Grafos conexos e controle em códigos de treliça

Jorge Pedraza Arpasi , Edson Donizete de Carvalho , Leandro Rosniak Tibola

***Resumo*— A treliça de um código convolucional binário é um grafo conexo, isto é, todos os estados estão conectados por algum caminho formado pela concatenação de transições rotuladas pelos bits de informação codificada. Quando o código convolucional é não-binário, a treliça nem sempre vai ser um grafo conexo. Neste trabalho é mostrado a equivalência entre conexidade de grafos e controlabilidade dos códigos convolucionais de grupo que são gerados a partir de extensões de grupos. Mais precisamente; dado um grupo G como uma extensão U por S, i.e. $U \times S = G$, considere a família $\mathcal{H} = \{\nu : U \times S \to S \ ; \ \nu$ é um homomorfismo sobrejetor$\}$. Cada ν gera um grafo cujo conjunto de vértices é S, e conjunto de arestas é $\{(s, \nu(u, s)), u \in U, s \in S\}$.**
Então para G finito e não abeliano é discutido a existência de alguma extensão $U \times S = G$, S não abeliano, $|U| < \frac{|S|}{2}$, e algum $\nu \in \mathcal{H}$, tais que o grafo seja conexo.

***Abstract*— The trellis of a binary convolutional code is a connected graph, that is, all the states are connected by some path that is compounded by the concatenation of transitions labeled by encoded bits. When the convolucional code is not binary, then its trellis can be a disconnected graph. In this work it is shown the equivalence between connectedness of graphs and controllability of group codes which are generated from extensions of groups. More precisely; given a group G as an extension U by S, i.e. $U \times S = G$, consider a family $\mathcal{H} = \{\nu : U \times S \to S \ ; \ \nu$ is a surjective homomorphism$\}$. Each ν generates a graph whose vertex set is S, and edges set is $\{(s, \nu(u, s)), u \in U, s \in S\}$.**
Then for a finite and non-abelian G is discussed the existence of some extension $U \times S = G$, S non-abelian, $|U| < \frac{|S|}{2}$, and some $\nu \in \mathcal{H}$, such that the graph is connected.

***Palavras-Chave*— Grafos conexos, controle, códicos de treliça, TCM, extensão de grupos**

***Keywords*— Connected graphs, factor graphs control, trellis codes, TCM, extension of groups**

I. INTRODUÇÃO

A interpretação recente dos turbo codes e os códigos LDPC como exemplos notáveis de grafos tem despertado um enorme interesse no estudo dos grafos em diferentes áreas de estudo que vão desde Estatística, passando por filtros de Kalman, e até a teoria dos códigos [1]. A versatilidade da família dos *factor graphs* parece bastante promissória para resolver, de maneira unificada, problemas que até então estavam isoladas dentro dos limites de suas áreas específicas. Nessa "onda gráfica", o objetivo deste trabalho é transladar o problema de controlabilidade de códigos convolucionais sobre grupos não abelianos a uma linguagem gráfica, isto é, mostraremos que dizer que um código é controlável é equivalente a dizer que o grafo do código é conexo. Logo, a pergunta "que família de códigos convolucionais sobre grupos não abelianos é controlável?" se traduz como "que grafos conexos possuem grupo não abeliano subjacente?".

Para cada subgrupo N de um grupo G existem grupos U e S tais que: a) U é isomorfo a N, b) S é isomorfo ao grupo quociente $\frac{G}{N}$, e c) G é uma extensão de U por S. Cada elemento de G é um par ordenado de $(u, s) \in U \times S$. O produto direto de grupos e o produto semidireto de grupos são exemplos de extensão de grupos. Para cada homomorfismo sobrejetor $\nu : G = U \times S \to S$ existe um grafo cujo conjunto de vértices é S e cujo conjunto de arestas é $\{(s, \nu(u, s)); \ ; u \in U, \ s \in S\}$. Para cada grupo abeliano G que seja o produto direto $\mathbb{Z}_2^k \times \mathbb{Z}_2^m$, $k \leq m$; onde $\mathbb{Z}_2$ é o grupo binário $\{0, 1\}$ com a operação adição modulo 2, e $\mathbb{Z}_2^n = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ é o produto direto de grupos com a operação adição modulo 2 induzida componente a componente; é possível encontrar homomorfismos sobrejetores $\nu : \mathbb{Z}_2^k \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ tal que o grafo seja **conexo** e sem arestas **paralelas**.

