Seja $\alpha \in \Sigma^+$ soletrada na seguinte forma,
 $\alpha = L_0^{n(0)} L_1^{n(1)} L_2^{n(2)} \dots L_p^{n(p)}$, para algum $\{L_0, L_1, L_2, \dots, L_p\} \subseteq \Sigma$
 e algum $\{n(i) : i \in \underline{p+1}\} \subseteq \mathbb{Z}-1$. A quantidade de letras $L \in \Sigma$ na palavra α será denotada por $q(L, \alpha)$, significando $\sum_{k \in I} n(k)$ onde $I = \{k : L_k = L\}$ e o comprimento de α será denotado por $|\alpha|$ e significa $\sum_{k=0}^p |n(k)|$. Por $mdc(\alpha)$ denotaremos $mdc\{q(L_i, \alpha) : i \in \underline{p+1}\}$ sempre que $q(L_i, \alpha) \neq 0$ para algum $i \in \underline{p+1}$. Nem sempre é definido $mdc(\alpha)$. Exemplo : Se α é a palavra $ABA^{-1}B^{-1}$ então $q(A, \alpha) = 0 = q(B, \alpha)$, e não se define $mdc(\alpha)$, neste caso.

Diremos que α é *trivial* se e somente se $mdc(\alpha) = 1$. Observe que α é trivial se existe $L \in \Sigma$ tal que $|q(L, \alpha)| = 1$.

Uma palavra α é dita *vulnerável* se e somente se existe $k \in \underline{p+1}$ tal que $mdc(\alpha) \neq mdc\{q(L_i, \alpha) : k \neq i \in \underline{p+1}\}$ sempre que estes dois mdc são definidos.

Nós identificamos duas palavras α e β de Σ^+ como $\alpha = \beta$ não somente quando possuem a mesma soletração, mas também quando $\alpha = \mu\lambda$ enquanto que $\beta = \mu\gamma\gamma^{-1}\lambda$ para algum $\{\mu, \gamma, \lambda\} \subseteq \Sigma^+$.

Designaremos por *redução* de α , a palavra mais curta β tal que $\alpha = \beta$. Quando α é igualmente soletrada à sua redução, dizemos que α é *reduzida*. O número de blocos da redução de α é denotado por $cplx(\alpha)$ e será denominado de *complexidade* de α . Claramente $|\alpha\beta| \leq |\alpha| + |\beta|$ e $cplx(\alpha\beta) \leq cplx(\alpha) + cplx(\beta)$ sempre que $\{\alpha, \beta\} \subseteq \Sigma^+$. Quando $\{\alpha, \beta\} \subseteq \Sigma^+$, então vale a igualdade nas expressões acima.

Quando $\{\alpha, \beta\} \subseteq \Sigma^+$, diremos que α é *ciclicamente conjugada* a β e anotamos $\alpha \sim \beta$ se e somente se $\alpha = \mu\lambda$ enquanto que $\beta = \lambda\mu$ para algum $\{\mu, \lambda\} \subseteq \Sigma^+$. Facilmente se vê que $\sim$ é uma relação de equivalência de Σ^+ . O conjunto $\{\beta : \beta \sim \alpha\}$ das palavras ciclicamente conjugadas a α será denotado por $\alpha/\sim$.

Diremos que a palavra $\beta \neq \phi$ é *raiz* da palavra $\alpha \in \Sigma^+$ quando $\alpha = \beta^n$ para algum inteiro positivo n . A raiz mais curta de α será denotada por $\pi(\alpha)$. Uma palavra α é dita *primitiva* se e somente se $\pi(\alpha) = \alpha$.

Lema 1.14 : Seja $\alpha \in \{A, B\}^+$ primitiva e de complexidade $2i+1 > 1$. Então existe $\beta \in \{A, B\}^+$ primitiva e ciclicamente conjugada a α tal que $cplx(\beta) \in \{2i, 2i-1\}$.

Demonstração : Claramente podemos escrever $\alpha = A^{n(0)}B^{n(1)} \dots B^{n(2i-1)}A^{n(2i)}$ para algum conjunto $\{n(j) : j \in \underline{2i+1}\}$ de inteiros não nulos. Seja $\lambda = A^{n(2i)}$ e $\mu = A^{n(0)}B^{n(1)} \dots B^{n(2i-1)}$. Então $\beta = \lambda\mu = A^{n(2i)}A^{n(0)}B^{n(1)} \dots B^{n(2i-1)} = A^m B^{n(1)}A^{n(2)} \dots B^{n(2i-1)}$, onde $m = n(2i) + n(0)$. Desta forma, temos que $\alpha \sim \beta$ e além disso que

$cplx(\beta) = 2i$ quando $m \neq 0$, mas que $cplx(\beta) = 2i-1$ quando $m = 0$. Portanto, em qualquer caso, temos que $cplx(\beta) \in \{2i, 2i-1\}$. Agora, já que $v^{-1}u^nv = (v^{-1}uv)^{-1}$, por uma extensão óbvia de [10, pg. 196, remark (vii)], vemos que se α é primitiva, então β é primitiva, pois $\alpha \sim \beta$. |

Definição 1.15 : Um homomorfismo $\xi : \Sigma^+ \rightarrow \{A, B\}^+$ chama-se *simplificação* se e somente se $\xi[\Sigma] \subseteq \{A, B\} \cup \{\phi\}$. Quando além disso, a palavra $\xi(\alpha)$ for primitiva, então ambos ξ e $\xi(\alpha)$ chamam-se *simplificação primitiva de α* , sempre que $\alpha \in \Sigma^+$. Obviamente, se α não for primitiva, então não existe simplificação primitiva de α .

Walter Taylor, ao ver a demonstração do [14, theorem 7] onde aparece a frase "It obviously suffices to show that the theorem holds for $\alpha \in \{A, B\}^+$ " duvidou que foi óbvio esta suficiência. Assim nasceu a nossa seguinte

Pergunta 1.16 : Sendo α qualquer palavra primitiva, então existe simplificação primitiva de α ?

Achamos que esta pergunta fica ainda em aberto, mas o seguinte lema é uma resposta parcial, exigida para a nossa dissertação.

LEMA 1.17 : Seja $\alpha \in \Sigma^+$ primitiva e de complexidade menos que seis. Então α tem uma simplificação primitiva.

DEMONSTRAÇÃO : Obviamente podemos supor que $cplx(\alpha) > 3$. Se existem duas letras distintas X e Y tais que X compare-

ce em exatamente um bloco de α e tais que Y comparece em exatamente um bloco de α , então o homomorfismo gerado pela função $\Sigma \rightarrow \{A, B\} \cup \{\phi\}$ definida por $X \rightarrow A$, por $Y \rightarrow B$, e por $U \rightarrow \phi$ sempre que $U \in \Sigma - \{X, Y\}$, obviamente é uma simplificação primitiva de α . Se nenhuma letra comparece em menos que dois blocos de α , então já que α é de complexidade menos que seis, é claro que α é uma palavra primitiva num alfabeto de exatamente duas letras, e neste caso nada temos a demonstrar; portanto, podemos supor que existe exatamente uma letra L que comparece em somente um bloco de α ; neste caso temos que $\alpha \sim_L x_u a_v b_u c_v d$ para algum $\{x, a, b, c, d\} \subseteq \Sigma - L$ e algum $\{u, v\} \subseteq \Sigma - \{L\}$, com $u \neq v$. Para definirmos o homomorfismo gerado pela função $\Sigma \rightarrow \{A, B\} \cup \{\phi\}$, consideremos três casos.

Caso : $a+b+c+d \neq 0$. Com $L \rightarrow A$, com $u \rightarrow B$, e com $v \rightarrow B$, obviamente temos uma simplificação primitiva de α .

Caso : $a+c = 0 = b+d$. Com $L \rightarrow \phi$, com $u \rightarrow A$, e com $v \rightarrow B$, obviamente temos também uma simplificação primitiva de α .

Caso : $a+c \neq 0$. Com $L \rightarrow A$, com $u \rightarrow B$, e com $v \rightarrow \phi$, temos novamente uma simplificação primitiva de α . |

Definição 1.18 : Seja $W \subseteq \Sigma^+$ e seja $\{\alpha, \beta\} \subseteq \Sigma^+$. Escrevemos $\alpha.W.\beta$ para dizer que α é W -equivalente a β , ou seja que existe seqüência finita $\alpha = \mu_0, \mu_1, \dots, \mu_n = \beta$ tal que para cada $i \in \underline{n}$, uma das seguintes condições é satisfeita :

1. $\mu_i \sim \mu_{i+1}$.

2. existe $\lambda \in W$ tal que ou $\mu_{i+1} = \mu_i \lambda$ ou

$$\mu_i = \mu_{i+1} \lambda.$$

Dizemos então que a seqüência $\mu_0, \mu_1, \dots, \mu_n$ leva α para β , via W .

Em [14 , proposition 2] é observado que se $\omega_1 \subseteq \omega_2 \subseteq \Sigma^+$, então ω_1 e ω_2 são relações de equivalência de Σ^+ . Além disso, temos que $\sim = \phi \subseteq \omega_1 \subseteq \omega_2 \subseteq \Sigma^+ = \Sigma^+ \times \Sigma^+$. Obviamente tal observação é válida também para palavras de grupo.

Definimos também $\alpha/W = \{ \beta : \alpha \cdot \omega \cdot \beta \}$.

Definição 1.19 : Seja $\alpha \in \Sigma^+$, seja G um semigrupo e seja $x \in G$. Diremos que α representa x em G , e anotamos $(\alpha \vdash x)G$, se e somente se existe um homomorfismo $H : \Sigma^+ \rightarrow G$ tal que $H(\alpha) = x$. Quando $(\alpha \vdash x)G$ para todo $x \in G$, diremos que α é universal para G , e anotamos $\alpha \vdash G$.

Seja M uma família de semigrupos. Diremos que α é M -universal se e somente se $\alpha \vdash G$ para todo $G \in M$. Além disso se α é universal para todo elemento finito em M , diremos que α é FM-universal ; e se α é universal para todo elemento infinito em M , diremos que α é IM-universal .

Em [3 , proposition 1] temos que cada palavra trivial é universal para todo grupo. Portanto o estudo da universalidade para grupos fica interessante somente para palavras não triviais .

O seguinte lema é uma generalização natural de [15 , corolário 3.11] .

Lema 1.20 : Seja $\alpha \in \Sigma^+$, seja $\omega \subseteq \Sigma^+$ e seja $\phi \in S_X$ para algum conjunto X . Se existe homomorfismo $H : \Sigma^+ \rightarrow S_X$ tal que $H(\alpha) = \phi$ enquanto que $H(\mu) = id \upharpoonright X$ para cada $\mu \in \omega$,

então temos que $(\beta + \delta)S_\chi$ para cada $\beta \in \alpha/W$.

Demonstração : [15 , lema 3.8 e lema 3.9] .

Apresentamos no Apêndice, a Tabela 4.7 , onde aparece um índice dos símbolos usados e das expressões técnicas cujas origens estão na presente dissertação.

Capítulo II :

HISTÓRICO

Já antes de 1965, Jan Mycielski introduziu as noções de *termos universais* com a seguinte

Pergunta 2.1 : Que palavras são universais para quais monoides X^* ?

A partir daí, uma seqüência de trabalhos publicados por Isbell [6] em 1966 ; McNulty [7] em 1972 e Silberger [11] em 1973 , culminaram em 1974 com a demonstração feita por McNulty e Silberger da seguinte generalização de um teorema de Isbell :

Teorema 2.2 : "Sejam X infinito e $J \subseteq \Sigma^+ - \{\emptyset\}$ tal que para $\{\alpha, \beta\} \subseteq J$ com $\alpha \neq \beta$ acontece que, nem α é segmento de β , nem existe $\mu \neq \emptyset$ tal que μ é , ao mesmo tempo, segmento à direita de α e segmento à esquerda de β . Seja $H : J \rightarrow \text{Prt}(X)$ função arbitrária. Então existe homomorfismo $K : \Sigma^+ \rightarrow \text{Prt}(X)$ tal que $K \upharpoonright J = H$." [15 , teorema 2.5] .

Em [12] , Silberger apresenta seu central

Teorema 2.3 : Seja $\alpha \in \Sigma^+$. Então α é Prt -universal se e somente se $(\alpha \upharpoonright f) \text{Prt}(Mnd(f))$ para toda função f conexa e injetiva.

Os principais corolários do Teorema 2.3 são os seguintes corolários 2.4 até 2.7 .

Corolário 2.4 : As palavras $(AB)^n A$, $B(BA)^n$ e $(BA)^n A$ são Prt -universais sempre que $n \in \omega$.

Corolário 2.5 : As palavras $A^3 B^2$ e $A^2 B^3$ são Prt -universais .

Corolário 2.6 : $A^x B^y$ é Prt -universal sempre que x e y são inteiros ímpares positivos .

O seguinte é uma resposta a uma pergunta de Isbell.

Corolário 2.7 : As palavras $AB^{n+1}AB^n$ e $A^n BA^{n+1}B$ são Prt -universais sempre que $1 \leq n \in \omega$.

Em 1977 , Ehrenfeucht e Silberger [4] estenderam um resultado dos principais de Isbell [6] , estabelecendo o

Teorema 2.8 : Seja n um inteiro positivo cujo menor fator primo ímpar é p e suponha que $2^k | n$ mas $2^{k+1} \nmid n$. Então as seguintes duas afirmações são equivalentes :

1. $2^{k+1} < p$,
2. Para todo conjunto X finito e para toda função $f \in {}^X X$, existe $g \in {}^X X$ e uma involução h tal que $f = g^n h$.

Relacionados com o Teorema 2.8 , temos os resultados principais de [5] :

Teorema 2.9 : Seja $\{m, n\} \subseteq \omega - \underline{3}$. Então as seguintes três afirmações são equivalentes :

1. $M(S(m)) \uparrow n$ e $M(S(n)) \uparrow m$,

2. $A^m B^n$ é Myc-universal ,
3. $A^m B^n$ é FSym-universal .

Corolário 2.10 : "Seja $n > 1$. Sejam $L_1, L_2, \dots, L_n$ letras distintas. Seja $n(j) > 1$ para todo j . Seja α a palavra de comprimento $\sum_{i=1}^n n(i)$, denotada por $\alpha = L_1^{n(1)} L_2^{n(2)} L_3^{n(3)} \dots L_n^{n(n)}$. Então as seguintes três afirmações são equivalentes :

1. Existem íteiros i e j tais que $1 \leq i < j \leq n$ e tais que $M(S(n(i))) \uparrow n(j)$ e $M(S(n(j))) \uparrow n(i)$,
2. α é Myc-universal ,
3. α é FSym-universal ." [15 , corolário 2.9]

Um resultado importante aparece no artigo [3] de Ehrenfeucht , Fajtlowicz , Malitz e Mycielski , que é o

Teorema 2.11 : Seja $\alpha \in \Sigma^+$. Suponha que $\alpha \uparrow\uparrow S_X$ para algum conjunto infinito X . Então também $\alpha \uparrow\uparrow S_Y$ para todo Y tal que $|Y| \geq \aleph_1$.

Em [3] também é visto que $A^2 B^2$ é ISym-universal . Tendo-se em conta que $A^2 B^2$ não é universal para S_2 , temos a

Proposição 2.12 : ISym-universalidade não implica na Sym-universalidade .

Sobre palavras de grupo, já em 1951 Ore mostrou em [9] e Bertram menciona em seu artigo [2] a seguinte

Proposição 2.13 : Cada elemento do semigrupo A_X é um comutador; isto é, se $\phi \in A_X$ para X finito qualquer, en-

tão $\delta = yxy^{-1}x^{-1}$ para algum $\{x,y\} \subseteq S_X$.

Mais recentemente Silberger exibiu permutações x e y formadas por componentes cíclicas infinitas em S_Z tais que $yxy^{-1}x^{-1} = c_{2k}$ sempre que $k \in \omega-1$. Veja o Diagrama 4.1a do Apêndice.

Em [15], Valente estabeleceu o

Teorema 2.14 : Seja $\{m(i), n(i)\} \subseteq \omega-1$ para todo $i \in \{1, 2, \dots, k-1\}$. Seja $m(k) > 0 \leq n(k)$ e seja a palavra $\alpha = A^{m(1)}B^{n(1)}A^{m(2)}B^{n(2)} \dots A^{m(k)}B^{n(k)}$ com exatamente um $m(i)$ ímpar e exatamente um $n(j)$ ímpar. Então α é *Sym*-universal.

Bem recentemente, Silberger e Valente em [14], demonstraram o seguinte

Teorema 2.15 : Seja α uma palavra de semigrupo, primitiva e de complexidade menos que seis. Então $(\alpha + \delta)S_Z$.

A extensão do Teorema 2.15 para palavras de grupo é a nossa principal contribuição na presente dissertação. Veja o nosso Capítulo III.

Em 1981, Arante em [1] comentou com exemplos, a representação de δ para palavras de semigrupo, conforme o Teorema 2.15; além de estabelecer os seguintes teoremas:

Teorema 2.16 : A palavra $A^m B^n$ é *ISym*-universal, sempre que $\{m, n\} \subseteq \omega-1$.

