Codificadores convolucionais generalizados com pacotes de informação de comprimento primo

Jorge Pedraza Arpasi

***Resumo*— Códigos convolucionais generalizados sobre grupos arbitrários são necessários a partir do trabalho de Ungerboeck, o mesmo que trata sobre casamento entre bits codificados e constelações de sinais. O conjunto das palavras de um código convolucional formam um sistema dinâmico que precisa ser bem comportado, isto é, ser controlável e observável. Um código que não seja controlável não pode ser um bom código. Neste trabalho mostramos que códigos convolucionais gerados pela extensão não-abeliana $\mathbb{Z}_p \boxtimes S$, onde $\mathbb{Z}_p$ é o grupo cíclico $\{0, 1, 2, \ldots, p-1\}$, p primo, não são controláveis ou tem distancia livre limitada por transições paralelas.**

Palavras-Chave.- Códigos convolucionais generalizados, códigos de treliça, controle, p-grupos

I. INTRODUÇÃO

Forney e Trott, em [1], perceberam que o codificador convolucional com taxa de transmissão $\frac{1}{3}$ e memória 2 da Figura 1 pode ser descrito como uma máquina de estados $M = (\mathbb{Z}_2, \mathbb{Z}_2^2, \mathbb{Z}_2^3, \nu, \omega)$. Este codificador, que em [2] é denotado por $(3, 1, 2)$, tem como alfabeto de entradas o conjunto $\mathbb{Z}_2 = \{0, 1\}$, como saídas $\mathbb{Z}_2^3 = \{000, 100, \ldots, 111\}$, e como o conjunto dos estados $\mathbb{Z}_2^2 = \{00, 10, 01, 11\}$. Cada um dos conjuntos $\mathbb{Z}_2, \mathbb{Z}_2^2, \mathbb{Z}_2^3$, com a operação soma módulo 2, executada componente a componente, é um grupo. Por exemplo, para o caso $\mathbb{Z}_2^3$ temos 100+111=011, 000+101=101, 101+101=000, etc. Isto mostra informalmente que $\mathbb{Z}_2^3$ com a soma módulo 2 possui as propriedades de clausura, associatividade, elemento neutro, e elemento inverso necessárias para ter estrutura de grupo. Mais ainda, estes grupos binários são grupos abelianos, pois a operação soma módulo 2 é comutativa. O conjuntos $\mathbb{Z}_2^2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, e $\mathbb{Z}_2^3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2^2$ são produtos cartesianos chamados de grupos **produto direto**. A dinâmica do codificador da Figura 1 pode ser descrita pelo mapeamento do próximo estado $\nu : \mathbb{Z}_2 \times \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$ e pelo mapeamento codificador $\omega : \mathbb{Z}_2 \times \mathbb{Z}_2^2 \to \mathbb{Z}_2^3$ sendo que ambos são homomorfismos de grupos definidos por $\nu(u, s_1 s_2) = (u, s_1)$ e $\omega(u, s_1 s_2) = (u + s_2, s_2, u + s_1)$. Em geral, para qualquer taxa de transmissão $\frac{k}{n}$ e qualquer memória m, um codificador convolucional binário pode ser definido como a máquina de estados $M = (\mathbb{Z}_2^k, \mathbb{Z}_2^m, \mathbb{Z}_2^n, \nu, \omega)$ onde $\nu : \mathbb{Z}_2^k \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ é o homomorfismo do próximo estado e $\omega : \mathbb{Z}_2^k \times \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ é o homomorfismo codificador. Como $k+m \geq m$, temos que ν é homomorfismo sobrejetor, enquanto que, para evitar códigos catastróficos o homomorfismo codificador ω deve ser injetor, isto é, $n \geq k + m$ necessariamente.

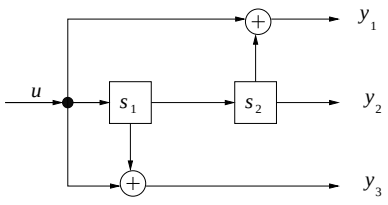

Fig. 1. O codificador de um código binário $(3, 1, 2)$

Desde o trabalho de Ungerboeck [3], onde o problema central era o casamento entre os pacotes de bits codificados que formam o grupo binário $\mathbb{Z}_2^n$, e uma constelação de sinais S, houve a necessidade de ampliar o conceito de códigos convolucionais. Então foram introduzidos conceitos de **códigos convolucionais generalizados** sobre grupos (*group codes*) [1], e **casamento** entre grupos e pontos discretos de um espaço Euclidiano, [4]. Os grupos referidos nesta generalização podem ser até grupos **não-abelianos**. Em [4], Loeliger mostra teoricamente que para um canal AWGN dado, usando códigos convolucionais abelianos sua capacidade de transmissão é limitada superiormente pela capacidade de um canal AWGN com modulação PSK (Phase Shift Keying). Assim, canais usando códigos convolucionais sobre grupos não-abelianos poderiam superar esta limitação.

Um conceito fundamental da álgebra que é necessário para definir codificadores convolucionais generalizados, e portanto códigos convolucionais generalizados, é a definição de **extensão de grupos** que introduziremos na Seção II, onde será mostrado que produto direto de grupos é um caso particular de extensão de grupos. Na seção III definiremos codificadores convolucionais generalizados e a abordagem dos códigos convolucionais como sequências bi-infinitas que para serem bons códigos precisam ser bem comportados quando identificados como **sistemas dinâmicos** [5], [4], [1], [6] Um sistema dinâmico bem comportado precisa ser **observável** e **controlável** [7]. Na Seção IV enfocaremos os codificadores convolucionais sobre a extensão não-abeliana $\mathbb{Z}_p \boxtimes S$, onde p é primo e $\mathbb{Z}_p$ é o grupo cíclico $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ e mostraremos que um código convolucional, definido sobre esta extensão, não é controlável ou tem distância livre limitada por transições paralelas.

