CODIFICADORES CONVOLUCIONAIS ABELIANOS

Jorge Pedraza Arpasi* **e Reginaldo Palazzo Jr.†**
DT/FEEC/UNICAMP
Caixa Postal 6101
13081-970 Campinas SP

Resumo - Neste trabalho são estabelecidas as condições necessárias e suficientes para a construção de codificadores convolucionais abelianos. Mostramos que tais codificadores são controláveis, completos e mínimos, esta última proposição via uma proposta de redução de estados, e tendo como subclasse os codificadores convolucionais elementares. Como consequência do fato de que os codificadores convolucionais abelianos controláveis, cuja seção de treliça é isomorfa a um grupo cíclico, não são controláveis, então propomos um algoritmo de construção de codificadores convolucionais abelianos tendo como grupo das entradas, de estados e de saídas, k-uplas, $(n-k)$-uplas e n-uplas binárias, respectivamente. Exemplos de codificadores convolucionais elementares e abelianos são apresentados.

Abstract - In this paper we establish the necessary and sufficient conditions for the construction of Abelian convolutional encoders. We show that such encoders are controllable, complete and minimal, the latter via a state reduction procedure, and having the elementary convolutional encoders as a subclass. As a consequence of the fact that the Abelian convolutional encoders whose trellis section is isomorphic to a cyclic group are noncontrollable, then an algorithm for the construction of controllable Abelian convolutional encoders whose trellis section is isomorphic to an Abelian group (not cyclic) is proposed having the group of input, the group of states, and the group of output binary k-tuples, $n-k$-tuples and n-tuples, respectively. Examples of elementary and Abelian convolutional encoders are presented.

Palavras Chaves : Máquinas, codificadores convolucionais elementares, codificadores convolucionais abelianos, controlabilidade.

1. INTRODUÇÃO

Se para cada $s \in S$ existe $g \in \Gamma(S)$ tal que $s = g(s_0)$, para algum $s_0 \in S$, então dizemos que $\Gamma(S)$ atua transitivamente sobre S. O ponto $s_0 \in S$ é denominado *semente* ou *gerador* de S. Note que podem existir vários geradores de S.

Para se obter códigos Euclidianos de uma maneira prática e efetiva os *códigos de grupo* devem ser constituídos de seqüências de simetrias, denominados *códigos de simetrias*. Um código de simetria $\mathcal{G}$ é um subgrupo do produto direto de um número infinito de grupos, isto é, $\oplus_{k\in\mathbb{Z}} G_k = \ldots \oplus G_{-i} \oplus \ldots \oplus G_{-1} \oplus G_0 \oplus G_1 \oplus \ldots \oplus G_i \oplus \ldots, i \in \mathbb{N}$, onde para cada $k \in \mathbb{Z}$, $G_k \subseteq \Gamma(S_k)$ é o grupo de simetrias do conjunto discreto $S_k \subset \mathbb{R}^{n_k}$.

O código Euclidiano $\mathcal{C}$ casado a $\mathcal{G} \subset \oplus_{k\in\mathbb{Z}} G_k$ é obtido a partir de uma seqüência semente $\{x_k\}_{k\in\mathbb{Z}}$, $x_k \in \mathbb{R}^{n_k}$. Isto significa que cada palavra-código $\{y_k\}_{k\in\mathbb{Z}} \in \mathcal{C}$ é tal que para cada $k \in \mathbb{Z}$, $y_k = g_k(x_k)$, $g_k \in G_k$. Estes códigos Euclidianos são denominados *códigos geometricamente uniformes*, [3].

Neste trabalho iremos considerar códigos invariantes no tempo e com um número finito de estados, isto é, um código tendo como base um conjunto discreto Euclidiano $S \subset \mathbb{R}^n$ com cardinalidade $|S|$ finita, e tal que $S_k = S \subset \mathbb{R}^n$ para todo $k \in \mathbb{Z}$. Neste caso, $G_k = G$, $\forall\, k \in \mathbb{Z}$ com $|G|$ finito. Agora, seja $G^{\mathbb{Z}} = \oplus_{k\in\mathbb{Z}} G_k$, $G_k = G$, $\forall k \in \mathbb{Z}$, considere um subgrupo $\mathcal{G} \subset G^{\mathbb{Z}}$. Assim, $\mathcal{G}$ é um código de simetrias invariante no tempo e com um número finito de estados. Esta classe de códigos de simetrias invariantes no tempo é o exemplo fundamental dos *códigos de Schreier* [11] e, em particular, dos códigos convolucionais abelianos.

Os códigos convolucionais abelianos são subgrupos de $G^{\mathbb{Z}}$, onde G é um grupo finito arbitrário, não necessariamente um grupo de simetrias de algum conjunto Euclidiano discreto $S \subset \mathbb{R}^n$. Esta generalidade somente facilita a aplicação sobre grupos arbitrários.

Os códigos convolucionais abelianos admitem análise local, isto é, a análise da seção de treliça numa unidade do tempo é suficiente para determinar as propriedades tais como distância livre, controlabilidade, minimalidade, etc. de todo o código. Esta análise local permite determinar a relação equipotente entre a classe do produto direto e a classe dos códigos convolucionais abelianos, via os codificadores isomorfos. Isto significa que para cada código convolucional abeliano existe um único codificador isomorfo e para cada codificador isomorfo existe um único código convolucional abeliano.

Este trabalho está organizado da seguinte maneira. Na Seção 2, apresentamos uma rápida descrição de máquinas no sentido da teoria dos autômatas, pois todos os codificadores considerados neste trabalho usam este modelo. Na Seção 3, motivados pela descrição matricial dos codificadores convolucionais binários, definimos os codificadores convolucionais elementares sobre grupos (CCE). A classe dos codificadores convolucionais lineares binários está contida na classe dos CCEs. Estudamos algumas propriedades dos CCEs que servem como guia para definir os codificadores convolucionais abelianos. É também proposto um teste simples de exclusão de CCEs catastróficos. Ainda nesta seção, apresentamos uma

*O autor está atualmente no Departamento de Telemática, sob licença do Departamento de Matemática, Universidade Nacional San Luis Gonzaga de Ica, Peru.

†O autor está no Departamento de Telemática, FEEC-UNICAMP, C.P. 6101, 13081-970, Campinas, SP, Brasil. Este trabalho foi financiado em parte pela Fundação de Amparo à Pesquisa do Estado de São Paulo - FAPESP, No. 95/4720-8, e em parte pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, No. 301416/85-0, Brasil. palazzo@dt.fee.unicamp.br

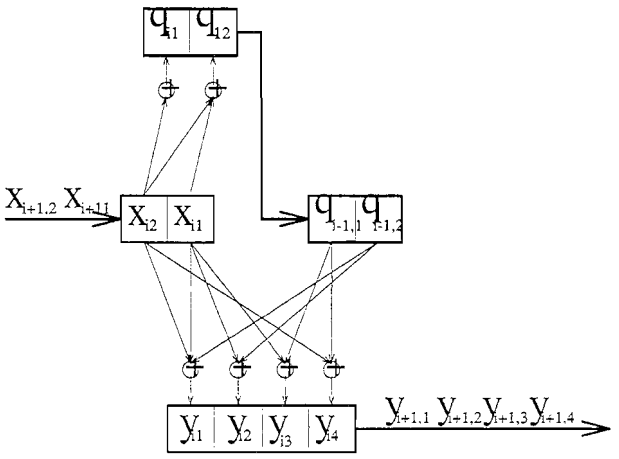

Figura 1. Máquina generalizada

proposta de redução de estados de um CCE, especialmente se este for catastrófico. Na Seção 4, estabelecemos as condições para a construção de codificadores convolucionais abelianos, onde propomos um algoritmo de construção e apresentamos um exemplo. Finalmente, na Seção 5, apresentamos as conclusões.

2. MÁQUINAS

A descrição de um sistema sob a excitação de alguma classe de entrada produzindo uma outra classe de saída tal que a sua estrutura interna possa também ser modificada, tem sido e será útil no modelamento de muitos dispositivos abstratos e fenômenos. Dentre as possíveis descrições, escolhemos aquela relativa à teoria dos autômatas, devido ao uso do conceito de máquinas, [5] e [9].