Teorema 2.17 : Seja $\alpha = A^{m(1)} B^{n(1)} A^{m(2)} B^{n(2)} A^{m(3)} B^{n(3)}$ com $\{m(i), n(i)\} \subseteq \omega - 1$ sempre que $i \in \{1, 2, 3\}$, e tal que $m(3)$ não seja múltiplo de $(m(1), m(2))$. Então $(\alpha + \delta) S_Z$.

Teorema 2.18 : Se α é palavra vulnerável de semi-grupo então $(\alpha + \delta) S_Z$.

Arante também observou que as palavras $A^3 B^2 A^2 BAB$ e $A^3 B A^2 B^2 AB$ são as mais curtas conhecidas palavras de semi-grupo que ainda não está estabelecida a sua capacidade em relação à representatividade de δ em S_Z .

Os autores mencionados neste capítulo costumam perguntar; algumas vezes mais geralmente que outras :

Pergunta 2.19 : Se $\alpha \in \{A^3 B^2 A^2 BAB, A^3 B A^2 B^2 AB, (A^2 B^2)^2 A^2 B^4\}$ então $(\alpha + \delta) S_Z$?

Pergunta 2.20 : Se $\phi \neq \alpha \in \Sigma^+$ não é da forma $\alpha = \beta \gamma \beta$ para $\beta \neq \phi$, então α é ISym-universal ?

Pergunta 2.21 : Se $\pi(\alpha) = A^m B^n A^p B^q$ então $\pi(\alpha)$ é ISym-universal ?

Pergunta 2.22 : $\pi(\alpha)$ é ISym-universal ?

Pergunta 2.23 : Toda palavra de grupo, primitiva é Sym-universal ?

Capítulo III :

$A^m B^n A^p B^q$ REPRESENTA δ SE E SOMENTE SE
 $m \neq p$ OU $n \neq q$

Nosso principal teorema deste capítulo é o seu título. Nós o estabeleceremos em duas partes. Estamos supondo sempre que $0 \notin \{m, n, p, q\} \subseteq \mathbb{Z}$, e que $\langle m, n \rangle \neq \langle p, q \rangle$.

Na primeira parte, trata-se do caso em que $m+p \neq 0 \neq n+q$, e termina no TEOREMA 3.6, que é uma generalização natural do principal teorema de [14], cujo resultado estendemos para palavras de grupo.

Na segunda parte, trata-se do caso em que $m+p = 0$ ou que $n+q = 0$. O seu ponto culminante é o TEOREMA 3.8, nossa principal contribuição.

Definição 3.1 : Seja h uma permutação de $\mathbb{Z}$. Diremos que h é *intercalável* se e somente se $C_{\mathbb{Z}}(h; k)$ é ou vazio ou infinito sempre que $1 < k$.

Lema 3.2 : Seja h um elemento intercalável de $S_{\mathbb{Z}}$, com $C_{\mathbb{Z}}(h) = C_{\mathbb{Z}}(h; k)$ para algum $k > 1$. Seja $0 \neq p \in \mathbb{Z}$. Então existe elemento intercalável a de $S_{\mathbb{Z}}$ tal que $a^p = h$.

Demonstração : Inicialmente suporemos $p > 0$. Sem perder a generalidade, podemos supor que $C_{\mathbb{Z}}(h) = \{h_i : i \in \omega\}$ onde $h_i = (ki \ ki+1 \ \dots \ ki+k-1)$. Agora, para cada $j \in \omega$, seja $H_j = h_{pj} \ h_{pj+1} \ \dots \ h_{pj+p-1}$. Observe que $h = \prod_{i=0}^{\infty} h_i = \prod_{j=0}^{\infty} H_j$. Seja agora, para cada $j \in \omega$, o pk -ciclo

$a_j = (pjk \ pjk+k \ pjk+2k \ \dots \ pjk+pk-k \ pjk+1 \ pjk+k+1 \ pjk+2k+1$
 $\dots \ pjk+pk-k+1 \ \dots \ \dots \ pjk+k-1 \ pjk+2k-1 \ \dots \ pjk+pk-1)$.
 Com isto, temos que $a_j^p = H_j$. Mas o conjunto $\{a_j : j \in \omega\}$ é
 dep. Assim podemos definir a permutação intercalável a de Z
 por $C_Z(a) = \{a_j : j \in \omega\}$. É claro que $a^p = \prod_{j=0}^{\infty} a_j^p = \prod_{j=0}^{\infty} H_j = h$.
 O caso em que $k = \aleph_0$ se faz analogamente.

Finalmente, suporemos $p < 0$. Seja $-p = m > 0$. Então
 existe elemento intercalável b de S_Z tal que $b^m = h$. Seja
 $a = b^{-1}$. Assim, $a^p = b^{-p} = b^m = h$.

Em casos particulares, podemos construir a permutação
 intercalável a de Z de outras maneiras mais convenientes :

Nota 3.2.1 : Seja $(k, p) = 1$. Então pelo Lema 1.9 ,
 temos que existe permutação a_i de Z tal que $a_i^p = h_i$, já
 que $\|h_i\| = k$. Seja $a = \prod_{i=0}^{\infty} a_i$. Assim $a^p = \prod_{i=0}^{\infty} a_i^p = \prod_{i=0}^{\infty} h_i = h$.

Nota 3.2.2 : Lembrando que c_x^p tem exatamente (p, x)
 componentes cíclicas de comprimento $x/(p, x)$, podemos construir
 a permutação intercalável a de Z com x -ciclos no lugar de
 $|pk|$ -ciclos, quando h for convenientemente composta por compo-
 nentes cíclicas de comprimento $k = x/(p, x)$. Apresentamos no
 Apêndice, o Diagrama 4.2, ilustrando um exemplo, com $k = 3$,
 $p = -8$ e $x = 12$.

Corolário 3.3 : Se h é permutação intercalável de Z
 então existe $a \in S_Z$ tal que $a^p = h$ sempre que $0 \neq p \in Z$.

Demonstração : Seja $h = \prod_{k=2}^{\infty} h_k$, onde para cada $k > 1$
 tal que $C_Z(h; k) = \emptyset$, consideremos $h_k = id \upharpoonright Z$, e para cada

$k > 1$ tal que $C_Z(h; k) \neq \emptyset$, consideremos h_k com $C_Z(h_k) = C_Z(h; k)$, que é infinito, pois h é intercalável. Assim, pelo Lema 3.2, temos para cada $k > 1$, que existe $a_k \in S_Z$ tal que $a_k^p = h_k$ e tal que $\{a_k : k > 1\}$ é dcp. Definindo $a = \prod_{k=2}^{\infty} a_k$, temos que $a^p = \prod_{k=2}^{\infty} a_k^p = h$. ■

O resultado seguinte é um caso particular de [14, lema 4]. A idéia da nossa demonstração dele aparece no Diagrama 4.3 do Apêndice.

Lema 3.4 : Seja $\{t, u\} \subseteq \omega - 2$. Então existem permutações intercaláveis F e G de Z com $C_Z(F) = C_Z(F; t)$ e com $C_Z(G) = C_Z(G; u)$ tais que $s = GF$.

Demonstração : Seja $T = t + u - 3$. Observemos que $T \geq 2 + 2 - 3 = 1$. Para cada $k \in \omega$, seja F_k o t -ciclo $(kT \ kT+1 \ \dots \ kT+t-2 \ -k-1)$ em Z , e seja G_k o u -ciclo $(kT+t-1 \ kT+t \ \dots \ kT+T \ -k-1)$ em Z . Observemos que ambos os conjuntos $\{F_k : k \in \omega\}$ e $\{G_k : k \in \omega\}$ são dcp. Portanto as permutações F e G de Z podem ser e serão definidas por $C_Z(F) = \{F_k : k \in \omega\}$ e por $C_Z(G) = \{G_k : k \in \omega\}$. É óbvio que F e G são intercaláveis. Afirmamos que $s = GF$. A fim de estabelecer isto, escolhemos $x \in Z$. Há três casos a considerar.

Caso : $x < -1$. Então existe inteiro $k > 0$ tal que $x = -k-1$. Segue que $F(x) = F(-k-1) = F_k(-k-1) = kT$ e também que $G(kT) = G((k-1)T+T) = G_{k-1}((k-1)T+T) = -(k-1)-1 = -k = x+1$.

Caso : $x = -1$. Então $F(x) = F_0(-1) = 0$. É claro que $0 \notin 2G$, e portanto que $G(0) = 0 = -1+1 = x+1$.

Caso : $x > -1$. Então, pelo algoritmo da divisão de Euclides, existe $\langle k, y \rangle \in \omega \times \mathbb{I}$ tal que $x = kT + y$. Há três sub-ca-

sos a considerar agora.

Sub-caso : $0 \leq y \leq t-3$. Então $F(x) = F(kT+y) = F_k(kT+y)$
 $= kT+y+1$. Observe agora, da definição dos u -ciclos G_k em Z
 que para todo $v \in \omega$ temos que $v \in ZG$ se e somente se
 $(v)_t \in \{t-1, t, \dots, T-1, T, 0\}$. Mas já que $1 \leq y+1 \leq t-2$, temos que
 $y+1 \notin \{t-1, t, \dots, T-1, T, 0\}$. Segue que $kT+y+1 \notin ZG$. Inferimos
 portanto que $G(kT+y+1) = kT+y+1 = x+1$.

Sub-caso : $y = t-2$. Então $F(x) = F(kT+y) =$
 $F_k(kT+t-2) = -k-1$, e também $G(-k-1) = G_k(-k-1) = kT+t-1 = x+1$.

Sub-caso : $t-1 \leq y \leq T-1$. Observamos agora que para todo
 $v \in \omega$, temos que $v \in ZF$ se e somente se $(v)_t \in \underline{t-1}$. Mas já que
 $t-1 \leq y \leq T-1$, temos que $y \notin \underline{t-1}$. Segue que $kT+y \notin ZF$ e então
 que $GF(x) = GF(kT+y) = G(kT+y) = G_k(kT+y) = kT+y+1 = x+1$.

Em todos os casos e sub-casos, vimos que
 $GF(x) = x+1 = \delta(x)$.

A demonstração do seguinte resultado é fundamentalmen-
 te baseada na demonstração apresentada em [14 , teorema 6]
 para semigrupo .

Corolário 3.5 : Sejam m, n, x e y inteiros não nulos
 com $x > |m|$ e com $y > |n|$. Então existem elementos intercaláveis
 δ e g de S_Z com $\text{ord}(\delta) = x$, com $\text{ord}(g) = y$ e tais que
 $\delta = g^n \delta^m$.

Demonstração : Notemos que ambos os inteiros
 $t = |x/(m, x)|$ e $u = |y/(n, y)|$ são maiores que 1 . Portanto,
 pelo Lema 3.4 , temos que existem permutações intercaláveis F
 e G de Z tais que $C_Z(F) = C_Z(F; t)$, que $C_Z(G) = C_Z(G; u)$
 e que $\delta = GF$. Com base na Nota 3.2.2 , intecalemos conveni-

entamente t -ciclos de F em Z , agrupados de (m, x) em (m, x) , para obter a permutação intercalável δ de Z tal que $\delta^m = F$. Claramente $C_Z(\delta) = C_Z(\delta; x)$, e portanto $\text{ord}(\delta) = x = |x/(m, x)|(m, x)$. Analogamente, agrupemos os u -ciclos de G em Z de (n, y) em (n, y) para intercalá-los convenientemente e obter $g \in S_Z$ tal que $g^n = G$ e tal que $\text{ord}(g) = y = |y/(n, y)|(n, y)$. Assim, já temos δ e g , elementos intercaláveis de S_Z tais que $\text{ord}(\delta) = x$, que $\text{ord}(g) = y$ e tais que $s = GF = g^n \delta^m$. ■

TEOREMA 3.6 : Sejam m, n, p e q inteiros com $m+p \neq 0 \neq n+q$ e com $m \neq p$ ou $n \neq q$. Então a palavra $\alpha = A^m B^n A^p B^q$ representa a permutação cíclica s de Z em S_Z .

Demonstração : O Corolário 3.5 nos garante que $A^i B^j$ claramente representa s em S_Z sempre que $\{i, j\} \subseteq Z-1$. Então podemos supor que m, n, p e q são inteiros não nulos. Já que claramente $|p| \neq |m|$ ou $|q| \neq |n|$, então pelo Lema 1.20 podemos supor sem perder a generalidade que $|q| > |n| > 0$. Seja, desta forma $W = \{B^q\}$. Então $\alpha.W.A^{m+p}B^n$. Pelo Corolário 3.5 temos que existem permutações δ e g de Z com $\text{ord}(\delta) = |q| > |n|$, com $\text{ord}(g) = |m+p|+1 > |m+p|$ e tais que $s = g^{m+p} \delta^n$. Já que $\text{ord}(g) = |q|$ implica que $\delta^q = \text{id}_Z$, segue pelo Lema 1.20 que $(\alpha s) S_Z$. ■

O TEOREMA 3.6 nos diz que toda palavra $\alpha = A^m B^n A^p B^q$ primitiva e de complexidade quatro representa s em S_Z sempre que $m+p \neq 0 \neq n+q$. Veremos no TEOREMA 3.8 que também a palavra $A^k B^m A^{-k} B^n$ representa s em S_Z , sempre que $\{m, n, k\} \subseteq Z-1$. Com isto teremos então que toda palavra pri-

mitiva de complexidade quatro no alfabeto de duas letras representa δ em S_Z . Para estabelecer o TEOREMA 3.8, veremos inicialmente o seu lema, que é o fundamental deste capítulo.

LEMA 3.7 : Sejam

1. $4 < t \in \omega$,
2. $c_0, c_1, \dots$ e $d_0, d_1, \dots$ duas seqüências infinitas e injetivas de inteiros,
3. $\delta_0, \delta_1, \dots$ e $g_0, g_1, \dots$ duas seqüências infinitas e injetivas de t -ciclos em Z , e
4. $p < t$ e $q < t$ dois inteiros positivos tais que
5. $\{c_i : i \in \omega\} \cap \{d_i : i \in \omega\} = \emptyset$,
6. ambos os conjuntos $\{\delta_i : i \in \omega\}$ e $\{g_i : i \in \omega\}$ são dcp,

7. $Z\delta_j \cap Zg_j = \{c_j\}$ para cada $j \in \omega$,
8. $Z\delta_{j+1} \cap Zg_j = \{d_j\}$ para cada $j \in \omega$,
9. $Z\delta_i \cap Zg_j = \emptyset$ sempre que $j \in \omega$ e que $i \in \omega - \{j, j+1\}$, e

10. $\delta_{i+1}^p(c_{i+1}) = d_i = g_i^q(c_i)$ para cada $i \in \omega$.

Sejam δ e g as permutações de Z definidas por $C_Z(\delta) = \{\delta_i : i \in \omega\}$ e por $C_Z(g) = \{g_i : i \in \omega\}$. Então existe permutação intercalável h de Z tal que $g = h\delta h^{-1}$.

PLANO DA DEMONSTRAÇÃO : Definimos o conjunto

11. $\mathcal{D} = \underline{t} - \{0, p, t-q, (p-q)\}$.

Já que $t > 4$, temos que $\mathcal{D} \neq \emptyset$. Portanto podemos escolher $e \in \mathcal{D}$. Assim, para cada $i \in \omega$, definimos

12. $a_i = \delta^e(c_i)$,
13. $b_i = g^{-e}(c_i)$,

$$14. x_i = f^{q+e}(c_i) \text{ e}$$

$$15. y_i = g^{p-e}(c_{i+1}) .$$

Definimos também os conjuntos

$$16. E = \underline{x} - \{0, e, p, (q+e)_k\} ,$$

$$17. X_i = \{a_i, b_i, c_i, d_i, x_i, y_i\} \text{ para cada } i \in \omega , \text{ e}$$

$$18. V_i = \{f^h(c_i) : h \in E\} \cup \{g^h(b_i) : h \in E\} \text{ para cada } i \in \omega .$$

Demonstraremos depois as seguintes seis afirmações :

$$19. |X_i| = 6 \text{ para cada } i \in \omega ,$$

$$20. X_i \cap X_j = \emptyset \text{ sempre que } \{i, j\} \subseteq \omega \text{ com } i \neq j ,$$

$$21. |\{f^p(c_0), g^p(b_0)\} \cup V_i| = 2+2|E| \text{ para cada } i \in \omega ,$$

$$22. V_i \cap V_j = \emptyset \text{ sempre que } \{i, j\} \subseteq \omega , \text{ com } i \neq j ,$$

$$23. V_i \cap X_j = \emptyset \text{ sempre que } \{i, j\} \subseteq \omega , \text{ e}$$

$$24. \{f^p(c_0), g^p(b_0)\} \cap X_i = \emptyset \text{ sempre que } i \in \omega .$$

Uma vez demonstradas estas afirmações, mostraremos como podemos definir a permutação h de Z por

$$C_Z(h) = C_Z(h;3) \cup C_Z(h;2) = Y \cup V, \text{ onde}$$

$$Y = \{(a_i \ c_i \ b_i) : i \in \omega\} \cup \{(x_i \ d_i \ y_i) : i \in \omega\} \text{ e onde}$$

$$V = \{(f^h(c_i) \ g^h(b_i)) : \langle h, i \rangle \in E \times \omega\} \cup \{(f^p(c_0) \ g^p(b_0))\} ,$$

pois veremos que o conjunto $Y \cup V$ é dcp .

Como $t > 4$, veremos que $E \neq \emptyset$ e portanto que $C_Z(h;2)$ é infinito. Veremos também que claramente $C_Z(h;3)$ é infinito, e então que h é intercalável.