II. EXTENSÃO DE GRUPOS

Definições padrão de extensão de grupos são dados em [8], [9], entre outros. Para a definição que daremos a seguir, ao elemento neutral(identidade) de um grupo genérico G

Departamento de Ciências Exatas e Engenharias, Universidade Regional Integrada - URI, Frederico Westphalen, RS. Email: arpasi@fw.uri.br

denotaremos por e, a notação $N \triangleleft G$ significa N é um subgrupo normal de G, enquanto que $H \cong K$ será a notação para um isomorfismo entre H e K.

Definição 1: Uma **extensão** de um grupo U por outro S é um grupo G que possui um subgrupo normal $N \triangleleft G$, tal que $N \cong U$ e $\frac{G}{N} \cong S$. ∘

Dado que cada grupo G, pelo menos, possui seus subgrupos normais triviais, então cada grupo G sempre é a extensão de algum grupo U por grupo S, à qual denotaremos por $U \boxtimes S$. Isto significa que cada elemento $g \in G$ pode ser "factorado"ou decomposto como um único par ordenado (u, s), $u \in U$ e $s \in S$. A construção desta fatoração é baseada na escolha dos isomorfismos $\psi : S \to \frac{G}{N}$ e $\upsilon : N \to U$ referidos na Definição 1, e de um levantamento $l : \frac{G}{N} \to G$, chamado também escolha de representante de classe, tal que $l(N) = e$. Com estas escolhas são definidos os mapeamentos $\varsigma : S \times S \to U$ e $\phi : S \to Aut(U)$,

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

e

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

Então $U \boxtimes S$ com a operação

$$(u_1, s_1) * (u_2, s_2) = (u_1.\phi(s_1)(u_2).\varsigma(s_1, s_2)\,,\, s_1 s_2) \quad (3)$$

é um grupo isomorfo com G.

O produto semidireto $U \rtimes S$ é um caso particular de extensão, onde $\varsigma(s,t) = e \in U$ para quaisquer $s, t \in S$. Por outro lado, o produto direto é um caso particular de extensão, onde $\varsigma(s,t) = e \in U$ para quaisquer $s, t \in S$, e $\phi(s)$ é o automorfismo identidade para qualquer $s \in S$. Portanto a extensão $U \boxtimes S$ é uma generalização do produto direto $U \times S$, conforme dizeramos linhas acima.

Exemplo 1: Considere o grupo $\mathbb{Z}_2^3 = \{(x_1, x_2, x_3)\ ;\ x_i \in \mathbb{Z}_2\}$. Este grupo abeliano pode ser decomposto como o produto direto $\mathbb{Z}_2 \times \mathbb{Z}_2^2$ e portanto uma extensão de $\mathbb{Z}_2$ por $\mathbb{Z}_2^2$. ∘

Exemplo 2: Considere o grupo das simetrias do quadrado, $D_8 = \{R_0, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}, d_1, d_2, H, V\}$, onde $R_{i\frac{\pi}{2}}$ é uma rotação do quadrado, no sentido anti-horário, de $i\frac{\pi}{2}$ radianos, d_1, e d_2 são reflexões referidas às diagonais, e H, V são as reflexões horizontal e vertical respectivamente.

Um subgrupo normal é $N = \{R_0, R_\pi\} \cong \mathbb{Z}_2$, e para o grupo dos cosets $\frac{D_8}{N}$ temos $\mathbb{Z}_2^2 \cong \frac{D_8}{N}$. Na Tabela I temos as escolhas de ψ, υ, e l. Por exemplo, $\psi(10) = \{R_{\pi/2}, R_{3\pi/2}\}$, $\upsilon(R_0) = 0$, e $l(\{R_{\pi/2}, R_{3\pi/2}\}) = R_{\pi/2}$. Com isto, a operação de grupo para $D_8 = \mathbb{Z}_2 \boxtimes \mathbb{Z}_2^2$ é dada por $(i_1, i_2 i_3)(j_1, j_2 j_3) = (i_1 + j_1 + \varsigma(i_2 i_3, j_2 j_3), i_2 i_3 + j_2 j_3)$. Por exemplo; $(0, 10)(1, 10)$ = $(0 + 1 + \varsigma(10, 10), 10 + 10)$ = $(1 + \upsilon(l(\psi(10))l(\psi(10))(l(\psi(00)))^{-1}), 00)$ = $(1 + \upsilon(R_{\frac{\pi}{2}} R_{\frac{\pi}{2}}), 00)$ = $(R_0, 00)$. ∘

Notemos que o resultado de $(u_1, s_1).(u_2, s_2)$, da operação acima (3), é $(u', s_1 s_2)$ para algum u' e onde $s_1 s_2$ é a operação do grupo S. Esta propriedade nos deixa livres da preocupação do cálculo exato do produto de múltiplos pares. Por exemplo na prova de alguns Lemas será suficiente saber que $(u', s_1 s_2 \dots s_n)$, é o par resultante do produto múltiplo $(u_1, s_1) \cdot (u_2, s_2) \cdot (u_3, s_3) \dots (u_n, s_n)$, onde u' é algum elemento de U. Analogamente, $(u, s)^n = (u', s^n)$ para algum $u' \in U$.

