Esta Tese foi julgada adequada para a obtenção do título de

"MESTRE EM CIÊNCIAS"

especialidade em Matemática, e aprovada em sua forma final pelo Curso de Pós-Graduação em Matemática da Universidade Federal de Santa Catarina

William G. Whitley

Prof. William Glenn Whitley

Coordenador

Banca Examinadora:

Donald Morison Silberger

Prof. Donald Morison Silberger, Ph.D.

Orientador

Prof. Paulo Augusto Silva Veloso, Ph.D.

William G. Whitley

Prof. William Glenn Whitley, Ph.D.

UNIVERSIDADE FEDERAL DE SANTA CATARINA

SOBRE A UNIVERSALIDADE DE PALAVRAS PARA GRUPOS SIMÉTRICOS

Milton Luiz Valente

Setembro - 1979

AGRADECIMENTOS

Ao Professor Donald Morison Silberger por sua criteriosa e segura orientação, por sua dedicação, despreendimento e amizade.

A todos aqueles que são responsáveis pela formação que tenho: meus professores da primeira série do primeiro grau a última disciplina do Pós-Graduação.

Aos colegas de magistério pelo incentivo, apoio e colaboração; pelos exemplos e contra exemplos que me proporcionaram e pelo alto grau de solidariedade.

À Joanete, à Cláudia, à Izabela e ao Junior pelas horas que deles tirei para poder realizar este trabalho.

À Universidade Federal de Santa Catarina que forneceu os meios para a realização do presente trabalho.

Àqueles que há muito Deus me tirou:

Meus Pais

RESUMO

O presente trabalho caracteriza uma nova classe, de tamanho considerável, de palavras no alfabeto de duas letras e de complexidade arbitrária maior que um, que são universais para todo grupo simétrico.

ABSTRACT

The present work characterizes a sizable new class of a words in a two-letter alphabet, and of arbitrary complexity greater than one, which are universal for every symmetric group.

ÍNDICE

INTRODUÇÃO

No estudo de uma classe C das álgebras gerais, que são definidas equacionalmente, Jan Mycielski em 1963 considerou útil identificar aquelas formas equacionais que não fazem distinção entre subclasses de C. Estas formas podem ser denominadas C-universais.

Em particular, para uma dada classe C dos semigrupos quer-se identificar as palavras $W(L_1,\dots,L_n)$ tais que, para cada $S \in C$ e para cada $z \in S$ a equação $z = W(x_1,\dots,x_n)$ apresenta solução para algum $\langle x_1,\dots,x_n\rangle \in S^n$. Tais palavras são ditas C-universais.

O presente trabalho considera, principalmente, as seguintes classes de monóides: A classe FSym de todos os grupos simétricos finitos, a classe ISym de todos os grupos simétricos infinitos e a classe Sym que é a união das anteriores. Nossos três principais resultados oferecem condições suficientes para $W(L_1,L_2)$ ser C-universal para cada uma das três classes acima. Nós obtivemos estes resultados pela extensão de algumas técnicas usadas por A. Ehrenfeucht e D.M. Silberger, que trataram das palavras da forma B^nA^m. Nossa contribuição envolve a consideração de uma família de relações .W. de equivalência em um monóide livre.

CAPÍTULO I - Generalidades

1.1. Preliminares: Neste capítulo introduzimos convenções e notações que utilizaremos no presente trabalho. Além disso apresentamos definições e propriedades específicas da área objeto do estudo realizado. Alguns dos resultados que serão utilizados posteriormente são também listados e demonstrados como lemas ou corolários.

1.2. Notações: Neste trabalho ω denota $\{0,1,2,\ldots\}$ e Z denota $\omega\cup\{n:-n\in\omega\}$. Para $k\in\omega$ o símbolo k também denota o conjunto $\{x:x\in\omega$ e $x<k\}$.

Para um conjunto arbitrário X a expressão $|X|$ denota o número cardinal de X. Assim temos, por exemplo, que para todo $k\in\omega$ segue-se que $|k|=k$ e que $|\omega|=\aleph_0$.

Outros exemplos: $0=\phi$; $5=\{0,1,2,3,4\}$; $5\setminus 3=\{x:x\in 5$ e $x\notin 3\}=\{3,4\}$; $5-3=2=\{0,1\}$. Em geral, para $n\in m\in\omega$ temos que $|m\setminus n|=|m-n|=m-n$ e que $\omega\setminus m=\{m,m+1,m+2,\ldots\}$, e ainda que, $m\omega=\{m,2m,3m,\ldots\}$. Também $Z\setminus 1=Z\setminus\{0\}=\{\ldots,-2,-1,0,1,2,\ldots\}$.

Seja $n\in\omega\setminus 1$. A expressão $n|m$ significa que $m/n\in Z$; isto é; que existe $q\in Z$ tal que $m=nq$. Nesta situação dizemos que n é um divisor ou fator de m, e que m é múltiplo de n. Para $i\in\omega$, quando $n^i|m$ mas $n^{i+1}\nmid m$, então dizemos que n^i divide exatamente m, e anotamos $n^i||m$.

Para $k\in\omega\setminus 1$ e $x\in Z$, a expressão $|x|_k$ denota o único elemento $y\in k$ tal que $k|(x-y)$.

Sejam $k\in\omega\setminus 2$ e $C=\{n_j: j\in k\}\subseteq Z\setminus 1$. Então por máximo divisor comum de C entendemos o elemento máximo do conjunto $\{x: x\in\omega\setminus 1$ e para todo $j\in k$ $(x|n_j)\}$; a expressão $(n_o,n_1,\ldots,n_{k-1})$ denota o maior fator comum de C. Também por menor múltiplo comum de C entendemos o elemento mínimo do conjunto $\{x: x\in\omega\setminus 1$ e para todo $j\in k$ $(n_j|x)\}$; a expressão $[n_o,n_1,\ldots,n_{k-1}]$ denota o menor múltiplo comum de C.

Seja $n\in\omega\setminus 2$. Então $S(n)$ denota o menor fator primo de n e $M(n)$ denota $[2,3,\ldots,n]$. Um par ordenado de inteiros positivos $<n,m>$ é dito par de ehrenfeucht se, e somente se, $M(S(n))\nmid m$ e $M(S(m))\nmid n$.

Observemos que quando $\{n,m\}\subseteq\omega\setminus 1$ segue que $<2n+1,2m+1>$ é par de ehrenfeucht e que $<2n,2m>$ não o é. Outros exemplos: $<12,9>$ não é par de ehrenfeucht, mas $<30,35>$ é par de ehrenfeucht. Além disso, $<m,n>$ é par de ehrenfeucht se, e somente se, $<n,m>$ é par de ehrenfeucht.

Sejam X um conjunto arbitrário e $f\subseteq X\times X$. Seja A um conjunto qualquer. Por $f\restriction A$ denotamos $(A\times X)\cap f$. A expressão $f[A]$ denota $\{y: <x,y>\in f$, para algum $x\in A\}$ enquanto que $Wrld(f)$ denota $Dom(f)\cup Im(f)$. Utilizaremos $Prt(X)$ para denotar $\{f$: f é função com $Wrld(f)\subseteq X\}$. Além disso ${}^X X$ denota $\{f: f\in Prt(X)$ e tal que $Dom(f)=X\}$, enquanto que $Sym(X)$ denota o conjunto de todas as permutações em X. Observemos que $Prt(X)$ é um monóide, que ${}^X X$ é um submonóide de $Prt(X)$ e que, $Sym(X)$ é um subgrupo de ${}^X X$. A composição da relação binária f com a relação binária g será denotada simplesmente por fg. Por $id \restriction X$ nós indicamos $\{\langle x,x\rangle: x\in X\}$. Quando $f\subseteq X\times X$ usaremos f^{o} para denotar $id\restriction X$; f^{o} também denota $id\restriction Wrld(f)$.

Sejam f e g relações binárias. Diremos que f é isomórfica bigraficamente com g se, e somente se, existem um conjunto Y e $h\in Sym(Y)$ tais que $f=\{\langle h(x),h(y)\rangle : \langle x,y\rangle\in g\}$. Quando f é isomórfica bigraficamente com g anotamos $f\approx g$. Além disso temos que $\approx$ é relação de equivalência e que $f\approx f^{-1}$ para qualquer função injetiva f.

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

Observemos que uma família $F\subseteq Sym(X)$ poderá ser dcp sem ser "disjunta aos pares". Por outro lado, F pode ser "disjunta aos pares" sem ser dcp.

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

Demonstração: Se $f=g$, então $fg=gf$. Portanto suporemos que $f\neq g$. Seja $x\in X$. Se $f(x)=x=g(x)$, então $fg(x)=gf(x)$. Desta forma, sem perda de generalidade, suponhamos que $x\neq f(x)$. Então, como F é dcp, temos que $x=g(x)$. Além disso $f(x)\neq ff(x)$ pois $f\in Sym(X)$. Segue-se que $gf(x)=f(x)$ porque F é dcp. Logo $gf(x)=fg(x)$. (F.P.)

Seja F dcp, com $F \subseteq Sym(X)$. A expressão ΠF denota o subconjunto de $X \times X$ cujos elementos são todos os $\langle x,y \rangle$ tais que para todo $f \in F(x=f(x)=y)$ ou existe $f \in F(x \neq f(x)=y)$.

1.4. Corolário: Seja F dcp, com $F \subseteq Sym(X)$. Então $\Pi F \in Sym(X)$.

Demonstração: Temos que $Dom(\Pi F)=X \supseteq Im(\Pi F)$. Seja $y \in X$. Se $y=f(y)$ para toda $f \in F$, então $\langle y,y \rangle \in \Pi F$. Por outro lado, se $y \neq f(y)$ para algum $f \in F$, então $\langle f^{-1}(y),y \rangle \in \Pi F$, portanto, $y \in Im(\Pi F)$. Segue-se que $X=Im(\Pi F)$. Desde que $\Pi\{f\}=f$ para $f \in Sym(X)$, e que $\Pi\phi=id \restriction X$, podemos supor que $|F|>1$.

Se $y=f(t)$ para todo $f \in F$, então $\langle y,t \rangle \in \Pi F$ se e somente se $y=t$. Suponhamos que existe $g \in F$ tal que $y \neq g(y)$. Então $\langle y,y \rangle \notin \Pi F$ mas $\langle y,g(y) \rangle \in \Pi F$. Além disso, F não contém mais do que um elemento f tal que $y \neq f(y)$, porque F é dcp. Segue-se que $\langle y,g(y) \rangle$ é o único elemento em ΠF tendo y como primeira coordenada. Portanto f é uma função.

Seja $\Pi F(x)=z=\Pi F(y)$. Admitamos que $x \neq y$. Então sem perda de generalidade suponhamos que $y \neq z$. Logo, existe $g \in F$ tal que $z=g(y)$. Se $x=f(x)$ para todo $f \in F$, então $g(x)=x=\Pi F(x)=z=g(y)$, e consequentemente $x=y$ porque $g \in Sym(X)$. Portanto, existe $h \in F$ tal que $x \neq h(x)=z$. Resumindo vimos que $x \neq h(x)=z=g(y) \neq y$. Se $h=g$, então $x=y$ porque $h \in Sym(X)$. Segue-se que $h \neq g$. Desta forma, F sendo dcp temos que $x=g(x)$ e que $y=h(y)$. Logo, pelo Lema 1.3, inferimos que $gh(x)=hg(x)=h(x)=z=g(y)=gh(y)$, e portanto que $x=y$ porque $gh \in Sym(X)$. Desta contradição concluimos que ΠF é injetiva. Portanto ΠF é uma permutação de X. (F.P.)

Observação: $f\subsetneq X\times X$ se, e somente se, f é um digrafo (grafo direto) cujo conjunto dos vértices é o subconjunto Wrld(f), de X.

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

Seja $g\subseteq X\times X$. Então g é chamado subdigrafo de f se, e somente se, $g\subseteq f$.

Denominamos $id\restriction X$ ciclo trivial em X, ou 1-ciclo em X, ou ciclo de comprimento 1 em X.

Seja $id\restriction X\neq f\in Sym(X)$. Chamamos f ciclo não trivial em X se, e somente se, existir exatamente um $g\subseteq f$ tal que (1) $|g|>1$, tal que (2) g é conexo, e tal que (3) se $g\subseteq h\subseteq f$ e se h é conexo, então $g=h$.

Quando f é um ciclo não trivial cujo subdigrafo maximal conexo é g como no parágrafo anterior, então f é chamado $|g|$-ciclo em X, ou ciclo de comprimento $|g|$ em X.

Observações: Se g não é finito então $|g|=\aleph_0$. Neste caso chamamos f ciclo infinito em X, ou ω-ciclo em X. De outra forma, f é dito ciclo finito em X.

Se $f\in Sym(X)$ é conexo, então f é ciclo em X. O recíproco não é verdadeiro.

1.5. Lema: Seja $id\restriction X \neq f \subsetneq Sym(X)$. Então existe exatamente uma família F dos ciclos não triviais em X tal que F é dcp e tal que $f=\Pi F$.

Demonstração: Seja $G=\{g: g\subseteq f, |g|>1, g$ é conexo e $((g\subseteq h\subseteq f$ e h é conexo) implica que $g=h)\}$. Para cada $g\in G$ seja $c(g)=g \cup id\restriction(X\setminus Wrld(g))$. Seja $F=\{c(g): g\in G\}$. Então F é uma família dcp dos ciclos não triviais em X tal que $f=\Pi F$.

Seja F_1 uma família dcp dos ciclos não triviais em X tal que $f=\Pi F_1$. Temos que demonstrar que $F_1=F$.

Escolhamos $h_1\in F_1$. Existe $g_1\subseteq h_1$ tal que $|g_1|>1$, tal que g_1 é conexo, e tal que se $g_1\subseteq h\subseteq h_1$ e se h é conexo, então $g_1=h$.

