Classe de Equivalência de Códigos de Treliça Via Partições de Reticulados

João Coelho Silva Filho
Departamento de Matemática, CECEN, UEMA,
São Luís, MA
E-mail: jcoelhof@dt.fee.unicamp.br,

Emília de Mendonça Rosa Marques
Departamento de Matemática, FC, UNESP,
Bauru, SP
E-mail: emilia@fc.unesp.br

Walter da Cunha Borelli
Departamento de Telemática, FEEC, UNICAMP,
Campinas, SP
E-mail: borelli@dt.fee.unicamp.br,

Resumo Neste trabalho é proposta uma técnica para determinar códigos equivalentes (mesmo espectro de peso) para o sistema de codificação de códigos de treliça via partição de reticulados. No conjunto dos códigos de treliça ótimos é investigada a equivalência através de operadores lineares e propriedades de grupos. Uma nova equivalência é determinada com a utilização de uma composição nos operadores, gerando grupos diedrais e o grupo de Klein.

Palavras-chave Códigos Equivalentes; Grupos e Códigos de Treliça; Reticulados; Grupos Diedrais.

1 Introdução

O sistema de codificação do código de treliça usado neste trabalho é baseado em [1]. O código usa constelações de sinais mapeadas por pontos de um reticulado n-dimensional Λ e um subreticulado Γ de Λ, com o mesmo número de pontos em cada classe lateral de Λ/Γ. A entrada do codificador convolucional utilizado no código de treliça é uma sequência de símbolos de um alfabeto de um anel $A = GF(q)$ e a saída é uma sequência de símbolos de uma constelação de sinais mapeada por um reticulado quociente. Este processo consiste na codificação de constelações de sinais provenientes de reticulados de boa densidade. O particionamento do reticulado mapeia as constelações escolhidas dentre as de melhor energia média.

A construção do código de treliça inicia-se com a escolha de um reticulado Λ em $\mathbb{R}^n$ e um subreticulado Γ de Λ, sendo que as classes laterais $\frac{\Lambda}{\Gamma} = \{x + \Gamma : x \in \Lambda\}$ formam o reticulado quociente, denotado por R, o qual é finito e tem ordem $|R|$. Se $M = \{x_i : 1 \leq i \leq n\}$ é a matriz de Λ e $N = \{y_i : 1 \leq i \leq n\}$ é a matriz de Γ, então $|R| = (\Lambda : \Gamma) = |\det N| \,/\, |\det M|$.

O código de treliça possui $k = k_1 + k_2$ bits de entrada e um ponto de saída entre os elementos do reticulado quociente R, onde os k_1 bits são codificados pelo codificador convolucional e os k_2 bits são os não codificados, usados na escolha dos pontos da constelação de sinais. A constelação possui $|R|^{k_1}$ pontos, o código posssui $|A|^{k_1}$ entradas possíveis e a taxa é dada por:

$$\rho = (k/n) \log_2 |A| \; bits/\dim .$$

Entre os códigos de treliça ótimos de [5] e [6], existem códigos equivalentes, isto é, que apresentam a mesma distribuição de peso entre as suas palavras-código (espectro de peso).

Neste trabalho a equivalência dos códigos de treliça é obtida através da utilização de operadores lineares com propriedades estruturais semelhantes às estruturas algébricas da Teoria de Grupo. A existência da equivalência de códigos de treliça, dentro de conjuntos de matrizes geradoras de códigos ótimos, definidos como *subconjuntos especiais* [3] e [4], é comprovada com a utilização de operadores lineares munidos de uma operação de composição de operadores formando estruturas de grupos diedrais e do grupo de Klein.

Na Seção 2 está apresentada a estrutura e a escolha de subconjuntos especiais. Na Seção 3 é apresentada a proposta de uma nova classe de equivalência para os códigos de treliça e na Seção 4 são apresentados alguns resultados da aplicação desta classe de equivalência em dois exemplos práticos de Códigos de Treliça.