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

TABELA I
ESCOLHAS DOS ISOMORFISMOS ψ E υ, E O LEVANTAMENTO l PARA O EXEMPLO 2

III. CODIFICADORES E CÓDIGOS CONVOLUCIONAIS GENERALIZADOS

Definição 2: Um codificador homomorfo generalizado é uma máquina $M = (U, Y, S, \omega, \nu)$, onde o alfabeto de entrada U, o alfabeto de saída Y, e o conjunto dos estados da máquina S são grupos tais que o mapeamento do próximo estado ν é um homomorfismo sobrejetor e o mapeamento codificador ω é um homomorfismos injetor, ambos definidos assim;

$$\begin{cases} \nu : U \boxtimes S \to S \\ \omega : U \boxtimes S \to G \end{cases}$$

∘

Exemplo 3: Considere o grupo produto direto $\mathbb{Z}_2^3 = \{(x_1, x_2, x_3)\ ;\ x_i \in \mathbb{Z}_2\}$ (Exemplo 1). Definindo $\nu : \mathbb{Z}_2 \times \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$ como sendo $\nu(u, s_1, s_2) = (u, s_1)$ e $\omega : \mathbb{Z}_2 \times \mathbb{Z}_2^2 \to \mathbb{Z}_2^3$ por $\omega(u, s_1, s_2) = (u + s_2, s_2, u + s_1)$; temos um codificador $M = (\mathbb{Z}_2, \mathbb{Z}_2^2, \mathbb{Z}_2^3, \nu, \omega)$ que gera o codificador binário da Figura 1.

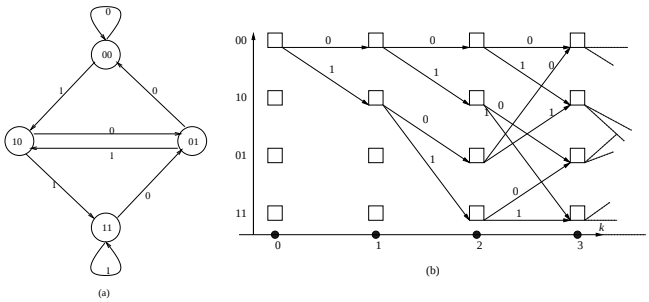

Fig. 2. Representação gráfica do código convolucional $(3, 1, 2)$: (a) Diagrama de estados estático conforme Teoria dos grafos, (b) Dinâmica da Treliça conforme Teoria de códigos corretores de erros.

Supondo que o estado inicial do codificador M seja 00, temos que a sequência de bits de entrada $1, 1, 0, 1, 0, 0, 1, 1, 1, 0, \dots$ gera de maneira única a sequência de estados $10, 11, 01, 10, 01, 00, 10, 11, 11, 01, \dots$ e a sequência de bits codificados $101, 100, 111, 011, 001, 110, 101, 100, 010, 111, \dots$ da

seguinte forma;

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

$\circ$

Exemplo 4: Considere o grupo das simetrias do quadrado, D_8 (Exemplo 2). Considere o codificador dado por $\omega(a, bc) = (a, bc)$ e $\nu(a, bc) = bc$ temos um codificador $M = (\mathbb{Z}_2, \mathbb{Z}_2^2, D_8, \nu, \omega)$.
O codificador para esta extensão não-abeliana, não é implementável como um circuito registrador de deslocamentos. No entanto ele possui um diagrama de estados e um diagrama de treliça mostrados na Figura 3. $\circ$

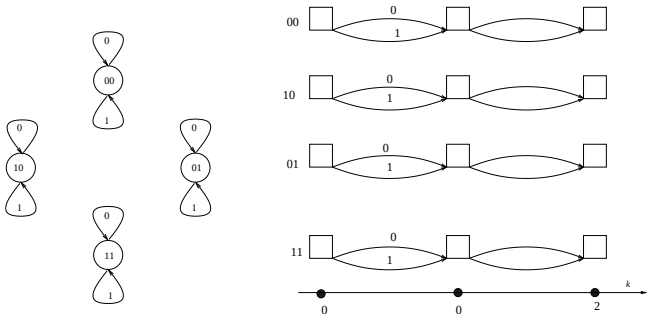

Fig. 3. (a) Grafo disconexo do codificador 4 (b)Treliça

Seja $\mathcal{C}$ o código binário produzido pelo codificador da Figura 1 e Exemplo 1, temos que $\mathcal{C}$ é um conjunto de sequências de pacotes de três bits, por exemplo $\{101, 100, 111, 011, 001, 110, 101, 100, 010, 111, \dots\} \in \mathcal{C}$. Então, considerando o produto direto infinito $(\mathbb{Z}_2^3)^{\mathbb{N}} = \mathbb{Z}_2^3 \times \mathbb{Z}_2^3 \times \dots$ temos $\mathcal{C}$ é um subgrupo de $(\mathbb{Z}_2^3)^{\mathbb{N}}$. Sob o ponto de vista dos sistemas dinâmicos, $\mathcal{C}$ pode ser descrito como um sistema invariante no tempo, pois para cada índice em $\mathbb{N}$, o grupo $\mathbb{Z}_2^3$ é repetido. Por isso, também, estes códigos são chamados códigos convolucionais invariantes no tempo.
Um código convolucional generalizado é indexado sobre os inteiros $\mathbb{Z}$.

Definição 3: Considere uma família de grupos $\{G_k\}_{k\in\mathbb{Z}}$ e o produto direto, indexado em $\mathbb{Z}$, $\mathcal{G} = \cdots \times G_{k-1} \times G_k \times G_{k+1} \times \dots$. Temos que cada elemento deste produto é um sequência $\{g_k\}_{k\in\mathbb{Z}}$, $g_k \in G_k$, e com as operações de grupo induzidas componente a componente sobre cada G_k, $\mathcal{G}$ também é grupo. Então, um código convolucional generalizado $\mathcal{C}$, é um subgrupo de $\mathcal{G}$. $\circ$
Se para cada G_k temos que $G_k = G$, então temos $\mathcal{G} = G^{\mathbb{Z}} = \cdots \times G \times G \times G \times \dots$. E neste caso temos que um subgrupo $\mathcal{C}$ de $\mathcal{G}$ chamado de *código convolucional invariante no tempo* [5], [4], [1], [6].