Seja $<x,y>\in g_1$. Sendo $|g_1|>1$, e sendo g_1 um subdigrafo conexo da permutação h_1 de X, então $x\neq y$. Desde que $x\neq g_1(x)=h_1(x)=y$, segue-se que $f(x)=(\Pi F_1)(x)=y\neq x$. Assim vimos que $g_1\subseteq f$, e também que existe $h=c(g)\in F$ para $g\in G$ tal que $<x,y>=<x,f(x)>\in g_1\cap g$. Observe que $g_1\subseteq g_1\cup g\subseteq f$ e que $g_1\cup g$ é conexo. Portanto $g\subseteq g_1$, logo $g=g_1$. Lembrando que h_1 é um ciclo em X, concluimos que $h=h_1$. Demonstámos que $F_1\subseteq F$. Semelhantemente inferimos que $F\subseteq F_1$. (F.P.)

Seja f um ciclo não trivial em X e seja g o subconjunto (unicamente determinado) de f tal que $|g|>1$, tal que g é conexo, e tal que se h é conexo e se $g\subseteq h\subseteq f$ então $g=h$. Temos basicamente dois casos a considerar:

I: $|g|=k\in\omega$. Então existe uma injeção $i\to x_i$ de k em X, e g tem a forma $x_o\to x_1\to\ldots\to x_{k-1}\to x_o$. Escreveremos $f=(x_o\ x_1\ \ldots\ x_{k-1})$.

II: $|g|=\aleph_o$. Então existe uma injeção $i\to x_i$ de Z em X e g tem a forma $x_i\to x_{i+1}$ para todo $i\in Z$. Escreveremos $f=(\ldots x_{-2}\ x_{-1}\ x_o\ x_1\ x_2\ldots)$.

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

Seja $f\in Sym(X)$. Então $V'(f)$ denota ϕ se $f=id\restriction X$. Se $f\neq id\restriction X$, então $V'(f)$ denota a unicamente determinada família F tratada no Lema 1.5. Os elementos de $V'(f)$ são chamados "componentes não triviais de f".

A expressão $V(f)$ denota $V'(f)\cup\{(x): f(x)=x\in X\}$. Pretendemos, nesta definição, "contar" (incluir em $V(f)$) a identidade $id\restriction f$ exatamente uma vez para cada ponto $x\in X$ que é fixado por f. Cada tal (x) é chamada "uma componente trivial de f".

Exemplo: Seja $f=(0\ 1)(2\ 3)(4\ 5\ 6)$, com $f\in Sym(X)$. Quando $X=7$, então $V(f)=V'(f)=\{(0\ 1),(2\ 3),(4\ 5\ 6)\}$ e $|V(f)|=3$. Mas, por outro lado, quando $X=9$, então $V(f)=V'(f)\cup\{(7),(8)\}=\{(0\ 1),(2\ 3),(4\ 5\ 6),(7),(8)\}$, e $|V(f)|=5$.

Seja $f\in Sym(X)$. Então $\Lambda(f)$ denota $\{|g|:c(g)\in V'(f)\}\cup T$, com $T=\phi$ se $x\neq f(x)$ para cada $x\in X$, mas com $T=\{1\}$ se existe $x\in X$ tal que $x=f(x)$.

Observação: No exemplo anterior $\Lambda(f)=\{2,3\}$ quando $X=7$, mas $\Lambda(f)=\{1,2,3\}$ quando $X=9$.

No caso em que $f\in Sym(X)$ e $f^2=id\restriction X$, f é chamada uma involução de X. Segue-se que $f\in Sym(X)$ é uma involução se, e somente se, $\Lambda(f)\subseteq\{1,2\}$.

Observação: Para $f\in Sym(X)$ e $n\in Z$ temos que $|V(f)|\leq|V(f^n)|$ porque as potências de f não podem "ligar" componentes distintas de f.

Por convenção $\pi\phi=id\restriction X$ quando X é definido.

1.6. Corolário: Seja $k\in\omega$. Seja $f\in Sym(X)$ tal que $|V'(f)|=k$, com $V'(f)=\{g_i:i\in k\}$. Então para cada $h\in Sym(k)$ temos que $f=g_{h(o)}g_{h(1)}\cdots g_{h(k-1)}=g_o g_1\cdots g_{k-1}$.

Demonstração: Suporemos que $k>1$. Suporemos também que para todo conjunto Y e para todo $\mu\in Sym(Y)$ com $m=|V'(\mu)|<k$ e $V'(\mu)=\{v_i: i\in m\}$ acontece que $\mu=v_o v_1\cdots v_{m-1}=v_{H(o)}\cdots v_{H(m-1)}$ para todo $H\in Sym(m)$.

Escolhamos, agora, $h\in Sym(k)$. Existe $j\in k$ tal que $h(j)=k-1$. Seja $H_1=h(j\ k-1)$, e seja $H=H_1\restriction k-1$. Observemos que $H_1(k-1)=k-1=H_1[k-1]=H[k-1]$. Assim vimos que $H\in Sym(k-1)$.

Seja $\mu=g_o g_1\cdots g_{k-2}$. Então, por hipótese de indução, $\mu g_{k-1}=g_o\cdots g_{k-2}g_{k-1}=g_{H(0)}\cdots g_{H(k-2)}g_{k-1}=g_{H_1(0)}\cdots g_{H_1(k-2)}g_{H_1(k-1)}$. Segue,se pelo Lema 1.3, aplicado $(k-1-j)(k-2-j)$ vezes, que $\mu g_{k-1}=g_{h(0)}\cdots g_{h(k-2)}g_{h(k-1)}$.

Mas $V'(\mu)=\{g_i : i\in k-1\}$ é dcp, e também $\{\mu, g_{k-1}\}$ é dcp. Portanto, se $g_{k-1}(x)\neq x$, então $\mu(x)=x$ e $f(x)=\pi V'(f)(x)=(\pi V'(\mu))g_{k-1}(x)=g_{k-1}\pi V'(\mu)(x)=g_{k-1}(x)$. Semelhantemente, se $g_{k-1}(x)=x$, então $f(x)=(\pi V'(\mu))g_{k-1}(x)=(\pi V'(\mu))(x)=\mu(x)$. Inferimos que $f=\mu g_{k-1}$, e portanto, que $f=g_{h(o)}\cdots g_{h(k-2)}g_{h(k-1)}$. O corolário segue por indução. (F.P.)

Seja X um conjunto arbitrário. Uma permutação $f\in \mathrm{Sym}(X)$ é dita cíclica se, e somente se, $|V(f)|=1$.

Para cada $k\in\omega\setminus 1$ a expressão c_k significa a permutação cíclica $(0\ 1\ \ldots\ k-1)$ do conjunto k. Além disso a expressão s denota $(\ \ldots -2\ -1\ \ 0\ \ 1\ \ 2\ldots)$. Verifiquemos que $\Lambda(c_k)=\{k\}$, $\Lambda(s)=\{\aleph_o\}$, $|V(c_k)|=1=|V(s)|$. Para $n\in\omega$ e para todo $x\in k$, temos que $c_k^n=|x+n|_k$. Segue se que $c_k^k=c_k^o=id\restriction k$. Também que, para $\{t,p\}\subseteq Z$ $c_k^{pk+t}=c_k^t$.

1.7. Lema: Seja $\{n,k\}\subseteq\omega\setminus 1$, com $(n,k)=1$. Então existe uma permutação cíclica $f\in \mathrm{Sym}(k)$ tal que $f^n=c_k$. Além disso, a permutação c_k^n é cíclica.

Demonstração: Por [1, Theorem 1] existem inteiros x e y tais que $nx+ky=1$. Segue que $c_k=c_k^{nx+ky}=(c_k^x)^n(c_k^k)^y=(c_k^x)^n id\restriction k=(c_k^x)^n$. Seja $f=c_k^x$. Então, $c_k=f^n$, e $f\in \mathrm{Sym}(k)$. Observando também que $1\leq|V(f)|\leq|V(f^n)|=|V(c_k)|=1$, vemos que a permutação f do conjunto k é cíclica. Finalmente observamos que c_k^{nx} não é cíclica se c_k^n não é cíclica. Mas $c_k^{nx}=c_k$. Portanto, c_k^n é cíclica. (F.P.)

1.8. Lema: Sejam $\{k,n\}\subseteq\omega\setminus 1$ e $j=(n,k)$. Então $\Lambda(c_k^n)=\{k/j\}$ e $|V(c_k^n)|=j$.

Demonstração: Consideremos primeiramente o caso especial, $n|k$. Existe $q\in\omega\setminus 1$ tal que $k=nq$. Então $c_k^n=(0\ 1\ \ldots\ nq-2\ nq-1)^n$ tem a componente $(i\ i+n\ \ldots\ i+(q-1)n)$ para cada $i\in n$. Segue-se que $\Lambda(c_k^n)=\{q\}=\{k/n\}$, e que $|V(c_k^n)|=n$.

Do parágrafo anterior temos que $\Lambda(c_k^j)=\{k/j\}$ e que $|V(c_k^j)|=j$. Sejam $g_o,g_1,\ldots,g_{j-1}$ os j subdigrafos maximais conexos do digrafo c_k^j. Para cada $i\in j$ a função g_i é uma permutação cíclica de $Dom(g_i)$. Também, $|Dom(g_i)|=k/j$. Observando que $(k/j,n/j)=(k,n)/j=1$, vemos, pelo Lema 1.7, que $g_i^{n/j}$ é uma permutação cíclica de $Dom(g_i)$, para cada $i\in j$. Então, $c_k^n=(c_k^j)^{n/j}=(\bigcup\{g_i:i\in j\})^{n/j}=\bigcup\{g_i{}^{n/j}: i\in j\}$. Concluimos que $\Lambda(c_k^n)=\{k/j\}$, e portanto que c_k^n tem exatamente $k/(k/j)=j$ componentes, e que cada tal componente é um ciclo de comprimento k/j. (F.P.)

1.9. Desdobramento de ciclos: Seja $c=(x_o\ x_1\ \ldots\ x_{q-1})$ um ciclo em um conjunto arbitrário. Seja $\{i,j\}\subseteq\omega$ tal que $i<j<q-1$. Então a operação $c\mapsto c(x_i\ x_j)$ "desdobra" (ou "quebra") o q-ciclo c em um (q+i-j)-ciclo $(x_o\ \ldots\ \underline{x_i}\ x_{j+1}\ldots x_{q-1})$ e em um (j-i)-cíclo $(x_{i+1}\ x_{i+2}\ \ldots\ \underline{x_j})$. Observemos que x_i e x_j aparecem sublinhados para indicar que x_i e x_j são pontos de c "usados por $(x_i\ x_j)$". É claro que cada um dos ciclos obtidos pode ser novamente quebrado.

A "quebra" $c \to c(x_i\ x_j)$ observada acima é um só tipo de transformação $\mathrm{Sym}(X) \to \mathrm{Sym}(X)$ que iremos empregar para mudar a forma digráfica de c. Realmente, para esta finalidade, vamos empregar uma sequência $c \to cf_0 \to cf_0 f_1 \to \ldots \to cf_0 f_1 \ldots f_{p-1}$ das transformações de Sym(X). O nosso motivo em apontar os pontos"usados por cada f_i" com $i \in p$, é para garantir que a família $\{f_i : i \in p\}$ seja dcp. Na figura 3 do apêndice vemos duas quebras, de um ciclo, por dois ciclos disjuntos.

1.10. Encurtamento de ciclos: Sejam $c=(x_0\ x_1\ \ldots\ x_{q-1})$ e $\{i,j\} \subseteq \omega$ tal que $i<j<q$. A operação $c \to c(x_j\ x_{j-1} \ldots x_{i+1}\ x_i)$ "encurta" o q-ciclo c de exatamente $j-i$. Isto é, resulta em um $(q-(j-i))$-ciclo e em $(j-i)$ pontos fixados por $(x_j\ x_{j-1} \ldots\ x_{i+1}\ x_i)$. Observemos que $(x_j\ x_{j-1}\ \ldots\ x_{i+1}\ x_i)$ é de comprimento $j-i+1$, e também que o $(q-j+i)$-ciclo $(x_0\ x_1\ \ldots\ \underline{x_i}\ x_{j+1} \ldots x_{q-1})$ terá exatamente um ponto "usado por $(x_j\ x_{j-1}\ \ldots\ x_{i+1}\ x_i)$". Vemos que se $i=0$ e $j=q-1$ na operação anterior, teremos destruído o ciclo c completamente, passando a ter q pontos fixos. (Figura 4 do apêndice).

1.11. Estudo das palavras: Seja $\Sigma=\{A,B,C,\ldots\}$ um alfabeto fixo, finito e arbitrário. Designaremos por Σ^* ao monóide das palavras finitas no alfabeto Σ. Os elementos de Σ^*, denominados palavras, serão denotados por letras gregas minúsculas. A letra ϕ denotará a palavra vazia. Quando $\{\alpha,\beta\} \subseteq \Sigma^*$, então $\alpha\beta$ significa a palavra construída pela concatenação de α e β.

Exemplos: $\alpha\phi=\phi\alpha=\alpha$. Se $\alpha=ABA$ e $\beta=BBA$ então $\alpha\beta=ABABBA$ enquanto que $\beta\alpha=BBAABA$.

Observação: Para todo $\{\alpha,\beta,\gamma\}\subseteq\Sigma^*$ temos que $(\alpha\beta)\gamma=\alpha(\beta\gamma)$. Porém $\alpha\beta=\beta\alpha$ nem sempre é válido. Basta ver o exemplo anterior.

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

Exemplos: Se $\alpha=AABBBA=A^2B^3A$ então $|\alpha|=6$. Se $\beta=L^n$ para $L\in\Sigma$ e $n\in\omega$, então $|\beta|=n$.

Por $\overline{\alpha}$ denotamos a palavra formada pelos mesmos elementos que compõe α, concatenados em ordem inversa.

Exemplos: $\phi=\overline{\phi}$; $L^n=\overline{L^n}$ para todo $L\in\Sigma$ e todo $n\geqslant 1$. Se $\alpha=A^2B^3CAB^4$ então $\overline{\alpha}=B^4ACB^3A^2$. Além disso, para todo $\alpha\in\Sigma^*$, temos que $|\overline{\alpha}|=|\alpha|$.