2 Subconjuntos Especiais de Códigos de Treliça

Considerando um reticulado Λ em $\mathbb{R}^n$ e um subreticulado Γ de Λ, as classes laterais $\frac{\Lambda}{\Gamma} = \{x + \Gamma : x \in \Lambda\}$ formam um reticulado quociente,

denotado por R, o qual é finito com ordem $|R|$. O codificador possui $k = k_1 + k_2$ bits de entradas e um ponto de saída dentre os $|R|$ elementos, os quais são pontos da constelação de sinais. A matriz geradora do código de treliça é dada por:

$$G = [\ g_{vk_1} \quad \cdots \quad g_{v1} \quad \cdots \quad g_{0k_1} \quad \cdots \quad g_{01}\ ],$$

onde $g_{ij} \in R$, $v = \max_{1\leq j\leq k_1}\{v_j\}$, com v_j o número de memórias em cada entrada do codificador e o número de memórias do codificador é $V = \sum v_{k_1 j}$. Os símbolos de entrada são rotulados por u_{ij}, onde $(u_{01}, u_{02}, \ldots, u_{0k_1})$ é o bloco de entrada atual e $(u_{11}, u_{12}, \ldots, u_{1k_1})$ é o bloco de entrada anterior e assim sucessivamente. A saída é definida por

$$r = \sum_{i=0}^{v}\sum_{j=1}^{k_1} u_{ij} g_{ij}.$$

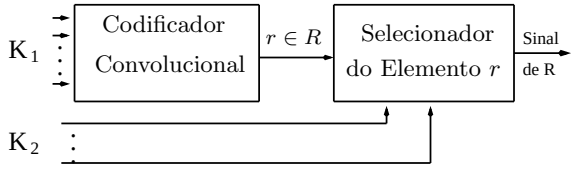

Figura 1: O Esquema de Codificação.

O código possui parâmetros (k_1, V, q), com $G = [g_{ij}]_{n\times(v+k_1)}$. A distância d do código de treliça é a mínima entre o mínimo dentre as métricas dos caminhos fechados com início e final no estado inicial da treliça d_{free} e a distância da partição $d_{\min}$, isto é, $d = \min(d_{free}, d_{\min})$. A Figura 1 mostra o esquema de codificação do código de treliça, a estrutura do codificador é mostrada na Figura 2 e a técnica de codificação é a usada em [5].

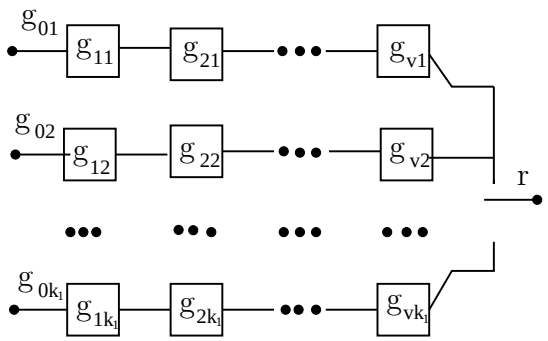

Figura 2: O Codificador Convolucional.

Definição 1 *Um código de treliça é dito ser um* código de treliça ótimo, *quando a distância mínima é a máxima entre os demais códigos de treliça do mesmo sistema de codificação.*

A escolha dos *Subconjuntos Especiais* [3] e [4], conduz a um número reduzido de matrizes que geram códigos ótimos e geram o reticulado quociente R na saída do codificador. A maximização da distância é feita atravcés da matriz geradora de melhor norma. A maximização da matriz norma é calculada a partir dos parâmetros $\Delta_{\inf}$ e $\Delta_{\sup}$, generalizados pelas expressões:

$$\Delta_{inf} = \min_{\{u_l\}}\left\{\left\|\sum_{j=1}^{s} u_{1j}g_{vj} + \sum_{j=s+1}^{k_1} u_{1j}g_{(v-1)j}\right\|\right\} + \min_{\{u_l\}}\left\{\left\|\sum_{j=1}^{k_1} u_{1j}g_{0j}\right\|\right\},$$

onde $s = V - k_1(v-1)$ e

$$\Delta_{sup} = \min_{\{u_l\}}\left\{\sum_{i=0}^{v}\left\|\sum_{j=1}^{k_1} u_{1j}g_{ij}\right\|\right\}.$$

As matrizes geradoras de códigos ótimos serão escolhidas no subconjunto especial associado a melhor matriz norma $GN = [\|g_{ij}\|]_{1\times(v+k_1)}$, com

$$GN = [\|g_{vk_1}\| \cdots \|g_{v1}\| \cdots \|g_{0k_1}\| \cdots \|g_{01}\|].$$

Os elementos do reticulado quociente serão rotulados de 0 a $(|R|-1)$, definindo a matriz dos rótulos $GR = [a_{ij}]_{1\times(v+k_1)}$, com $a_{ij} \in R$, onde $0 \leq i \leq |R|-1$. Na matriz dos rótulos é aplicada a Tabela de Cayley simplificando a operação na saída do codificador.