Definição 1 *Uma máquina é uma quíntupla* $M = (X, Y, Q, \delta, \beta)$, *onde*

- X *é o conjunto finito das entradas;*
- Y *é o conjunto finito das saídas;*
- Q *é o conjunto dos estados (não necessariamente finito);*
- $\delta : X \times Q \to Q$ *é o mapeamento do próximo estado;*
- $\beta : X \times Q \to Y$ *é o mapeamamento das saídas.*

Esta definição é bastante geral no sentido de que máquinas podem caracterizar sistemas abstratos como por exemplo os sistemas de equações diferenciais, chegando até o processo evolutivo do comportamento de um ser humano. Willems, [4], usa de maneira precisa o termo *comportamento de um sistema* como sendo uma subclasse de seqüências bi-infinitas de algum produto cartesiano $\prod_{k\in\mathbb{Z}} S_k$, onde cada S_k é um corpo algébrico sendo este o alfabeto de saída da respectiva máquina M_k. A proposta de Trott [1], [10] sobre o conceito de comportamento de um sistema é no sentido de que cada S_k seja um grupo algébrico. A noção de uma máquina generalizada, veja Figura 1., tendo como ponto de partida a Definição 1, ocorre quando cada S_k é um conjunto arbitrário podendo apresentar ou não alguma estrutura algébrica.

Seja $\Psi : X \times Q \to Q \times Y \times Q$ a aplicação definida por

$$\Psi(x, q) = (q, \beta(x, q), \delta(x, q)). \tag{1}$$

Então, o conjunto $T \subset Q \times Y \times Q$, definido por

$$T = Im(\Psi) = \Psi(X \times Q), \tag{2}$$

é chamado *seção de treliça* associada à máquina M, ou simplesmente a *treliça* de M. Cada elemento $t = (q, \beta(x, q), \delta(x, q)) \in T$ é chamado uma *transição* ou um *ramo* da treliça.

Considere a classe de seqüências finitas do conjunto das entradas $X^* = \{x^* = \{x_i\}_{i=1}^n : x_i \in X\, n \in \mathbb{N}\}$. Dada uma seqüência finita $x^* = \{x_i\}_{i=1}^n$, denotamos o seu comprimento por $|x^*|$, e assim $|x^*| = n$.

Definição 2 *Dizemos que a máquina* $M = (X, Y, Q, \delta, \beta)$ *é* ***controlável*** *se para todos* q *e* $q' \in Q$, *existir uma seqüência finita* x^*, *com* $1 \leq |x^*| \leq n$, *tal que* $q' = \delta^*(x^*, q)$, *onde*

$$\delta^*(x^*, q) = \delta(x_n, \delta(x_{n-1}, \ldots, \delta(x_1, q)\ldots),$$

Dado $j \in \mathbb{N}$, se para todos q, $q' \in Q$ existir um $x^* \in X^*$ com $1 \leq |x^*| \leq j$ tal que $q' = \delta^*(x^*, q)$ então, dizemos que a máquina é j-controlável. Dessa forma, fica fácil de precisar que se a máquina é j-controlável então, ela também será $(j+1)$-controlável.

O número $\nu = min\{j : M \text{ é } j\text{-controlável}\}$ é o **índice de controlabilidade** de M. Na verdade, controlabilidade é uma propriedade da classe de seqüências de saída C da máquina M ou, equivalentemente, do comportamento do sistema. Mas como para uma máquina M existe uma única classe C de seqüências de saída associada a M, então é natural dizer que M é controlável para dizer que C é controlável. Assim, esta característica ocorrerá de maneira similar com as demais propriedades de C. Isto é, quando M apresentar uma certa propriedade $\mathcal{P}$, então C apresentará a mesma propriedade $\mathcal{P}$.

3. CODIFICADORES CONVOLUCIONAIS ELEMENTARES SOBRE GRUPOS

Sejam k e n números naturais. Seja L uma matriz $k \times n$ definida por $L = (l_{ij})$,onde $l_{ij} \in Z$, $1 \leq i \leq k$ e $1 \leq j \leq n$. Seja G um grupo abeliano. Para qualquer $n \in N$, considere G^n como sendo n cópias de G, com a G-operação sobre as respectivas coordenadas. Então, G^n é também um grupo abeliano. Dados $x \in G^k$ e L, defina o produto $x.L$ como sendo

$$x.L = \left(\sum_{i=1}^{k} x_i l_{i1}, \sum_{i=1}^{k} x_i l_{i2}, \cdots, \sum_{i=1}^{k} x_i l_{in}\right), \tag{3}$$

onde

$$x_i l_{ij} \triangleq \begin{cases} \overbrace{x_i * x_i * \ldots * x_i}^{l_{ij}-termos}, & se\ l_{ij} > 0 \\ e_G, & se\ l_{ij} = 0 \\ \overbrace{(x_i * x_i * \ldots * x_i)^{-1}}^{l_{ij}-termos}, & se\ l_{ij} < 0. \end{cases}$$

Devido a condição abeliana de G e G^n podemos usar o símbolo de adição + em lugar do símbolo *, e também para o elemento identidade usar o símbolo 0 em lugar de e_G. Sob estas condições temos a seguinte definição para o codificador convolucional elementar.

Definição 3 *Sejam n, k e m números naturais tais que $n > k \geq 1$ e $m \geq 1$. Considere as matrizes $L_0, L_1, ..., L_m$, com $L_i = (l^i_{rs})$, onde $l^i_{rs} \in \mathbb{Z}$, $1 \leq r \leq k$, $1 \leq s \leq n$ e $i = 0, 1, ..., m$. Um codificador convolucional elementar (CCE) com parâmetros (n, k, m) sobre G, onde n é o comprimento da palavra-código de transição, k é o número de dígitos de informação e m a memória total, é uma máquina $M \triangleq (X, Y, Q, \delta, \beta)$ onde*

- *$X \subset G^k$ é o alfabeto das entradas;*
- *$Y \subset G^n$ é o alfabeto das saídas;*
- *$Q = \{q = (x_1, x_2, ..., x_m) \mid x_i \in X\} \subset (G^k)^m \cong G^{km}$, é o conjunto (ou espaço) dos estados da máquina;*
- *$\delta : X \times Q \rightarrow Q$, é uma aplicação definida por $\delta(x_0; q) = \delta(x_0; x_1, x_2, ..., x_{m-1}, x_m) = (x_0; x_1, x_2, ..., x_{m-1})$ (aplicação do próximo estado);*
- *$\beta : X \times Q \rightarrow Y$, é uma aplicação definida por $\beta(x_0; q) = \beta(x_0; x_1, ..., x_m) = x_0 L_0 + x_1 L_1 + ... + x_m L_m$ (aplicação das saídas).*

Note que um CCE é um exemplo de máquina, isto é, satisfaz a Definição 1. Desse modo, a classe dos CCEs está contida na classe das máquinas.

Da Definição 3, podemos extrair as seguintes propriedades dos codificadores convolucionais elementares.

Proposição 4 *Se X é um grupo, então*

i) Q e $\beta(X_{\oplus}Q) \subset Y$ são grupos.

ii) O produto cartesiano $X \times Q$ converte-se em um produto direto de grupos e as funções δ e β são homomorfismos de grupos, com δ sendo sobrejetora.

iii) Os conjuntos $Y_0 = \{\beta(x, e_Q)\}_{x \in X}$ e $Y_1 = \{\beta(x, q) : \delta(x, q) = e_Q\}$ são subgrupos normais de $\beta(X, Q)$. Além disso, $\frac{\beta(X,Q)}{Y_0} \cong \frac{\beta(X,Q)}{Y_1} \cong Q$.

iv) O CCE é uma máquina controlável, com índice de controlabilidade $\nu \leq m$.