Uma palavra não vazia β é dita raiz de $\alpha\in\Sigma^*$ se, e somente se, $\alpha=\beta^n$ para algum inteiro positivo n. Vemos que toda palavra $\alpha\neq\phi$ admite exatamente uma raiz de menor comprimento, que é denominada raiz primitiva de α, e é anotada por $\pi(\alpha)$. Uma palavra $\alpha\neq\phi$ é primitiva se, e somente se, $\alpha=\pi(\alpha)$. Caso contrário, isto é, quando $\alpha\neq\pi(\alpha)$, denominaremos α não primitiva. Observemos que $\pi(\pi(\alpha))=\pi(\alpha)$ para toda $\alpha\in\Sigma^*\setminus\{\phi\}$.

Exemplos: $\pi(L^n)=L$, para todo $L\in\Sigma$. Se $\alpha=AB^2AB^2AB^2AB^2AB^2AB^2=(AB^2)^6$ então AB^2, $(AB^2)^2$ e $(AB^2)^3$ são raízes de α e $\pi(\alpha)=AB^2$.

A palavra $\beta=A^2B^3C$ é primitiva pois $\pi(\beta)=A^2B^3C=\beta$.

Para cada $L\in\Sigma$ a expressão $Mult(L,\alpha)$ denota o conjunto de todas as posições nas quais a letra L ocorre para a formação da palavra α.

Uma palavra α é dita não trivial se, e somente se, $|Mult(L,\alpha)|\neq 1$ para todo $L\in\Sigma$.

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

Exemplos: Se $\alpha=A^2B^3AB$ então $Mult(A,\alpha)=\{1,2,6\}$ pois A ocorre nas "posições" 1,2 e 6 da palavra α; $Mult(B,\alpha)=\{3,4,5,7\}$; $|Mult(A,\alpha)|=3$ e $|Mult(B,\alpha)|=4$ logo α é não trivial. Além disso $gcd(\alpha)=1$. Se $\beta=A^2B^3A^5B^4$ então $gcd(\beta)=7$.

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

Demonstração: [8, Lemma 2.2.] (Ver apêndice, página 50)

1.13. Bordos: Uma palavra $\beta\neq\phi$ é denominada segmento de $\alpha\in\Sigma^*$ se, e somente se, $\alpha=\lambda\beta\delta$ para algum $\{\lambda,\delta\}\subseteq\Sigma^*$. A palavra β é dita segmento a direita (respectivamente, segmento a esquerda) de α se, e somente se, $\alpha=\lambda\beta$ ($\alpha=\beta\lambda$) para algum $\lambda\in\Sigma^*$. Se β é segmento de α tal que $0<|\beta|<|\alpha|$ então β é chamado segmento próprio de α. Uma palavra β é dita bordo de α se, e somente se β é, ao mesmo tempo, segmento próprio a direita e a esquerda de α.

Exemplo: Se $\alpha=A^2B^3CDA^2B$ então $\beta=A^2B$ é bordo de α pois, sendo $\lambda_1=B^2CDA^2B$ e $\lambda_2=A^2B^3CD$ segue-se que $\alpha=\beta\lambda_1=\lambda_2\beta$. Além disso $0<|\lambda_1|=7=|\lambda_2|<10=|\alpha|$.

Uma palavra $\beta\neq\phi$ é chamada bordo curto de $\alpha\in\Sigma^*$ se, e somente se, $\alpha=\beta\gamma\beta$ para algum $\gamma\in\Sigma^*$.

Exemplo: α=ABABABA tem bordos A, ABA e ABABA. Porém os bordos curtos de α são apenas A e ABA. Observemos que um bordo β de α é curto se, e somente se, $2|\beta|\leqslant|\alpha|$.

1.14. Lema: Seja $\{\alpha,\beta,\gamma,\delta\}\subseteq\Sigma^*$ e seja $\alpha\beta=\gamma\delta$ com $|\alpha|\leqslant|\gamma|$. Então existe $\mu\in\Sigma^*$ tal que $\alpha\mu=\gamma$ e $\beta=\mu\delta$.

Demonstração: A existência de $\mu\in\Sigma^*$ tal que $\alpha\mu=\gamma$ é óbvia. Desta forma $\alpha\beta=\alpha\mu\delta$ e, portanto, $\beta=\mu\delta$. (F.P.)

1.15. Proposição: Uma palavra $\alpha\in\Sigma^*$ tem bordo se, e somente se, α tem bordo curto.

Demonstração: Temos que um bordo curto de α é também bordo de α. A recíproca é menos trivial.

Suponhamos que α admite um bordo β_1 e que $2|\beta_1|>|\alpha|$. Temos assim que $\lambda_1\beta_1=\alpha=\beta_1\rho_1$ para algum $\{\lambda_1,\rho_1\}\subseteq\Sigma^*\setminus\{\phi\}$. Notemos que $2|\beta_1|>|\alpha|=|\lambda_1\beta_1|=|\lambda_1|+|\beta_1|$. Assim $|\lambda_1|<|\beta_1|$ e, pelo Lema 1.14, existe $\beta_2\in\Sigma^*\setminus\{\phi\}$ tal que $\lambda_1\beta_2=\beta_1=\beta_2\rho_1$. Então $0<|\beta_2|<|\beta_1|$ e também, $\lambda_1{}^2\beta_2=\lambda_1\beta_1=\alpha=\beta_1\rho_1=\beta_2\rho_1{}^2$. Assim β_2 é bordo de α. De modo análogo obteríamos bordos $\beta_3,\beta_4,\ldots$ de α tais que $|\beta_1|>|\beta_2|>|\beta_3|>\ldots$ A sequência de bordos $\beta_1,\beta_2,\beta_3,\ldots$ tem que ser finita, portanto admite um último termo β_j. Mas $2|\beta_j|\leqslant|\alpha|$ porque, caso contrário, β_j não seria o último elemento da sequência. Concluímos então que β_j é bordo curto de α. (F.P.)

1.16. Complexidade de uma palavra: Sejam $\{\alpha,\lambda\}\subseteq\Sigma^*$, $L\in\Sigma$ e $n\in\omega\setminus 1$. O par ordenado $\langle\lambda,L^n\rangle$ é dito L-bloco de tamanho n de α se e somente se:

(i) λL^n é segmento a esquerda de α;

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

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

Quando $\langle\lambda,L^n\rangle$ for bloco de α, então L^n é dito segmento individual máximo de α.

Denominamos complexidade de uma palavra $\alpha\in\Sigma^*$ ao número de blocos distintos de α.

Exemplos: Se $\alpha=AB^2A^3B^2$ então seus segmentos individuais máximos são A, B^2 e A^3. Os blocos de α são $\langle\phi,A\rangle$, $\langle A,B^2\rangle$, $\langle AB^2,A^3\rangle$ e $\langle AB^2A^3,B^2\rangle$. Portanto a complexidade de α é 4. Se $L\in\Sigma^*$ e $n\geqslant 1$ então a complexidade de L^n é 1. Com $\{A,B\}\subseteq\Sigma^*$ e para $\{m,p,n\}\subseteq\omega\setminus 1$ temos que A^nB^m tem complexidade 2 enquanto que $B^nA^mB^p$ tem complexidade 3.

1.17. Palavras ciclicamente equivalentes: Seja $\{\alpha,\beta\}\subseteq\Sigma^*$. Anotamos $\alpha\sim\beta$ para indicar que α é ciclicamente equivalente a β. Dizemos que $\alpha\sim\beta$ se e somente se existir $\{\mu,\lambda\}\subseteq\Sigma^*$ tal que $\alpha=\mu\lambda$ enquanto que $\beta=\lambda\mu$.

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

1.18. Proposição: A relação $\sim$ é relação de equivalência em Σ^*.

Demonstração: (i) $\alpha=\phi\alpha=\alpha\phi=\alpha$; logo $\alpha\sim\alpha$, para todo $\alpha\in\Sigma^*$.

(ii) Se $\alpha\sim\beta$ então $\alpha=\lambda\mu$ e $\beta=\mu\lambda$ para algum $\{\mu,\lambda\}\subseteq\Sigma^*$. Assim $\beta=\mu\lambda$ enquanto que $\alpha=\lambda\mu$. Temos então que $\beta\sim\alpha$.

(iii) Sejam $\alpha\sim\beta$ e $\beta\sim\gamma$. Então existe $\{\mu_1,\mu_2,\lambda_1,\lambda_2\}\subseteq\Sigma^*$ tal que $\alpha=\mu_1\lambda_1$, $\lambda_1\mu_1=\beta=\mu_2\lambda_2$ e $\gamma=\lambda_2\mu_2$. Há dois casos a considerar:

1º caso: $|\mu_1\mu_2|\leqslant|\alpha|$. Temos que $|\lambda_1|=|\alpha|-|\mu_1|\geqslant |\mu_1\mu_2|-|\mu_1|=|\mu_1|+|\mu_2|-|\mu_1|=|\mu_2|$. Além disso $\lambda_1\mu_1=\mu_2\lambda_2$ e, como $|\mu_2|\leqslant|\lambda_1|$, pelo Lema 1.14 segue-se que existe $\mu_3\in\Sigma^*$ tal que $\mu_2\lambda_3=\lambda_1$ e tal que $\lambda_2=\lambda_3\mu_1$. Anotando $\mu_1\mu_2=\mu_3$ temos que $\mu_3\lambda_3=\mu_1\mu_2\lambda_3=\mu_1\lambda_1=\alpha$. Por outro lado $\gamma=\lambda_2\mu_2=\lambda_3\mu_1\mu_2=\lambda_3\mu_3$. Portanto, neste caso temos que $\alpha\sim\gamma$.

2º caso: $|\mu_1\mu_2|>|\alpha|$. Temos que $|\mu_1|+|\lambda_1|=|\mu_1\lambda_1|=|\alpha|<|\mu_1\mu_2|=|\mu_1|+|\mu_2|$ e portanto, que $|\lambda_1|<|\mu_2|$. Lembrando que $\lambda_1\mu_1=\mu_2\lambda_2$ temos, pelo Lema 1.14, que existe $\mu_3\in\Sigma^*$ tal que $\lambda_1\mu_3=\mu_2$ e $\mu_1=\mu_3\lambda_2$. Seja $\lambda_3=\lambda_2\lambda_1$. Então $\alpha=\mu_1\lambda_1=\mu_3\lambda_2\lambda_1=\mu_3\lambda_3$. Por outro lado $\gamma=\lambda_2\mu_2=\lambda_2\lambda_1\mu_3=\lambda_3\mu_3$. Assim também para $|\mu_1\mu_2|>|\alpha|$ temos que $\alpha\sim\gamma$. (F.P.)

O símbolo $\alpha/\sim$ denota $\{\beta:\beta\sim\alpha\}$.

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

Demonstração: [8, Lema 3.2].

1.20. Proposição: Seja $\alpha\in\Sigma^*$ tal que $\alpha\neq\phi$. Então $|\alpha/\sim|=|\pi(\alpha)|$.

Demonstração: Consideremos primeiramente o caso $\alpha=\pi(\alpha)$. Admitamos que $\pi(\alpha)=\mu\nu=\mu_1\nu_1$ com $\{\mu,\nu,\mu_1,\nu_1\}\subseteq\Sigma^*$ e $0<|\mu|<|\mu_1|$. Afirmamos que $\nu\mu\neq\nu_1\mu_1$. Observemos que $|\nu|>|\nu_1|$. Supondo que $\nu\mu=\nu_1\mu_1$ pelo Lema 1.14. temos que existe $\gamma\in\Sigma^*\setminus\{\phi\}$ tal que $\nu_1\gamma=\nu$ e $\gamma\mu=\mu_1$. Então $\pi(\alpha)=\mu\nu=\mu\nu_1\gamma$ e $\pi(\alpha)=\mu_1\nu_1=\gamma\mu\nu_1$. Ou seja: $(\mu\nu_1)\gamma=\pi(\alpha)=\gamma(\mu\nu_1)$. Além disso temos que $|\mu\nu_1|\geqslant|\mu|>0$ e $|\gamma|>0$ e, pelo Lema 1.12 segue que $\pi(\gamma)=\pi(\mu\nu_1)=\pi(\alpha)$ o que é impossível já que $|\pi(\gamma)|\leqslant|\gamma|<|\gamma|+|\mu\nu_1|=|\gamma\mu\nu_1|=|\pi(\alpha)|$. Portanto $|\pi(\alpha)/\sim|=|\{\lambda_i\colon\ |\lambda_i|<|\pi(\alpha)|$ e λ_i é segmento a esquerda de $\pi(\alpha)\}|$. Mas, como o número de segmentos a esquerda de $\pi(\alpha)$ é igual a $|\pi(\alpha)|$ conclui-se que $|\pi(\alpha)/\sim|=|\pi(\alpha)|$.

Agora consideremos o caso que $\alpha=\pi(\alpha)^n$ com $n>1$. Consideremos também que $\alpha=\mu\nu=\mu_1\nu_1$ com $|\mu|-|\mu_1|$ múltiplo de $|\pi(\alpha)|$. Segue-se que existe $\{i,j\}\subseteq n$ e existe uma palavra λ tal que $\mu=\pi(\alpha)^i\lambda$ e $\mu_1=\pi(\alpha)^j\lambda$. Vemos então que λ é segmento a esquerda de $\pi(\alpha)$. Assim existe σ tal que $\lambda\sigma=\pi(\alpha)$. Então $\nu=\sigma\pi(\alpha)^{n-1-i}$ e $\nu_1=\sigma\pi(\alpha)^{n-1-j}$. Logo $\nu\mu=\sigma\pi(\alpha)^{n-1-i}\pi(\alpha)^i\lambda=\sigma\pi(\alpha)^{n-1}\lambda$, e semelhantemente $\nu_1\mu_1=\sigma\pi(\alpha)^{n-1}\lambda$. Segue-se que $\nu\mu=\nu_1\mu_1$ quando $|\mu|-|\mu_1|$ é múltiplo de $|\pi(\alpha)|$. Vemos portanto que o número $|\alpha/\sim|$ é igual ao número dos segmentos ν a esquerda de $\pi(\alpha)$. Do parágrafo anterior segue então que $|\alpha/\sim|=|\pi(\alpha)|$. (F.P.)