Finalmente afirmamos que

$$25. g = h f h^{-1} .$$

Deste modo, a demonstração do LEMA 3.7 acabará, depois que ficarem provadas as afirmações de 3.7.19 a 3.7.25 , baseadas nas hipóteses de 3.7.1 a 3.7.10 , nas definições de 3.7.11 a 3.7.18 e ainda na definição de $C_Z(h)$ para estabelecer a última afirmação 3.7.25 .

Apresentamos, no Apêndice, o Diagrama 4.4 , que ilustra tais funções ϕ , g e h .

DEMONSTRAÇÃO de 3.7 :

Demonstração de 3.7.19 : Escolhemos arbitrariamente $i \in \omega$. Por 3.7.10 temos que $d_i = g^q(c_i)$, e por 3.7.13 temos que $c_i = g^e(b_i)$. Segue que $d_i = g^{q+e}(b_i)$.

Por 3.7.4 temos que $0 < q < t$. Já que $e \in \mathcal{D}$, temos que $0 < e < t$. Segue que $0 < q+e < 2t$. Mas $e \in \mathcal{D}$ implica também que $e \neq t-q$; assim temos que $q+e \neq t$. Os fatos $q+e \neq t$ e $0 < q+e < 2t$ garantem que $t \nmid q+e$. Portanto podemos concluir que $c_i \neq d_i$, já que $0 < q < t$ e que $d_i = g^q(c_i)$; que $c_i \neq b_i$, já que $0 < e < t$ e que $c_i = g^e(b_i)$; e que $d_i \neq b_i$, já que $t \nmid q+e$ e que $d_i = g^{q+e}(b_i)$. Em resumo, $|\{b_i, c_i, d_i\}| = 3$.

Já que, por 3.7.7 e 3.7.8 e 3.7.12 a 3.7.14 temos que $\{a_i, c_i, x_i\} \times \{d_i, b_i\} \subseteq Z\phi_i \times Zg_i$, e que $c_i \notin \{b_i, d_i\}$ pois $|\{b_i, c_i, d_i\}| = 3$, segue agora por 3.7.7 que $\{a_i, c_i, x_i\} \cap \{b_i, d_i\} = \emptyset$.

Argumentaremos agora, num esboço análogo aos parágrafos anteriores. Por 3.7.14 temos que $x_i = \phi^{q+e}(c_i)$. Por 3.7.12 temos que $c_i = \phi^{-e}(a_i)$. Portanto temos que $x_i = \phi^q(a_i)$. Daí é fácil ver que $x_i \neq c_i$, já que $t \nmid q+e$; que $c_i \neq a_i$, já que $0 < e < t$; e que $x_i \neq a_i$, já que $0 < q < t$. Inferimos que $|\{a_i, c_i, x_i\}| = 3$. Portanto $|\{a_i, c_i, x_i, b_i, d_i\}| = 5$, já que $\{a_i, c_i, x_i\} \cap \{b_i, d_i\} = \emptyset$ e que $|\{b_i, d_i\}| = 2$. Para acabar a demonstração de 3.7.19 , bas-

ta mostrar que $y_i \notin \{a_i, c_i, x_i, b_i, d_i\}$.

Por 3.7.6 temos que $Zg_{i+1} \cap Zg_i = \phi$. Por 3.7.9 temos que $Z\delta_i \cap Zg_{i+1} = \phi$. Mas por 3.7.7 e 3.7.15 temos que $y_i \in Zg_{i+1}$. Também temos que $\{a_i, b_i, c_i, d_i, x_i\} \subseteq Z\delta_i \cup Zg_i$, pois $\{a_i, c_i, x_i\} \times \{b_i, d_i\} \subseteq Z\delta_i \times Zg_i$. Portanto temos que $\{y_i\} \cap \{a_i, b_i, c_i, d_i, x_i\} \subseteq Zg_{i+1} \cap (Zg_i \cup Z\delta_i) = (Zg_{i+1} \cap Zg_i) \cup (Zg_{i+1} \cap Z\delta_i) = \phi \cup \phi = \phi$. A afirmação 3.7.19 fica provada.

Demonstração de 3.7.20 : Escolhemos i e j inteiros não negativos com $i \neq j$. Já vimos que $\{a_v, b_v, c_v, d_v, x_v\} \subseteq Z\delta_v \cup Zg_v$ para cada $v \in \omega$. Assim temos que $\{a_i, b_i, c_i, d_i, x_i\} \cap \{a_j, b_j, c_j, d_j, x_j\} \subseteq (Z\delta_i \cup Zg_i) \cap (Z\delta_j \cup Zg_j) = (Z\delta_i \cap Zg_j) \cup (Zg_i \cap Z\delta_j)$, pois por 3.7.6 temos que $Z\delta_i \cap Z\delta_j = \phi = Zg_i \cap Zg_j$. Sem perder a generalidade, podemos supor que $i < j$. Então por 3.7.2 e 3.7.5 e por 3.7.7 a 3.7.9, temos que $Z\delta_j \cap Zg_i = \{d_i\}$ se e somente se $j = i+1$. Segue que $\{a_i, b_i, c_i, d_i, x_i\} \cap \{a_j, b_j, c_j, d_j, x_j\} = \phi$ se $j \neq i+1$ mas que $\{a_i, b_i, c_i, d_i, x_i\} \cap \{a_{i+1}, b_{i+1}, c_{i+1}, d_{i+1}, x_{i+1}\} \subseteq \{d_i\}$.

Agora mostraremos que $d_i \notin \{a_{i+1}, b_{i+1}, c_{i+1}, d_{i+1}, x_{i+1}\}$.

Por 3.7.5 temos que $d_i \neq c_{i+1}$.

Por 3.7.10 temos que $d_i = \delta^p(c_{i+1})$ e por 3.7.12 temos que $c_{i+1} = \delta^{-e}(a_{i+1})$. Segue que $d_i = \delta^{p-e}(a_{i+1})$. Já que $\langle e, p \rangle \in \mathcal{D} \times (\mathcal{T} - \mathcal{D})$ temos que $0 < |e-p| < \mathcal{T}$, e assim que $\mathcal{T} \nmid p-e$. Segue agora que $d_i \neq a_{i+1}$.

Por 3.7.10 temos que $d_i = \delta^p(c_{i+1})$ e por 3.7.14 temos que $c_{i+1} = \delta^{-q-e}(x_{i+1})$. Segue que $d_i = \delta^{p-q-e}(x_{i+1})$. Já que $\langle e, (p-q)_t \rangle \in \mathcal{D} \times (\underline{t}-\mathcal{D})$ temos que $t \nmid (p-q)_t - e$. Mas obviamente $t \mid p-q-e$ se e somente se $t \mid (p-q)_t - e$. Segue que $t \nmid p-q-e$, e então que $d_i \neq x_{i+1}$.

Também por 3.7.7 e 3.7.13 temos que $b_{i+1} \in Zg_{i+1}$. Segue por 3.7.6 que $b_{i+1} \notin Zg_i$. Mas por 3.7.8 temos que $d_i \in Zg_i$. Segue que $d_i \neq b_{i+1}$.

Por 3.7.2 temos que $d_i \neq d_{i+1}$. Portanto pelos quatro parágrafos anteriores, inferimos como foi proposto, que $d_i \notin \{a_{i+1}, b_{i+1}, c_{i+1}, d_{i+1}, x_{i+1}\}$. Portanto, como já foi observado que $\{a_i, b_i, c_i, d_i, x_i\} \cap \{a_{i+1}, b_{i+1}, c_{i+1}, d_{i+1}, x_{i+1}\} \subseteq \{d_i\}$, concluímos que esta intersecção é vazia.

Agora temos em geral que $\{a_i, b_i, c_i, d_i, x_i\} \cap \{a_j, b_j, c_j, d_j, x_j\} = \emptyset$ pois $i \neq j$. Portanto para acabar a demonstração de 3.7.20, basta mostrar que $y_i \notin X_j$.

Notemos por 3.7.7 e 3.7.15 que $y_i \in Zg_{i+1}$. Lembremos também que $\{b_j, d_j\} \subseteq Zg_j$. Se $j \neq i+1$, então por 3.7.6 temos que $Zg_{i+1} \cap Zg_i = \emptyset$ e portanto que $y_i \neq b_j$. Mas por 3.7.15 e 3.7.13 temos que $y_i = g^{p-e}(c_{i+1}) = g^p(b_{i+1})$. Portanto, já que $0 < p < t$ segue que $y_i \neq b_{i+1}$. Em geral $y_i \neq b_j$.

Por 3.7.15 e 3.7.10 temos que $y_i = g^{p-e}(c_{i+1}) = g^{p-e-q}(d_{i+1})$. Lembrando que $t \nmid p-e-q$, inferimos que $y_i \neq d_{i+1}$. Por outro lado, para $j \neq i+1$, temos que $\langle y_i, d_j \rangle \in Zg_{i+1} \times Zg_j$,

e segue então por 3.7.6 que $y_i \neq d_j$. Em qualquer caso, temos que $y_i \neq d_j$.

Pelos dois parágrafos anteriores, temos que $y_i \notin \{b_j, d_j\}$.

Afirmamos que também $y_i \notin \{a_j, c_j, x_j\}$. Lembrando que $y_i \in Zg_{i+1}$, observamos que $\{y_i\} \cap \{a_j, c_j, x_j\} \subseteq Zg_{i+1} \cap Z\delta_j$ pois $\{a_j, c_j, x_j\} \subseteq Z\delta_j$. Há três casos a considerar.

Caso : $j = i+1$. Então $\{y_i\} \cap \{a_j, c_j, x_j\} \subseteq \{c_{i+1}\}$. Mas já que $y_i = g^{p-e}(c_{i+1})$ e que $x \nmid p-e$, inferimos que $y_i \neq c_{i+1}$. Portanto $y_i \notin \{a_j, c_j, x_j\}$ quando $j = i+1$.

Caso : $j = i+2$. Então $\{y_i\} \cap \{a_j, c_j, x_j\} \subseteq \{d_{i+1}\}$. Mas lembrando que $y_i \notin \{b_{i+1}, d_{i+1}\}$, inferimos que $y_i \neq d_{i+1}$. Portanto $y_i \notin \{a_j, c_j, x_j\}$ quando $j = i+2$.

Caso : $j \notin \{i+1, i+2\}$. Então $Zg_{i+1} \cap Z\delta_j = \emptyset$ e portanto $y_i \notin \{a_j, c_j, x_j\}$ também no caso final, quando $j \notin \{i+1, i+2\}$.

Recolhendo os fatos, temos agora que $y_i \notin \{b_j, d_j\} \cup \{a_j, c_j, x_j\}$. Para acabar nossa demonstração de 3.7.20, basta mostrar que $y_i \neq y_j$. Mas $\langle y_i, y_j \rangle \in Zg_{i+1} \times Zg_{j+1}$ e $Zg_{i+1} \cap Zg_{j+1} = \emptyset$, pois $i+1 \neq j+1$. A afirmação 3.7.20 fica provada.

Demonstração de 3.7.21 : Seja arbitrariamente $\langle u, v, i \rangle \in E^2 \times \omega$. Então por 3.7.7 temos que $\delta^u(c_i) \in Z\delta_i$, e por 3.7.13 temos que $g^v(b_i) \in Zg_i$. Portanto temos que $\{\delta^u(c_i)\} \cap \{g^v(b_i)\} \subseteq Z\delta_i \cap Zg_i = \{c_i\}$. Mas $\delta^u(c_i) \neq c_i$, já que $0 < u < t$. Assim temos que $\delta^u(c_i) \neq g^v(b_i)$. Em particular,

temos que $f^h(c_i) \neq g^h(b_i)$ sempre que $h \in E$.

Do parágrafo anterior inferimos que

$\{f^h(c_i) : h \in E\} \cap \{g^h(b_i) : h \in E\} = \emptyset$. Também, já que $E \subseteq \underline{x}$, que $c_i \in Zf_i$ e que f_i é componente x -cíclica de f em Z , é claro que $|\{f^h(c_i) : h \in E\}| = |E|$. Semelhantemente, temos que $|\{g^h(b_i) : h \in E\}| = |E|$, já que por 3.7.13 temos que $b_i \in Zg_i$, e que g_i é componente x -cíclica de g em Z . Segue que $|V_i| = 2|E|$.

Certamente $V_i = \{f^h(c_i) : h \in E\} \cup \{g^h(b_i) : h \in E\} = \cup\{\{f^h(c_i), g^h(b_i)\} : h \in E\}$. A segunda forma do conjunto é a mais informativa para os nossos fins.

Lembramos que $\langle f^p(c_0), g^p(b_0) \rangle \in Zf_0 \times Zg_0$ e que $Zf_0 \cap Zg_0 = \{c_0\}$. Mas, já que $0 < p < x$, segue que $f^p(c_0) \neq c_0$. Portanto $f^p(c_0) \neq g^p(b_0)$.

Para acabar a nossa demonstração de 3.7.21, falta ainda mostrar que $\{f^p(c_0), g^p(b_0)\} \cap V_i = \emptyset$.

Já vimos que $\langle f^p(c_0), f^u(c_i) \rangle \in Zf_0 \times Zf_i$, e que $Zf_0 \cap Zf_i = \emptyset$ sempre que $i \neq 0$. Mas já que $\langle u, p \rangle \in E \times (\underline{x} - E)$, temos que $f^p(c_0) \neq f^u(c_0)$. Portanto $f^p(c_0) \neq f^u(c_i)$ sempre que $i \in \omega$.

Semelhantemente, $\langle g^p(b_0), g^v(b_i) \rangle \in Zg_0 \times Zg_i$. Também se $i \neq 0$ então $Zg_0 \cap Zg_i = \emptyset$, e portanto $g^p(b_0) \neq g^v(b_i)$. Mas já que $\langle v, p \rangle \in E \times (\underline{x} - E)$, temos que $g^p(b_0) \neq g^v(b_0)$. Em resumo, $g^p(b_0) \neq g^v(b_i)$ sempre que $i \in \omega$.

Lembramos que $\langle f^p(c_0), g^v(b_i) \rangle \in Zf_0 \times Zg_i$ e que $Zf_0 \cap Zg_0 = \{c_0\}$. Assim, lembrando que $f^p(c_0) \neq c_0$, inferimos que $f^p(c_0) \neq g^v(b_0)$. Mas por 3.7.9 temos que $Zf_0 \cap Zg_i = \emptyset$ quando $i \neq 0$. Portanto, $f^p(c_0) \neq g^v(b_i)$ quando $i \neq 0$. Em geral, temos que $f^p(c_0) \notin \{g^v(b_k) : k \in \omega\}$.

Finalmente notemos que $\langle g^p(b_0), f^u(c_i) \rangle \in Zg_0 \times Zf_i$. Há três casos a considerar.

Caso : $i = 0$. Vimos que $f^u(c_0) \neq c_0$. Portanto, já que $\{g^p(b_0)\} \cap \{f^u(c_0)\} \subseteq Zg_0 \cap Zf_0 = \{c_0\}$, temos que $g^p(b_0) \neq f^u(c_i)$ no caso em que $i = 0$.

Caso : $i = 1$. Por 3.7.8 temos que $Zg_0 \cap Zf_i = \{d_0\}$. por 3.7.13 e 3.7.10 temos que $g^p(b_0) = g^{p-e}(c_0) = g^{p-e-q}(d_0)$. Mas como já foi visto que $i \nmid p-e-q$, inferimos que $g^p(b_0) \neq d_0$. Portanto $\{g^p(b_0)\} \cap \{f^u(c_i)\} \subseteq Zg_0 \cap Zf_i = \{d_0\}$ implica que $g^p(b_0) \neq f^u(c_i)$ no caso em que $i = 1$.

Caso : $i > 1$. Por 3.7.9 temos que $Zg_0 \cap Zf_i = \emptyset$. Portanto $\{g^p(b_0)\} \cap \{f^u(c_i)\} \subseteq \emptyset$, e concluimos que $g^p(b_0) \neq f^u(c_i)$ no caso também quando $i > 1$. Em resumo, temos que $g^p(b_0) \notin \{f^u(c_k) : k \in \omega\}$.

Juntando os fatos, concluimos que $\{f^p(c_0), g^p(b_0)\} \cap v_i = \emptyset$, já que $\langle u, v \rangle \in E^2$ foi arbitrariamente escolhido. Já que também $i \in \omega$ foi arbitrário, a afirmação 3.7.21 fica provada.

Demonstração de 3.7.22 : Por 3.7.7 e por 3.7.13 temos que $v_i \subseteq Zf_i \cup Zg_i$ sempre que $i \in \omega$. Escolhemos $\{i, j\} \subseteq \omega$ com $i \neq j$. Então $v_i \cap v_j \subseteq (Zf_i \cup Zg_i) \cap (Zf_j \cup Zg_j) = (Zf_i \cap Zg_j) \cup (Zf_j \cap Zg_i)$, já que

3.7.3 e 3.7.6 nos dão que $Z\delta_i \cap Z\delta_j = \phi = Zg_i \cap Zg_j$.

Sem perder a generalidade, podemos supor que $i < j$. Então já temos que $V_i \cap V_j \subseteq Z\delta_j \cap Zg_i$, já que 3.7.9 nos dá que $Z\delta_i \cap Zg_j = \phi$.