Quando G é um grupo não abeliano e é uma extensão $U \times S$, com $|U| \leq |S|$, S não abeliano, com o software GAP, [2], foram testados todos os G com ordem menor ou igual a 256 e os únicos casos de extensão $U \times S$ com grafo conexo e sem arestas paralelas encontrados foram para algumas extensões onde $|U| = |S|$ ou $|U| = \frac{|S|}{2}$. Por outro lado em [3] foi mostrado que quando G é um p-grupo não abeliano; para a extensão $U \times S$, $|U| = p$, e S não abeliano; não existe um grafo conexo.
O problema é então: existe algum grupo não abeliano G que seja a extensão $U \times S$ com $|U| < \frac{|S|}{2}$ tal que o grafo respectivo seja conexo e sem transições paralelas?

A busca por grupos $G = U \times S$ com algum homomorfismo sobrejetor $\nu : U \times S \to S$ cujo grafo seja conexo e sem transições paralelas vem da teoria dos códigos convolucionais para detecção e correção de erros de transmissão de informação. Existem duas classes de códigos convolucionais: 1) os binários, sobre $\mathbb{Z}_2$ que é o grupo binário $\{0, 1\}$ com a operação adição modulo 2, e 2) os generalizados, sobre qualquer grupo, chamados de códigos de grupo, *group codes*. Em aplicações práticas em sistemas de telecomunicações os códigos convolucionais binários são amplamente usados, por exemplo, recentes modelos de telefones celulares e outros aparelhos que usam a tecnologia *wireless*, usam implementações, em forma de *turbo codes*, de códigos convolucionais binários. A busca por bons códigos convolucionais generalizados sobre grupos vem do fato que em [4] tem sido mostrado que para qualquer canal AWGN

Departamento de Ciências e Engenharias, Universidade Regional Integrada - URI, Frederico Westphalen, RS. Email: arpasi@fw.uri.br
Departamento de Matemática, Universidade Estadual Paulista - UNESP, Ilha Solteira, SP. Email: edson@mat.feis.unesp.br
Departamento de Ciências e Engenharias, Universidade Regional Integrada - URI, Frederico Westphalen, RS. Email: tibola@fw.uri.br

usando códigos abelianos com capacidade C_1, existe um canal AWGN com modulação PSK (Phase Shift Keying) com capacidade C_2, tal que $C_1 < C_2$.

Um bom código convolucional, além de outras, deve possuir duas propriedades: **controlabilidade**, e uma boa **distância mínima** d_{min}. Veremos que controlabilidade é equivalente a conexidade do grafo, e a existência de arestas paralelas é um limitante superior de d_{min}.

II. Códigos convolucionais binários

Uma máquina de estado finito ou autômato finito é uma quintupla $M = (U, S, Y, \nu, \omega)$, onde U é o conjunto das entradas, S é o conjunto dos estados e é finito, Y é o conjunto das saídas, $\nu : U \times S \to S$ é o mapeamento do próximo estado, e $\omega : U \times S \to Y$ é o mapeamento das saídas, [5], [6].

Considerando o produto direto de grupos $\mathbb{Z}_2^n = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, com a operação soma modulo 2 induzida componente a componente, temos que o codificador de um código convolucional binário de parâmetros (n, k, m) é uma máquina de estado finito $M = (\mathbb{Z}_2^k, \mathbb{Z}_2^m, \mathbb{Z}_2^n, \nu, \omega)$, com $k \leq m$, e $k < n$, $\nu : \mathbb{Z}_2^k \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ é o homomorfismo das transições entre estados, e $\omega : \mathbb{Z}_2^k \times \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ é chamado de homomorfismo codificador. O grupo $\mathbb{Z}_2^k$ é o grupo das entradas ou da informação não codificada, $\mathbb{Z}_2^m$ é o grupo dos estados(grupo latente ou não observável), e $\mathbb{Z}_2^n$ é o grupo da informação codificada. [7], [8]