Prova :

i) Dados $y = \sum_{i=0}^{m} x_i L_i \in Y$ e $y' = \sum_{i=0}^{m} x'_i L_i \in Y$, temos que $y + y' = \sum_{i=0}^{m} (x_i L_i + x'_i L_i) = \sum_{i=0}^{m} x''_i L_i \in Y$, pois X é um grupo. Analogamente, dados $q = (x_1, x_2, ..., x_m)$ e $q' = (x'_1, x'_2, ..., x'_m)$, temos que $q + q' = (x_1 + x'_1, x_2 + x'_2, ..., x_m + x'_m) \in Q$, pois X é um grupo.

ii) Como X e Q são grupos, o produto direto $X_{\oplus}Q$ é um grupo. Assim, δ é um mapeamento entre dois grupos. Sejam (x, q) e (x', q') dois elementos de $X \times Q$, com $q = (x_1, x_2, ..., x_m)$ e $q' = (x'_1, x'_2, ..., x'_m)$. Então,

$$\begin{aligned}\delta((x,q) + (x',q')) &= \delta(x + x', q + q') \\ &= (x + x', x_1 + x'_1, x_2 + x'_2, ..., x_m + x'_m) \\ &= (x, x_1, x_2, ..., x_m) + (x', x'_1, x'_2, ..., x'_m) \\ &= \delta(x, q) + \delta(x', q').\end{aligned}$$

Portanto, δ é um homomorfismo de grupos. Por outro lado, dado $q = (x_1, x_2, ..., x_m) \in Q$, assuma $q_0 = (x_2, x_3, ..., x_{m+1}) \in Q$ e $x_1 \in X$. Então, $\delta(x_1, q_0) = q$. Com isso, temos que δ é sobrejetora.

De maneira análoga, podemos mostrar que β é também um homomorfismo de grupos.

iii) Defina o mapeamento auxiliar $\psi : \beta(X_{\oplus}Q) \rightarrow Q$ por $\psi(\beta(x, q)) \triangleq q$. Então,

$$\begin{aligned}\psi(\beta(x,q) + \beta(x',q')) &= \psi(\beta(x + x', q + q')) \\ &= q + q' = \psi(\beta(x,q)) + \psi(\beta(x',q')).\end{aligned}$$

Assim, ψ é um homomorfismo sobrejetor. Consequentemente, temos que

$$Ker(\psi) = \{\beta(x, q) : q = \psi(\beta(x, q)) = e_Q\} = Y_0.$$

Logo, pelo teorema fundamental dos homomorfismos, [6] e [7], concluímos que $\frac{\beta(X_{\oplus}Q)}{Y_0} \cong Q$.

A prova para Y_1 é análoga. Neste caso definimos o mapeamento auxiliar $\psi : \beta(X_{\ominus}Q) \rightarrow Q$ como $\psi(\beta(x, q)) \triangleq \delta(x, q)$.

iv) *Dados os estados $q = (x_1, x_2, \ldots, x_m)$ e $q' = (x'_1, x'_2, \ldots, x'_m)$, considere a seqüência finita $x^* = x'_1 x'_2 \ldots x'_m \in X^*$, temos que,*

$$q' = \delta^*(x^*, q).$$

Portanto, M é sempre m-controlável. ■

A seguir, iremos consdiderar X como sendo um grupo. Portanto, todas as propriedades da Proposição 4 continuam válidas.

Lema 5 *A seção de treliça do CCE, não possui transições paralelas. Portanto, o mapeamento Ψ, dado em (1), é injetor.*

Prova : *Lembremos que duas transições $t_1 = (q_1, \beta(x_1, q_1), \delta(x_1, q_1)) \in T$ e $t_2 = (q_2, \beta(x_2, q_2), \delta(x_2, q_2)) \in T$ são ditas transições paralelas se $q_1 = q_2$ e $\delta(x_1, q_1) = \delta(x_2, q_2)$. Agora, se a treliça do CCE tiver t_1 e t_2 como transições paralelas, então existe um $q \in Q$ tal que $t_1 = (q, \beta(x_1, q), \delta(x_1, q))$ e $t_2 = (q, \beta(x_2, q), \delta(x_2, q))$ com $\delta(x_1, q) = \delta(x_2, q)$. Disto, temos que $\delta(x_1 - x_2, 0) = 0 \in G^{km}$. Isto implica pela definição de δ, que $x_1 = x_2$. Logo, $t_1 = t_2$.* ■

Seja $M = (X, Y, Q, \delta, \beta)$. Considere uma seqüência de entradas $\{x_i\}_{i=1}^{\infty}$, $x_i \in X$, e q_0 o estado inicial, com $q_0 \in Q$. Seja $\{q_i\}_{i=1}^{\infty}$, $q_i \in Q$, a seqüência de estados gerada por $\{x_i\}_{i=1}^{\infty}$ através de M, definida por

$$\begin{aligned} q_1 &= \delta(x_1, q_0) \\ q_2 &= \delta(x_2, q_1) \\ &\vdots \\ q_i &= \delta(x_i, q_{i-1}) \\ &\vdots \end{aligned} \tag{4}$$

Seja $\{y_i\}_{i=1}^{\infty}$, $y_i \in Y$ a seqüência da saída gerada por $\{x_i\}_{i=1}^{\infty}$ através de M, definida por

$$
\begin{aligned}
y_1 &= \beta(x_1, q_0) \\
y_2 &= \beta(x_2, q_1) \\
&\vdots \\
y_i &= \beta(x_i, q_{i-1}) \\
&\vdots
\end{aligned}
$$

Definição 6 *Dado o* $CCE = (X, Y, Q, \delta, \beta)$, *o código convolucional* C *associado ao CCE é a família de seqüências* $\{y_i\}_{i=1}^{\infty}$ *definida em (3.).*

Cada seqüência $\{y_i\}_{i=1}^{\infty}$ é chamada de *palavra-código*. Este código é *invariante* no tempo, pois é produzido por um único CCE.

Definição 7 *Seja* C *um código qualquer. Seja* $\{C_i\}_{i\in\mathbb{N}}$ *a família de codificadores associados com o código* C. *Seja* $\{s_i\}_{i\in\mathbb{N}}$ *a família de números naturais tal que, cada* s_i *é a cardinalidade dos estados de cada codificador* C_i. *Então, um codificador* C_j *é dito mínimo quando seu número de estados* s_j *é mínimo, isto é,* $s_j \leq s_i$, *para todo* $i \in \mathbb{N}$.

Quando da determinação de codificadores dos códigos de treliça, é importante que sejam estabelecidas as condições de eliminação de códigos catastróficos, pois os mesmos, são tais que para um número finito de erros introduzidos pelo canal conduzem a um número infinito de erros na decodificação. O Teorema 3.4 de [2], válido para *códigos completos*, veio resolver este problema. A versão deste teorema para os CCEs é a seguinte,

Teorema 8 *Seja a máquina* $M = (X, Y, Q, \delta, \beta)$ *tal que* $X = G^k$, $Y = G^n$ *e* $Q = G^{km}$, *onde* G *é um grupo finito com caraterística* p *tal que o* $mdc(p, (m+1)) = 1$. *Sejam* $L_0, \ldots, L_m$ *as matrizes que definem* β. *Então, o código* C *associado com* M *é não catastrófico se, e somente se,* $L = \sum_{i=0}^{m} L_i$ *é tal que* $x.L \neq 0 \in G^n$ *e* $m+1$ *não é um múltiplo da caraterística do grupo* G, *para todo* $x \in X$ *tal que* $x \neq 0$.

Prova : *Seja* $t \in T$ *uma transição horizontal definida como sendo* $t = (q, \beta(x,q), \delta(x,q))$, *tal que* $\delta(x,q) = q$. *Se* $q = (x_1, \ldots, x_m)$, *temos que* $\delta(x,q) = q$ *se, e somente se,* $x = x_1 = \cdots = x_m$.

Em [2] é provado que para o codificador ser mínimo uma condição necessária e suficiente é que a única transição horizontal rotulada com $0 \in Y$ *deve ser a transição trivial* $(0, \beta(0,0), \delta(0,0))$. *Portanto, se* $(x,q) \in X_{\oplus}Q$ *é tal que* $q = \delta(x,q)$ *teremos que* $\beta(x,q) = xL_0 + xL_1 + \ldots xL_m = (m+1)xL$. ■

Dessa forma, o Teorema 8 é um critério de se evitar catastroficidade na construção do CCE. Por outro lado, o código catastrófico poderá ser transformado em um código não catastrófico através da determinação do correspondente codificador mínimo. Para isso necessitamos de técnicas que permitam a redução da cardinalidade dos estados.

3.1. REDUÇÃO DOS ESTADOS

Nesta subseção assumiremos que o mapeamento β é sobrejetor, isto é, $\beta(X_{\oplus}Q) = Y$.