3 Uma Classe de Códigos Equivalentes

Considere uma partição de reticulado em um espaço de dimensão n, onde os elementos são as classes laterais $g = (x_1, x_2, \ldots, x_n) \in \Lambda/\Gamma$. Uma família de transformações lineares é definida por

$$\begin{array}{rcl} \varphi & : & R \longrightarrow R \\ & : & g_i \longmapsto g_j, \end{array} \qquad (1)$$

tal que $\varphi(x_1, x_2, \ldots, x_n) = (y_1, y_2, \cdots, y_n)$, com

$$\begin{cases} y_i = x_j, \ para\ algum\ \ i, j \in \{1, \ldots, n\}, \\ y_i = -x_i, \ para\ \ algum\ \ i \in \{1, \cdots, n\}\ e/ou \\ y_i = x_i, \ \ para\ \ os\ \ demais. \end{cases}$$

A transformação linear

$$\varphi \ : \ \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

é denominada de operador linear, assim, a transformação linear definida em (1) é um operador linear. Quando $\varphi(g) = g$, para todo g, φ é denominado de operador identidade e é indicado por I.

Por definição

$$\|g\| = \sum_{i=1}^{n} x_i^2$$

e por (1):

$$\|\varphi(x_1, x_2, \ldots, x_n)\| = \sum_{j=1}^{n} y_j^2.$$

Assim,

$$\begin{aligned} \|\varphi(g)\| &= \sum x_i^2 + \sum (-x_i)^2 + \sum x_j^2 \\ &= \sum_{i=1}^{n} x_i^2 = \|g\|. \end{aligned}$$

Logo,

$$\|\varphi(g)\| = \|g\|$$

Nestas condições, concluímos que,

$$\left\| \sum_{i,j} u_{ij} \varphi(g_{ij}) \right\| = \left\| \sum_{i,j} u_{ij} g_{ij} \right\|. \qquad (2)$$

e além disso, se φ_1 e φ_2 são dois operadores lineares, então o operador composição $\varphi = \varphi_1 \circ \varphi_2$ é tal que:

$$\|(\varphi_1 \circ \varphi_2)(g)\| = \|\varphi(g)\| = \|g\|.$$

Portanto, $\varphi = \varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_m$ é tal que:

$$\|(\varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_m)(g)\| = \|\varphi(g)\| = \|g\|.$$

Definição 2 *Dois códigos convolucionais C_1 e C_2 são ditos códigos equivalentes se seus espectros de peso são idênticos e denotado por $C_1 \equiv C_2$.*

Teorema 1 *Considere C_1 um código convolucional com k_1 entradas e V memórias, gerado pela matriz*

$$G = [\ g_{vk_1} \quad \cdots \quad g_{v1} \quad \cdots \quad g_{0k_1} \quad \cdots \quad g_{01}\ ].$$

Seja $\varphi : R \to R$ uma composição formada por uma família de opreradores lineares, tal que $\varphi = \varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_m$ e

$$\begin{aligned} \varphi(G) = [\ &\varphi(g_{vk_1}) \quad \cdots \quad \varphi(g_{v1}) \quad \cdots \\ &\varphi(g_{0k_1}) \quad \cdots \quad \varphi(g_{01})\ ]. \end{aligned}$$

Então o código convolucional C_2 gerado por $\varphi(G)$ é equivalente ao código C_1 gerado por G.

A prova do Teorema é direta do resultado mostrado em (2).

Tabela 1: Imagens dos Operadores Lineares

$R = \frac{\mathbb{Z}^2}{P_1\mathbb{Z}^2}$	$\rho(R)$	$\phi(R)$
$(0,0)$	$(0,0)$	$(0,0)$
$(1,0)$	$(0,1)$	$(0,1)$
$(0,1)$	$(1,0)$	$(-1,0)$
$(-1,0)$	$(0,-1)$	$(0,-1)$
$(0,-1)$	$(-1,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(1,-1)$
$(1,-1)$	$(1,-1)$	$(1,1)$
$(2,0)$	$(2,0)$	$(2,0)$

4 Aplicação da Equivalência aos Códigos de Treliça

Dois códigos de treliça equivalentes diferem apenas por permutações de elementos do reticulado quociente com mesma norma. Neste caso, dois códigos C_1 e C_2 são equivalentes se um é obtido da permutação de n elementos com mesma norma. Dois casos são apresentados, para elucidar os conceitos abordados e mostrar a existência de tal equivalência, dentre os códigos de treliça de um mesmo subconjunto especial.