Dados $j, k \in \mathbb{Z}$, $j \leq k$, consideremos os intervalos de inteiros $[j, k] = \{j, j+1, \ldots, k\}$, $(j, k] = \{j+1, j+2, \ldots, k\}$ e assim por diante. Isto pode ser estendido para $\pm\infty$, $(-\infty, j] = \{\ldots, j-2, j-1, j\}$, etc. Com esta notação se convenciona dizer que o passado de uma seqüência de informação não codificada $\{u_i\}_{i\in\mathbb{Z}}$, $u_i \in \mathbb{Z}_2^k$, é $\{u_i\}|_{(-\infty,0]} = \{\ldots, u_2, u_1, u_0\}$, o futuro é $\{u_i\}|_{[2,+\infty)}$, e a informação presente é u_1. Análogamente para uma seqüência de informação codificada $\{y_i\}_{i\in\mathbb{Z}}$, $y_i \in \mathbb{Z}_2^n$, onde $\{y_i\}|_{(-\infty,0]}$, $\{y_i\}|_{[2,+\infty)}$, $\{y_1\}$, são o passado, o futuro e o presente respectivamente. Para o caso de uma seqüência de estados $\{s_i\}_{i\in\mathbb{Z}}$, $s_i \in \mathbb{Z}_2^m$, o estado presente é s_0, e $\{s_i\}|_{(-\infty,-1]}$, $\{s_i\}|_{[1,+\infty)}$ são o passado e o futuro.

Dada uma seqüência de informação não codificada $\{u_i\}_{i\in\mathbb{Z}}$, e um estado presente s_0, usando a informação do presente M gera o próximo estado $s_1 = \nu(u_1, s_0)$, e a informação codificada do presente $y_1 = \omega(u_1, s_0)$. O estado presente depende do passado pois $s_0 = \nu(u_0, s_1)$, por isso M é dito um codificador com memória. A relação das três seqüências é dado no seguinte arranjo;

$$\begin{array}{cc} \vdots & \vdots \\ s_{-1} = \nu(u_{-1}, s_{-2}) & y_{-1} = \omega(u_{-1}, s_{-2}) \\ s_0 = \nu(u_0, s_{-1}) & y_0 = \omega(u_0, s_{-1}) \\ s_1 = \nu(u_1, s_0) & y_1 = \omega(u_1, s_0) \\ s_2 = \nu(u_2, s_1) & y_2 = \omega(u_2, s_1) \\ \vdots & \vdots \\ s_i = \nu(u_i, s_{i-1}) & y_i = \omega(u_i, s_{i-1}) \\ \vdots & \vdots \end{array}$$

Note-se a dependência da seqüência $\{y_i\}_{i\in\mathbb{Z}}$, de $\{s_i\}_{i\in\mathbb{Z}}$. Dizemos que a seqüência $\{u_i\}_{i\in\mathbb{Z}}$ é codificada na palavra-código $\{y_i\}_{i\in\mathbb{Z}}$. O conjunto das palavras-código é o código convolucional binário gerado por M.

Exemplo 1: Considere o código convolucional binário $(3, 1, 2)$ definido pelos homomorfismos $\nu(u, s_1, s_2) = (u, s_1)$ e $\omega(u, s_1, s_2) = (u + s_2, s_2, u + s_1)$, $u \in \mathbb{Z}_2$, $(s_1, s_2) \in \mathbb{Z}_2^2$ Por economia de notação, e desde que não exista perigo de confusão, é usual denotar $(0, 0) \in \mathbb{Z}_2^2$ por 00, $(0, 0, 0) \in \mathbb{Z}_2^3$ por 000, e assim por diante. Com esta notação econômica, suponha que estado inicial do codificador $M = (\mathbb{Z}_2, \mathbb{Z}_2^2, \mathbb{Z}_2^3, \nu, \omega)$ seja $00 \in \mathbb{Z}_2^2$ então a sequência $1, 1, 0, 1, 0, 0, 1, 1, 1, 0, \ldots$ gera de maneira única a sequência de estados $10, 11, 01, 10, 01, 00, 10, 11, 11, 01, \ldots$ a sequência de informação codificada $101, 100, 111, 011, 001, 110, 101, 100, 010, 111, \ldots$ do seguinte modo;