Proposição 9 *Seja* $Q' \subset Q$ *um subgrupo normal de* Q. *Se* Y' *é definido como* $Y' = \{\beta(x,q) \in Y : x \in X \text{ e } q,\ \delta(x,q) \in Q'\}$, *então* Y' *é um subgrupo normal de* Y.

Prova : *Defina a aplicação auxiliar* $\psi : Y \to \frac{Q}{Q'} \times \frac{Q}{Q'}$ *como sendo*

$$\psi(\beta(x,q)) \triangleq (q + Q', \delta(x,q) + Q').$$

Então,

$$
\begin{aligned}
&\psi(\beta(x,q) + \beta(x',q')) = \\
&= \psi(\beta(x + x', q + q')) \\
&= ((q+q') + Q', \delta(x + x', q + q') + Q') \\
&= ((q + Q'), \delta(x,q) + Q') + ((q' + Q'), \delta(x', q') + Q') \\
&= \psi(\beta(x,q)) + \psi(\beta(x', q')).
\end{aligned}
$$

Por outro lado,

$$
\begin{aligned}
Ker(\psi) &= \{\beta(x,q) : \psi(\beta(x,q)) = (Q', Q')\} \\
&= \{\beta(x,q) \in Y : q \in Q' \text{ e } \delta(x,q) \in Q'\} = Y'.
\end{aligned}
$$

Assim, Y' *é normal em* Y. ■

Definição 10 *Dada uma máquina* $M = (X, Y, Q, \delta, \beta)$, *sejam* $Y' \subset Y$ *e* $Q' \subset Q$, *definidos como na Proposição 9, e tal que* $\delta(0,q) \in Q'$, *para todo* $q \in Q'$. *Então, definimos a máquina* $M' = (X, \frac{\beta(X_{\oplus}Q)}{Y'}, \frac{Q}{Q'}, \delta', \beta')$ *onde*

- $\delta' : X \times \frac{Q}{Q'} \to \frac{Q}{Q'}$ *é dado por* $\delta'(x, q+Q') = \delta(x,q) + Q'$;
- $\beta' : X \times \frac{Q}{Q'} \to \frac{Y}{Y'}$ *é dado por* $\beta'(x, q+Y') = \beta(x,q) + Y'$ *(classe das transições paralelas).*

Geralmente, uma máquina M' não é um CCE, pois se Y' é um subgrupo não trivial, então M' possui transições paralelas. O Exemplo 14, a seguir, ilustra esta afirmação.

Proposição 11 *As aplicações* δ' *e* β' *têm as seguintes propriedades :*

- δ' *e* β' *são bem definidas, i.e., elas não dependem da escolha do representante da classe* $q + Q'$.
- δ' *e* β' *são homomorfismos de grupos com* δ' *sendo sobrejetora.*
- β' *é tal que os conjuntos*

$$Y_{Q'_0} = \{\beta'(x, Q') : x \in X\},$$

e

$$Y_{Q'_1} = \{\beta'(x, q+Q') : (x, q+Q') \in X \times \tfrac{Q}{Q'},\ \delta'(x, q+Q') = Q'\},$$

são subgrupos normais de $\frac{Y}{Y'}$. *Além disso,*

$$\frac{\frac{Y}{Y'}}{Y_{Q'_0}} \cong \frac{\frac{Y}{Y'}}{Y_{Q'_1}} \cong \frac{Q}{Q'}.$$

Prova :

- *Se* $q, q_1 \in q + Q'$, *então* $\delta'(x, q + Q') = \delta(x, q) + Q'$ *e* $\delta'(x, q_1 + Q') = \delta(x, q_1) + Q'$. *Logo,* $\delta'(x, q + Q') - \delta'(x, q_1 + Q') = \delta(0, q - q_1) + Q'$. *Como* $\delta(0, q) \in Q'$ *para todo* $q \in Q'$, *temos que* $\delta'(x, q + Q') - \delta'(x, q_1 + Q') = Q'$.

  A prova para β' *é similar, pois pela definição de* Y', $\beta(0, q) \in Y'$ *para todo* $q \in Q'$.
- $\delta'(x, q+Q') + \delta'(x_1, q_1 + Q') = \delta(x, q) + \delta(x_1, q_1) + Q' = \delta(x + x_1, q + q_1) + Q' = \delta'(x + x_1, q + q_1 + Q')$. *A prova para* β' *é similar.*

■

3.2. EXEMPLOS

Nesta seção, iremos apresentar alguns exemplos de modo a ilustrar os conceitos estabelecidos.

Exemplo 12 *Dados* $G = \mathbb{Z}_2$, $n = 3$, $k = 2$, $m = 2$, *e* $L_0 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$; $L_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$; $L_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$. *Considere a máquina* M *dada por*

$X = \mathbb{Z}_2^2 = \{00, 01, 10, 11\}$

$Q = X^2 = \mathbb{Z}_2^4 = \left\{ \begin{array}{lllll} 0000 & 0100 & 1000 & 1100 & 0001 \\ 0010 & 0110 & 1010 & 1110 & 0011 \\ 0101 & 1001 & 1101 & & \\ 0111 & 1011 & 1111 & & \end{array} \right\}$

$Y = \mathbb{Z}_2^3 = \{000, 001, 010, 100, 011, 110, 101, 111\}$

$\delta(x_0, q) = \delta(x_0, (x_1, x_2)) = (x_0, x_1)$, *com* $x_i \in \mathbb{Z}_2^2$

$\beta(x_0, q) = \beta(x_0, (x_1, x_2)) = x_0 L_0 + x_1 L_1 + x_2 L_2$

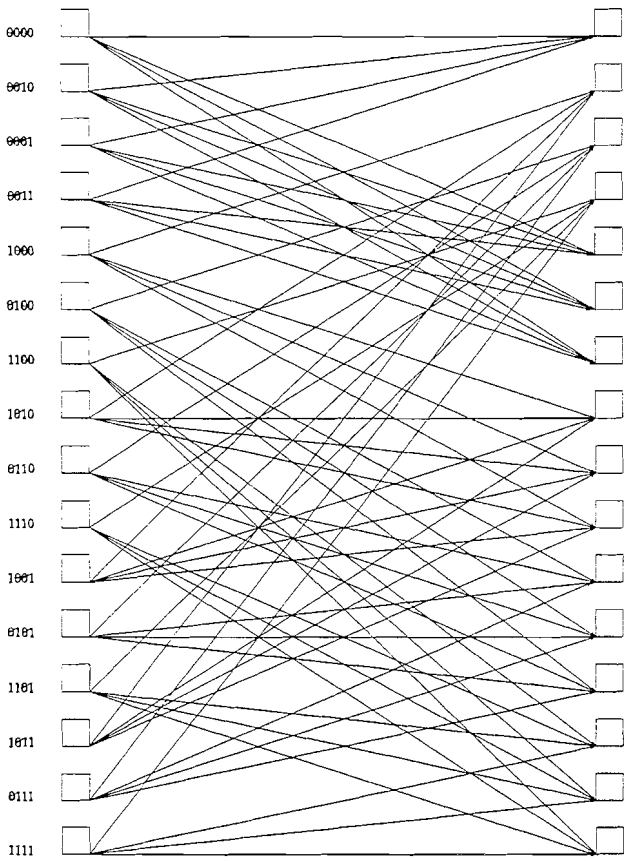

Figura 2. Treliça para o CCE do Exemplo 12

A seção de treliça da máquina $M = (\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2^4, \delta, \beta)$ *é mostrada na Figura 2.. O código associado é um código convolucional binário com distância* $d_{free} = 3$, *taxa* $R_C = 2/3$ *e memória 2, onde* d_{free} *é a menor distância de Hamming entre todas as palavras do código.*

Exemplo 13 *Considere os grupos* $X = \mathbb{Z}_2^2$, $Y = \mathbb{Z}_2^3$, $Q = \mathbb{Z}_2^2$ *e as matrizes* $L_0 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ *e* $L_1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$. *O mapeamento* $\delta : X_{\oplus} Q \rightarrow Q$ *é dado por* $\delta(x, q) = x$. *O mapeamento* $\beta : X_{\oplus} Q \rightarrow Y$ *é dado por* $\beta(x, q) = xL_0 + qL_1$. *A seção de treliça desta máquina* $M = (\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2^2, \delta, \beta)$ *é mostrado na Figura 3.. O código associado possui* $d_{free} = 3$, $R_C = \frac{2}{3}$ *e memória 2. Este código é catastrófico, pois para o estado inicial 01 a seqüência ....0101010101 é codificada na palavra código 00000000.....*