Por 3.7.8 temos que $Z\delta_{i+1} \cap Zg_i = \{d_i\}$. Mas lembramos que $Z\delta_j \cap Zg_i = \phi$ se $j > i+1$. Segue que $V_i \cap V_j \subseteq \{d_i\}$ para $j = i+1$, mas que $V_i \cap V_j = \phi$ para $j > i+1$. Resta-nos portanto, para demonstrar 3.7.22, mostrar que $d_i \notin V_i \cap V_{i+1}$. Para isto, basta mostrar que $d_i \notin V_i$.

Por 3.7.8 temos que $d_i \in Z\delta_{i+1}$ e então por 3.7.6, que $d_i \notin Z\delta_i$. Segue que $d_i \notin \{\delta^n(c_i) : n \in E\}$, pois $\{\delta^n(c_i) : n \in E\} \subseteq Z\delta_i$.

Por 3.7.10 e 3.7.13 temos que $d_i = g^q(c_i) = g^{q+e}(b_i)$. Mas $(q+e)_t \in \underline{t-E}$. Portanto $d_i \notin \{g^n(b_i) : n \in E\}$.

Os dois últimos parágrafos nos garantem que $d_i \notin V_i$ e portanto fica a afirmação 3.7.22 demonstrada.

Demonstração de 3.7.23 : Seja $\langle n, i, j \rangle \in E \times \omega^2$. Por 3.7.7 temos que $\delta^n(c_i) \in Z\delta_i$. Por 3.7.7, 3.7.12 e 3.7.14 temos que $\{a_j, c_j, x_j\} \subseteq Z\delta_j$. Segue por 3.7.6 que $\delta^n(c_i) \notin \{a_j, c_j, x_j\}$ no caso em que $i \neq j$.

Já que $\langle n, e \rangle \in E \times (\underline{t-E})$, temos que $\delta^n(c_i) \neq \delta^e(c_i)$, e portanto por 3.7.12 que $\delta^n(c_i) \neq a_i$.

Já que $0 < n < t$, temos que $\delta^n(c_i) \neq c_i$.

Já que $\langle n, (q+e)_k \rangle \in E \times (\underline{x}-E)$, temos que $f^n(c_i) \neq f^{q+e}(c_i)$, e portanto por 3.7.14 que $f^n(c_i) \neq x_i$. Em resumo, $f^n(c_i) \notin \{a_i, c_i, x_i\}$. Já tendo que $f^n(c_i) \notin \{a_j, c_j, x_j\}$ para $i \neq j$, temos finalmente que $f^n(c_i) \notin \{a_j, c_j, x_j\}$ para qualquer $\{i, j\} \subseteq \omega$.

Já vimos que $f^n(c_i) \in Zb_i$. Por 3.7.7 e por 3.7.13 e 3.7.10, temos que $\{b_j, d_j\} \subseteq Zg_j$. Há três casos a considerar.

Caso : $i = j$. Então $\{f^n(c_i)\} \cap \{b_j, d_j\} \subseteq Zb_i \cap Zg_j = \{c_i\}$. Portanto, já que $f^n(c_i) \neq c_i$, temos que $f^n(c_i) \notin \{b_j, d_j\}$ quando $i = j$.

Caso : $i = j+1$. Então $\{f^n(c_i)\} \cap \{b_j, d_j\} \subseteq \{d_j\}$. Mas já que $\langle n, p \rangle \in E \times (\underline{x}-E)$, temos que $f^n(c_i) \neq f^p(c_i)$, e portanto por 3.7.10 que $f^n(c_i) \neq d_j$. Segue que $f^n(c_i) \notin \{b_j, d_j\}$ quando $i = j+1$.

Caso : $i \notin \{j, j+1\}$. Então $\{f^n(c_i)\} \cap \{b_j, d_j\} \subseteq Zb_i \cap Zg_j = \emptyset$. Portanto, em geral, concluimos que $f^n(c_i) \notin \{b_j, d_j\}$ para qualquer que seja $\{i, j\} \subseteq \omega$. Segue finalmente que $f^n(c_i) \notin \{a_j, c_j, x_j, b_j, d_j\}$.

Agora, por 3.7.7 e 3.7.15, temos que $\langle f^n(c_i), y_j \rangle \in Zb_i \times Zg_{i+1}$. Novamente consideraremos três casos.

Caso : $i = j+1$. Então $\{f^n(c_i)\} \cap \{y_j\} \subseteq Zb_i \cap Zg_{j+1} = \{c_i\}$. Mas $f^n(c_i) \neq c_i$. Segue que $f^n(c_i) \neq y_j$ quando $i = j+1$.

Caso : $i = j+2$. Então $\{f^n(c_i)\} \cap \{y_j\} \subseteq Zb_i \cap Zg_{j+1} = \{d_{j+1}\}$. Três parágrafos atrás, vimos que $f^n(c_i) \notin \{d_v : v \in \omega\}$. Em particular $f^n(c_i) \neq d_{j+1}$. Segue que $f^n(c_i) \neq y_j$ quando $i = j+2$.

Caso : $i \notin \{j+1, j+2\}$. Então $\{f^n(c_i)\} \cap \{y_j\} \subseteq Zf_i \cap Zg_{j+1} = \emptyset$. Em geral, portanto, temos que $f^n(c_i) \neq y_j$ para qualquer que seja $\{i, j\} \subseteq \omega$. Resumindo, temos até este ponto que $f^n(c_i) \notin X_j$ para qualquer que seja $\{i, j\} \subseteq \omega$.

A fim de acabar a demonstração de 3.7.23 , falta mostrar que também $g^n(b_i) \notin X_j$. O argumento é bastante similar ao terminado no parágrafo anterior.

Por 3.7.7 , 3.7.10 e 3.7.13 é fácil ver que $\{g^n(b_i)\} \times \{b_j, c_j, d_j\} \subseteq Zg_i \times Zg_j$. Segue por 3.7.6 que $g^n(b_i) \notin \{b_j, c_j, d_j\}$ se $i \neq j$.

Já que $0 < n < t$, temos que $g^n(b_i) \neq b_i$.

Já que $\langle n, e \rangle \in E \times (\underline{t} - E)$, temos que $g^n(b_i) \neq g^e(b_i)$, e portanto, por 3.7.13 temos que $g^n(b_i) \neq c_i$.

Já que $\langle n, (q+e)_t \rangle \in E \times (\underline{t} - E)$, temos que $g^n(b_i) \neq g^{q+e}(b_i)$. Mas por 3.7.10 e 3.7.13 temos que $d_i = g^q(c_i) = g^{q+e}(b_i)$. Portanto $g^n(b_i) \neq d_i$. Em resumo destes três parágrafos, temos que $g^n(b_i) \notin \{b_i, c_i, d_i\}$. Assim vimos que $g^n(b_i) \notin \{b_j, c_j, d_j\}$ para qualquer que seja $\{i, j\} \subseteq \omega$.

Por 3.7.7 , 3.7.12 , 3.7.13 e 3.7.14 temos que $\{g^n(b_i)\} \times \{a_j, x_j\} \subseteq Zg_i \times Zf_j$. Para mostrar que $g^n(b_i) \notin \{a_j, x_j\}$, há três casos a considerar.

Caso : $j = i$. Então $\{g^n(b_i)\} \cap \{a_j, x_j\} \subseteq Zg_i \cap Zf_j = \{c_i\}$. Já que $g^n(b_i) \notin \{b_j, c_j, d_j\}$ para qualquer $j \in \omega$, temos em particular que $g^n(b_i) \neq c_i$. Portanto

$g^h(b_i) \notin \{a_j, x_j\}$ quando $j = i$.

Caso : $j = i+1$. Então $\{g^h(b_i)\} \cap \{a_j, x_j\} \subseteq Zg_i \cap Z\delta_j = \{d_i\}$. Mas também temos, em particular, que $g^h(b_i) \neq d_i$. Portanto $g^h(b_i) \notin \{a_j, x_j\}$ quando $j = i+1$.

Caso : $j \notin \{i+1, i\}$. Então $\{g^h(b_i)\} \cap \{a_j, x_j\} \subseteq Zg_i \cap Z\delta_j = \emptyset$. Portanto $g^h(b_i) \notin \{a_j, x_j\}$ sempre que $\{i, j\} \subseteq \omega$. Juntando este fato com o já obtido quatro parágrafos atrás, temos que $g^h(b_i) \notin \{b_j, c_j, d_j, a_j, x_j\}$, para qualquer que seja $\{i, j\} \subseteq \omega$.

Por 3.7.7, 3.7.13 e 3.7.15 temos que $\langle g^h(b_i), y_j \rangle \in Zg_i \times Zg_{j+1}$. Portanto se $i \neq j+1$, então $\{g^h(b_i)\} \cap \{y_j\} \subseteq Zg_i \cap Zg_{i+1} = \emptyset$; isto é $g^h(b_i) \neq y_j$ quando $i \neq j+1$.

Já que $\langle h, p \rangle \in E \times (\underline{t} - E)$, temos que $g^h(b_i) \neq g^p(b_i)$. Mas, por 3.7.15 e 3.7.13 temos que $y_j = g^{p-e}(c_{j+1}) = g^p(b_{j+1})$. Segue que $g^h(b_i) \neq g^p(b_{j+1}) = y_j$ quando $i = j+1$. Assim temos que $g^h(b_i) \neq y_j$ para qualquer que seja $\{i, j\} \subseteq \omega$, e portanto finalmente que $g^h(b_i) \notin X_j$. A afirmação 3.7.23 fica provada.

Demonstração de 3.7.24 : Seja $i \in \omega$. Por 3.7.7, 3.7.12 e 3.7.14 temos que $\{\delta^p(c_0)\} \times \{a_i, c_i, x_i\} \subseteq Z\delta_0 \times Z\delta_i$. Segue por 3.7.6 que $\delta^p(c_0) \notin \{a_i, c_i, x_i\}$ quando $i \neq 0$.

Já que $\langle e, p \rangle \in D \times (\underline{t} - D)$, temos que $\delta^p(c_0) \neq \delta^e(c_0)$ e portanto por 3.7.12 que $\delta^p(c_0) \neq a_0$.

Já que $0 < p < t$, temos que $\delta^p(c_0) \neq c_0$.

Várias vezes observamos que $t \nmid p-q-e$. Segue que $x_0 \neq f^{p-q-e}(x_0)$. Mas por 3.7.14 temos que $f^p(c_0) = f^{p-q-e}(x_0)$. Segue que $f^p(c_0) \neq x_0$. Em resumo destes três parágrafos, temos que $f^p(c_0) \notin \{a_0, c_0, x_0\}$. Assim vimos que $f^p(c_0) \notin \{a_i, c_i, x_i\}$ para qualquer que seja $i \in \omega$.

Por 3.7.7, 3.7.8 e 3.7.13 é fácil de ver que $\{f^p(c_0)\} \times \{b_i, d_i\} \subseteq Zf_0 \times Zg_i$. Em particular, $\{f^p(c_0)\} \cap \{b_0, d_0\} \subseteq Zf_0 \cap Zg_0 = \{c_0\}$. Mas já que $f^p(c_0) \neq c_0$, temos que $\{f^p(c_0)\} \cap \{b_0, d_0\} = \emptyset$.

Por outro lado, se $i > 0$, temos que $\{f^p(c_0)\} \cap \{b_i, d_i\} \subseteq Zf_0 \cap Zg_i = \emptyset$. Com isto, vimos que $f^p(c_0) \notin \{b_i, d_i\}$ para qualquer que seja $i \in \omega$. Juntando este fato com o obtido dois parágrafos atrás, temos que $f^p(c_0) \notin \{a_i, c_i, x_i, b_i, d_i\}$ para todo $i \in \omega$.

Por 3.7.7 e 3.7.15 temos que $\langle f^p(c_0), y_i \rangle \in Zf_0 \times Zg_{i+1}$. Então $\{f^p(c_0)\} \cap \{y_i\} \subseteq Zf_0 \cap Zg_{i+1} = \emptyset$ e portanto $f^p(c_0) \neq y_i$ para qualquer que seja $i \in \omega$. Finalmente, temos agora que $f^p(c_0) \notin x_i$ para qualquer que seja $i \in \omega$.

A fim de acabar a demonstração da afirmação 3.7.24, falta mostrar analogamente que também $g^p(b_0) \notin x_i$ para $i \in \omega$.

Lembrando que $\{g^p(b_0)\} \times \{b_i, c_i, d_i\} \subseteq Zg_0 \times Zg_i$, temos por 3.7.6 que $g^p(b_0) \notin \{b_i, c_i, d_i\}$ quando $i \neq 0$.

Já que $0 < p < t$ temos que $g^p(b_0) \neq b_0$.

Já que $\langle e, p \rangle \in \mathcal{D} \times (\underline{t} - \mathcal{D})$ temos que $g^p(b_0) \neq g^e(b_0)$ e portanto, por 3.7.13, que $g^p(b_0) \neq c_0$.

Já que $t \nmid p-e-q$, temos que $g^{p-e-q}(d_0) \neq d_0$. Mas, por 3.7.13 e 3.7.10, temos que $g^p(b_0) = g^{p-e}(c_0) = g^{p-e-q}(d_0)$. Segue que $g^p(b_0) \neq d_0$. Em resumo, temos também que $g^p(b_0) \notin \{b_0, c_0, d_0\}$. Portanto $g^p(b_0) \notin \{b_i, c_i, d_i\}$ para qualquer $i \in \omega$.

Lembramos agora que $\{g^p(b_0)\} \times \{a_i, x_i\} \subseteq Zg_0 \times Z\delta_i$. Para mostrar que $g^p(b_0) \notin \{a_i, x_i\}$, consideremos três casos.

Caso : $i = 0$. Então $\{g^p(b_0)\} \cap \{a_i, x_i\} \subseteq Zg_0 \cap Z\delta_i = \{c_0\}$. Mas já vimos, dois parágrafos atrás, que $g^p(b_0) \notin \{b_i, c_i, d_i\}$ para qualquer $i \in \omega$. Em particular, temos que $g^p(b_0) \neq c_0$. Segue que $g^p(b_0) \notin \{a_i, x_i\}$ quando $i = 0$.

Caso : $i = 1$. Então $\{g^p(b_0)\} \cap \{a_i, x_i\} \subseteq Zg_0 \cap Z\delta_i = \{d_0\}$. Mas temos também que $g^p(b_0) \neq d_0$, pois lembramos que $g^p(b_0) \notin \{b_0, c_0, d_0\}$. Segue que $g^p(b_0) \notin \{a_i, x_i\}$ quando $i = 1$.

Caso : $i > 1$. Então $\{g^p(b_0)\} \cap \{a_i, x_i\} \subseteq Zg_0 \cap Z\delta_i = \emptyset$. Segue que $g^p(b_0) \notin \{a_i, x_i\}$ para qualquer que seja $i \in \omega$. Juntando este fato com o anteriormente obtido, já temos então que $g^p(b_0) \notin \{b_i, c_i, d_i, a_i, x_i\}$ para qualquer $i \in \omega$.

Finalmente lembrando que $\langle g^p(b_0), y_i \rangle \in Zg_0 \times Zg_{i+1}$ e que $Zg_0 \cap Zg_{i+1} = \emptyset$, vemos que $g^p(b_0) \neq y_i$ para qualquer que seja $i \in \omega$. Com isto, concluímos que $g^p(b_0) \notin x_i$ para qualquer que seja $i \in \omega$, e então a afirmação 3.7.24 fica provada.

Como proposto anteriormente estamos agora em condições de construir a permutação h intercalável de Z .

A afirmação 3.7.19 nos garante que tanto $(a_i \ c_i \ b_i)$ como $(x_i \ d_i \ y_i)$ são 3-ciclos em Z e que a família $\{(a_i \ c_i \ b_i), (x_i \ d_i \ y_i)\}$ é dcp para qualquer que seja $i \in \omega$.

Com mais a afirmação 3.7.20, temos que também a família $\{(a_i \ c_i \ b_i), (a_j \ c_j \ b_j), (x_i \ d_i \ y_i), (x_j \ d_j \ y_j)\}$ é dcp para qualquer que seja $\{i, j\} \subseteq \omega$.

Definindo agora a família $Y = \{(a_i \ c_i \ b_i) : i \in \omega\} \cup \{(x_i \ d_i \ y_i) : i \in \omega\}$, fica óbvio pelos parágrafos anteriores que Y é uma família dcp de 3-ciclos em Z .

Definindo também a família $V = \{(\phi^p(c_0) \ g^p(b_0))\} \cup \{(\phi^n(c_i) \ g^n(c_i)) : \langle n, i \rangle \in E \times \omega\}$, fica igualmente óbvio por 3.7.21 e 3.7.22 que V é uma família dcp de 2-ciclos em Z .

Agora por 3.7.23 e 3.7.24, temos finalmente que também $Y \cup V$ é dcp e portanto podemos definir a permutação h de Z por

$$C_Z(h) = C_Z(h; 3) \cup C_Z(h; 2),$$

onde

$$C_Z(h; 3) = Y \quad \text{e} \quad C_Z(h; 2) = V.$$

Segue facilmente de 3.7.19 e 3.7.20 que o conjunto $Y = C_Z(h; 3)$ é infinito.

Igualmente, no conjunto $V = C_Z(h; 2)$, temos exatamente um 2-ciclo $(f^h(c_i), g^h(b_i))$ em Z para cada par $\langle \kappa, i \rangle \in E \times \omega$. Já que $t > 4$ implica que $E \neq \emptyset$, segue que também $C_Z(h; 2)$ é infinito.