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

(i) $\alpha_i\sim\alpha_{i+1}$ ou

(ii) existe $\psi\in W$ tal que $\alpha_{i+1}=\alpha_i\psi$ ou

(iii) existe $\psi\in W$ tal que $\alpha_i=\alpha_{i+1}\psi$.

Diremos que a sequência $\alpha=\gamma_o,\gamma_1,\ldots,\gamma_j=\beta$ leva α em β por W.

1.22. Lema: A relação .W. é relação de equivalência em Σ^*.

Demonstração: Decorre da definição e da Proposição 1.18.

O símbolo α/W denota $\{\beta:\beta.W.\alpha\}$.

1.23. Universalidade de uma palavra para um semigrupo. Seja $\alpha\in\Sigma^*\setminus\{\phi\}$. Seja S um semigrupo e seja $x\in S$. Dizemos que α representa x em S, e anotamos $(\alpha\downarrow x)S$, se existe um homomorfismo $H:\Sigma^*\to S$ tal que $H(\alpha)=x$. Denominamos α universal para S, se e somente se $(\alpha\downarrow x)S$ para todo $x\in S$. Quando α é universal para S escrevemos que $(\alpha\downarrow\downarrow S)$ ou, simplesmente, que é S-universal. (Figuras 1 e 2 do apêndice)

Exemplo: Seja S um semigrupo arbitrário munido da operação $_*$ definida por $a_*b=b$ para todo $\{a,b\}\subseteq S$. Seja $\alpha\in\Sigma^*\setminus\{\phi\}$. Seja $L\in\Sigma$ segmento a direita de α. Então, se $x\in S$ e se $H:\Sigma^*\to S$ é qualquer homomorfismo satisfazendo $H(L)=x$ nós temos que $(\alpha\downarrow x)S$. Basta notar que $\alpha=\beta L$ para algum $\beta\in\Sigma^*\setminus\{\phi\}$ implica em $H(\alpha)=H(\beta L)=H(\beta)_*H(L)=x$. Além disso, como para todo $x\in S$ podemos escolher um homomorfismo $H_x:\Sigma^*\to S$, de modo análogo ao anterior, temos que $(\alpha\downarrow\downarrow S)$ qualquer que seja $\alpha\in\Sigma^*\setminus\{\phi\}$.

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

Neste trabalho, Prt denota $\{Prt(X):X$ é um conjunto$\}$; Myc denota $\{{}^{X}X:X$ é um conjunto$\}$ e Sym denota $\{Sym(X):X$ é um conjunto$\}$.

Observemos que, para mostrar que uma palavra é FSym-universal, basta mostrar que para todo $k\in\omega\setminus 2$, esta palavra representa c_k em Sym(k). Mas, para mostrar que uma palavra é ISym-universal, devemos mostrar também que esta palavra representa s em Sym(Z).

CAPÍTULO II - Termos universais

Preliminares: Em 1963 Jan Mycielski introduziu as noções de "Termo Universal" e de "Junção Universal", dando início ao estudo de uma nova área. Ele perguntou quais palavras são universais para quais monóides; especificamente, quais palavras são universais para todos os monóides simétricos ${}^{X}X$.

O primeiro trabalho publicado, em 1966, so- 19
bre o "problema de Mycielski" é de autoria de J.R. Isbell [5]. Seus principais resultados são os Teoremas 2.1 e 2.2, que listamos abaixo, juntamente com corolários e casos particulares de relevante importância.

2.1. Teorema: Se uma palavra não tem bordos curtos, então é IMyc-universal.

2.2. Teorema: Sejam p primo e $n=p^i$ para algum $i\in\omega\setminus 1$. Então para qualquer X finito e para qualquer $f\in {}^{X}X$ existe uma involução $h\in Sym(X)$ e existe $g\in {}^{X}X$ tal que $f=g^n h$.

(1) Segue-se do Teorema 2.1 que, se $\alpha=A^2B^2$, então α é IMyc-universal. Porém α não é FMyc-universal já que α não é universal para ${}^{2}2$.

(2) Se $\alpha=A^2B^2A$ então α é FMyc-universal.

(3) Se $\alpha=B^{p^k}A^{2n+1}$ ou se $\alpha=B^{2n+1}A^{p^k}$ onde $\{n,p,k\}\subseteq\omega$ e p é primo, então α é Myc-universal.

Neste mesmo artigo Isbell formula algumas perguntas:

(1) São Myc-universais as palavras BA^2BA e BAB^2A, as quais são FMyc-universais?

(2) Se uma palavra α é ${}^XX$-universal para algum X infinito então α é IMyc-universal?

(3) Existe uma palavra α não trivial tal que é possível demonstrar, sem usar o Lema de Zorn, que α é Myc-universal?

Em 1972 G.F.McNulty [6] em sua dissertação de doutoramento, na qual estuda a noção de "Junção Universal", apresenta uma generalização do Teorema 2.1. Ela é a seguinte:

2.3. Teorema: Seja X infinito. Seja $J\subseteq\Sigma^*\setminus\{\phi\}$ tal que para $\{\alpha,\beta\}\subseteq J$ com $\alpha\neq\beta$ acontece que, nem α é segmento de β, nem existe $\mu\neq\phi$ tal que μ é, ao mesmo tempo, segmento a direita de α e segmento a esquerda de β. Seja $H:J\to{}^XX$ função arbitrária. Então existe um homomorfismo $K:\Sigma^*\to{}^XX$ tal que $K\restriction J=H$.

Um outro tipo de generalização do Teorema 2.1 é apresentada por D.M.Silberger [9] em 1973:

2.4. Teorema: Seja α uma palavra que não admite bordos. Então α é IPrt-universal.

Combinando as técnicas das demonstrações dos Teoremas 2.3 e 2.4 Silberger e McNulty, em 1974, provam que:

2.5. Teorema: Sejam X infinito e $J\subseteq\Sigma^*\setminus\{\phi\}$ tal que para $\{\alpha,\beta\}\subseteq J$ com $\alpha\neq\beta$ acontece que, nem α é segmento de β, nem existe $\mu\neq\phi$ tal que μ é, ao mesmo tempo, segmento a direita de α e segmento a esquerda β. Seja $H:J\to Prt(X)$ função arbitrária. Então existe um homomorfismo $K:\Sigma^*\to Prt(X)$ tal que $K\restriction J=H$.

Na caracterização das palavras IMyc-universais é importante citar que, de acordo com vários matemáticos, entre os quais Sierpinski e R.A. McKenzie, basta estudar o alfabeto $\Sigma=\{A,B\}$ de duas letras. Observação mais ampla, de Silberger, afirma que o mesmo sucede para caracterizar palavras que são IPrt-universais.

Observa-se facilmente que, para todo X, se α é Prt(X)-universal então α é ${}^XX$-universal. Desta forma, o principal teorema de [10], de autoria de Silberger, contribui na solução do "problema de Mycielski". Este é:

2.6. Teorema: Seja $\alpha\in\Sigma^*$. Então α é Prt-universal se e somente se α representa f em Prt(Wrld f) para toda função f injetiva e conexa.

Alguns dos resultados decorrentes deste teorema que fazem parte do trabalho são:

(1) Para todo $n\in\omega$ as palavras $(AB)^nA$, $B(BA)^n$ e $(BA)^nA$ são Prt-universais.

(2) B^3A^2 e B^2A^3 são Prt-universais.

(3) Se x e y são inteiros ímpares positivos então B^xA^y é Prt-universal.

(4) Se $n \geq 1$ então as palavras $BA^{n+1}BA^{n}$ e $B^{n}AB^{n+1}A$ são Prt-universais.

Observe-se que, quando $n=1$, os resultados de (4) respondem, de modo afirmativo, a pergunta (1) de Isbell.

Uma importante pergunta é: Se α é Myc-universal então α é Prt-universal?

Basta observar que em (2) Isbell prova que A^2B^2A é ^{X}X-universal para todo X finito mas que Silberger em [9, 6.22] mostra que, se X=3 então A^2B^2A não é Prt(X)-universal. Assim vimos que, pelo menos para X=3, a implicação, α é ^{X}X-universal $\rightarrow$ α é Prt(X)-universal, não é verdadeira.

Em 1977 A.Ehrenfeucht e D.M.Silberger [3] estendendo o método usado por Isbell para estabelecer o Teorema 2.2, demonstraram o:

2.7. Teorema: Seja n inteiro positivo tendo um menor fator primo ímpar p. Seja $2^{k}||n$. Então as seguintes afirmações são equivalentes:

(I) $2^{k+1} < p$

(II) Para todo conjunto X finito e para toda $f \in {}^{X}X$ existem $g \in {}^{X}X$ e uma involução h tal que $f=g^{n}h$.

Os seguintes resultados relacionados com os Teoremas 2.2 e 2.7 são também de autoria de Ehrenfeucht e Silberger [4]. Deste trabalho destacamos o teorema principal e um importante corolário.

2.8. Teorema: Sejam n e m inteiros maiores que 2. Então as três afirmações seguintes são equivalentes:

(I) $M(S(m)) \nmid n$ e $M(S(n)) \nmid m$;

(II) B^nA^m é Myc-universal;

(III) B^nA^m é FSym-universal.

2.9. Corolário: Seja $s>1$. Sejam $L_1, L_2, \ldots, L_s$ letras distintas. Seja $n(j)>1$ para todo j. Seja α a palavra de comprimento $\Sigma_{i=1}^{s} n(i)$ denotada por $\alpha = L_1^{n(1)} L_2^{n(2)} \ldots L_s^{n(s)}$. Então as afirmações seguintes são equivalentes:

(I) Existem inteiros i e j tais que $1 \leqslant i < j \leqslant s$ e tais que $M(S(n(i))) \nmid n(j)$ e $M(S(n(j))) \nmid n(i)$;

(II) α é Myc-universal;

(III) α é FSym-universal.

A mais recente contribuição na área, a ser publicada, é escrita por D.M.Silberger [7]. Seu principal teorema segue:

2.10. Teorema: Sejam n e m inteiros maiores que 2. As afirmações seguintes são equivalentes:

(I) $M(S(n)) \nmid m$ e $M(S(m)) \nmid n$;

(II) B^nA^m é Prt-universal;

(III) B^nA^m é Myc-universal;

(IV) B^nA^m é Sym-universal.

Na demonstração deste teorema Silberger observa que existem involuções g e f de Z tais que $s=gf$. (Ver figura 5.) Segue-se que $(B^nA^m \downarrow s)\mathrm{Sym}(Z)$ para n e m inteiros quaisquer.

Para o trabalho que desenvolvemos é relevante citar o artigo de A.Ehrenfeucht, S.Fajtlowicz, J. Malitz e J.Mycielski [2] onde aparece:

2.11. Teorema: Seja $\alpha \in \Sigma^*$. Se α é Sym(X)-universal para algum conjunto infinito X então α é Sym(Y)-universal para todo Y tal que $|Y| = \aleph_1$.

Estes autores observam também que existe $\{f,g\} \subseteq \mathrm{Sym}(Z)$ tal que $\Lambda(f)=\{3\}$, tal que $\Lambda(g)=\{1,2\}$ e tal que $s=fg$. (Ver figura 6.)

Eles remarcam que a palavra B^2A^2 é Sym(Z)-universal. Deste fato concluímos que α ISym-universal não implica α Sym-universal.

CAPÍTULO III - Grupos simétricos finitos

3.1. Preliminares: No presente capítulo aplicamos algumas das técnicas introduzidas em [4, Theorem 1], para estudo de palavras de complexidade dois, com a finalidade de caracterizar uma nova classe infinita de palavras de complexidade arbitrária que são FSym-universais. Esta aplicação depende das classes de equivalência .W. em Σ^*, introduzidas em 1.21 e 1.22, e culmina no Teorema 3.13. Além disso demonstramos que, se uma palavra não vazia é FSym-universal, então essa palavra é primitiva.

3.2. Lema: Seja $k \in \omega \setminus 2$. Então existe $h \in Sym(k)$ tal que h e $c_k h$ são involuções, e tal que $h(0)=0$.

Demonstração: Seja $k=2$. Então se $h = id \restriction 2$ o lema segue.

Suporemos que $k \geq 3$. Seja $f_1 = (1 \quad k-1)$. Então $c_k f_1 = (0\ 1\ \ldots\ k-1)(1 \quad k-1) = (0\ \underline{1})(2\ 3\ \ldots\ \underline{k-1})$. Da mesma forma vemos que $(\underline{k-1}\ 2\ 3\ \ldots\ k-2)(2 \quad k-2) = (\underline{k-1} \quad \underline{2})(3\ 4\ \ldots\ \underline{k-2})$. Portanto, com $f_2 = (2 \quad k-2)$, segue-se que $c_k f_1 f_2 = (0\ \underline{1})(\underline{k-1} \quad \underline{2})(\underline{k-2}\ 3\ 4\ \ldots\ k-3)$. Seja j o maior número inteiro menor que $(k-1)/2$ e seja $h = f_1 f_2 \ldots f_j$ onde $f_i = (i \quad k-i)$ para todo $i \in \{1,2,\ldots,j\}$. Então h é uma involução com $h(0)=0$ e $c_k h$ é uma involução. (F.P.)

3.3. Corolário: Seja $k \in \omega \setminus 2$. Seja $i \in \omega$. Então existe $h \in Sym(k)$ tal que $\Lambda(h) \subseteq 2^{i+1}+1$, tal que $c_k h$ tem exatamente $q2^i$ componentes 2-cíclicas para algum $q \in \omega$, e tal que $\Lambda(c_k h) \subseteq \{1,2\}$.

Demonstração: Suporemos que $2^{i+1}>k$. Então seja $h=c_k^{-1}$. Observemos que h satisfaz as condições do corolário. Desta forma podemos supor que $2^{i+1}\leqslant k$.