Uma sequência $\{\mathbf{c}_k\}_{k\in\mathbb{Z}} \in \mathcal{C}$ é chamada de *palavra-código*. Dados dois inteiros i, j, com $i \leq j$, usaremos as notações $[i, j]$, $[i, j)$, $(i, j]$, e (i, j) para intervalos inteiros. Por exemplo, $[i, j] = \{i, i + 1, \dots, j - 1, j\}$, $[i, j) = \{i, i + 1, \dots, j - 1\}$, e assim por diante. Esta notação também funciona em em conjuntos discretos infinitos tal como $\{k \in \mathbb{Z} \ ; \ k \leq j\}$ = $(-\infty, j]$. Com isto a projeção de uma palavra-código $\{\mathbf{c}_k\}_{k\in\mathbb{Z}}$ sobre o conjunto de índices $[i, j]$ é denotado por $\{\mathbf{c}\}|_{[i,j]} = \{\mathbf{c}_i, \mathbf{c}_{i+1}, \dots, \mathbf{c}_j\}$.

Dadas duas palavras-código $\{\mathbf{c_1}_k\}_{k\in\mathbb{Z}}$, $\{\mathbf{c_2}_k\}_{k\in\mathbb{Z}} \in \mathcal{C}$, uma *concatenação* de $\{\mathbf{c_1}_k\}_{k\in\mathbb{Z}}$ e $\{\mathbf{c_2}_k\}_{k\in\mathbb{Z}}$ no instante j é uma palavra código $\{(\mathbf{c_1} \wedge_j \mathbf{c_2})_k\}_{k\in Z}$ definida como $(\mathbf{c_1} \wedge_j \mathbf{c_2})_k = \begin{cases} \mathbf{c_1}_k|_{(-\infty,j)}; \ k < j \\ \mathbf{c_2}_k|_{[j,+\infty)}; \ k \geq j. \end{cases}$.

Se L é um inteiro maior do que um, então o código de grupo $\mathcal{C}$ é dito L-controlável quando para dadas duas palavras $\mathbf{c_1}$ e $\mathbf{c_2}$, existir uma terceira palavra $\mathbf{c_3}$ e um inteiro k tal que a concatenação $\mathbf{c_1} \wedge_k \mathbf{c_3} \wedge_{k+L} \mathbf{c_2}$ é uma palavra do código de grupo $\mathcal{C}$. [6], [5]. É dito que um número natural $l > 1$ é o índice de controlabilidade do código $\mathcal{C}$ quando $l = min\{L \ ; \ \mathcal{C}$ é $L-$controlável $\}$. Qualquer código de grupo que tenha uma aplicação prática em transmissão o armazenamento de dados precisa ter um índice de controlabilidade.

Definição 4: Um código de grupo $\mathcal{C}$ é dito controlável quando existir um inteiro $l > 1$ tal que l é o índice de controle de $\mathcal{C}$. $\circ$

Em [1] tem sido provado que códigos invariantes no tempo podem ser gerados por um codificador convolucional generalizado. Conforme foi notado em [5], [10], considerando códigos convolucionais generalizados como sistemas dinâmicos os codificadores convolucionais generalizados são a **realização** destes códigos.
A seção de treliça é o conjunto de arestas $(s, \omega(u, s), \nu(u, s)) \in S \times Y \times S$, e se pode provar que o conjunto de todas as arestas $B = \{(s, \omega(u, s), \nu(u, s)) \ ; \ (u, s) \in U \boxtimes S\}$ é um grupo que é isomorfo a $U \boxtimes S$

O código de grupo $\mathcal{C}$ gerado pelo codificador da Definição 2 **não será controlável** se existirem dois estados s e s' tais que $s \neq \nu(u_n, \nu(u_{n-1}, \nu(u_{n-2}, \dots, \nu(u_2, \nu(u_1, s')) \dots)))$, para quaisquer sequência de $\{u_i\}_{i=1}^n$ entradas.

Exemplo 5: Para o caso do codificador binário do Exemplo 3, Figura 1, temos que o código resultante é controlável conforme pode ser visualizado na Figura 2. Para o caso do codificador do Exemplo 4. Por uma simples inspeção visual da Figura 3, podemos concluir que o código não é controlável. Mais ainda, podemos mostrar que para todas as outras extensões dos subgrupos normais $\{R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}\}$, $\{R_0, R_\pi, H, V\}$, e $\{R_0, R_\pi, d_1, d_2\}$ não é possível construir grafos conexos, o que significa que não existe homomorfismos sobrejetores $\nu : D_8 = U \boxtimes S \to S$ tais que produzam codificadores controláveis. $\circ$
Dado um codificador da Definição 2, considere a família de subconjuntos $\{S_i\}$, do grupo dos estados S definidos recursivamente por;

$$\begin{array}{lcl} S_0 & = & \{e\} \\ S_1 & = & \{\nu(u,s)\ ;\ u \in U, s \in S_0\} \\ S_2 & = & \{\nu(u,s)\ ;\ u \in U, s \in S_1\} \\ \vdots & \vdots & \vdots \\ S_i & = & \{\nu(u,s)\ ;\ u \in U, s \in S_{i-1}\}, i \geq 0 \\ \vdots & = & \vdots \end{array} \quad (4)$$

Teorema 1: Algumas propriedades de $\{S_i\}$;

1) Cada S_i é um subgrupo de S
2) S_{i-1} é normal em S_i, para cada $i = 1, 2, \ldots$.
3) Se $S_{i-1} = S_i$ então $S_i = S_{i+1}$.
4) Se o código é controlável então $S = S_k$ para algum $k \in \mathbb{N}$.