$$\begin{array}{l|l} \nu(0,00) = 10 & \omega(0,00) = 101 \\ \nu(1,10) = 11 & \omega(1,10) = 100 \\ \nu(0,11) = 01 & \omega(0,11) = 111 \\ \nu(1,01) = 10 & \omega(1,01) = 011 \\ \nu(0,10) = 01 & \omega(0,10) = 001 \\ \nu(0,01) = 00 & \omega(0,01) = 110 \\ \nu(1,00) = 10 & \omega(1,00) = 101 \\ \nu(1,10) = 11 & \omega(1,10) = 100 \\ \nu(1,11) = 11 & \omega(1,11) = 010 \\ \nu(0,11) = 01 & \omega(0,11) = 111 \\ \vdots & \vdots \end{array}$$

Definição 1: Dados dois conjunto não vazios V, E, um *grafo* é definido como sendo um par ordenado (V, E) tal que $E \subseteq V^2$ [9]. O conjunto V é o conjunto de vértices do grafo e E é o conjunto das arestas do grafo.
O diagrama de estados que descreve o codificador do Exemplo 1, é mostrado na Figura 1. É um grafo cujos vértices são os estados $\mathbb{Z}_2^2$ e cujas arestas são as transições entre estados $s \mapsto \nu(u, s)$, que significa que a entrada u modificou o estado s da máquina para o estado $\nu(u, s)$. Cada transição pode ser caracterizada de maneira única por $(s, \omega(u, s), \nu(u, s))$, de maneira que a rotulação das arestas pode ser feita usando as entradas $u \in \mathbb{Z}_2$, Figura 1 (a), ou as saídas $y \in \mathbb{Z}_2^3$, Figura 1 (b).◀

Definição 2: Um grafo é conexo quando para quaisquer par de vértices s, r, existir um caminho de arestas e vértices justapostos conectando r e s, [9].

Fig. 1. Diagrama de estados do Exemplo 1, (a):a rotulação de transições é feita usando o grupo de entradas, (b): a rotulação de transições é feita usando o grupo de saídas

III. EXTENSÕES DE GRUPOS, CÓDIGOS E GRAFOS

A definição de código convolucional binário pode ser estendida a qualquer grupo finito usando o conceito de extensão de grupos. Nesta generalização, o codificador convolucional é um autômato finito $M = (U, S, Y, \nu, \omega)$, onde os componentes U, S, e Y são grupos finitos, chamados de grupo das entradas, grupo dos estados, e grupo das saidas, respectivamente; ν e ω são homomorfismos de grupos definidos sobre a extensão de U por S, tais que, $\nu : U \times S \rightarrow S$ é sobrejetor e $\omega : U \times S \rightarrow Y$ é injetor [10]. Semelhantemente ao caso binário, o conjunto dos vértices, do grafo do codificador de grupo, é o grupo dos estados S, e conjunto das arestas é $\{(s, \omega(u, s), \nu(u, s)) \ ; \ u \in U, s \in S\}$. Dado um $s \in S$ fixo, uma palavra-código é a seqüência $\{\omega(u_k, s)\}_{k \in \mathbb{Z}}$. A classe de todas as palavras-código é o código de grupo (group code) gerado por M.

Para cada extensão $U \times S$, com U e S finitos, considere o conjunto $\mathcal{H} = \{\nu : U \times S \rightarrow S \ ; \ \nu$ é homomorfismo sobrejetor$\}$, que não é vazio, pelo menos, a projeção $\nu(u, s) = s$ é um elemento dele.

Cada máquina $M = (U, S, Y, \nu, \omega)$ define um único grafo cujos vértices são os estados S, enquanto que as arestas são os pares ordenados $E = \{(s, \nu(u, s)) \ ; \ s \in S\}$, e desde que cada aresta $(s, \nu(u, s)) \in E$ pode ser rotulada simplesmente por u, Figura 1 (a) , temos que a dinâmica do grafo é independente de ω e Y. Assim, para estudar as propriedades do grafo, podemos reduzir nossa máquina a $M = (U, S, \nu)$.