Os dois últimos parágrafos estabelecem que h é intercalável.

Agora, para ajudar a demonstração da afirmação 3.7.25 definimos os seguintes conjuntos:

$$25.1 : A = \{f^h(c_i) : \langle \kappa, i \rangle \in E \times \omega\} \cup \{f^p(c_0)\},$$

$$25.2 : B = \{g^h(b_i) : \langle \kappa, i \rangle \in E \times \omega\} \cup \{g^p(b_0)\} \text{ e}$$

$$25.3 : X = \bigcup \{X_i : i \in \omega\}.$$

Então notemos os seguintes fatos óbvios:

$$25.4 : h \upharpoonright (A \cup B) \text{ é involução de } A \cup B \text{ e}$$

$$25.5 : h[A] \subseteq B \subseteq Zg \text{ e } h[B] \subseteq A \subseteq Zf.$$

Agora por 3.7.7, 3.7.8 e 3.7.9 é fácil ver que $Zf \cap Zg = \{c_i : i \in \omega\} \cup \{d_i : i \in \omega\} \subseteq X$. Já que $B \subseteq Zg$, temos que $Zf \cap B \subseteq Zf \cap Zg \subseteq X$. Mas por 3.7.17, 3.7.18, 3.7.23 e 3.7.24 temos que $X \cap A = \emptyset = B \cap X$. Segue que $Zf \cap B = Zf \cap B \cap X \subseteq B \cap X = \emptyset$. Semelhantemente, vemos que $Zg \cap A = \emptyset$. Portanto notemos também que

$$25.6 : f \upharpoonright B = id \upharpoonright B \text{ e } g \upharpoonright A = id \upharpoonright A.$$

Lembrando ainda que $\{a_j, x_j\} \times \{b_j, y_j\} \subseteq Zf \times Zg$ sempre que $j \in \omega$, vemos que $\{a_j, x_j\} \cap Zg \subseteq Zf \cap Zg = \bigcup \{\{c_i, d_i\} : i \in \omega\}$. Mas por 3.7.19 e 3.7.20 temos que $\{a_j, x_j, b_j, y_j\} \cap \bigcup \{\{c_i, d_i\} : i \in \omega\} = \emptyset$ sempre que $j \in \omega$. Segue

portanto que $\{a_j, x_j\} \cap Zg = \emptyset$ e semelhantemente que $\{b_j, y_j\} \cap Zf = \emptyset$, sempre que $j \in \omega$. Portanto, notemos ainda que

$$\begin{aligned} 25.7 : f \{b_j, y_j\} &= id \{b_j, y_j\} \text{ e} \\ g \{a_j, x_j\} &= id \{a_j, x_j\} \end{aligned}$$

Já que para cada $i \in \omega$, temos que f_i é uma componente t -cíclica da permutação f em Z , segue que $z \in Zf$ implica que $z = f^n(c_i)$ para algum $\langle n, i \rangle \in \underline{t} \times \omega$. Consideremos os seguintes cinco casos.

Caso : $n \in E = \underline{t} - \{0, e, p, (q+e)_t\}$. Então $z = f^n(c_i) \in A$.

Caso : $n = 0$. Então $z = f^n(c_i) = c_i \in X$.

Caso : $n = e$. Então $z = f^n(c_i) = f^e(c_i) = a_i \in X$.

Caso : $n = p$. Então $z = f^n(c_i) = f^p(c_i) = d_{i-1} \in X$, quando $i > 0$ e $z = f^p(c_0) \in A$ quando $i = 0$. Em qualquer situação, $z = f^n(c_i) \in A \cup X$ quando $n = p$.

Caso : $n = (q+e)_t$. Então $z = f^n(c_i) = f^{q+e}(c_i) = x_i \in X$.

Em resumo, vimos que em qualquer caso, $z \in Zf$ implica que $z \in A \cup X$. Semelhantemente é fácil ver que $y \in Zg$ implica que $y \in B \cup X$. Segue que

$$25.8 : Zf \subseteq A \cup X \text{ e } Zg \subseteq B \cup X.$$

Finalmente afirmamos que

$$25.9 : \text{ Para todo } \langle u, i \rangle \in Z \times \omega, \text{ temos que } h f^u(c_i) = g^u(b_i).$$

Para estabelecer 25.9, seja $\langle u, i \rangle \in Z \times \omega$. Claramente $\langle u \rangle_t \in \underline{t}$. Consideremos os seguintes cinco casos.

Caso : $\langle u \rangle_t \in E$. Então $(f^u(c_i), g^u(b_i)) \in C_Z(h; 2)$.

Segue que $h\delta^u(c_i) = g^u(b_i)$ para $(u)_k \in E$.

Caso : $(u)_k = 0$. Então $h\delta^u(c_i) = h(c_i)$. Mas $(a_i \ c_i \ b_i) \in C_Z(h; 3)$. Segue que $h(c_i) = b_i = g^u(b_i)$. Portanto $h\delta^u(c_i) = g^u(b_i)$ para $(u)_k = 0$.

Caso : $(u)_k = e$. Então $h\delta^u(c_i) = h\delta^e(c_i) = h(a_i)$. Mas $(a_i \ c_i \ b_i) \in C_Z(h; 3)$. Segue que $h(a_i) = c_i = g^e(b_i) = g^u(b_i)$. Portanto $h\delta^u(c_i) = g^u(b_i)$ para $(u)_k = e$.

Caso : $(u)_k = p$. Então $h\delta^u(c_0) = h\delta^p(c_0)$. Mas $(\delta^p(c_0) \ g^p(b_0)) \in C_Z(h; 2)$. Segue que $h\delta^p(c_0) = g^p(b_0) = g^u(b_0)$. Portanto $h\delta^u(c_i) = g^u(b_i)$ quando $\langle (u)_k, i \rangle = \langle p, 0 \rangle$. Também, para $i > 0$, temos que $h\delta^u(c_i) = h\delta^p(c_i) = h(d_{i-1})$. Mas $(x_{i-1} \ d_{i-1} \ y_{i-1}) \in C_Z(h; 3)$. Segue que $h(d_{i-1}) = y_{i-1} = g^{p-e}(c_i) = g^p(b_i) = g^u(b_i)$. Portanto $h\delta^u(c_i) = g^u(b_i)$ sempre que $(u)_k = p$.

Caso : $(u)_k = (q+e)_k$. Então $h\delta^u(c_i) = h\delta^{q+e}(c_i) = h(x_i)$. Mas $(x_i \ d_i \ y_i) \in C_Z(h; 3)$. Segue que $h(x_i) = d_i = g^q(c_i) = g^{q+e}(b_i) = g^u(b_i)$. Portanto $h\delta^u(c_i) = g^u(b_i)$ também quando $(u)_k = (q+e)_k$, e assim fica provada 25.9.

Demonstração de 3.7.25 : Consideremos $x \in Z$ nos seguintes quatro casos.

Caso : $x \notin Z\delta \cup Zg$. Então $\delta(x) = x = g(x)$. Isto implica que $h(x) = x$. Segue que $h\delta h^{-1}(x) = x = g(x)$, para $x \notin Z\delta \cup Zg$.

Caso : $x \in A$. Então $x \in A \cup B$ e por 25.4 temos que $h^{-1}(x) = h(x)$. Já que $x \in A$, a afirmação 25.5 dá que $h(x) \in B$ e então por 25.6 temos que $\delta h(x) = h(x)$. Segue que $h\delta h^{-1}(x) = h\delta h(x) = hh(x) = h^2(x)$. Já que $x \in A \subseteq A \cup B$, a

afirmação 25.4 dá que $h^2(x) = x$. Mas $x \in A$ também implica por 25.6 que $x = g(x)$. Segue que $h^2(x) = x = g(x)$. Portanto, vimos que $h\delta h^{-1}(x) = g(x)$ quando $x \in A$.

Caso : $x \in B$. Então $x = g^v(b_i)$ para algum $\langle v, i \rangle \in (E \times \omega) \cup \{\langle p, 0 \rangle\}$. Já que $\{(\delta^n(c_i), g^n(b_i)), (\delta^p(c_0), g^p(b_0))\} \subseteq C_Z(h; 2)$ para todo $\langle n, i \rangle \in E \times \omega$, temos que $h^{-1}g^v(b_i) = \delta^v(c_i)$. Segue que $h\delta h^{-1}(x) = h\delta h^{-1}g^v(b_i) = h\delta\delta^v(c_i) = h\delta^{1+v}(c_i)$. Mas 25.9 dá que $h\delta^{1+v}(c_i) = g^{1+v}(b_i)$. Portanto $h\delta h^{-1}(x) = h\delta^{1+v}(c_i) = g^{1+v}(b_i) = gg^v(b_i) = g(x)$. Concluimos que $h\delta h^{-1}(x) = g(x)$ para $x \in B$.

Caso : $x \in X$. Consideremos aqui seis sub-casos.

Sub-caso : $x = a_i$ para algum $i \in \omega$. Então $h\delta h^{-1}(x) = h\delta h^{-1}(a_i)$. Mas já que $(a_i, c_i, b_i) \in C_Z(h; 3)$, temos que $h^{-1}(a_i) = b_i$ e que $h(b_i) = a_i$. Por 25.7 temos que $\delta(b_i) = b_i$ e que $a_i = g(a_i)$. Segue que $h\delta h^{-1}(a_i) = h\delta(b_i) = h(b_i) = a_i = g(a_i) = g(x)$. Portanto $h\delta h^{-1}(x) = g(x)$ quando $x = a_i$.

Sub-caso : $x = b_i$ para algum $i \in \omega$. Então $h\delta h^{-1}(x) = h\delta h^{-1}(b_i)$. Mas já que $(a_i, c_i, b_i) \in C_Z(h; 3)$, temos que $h^{-1}(b_i) = c_i$. Por 25.9 temos que $h\delta(c_i) = g(b_i)$. Segue que $h\delta h^{-1}(b_i) = h\delta(c_i) = g(b_i) = g(x)$. Portanto $h\delta h^{-1}(x) = g(x)$ quando $x = b_i$.

Sub-caso : $x = c_i$ para algum $i \in \omega$. Então $h\delta h^{-1}(x) = h\delta h^{-1}(c_i)$. Mas já que $(a_i, c_i, b_i) \in C_Z(h; 3)$, temos que $h^{-1}(c_i) = a_i$. Por 25.9 temos que $h\delta^{1+e}(c_i) = g^{1+e}(b_i)$. Segue que $h\delta h^{-1}(c_i) = h\delta(a_i) = h\delta\delta^e(c_i) = h\delta^{1+e}(c_i) = g^{1+e}(b_i) = gg^e(b_i) = g(c_i) = g(x)$. Portanto $h\delta h^{-1}(x) = g(x)$ quando $x = c_i$.

Sub-caso : $x = d_i$ para algum $i \in \omega$. Então $hfh^{-1}(x) = hfh^{-1}(d_i)$. Mas já que $(x_i \ d_i \ y_i) \in C_Z(h;3)$, temos que $h^{-1}(d_i) = x_i$. Por 25.9 temos que $h\delta^{1+q+e}(c_i) = g^{1+q+e}(b_i)$. Segue que $hfh^{-1}(d_i) = h\delta(x_i) = h\delta\delta^{q+e}(c_i) = h\delta^{1+q+e}(c_i) = g^{1+q+e}(b_i) = gg^{q+e}(b_i) = gg^q(c_i) = g(d_i) = g(x)$. Portanto $hfh^{-1}(x) = g(x)$ quando $x = d_i$.

Sub-caso : $x = x_i$ para algum $i \in \omega$. Então $hfh^{-1}(x) = hfh^{-1}(x_i)$. Mas $(x_i \ d_i \ y_i) \in C_Z(h;3)$. Segue que $h^{-1}(x_i) = y_i$ e que $h(y_i) = x_i$. Por 25.7 temos que $\delta(y_i) = y_i$ e que $x_i = g(x_i)$. Segue agora que $hfh^{-1}(x_i) = h\delta(y_i) = h(y_i) = x_i = g(x_i) = g(x)$. Portanto, temos que $hfh^{-1}(x) = g(x)$ quando $x = x_i$.

Sub-caso : $x = y_i$ para algum $i \in \omega$. Então $hfh^{-1}(x) = hfh^{-1}(y_i)$. Mas já que $(x_i \ d_i \ y_i) \in C_Z(h;3)$ temos que $h^{-1}(y_i) = d_i$. Por 25.9 temos que $h\delta^{1+p}(c_{i+1}) = g^{1+p}(b_{i+1})$. Segue que $hfh^{-1}(y_i) = h\delta(d_i) = h\delta\delta^p(c_{i+1}) = h\delta^{1+p}(c_{i+1}) = g^{1+p}(b_{i+1}) = gg^p(b_{i+1}) = gg^{p-e}(c_{i+1}) = g(y_i) = g(x)$. Portanto $hfh^{-1}(x) = g(x)$ também quando $x = y_i$.

Assim vimos que $hfh^{-1}(x) = g(x)$ quando $x \in X$.

Já que 25.8 diz que $Z\delta \subseteq A \cup X$ e que $Zg \subseteq B \cup X$, temos que $Z\delta \cup Zg \subseteq A \cup B \cup X$. Assim, pelos quatro casos acima, ficou provada a afirmação 3.7.25, que comprova o LEMA 3.7. ■

TEOREMA 3.8 : Seja $\{m, n, k\} \subseteq \mathbb{Z}_{>1}$. Então existem permutações a e δ de $\mathbb{Z}$ tais que $s = a^k \delta^n a^{-k} \delta^m$.

DEMONSTRAÇÃO : Seja $4 < t \in \omega$, tal que $(m, t) = 1 = (n, t)$. Então $t \in \omega - \underline{2}$ e por Lema 3.4 temos que existem permutações F

e G de Z com $C_Z(F) = C_Z(F; t)$ e com $C_Z(G) = C_Z(G; t)$ tais que $s = GF$. Além disso, pela Demonstração do Lema 3.4, lembramos que tais permutações F e G foram definidas por $C_Z(F) = \{F_i : i \in \omega\}$ e por $C_Z(G) = \{G_i : i \in \omega\}$, onde para cada $i \in \omega$, $F_i = (iT \ iT+1 \ iT+2 \ \dots \ iT+t-2 \ -i-1)$ e $G_i = (iT+t-1 \ iT+t \ iT+t+1 \ \dots \ iT+T \ -i-1)$ com $T = 2t-3$.

Já que $(m, t) = 1 = (n, t)$, temos pelo Lema 1.9 que existem permutações f e g de Z tais que $f^m = F$ e $g^n = G$. Com isto, temos agora que $s = GF = g^n f^m$. Claramente estas permutações f e g podem ser escolhidas de forma que $C_Z(f) = C_Z(f; t)$ e que $C_Z(g) = C_Z(g; t)$. É claro que podemos estipular também que $f_i^m = F_i$ e que $g_i^n = G_i$ para cada $i \in \omega$, e que $Zf_i = ZF_i$ e que $Zg_i = ZG_i$ para cada tal i .

Faremos uma listagem de fatos para assegurar que as permutações f e g de Z satisfazem as hipóteses do LEMA 3.7.

Por nossa escolha inicial para t , lembramos que

1. $4 < t \in \omega$

Seja $c_i = -i-1$ e $d_i = (i+1)T$ para cada $i \in \omega$, onde $T = 2t-3$. Segue que

2. $c_0, c_1, \dots$ e $d_0, d_1, \dots$ são duas seqüências infinitas e injetivas de inteiros.

Na Demonstração do Lema 3.4 foram exibidas permutações F e G determinadas pelas seqüências $F_0, F_1, \dots$ e $G_0, G_1, \dots$

infinitas e injetivas de t -ciclos em Z . É claro, pelas nossas estipulações na construção das permutações δ e g que

3. $\delta_0, \delta_1, \dots$ e $g_0, g_1, \dots$ são duas seqüências infinitas e injetivas de t -ciclos em Z .

Sejam $p = (m)_t$ e $q = (-n)_t$. Então, já que $(m, t) = 1 = (n, t)$, temos que

4. $p < t$ e $q < t$ são dois inteiros positivos.

Já que, para todo $i \in \omega$, temos que $c_i = -i-1 \notin \omega$ e que $d_i = (i+1)T \in \omega$, segue que

5. $\{c_i : i \in \omega\} \cap \{d_i : i \in \omega\} = \emptyset$.

Na Demonstração do Lema 3.4 foi observado que ambos os conjuntos $\{F_i : i \in \omega\}$ e $\{G_i : i \in \omega\}$ eram dcp. Mas para cada $i \in \omega$, temos que $Z\delta_i = ZF_i$ e $Zg_i = ZG_i$. Segue então que

6. ambos os conjuntos $\{\delta_i : i \in \omega\}$ e $\{g_i : i \in \omega\}$ são dcp.

Olhando os t -ciclos citados, vemos que para cada $j \in \omega$, temos que $Z\delta_j = ZF_j = \{jT, jT+1, \dots, jT+t-2\} \cup \{-j-1\}$ e que $Zg_j = ZG_j = \{jT+t-1, jT+t, \dots, jT+T\} \cup \{-j-1\}$. Nota-se que

7. $Z\delta_j \cap Zg_j = \{-j-1\} = \{c_j\}$ para cada $j \in \omega$.