Prova.-

1) Considere $r, s \in S_i$, como ν é sobrejetor, existem (u_1, s_1) e (u_2, s_2) com $s_1, s_2 \in S_{i-1}$ e $u_1, u_2 \in U$ tal que $r = \nu(u_1, s_1)$ e $s = \nu(u_2, s_2)$. Daí, $sr = \nu(u_3, s_1 s_2)$, $u_3 \in U$ e assim $sr \in S_i$.
2) Claramente $S_0 \triangleleft S_1$. Para $i > 1$, suponha $S_{j-1} \triangleleft S_j$, para cada $j \leq i$. Dados $s \in S_{i+1}$ e $r \in S_i$, considere $s.r.s^{-1}$ = $\nu(u, s_1).\nu(v, r_1).\nu(u, s_1)^{-1}$, onde $s_1 \in S_i$, $r_1 \in S_{i-1}$, $u, v \in U$. Daí, $s.r.s^{-1}$ = $\nu(u_1, r_1.s_1.r_1^{-1}) \in S_i$, pois $r_1.s_1.r_1^{-1} \in S_{i-1}$.
3) Dado $s \in S_{i+1}$ existem $r \in S_i$ e $u \in U$ tais que $\nu(u, r) = s$. Como $S_i = S_{i-1}$, $r \in S_{i-1}$. Portanto $\nu(u, r) = s \in S_i$.
4) Em caso contrário, existem $s \in S_k$ e $s' \in S$ tais que $s' \neq \nu(u_n, \nu(u_{n-1}, \nu(u_{n-2}, \ldots, \nu(u_2, \nu(u_1, s)) \ldots)))$, para qualquer sequência $\{u_i\}_{i=1}^n$ de entradas.

□

O conjunto de transições $(s, \omega(u,s), \nu(u,s)) \in (S \times Y \times S)$ de um código de grupo invariante no tempo é um grafo orientado cujos conjunto de **vértices** é o grupo de estados S e as **arestas** é o conjunto das triplas $(s, \omega(u,s), \nu(u,s))$. Em cada tripla, o estado s é o ponto de partida da aresta, enquanto que $\nu(u,s)$ é o ponto final da aresta. Com a operação componente a componente $(s_1, \omega(u_1, s_1), \nu(u_1, s_1)) * (s_2, \omega(u_2, s_2), \nu(u_2, s_2))$ = $(s_1 s_2, \omega((u_1, s_1)(u_2, s_2)), \nu((u_1, s_1)(u_2, s_2)))$ este conjunto de arestas orientadas, será denotada por E. Dentro da área da Teoria dos Códigos Corretores de Erros, as arestas são melhor conhecidas como *transições* e um exemplo de estas duas representações gráficas é mostrada nas Figuras 2 e 3
Desde que ω é injetora, o mapeamento $\Psi : U \boxtimes S \to E$ definido por,

$$\Psi(u,s) = (s, \omega(u,s), \nu(u,s)) \quad (5)$$

é um isomorfismo de grupos.

Lema 1: Considere o codificador ω, ν, e $U \boxtimes S$ da Definição 2. Suponha $U \boxtimes S$ não-abeliano. Sejam E^+ e E^- subconjuntos do grupo seção de treliça E tal que $E^+ = \{(e, \omega(u,e), \nu(u,e)\ ;\ u \in U\}$, as arestas saindo do estado neutro $\{e\}$, e $E^- = \{(s, \omega(u,s), \nu(u,s)\ ;\ \nu(u,s) = e\}$, as arestas chegando no estado neutro $\{e\}$ então;

1) Ambos E^+ e E^- são subgrupos normais de E, com $|U| = |E^+| = |E^-|$
2) Os grupos quocientes $\frac{E}{E^+}$ e $\frac{E}{E^-}$ são isomorfos e $\frac{E}{E^+} \cong \frac{E}{E^-} \cong S$.
3) O número de arestas saindo/chegando de/em qualquer estado s é $|U| = |E^+| = |E^-|$

Prova.-

1) Imediato
2) O mapeamento de S a $\frac{E}{E^+}$ dado por $s \mapsto (s, \omega(u,s), \nu(u,s))E^+$, é um homomorfismo bijetor, daí $\frac{E}{E^+} \cong S$. Por outro lado, a projeção $(s, \omega(u,s), \nu(u,s)) \mapsto \nu(u,s)$, de E a S, é um homomorfismo sobrejetor com kernel E^-, pelo Teorema fundamental dos homomorfismos, $\frac{E}{E^-} \cong S$
3) Considere a transição $t_0 = (s, \omega(e,s), \nu(e,s))$ saindo de um estado qualquer s, e o coset $t_0 E^+ = t_0\{\Psi(u,e); u \in U\} = \{\Psi(u,s); u \in U\}$ que é o conjunto das transições saindo de s e que possui $|E^+|$ arestas. Analogamente considerando sE^- podemos mostrar que as transições chegando no estado s tem cardinalidade $|E^-|$.