Definição 3: Sejam U e S grupos. Uma extensão de U por S é um grupo G tal que possui um subgrupo normal N isomorfo a U e com o grupo quociente $\frac{G}{N}$ isomorfo a S [11], [12].

De acordo com a Definição 3, todo grupo G é uma extensão de algum grupo U por algum outro grupo S, pois qualquer grupo possui pelo menos os subgrupos normais triviais. Se N é não trivial então U e S também serão não triviais. A operação do grupo extensão G em função das operações de U e S, pode ser construída fazendo três escolhas arbitrárias: 1) do conjunto dos representantes de $\frac{G}{N}$, 2) do isomorfismo entre $N \approx U$, e 3) do isomorfismo $\frac{G}{N} \approx S$. Mais precisamente;

Sejam l, υ e ϕ tais que; $l : \frac{G}{N} \rightarrow G$ é o mapeamento de escolha de representantes das classes laterais tal que o representante de N é o elemento identidade de G, isto é, $l(N) = id$; $\upsilon : N \rightarrow U$ é um isomorfismo entre N e U; e $\psi : S \rightarrow \frac{G}{N}$ é um isomorfismo entre S e o grupo quociente $\frac{G}{N}$.

Assim a operação de grupo sobre os pares (u, s) da extensão $U \times S$ é dada por;

$$(u_1, s_1).(u_2, s_2) = (u_1.\phi(s_1)(u_2).\varsigma(s_1, s_2) \ , \ s_1 s_2), \qquad (1)$$

onde $\phi : S \rightarrow Aut(U)$ e $\varsigma : S \times S \rightarrow U$ são definidas como

$$\phi(s)(u) = \upsilon[l(\psi(s)).\upsilon^{-1}(u).(l(\psi(s)))^{-1}], \qquad (2)$$

e

$$\varsigma(s, t) = \upsilon[l(\psi(s)).l(\psi(t)).(l(\psi(st)))^{-1}]. \qquad (3)$$

Algumas observações importantes sobre ϕ, ς, e l:

- Se G é abeliano, então para qualquer $s \in S$, $\phi(s)$ é o automorfismo identidade de U. A recíproca é falsa (Exemplo 3)
- Quando o conjunto dos representes $l(\frac{G}{N})$ é grupo então l é homomorfismo e $\varsigma(s, t) = id$, para todo $s, t \in S$. Neste caso ϕ é homomorfismo e temos que a extensão é um produto semidireto.
- Quando $\phi \neq id$ temos que a extensão é um grupo não abeliano.
- Da primeira observação, todo produto direto e produto semidireto de grupos são casos particulares de uma extensão de grupos.

Exemplo 2: Considere o grupo $G = \mathbb{Z}_2^3 = \{abc \ ; \ a, b, c \in \mathbb{Z}_2\}$, com a operação produto direto $(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_2 + c_2)$ modulo 2. Temos que $N = \{000, 100\}$ é um subgrupo normal de $\mathbb{Z}_2^3$, e $\frac{\mathbb{Z}_2^3}{N}$ é isomorfo a $\mathbb{Z}_2^2$.

A operação de grupo, natural, de $\mathbb{Z}_2^3 = \mathbb{Z}_2 \times \mathbb{Z}_2^2$ é: $(u_1, s_1)(u_2, s_2) = (u_1 + u_2, s_{11} + s_{21}, s_{12} + s_{22})$ modulo 2, onde $s_i = s_{i1} s_{i2} \in \mathbb{Z}_2^2$. Fazendo o procedimento de escolhas adequadas de l, υ, e ψ e posterior uso da equação (1) também obteremos a mesma operação. Para isto, considere as seguintes escolhas de l, υ, e ψ;

$\mathbb{Z}_2^2$	ψ	$\frac{\mathbb{Z}_2^3}{N}$	l	$\mathbb{Z}_2^3$
00	$\mapsto$	$\{000, 100\}$	$\mapsto$	000
10	$\mapsto$	$\{010, 110\}$	$\mapsto$	010
01	$\mapsto$	$\{001, 101\}$	$\mapsto$	001
11	$\mapsto$	$\{011, 111\}$	$\mapsto$	011
		$\downarrow \upsilon$		
		$\{0, 1\}$		
		$\mathbb{Z}_2$		