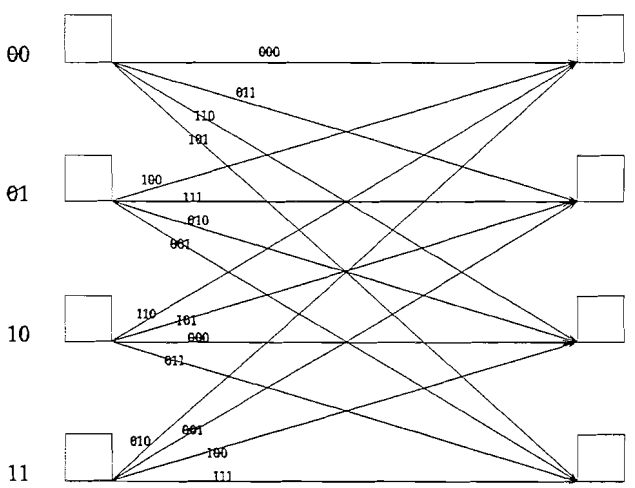

Figura 3. Treliça para o CCE do Exemplo 13

Exemplo 14 *Dado o CCE do Exemplo 13, considere o subgrupo normal* Q' *de* Q, *denotado por* $Q' \lhd Q$, *e especificado por* $Q' = \{00, 10\}$. *Então* $Y' \lhd Y$ *é dado por* $Y' = \{000, 110\}$. *Com isso, as classes determinadas por* Q' *são*

$$\begin{aligned} Q' &= \{00, 10\} \\ 01 + Q' &= \{01, 11\}. \end{aligned}$$

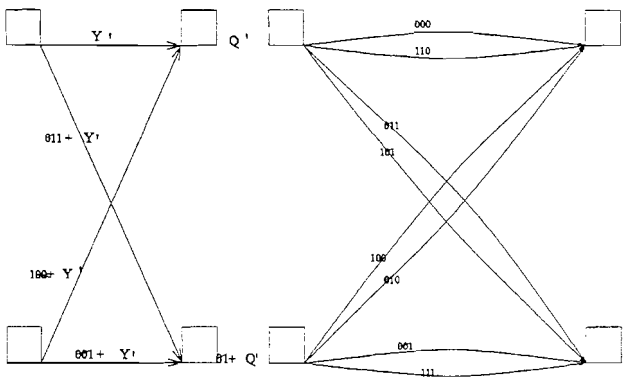

Figura 4. Treliça para a máquina do Exemplo 14.

As classes determinadas por Y' são :

$$\begin{aligned} Y' &= \{000, 110\} \\ 100 + Y' &= \{100, 010\} \\ 001 + Y' &= \{001, 111\} \\ 011 + Y' &= \{011, 101\} \end{aligned}$$

Então a nova máquina $(X, \frac{Y}{Y'}, \frac{Q}{Q'}, \delta', \beta')$ é especificada pelo mapeamento $\delta' : X_{\oplus}\frac{Q}{Q'} \rightarrow \frac{Q}{Q'}$ definido por $\delta'(x, q + Q') = \delta(x, q) + Q'$ e pelo mapeamento $\beta' : X_{\ominus}\frac{Q}{Q'} \rightarrow \frac{Y}{Y'}$ definido por $\beta'(x, q + Q') = \beta(x, q) + Y'$, onde δ e β estão definidos no Exemplo 13.

Uma representação da seção de treliça desta máquina é mostrada no lado esquerdo da Figura 4..

No lado direito da mesma figura, é mostrado a representação completa, isto é, os elementos das classes de Y'. Nenhuma destas treliças corresponde à de um CCE. Considerando que $\{Q', 01 + Q'\} \cong \mathbb{Z}_2$, a treliça do lado direito é produzida pela máquina $M = (\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2, \delta, \beta)$ onde $\delta : \mathbb{Z}_2^2 \oplus \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ é definido por $\delta(x_1, x_2; q) = x_2$, e $\beta : \mathbb{Z}_2^2 \oplus \mathbb{Z}_2 \rightarrow \mathbb{Z}_2^3$ é definido por $\beta(x_1, x_2; q) = (x_1 + q, x_1 + x_2, x_2)$. Esta máquina produz o mesmo código que o CCE do Exemplo 13. Note que esta máquina **não satisfaz** *todas as propriedades do CCE (por exemplo a cardinalidade dos estados é menor do que a cardinalidade do grupo de entradas). Por isso uma definição mais geral é necessária.*

Definição 15 *Um codificador abeliano é uma máquina $M_{\oplus} = (X, Y, Q, \delta, \beta)$, onde X, Y, Q são grupos abelianos finitos, e $\delta : X_{\oplus}Q \rightarrow Q$ e $\beta : X_{\ominus}Q \rightarrow Y$ são tais que*

- *δ é homomorfismo sobrejetor ;*
- *β é um homomorfismo tal que a aplicação Ψ, dada em (1), é injetora.*

Assim, o CCE é um caso particular do codificador abeliano. Porém, um codificador abeliano não está definido para grupos não abelianos. Na próxima seção iremos estabelecer as condições para a construção de codificadores abelianos.

4. CONSTRUÇÃO DE CODIFICADORES CONVOLUCIONAIS ABELIANOS

Seja $H_{\oplus}K$ o produto direto de H e K. Seja Φ_K a classe de homomorfismos sobrejetores entre $H_{\oplus}K$ e K, isto é ,

$$\Phi_K = \{\phi : H_{\oplus}K \rightarrow K \ : \ \phi \text{ é sobrejetora}\}. \quad (5)$$

Seja $\mathcal{X}$ uma família de subconjuntos de $H_{\ominus}K$, definido por

$$\mathcal{X} = \{S \ : \ S = Ker(\phi), \ \phi \in \Phi_K\}. \quad (6)$$

Então, pelo teorema fundamental dos homomorfismos [6], [7], para cada $S \in \mathcal{X}$ temos que $S \lhd H_{\ominus}K$ e $\frac{H_{\oplus}K}{S} \cong K$.

Seja H_0 o subconjunto de $H_{\oplus}K$ definida por

$$H_0 = \{(h, e_K) \ : \ h \in H\}. \quad (7)$$

Então, $H_0 \in \mathcal{X}$ pois $H_0 = Ker(p_2)$, onde $p_2 : H_{\oplus}K \rightarrow K$ é a projeção dada por $p_2(h, k) = k$. Consequentemente, $p_2 \in \Phi_K$ e $\mathcal{X}$ é uma subclasse não vazia. Veremos que para efeito de construção de bons códigos, $\mathcal{X}$ terá que ter mais do que um elemento.

Considere a classe $\mathcal{X}$ definida em (6). Defina $H_1 \in \mathcal{X}$ como sendo

$$H_1 = Ker(\delta). \quad (8)$$

Os subgrupos H_0 e H_1, onde H_0 é definido em (7), são fundamentais na construção de codificadores, como veremos a seguir.

Sejam G e H grupos tais que H é um subgrupo normal de G, isto é, $H \lhd G$. Seja $\mathcal{N}_G$ a classe dos subgrupos normais de G, isto é ,

$$\mathcal{N}_G = \{H \ : \ H \lhd G\}. \quad (9)$$

Omitiremos a demonstração do próximo teorema, pois a mesma é simples.