Igualmente vemos que $Z\delta_{j+1} = ZF_{j+1} = \{(j+1)T, (j+1)T+1, \dots, (j+1)T+t-2\} \cup \{-j-2\}$. Lembrando que

$Zg_j = \{jT+t-1, jT+t, \dots, (j+1)T\} \cup \{-j-1\}$, notamos também que

$$8. Z\delta_{j+1} \cap Zg_j = \{(j+1)T\} = \{d_j\} \text{ para cada } j \in \omega.$$

Mas também é fácil ver, das nossas construções de δ e de g , que

$$9. Z\delta_i \cap Zg_j = \emptyset \text{ sempre que } j \in \omega \text{ e que } i \in \omega - \{j, j+1\}.$$

Agora seja $i \in \omega$. Lembrando que $p = (m)_t$, que

$\delta_{i+1}^m = F_{i+1}$ e que $c_{i+1} = -i-2$, temos então que $\delta_{i+1}^p(c_{i+1}) = \delta_{i+1}^m(c_{i+1}) = F_{i+1}(c_{i+1}) = F_{i+1}(-i-2)$. Pela definição do t -ciclo $F_{i+1} = (iT+T \ iT+T+1 \ \dots \ iT+T+t-2 \ -i-2)$, vemos que $F_{i+1}(-i-2) = iT+T = (i+1)T$. Mas $(i+1)T = d_i$. Portanto vimos que $\delta_{i+1}^p(c_{i+1}) = (i+1)T = d_i$. Semelhantemente, pelos fatos $q = (-n)_t$, $g_i^n = G_i$ e $c_i = -i-1$, temos que $g_i^q(c_i) = g_i^{-n}(c_i) = G_i^{-1}(c_i) = G_i^{-1}(-i-1)$. Pela definição do t -ciclo G_i , vemos que $G_i^{-1}(-i-1) = iT+T$. Segue que $g_i^q(c_i) = G_i^{-1}(-i-1) = iT+T = (i+1)T = d_i$. Resumindo, temos que

$$10. \delta_{i+1}^p(c_{i+1}) = d_i = g_i^q(c_i) \text{ para cada } i \in \omega.$$

Por 3.81 a 3.8.10, vemos que as permutações δ e g construídas nesta demonstração satisfazem as hipóteses do LEMA 3.7. Então pelo LEMA 3.7 temos que existe permutação h intercalável de Z tal que $g = h\delta h^{-1}$. Portanto, já temos que $s = GF = g\delta^m = (h\delta h^{-1})\delta^m = h\delta^n h^{-1}\delta^m$. Mas já que h é intercalável e que $0 \neq k \in Z$, temos pelo Corolário 3.3 que existe permutação a de Z tal que $a^k = h$. Assim, temos finalmen-

te que $s = h f^n h^{-1} f^m = a^k f^n a^{-k} f^m$. $\square$

Outra tentativa de demonstração do TEOREMA 3.8, sem a necessidade do LEMA 3.7, se ilustra sem demonstração, nos Diagramas 4.5 do Apêndice.

Para finalmente estabelecer o proposto no título deste capítulo, falta ver agora o

Teorema 3,9 : Se $m = p$ e $n = q$ então $\alpha = A^m B^n A^p B^q$ não representa s em S_Z .

Demonstração : Seja $m = p$ e $n = q$. Então $\alpha = A^m B^n A^p B^q = (A^m B^n)^2$. Suponha agora que $(\alpha + s) S_Z$. Então existem permutações f e g de Z tais que $s = (f^m g^n)^2$. Seja $f^m g^n = h$. Assim temos que $h^2 = s$, o que pelo Lema 1.10 é um absurdo. $\square$

Veremos agora uma generalização mais ampla do nosso resultado, que é o

Teorema 3.10 : Seja α uma palavra primitiva de complexidade menos que seis. Então $(\alpha + s) S_Z$.

Demonstração : Obviamente, pelo LEMA 1.17 é suficiente considerar $\alpha \in \{A, B\}^+$. Além disso, pelo Lema 1.14 temos que toda palavra em $\{A, B\}^+$ primitiva de complexidade $2i+1 > 1$ é ciclicamente conjugada a outra palavra primitiva de complexidade $2i$ ou $2i-1$. Conclui-se, pelo Lema 1.20 que é suficiente considerar palavras da forma $A^i B^j$ com $\{i, j\} \subseteq \underline{Z-1}$ e da for-

ma $A^m B^n A^p B^q$ com $\{m, n, p, q\} \subseteq \mathbb{Z} - 1$ e com $m \neq p$ ou $n \neq q$.
Então por [5, theorem 4.3] e pelos TEOREMAS 3.6 e 3.8,
fica o Teorema 3.10 provado. ■

Capítulo IV :

COMENTÁRIOS GERAIS E PERGUNTAS

A pergunta geral, de D. M. Silberger, é a seguinte

Pergunta 4.1 : Toda palavra primitiva é $ISym$ -universal ?

Procuramos, sem sucesso total, estabelecer uma resposta afirmativa para palavras de complexidade quatro. Nossa pesquisa nisto tentou aplicar as técnicas empregadas em [1] , [14] e [15] .

Listamos neste capítulo, sem demonstrações, nossos principais resultados parciais a respeito da questão da $ISym$ -universalidade de palavras de complexidade quatro. Também listamos as nossas conjecturas e algumas perguntas relevantes.

Nós acreditamos que podemos demonstrar as afirmações 4.2 até 4.7 que seguem.

Afirmção 4.2 : Se $n(m+u) \neq 0$ então a palavra $\alpha = A^m B^n A^u B^{2nv}$ representa s em S_Z , sempre que $k \in \omega-1$ e que $\{m, n, u, v\} \subseteq Z$.

Além disso,

1. Se um dos inteiros k, n ou $m+u$ for ímpar então $(\alpha + c_k) S_M$ para algum subconjunto M finito de Z .
2. Se ambos os inteiros n e $m+u$ forem ímpares então $(\alpha + c_k) S_{\underline{k}}$.

Afirmção 4.3 : Se k é inteiro ímpar positivo então existe $\{x, y\} \subseteq S_{\underline{k}}$ com $yxy^{-1}x^{-1} = c_k$, com y sendo involução de $\underline{k}$ e x sendo uma permutação cíclica de $\underline{k}$ de comprimento $(k+1)/2$.

Também se $k \in \omega-1$ então a equação $yxy^{-1}x^{-1} = c_k$ tem solução em S_Z onde x é permutação intercalável de Z tal que $Z-Zx$ é infinito e tal que $C_Z(x) = C_Z(x; k)$, e onde $y = s^{-k}$. Veja o Diagrama 4.1b do Apêndice. Pode-se concluir que também a equação $y^k x^m y^{-k} x^{-m} = c_{|k|}$ tem solução em S_Z sempre que $\{k, m\} \subseteq Z-1$.

Afirmção 4.4 : Se $n(m+p) \neq 0$ então a equação $y^n x^m y^{npk} x^p = c_k$ tem solução em S_Z .

Obviamente, se $(n, k) = 1$ ou se $(m+p, k) = 1$ então esta equação tem solução também em $S_{\underline{k}}$, pois se $(n, k) = 1$ ou se $(m+p, k) = 1$ então $(\text{mdc}(\alpha), k) = 1$, onde $\alpha = A^n B^m A^{npk} B^p$.

Afirmção 4.5 : Se $m \neq 0$ então as palavras α da forma $A^m B A^{\pm m} B^{-1}$ representam c_k em S_Z , sempre que $k \in \omega-1$.

Além disso,

1. Se k é ímpar e $(m, k) = 1 = (n, k)$ então $(A^m B A^n B^{-1} + c_k) S_{\underline{k}}$.
2. Se os inteiros k, m, n e p forem ímpares, então $(A^m B^p A^n B^{-p} + c_k) S_{\underline{k}}$.

Afirmção 4.6 : Seja $k = 2t+1$ para algum $t \in \omega$, e seja m tal que $(m, t+1) = 1$. Seja $\beta = A^m B^p A^m B^{-p}$. Nestas condições temos que

1. Se p for ímpar então $(\beta + c_k) S_{\underline{k}}$,
2. Se $p|t$ então $(\beta + c_k) S_{\underline{k}}$,
3. Se $(p, k) = 1$ então $(A^m B^p A^{-m} B^{-p} + c_k) S_{\underline{k}}$.

Afirmção 4.7 : Se para todo $k \in \omega - 1$ temos que $(\alpha + c_k)S_Z$, então $(\alpha + \delta)S_Z$ desde que δ tenha infinitos pontos fixos e que $(\alpha + \delta)S_Z$.

As afirmações 4.8 e 4.9 que seguem são apenas nossas conjecturas.

Conjectura 4.8 : Seja $\alpha = A^m B^p A^n B^{-p}$ com $(m, t) = 1 = (n, t)$ para algum $t > 1$ e seja $k = 2h(t-1) + 1$ para algum $h > 0$. Então $(\alpha + c_k)S_{\underline{k}}$ desde que se cumpra uma das condições :

1. $(p, 6) = 1$,
2. $p \mid (h-1, h(t-3)+2)$,
3. $(p, k-h) = 1$,
4. $(p, 4h+2) = 1$,
5. $(p, 2h+1) = 1$ e $p \mid h(t-2)$.

Conjectura 4.9 : Seja $I \subseteq \omega$ e seja $\{\delta_i : i \in I\}$ o conjunto das componentes cíclicas finitas de $\delta \in S_X$ para algum subconjunto X de inteiros. Suponha que para cada $i \in I$, exista $M(i) \subseteq X$, com $|M(i)| < \aleph_0$ tal que $(\alpha + \delta_i + M(i))S_{M(i)}$. Assim se $(\alpha + \delta)S_Z$ então $(\alpha + \delta)S_X$ desde que δ tenha no mínimo $\sum_{i \in I} (|M(i)| - |\chi \delta_i|)$ pontos fixos.

Em particular vimos que

Proposição 4.10 : $(A^2 B^3 A^{-2} B^3 + c_2)S_Z$.

Proposição 4.11 : $(A^{-4} B A^4 B^{-1} + c_4)S_Z$.

Não ousamos adivinhar as respostas às perguntas 4.12 até 4.15, aparentemente em aberto, que agora listamos.

Pergunta 4.12 : $(A^m B A^n B^{-1} + c_k) S_k$ para que $\{k, m, n\}$?
(sugerida pela Afirmação 4.5)

Pergunta 4.13 : $(A^m B^p A^{\pm m} B^{-p} + c_k) S_k$ para que $\{k, p, m\}$? (sugerida pela Afirmação 4.6)

Pergunta 4.14 : $(A^m B^p A^{\pm m} B^{-p} + c_k) S_k$ sempre que $p=k$?
(sugerida pelas Proposições 4.10 e 4.11)

Pergunta 4.15 : Seja α de complexidade mais que três e suponha que $(\alpha + c_k) S_Z$ para todo $k \in \omega - 1$. Então $(\alpha + s) S_Z$ implica que $\alpha + s S_Z$?

Finalmente, concluímos o capítulo com as particulares perguntas, que em especial muito trabalhamos, sem total êxito, por não se enquadrar nas técnicas até aqui desenvolvidas; uma, a PERGUNTA 4.16 para ciclos finitos, e outra, a PERGUNTA 4.17 para ciclos infinitos.

PERGUNTA 4.16 : Pode $x^3 y^3 x y$ ser uma transposição, quando $\{x, y\} \subseteq S_Z$?

Para responder afirmativamente, basta mostrar que $x^3 y^3 x y = (0 \ 1)$ tem solução $\langle x, y \rangle \in S_Z^2$.

PERGUNTA 4.17 : Para cada $\{m, n, t\} \subseteq \mathbb{Z} - 1$ com $t > 3$ e com $(m, t) = 1 = (n, t)$ serão todos os "vértices" dos polígonos de lado t dos Diagramas 4.5 do Apêndice, "nomeados" por exatamente um inteiro ?

APÊNDICE :

Diagramas 4.1 - "	$yxy^{-1}x^{-1} = c_n$	"	65
Diagrama 4.2 - "	Intecalação de ciclos	"	68
Diagrama 4.3 - "	$s = GF$	"	69
Diagrama 4.4 - "	$g = hgh^{-1}$	"	70
Diagramas 4.5 - "	Outra opção p/ TEOREMA 3.8	"	72
Tabela 4.6 - "	Índice das numerações	"	76
Tabela 4.7 - "	Índice de símbolos	"	78

Diagramas 4.1 :

$$"yxy^{-1}x^{-1} = c_n"$$

Inicialmente Silberger exibiu permutações x e y de Z , conforme mencionado na página 28, tais que $yxy^{-1}x^{-1} = c_{2k}$ para $k \in \omega-1$. Tais permutações aparecem na Figura 1a, onde podemos ver que x ($\dashrightarrow$) é composta por exatamente $4k$ componentes ω -cíclicas em Z (que pode ser $x = s^{4k}$) e que y ($\longrightarrow$) é composta por exatamente $2k$ componentes ω -cíclicas em Z . Para esta figura, tomamos como exemplo, $k = 2$. Assim, $yxy^{-1}x^{-1} = c_4 = (0 \ 1 \ 2 \ 3)$. Veja a Figura 1a na página seguinte.

Mais tarde, conseguimos generalizar este resultado, achando permutações de Z tais que a mesma equação também era válida para c_n quando $n \in \omega-1$; isto é $yxy^{-1}x^{-1} = c_n$, como mencionamos na página 61. Tais permutações aparecem na Figura 1b, onde podemos ver que x ($\dashrightarrow$) tem uma infinidade de pontos fixos, e é intercalável, enquanto que y ($\longrightarrow$) é composta por exatamente n componentes ω -cíclicas em Z (que pode ser $y = s^{-n}$). Para esta figura, tomamos como exemplo, também $n = 4$. Assim, $yxy^{-1}x^{-1} = c_4 = (0 \ 1 \ 2 \ 3)$. Veja a Figura 1b na página 67.

Nesta figura temos as seguintes convenções :

o os inteiros "restantes" ; $\mathbb{Z}_4$.

$\longrightarrow$ y

$\dashrightarrow$ x

Observe que

$$y \ x \ y^{-1} \ x^{-1} = (0 \ 1 \ 2 \ 3)$$

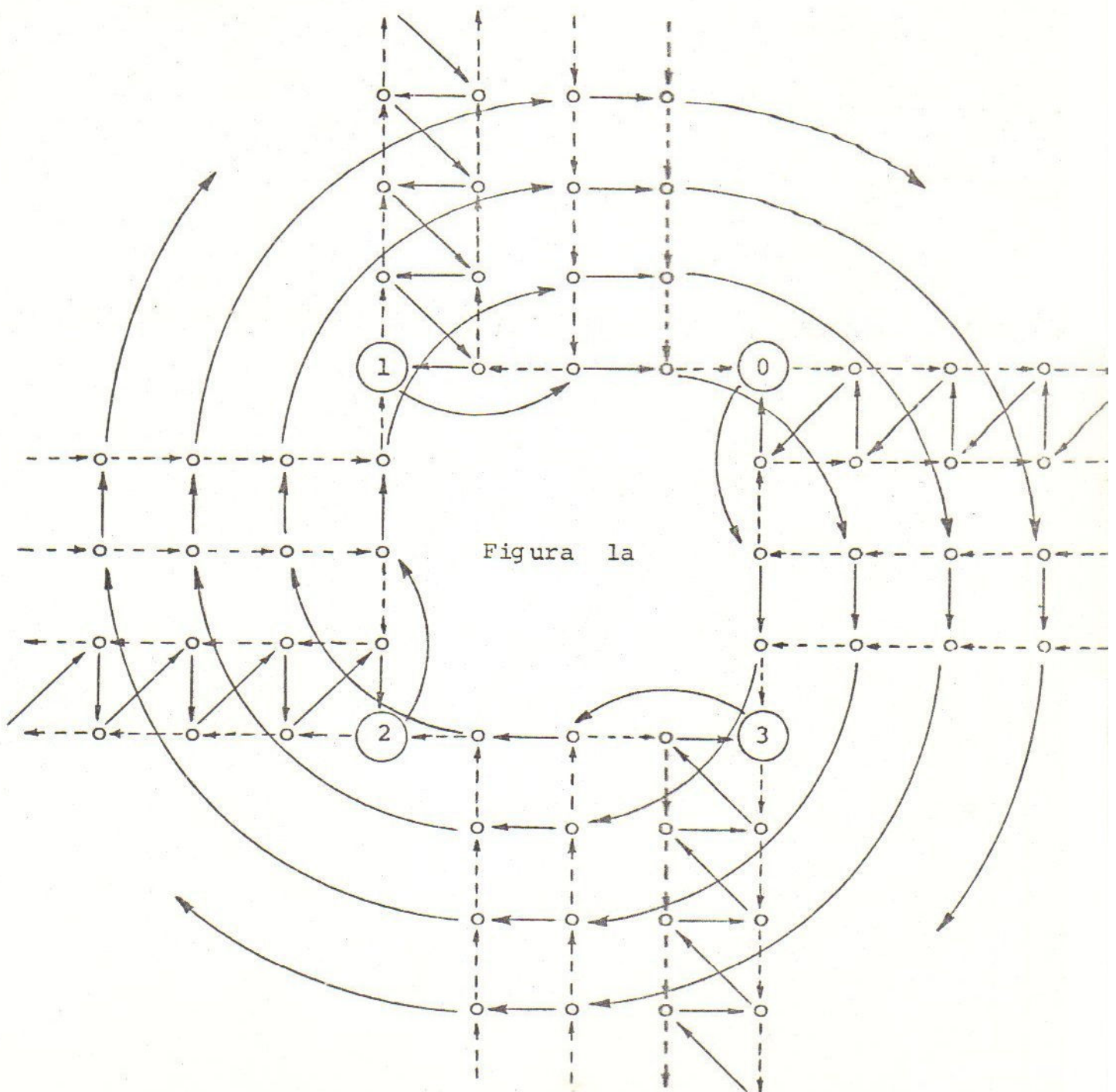
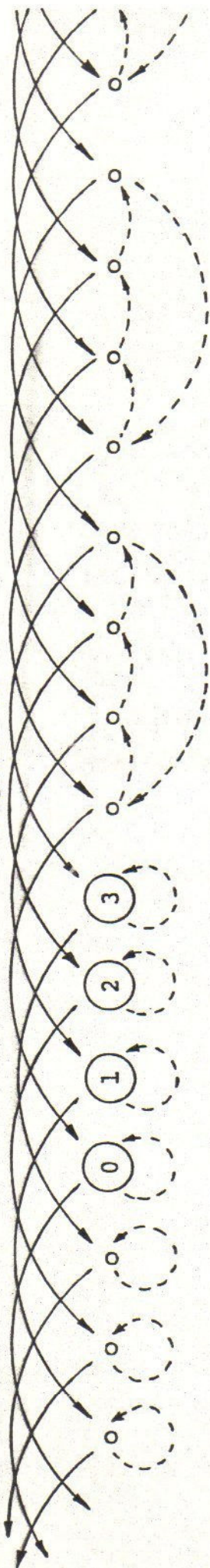


Figura 1a

Figura 1b



Nesta figura temos as seguintes convenções :

o os inteiros " restantes " ; $\underline{2-4}$.