Alguns exemplos desta escolha: $l(010N) = 010$, $\upsilon(100) = 1 \in \mathbb{Z}_2$, $\psi(01) = 001N$, etc. Por ser $\mathbb{Z}_2^3$ abeliano, ϕ da equação (2) é trivial, e como l é homomorfismo, temos ς da equação (3) também é trivial. Logo a operação em $\mathbb{Z}_2^3$, considerado como extensão $\mathbb{Z}_2 \times \mathbb{Z}_2^2$, é dado por $(u_1, s_1)(u_2, s_2) = (u_1 + u_2, s_{11} + s_{21}, s_{12} + s_{22})$ modulo 2, onde $s_i = s_{i1} s_{i2} \in \mathbb{Z}_2^2$, a mesma operação descrita anteriormente. Para este produto direto binário, existem

muitos homomorfismos sobrejetores $\nu : \mathbb{Z}_2 \times \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$ além da projeção $\nu(u, s_1 s_2) = (u, s_1)$ do código $(3, 1, 2)$, do Exemplo 1. Em geral para os grupos binários $G = \mathbb{Z}_2^n$, expressos como extensões $\mathbb{Z}_2^k \times \mathbb{Z}_2^m$, $k + m = n$, podemos sempre obter homomorfismos sobrejetores $\nu : \mathbb{Z}_2^k \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ de modo que o grafo seja conexo. ◄

Exemplo 3: Considere o grupo das simetrias do quadrado, $D_8 = \{R_0, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}, d_1, d_2, H, V\}$ e o subgrupo normal $N = \{R_0, R_\pi\}$.
Temos $N \approx \mathbb{Z}_2$, e $\frac{D_8}{N} \approx \mathbb{Z}_2^2$. Logo D_8 também é uma extensão de $\mathbb{Z}_2$ por $\mathbb{Z}_2^2$. Consideremos as escolhas l, υ, e ψ dadas no seguinte arranjo;

$\mathbb{Z}_2^2$	ψ	$\frac{D_8}{N}$	l	D_8
00	$\mapsto$	$\{R_0, R_\pi\}$	$\mapsto$	R_0
10	$\mapsto$	$\{R_{\frac{\pi}{2}}, R_{\frac{3\pi}{2}}\}$	$\mapsto$	$R_{\frac{\pi}{2}}$
01	$\mapsto$	$\{d_1, d_2\}$	$\mapsto$	d_1
11	$\mapsto$	$\{H, V\}$	$\mapsto$	H
		$\downarrow \upsilon$		
		$\{0, 1\}$		
		$\mathbb{Z}_2$		

Para estas escolhas temos que l não é homomorfismo, mais ainda, para esta extensão, nenhuma escolha de l é homomorfismo. Como $Aut(\mathbb{Z}_2) = id$, temos ϕ da equação (2) é trivial. Logo a operação da equação (1), para este caso é dada por $(i_1, i_2 i_3)(j_1, j_2 j_3) = (i_1 + j_1 + \varsigma(i_2 i_3, j_2 j_3), i_2 i_3 + j_2 j_3)$. Exemplifiquemos esta operação por $(0, 10)(1, 10)$ = $(0 + 1 + \varsigma(10, 10), 10 + 10)$ = $(1 + \upsilon(l(\psi(10))l(\psi(10))(l(\psi(00)))^{-1}), 00)$ = $(1 + \upsilon(R_{\frac{\pi}{2}} R_{\frac{\pi}{2}}), 00)$ = $(0, 00)$. Como o único subgrupo normal de ordem 2 é $N = \{R_0, R_\pi\}$ = $\{(0, 00), (1, 00)\}$. Segue que para todo homomorfismo sobrejetor $\nu : \mathbb{Z}_2 \times \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$, o kernel $ker(\nu)$ deve ser N. Isto acontece independentemente da escolha do conjunto de representantes l dado na equação (1). Portanto não existe uma grafo conexo para $N = \{(0, 00), (1, 00)\}$.
Na Figura 2 é mostrado o grafo desconexo de D_8 para o homomorfismo $\nu(a, bc) = bc$. Por outro lado, se considerarmos as outras possíveis extensões associadas aos subgrupos normais $\{R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}\}$, $\{R_0, R_\pi, H, V\}$, e $\{R_0, R_\pi, d_1, d_2\}$ também verificaremos que não existe maneira de construir um grafo associado que seja conexo.
Portanto, para o grupo D_8 não existe uma extensão U por S tal que o grafo seja conexo. ◄