$1^{\underline{0}}$ **Caso -** Considere a partição de reticulado $R = \frac{\mathbb{Z}^2}{P_1\mathbb{Z}^2}$, onde

$$P_1 = \begin{pmatrix} 2 & -2 \\ 2 & 2 \end{pmatrix}.$$

e os operadores lineares

$$\rho, \phi : R \to R,$$

com

$$\rho(x,y) = (y,x) \ \text{ e } \ \phi(x,y) = (-y,x).$$

Os elementos de R, $\rho(R)$ e $\phi(R)$ estão mostrados na Tabela 1.

A operação de composição dos operadores possuem estruturas de grupo. Observe que:

$$\begin{cases} (\rho \circ \rho)(x,y) = \rho^2(x,y) = I(x,y) = (x,y), \\ (\phi^2 \circ \phi^2)(x,y) = \phi^4(x,y) = I(x,y) = (x,y), \\ (\phi^3 \circ \rho)(x,y) = (\rho \circ \phi)(x,y) = (x,-y). \end{cases}$$

Assim, a ordem dos elementos ρ e ϕ é 2 e 4 respectivamente. Logo o conjunto $\{\rho, \phi\}$ munido da operação de composição, gera um grupo $(\mathcal{G}, \circ)$, descrito por:

$$\mathcal{G} = \{I, \phi, \phi^2, \phi^3, \rho, \phi\rho, \phi^2\rho, \phi^3\rho\}$$

e por simplicidade escreve-se apenas $\phi\rho$ para denotar $\phi \circ \rho(x,y)$. O grupo $\mathcal{G}$ possui ordem $|\mathcal{G}| = 8$ e é isormorfo ao grupo diedral D_4 das simetrias espaciais do quadrado.

Usando o codificador de parâmetros $(2,4,2)$, sobre o reticulado quociente da Tabela 2, onde a

Tabela 2: Normas e Rótulos

$R=\frac{\mathbb{Z}^2}{P_1\mathbb{Z}^2}$	Rótulo	Norma	Ordem
$(0,0)$	0	0	1
$(1,0)$	1	1	4
$(0,1)$	2	1	4
$(-1,0)$	3	1	4
$(0,-1)$	4	1	4
$(1,1)$	5	2	2
$(1,-1)$	6	2	2
$(2,0)$	7	4	2

Tabela 3: Tabela de Cayley

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	7	5	0	6	4	2	3
2	2	5	7	6	0	3	1	4
3	3	0	6	7	5	2	4	1
4	4	6	0	5	7	1	3	2
5	5	4	3	2	1	0	7	6
6	6	2	1	4	3	7	0	5
7	7	3	4	1	2	6	5	0

operação de adição é mostrada na Tabela 3. A matriz norma do subconjunto especial que contém um código de treliça ótimo, para o sistema considerado é dada por:

$$GN = [\ 4 \quad 2 \quad 1 \quad 2 \quad 4 \quad 2\ ].$$

No subconjuto representado pela GN dada, é realizada a busca da matriz geradora de um código de treliça ótimo e é encontrada a matriz dos rótulos:

$$GR = [\ 7 \quad 5 \quad 2 \quad 1 \quad 5 \quad 7\ ],$$

obtida dentre as matrizes que geram códigos ótimos, com a utilização do algoritmo de busca dos códigos de treliça ótimos, mostrado em [5] e [6]. A utilização da matriz dos rótulos reduz o tempo operacional de cálculo do d_{free} do código de treliça.

Aplicando os Operadores Lineares do grupo $\mathcal{G}$ (Tabela 4), obtém-se 8 matrizes geradoras $\mathcal{G}(GR)$ distintas, correspondentes a 8 códigos equivalentes.