Definição 5: Dado um grupo G, o subgrupo dos comutadores de G é definido por $G' = \{aba^{-1}b^{-1}\ ;\ a, b \in G\}$

Definição 6: Duas arestas diferentes $(s_1, \omega(u_1, s_1), \nu(u_1, s_1))$ e $(s_2, \omega(u_2, s_2), \nu(u_2, s_2))$ são ditas paralelas se $s_1 = s_2$ e $\nu(u_1, s_1) = \nu(u_2, s_2)$ e $\omega(u_1, s_1) \neq \omega(u_2, s_2)$

Quando o grupo seção de treliça E não possui transições paralelas, qualquer arco pode ser representado, de maneira unívoca, por um par $(s, \nu(u,s))$, onde o estado s é o vértice de saída, e $\nu(u,s)$ é o vértice de chegada. O seguinte Lema é uma versão para codificadores homomorfos do Teorema 4 de [11]

Lema 2: Considere o codificador ω, ν, e $U \boxtimes S$ da Definição 2. Sejam H^+ e H^- subconjuntos de $U \boxtimes S$ tais que $H^+ = U \boxtimes \{e\} = \{(u,e)\ ;\ u \in U\}$ e $H^- = Ker(\nu) = \{(u,s)\ ;\ \nu(u,s) = e\}$, então;

1) $H^+ \cong E^+$ e $H^- \cong E^-$,
2) Ambos H^+ e H^- são subgrupos normais de $U \boxtimes S$,
3) Se $H^+ \cap H^- \neq \{(e,e)\}$ então a seção de treliça E possui transições paralelas,
4) Se $U \boxtimes S$ é não-abeliano e o grupo de estados S é abeliano então E possui transições paralelas

Prova.-

1) Temos $E^+ = \Psi(H^+)$ e $E^+ = \Psi(H^+)$, com Ψ definido pela equação (5).
2) Imediato.
3) Existe $(u,e) \in H^+ \cap H^-$, com $u \neq e$ tal que $\nu(u,e) = e$, pois Ψ de (5) é bijetor, $\omega(u,e) \neq e$. Portanto, as transições $(e, \omega(e,e), \nu(e,e))$ e $(e, \omega(u,e), \nu(u,e))$ são paralelas.
4) O fato do grupo dos estados S ser abeliano implica que $\frac{G}{H^+} \cong \frac{G}{H^-}$ são grupos quocientes abelianos. Então o subgrupo dos comutadores $(U \boxtimes S)'$ é um subgrupo de $H^+ \cap H^-$ [8]. Mas $U \boxtimes S$ é não abeliano, então $(U \boxtimes S)' \neq \{(e,e)\}$. Portanto do anterior item 2, B tem transições paralelas.

□

IV. CODIFICADOR HOMOMORFO DEFINIDO EM $\mathbb{Z}_p \boxtimes S$ COM p PRIMO

A pesar da sua aparente simplicidade, ainda não existe uma classificação geral para p-grupos. Somente os p-grupos com ordem menor ou igual a p^6 tem sido completamente classificados, quando $p \geq 3$, [12]. E para o caso $p = 2$, uma classificação completa tem sido feita para grupos com ordem $\leq 2^8$, [13], [14]. Esta classificação dos 2-grupos tem sido implementado em alguns softwares como o GAP, [14], que inclui em sua biblioteca todos os grupos de ordem 256. Os grupos cíclicos $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$, onde a operação de grupo é dada por $i + j$ modulo p, são os exemplos mais simples de p-grupos. Os resultados acerca de codificadores homomorfos generalizados, envolvendo $\mathbb{Z}_p$ como grupo de informação, são válidos para qualquer p-grupo independentemente da existência de sua classificação.

Lema 3: Seja $\mathbb{Z}_p \boxtimes S$ uma extensão que é um p-grupo. Se $\mathbb{Z}_p \boxtimes S_0 \subset (\mathbb{Z}_p \boxtimes S)'$, então $\mathbb{Z}_p \boxtimes S_i \subset (\mathbb{Z}_p \boxtimes S)'$, e $S_i \subset S'$, para cada $i \geq 1$.

Prova.- Desde que ν é um homomorfismo de grupos, a imagem $\nu(\mathbb{Z}_p \boxtimes S_0) = S_1$ esta contida no subgrupo de comutadores S' de S. Se $S_1 = S_0$ o Lema se cumpre trivialmente, (Figura 4 (a)).Se $S_1 \neq S_0$, pelo teorema longo dos comutadores de [15], existem $s \in (S_1 - S_0)$ e $a_1, a_2, \ldots, a_t \in S$ tais que $s = a_1 a_2 \ldots a_t a_1^{-1} a_2^{-1} \ldots a_t^{-1}$. Agora considere $u \in \mathbb{Z}_p$ e $\{u_1, u_2, \ldots, u_t\} \subset \mathbb{Z}_p$ tal que $(u, s) = (u_1, a_1)(u_2, a_2)\ldots(u_t, a_t)(u_1, a_1)^{-1}(u_2, a_2)^{-1}\ldots(u_t, a_t)^{-1}$. temos $(u, s) \in (\mathbb{Z}_p \boxtimes S)'$ e $(u, s) \notin \mathbb{Z}_p \boxtimes S_0$. Portanto $\mathbb{Z}_p \boxtimes S_1 \subset (\mathbb{Z}_p \boxtimes S)'$ (Figura 4 (b)).

De novo, e desde que ν é um homomorfismo de grupos, $\nu(\mathbb{Z}_p \boxtimes S_1) = S_2$ esta contido no subgrupo dos comutadores S' de S. Então com argumentos muito semelhantes, podemos provar que se $S_2 \neq S_1$, então $(\mathbb{Z}_p \boxtimes S_2) \subset (\mathbb{Z}_p \boxtimes S)'$ e $\nu(\mathbb{Z}_p \boxtimes S_2) = S_3 \subset S'$. Continuando da mesma maneira teremos $(\mathbb{Z}_p \boxtimes S)'$ e $S_i \subset S'$, para qualquer $i \geq 1$. □

Lema 4: Seja $\mathbb{Z}_p \boxtimes S$ uma extensão que é um p-grupo. Considere os subgrupos $\{S_i\}$ definidos na equação (4). Então, S_i é abeliano ou $S_i \subset S'$, para cada i.