Definição 4: Duas arestas $(s_1, \nu(u_1, s_1))$ e $(s_2, \nu(u_2, s_2))$ são ditas paralelas quando $s_1 = s_2$, e $\nu(u_1, s_1) = \nu(u_2, s_2)$ com $u_1 \neq u_2$.

O conjunto das arestas E com a operação $(s_1, \nu(u_1, s_1)) * (s_2, \nu(u_2, s_2))$ = $(s_1 s_2, \nu(u_1, s_1)$
$\nu(u_2, s_2))$ = $(s_1 s_2, \nu((u_1, s_1)(u_2, s_2)))$ forma um grupo, sendo o grupo das arestas do grafo da máquina $M = (U, S, \nu)$.

Proposição 1: Se $U \times S$ é uma extensão e $\nu : U \times S \to S$ é um homomorfismo sobrejetor, então o grupo das arestas E do grafo associado à máquina de estados $M = (U, S, \nu)$ possui as seguintes propriedades:

1) $E \approx G$

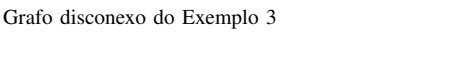

Fig. 2. Grafo disconexo do Exemplo 3

2) Se id é o elemento identidade do grupo de estados S. Então o conjunto das arestas que saem de id, $E_0 = \{(id, \nu(u, id));\ u \in U\}$ é um subgrupo normal de E. Mais ainda, $E_0 \approx U$ e $\frac{E}{E_0} \approx S$.
3) O conjunto das arestas que chegam em id, $E_1 = \{(u, s) \in Ker(\nu);\ u \in U, s \in S\}$ é um subgrupo normal de E, e $\frac{E}{E_1} \approx S$.
4) De cada estado saem e chegam a mesma quantidade de arestas.
5) Se $E_0 \cap E_1 \neq \{(id, \nu(id, id))\}$ então E possui transições paralelas.
6) Se G é não abeliano e o grupo de estados S é abeliano, então o grafo possui arestas paralelas.

O ítem (6) da Proposição 1 serve como um critério necessário para construir grafos sem arestas paralelas. A prova desta propriedade é baseada no fato que se $\frac{E}{E_0} \approx \frac{E}{E_1} \approx S$ é abeliano, então o grupo dos comutadores E' esta contido em $E_0 \cap E_1$. Como E é não abeliano, $E' \neq (id, \nu(id, id))$. Logo, pelo ítem (5) da Proposição 1, concluimos que o grafo têm arestas paralelas.

Uma propriedade importante de um código de grupo é a controlabilidade, que significa que dados dois estados quaisquer $s, r \in S$ deve existir uma seqüência finita de entradas $\{u_k\}_{k=1}^n$, tal que $s = \nu(u_1, \nu(u_2, \ldots, \nu(u_n, r) \ldots))$. Portanto, de acordo a Definição 2, temos então que conexidade e controlabilidade são conceitos equivalentes.

Para o caso binário, dados os parâmetros (n, k, m), sempre é possível encontrar um homomorfismo sobrejetor $\nu : \mathbb{Z}_2^k \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ tal que o código seja controlável, por exemplo podemos tomar a projeção $\nu(u_1, \ldots, u_k, s_1, \ldots, s_m)$

= $(u_1, \ldots, u_k, s_1, \ldots, s_{m-k})$. Para o caso geral, especialmente o caso não abeliano, dada a extensão $U \times S$ nem sempre é possível encontrar ν tal que $\nu : U \times S \to S$ é um homomorfismo sobrejetor tal que o código seja controlável, ou seja com grafo conexo, Exemplo 3. Um código não controlável não pode ser um bom código.