Sejam r e q inteiros tais que $0<k-q2^{i+1}=r<2^{i+1}$. Seja $h_1=(q2^{i+1}+r-1 \;\; q2^{i+1}+r-2 \;\ldots\; q2^{i+1} \;\; q2^{i+1}-1)$ com $h_1\in Sym(k)$. Então $\Lambda(h_1)=\{1,r+1\}$. Além disso $c_k h_1=(0\;1\;2\;\ldots\;\underline{q2^{i+1}-1})$ cuja única componente não trivial é um $q2^{i+1}$-ciclo tendo menos que dois pontos usados. Agora, nas condições do Lema 3.2, existe $h_2\in Sym(k)$ com $h_2(q2^{i+1}-1)=q2^{i+1}-1$, tal que $c_k h_1 h_2$ tem exatamente $q2^i$ componentes 2-cíclicas, tal que $\Lambda(h_1h_2)\subseteq\{1,2,r+1\}\subseteq 2^{i+1}+1$, e tal que $\Lambda(c_k h_1 h_2)\subseteq\{1,2\}$. Desta forma h_1h_2 satisfaz o corolário. (F.P.)

3.4. Lema: Seja $\{p,k+2\}\subseteq\omega\setminus 3$. Seja $h=(p-1 \;\; pk-1)$ com $h\in Sym(pk)$. Então $h\restriction 2=id\restriction 2$ e as componentes de $c_{pk}h$ são uma de comprimento p e outra de comprimento $pk-p$.

Demonstração: $c_{pk}h=(0\;1\;\ldots\;p-1\;\;p\;\;p+1\ldots pk-2\;\;pk-1)(p-1\;\;pk-1)=(0\;1\;\ldots\;\underline{p-1})(p\;\;p+1\;\ldots\;pk-2\;\;\underline{pk-1})$. (F.P.)

Observemos que o ciclo $(p\;\;p+1\;\ldots\;pk-2\;\;\underline{pk-1})$ tem um só ponto usado por h.

3.5. Corolário: Seja $k\in\omega\setminus 1$. Seja $p\in\omega\setminus 3$. Então existe uma involução $h\in Sym(pk)$ tal que $\Lambda(c_{pk}h)=\{p\}$ e tal que $h\restriction 2=id\restriction 2$.

Demonstração: Seja $h=\pi_{j=1}^{k-1}h_j$ onde para cada $j\in k\setminus 1$ temos que $h_j\in Sym(pk)$ e que $h_j=((p-1)j \;\; pk-j)$. Temos que h é uma involução, e que $h\restriction 2=id\restriction 2$ porque $p\geqslant 3$. Seja $h^{(j)}=h_1h_2\ldots h_j$ para cada $j\in(k-1)\setminus 1$. Segue que as componentes de $c_{pk}h^{(j)}$ são exatamente

j de comprimento p e uma de comprimento $p(k-j)$.

Podemos então concluir que $\Lambda(c_{pk}h)=\{p\}$.(F.P.)

3.6. Corolário: Sejam $\{k+1,p\}\subseteq\omega\setminus 3$ e $i\in\omega$. Então existe $h\in \mathrm{Sym}(k)$ tal que $\Lambda(h)\subseteq p^{i+1}$, tal que $\Lambda(c_k h)\subseteq\{1,p\}$, e tal que $c_k h$ tem exatamente qp^i componentes p-cíclicas para algum $q\in\omega$.

Demonstração: Existe $\{q,r\}\subseteq\omega$ tal que $k-qp^{i+1}=r\subsetneq p^{i+1}$. Se $q=0$, então consideremos $h=c_k^{-1}$ e observemos que $\Lambda(h)=\{r\}\subseteq p^{i+1}$, que $\Lambda(c_k h)=\{1\}\subseteq\{1,p\}$, e que $c_k h$ tem $0=qp^{i+1}$ componentes p-cíclicas. Portanto poderemos supor que $q>0$. Agora, no caso que $r=0$, temos que $k=qp^{i+1}$, e o corolário segue imediatamente do Corolário 3.5. Portanto suporemos também que $r>0$. Seja $h_1=(k-1\ \ k-2\ \ldots\ k-r)(k-r-1\ \ k-r-2)$, com $h_1\in\mathrm{Sym}(k)$, e observemos que $c_k h_1=(0\ 1\ \ldots\ \underline{qp^{i+1}-2}\ \ \underline{qp^{i+1}})$. Além disso, observemos que, se $r=1$ então $c_k h_1$ tem exatamente um ponto $qp^{i+1}-2$ que é usado por h_1, mas se $r>1$ então $c_k h_1$ tem o bloco de exatamente dois pontos (de fato, adjacentes no ciclo) $qp^{i+1}-2$ e qp^{i+1} que são usados por h_1. Então, segue-se do Corolário 3.5, que existe $h_2\in\mathrm{Sym}(k)$ que é uma involução tal que a família $\{h_1,h_2\}$ é dcp, e tal que $\Lambda(c_k h_1 h_2)\subseteq\{1,p\}$. Com efeito, h_2 quebra a componente qp^{i+1}-cíclica $(0\ 1\ \ldots\ qp^{i+1}-2\ \ qp^{i+1})$ de $c_k h_1$ em exatamente qp^i componentes p-cíclicas. Seja $h=h_1h_2$, e observemos que $\Lambda(h)\subseteq\{1,2,r\}\subsetneq p^{i+1}$. (F.P.)

3.7. Lema: Sejam $p\in\omega\setminus 2$, $i\in\omega\setminus 1$ e $k=qp^{i+1}+r$ com $\{q,r\}\subseteq\omega$ e com $r<p^{i+1}$. Seja $f\in\mathrm{Sym}(k)$ tal que $\Lambda(f)\subseteq\{1,p\}$ e tal que f

tem exatamente qp^i componentes p-cíclicas. Então existe $g\in Sym(k)$ tal que g tem exatamente q componentes p^{i+1}-cíclicas, tal que $g(x)=x$ se e somente se $f(x)=x$ para todo $x\in k$ e tal que $g^{p^i}=f$.

Demonstração: [3, Lemma3]. Sejam x e y inteiros positivos. Seja d a permutação cíclica $(1\ 2\ \ldots\ x\ x+1\ \ldots\ 2x\ \ldots\ yx-1\ yx)$ do conjunto $\{1,2,\ldots,xy\}$. Seja h a permutação $(1\ x+1\ \ldots\ (y-1)x+1)(2\ x+2\ \ldots(y-1)x+2)\ \ldots\ (x\ 2x\ \ldots\ yx)$ do conjunto $\{1,2,\ldots,xy\}$ tendo exatamente x componentes y-cíclicas e tal que $\Lambda(h)=\{y\}$. Então $d^x=h$. Vemos que, começando com h por intercalação das x componentes y-cíclicas de h, temos as condições para construir uma permutação d cíclica de $\{1,2,\ldots,xy\}$ tal que $d^x=h$.

Agora listaremos as componentes p-cíclicas de f em q sequências cada qual tendo exatamente p^i termos. Usando a técnica explicada no parágrafo anterior, construiremos uma permutação g do conjunto k tal que g fixa exatamente os mesmos elementos de k que são fixados por f, tal que $\Lambda(g)\subseteq\{1,p^{i+1}\}$, tal que g tem exatamente q componentes não triviais, e tal que $g^{p^i}=f$. (F.P.)

3.8. Lema: Seja X um conjunto arbitrário. Seja $H:\Sigma^*\to Sym(X)$ um homomorfismo tal que $H(\gamma)=id\restriction X$ para todo $\gamma\in W\subseteq\Sigma^*$. Então, para todo $\beta\in\alpha/W$ temos que $H(\alpha)\approx H(\beta)$.

Demonstração: Seja $\beta\in\alpha/W$. Então existe uma sequência $\alpha=\gamma_o$, $\gamma_1,\ldots,\gamma_j=\beta$ que leva α em β por W. Suporemos que $H(\gamma_o)\approx H(\gamma_1)\approx\ldots\approx H(\gamma_i)$ para algum $i\in j$ arbitrário.

Se $\gamma_{i+1}\sim\gamma_i$ então $\gamma_{i+1}=\mu\nu$ e $\gamma_i=\nu\mu$ para algum

$\{\mu,\nu\}\subseteq\Sigma^*$. Podemos supor que $\nu\neq\phi\neq\mu$. Logo, por [11, Theorem 1] segue-se que $H(\gamma_{i+1})=H(\mu)H(\nu)\simeq H(\nu)H(\mu)H(\nu)H(\nu)^{-1}=H(\nu)H(\mu)=H(\gamma_i)$. Portanto $H(\gamma_{i+1})\simeq H(\gamma_i)$.

Agora, se $\gamma_i\psi=\gamma_{i+1}$ para algum $\psi\in W$, então $H(\gamma_i)=H(\gamma_i)\mathrm{id}\restriction X=H(\gamma_i)H(\psi)=H(\gamma_i\psi)=H(\gamma_{i+1})$ e novamente temos que $H(\gamma_{i+1})\simeq H(\gamma_i)$.

De modo análogo se $\gamma_i=\gamma_{i+1}\psi$ para algum $\psi\in W$ temos que $H(\gamma_i)\simeq H(\gamma_{i+1})$.

Segue-se então que, quaisquer que sejam γ_i e γ_{i+1} da sequência $\alpha=\gamma_0,\gamma_1,\ldots,\gamma_j=\beta$ temos que $H(\gamma_i)\simeq H(\gamma_{i+1})$ e assim, por indução, que $H(\alpha)\simeq H(\beta)$. (F.P.)

3.9. Lema: Seja $f\simeq g$ com $\{f,g\}\subseteq\mathrm{Sym}(X)$. Seja $\alpha\in\Sigma^*$ com $(\alpha\downarrow f)\mathrm{Sym}(X)$. Então $(\alpha\downarrow g)\mathrm{Sym}(X)$.

Demonstração: Por hipótese temos que $(\alpha\downarrow f)\mathrm{Sym}(X)$. Então existe um homomorfismo $H_f:\Sigma^*\to\mathrm{Sym}(X)$ tal que $H_f(\alpha)=f$. Como $f\simeq g$ e $\{f,g\}\subseteq\mathrm{Sym}(X)$ segue-se, por [11, Theorem 1] que existe $h\in\mathrm{Sym}(X)$ tal que $hfh^{-1}=g$. Seja $H_g:\Sigma^*\to\mathrm{Sym}(X)$ definido por $H_g(\tau)=hH_f(\tau)h^{-1}$ para cada $\tau\in\Sigma^*$. Então para $\{\sigma,\tau\}\subseteq\Sigma^*$ temos que $H_g(\sigma\tau)=hH_f(\sigma\tau)h^{-1}=hH_f(\sigma)H_f(\tau)h^{-1}=hH_f(\sigma)\mathrm{id}\restriction XH_f(\tau)h^{-1}=hH_f(\sigma)h^{-1}hH_f(\tau)h^{-1}=H_g(\sigma)H_g(\tau)$, e portanto que H_g é um homomorfismo. Além disso $H_g(\alpha)=hH_f(\alpha)h^{-1}=hfh^{-1}=g$. (F.P.)

3.10. Corolário: Seja X um conjunto arbitrário. Seja $f\in\mathrm{Sym}(X)$. Seja $(\alpha\downarrow f)\mathrm{Sym}(X)$. Então $(\overline{\alpha}\downarrow f)\mathrm{Sym}(X)$.

Demonstração: Seja $H:\Sigma^*\to\mathrm{Sym}(X)$ um homomorfismo tal que $H(\alpha)=f$. Então, certamente $H(\overline{\alpha})=f^{-1}$. Mas $f^{-1}\simeq f$ porque $f\in\mathrm{Sym}(X)$. Agora o corolário segue diretamente do Lema 3.9. (F.P.)

3.11. Corolário: Sejam $W\subseteq\Sigma^*$, $f\in Sym(X)$ e $\alpha\in\Sigma^*$. Seja $H_\alpha:\Sigma^*\to Sym(X)$ um homomorfismo tal que $H_\alpha(\alpha)=f$ e tal que $H_\alpha(\gamma)=id\restriction X$ para todo $\gamma\in W$. Seja $\beta\in\alpha/W$. Então existe um homomorfismo $H_\beta:\Sigma^*\to Sym(X)$ tal que $H_\beta(\beta)=f$.

Demonstração: Pelo Lema 3.8, temos que $H_\alpha(\beta)=H_\alpha(\alpha)=f$. O corolário decorre agora do Lema 3.9. (F.P.)

3.12. Corolário: Sejam $W\subseteq\Sigma^*$ e $\alpha\in\Sigma^*$. Para toda $f\in Sym(X)$ consideremos a existência de um homomorfismo $H_f:\Sigma^*\to Sym(X)$ tal que $H_f(\alpha)=f$ enquanto que $H_f(\psi)=id\restriction X$ para todo $\psi\in W$. Então cada elemento de α/W é $Sym(X)$-universal.

Demonstração: É consequência imediata do Corolário 3.11.(F.P.)

3.13. Teorema: Seja $\{n,m,p\}\subseteq\omega\setminus 2$, com m impar e p primo tal que $p^i||n$ enquanto que $p^{i+1}\leqslant S(m)$. Sejam $P=p^{i+1}$ e $Q=M(P+1)$ quando $p=2$ mas $Q=M(P)$ quando $p>2$. Sejam ainda $W_1=\{B^P,A^Q\}$ e $\beta\in B^nA^m/W_1$. Então β é FSym-universal.

Demonstração: Basta mostrar que $(\beta\downarrow c_k)Sym(k)$ para todo $k\in\omega\setminus 2$.

Primeiramente, seja $p=2$. Pelo Corolário 3.3 temos que existe $h\in Sym(k)$ tal que $\Lambda(c_kh)\subseteq\{1,2\}$, tal que $\Lambda(h)\subseteq 2^{i+1}+1\leqslant S(m)$ e tal que c_kh tem exatamente $q2^i$ componentes 2-cíclicas para algum $q\in\omega$. Desta forma, como m é impar, se $x\in\Lambda(h)$ então $x\leqslant 2^{i+1}<S(m)$ e portanto, $(x,m)=1$. Segue-se, pelo Lema 1.7, que existe $a\in Sym(k)$ tal que $a^m=h^{-1}$ e tal que $\Lambda(a)=\Lambda(h)$. Além disso temos que $a^Q=a^{M(2^{i+1}+1)}=id\restriction k$.