Prova.- Desde que S_1 é cíclico e S_2 tem ordem menor ou igual a p^2, temos que ambos S_1 e S_2 são abelianos. Então, seja $i \geq 2$ tal que $S_1, S_2, \ldots, S_i$ são todos abelianos com S_{i+1} não abeliano. Então, existem $s_1, s_2 \in S_{i+1}$ tais que $s_1 s_2 \neq s_2 s_1$. Também deve existir $u_1, u_2 \in \mathbb{Z}_p$ e $r_1, r_2 \in S_i$, com $r_1 r_2 = r_2 r_1$, tal que $s_1 = \nu(u_1, r_1)$ e $s_2 = \nu(u_2, r_2)$. Então;

$s_1 s_2 \neq s_2 s_1$,
$\nu(u_1, r_1).\nu(u_2, r_2) \neq \nu(u_2, r_2).\nu(u_1, r_1)$,
$\nu((u_1, r_1).(u_2, r_2).(u_1, r_1)^{-1}.(u_2, r_2)^{-1}) \neq e$
$\nu(u', r_1 r_2 r_1^{-1} r_2^{-1}) \neq e$, para algum $u' \in \mathbb{Z}_p$
$\nu(u', e) \neq e$

Daí, $u' \neq e$ e $(u', e) \in (\mathbb{Z}_p \boxtimes S)' \cap (\mathbb{Z}_p \boxtimes S_0)$. Desde que a ordem de $\mathbb{Z}_p \boxtimes S_0$ é p, temos que $\mathbb{Z}_p \boxtimes S_0 \subset (\mathbb{Z}_p \boxtimes S)'$.

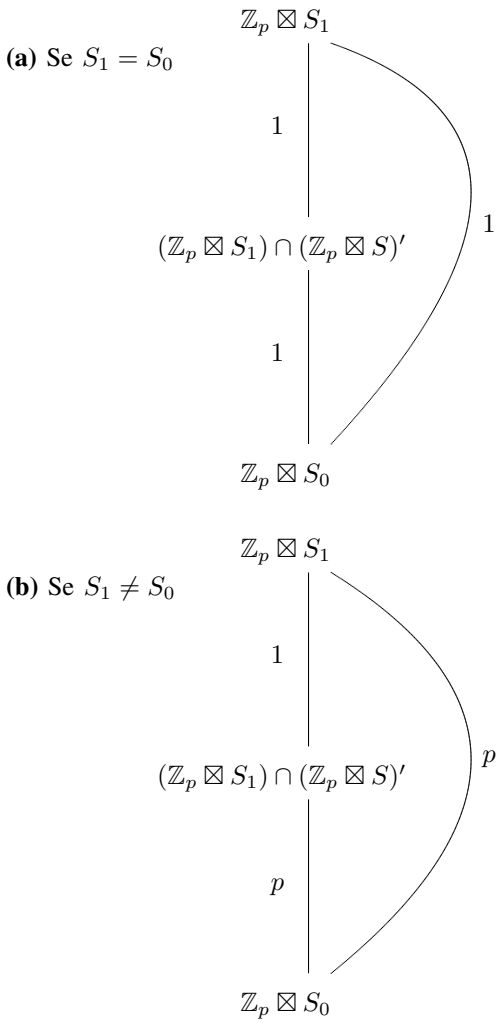

Fig. 4. A interseção $(\mathbb{Z}_p \boxtimes S_1) \cap (\mathbb{Z}_p \boxtimes S)'$ quando $\mathbb{Z}_p \boxtimes S_0 \subset (\mathbb{Z}_p \boxtimes S)'$

Pelo lema 3, $(\mathbb{Z}_p \boxtimes S_i) \subset (\mathbb{Z}_p \boxtimes S)'$ e $S_i \subset S'$, para cada i. Portanto S_i é um grupo abeliano ou $S_i \subset S'$. □

Suponha agora que não temos informação acerca da ordem de $\mathbb{Z}_p \boxtimes S$, isto é, não possamos usar a hipótese de $\mathbb{Z}_p \boxtimes S$ ser um p-grupo. Neste caso temos que S deve ser um grupo finito e genérico. Trabalhando, outra vez, com a família $\{S_i\}$ definida na equação (4) mostraremos que quando $U = \mathbb{Z}_p$, cada S_i deve ser um p-grupo. Em esta direção começamos mostrando um resultado sobre um importante subgrupo normal do grupos dos estados S. Este subgrupo é o conjunto dos estados de partida das transições que chegam no estado neutro e. Ou de uma maneira mais formal é o conjunto de estados resultantes da segunda projeção sobre o kernel de ν;

$$S_d = \{s \in S \ ; \ \nu(u, s) = e \text{ for some } u \in \mathbb{Z}_p\} \qquad (6)$$

Notemos que este subgrupo normal também é isomorfo com $\mathbb{Z}_p$ e;

Lema 5: Considere o codificador ν, ω, e $\mathbb{Z}_p \boxtimes S$ da Definição 2. Além disso considere o subgrupo S_d definido na equação (6), então;

1) Se existir $s \neq e$ e $s \in S_d \cap S_i$ então $S_d \subset S_i$, para $i \geq 0$
2) Se $S_d \subset S_i$ então $\nu(\mathbb{Z}_p, S_d) \subset S_i$, para $i \geq 0$.