$\longrightarrow$ y

$\dashrightarrow$ x

Observe que

$$y \times y^{-1} \quad x^{-1} = (0 \quad 1 \quad 2 \quad 3)$$

Diagrama 4.2 :

"Intercalação de ciclos"

Conforme mencionamos na página 31 , seja

$h = (0 \ 1 \ 2)(3 \ 4 \ 5)(6 \ 7 \ 8)(9 \ 10 \ 11)(12 \ 13 \ 14)$
 $(15 \ 16 \ 17)(18 \ 19 \ 20)(21 \ 22 \ 23) \dots \in S_7$. Notemos que h
 é intercalável e que $C_7(h) = C_7(h;3)$. Suponha que queremos
 obter $g \in S_7$ tal que $g^{-8} = h$.

Uma das maneiras de obter tal permutação g é agrupar os 3-ciclos de h em 7, de 8 em 8 e intercalá-los. Assim, se $g_* = (0 \ 3 \ 6 \ 9 \ 12 \ 15 \ 18 \ 21 \ 1 \ 4 \ 7 \ 10 \ 13$
 $16 \ 19 \ 22 \ 2 \ 5 \ 8 \ 11 \ 14 \ 17 \ 20 \ 23)(24 \ 27 \ 30 \dots 47) \dots$
 então notemos que $g_* \in S_7$, que $\text{ord}(g_*) = 24$ e que $g_*^8 = h$.
 Basta agora fazer $g = g_*^{-1}$ para que $g^{-8} = (g_*^{-1})^{-8} = g_*^8 = h$.

Se, no entanto, adicionalmente estipularmos que queremos $a \in S_7$ tal que $a^{-8} = h$ enquanto que $\text{ord}(a) = 12$, devemos então agrupar os 3-ciclos de h em 7, de 4 em 4 e intercalá-los convenientemente, pois $(-8, 12) = 4$ enquanto que $12/(-8, 12) = 12/4 = 3$. Assim, se $a_* = (0 \ 3 \ 6 \ 9 \ 2 \ 5 \ 8$
 $11 \ 1 \ 4 \ 7 \ 10)(12 \ 15 \ 18 \ 21 \ 14 \ 17 \ 20 \ 23 \ 13 \ 16 \ 19 \ 22)$
 $(24 \ 27 \ 30 \dots 34) \dots$ então notemos que $a_* \in S_7$, que $\text{ord}(a_*) = 12$
 e que $a_*^8 = h$. Basta agora fazer $a = a_*^{-1}$ para que $a^{-8} = h$.
 É claro que também $\text{ord}(a) = 12$.

" $\Delta = GF$ "

$ord(F) = t = 4$ e que $ord(G) = u = 5$; e ainda que

um caso particular de [14 , diagram] .

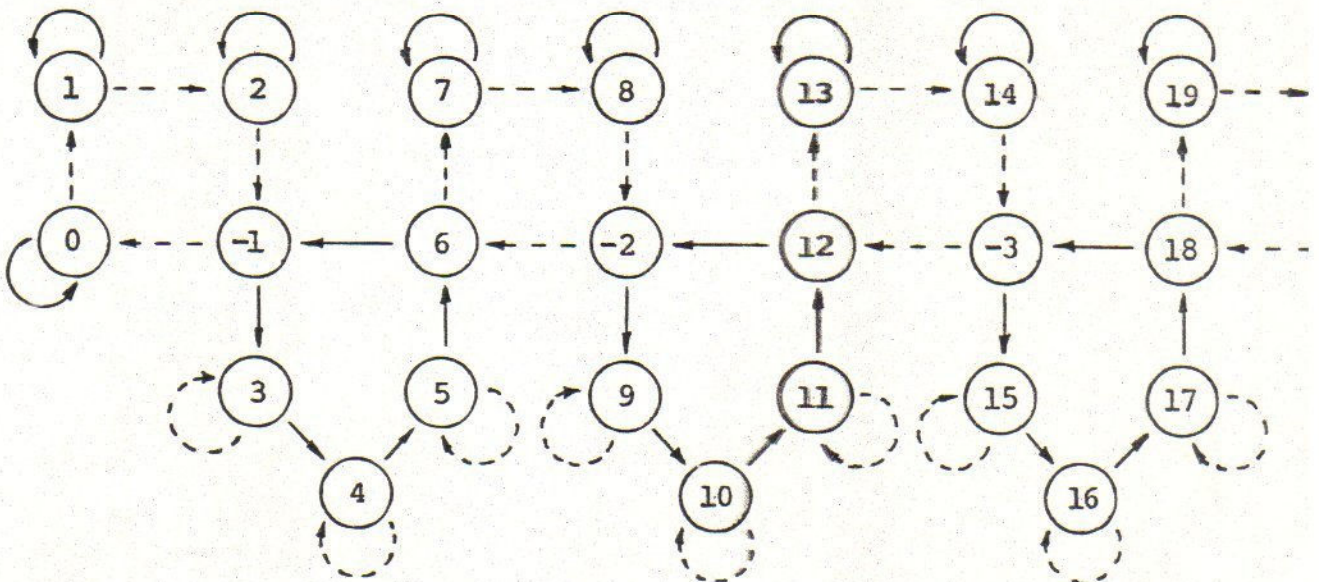


Diagrama 4.4 :

$$" g = hfh^{-1} "$$

Conforme mencionamos na página 37 , apresentamos um esboço das permutações f , g e h de Z , todas intercaláveis tais que $g = hfh^{-1}$. Veja a Figura 4 , na página seguinte.

Lembramos aqui, que :

$$C_Z(f) = C_Z(f;t) \quad \text{com} \quad t > 4$$

$$C_Z(g) = C_Z(g;t) = \{g_i : i \in \omega\}$$

$$Zf_i \cap Zg_i = \{c_i\} \quad \text{para} \quad i \in \omega$$

$$Zf_j \cap Zg_i = \{d_i\} \quad \text{para} \quad j = i+1$$

$$f^p(c_{i+1}) = d_i = g^q(c_i) \quad \text{para} \quad i \in \omega$$

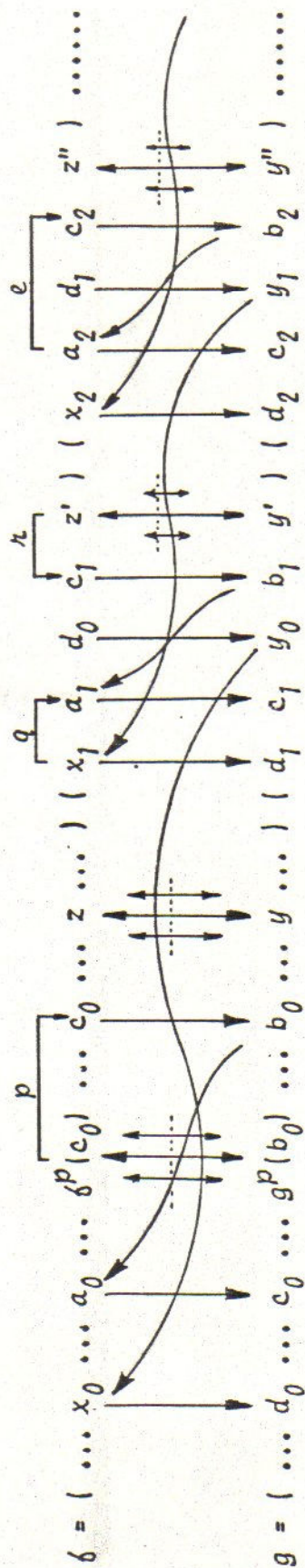
$$a_i = f^e(c_i) \quad \text{para} \quad i \in \omega$$

$$b_i = g^{-e}(c_i) \quad \text{para} \quad i \in \omega$$

$$x_i = f^{q+e}(c_i) \quad \text{para} \quad i \in \omega$$

$$y_i = g^{p-e}(c_{i+1}) \quad \text{para} \quad i \in \omega$$

Figura 4



$$h = \prod_{i=0}^{\infty} (a_i \ c_i \ b_i) \ (x_i \ d_i \ y_i) \prod_{z \in A} y \in B \ (z \ y)$$

$$z(i) = f^h(c_i)$$

$$y(i) = g^h(b_i)$$

$$A = Z\delta - \bigcup_{i=0}^{\infty} \{a_i, c_i, d_i, x_i\}$$

$$B = Zg - \bigcup_{i=0}^{\infty} \{b_i, c_i, d_i, y_i\}$$

Legenda :

As setas $\longrightarrow$ indicas a permutação h ; e as setas $\longleftarrow$ indicam potências.

$$g = h \delta h^{-1}$$

ou

$$g h = h \delta$$

Diagramas 4.5 :

" Outra opção p/ TEOREMA 3.8 "

Conforme mencionamos nas páginas 8 , 58 e 63 , apresentamos aqui nossa tentativa de demonstração do TEOREMA 3.8 através de um exemplo, com $m = 4$ e $n = 2$, mas "independente" do LEMA 3.7 . Assim veremos que a equação $y^k x^2 y^{-k} x^4 = s$ tem solução em S_7 para todo k inteiro não nulo.

Podemos escolher $t = 5$, já que $(4,5)=1=(2,5)$ e que $5>3$. Então construímos uma sequência de pentágonos ($t=5$), cujos lados representam as setas indicando as funções F ($-->$) e G ($--->$) , e cujos vértices esperamos representar os inteiros que darão "nomes" aos vértices segundo a relação $G^n F^m(x) = G^2 F^4(x) = s(x) = x+1$, da seguinte maneira :

Inicialmente, todo vértice é "sem nome". Veja a Figura 5a na página seguinte. Começamos por colocar "0" em qualquer vértice. Agora, a partir de "0" , seguindo 4 setas de F ($-->$) e em seguida 2 setas de G ($--->$) , chegamos a um vértice que o "denominaremos" de "1" , isto é $G^2 F^4(0) = 1$.

Continuando, a partir de "1" , seguindo novamente 4 setas de F e a seguir mais 2 setas de G , chegamos a outro vértice que o "denominaremos" de "2" , ou seja $G^2 F^4(1) = 2$.

Semelhantemente, a partir de "2" , com F^4 e G^2 chegaremos a outro vértice que o "denominaremos" de "3" , então $G^2 F^4(2) = 3$; etc...

$$G^2 F^4(x) = x+1$$

$\cdots \rightarrow F$
 $\longrightarrow G$

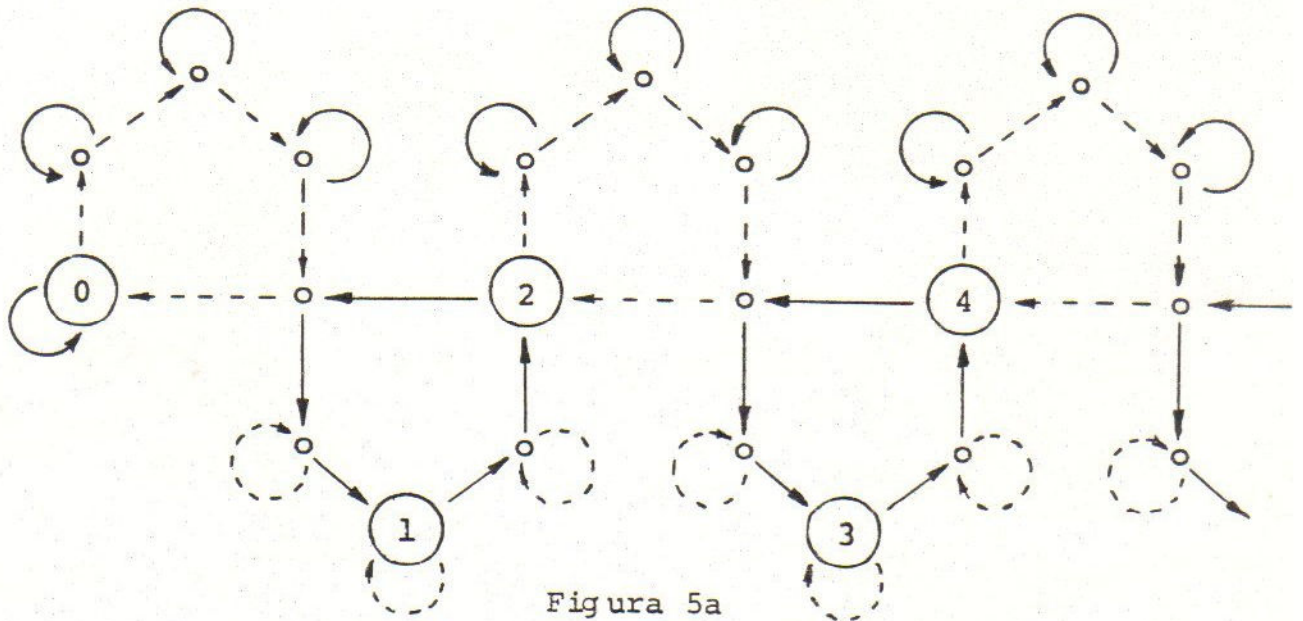


Figura 5a

$\circ \equiv$ vértices "sem nome"

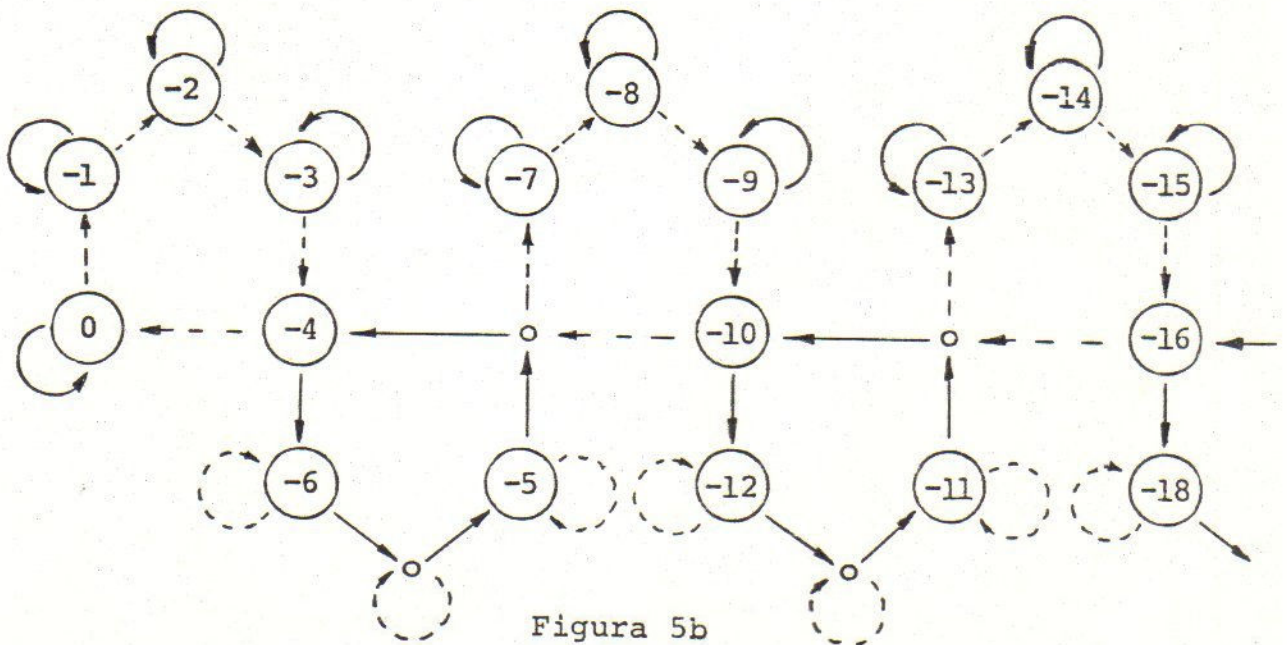


Figura 5b

Desta forma, todos os inteiros não negativos dão "nomes" a vértices; e acreditamos que assim nenhum vértice receba mais que um tal "nome". Acreditamos também que sobrarão uma infinidade de vértices convenientemente localizados, ainda "sem nome".