Seja agora $p\geqslant 3$. Pelo Corolário 3.6 existe $h\in Sym(k)$ tal que $\Lambda(h)\subseteq p^{i+1}\leqslant S(m)$, tal que $\Lambda(c_kh)\subseteq\{1,p\}$, e tal que c_kh tem exatamente qp^i componentes p-cíclicas para algum $q\in\omega$. Então, se $x\in\Lambda(h)$, temos que $(x,m)=1$ e, novamente pelo Lema 1.7, que existe $a\in Sym(k)$ tal que $a^m=h^{-1}$ com $\Lambda(a)\subseteq p^{i+1}$. Além disso $a^Q=a^{M(p^{i+1})}=id\restriction k$.

Desta forma, em qualquer dos casos anteriores, seja $f=c_k h$. Então, pelo Lema 3.7, segue-se que existe $g\in Sym(k)$ tal que g tem exatamente q componentes p^{i+1}-cíclicas e tal que $g^{p^i}=f$. Lembrando que $p^i\|n$, vemos que $(n/p^i,p)=1$. Portanto, pelo Lema 1.7, existe $b\in Sym(k)$ tal que $b^{n/p^i}=g$ com $\Lambda(b)=\Lambda(g)\subseteq\{1,p^{i+1}\}$. Desta forma $b^P=b^{p^{i+1}}=id\restriction k$.

Além disso $c_k=c_k hh^{-1}=g^{p^i}a^m=(b^{n/p^i})^{p^i}a^m=b^n a^m$.

Seja $H_k:\Sigma^*\to Sym(k)$ o homomorfismo gerado por $H_k(A)=a$ e $H_k(B)=b$. Então $H_k(B^nA^m)=c_k$ enquanto que $H_k(\psi)=id\restriction k$ para todo $\psi\in W_1$. Segue-se, pelo Corolário 3.12, que β é $Sym(k)$-universal para todo $k\in\omega$. Portanto β é **FSym**-universal. (**F.P.**)

3.14. Proposição: Seja $\{n,k\}\subseteq\omega\setminus 2$. Então $(A^n\downarrow c_k)Sym(k)$ se e somente se $(n,k)=1$.

Demonstração: Suporemos primeiramente que $(A^n\downarrow c_k)Sym(k)$ e que $(n,k)=j$ para algum $j\in\omega\setminus 2$. Então existe $f\in Sym(k)$ tal que $f^n=c_k$ com $(n,k)=j$. Mas, pelo Lema 1.8, temos que $\Lambda(f^n)=\{k/j\}$. Observemos agora que $\Lambda(c_k)=\{k\}$ e, desta forma $f^n\neq c_k$. Temos a contradição.

Consideremos agora que $(n,k)=1$. Então, pelo Lema 1.7, existe $f\in Sym(k)$ tal que $f^n=c_k$. Portanto, $(A^n\downarrow c_k)Sym(k)$. (F.P.)

3.15. Corolário: Seja $\alpha \in \Sigma^* \setminus \{\phi\}$. Se α é FSym-universal então $\alpha = \pi(\alpha)$.

Demonstração: Suponhamos que $\alpha \neq \pi(\alpha)$. Então existe $n \in \omega \setminus 2$ tal que $\alpha = \pi(\alpha)^n$. Seja $k \in \omega \setminus 2$. Por hipótese temos que $(\alpha \downarrow c_k)$ Sym(k). Então existe um homomorfismo $H: \Sigma^* \to Sym(k)$ tal que $H(\alpha) = c_k$. Desta forma $H(\alpha) = H(\pi(\alpha)^n) = c_k$. Observando-se que para vários valores de k, $(n,k) \neq 1$ temos, pela Proposição 3.14, um absurdo. Assim sendo $\alpha = \pi(\alpha)$. (F.P.)

É interessante observar que a recíproca não é verdadeira. Temos por [12, Theorem §1], que B^2A^2 não representa c_2 em Sym(2), mas noentanto, $\pi(B^2A^2) = B^2A^2$.

CAPÍTULO IV - Representação em Sym(Z) de uma permutação cíclica de Z.

4.1. Preliminares: Apresentamos neste capítulo resultados conhecidos, de palavras de complexidade dois e três que representam s em Sym(Z). Mostramos que palavras não primitivas não podem representar s em Sym(Z) e, principalmente, com técnicas similares as do Capítulo III, caracterizamos, no Teorema 4.6 uma nova classe infinita de palavras que representam s em Sym(Z).

4.2. Lema: A^n não representa s em Sym(Z) qualquer que seja $n>1$.

Demonstração: Basta provar que é impossível escrever s na forma f^n onde $f \in \mathrm{Sym}(Z)$.

Suporemos que existe $f \in \mathrm{Sym}(Z)$ tal que $f^n = s$ para algum $n>1$.

Observemos que, qualquer que seja o conjunto X, se $g \in \mathrm{Sym}(X)$ então, cada componente cíclica de g não será ligada com outras componentes cíclicas de g quando g^n é construida, mas pode ser desmembrada em ciclos disjuntos. Assim temos que $|V(g^n)| \geqslant |V(g)|$.

Temos agora que $1 = |V(s)| = |V(f^n)| \geqslant |V(f)|$ e, desta forma, que $|V(f)| = 1$. Portanto f é uma permutação cíclica de Z. Mas, neste caso $f \simeq s$. Vemos portanto que $|V(f^n)| = n$ para $n>1$ o que é, claramente, um absurdo. Logo não existe $f \in \mathrm{Sym}(Z)$ tal que $f^n = s$. (F.P.)

Observação: Segue do Lema 4.2 que não é verdade que $(A^n\downarrow s)M$ para $n>1$ para qualquer monóide M das relações binárias em Z. Para ver isto, observemos que se $s=h^n$, então é necessário que $h\in Sym(Z)$, o que, por 4.2 é impossível.

4.3. Corolário: Seja $\alpha\in\Sigma^*\setminus\{\phi\}$. Se α é palavra não primitiva então α não representa s em $Sym(Z)$.

Demonstração: Seja α uma palavra não primitiva. Então $\alpha=\pi(\alpha)^n$ para algum $n>1$. Admitamos que $(\alpha\downarrow s)Sym(Z)$. Decorre que existe um homomorfismo $H:\Sigma^*\to Sym(Z)$ tal que $H(\alpha)=s$. Seja $f\in Sym(Z)$ tal que $H(\pi(\alpha))=f$. Desta forma temos que $s=H(\alpha)=H(\pi(\alpha)^n)=H(\pi(\alpha))^n=f^n$. Segue, do Lema 4.2, que isto é absurdo. (F.P.)

4.4. Lema: Sejam n e m números inteiros positivos. Seja $\alpha=B^nA^m$. Então $(\alpha\downarrow s)Sym(Z)$.

Demonstração: Sejam v e u números inteiros ímpares tais que $n=2^{i-1}v$ e também que $m=2^{j-1}u$ para $\{i,j\}\subseteq\omega\setminus 1$. Seja $\{g_1, h_1\}\subseteq Sym(Z)$ tal que $g_1=\Pi_{k\in\omega}(-k \;\; k+1)$ e $h_1=\Pi_{k\in\omega}(-k \;\; k)$. Então $\Lambda(g_1)=\{2\}$ enquanto que $\Lambda(h_1)=\{1,2\}$. Além disso observamos que $g_1s=h_1$. Portanto $s=g_1^{-1}h_1$.

Vamos agora definir $g_i=\Pi_{k\in 2^{i-1}\omega}(-k \;\; -(k+1) \; \ldots \; -(k+2^{i-1}-1) \;\; k+1 \;\; k+2 \; \ldots \; k+2^{i-1})$ e $h_j=(0)\;\Pi_{k\in 2^{j-1}\omega}(-(k+1) \;\; -(k+2) \; \ldots \; -(k+2^{j-1}) \;\; k+1 \;\; k+2 \; \ldots \; k+2^{j-1})$. Então temos que $\{g_i,h_j\}\subseteq Sym(Z)$, que $\Lambda(g_i)=\{2^i\}$ e que $\Lambda(h_j)=\{1, 2^j\}$. Além disso $g_i^{2^{i-1}}=g_1$ enquanto que $h_j^{2^{j-1}}=h_1$.

Observemos que $(2^i,v)=1$. Então, por [1,Theorem 1], existe $\{r,t\}\subseteq Z$ tal que $r2^i+tv=1$. Assim $g_i=$

$g_i^{r2^i+tv}=(g_i^{2^i})^r(g_i^t)^v=id\restriction Z(g_i^t)^v=(g_i^t)^v$. Seja $g\in Sym(Z)$ tal que $g^{-1}=g_i^t$. Então $(g^{-1})^v=(g_i^t)^v$ e, portanto, $g^{-v}=g_i$ ou $g^v=g_i^{-1}$.

De modo análogo, com $(2^j,u)=1$ segue que, por [1, Theorem 1], existe $\{p,q\}\subseteq Z$ tal que $p2^j+qu=1$. Deste modo $h_j=h_j^{p2^j+qu}=(h_j^{2^j})^p(h_j^q)^u=id\restriction Z(h_j^q)^u=(h_j^q)^u$. Seja $h\in Sym(Z)$ tal que $h=h_j^q$. Então $h^u=h_j$.

Desta forma $s=g_1^{-1}h_1=(g_i^{2^{i-1}})^{-1}h_j^{2^{j-1}}=(g^{-v})^{-2^{i-1}}(h^u)^{2^{j-1}}=g^{2^{i-1}v}h^{2^{j-1}u}=g^nh^m$. Assim, se $H:\Sigma^*\to Sym(Z)$ é um homomorfismo gerado por $H(A)=h$ e $H(B)=g$ segue-se que $(\alpha\downarrow s)Sym(Z)$. (F.P.)

4.5. Corolário: Sejam n, x e y inteiros tais que $n\neq 0$ e ($x\neq 0$ ou $y\neq 0$). Então, se $\alpha=B^xA^nB^y$ segue-se que $(\alpha\downarrow s)Sym(Z)$.

Demonstração: Basta provar que $s=h^xg^nh^y$ onde $\{g,h\}\subseteq Sym(Z)$.

Seja $\{h,g_1\}\subseteq Sym(Z)$ tal que $s=g_1^nh^m$, nas condições do Lema 4.4 e tal que $x+y=m$. Então temos que $s=g_1^nh^m=id\restriction Zg_1^nh^m=h^xh^{-x}g_1^nh^xh^y$. Seja $g\in Sym(Z)$ tal que $g=h^{-x}g_1h^x$. Segue que $g^n=(h^{-x}g_1h^x)^n=h^{-x}g_1^nh^x$. Portanto $s=h^xg^nh^y$ e assim $(A^xB^nA^y\downarrow s)Sym(Z)$. (F.P.)

4.6. Teorema: Seja $\{i,j,n,m\}\subseteq\omega\setminus 1$ tal que $2^{i-1}||n$ e tal que $2^{j-1}||m$. Sejam $L=2^i$ e $M=2^j$. Sejam ainda $W_2=\{B^L,A^M\}$ e $\beta\in B^nA^m/W_2$. Então $(\beta\downarrow s)Sym(Z)$.

Demonstração: Por hipótese temos que $2^{i-1}||n$ e que $2^{j-1}||m$. Então existem v e u inteiros ímpares tais que $2^{i-1}v=n$ enquanto que $2^{j-1}u=m$. Seja H o homomorfismo definido no último parágrafo da prova do Lema 4.4. Basta observar que $H(A^M)=$

$H(A)^M = h^{2^j} = id\restriction Z$ e também que $H(B^L) = H(B)^L = g^{2^i} = id\restriction Z$. Portanto aquele homomorfismo, $H:\Sigma^* \to Sym(Z)$ tem a propriedade adicional que $H(\psi) = id\restriction Z$ para todo $\psi \in W_2$. Então, pelo Corolário 3.11, segue-se que, para todo $\beta \in B^n A^m / W_2$ tem-se que $(\beta \downarrow s)$ $Sym(Z)$. (F.P.)

CAPÍTULO V - Palavras Sym-universais

5.1. Preliminares: Nos capítulos III e IV apresentamos técnicas que, mediante a utilização de classes de relações de equivalência em Σ^*, nos davam condições para caracterizar classes de palavras de complexidade arbitrárias que são, respectivamente, Sym(k)-universais para todo $k\in\omega$ e Sym(Z)-universais. Neste capítulo fazemos a "interseção" destes resultados para obter nosso principal Teorema 5.2. Além disso apresentamos outros resultados relacionados que obtivemos.

5.2. Teorema: Seja $\{p,q,i\}\subseteq\omega$ onde p é primo e q é primo ímpar tal que $p^{i+1}\leqslant q$. Seja $\alpha=B^{p^i}A^q$. Sejam $x=2^{i+1}$ e $y=M(1+2^{i+1})$ quando $p=2$; mas, sejam $x=2p^{i+1}$ e $y=M(p^{i+1})$ quando $p>2$. Sejam ainda $W=\{B^x,A^y\}$ e $\{\beta,\overline{\beta}\}\cap\alpha/W\neq\phi$. Então β é Sym-universal.

Demonstração: Pelo Corolário 3.10 segue-se que β é Sym-universal se e somente se $\overline{\beta}$ é Sym-universal. Portanto, sem perda de generalidade, suporemos que $\beta\in\alpha/W$. Lembrando os Teoremas 3.13 e 4.6 observamos que $x=[P,L]$ e que $y=[Q,M]$. Portanto nosso teorema decorre imediatamente dos teoremas citados. (F.P.)

5.3. Proposição: Seja $\alpha\in\Sigma^*$ tal que $\gcd(\alpha)=1$. Então α é Sym-universal.

Demonstração: Seja $k\in\omega\setminus 1$. Mostraremos que $(\alpha\downarrow c_k)\mathrm{Sym}(k)$.