Teorema 16 *Se $N \in \mathcal{N}_G$, então $G \cong N_{\oplus}\frac{G}{N}$.*

Lema 17 *Seja $Q_{0i} \subset Q$ definido por $Q_{0i} = \left\{q \in Q \ : \ \delta_i\left(\overset{(i)}{x}, e_Q\right) = q\right\}$, onde $\overset{(i)}{x} = (x_j, x_{j+1}, \ldots, x_{j+1-i})$. Então $Q_{0i} \lhd Q$.*

Prova : *Seja $H_i' = \left\{\left(\overset{(i)}{x}, e_Q\right) \ : \ \overset{(i)}{x} \in X^i\right\}$, onde X^i denota i cópias de X, então considerando a projeção $p_2 : X^i{}_{\oplus}Q \rightarrow Q$ dada por $p_2\left(\overset{(i)}{x}, q\right) = q$, temos que p_2 é um homomorfismo sobrejetor com $Ker(p_2) = H_i'$. Logo, $H_i' \lhd X^i{}_{\oplus}Q$. Por outro lado, uma vez que δ é sobrejetora temos que δ_i também é sobrejetora. Logo, $\delta_i(H_i') \lhd Q$ (a imagem de um subgrupo normal por um homomorfismo sobrejetor é também normal). Consequentemente, $\delta_i(H_i') = \left\{\delta_i\left(\overset{(i)}{x}, e_Q\right) \ : \ \overset{(i)}{x} \in X^i\right\} = Q_{0i}$.* ■

Lema 18 *Dado $q \in Q$, seja $Q_{qi} = \left\{\delta_i\left(\overset{(i)}{x}, q\right) \ : \ \overset{(i)}{x} \in X^i\right\}$. Então , Q_{qi} é uma classe lateral de Q_{0i}. Portanto, $|Q_{0i}| = |Q_{qi}|$.*

Prova : *Considere a classe* $\binom{(i)}{u},q).H_i'$ *de* H_i'. *Então,* $\binom{(i)}{u},q).H_i' = \binom{(i)}{u},q).\left\{\left(\binom{(i)}{x},e_Q\right) : \binom{(i)}{x} \in X^i\right\}$ $= \left\{\left(\binom{(i)}{x},q\right) : \binom{(i)}{x} \in X^i\right\}$. *Logo,* $\delta_i\left(\binom{(i)}{u},q).H_i\right) = \left\{\delta_i\left(\binom{(i)}{x},q\right) : \binom{(i)}{x} \in X^i\right\} = Q_{qi}$. *Por outro lado,* $\delta_i\left(\binom{(i)}{u},q).H_i'\right) = \delta_i\left(\binom{(i)}{u},q\right).\delta_i(H_i') = \delta_i\left(\binom{(i)}{u},q\right).Q_{0i}$. *Assim,* $Q_{qi} = \delta_i\left(\binom{(i)}{u},q\right).Q_{0i}$. *Isto mostra que* Q_{qi} *é uma classe lateral de* Q_{0i} *e que, portanto,* $|Q_{0i}| = |Q_{qi}|$. ■

Teorema 19 *Seja* $Q_{0i} \lhd Q$ *o subgrupo normal de* Q *definido no Lema 17. Então,* $M_\oplus = (X, Y, Q, \delta, \beta)$ *é controlável se, e somente se,* $Q_{0i} = Q$, *para algum* $1 \leq i < |Q|$.

Prova : *Suponha* $M_\ominus$ *controlável. Então, se*

$$i = max\left\{j \in \mathbb{N}, j < |Q| : \delta_j\left(\binom{(j)}{x},e_Q\right) = q, \binom{(j)}{x} \in X^j, q \in Q\right\}$$

teremos[1] *que para todo* $q \in Q$ *existe* $\binom{(i)}{x} \in X^i$ *tal que* $\delta_i\left(\binom{(i)}{x},e_Q\right) = q$, *pois se* $q = \delta_j\left(\binom{(j)}{u},e_Q\right)$ *para* $j < i$, *então tomando* $\binom{(i)}{x} = x_i, \ldots, x_{1+i-j}, \binom{(i-j)}{x}$, *onde* $\binom{(i-j)}{x} = \{elemento\ identidade\ de\ X^{i-j}{}_\oplus Q\}$, *e para* $s > i - j$, *considere* x_s *como sendo* $x_s = u_{s-(i-j)}$. *Temos então que* $q = \delta_i\left(\binom{(i)}{x},e_Q\right)$. *Portanto, para todo* $q \in Q$ *temos que* $q \in Q_{0i}$.

Na outra direção do teorema, suponha que $Q = Q_{0i}$, *para algum* $i \geq 1$. *Então, dados* q *e* $r \in Q$, *considere a classe* $Q_{qi} = \left\{\delta_i\left(\binom{(i)}{x},q\right) : \binom{(i)}{x} \in X^i\right\}$ *definida no Lema 18. Como* $|Q_{0i}| = |Q_{qi}| = |Q|$, *então existe* $\binom{(i)}{u} \in X^i$ *tal que* $\delta_i\left(\binom{(i)}{x},q\right) = r$. ■

Teorema 20 ***(Construção de codificadores controláveis isomorfos a partir das entradas e dos estados)*** *: Dado* $X_\oplus Q$, *seja* Y *qualquer grupo isomorfo a* $X_\oplus Q$ *via* β, *isto é* , $Y \overset{\beta}{\cong} X_\oplus Q$. *Seja* $m \in \mathbb{N}$ *definido por* $m = \frac{|Q|}{2}$ *se* $|Q|$ *é par e* $m = \frac{|Q|+1}{2}$ *se* $|Q|$ *é ímpar. Se* H_0 *e* H_1, *definidos respectivamente por (7) e (8), são tais que* $H_0 \neq H_1$, *e se existir um homomorfismo sobrejetor* $\delta : X_\oplus Q \to Q$ *tal que*

$$i) \quad Ker(\delta) = H_1$$
$$ii) \quad \left|\left\{\delta_m\left(\binom{(m)}{x},e_Q\right) : \binom{(m)}{x} \in X^m\right\}\right| > m.$$

Então, $M_\oplus = (X, Y, Q, \delta, \beta)$ *é um codificador isomorfo controlável.*

[1]Isto é o princípio da controlabilidade : j-controlabilidade implica $j+1$-controlabilidade.

Prova : *Pelas hipóteses do teorema é claro que* $M_\ominus = (X, Y, Q, \delta, \beta)$ *é um codificador isomorfo. Só resta então provar a controlabilidade. Para isso, seja* Q_{0i} *o subgrupo normal de* Q *definido no Lema 17. Pelo Teorema 19, temos que* $M_\ominus = (X, Y, Q, \delta, \beta)$ *é não controlável se e somente se* $|Q_{0i}| < |Q|$, *para todo* $i \in \mathbb{N}$. *Mas,* $|Q_{0i}| < |Q|$ *implica que* $|Q_{0i}| \leq \frac{|Q|}{2} \leq m$. *Assim,* $M_\ominus = (X, Y, Q, \delta, \beta)$ *é não controlável se, e somente se,* $|Q_{0i}| \leq m$. *Como* $|Q_{0m}| > m$, *então* $Q_{0m} = Q$. *Logo,* $M_\ominus = (X, Y, Q, \delta, \beta)$ *é controlável.* ■

Teorema 21 ***(Construção de codificadores isomorfos controláveis a partir das saídas)*** *: Dado um grupo finito* Y, *suponha que* $U_0 \lhd Y$ *e* $U_1 \lhd Y$ *são subgrupos normais tais que :*

$$i) \quad |U_0| = |U_1|$$
$$ii) \quad U_1 \neq U_0$$
$$iii) \quad \frac{Y}{U_1} \cong \frac{Y}{U_0}.$$

Então,

- $Y \overset{\xi}{\cong} X_\oplus Q$, *para algum isomorfismo* ξ.
- *Se* H_0 *e* H_1 *são os subgrupos normais de* $X_\ominus Q$ *tais que* $U_0 \overset{\xi}{\cong} H_0$ *e* $U_1 \overset{\xi}{\cong} H_1$, *então* H_0 *satisfaz a equação (7);* $H_1 \in \mathcal{X}$, *onde* $\mathcal{X}$ *é definido por (6). Além disso,* $H_0 \neq H_1$.
- *Se existir um homomorfismo sobrejetor* $\delta : X_\ominus Q \to Q$ *tal que*

$$i) \quad Ker(\delta) = H_1$$
$$ii) \quad \left|\left\{\delta_m\left(\binom{(m)}{x},e_Q\right) : \binom{(m)}{x} \in X^m\right\}\right| > m,$$

onde m *é definido pelo Teorema 20 e* $\beta = \xi^{-1}$. *Então,* $M_\ominus = (X, Y, Q, \delta, \beta)$ *é um codificador isomorfo controlável.*

Prova :