Prova.-

1) Desde que $p \in S_d \cap S_i$, então $\{s, s^2, \ldots, s^{p-1}, s^p = e\} \subset S_d \cap S_i$.
2) Dado $r \neq e$ tal que $r \in S_i \cap S_d$ suponha que existe algum $u \in \mathbb{Z}_p$ tal que $\nu(u, r) = s \notin S_i$. Para o subgrupo $S_1 = \{s_0, s_1 = \nu(u_1, e), s_2 = \nu(u_2, e), \ldots, s_{p-1} = \nu(u_{p-1}, e)\}$, temos que sS_1 é um coset onde cada elemento é $\nu(u, r)\nu(u_i, e) = \nu(u', r)$, para algum $u' \in \mathbb{Z}_p$. Daí $sS_1 = \{\nu(\mathbb{Z}_p, r)\}$ com $sS_1 \cap S_i = \emptyset$. Mas, desde que $r \in S_d$, existe pelo menos $u_0 \in \mathbb{Z}_p$ tal que $\nu(u_0, r) = e$ em contradição com $sS_1 \cap S_i = \emptyset$. □

Teorema 2: Considere o codificador ν, ω, e $\mathbb{Z}_p \boxtimes S$ da Definição 2, onde p é primo. Então cada S_i de (4) deve ser um p-grupo

Por indução sobre i. Para $i = 1$ temos $[S_1 : S_0] = p$ ou $[S_1 : S_0] = 1$. Agora suponha que existe um número natural $k > 1$ tal que $[S_i : S_{i-1}] = p$, para cada $i \leq k$. Temos que o subgrupo S_k tem p^k elementos e cada um dos seus elementos possui ordem p^i, $i \leq k$. Se $p > [S_{k+1} : S_k] > 1$ então $[S_{k+1} : S_k] = m = q_1^{r_1} q_2^{r_2} \ldots q_t^{r_t}$, onde cada q_i é um primo com $q_i < p$. Deve existir um elemento $s \in (S_{k+1} - S_k)$ tal que $s^{q_1} = e$.
Sejam $u \in \mathbb{Z}_p$ e $r \in S_k$ tais que $\nu(u, r) = s$, então $\nu(u_1, r^{q_1}) = e$. Daí $r^{q_1} \in S_d \cap S_k$.
Se $r \neq e$ então $r^{q_1} \neq e$, pois $q_1 < p$. Pelo Lema 5, $S_d \subset S_k$ e $\nu(u, r) = s \in S_k$, uma contradição.
Se $r = e$ então $\nu(u, r) = s \in S_1 \subset S_k$, também uma contradição.

Teorema 3: Considere o codificador ν, ω, e $\mathbb{Z}_p \boxtimes S$ da Definição 2, onde $\mathbb{Z}_p \boxtimes S$ é não abeliano e p é um primo positivo, então

1) Se S é abeliano então o código tem transições paralelas.
2) Se S é não abeliano então o código é não controlável

Prova.-

1) Pelo Lema 2
2) Se S não é um p-grupo então pelo Teorema 2 o código resultante é não-controlável. Se S é um p-grupo, então $\mathbb{Z}_p \boxtimes S$ é também um p-grupo, então pelo Lema 4 S é abeliano, uma contradição.

V. CONCLUSÕES

Mostramos que codificadores convolucionais generalizados definidos sobre extensões não-abelianas $Z_p \boxtimes S$, p primo não produzem bons códigos. Fica pendente obter resultados sobre extensões não abelianas $\mathbb{Z}_{p^n} \boxtimes S$ ou $(\mathbb{Z}_p)^n \boxtimes S$.

REFERÊNCIAS

[1] G.D. Forney and M.D. Trott. The dynamics of group codes; state spaces, trellis diagrams and canonical encoders. IT 39(5):1491–1513, 1993.
[2] Shu Lin and Daniel J. Costello. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, New Jersey, 1983.
[3] Gottfried Ungerboeck. Channel coding with multilevel-phase signals. *IEEE Transactions on Information Theory*, 28:55–67, 1982.
[4] H.A. Loeliger. Signal sets matched to groups. *IEEE Trans. Inform. Theory*, 37:1675–1682, November 1991.
[5] H. A. Loeliger and T. Mittelholzer. Convolutional codes over groups. *IEEE Transactions on Information Theory*, 42:1659–1687, 1996.
[6] Douglas Lind and Brian Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, New York, 1995.
[7] Jan C. Willems. Models for dynamics. In H. O. Walther U. Kirchgraber, editor, *Dynamics Reported*, volume 2, pages 171–269. Wiley and Teubner, 1989.
[8] Joseph J. Rotman. *An Introduction to the Theory of the Groups*. Springer Verlag, New York, fourth edition, 1995.
[9] Marshall Hall. *The Theory of Groups*. Mac Millan, New York, 1959.
[10] Fagnani F. and Zampieri S. Minimal syndrome formers for group codes. *IEEE Transactions on Information Theory*, 45(01):3–31, 1999.
[11] David G. Forney. On the hamming distance properties of group codes. *IEEE Transactions on Information Theory*, 38:1797–1801, 1992.
[12] R James. The groups of order p^6 (p an odd order prime). *Math. Comput.*, 34:613–637, 1980.
[13] E. A. O'Brien. The groups of order 256. *Journal of Algebra*, 143:219–235, 1991.
[14] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005. (`http://www.gap-system.org`).
[15] Yff P. On k-conjugacy in a group. *Proc. Edimburg Math. Soc.*, 2:14:1–4, 1964/65.