Seja L_i a letra que aparece em α exatamen te $n(i)$ vezes para todo $i\in\{1,2,\ldots,p\}$; isto é, $|\mathrm{Mult}(L_i,\alpha)|=n(i)$. Como $\gcd(\alpha)=1$, então por uma extensão de [1,Theorem 1], temos que existem inteiros $x_1,x_2,\ldots,x_p$ tais que $x_1n(1)+x_2n(2)+\ldots+x_pn(p)=1$. Seja $H:\Sigma^*\to \mathrm{Sym}(k)$ homomorfismo definido por $H(L_i)=c_k^{x_i}$ para $i\in\{1,2,\ldots,p\}$. Segue-se que $c_k=c_k^{x_1n(1)+x_2n(2)+\ldots+x_pn(p)}=(c_k^{x_1})^{n(1)}(c_k^{x_2})^{n(2)}\ldots(c_k^{x_p})^{n(p)}$ porque as potências de c_k obviamente comutam. Portanto temos que $H(\alpha)=c_k$.

Usando a mesma técnica onde $H(L_i)=s^{x_i}$, podemos mostrar que $(\alpha\downarrow s)\mathrm{Sym}(Z)$. Concluimos então que α é Sym-universal. (F.P.)

5.4. Lema: Seja $k\in\omega$. Então existem involuções g e h de $\mathrm{Sym}(k)$ tais que $c_k=gh$.

Demonstração: Decorre imediatamente do Lema 3.2. (F.P.)

5.5. Lema: Existem involuções g e h com $\{g,h\}\subseteq\mathrm{Sym}(k)$ tais que $s=gh$.

Demonstração: Decorre imediatamente do primeiro parágrafo da demonstração do Lema 4.4. (F.P.)

5.6. Corolário: Sejam X um conjunto arbitrário não vazio e $f\in\mathrm{Sym}(X)$. Então existem involuções g e h de $\mathrm{Sym}(X)$ tais que $f=gh$.

Demonstração: Decorrência direta dos Lemas 5.4 e 5.5. (F.P.)

5.7. Corolário: Seja $\{n(i),m(i)\}\subseteq\omega\setminus 1$ para todo $i\in\{1,2,\ldots k-1\}$. Seja $n(k)>0\leqslant m(k)$. Seja $\alpha=B^{n(1)}A^{m(1)}\ldots B^{n(k)}A^{m(k)}$ com exatamente um $n(i)$ impar e exatamente um $m(j)$ impar. Então α é Sym-universal.

Demonstração: Para toda $f \in Sym(X)$, pelo Corolário 5.6, temos que existem involuções g e h de X tais que $f=gh$. Assim, observando que $g^{impar}=g$, que $h^{impar}=h$ e também que $g^{par}=id\restriction X=h^{par}$ o corolário segue. (F.P.)

5.8. Proposição: Seja $\langle n,m\rangle$ par de inteiros tal que $\{n,m\}\subseteq \omega\setminus 2$ e tal que para todo $k\in\omega\setminus 2$ existe $i_k\in k$ tal que ou $(i_k+1, m)=1=(k-i_k,n)$ ou $(i_k+1,n)=1=(k-i_k,m)$. Então B^nA^m é Sym-universal.

Demonstração: Pelo Lema 4.4 temos que $(B^nA^m\downarrow s)Sym(Z)$. Seja $k\in\omega\setminus 1$. Observemos que $c_k=(0\ 1\ \dots\ i_k)(i_k\ i_{k+1}\ \dots\ k-1)$. Sem perda de generalidade suponhamos que $(i_k+1,n)=1=(k-i_k,m)$. Então, pelo Lema 1.7, segue que existe $\{g,h\}\subseteq Sym(k)$ tal que $g^n=(0\ 1\ \dots\ i_k)$ e tal que $h^m=(i_k\ i_{k+1}\ \dots\ k-1)$, porque $\Lambda(g)=\{i_k+1\}$ e $\Lambda(h)=\{k-i_k\}$. Assim vemos que para todo $k\in\omega\setminus 2$ $(B^nA^m\downarrow c_k)Sym(k)$. Segue-se que B^nA^m é Sym-universal por generalização do Corolário 3.10. (F.P.)

5.9. Corolário: Seja $\langle n,m\rangle$ par de inteiros nas condições da Proposição 5.8. Entaõ $\langle n,m\rangle$ é par de ehrenfeucht.

Demonstração: Decorre imediatamente da Proposição 5.8 e do Teorema 2.10. (F.P.)

Observação: A recíproca do Corolário 5.9 não é verdadeira. Basta notar que o par $\langle 30,35\rangle$ é par de ehrenfeucht mas, para $k=5$ este par não satisfaz as condições da Proposição 5.8.

CAPÍTULO VI - Perguntas abertas e comentário geral

Pergunta 1. (Mycielski): Se α é FSym-universal então α é Sym-universal?

Para responder de modo afirmativo a pergunta 1, basta que $(\alpha\downarrow s)\mathrm{Sym}(Z)$ se, para todo $k\in\omega$, nós tivermos que $(\alpha\downarrow c_k)\mathrm{Sym}(k)$.

Nosso Teorema 4.6 indica que muitas palavras em $\{A,B\}^*$ satisfazem a afirmação $(\pi(\alpha)\downarrow s)\mathrm{Sym}(Z)$.

Em [4] Ehrenfeucht e Silberger formulam a:

Pergunta 2: $(\pi(\alpha)\downarrow s)\mathrm{Sym}(Z)$ para todo $\alpha\neq\phi$?

Do Corolário 3.15 temos que, se $\phi\neq\alpha\neq\pi(\alpha)$ então α não é FSym-universal. Assim vemos que a resposta afirmativa para a pergunta 2 implica na resposta afirmativa para a pergunta 1.

Nós não fizemos consideração para uma possível extensão do argumento de R.A.McKenzie para ${}^{X}X$ infinitos, ou do argumento análogo de D.M.Silberger [9] para $\mathrm{Prt}(X)$ infinitos, que se aplique aos $\mathrm{Sym}(X)$ infinitos, o que poderia, talvez, indicar ser suficiente considerar Σ^* com $|\Sigma|=2$.

Pergunta 3: Existe algum algorítmo "razoável" que indique que se nós sabemos todos os elementos $\alpha\in\{A,B\}^*$ para os quais $(\alpha\downarrow s)\mathrm{Sym}(Z)$, então este algorítmo permite decidir se $(\beta\downarrow s)\mathrm{Sym}(Z)$ para $\beta\in\Sigma^*$ onde Σ é um alfabeto finito mas arbitrário?

Das figuras 5 e 6 do apêndice e seus respectivos argumentos algébricos temos que existe $\{g_p,h_q\}\subseteq Sym(Z)$ tal que $\Lambda(g_p)\subsetneq\{1,p\}$ e $\Lambda(h_q)\subsetneq\{1,q\}$ e ainda que $s=g_ph_q\approx h_qg_p$ para os casos $\langle p,q\rangle=\langle 2,2\rangle$ e $\langle p,q\rangle=\langle 2,3\rangle$. Desta forma temos a:

Pergunta 4: Para todo $\{p,q\}$, com p e q primos, existe $\{g_p, h_q\}\subseteq Sym(Z)$ tal que $s=g_ph_q$, tal que $\Lambda(g_p)\subsetneq\{1,p\}$, e tal que $\Lambda(h_q)\subsetneq\{1,q\}$?

Procurando aplicar as observações de Mycielski e as nossas, formulamos a:

Pergunta 5: Seja $\alpha\in\{A,B\}^*$. Se $(\alpha\downarrow s)Sym(Z)$ então existe $\{n,m,N,M\}\subseteq\omega\setminus 2$ tal que $W=\{B^N,A^M\}$ e $\alpha\in B^nA^m/W$?

A pergunta 5, na verdade, procura verificar o alcance que tem nossa técnica neste trabalho.

Em [4] Silberger e Ehrenfeucht perguntam se, quando X é finito e quando $(B^nA^m\downarrow\downarrow Sym(X))$ então $(B^nA^m\downarrow\downarrow {}^XX)$? Neste caso perguntamos:

Pergunta 6: Se $\alpha=B^nA^m$ com $\langle n,m\rangle$ par de ehrenfeucht, e se $\beta\in\alpha/W_1$, então β é FMyc-universal?

Mais geralmente:

Pergunta 7: Se $\beta\in\alpha/W$ nas condições do Teorema 5.2, então β é Myc-universal?

Finalmente de [2] sai a seguinte pergunta aberta:

Pergunta 8: Se existe Y infinito tal que α é $Sym(Y)$-universal então α é $\mathrm{I}Sym$-universal?

Na figura, $(\alpha \downarrow x)M$ por $H:\Sigma^* \to M$

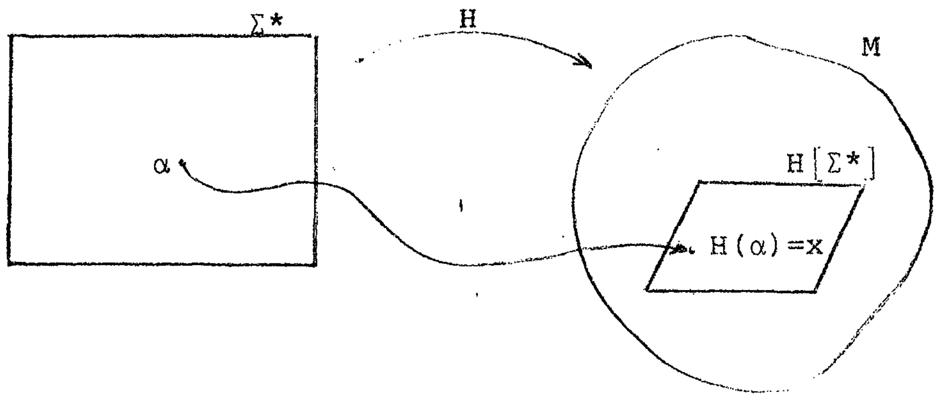


Figura 1.

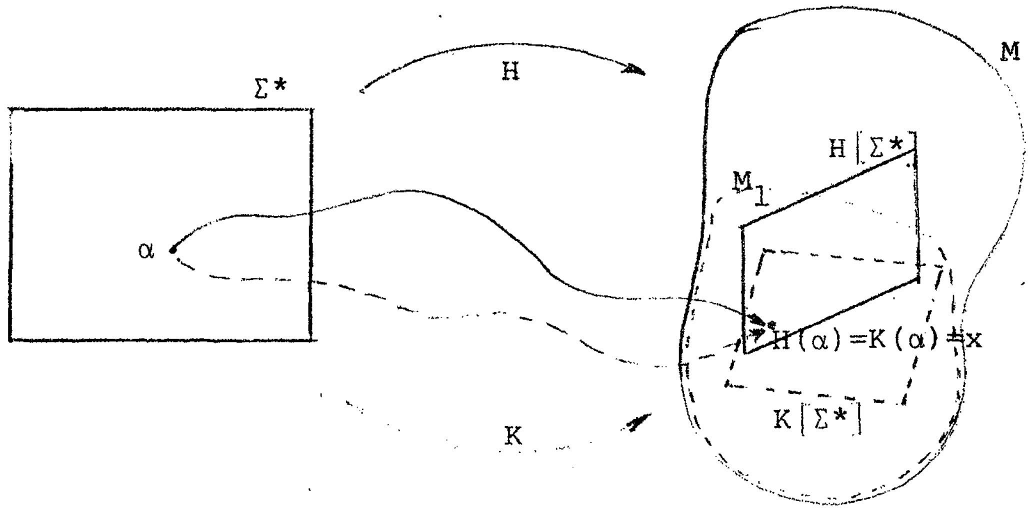


Figura 2.

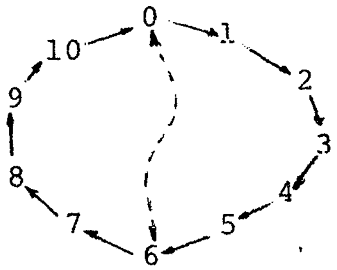
Agora observamos que $(\alpha \downarrow x)M$ por H; (aqui H é representado por linhas contínuas). Mas, $(\alpha \downarrow x)M_1$ por H não é válido pois $H[\Sigma^*] \not\subseteq M_1$. Porém $(\alpha \downarrow x)M_1$ por K; (K é representado por linhas tracejadas).

Para M_1 subsemigrupo do semigrupo M com $x \in M_1$, o fato que $(\alpha \downarrow x)M$ não garante automàticamente que $(\alpha \downarrow x)M_1$.

Desdobramento de ciclos

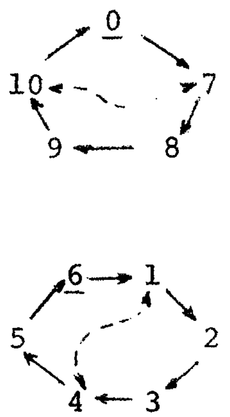
Vamos considerar o ciclo c_k com k=11 como exemplo.

c_{11}:



Enquanto que as linhas contínuas representam c_{11} seja $f_1=(0\ 6)$ representada pela linha tracejada.

$c_{11}f_1$:



Agora as linhas contínuas representam $c_{11}f_1$ e as tracejadas $f_2 = (1\ 4)(7\ 10)$. Observemos que f_2 não usa os pontos usados por f_1 que aparecem sublinhados. Obtivemos por $c_{11}f_1$ um 5-ciclo e um 6-ciclo

$c_{11}f_1f_2$:

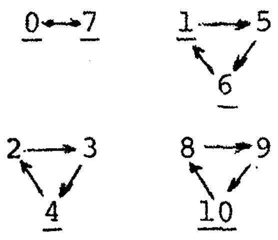


Figura 3

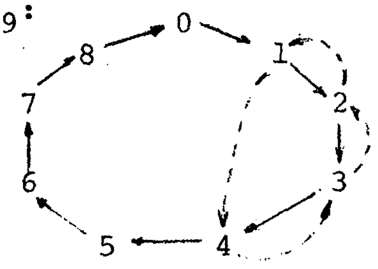
Temos agora desdobrado o 11-ciclo c_{11} em um 2-ciclo e em três 3-ciclos. Notemos que $f = f_1f_2$ é uma involução do conjunto 11. A fim de garantir isto, decorre a importância de f_2 não usar pontos usados por f_1.