- *Pelo Teorema* 16, $Y \cong U_0 \oplus \frac{Y}{U_0}$. *Para* $y \in Y$, seja $y_1 \in U_0$ *e seja* $y_2 \in Y$ *o representante de* $\frac{Y}{U_0}$, *tal que* $y = (y_1, y_2)$. *Sejam* X, Q *grupos tais que* $U_0 \overset{\theta_1}{\cong} X$ e $\frac{Y}{U_0} \overset{\theta_2}{\cong} Q$, *para alguns isomorfismos* θ_1 e θ_2. *Então,* $Y \cong U_0 \oplus \frac{Y}{U_0} \overset{\xi}{\cong} X_\oplus Q$, *onde* $\xi = (\theta_1, \theta_2)$;
- *Para* $y = (y_1, y_2) \in Y \cong U_0 \oplus \frac{Y}{U_0}$, *temos que o representante de* y *em* $X_\oplus Q$ *é* $(\theta_1(y_1), \theta_2(y_2))$. *Em particular, se* $y \in U_0$, *então* $y = (y, e_Y)$, *daí* $\xi(y) = \xi(y, e_Y) = (\theta_1(y), \theta_2(e_Y)) = (\theta_1(y), e_Q) \in H_0 \subset X_\oplus Q$. *Logo,* H_0 *satisfaz a equação (7). Por outro lado, como* $\frac{Y}{U_1} \cong \frac{Y}{U_0}$ *e* $\frac{Y}{U_0} \cong Q$ *temos que* $U_1 = Ker(\phi_1)$, *onde* ϕ_1 *é algum homomorfismo sobrejetor* $\phi_1 : Y \to Q$. *Considere a composição de homomorfismos* $\phi_1 \circ \xi^{-1} : X_\oplus Q \to Q$, *então* $\phi_1 \circ \xi^{-1}$ *é sobrejetor e* $Ker(\phi_1 \circ \xi^{-1}) = \{(x, q) : \phi_1 \circ \xi^{-1}(x, q) = e_Q\} = \{(x, q) : \phi_1(\xi^{-1}(x, q)) = e_Q\} = \{(x, q) : \xi(y) = (x, q), \phi_1(y) = e_Q\} = H_1$. *Finalmente, fica claro que* $U_0 \neq U_1$ *implica* $H_0 \neq H_1$;

– *Fazendo* $\delta = \phi_{1_o}\xi^{-1}$, *as condições do Teorema 20 são satisfeitas.* ■

Por outro lado, em [11] é provado que se a seção de treliça for isomorfa a um grupo abeliano cíclico, isto é, $Y \approx \mathbb{Z}_n$, então o correspondente codificador é não controlável. Com isso, somente os grupos abelianos não cíclicos é que poderão levar a bons códigos convolucionais abelianos.

Tendo como base o Teorema 21, iremos considerar o caso de códigos convolucionais abelianos cujos elementos do grupo das entradas são k-uplas binárias, o grupo dos estados são $(n-k)$-uplas binárias, e consequentemente o grupo das saídas são n-uplas binárias, mais especificamente $Y \approx \mathbb{Z}_2^n \approx \mathbb{Z}_2^k \oplus \mathbb{Z}_2^{n-k}$. A seguir, apresentamos um algoritmo para a construção da máquina $M_\oplus = (\mathbb{Z}_2^k, \mathbb{Z}_2^n, \mathbb{Z}_2^{n-k}, \delta, \beta)$ associada a um código convolucional binário de taxa $r = k/n$ e memória $m = n - k$.

Algoritmo

Passo 1 - *Encontrar* $U_0 \lhd \mathbb{Z}_2^n$ *e* $U_1 \lhd \mathbb{Z}_2^n$ *tal que,*
1a $|U_0| = |U_1| = 2^k$.
1b $U_0 \neq U_1$.
1c *Se os pesos de Hamming de* U_0 *e de* U_1, $w(U_0)$ *e* $w(U_1)$, *respectivamente, são* $w(U_0) = d_0$ *e* $w(U_1) = d_1$, *então* $d_0 + d_1 = d$, *deve ser tal que*

$$d = max\{w(V_0) + w(V_1)\},$$

V_0 *e* V_1 *estão sujeitos a* $V_0,\ V_1 \lhd \mathbb{Z}_2^n$; $|\ V_0\ | = |\ V_1\ | = 2^k$ *e* $V_0 \neq V_1$.
1d *De modo a evitar transições paralelas, então* $U_0 \cap U_1 = 0 \in \mathbb{Z}_2^n$.

Passo 2 - *Considere* U_0 *e* U_1 *como subespaços vetoriais de* $\mathbb{Z}_2^n$, *e considere as bases* $\{u_1, \ldots, u_k\}$ *de* U_0, *e* $\{u_1, \ldots, u_t, v_1, \ldots, v_{k-s}\}$ *de* U_1. *Note que* $s = 0$ *se, e somente se,* $U_0 \cap U_1 = 0 \in \mathbb{Z}_2^n$.

Passo 3 - *Seja* $\{e_i\}_{i=1}^n$ *a base canônica de* $\mathbb{Z}_2^n$, *onde* e_i *é definida por* $e_i = (x_1, \ldots, x_i, \ldots, x_n)$ *e seus componentes são tais que* $x_j = 0$ *if* $j \neq i$ *e* $x_j = 1$ *se* $j = i$. *Então, defina o mapeamento de rotulamentos como sendo o isomorfismo* $\beta : \mathbb{Z}_{2_\oplus}^k \mathbb{Z}_2^{n-k} \rightarrow \mathbb{Z}_2^n$ *tal que*

$$\beta^{-1}(u_i) = e_i,$$
$$\beta^{-1}(v_j) = e_{k+j};$$

com a finalidade de otimizar a distância livre, a definição de β *para os restantes* $n - (2k - s)$ *vetores da base* $\{e_i\}_{i=1}^n$ *é deixada para o* **Passo 7**.

Passo 4 - *Calcular* $H_0 = \beta^{-1}(U_0)$, $H_1 = \beta^{-1}(U_1)$, *e* $\Pi_2(H_1)$, *onde* $\Pi_2 : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^{n-k}$ *é a projeção definida por* $\Pi_2(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) = (x_{k+1}, \ldots, x_n)$.

Passo 5 - *Usando os elementos do grupo das classes laterais* $\frac{\mathbb{Z}_2^n}{H_1}$, *defina a aplicação do próximo estado como sendo o homomorfismo de grupos* $\delta : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^{n-k}$ *com as seguintes condições*

5a $Ker(\delta) = H_1$, *significando que*

$$\delta(e_{k+j}) = 0 \text{ para } j = 1, \ldots, k - s.$$

5b *Se* $n - (2k - s) > 0$ *então,* $\delta(H_0) \cap \Pi_2(H_1) = 0 \in \mathbb{Z}_2^{n-k}$, *significando que*

$$\delta(e_i) \notin \Pi_2(H_1), \text{ para } i = 1, \ldots, k.$$

Passo 6 - *A definição de* δ *para os remanescentes* $n-(2k-s)$ *vetores da base* $\{e_i\}_{i=1}^n$ *deve ser feito de modo que,*
6a *Satisfaça o teste de controlabilidade :* $\left|\left\{\delta_{2^{n-k-1}}\binom{(2^{n-k-1})}{x}, 00\right) : \binom{(2^{n-k-1})}{x} \in \mathbb{Z}_2^{k \cdot 2^{n-k-1}}\right\}\right| > 2^{n-k-1}$.
6b *Tratando de que* $\delta(x, \delta(H_0)) \notin \Pi_2(H_1)$ *para todo* $x \in X$.
6c *Se* $\delta(x, \delta(H_0)) \notin \Pi_2(H_1)$ *para todo* $x \in X$ *então, fazer outra tentativa para que* $\delta(x_2, \delta(x_1, \delta(H_0))) \notin \Pi_2(H_1)$, *para todo* $x_2,\ x_1 \in X$. *Tentar outra vez para* $x_3 \in X$, *e assim por diante. Usando a definição de* δ *com relação à base* $\{e_i\}_{i=1}^n$, *escrever a regra explícita de* δ.

Passo 7 - *Defina* β *para os remanescentes* $n - (2k - s)$ *vetores da base* $\{e_i\}_{i=1}^n$ *fazendo uma adequada distribuição dos pesos conforme a dinâmica da treliça obtida através de* δ *no* Passo 5 *e* Passo 6. *Usando a definição de* β *em relação à base* $\{e_i\}_{i=1}^n$, *escrever a regra explícita de* β.