Agora concluiremos o preenchimento dos vértices dos pentágonos com os inteiros negativos. Naturalmente, já que F e G supostamente serão permutações de Z , temos de $G^2 F^4 = \delta$ que $\delta^{-1} = F^{-4} G^{-2}$. Assim os "nomes" serão agora dados pela relação $F^{-4} G^{-2}(x) = x-1$.

Começando novamente de "0", seguindo de $\tilde{r}$ 2 setas de G ($\longrightarrow$) e em seguida também de $\tilde{r}$, 4 setas de F ($\dashrightarrow$), chegamos miraculosamente a um vértice "sem nome", que o "denominaremos" de "-1". Veja a Figura 5b na página anterior.

Semelhantemente, a partir de "-1", seguindo de $\tilde{r}$ 2 setas de G e também de $\tilde{r}$ 4 setas de F , chegamos a outro vértice e o "chamaremos" de "-2". Daí, com G^{-2} e F^{-4} , chegamos a "-3", etc...

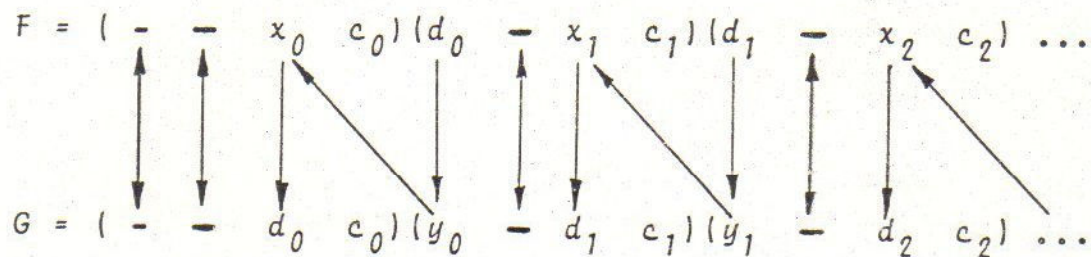
Claramente, justapondo as figuras 5a e 5b, teremos cada vértice preenchidos por exatamente um inteiro, e conseqüentemente conseguimos $\{F, G\} \subseteq S_Z$ tal que $G^2 F^4 = \delta$.

Mas observemos que

$$F = (0 \ -1 \ -2 \ -3 \ -4)(2 \ -7 \ -8 \ -9 \ -10)(4 \ -13 \ -14 \ -15 \ -16) \dots$$

$$G = (-6 \ 1 \ -5 \ 2 \ -4)(-12 \ 3 \ -11 \ 4 \ -10)(-18 \ 5 \ -17 \ 6 \ -16) \dots$$

Em geral podemos destacar as seqüências $c_0, c_1, \dots$ e $d_0, d_1, \dots$ das intersecções entre os suportes de F e de G , identificados pelos traços $\begin{array}{|c} \hline \end{array}$ e $\begin{array}{|c|} \hline \end{array}$ respectivamente. Assim, a permutação h intercalável de Z pode ser determinada pela seta  como segue :



Isto é

$$h = \dots (- -) \dots (x_0 \ d_0 \ y_0) (x_1 \ d_1 \ y_1) (x_2 \ d_2 \ y_2) \dots (- -) \dots$$

É possível ver que $G = hFh^{-1}$. Segue que $G^n = hF^n h^{-1}$. Assim, temos que $\delta = G^n F^m = hF^n h^{-1} F^m$.

Mas com $t > 3$, claramente teremos uma infinidade de 2-ciclos de h em Z ; e já tendo também uma infinidade de 3-ciclos de h em Z , inferimos que h é intercalável. Assim, existe $a \in S_Z$ tal que $a^k = h$ sempre que $k \neq 0$. Então $\delta = hF^n h^{-1} F^m = a^k F^n a^{-k} F^m$.

Veja a PERGUNTA 4.17 na página 63.

Tabela 4.6 :

" Índice das numerações "

Conforme mencionamos na página 9 , apresentamos aqui um índice da totalidade das numerações desta dissertação.

Definição	1.1	pg	12	Corolário	2.4	pg	26
Lema	1.2		13	Corolário	2.5		26
Definição	1.3		13	Corolário	2.6		26
Lema	1.4		13	Corolário	2.7		26
Lema	1.5		14	Teorema	2.8		26
Definição	1.6		14	Teorema	2.9		26
Exemplo	1.7		14	Corolário	2.10		27
Observação	1.8		16	Teorema	2.11		27
Lema	1.9		16	Proposição	2.12		27
Lema	1.10		17	Proposição	2.13		27
Exemplo	1.11		18	Teorema	2.14		28
Definição	1.12		18	Teorema	2.15		28
Exemplo	1.13		18	Teorema	2.16		28
Lema	1.14		20	Teorema	2.17		29
Definição	1.15		21	Teorema	2.18		29
Pergunta	1.16		21	Pergunta	2.19		29
LEMA	1.17		21	Pergunta	2.20		29
Definição	1.18		22	Pergunta	2.21		29
Definição	1.19		23	Pergunta	2.22		29
Lema	1.20		23	Pergunta	2.23		29
Pergunta	2.1		25	Definição	3.1		30
Teorema	2.2		25	Lema	3.2		30
Teorema	2.3		25	Nota	3.2.1		31

(continua)

(continuação)

Nota	3.2.2 ...pg	31	Afirmção	3.7.25 ..pg	36
Corolário	3.3	31	Definição	25.1	50
Lema	3.4	32	Definição	25.2	50
Corolário	3.5	33	Definição	25.3	50
TEOREMA	3.6	34	Nota	25.4	50
LEMA	3.7	35	Nota	25.5	50
Hipótese	3.7.1	35	Nota	25.6	50
Hipótese	3.7.2	35	Nota	25.7	51
Hipótese	3.7.3	35	Observação	25.8	51
Hipótese	3.7.4	35	Afirmção	25.9	51
Condição	3.7.5	35	TEOREMA	3.8	54
Condição	3.7.6	35	Teorema	3.9	58
Condição	3.7.7	35	Teorema	3.10	58
Condição	3.7.8	35	Pergunta	4.1	60
Condição	3.7.9	35	Afirmção	4.2	60
Condição	3.7.10	35	Afirmção	4.3	61
Definição	3.7.11	35	Afirmção	4.4	61
Definição	3.7.12	35	Afirmção	4.5	61
Definição	3.7.13	35	Afirmção	4.6	61
Definição	3.7.14	36	Afirmção	4.7	62
Definição	3.7.15	36	Conjectura	4.8	62
Definição	3.7.16	36	Conjectura	4.9	62
Definição	3.7.17	36	Proposição	4.10	62
Definição	3.7.18	36	Proposição	4.11	62
Afirmção	3.7.19	36	Pergunta	4.12	63
Afirmção	3.7.20	36	Pergunta	4.13	63
Afirmção	3.7.21	36	Pergunta	4.14	63
Afirmção	3.7.22	36	Pergunta	4.15	63
Afirmção	3.7.23	36	PERGUNTA	4.16	63
Afirmção	3.7.24	36	PERGUNTA	4.17	63

Tabela 4.7 :

" Índice de símbolos "

Conforme mencionamos na página 8 e também na 24 , apresentamos aqui, na ordem em que foram definidos, os símbolos utilizados nesta dissertação.

SÍMBOLO	≡ SIGNIFICADO	Pg - Li
$A-B$	$\equiv \{x : x \in A \text{ e } x \notin B\}$	10 - 6
$ A $	$\equiv$ cardinalidade de A	10 - 8
ω	$\equiv$ inteiros não negativos	10 - 9
$\mathbb{Z}$	$\equiv$ inteiros	10 - 11
$\underline{k}$	$\equiv \{x : k > x \in \omega\}$	10 - 12
$\aleph_0$	$\equiv$ cardinalidade dos enumeráveis	10 - 13
$\aleph_1$	$\equiv$ cardinalidade dos reais	10 - 14
$n m$	$\equiv n$ é fator de m	10 - 15
$n \nmid m$	$\equiv m$ não é múltiplo de n	10 - 16
$\{x_k\}$	$\equiv \underline{x} \cap \{x+kt : k \in \mathbb{Z}\}$	10 - 19
mdc	$\equiv$ máximo divisor comum	10 - 24
(a, b)	$\equiv mdc$ entre a e b	10 - 24
$[a, b]$	$\equiv mmc$ entre a e b	11 - 2
mmc	$\equiv$ mínimo múltiplo comum	11 - 2
$S(n)$	$\equiv$ menor fator primo de n	11 - 5
$M(n)$	$\equiv mmc\{2, 3, \dots, n\}$	11 - 6
$Dom(f)$	$\equiv$ domínio de f	11 - 9
$Im(f)$	$\equiv$ imagem de f	11 - 9
$Mnd(f)$	$\equiv Dom(f) \cup Im(f)$	11 - 11
$f \upharpoonright A$	$\equiv$ restrição de f a A	11 - 13
$F[A]$	$\equiv \{f(x) : x \in A\}$	11 - 14

(continua)

conexa	$\equiv$ relação conexa	pg 11 - 16
$\text{Pr}t(X)$	$\equiv \{f : f \text{ é função com } \text{Mnd}(f) \subseteq X\}$	11 - 21
X_X	$\equiv \{f : f \in \text{Pr}t(X) \text{ com } \text{Dom}(f) = X\}$	11 - 21
$S_X = \text{Sym}(X)$	$\equiv \{f : f \text{ é permutação de } X\}$	11 - 22
$\text{Pr}t$	$\equiv \{\text{Pr}t(X) : X \text{ é conjunto}\}$	12 - 4
Myc	$\equiv \{X_X : X \text{ é conjunto}\}$	12 - 4
Sym	$\equiv \{S_X : X \text{ é conjunto}\}$	12 - 4
fg	$\equiv$ composição de f com g	12 - 8
f^2	$\equiv ff$	12 - 14
f^n	$\equiv ff \dots f \quad (n \text{ vezes})$	12 - 14
f^0	$\equiv$ relação identidade	12 - 16
f^{-1}	$\equiv$ relação inversa	12 - 18
$f \approx g$	$\equiv$ isomorfismo bigráfico	12 - 22
dcp	$\equiv$ disjunto como permutação	13 - 9
ciclo	$\equiv$ componente cíclica da permutação	13 - 16
$\ f\ $	$\equiv$ comprimento do ciclo f	13 - 18
k -ciclo	$\equiv$ ciclo de comprimento k	13 - 22
$(a \ b \ c \ d)$	$\equiv a \rightarrow b \rightarrow c \rightarrow d \rightarrow a$	13 - 24
c_k	$\equiv k$ -ciclo $(0 \ 1 \ 2 \ \dots \ k-1)$	14 - 6
s	$\equiv$ permutação sucessora $x \rightarrow x+1$	14 - 7
$C_X(f)$	$\equiv$ componentes cíclicas de f em X	14 - 18
$(x \ y)$	$\equiv$ transposição $x \leftrightarrow y$	15 - 9
A_X	$\equiv \{f : f \text{ é permutação par de } X\}$	15 - 17
$C_X(f; m)$	$\equiv$ componentes m -cíclicas de f em X	15 - 23
Xf	$\equiv$ suporte de f em X	16 - 1
ponto fixo	$\equiv f(x) = x \in X - Xf$	16 - 5
$\text{ord}(f) = n$	$\equiv f^n = \text{identidade} \neq f^i \text{ para } 0 < i < n$	16 - 9
Σ	$\equiv$ alfabeto $\{A, B, C, \dots, L, U, V\}$	17 - 9
Σ^+	$\equiv$ palavras de semigrupo	17 - 11
Σ^+	$\equiv$ palavras de grupo	17 - 12

$\alpha\beta$	$\equiv$ concatenação das palavras α e βpg 17 - 17
α^n	$\equiv \alpha\alpha\alpha\dots\alpha$ (n vezes) 17 - 20
α^0	$\equiv$ palavra vazia ϕ 17 - 21
α^{-1}	$\equiv$ palavra inversa 17 - 22
$\bar{\alpha}$	$\equiv$ soletração reversa de α 17 - 24
segmento	$\equiv$ trecho da soletração de palavras 18 - 5
bloco	$\equiv$ segmento máximo da forma L^n 18 - 11
$q(L, \alpha)$	$\equiv$ quantidade de L em α 19 - 11
$ \alpha $	$\equiv$ comprimento de α 19 - 13
$\text{mdc}(\alpha)$	$\equiv \text{mdc}\{q(L, \alpha) : L \in \Sigma\}$ 19 - 13
α trivial	$\equiv \text{mdc}(\alpha) = 1$ 19 - 18
vulnerável	$\equiv \text{mdc}(\alpha) \neq \text{mdc}\{q(L, \alpha) : L \in \Sigma - \{B\}\}$ 19 - 21
$\alpha = \beta$	$\equiv \alpha = \mu\gamma\gamma^{-1}\lambda$ e $\beta = \mu\lambda$ 19 - 25
redução α	$\equiv \beta$ mais curta tal que $\alpha = \beta$ 20 - 1
$\text{cplx}(\alpha)$	$\equiv$ complexidade de $\alpha = n^\circ$ de blocos 20 - 4
$\alpha \sim \beta$	$\equiv \alpha = \mu\lambda$ e $\beta = \lambda\mu$ 20 - 9
$\alpha/\sim$	$\equiv \{\beta : \alpha \sim \beta\}$ 20 - 13
raiz α	$\equiv \beta$, quando $\beta^n = \alpha$ e $n \geq 1$ 20 - 14
$\pi(\alpha)$	$\equiv$ raiz mais curta de α 20 - 16
primitiva	$\equiv \alpha = \pi(\alpha)$ 20 - 17
simplificar	$\equiv \xi : \Sigma \rightarrow \{A, B\} \cup \{\phi\}$ 21 - 7
$\alpha.W.\beta$	$\equiv \alpha$ é W -equivalente a β 22 - 22
α/W	$\equiv \{\beta : \alpha.W.\beta\}$ 23 - 5
$(\alpha+x)G$	$\equiv \alpha$ representa x em G ; $H(\alpha) = x$ 23 - 8
$\alpha++G$	$\equiv (\alpha+x)G$ para todo $x \in G$ 23 - 10
M -universal	$\equiv \alpha++G$ sempre que $G \in M$ 23 - 12
FM -univer.	$\equiv \alpha++X$ quando $X \in M$ e X é finito 23 - 14
IM -univer.	$\equiv \alpha++Y$ quando $Y \in M$ e Y é infinito 23 - 15
intercalável	$\equiv C_X(\phi; m)$ é ou ϕ ou infinito 30 - 15

REFERÊNCIAS :

- [1] - ARANTE , J.M.C.- Sobre a Sym-universalidade de palavras primitivas , Dissertação de Mestrado , Universidade Federal de Santa Catarina , 1981 .
- [2] - BERTRAM , E.A.- Even permutations as a product of two conjugate cycles , Journal of Combinatorial Theory A, 12(1972) , 368-389 .
- [3] - EHRENFUCHT, A. ;FAJTLOWICZ, S. ;MALITZ, J. ;MYCIELSKI, J. - Some problems on universality of words in group , Algebra Universalis , 11(1980) , 261-263 .
- [4] - EHRENFUCHT, A. ;SILBERGER, D.M.- Decomposing a transformation with an involution , Algebra Universalis , 7(1977) , 179-190 .
- [5] - EHRENFUCHT, A. ;SILBERGER, D.M.- Universal terms of the form $B^n A^m$, Algebra Universalis , 10(1980) , 96-116 .
- [6] - ISBELL, J.R.- On the problem of universal terms , Bull de L'Academie Polonaise des Sciences , XIV(1966) , 593-595 .
- [7] - MC NULTY, G.F.- The decision problem for equational bases of algebras , Annals Math. Logic. , 11(1976) , 1-67 .
- [8] - MOORE, J.T.- Elements of Abstract Algebra , Mac Millan Company , New York , 1967 .

- [9] - ORE, O.- Some remarks on comutatore , Proc. Amer. Math. Soc. , 2(1951) , 301-314 .
- [10] - SILBERGER, D.M.- Borders and roots of a word , Portugaliae Mathematica , 30(1971) , 191-199 .
- [11] - SILBERGER, D.M.- Point universal terms in a free semi-group , Doctoral Dissertation , University of Washington , Seattle , 1973 .
- [12] - SILBERGER, D.M.- When is a term point universal ? , Algebra Universalis , 10(1980) , 135-154 .
- [13] - SILBERGER, D.M.- When is the directed graph fg isomorphic to gf ? , Pure and Applied Mathematical Sciences a ser publicado .
- [14] - SILBERGER, D.M. ; VALENTE, M.L.- Representing the infinite cycle , a ser publicado .
- [15] - VALENTE, M.L.- Sobre a Universalidade de palavras para grupos simétricos , Dissertação de Mestrado , Universidade Federal de Santa Catarina , 1979 .