Observemos que (a b)(b c) = (a b c). Assim vemos que pode acontecer que f_1f_2 não é uma involução se $\{f_1, f_2\}$ for uma família de involuções que não é dcp.

Encurtamento de ciclos

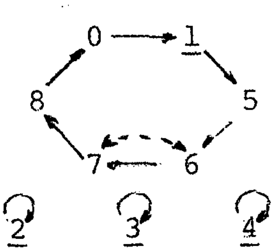
Vamos estudar o exemplo onde c_k é tal que $k = 9$.

c_9:



c_9 é representado por linhas contínuas e o 4-ciclo $f_1=(4\ 3\ 2\ 1)$ por linhas tracejadas.

c_9f_1:



O 4-ciclo f_1 "encurtou" o 9-ciclo c_9 para um $9-(4-1)=$ 6-ciclo obtendo ainda $4-1=$ 3 pontos fixos.

Seja $f_2=(7\ 6)$ o 2-ciclo representado por linhas tracejadas.

$c_9f_1f_2$:

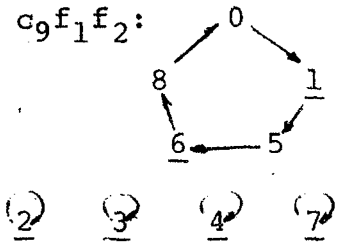


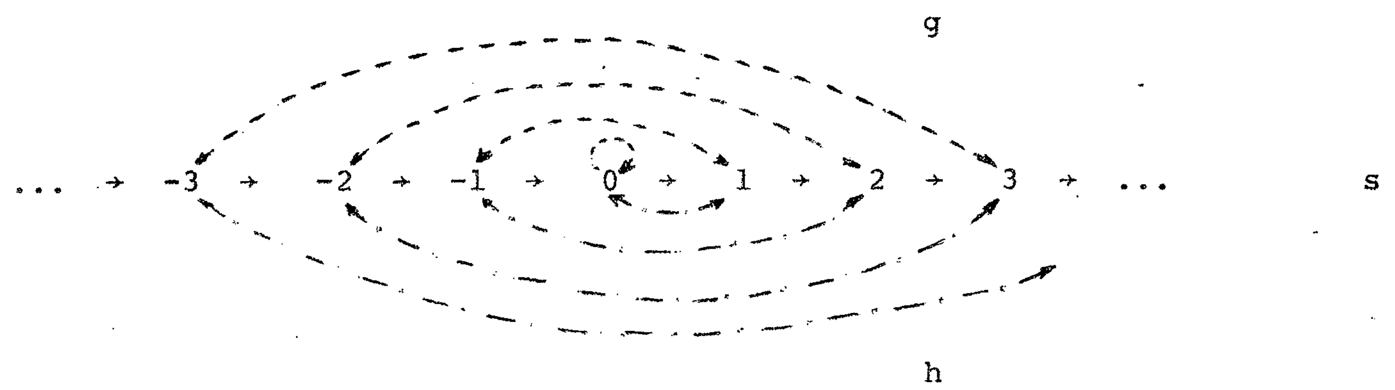
Figura 4

Agora o 6-ciclo c_9f_1 foi novamente encurtado por um 2-ciclo f_2 e obtivemos um $6-(2-1)=5$-ciclo $c_9f_1f_2$ e quatro ciclos triviais. (Observemos que $f=f_1f_2$ é uma permutação de 9, e que $\Lambda(f)=\Lambda(f_1)\cup\Lambda(f_2)$ porque f_2 não usa nenhum ponto em 9 que foi usado por f_1.

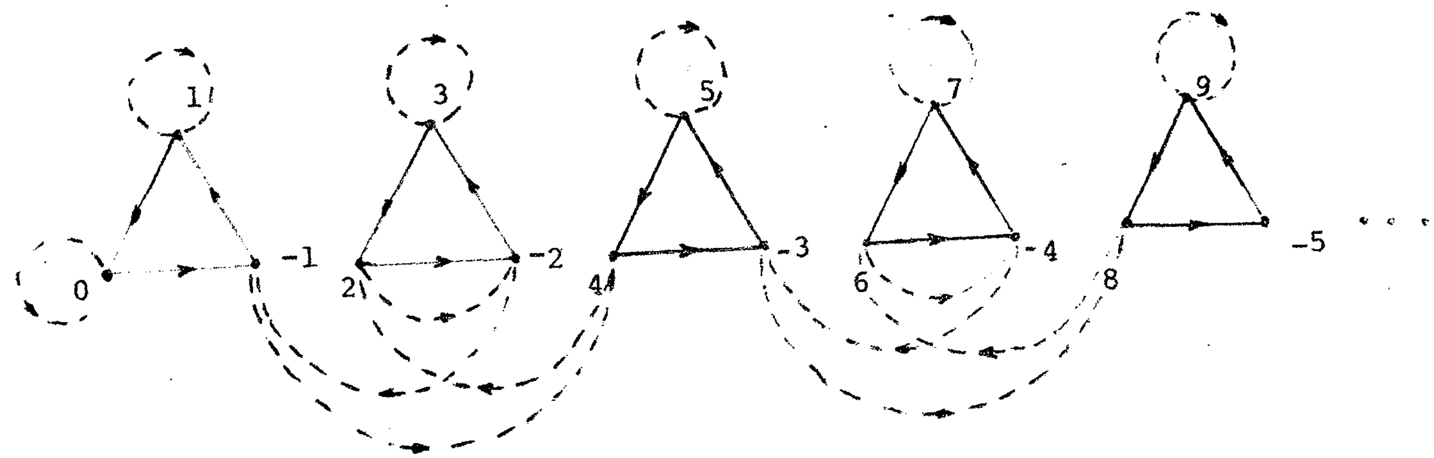
Desta forma temos que: $c_9f = (0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)(4\ 3\ 2\ 1)(7\ 6) = (0\ \underline{1}\ 5\ \underline{6}\ 8)$.

É claro que nós temos condições para encurtar, com uma f_3 que não usa pontos em 9 usados por f, um pouco mais.

Representação de s por involuções g e h: $s = hg$



A figura abaixo mostra a técnica, usada em [2], para mostrar que $s = g^2h^2$ com $\Lambda(g) = \{1,4\}$ e $\Lambda(h) = \{3\}$. Incidentalmente $\Lambda(g^2) = \{1,2\}$ e $\Lambda(h^2) = \{3\}$. Desta forma s pode ser escrita por um produto h_2h_3 ou $s \simeq s^{-1} \simeq h_3h_2$ onde $h_2 = g^2$ e $h_3 = h^2$. Tal fato pode constituir uma idéia para responder a pergunta 4.



g - linhas tracejadas

h - linhas contínuas.

Figura 6

Apresentamos a seguir uma nova demonstração do Lema 1.12, devida a D.M. Silberger, que não foi publicada anteriormente. Esta prova é por si só suficiente o que não ocorre com a demonstração original.

Demonstração: É evidente que se $\pi(\alpha)=\pi(\beta)=\pi(\alpha\beta)$, então $\alpha\beta=\beta\alpha$. Vamos demonstrar a recíproca.

Suponhamos que para quaisquer palavras σ e τ não vazias, se $|\sigma\tau|<|\alpha\beta|$ e se $\sigma\tau=\tau\sigma$, então $\pi(\sigma)=\pi(\tau)=\pi(\sigma\tau)$. Suponhamos também que $\alpha\beta=\beta\alpha$. Se $|\alpha|=|\beta|$, então $\alpha=\beta$ e portanto $\pi(\alpha)=\pi(\beta)$. Por outro lado, podemos supor, sem perda de generalização, que $|\alpha|<|\beta|$. Então existe $\rho\neq\phi$ tal que $\alpha\rho=\beta=\rho\alpha$, e portanto pela hipótese de indução segue que $\pi(\alpha)=\pi(\rho)=\pi(\alpha\rho)=\pi(\beta)$. Em qualquer caso $\pi(\alpha)=\pi(\beta)$. Basta agora mostrar que $\pi(\alpha)=\pi(\alpha\beta)$.

Desde que $\alpha\neq\phi\neq\beta$, então existe $\{a,b\}\subseteq \omega\setminus 1$ tal que $\pi(\alpha)^a=\alpha$ e $\pi(\alpha)^b=\beta$. Assim $\alpha\beta=\pi(\alpha)^{a+b}$; também existe $c\in\omega\setminus 1$ tal que $\alpha\beta=\pi(\alpha\beta)^c$. Segue-se que $|\pi(\alpha\beta)|\leq|\pi(\alpha)|$ e também que $c\geq a+b\geq 2$. Para concluir que $\pi(\alpha\beta)=\pi(\alpha)$, é suficiente demonstrar que $|\pi(\alpha\beta)|=|\pi(\alpha)|$.

Admitamos que $|\pi(\alpha\beta)|<|\pi(\alpha)|$. Então, da equação $\pi(\alpha\beta)^c=\pi(\alpha)^{a+b}$ temos que existem $n\in\omega\setminus 1$ e $\{\delta,\varepsilon\}\subseteq\Sigma^*$ tais que $|\delta|=|\varepsilon|<|\pi(\alpha\beta)|$ e tais que $\pi(\alpha\beta)^n\delta=\pi(\alpha)=\varepsilon\pi(\alpha\beta)^n$. Se $\delta=\phi$, então $\alpha=\pi(\alpha)^a=\pi(\alpha\beta)^{na}$ contradizendo a minimalidade de $|\pi(\alpha)|$. Segue-se que $0<|\delta|=|\varepsilon|<|\pi(\alpha\beta)|$.

Das relações $\varepsilon\pi(\alpha\beta)^n=\pi(\alpha\beta)^n\delta$ e $0<|\varepsilon|<|\pi(\alpha\beta)|$ temos que $\varepsilon\tau=\pi(\alpha\beta)$ para algum $\tau\in\Sigma^*\setminus\{\phi\}$. Então, $\varepsilon(\tau\varepsilon)^{n-1}\tau\delta=(\varepsilon\tau)^n\delta$ $=\pi(\alpha\beta)^n\delta=\varepsilon\pi(\alpha\beta)^n=\varepsilon(\varepsilon\tau)^n=\varepsilon(\varepsilon\tau)^{n-1}\varepsilon\tau$ e portanto $(\tau\varepsilon)^{n-1}\tau\delta=(\varepsilon\tau)^{n-1}\varepsilon\tau$. Inferimos que $\tau\delta=\varepsilon\tau$.

No caso que $n>1$ podemos inferir também que $\tau\varepsilon=\varepsilon\tau$ pois $(\tau\varepsilon)^{n-1}=(\varepsilon\tau)^{n-1}$, e então que $\tau\varepsilon=\tau\delta$, resultando que $\varepsilon=\delta$.

No outro caso, para $n=1$, temos que $\varepsilon\tau\delta=\pi(\alpha\beta)\delta=\pi(\alpha\beta)^n\delta=\pi(\alpha)=\varepsilon\pi(\alpha\beta)^n=\varepsilon\pi(\alpha\beta)=\varepsilon\varepsilon\tau$, e logo que $\varepsilon\tau\delta(\varepsilon\tau\delta)^{a+b-1}=(\varepsilon\tau\delta)^{a+b}=\pi(\alpha)^{a+b}=\alpha=\pi(\alpha\beta)^c=(\varepsilon\tau)^c=\varepsilon\tau(\varepsilon\tau)^{c-1}$, e então sendo $c\geqslant a+b\geqslant 2$ temos $\delta(\varepsilon\tau\delta)^{a+b-1}=(\varepsilon\tau)^{c-1}=\varepsilon\tau(\varepsilon\tau)^{c-2}$. Da equação seguinte $\delta(\varepsilon\tau\delta)^{a+b-1}=\varepsilon\tau(\varepsilon\tau)^{c-2}$ junto com a equação $|\delta|=|\varepsilon|$ inferimos que $\delta=\varepsilon$ também no caso em que $n=1$.

Em resumo, temos que $\pi(\alpha\beta)^n\delta=\pi(\alpha)=\varepsilon\pi(\alpha\beta)^n=\delta\pi(\alpha\beta)^n$, que $n\geqslant 1$ e que $\delta\neq\phi$, e também que $|\pi(\alpha\beta)^n\delta|=|\pi(\alpha)|\leqslant|\alpha|<|\alpha\beta|$. Portanto pela hipótese de indução segue que $\pi(\delta)=\pi(\pi(\alpha\beta)^n)=\pi(\delta\pi(\alpha\beta)^n)=\pi(\pi(\alpha))=\pi(\alpha)$. Mas, temos também que $|\pi(\delta)|\leqslant|\delta|<|\pi(\alpha\beta)|<|\pi(\alpha)|$, e portanto que $\pi(\delta)\neq\pi(\alpha)$. Da contradição obtida concluimos que $|\pi(\alpha\beta)|\not<|\pi(\alpha)|$. (F.P.)

BIBLIOGRAFIA

[1] Dickson, L.E. Introduction to theory of numbers. New York, Dover Publications Inc., 1957.

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

[3] Ehrenfeucht,A. e Silberger,D.M. Decomposing a transformation with an involution, Algebra Universalis 7(1977),179-190.

[4] Ehrenfeucht,A e Silberger,D.M. Universal terms of the form B^nA^m, Algebra Universalis.(A ser publicado.)

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

[6] McNulty,G.F. The decision problem for equational bases of algebras, Doctoral Dissertation, University of California, Berkeley,1972. (Ver também Annals of Math. Logic.)

[7] Silberger,D.M. B^nA^m is universal iff point universal, Algebra Universalis. (A ser publicado.)

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

[9] Silberger,D.M. Point universal terms in a free semigroup, Doctoral Dissertation, University of Washington, Seattle, 1973.

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

[11] Silberger,D.M. When is gf isomorphic to fg?, (A ser publicado)

[12] Weems (Harriss),M. Reverse spellings represent spikes for words of complexity two, Master's Thesis, Jackson State University, Jackson,Mississippi, 1977.