Este algoritmo gera a máquina $M_\oplus = (\mathbb{Z}_2^k, \mathbb{Z}_2^n, \mathbb{Z}_2^{n-k}, \delta, \beta)$ associada a um código convolucional binário, não catastrófico com taxa $r = k/n$, memória $m = n - k$ e $d_{free} \geq d$.

Exemplo 22 *Construção de um código convolucional binário a partir da máquina* $M_\oplus = (\mathbb{Z}_2^2, \mathbb{Z}_2^4, \mathbb{Z}_2^2, \delta, \beta)$

Passo 1 - *Determinação de* U_0 *e* U_1,

$$U_0 = \{0000, 1001, 1110, 0111\} \quad U_1 = \{0000, 1100, 0011, 1111\}$$

Então, os pesos de Hamming de U_0 *e de* U_1 *são* $w(U_0) = w(U_1) = 2$, *respectivamente.*

Passo 2 - *Determinação das bases para* U_0 *e para* U_1 : $\{1001, 1110\}$ *é uma base para* U_0, *e* $\{1100, 0011\}$ *é uma base para* U_1. *Note que, como* $U_0 \cap U_1 = \{0000\}$, *então* $s = 0$.

Passo 3 -

$$\beta^{-1}(1001) = 1000 \qquad \beta^{-1}(0011) = 0010$$
$$\beta^{-1}(1110) = 0100 \qquad \beta^{-1}(1100) = 0001$$

Passo 4 -

$$H_0 = \{(00, 00), (10, 00), (01, 00), (11, 00)\}$$
$$H_1 = \{(00, 00), (00, 10), (00, 01), (00, 11)\}$$

$$\Pi_2(H_1) = \{00, 10, 01, 11\}$$

Passo 5 - *Para que* $Ker(\delta) = H_1$, *temos*

$$\delta(00, 10) = 00$$
$$\delta(00, 01) = 00.$$

Como $n - (2k - s) = 4 - (4 - 0) = 0$ *então, não é possível que* $\delta(H_0) \cap \Pi_2(H_1) = \{00\}$. *Logo,*

$$\delta(10, 00) = 11$$
$$\delta(01, 00) = 01$$

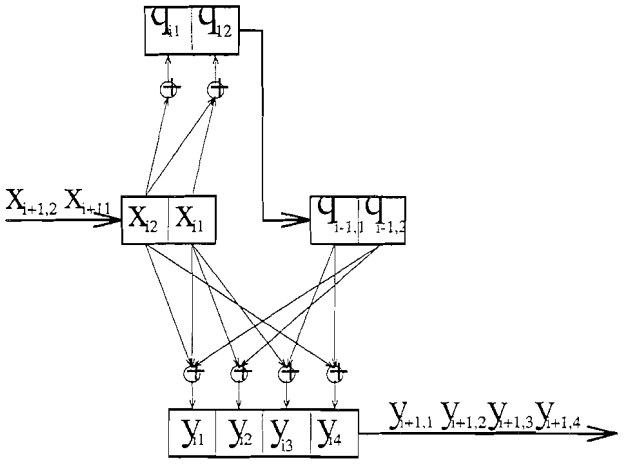

Figura 5. Codificador convolucional abeliano $M_{\oplus} = (\mathbb{Z}_2^k, \mathbb{Z}_2^n, \mathbb{Z}_2^{n-k}, \delta, \beta)$.

Passo 6 *-Neste exemplo não existem $n-(2k-s)$ vetores remanescentes $\{e_i\}_{i=1}^4$, pois $n-(2k-s) = 4-(4-0) = 0$. Portanto, δ é dado por*

$$\begin{aligned}\delta(x_2, x_1; q_1, q_2) &= x_2\delta(e_1) + x_1\delta(e_2) + q_1\delta(e_3) + q_2\delta(e_4)\\ &= x_2.11 + x_1.01 + q_1.00 + q_2.00\\ &= (x_2, x_2 + x_1)\end{aligned}$$

Passo 7 *- Como não há vetores remanescentes, resta escrever a regra de correspondência de β, isto é,*

$$\begin{aligned}\beta(x_2, x_1; q_1, q_2) &= x_2\beta(e_1) + x_1\beta(e_2) + q_1\beta(e_3) + q_2\beta(e_4)\\ &= x_2.1001 + x_1.1110 + q_1.0011 + q_2.1100\\ &= (x_2 + x_1 + q_2, x_1 + q_2, x_1 + q_1, x_2 + q_1)\end{aligned}$$

O codificador resultante é mostrado na Figura 5.. O código correspondente têm taxa $R_c = \frac{1}{2}$, distância livre $d_{free} = 5$ e um ganho assintótico de 3.98 dB.

5. CONCLUSÕES

Neste trabalho foram estabelecidas as condições necessárias e suficientes para a construção de códigos convolucionais abelianos. Mostramos que tais códigos são controláveis, completos e mínimos, esta última proposição via uma proposta de redução de estados, e tendo como subclasse os códigos convolucionais elementares. Como consequência do fato de que os códigos convolucionais abelianos cuja seção de treliça é isomorfa a um grupo cíclico implica em o correspondente codificador ser não controlável, então um algoritmo de construção de códigos convolucionais abelianos tendo como grupo das entradas, de estados e de saídas, k-uplas, $(n-k)$-uplas e n-uplas binárias, respectivamente, foi proposto. Exemplos de codificadores convolucionais elementares e abelianos foram apresentados.

REFERÊNCIAS

[1] M.D.Trott, The Algebraic Structure of Trellis Codes, Ph.D. Dissertation, Dept. of Elect. Eng., Stanford University, Stanford, CA, Aug. 1992.

[2] H.A.Loeliger, On Euclidean-Space Group Codes, Ph.D. Dissertation, Swiss Federal Institute of Technology, Zurich, 1992.

[3] G. D. Forney, "Geometrically uniform codes," IEEE Trans. Inform. Theory, vol. IT-37 No 5, pp. 1241-1260, 1991.

[4] J.C.Willems, "Models for dynamics," Dynamics Technical Report, vol. 2, U.Kirchgraber e H.O.Walther, Eds. Wiley and Teubner, 1989.

[5] M.A. Arbib, "Automaton Decomposition and Semigroup Structure," Algebraic Structure of Machine Languages, M.A. Arbib editor, 1968.

[6] M.Hall, The Theory of Groups, Macmillan, New York, 1961.

[7] J.J. Rotman, An Introduction to the Theory of Groups, Springer-Verlag, Fourth ed., 1995.

[8] H.A. Loeliger, G.D. Forney, T. Mittelholzer, and M.D. Trott, "Minimality and observability of group systems," Linear Algebra and its Applications, vol 205-206, pp 937-963, July 1994.

[9] M.A. Arbib, Brains, Machines, and Mathematics, Springer-Verlag, Second ed. ; 1986.

[10] G.D. Forney and M.D. Trott, "The dynamics of group codes : state spaces, trellis diagrams and canonical encoders", IEEE Trans. Inform. Theory, vol IT 39(5) :1491-1513, September 1993.

[11] J. P. Arpasi, Codificadores Convolucionais Homomorfos, Tese de Doutorado, FEEC-UNICAMP, Junho 1997.

Jorge Pedraza Arpasi nascido em Puno, Peru em 1961. Bacharel em Matemática pela Universidad San Agustin do Peru, 1987. Mestre em Matemática pelo Instituto de Matmática Pura e aplicada (IMPA), 1990. Doutor em Engenharia Elétrica, area de comunicações, 1996. Pos-Doutorado no Departamento de Telemática da Faculdades de Engenharia Elátrica e Computação (FEEC) da Universidade Estadual de Campinas desde 1997 até a presente data. Area de Trabalho : Códigos correctores de errros.

Reginaldo Palazzo JR. received the Electrical Engineering and MSEE degrees from University Estadual de Campinas - UNICAMP, SP, Brazil, in 1975 and 1977 respectively, and the Engineer and PH.D. degrees from the University of California,Los Angeles, CA, USA, in 1981 and 1984, respectively,. In May 1985 he joined the Faculty of Eletrical and Computing Engineering, UNICAMP, where he received the Livre-Docência degree in 1987. Since 1996 he is a Professor and Chair of the Algebraic and Geometric Coding Group. His research interests are in coding, information, and communication theory.