A distância de Hamming de duas palavras código $\{y_k\}_{k\in\mathbb{Z}}, \{y'_k\}_{k\in\mathbb{Z}}$ é dada por $d(\{y_k\}, \{y'_k\})$ = *número de posições em que são diferentes*. Por exemplo se $\{y_k\}_{k\in\mathbb{Z}}$ é tal que $\{y_k\}|_{[-2,2]} = \{0, 0, 0, 0, 0\}$, $\{y_k\}|_{(-\infty,-2)} = \{\ldots, 1, 1, 1\}$, e $\{y_k\}|_{(2,+\infty)} = \{1, 1, 1, \ldots\}$, e

$y'_k = \begin{cases} 0, & k = 0 \\ 1, & \text{em outro caso} \end{cases}$, teremos $d(\{y_k\}, \{y'_k\}) = 4$. Para o caso em que este número de posições não é finito se diz que a distância é infinita. Por exemplo, a distância de Hamming entre as seqüências $\ldots 1, 1, 1, 1, \ldots$ e $\ldots, 0, 0, 0, 0, \ldots$ é infinita.

A distância mínima do código é d_{min} = $\min\{d(\{y_k\}, \{y'_k\}) \;;\; \{y_k\}, \{y'_k\}$ palavras código$\}$. Esta d_{min} deve ser a maior possível. Se o grafo do codificador tem arestas paralelas $E_1 = (s, \nu(u_1, s))$ e $E_2 = (s, \nu(u_2, s)$ então teremos que $d_{min} \leq d(\omega(u_1, s), \omega(u_2, s))$. Daí o interesse em buscar extensões $G = U \times S$ com grafos sem arestas paralelas. Pelo ítem 6 da Proposição 1, temos que se G é não abeliano então S necessariamente deve ser não abeliano para o grafo não ter arestas paralelas.

Problema 1: Existe algum grupo não abeliano G para o qual exista uma extensão U por S, S não abeliano, $|U| < \frac{|S|}{2}$, tal que o grafo associado seja conexo?

Neste sentido em [3] tem sido provado que quando G é um p-grupo não abeliano, igual a uma extensão $\mathbb{Z}_p$ por S, $|S| = p^{m-1}$, para algum $m \in \mathbb{N}$, S não abeliano, então não existe grafo conexo para a extensão $\mathbb{Z}_p \times S$.

REFERÊNCIAS

[1] Hans-Andrea Loeliger. An introduction to factor graphs. *IEEE Signal Processing Magazine*, pages 28–41, January 2004.

[2] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005. (http://www.gap-system.org).

[3] Jorge P. Arpasi and Yurilev Chalco-Cano. p-groups as trellis section of a time invariant group code. *International Journal on Computational and Applied Mathematics*, 2(1):67–74, 2007.

[4] H.A. Loeliger. Signal sets matched to groups. *IEEE Trans. Inform. Theory*, 37:1675–1682, November 1991.

[5] Michael A. Arbib. Algebraic structure of machine languages. In M. A. Arbib, editor, *Automaton Decomposition and Semigroup Structure*. 1968.

[6] Michael A. Arbib. *Brains, Machines and Mathematics*. Springer Verlag, New York, second edition, 1986.

[7] Shu Lin and Daniel J. Costello. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, New Jersey, 1983.

[8] Sergio Benedetto, Ezio Biglieri, and Valentino Castellani. *Digital Transmission Theory*. Prentice Hall International, New Jersey, 1987.

[9] Reinhard Diestel. *Graph Theory*. Springer Verlag, New York, third edition, 2005.

[10] H. A. Loeliger and T. Mittelholzer. Convolutional codes over groups. *IEEE Transactions on Information Theory*, 42:1659–1687, 1996.

[11] Marshall Hall. *The Theory of Groups*. Mac Millan, New York, 1959.

[12] Joseph Jean Rotman. *An Introduction to the Theory of the Groups*. Springer Verlag, New York, fourth edition, 1995.