$\mathcal{G}(GR) = \{I(GR), \phi(GR), \phi^2(GR), \phi^3(GR),$

$\rho(GR), \phi\rho(GR), \phi^2\rho(GR)\phi^3\rho(GR)\} =$

$\{[\ 7 \quad 5 \quad 2 \quad 1 \quad 5 \quad 7\ ], [\ 7 \quad 6 \quad 3 \quad 2 \quad 6 \quad 7\ ],$

$[\ 7 \quad 5 \quad 4 \quad 3 \quad 5 \quad 7\ ], [\ 7 \quad 6 \quad 1 \quad 4 \quad 6 \quad 7\ ],$

$[\ 7 \quad 5 \quad 3 \quad 2 \quad 5 \quad 7\ ], [\ 7 \quad 6 \quad 2 \quad 3 \quad 6 \quad 7\ ],$

$[\ 7 \quad 5 \quad 3 \quad 4 \quad 5 \quad 7\ ], [\ 7 \quad 6 \quad 4 \quad 1 \quad 6 \quad 7\ ]\},$

nesta ordem.

Tabela 4: Imagens dos Operadores Lineares

$R=\frac{\Lambda}{P_2\Lambda}$	$\rho(R)$	$\phi(R)$
$(0,0)$	$(0,0)\,0$	$(0,0)\,0$
$\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right)$	$\left(\frac{1}{2},-\frac{\sqrt{3}}{2}\right)$	$\left(-\frac{1}{2},\frac{\sqrt{3}}{2}\right)$
$(-1,0)$	$(-1,0)$	$(1,0)$
$\left(-\frac{1}{2},\frac{\sqrt{3}}{2}\right)$	$\left(-\frac{1}{2},-\frac{\sqrt{3}}{2}\right)$	$\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right)$
$(0,\sqrt{3})$	$(0,\sqrt{3})$	$(0,\sqrt{3})$
$\left(\frac{1}{2},-\frac{\sqrt{3}}{2}\right)$	$\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right)$	$\left(-\frac{1}{2},-\frac{\sqrt{3}}{2}\right)$
$(1,0)$	$(1,0)$	$(-1,0)$
$\left(-\frac{1}{2},-\frac{\sqrt{3}}{2}\right)$	$\left(-\frac{1}{2},\frac{\sqrt{3}}{2}\right)$	$\left(\frac{1}{2},-\frac{\sqrt{3}}{2}\right)$

Analizando as colunas da matriz G, observa-se que existem 2, 4, 4 e 2 possibilidades para as colunas 2, 3, 4 e 5 respectivamente, mostrando a existência de 8 possíveis grupos para a GN, geradoras de códigos ótimos. Portanto, tem-se 64 matrizes geradoras distintas, mas geradoras de códigos de treliça equivalentes.

2º **Caso -** Considere a partição de reticulado $R = \frac{\Lambda}{P_2\Lambda}$, onde $\Lambda = \langle (1,0)\,; (1/2, \sqrt{3}/2)\rangle$ e

$$P_2 = \begin{pmatrix} 2 & -\sqrt{3} \\ 2 & \sqrt{3} \end{pmatrix}.$$

Sejam os operadores lineares

$$\rho, \phi : R \to R,$$

com

$$\rho\,(x,y) = (x,-y) \ \ e\ \phi\,(x,y) = (-x,y)\,.$$

Os elementos de R, $\rho(R)$ e $\phi(R)$ estão mostrados na Tabela 4.

A operação de composição dos operadores é dada por:

$$\begin{cases} (\rho\circ\rho)\,(x,y) = I\,(x,y)\,, \\ (\phi\circ\phi)\,(x,y) = I\,(x,y)\,, \\ (\phi\circ\rho)\,(x,y) = (\rho\circ\phi)\,(x,y)\,. \end{cases}$$

Assim, a ordem dos elementos ρ e ϕ é 2. Logo, o conjunto $\{\rho,\phi\}$ munido da operação de composição, gera um grupo $(\mathcal{G},\circ)$, descrito por:

$$\mathcal{G} = \{I, \rho, \phi, \rho\phi\}.$$

O grupo $\mathcal{G}$ possui ordem $|\mathcal{G}| = 4$ e é isormorfo ao grupo de Klein.

Considere o codificador de parâmetros $(2,4,2)$, sobre o reticulado quociente da Tabela 5, onde a operação de adição é mostrada na Tabela 6. A matriz norma do subconjunto especial que contém um código de treliça ótimo, para o sistema considerado é dada pela matriz norma:

$$GN = [\ 3 \quad 1 \quad 1 \quad 1 \quad 1 \quad 3\ ].$$

Tabela 5: Normas e Rótulos

$R = \frac{\Lambda}{P_2\Lambda}$	Rótulo	Norma	Ordem
$(0,0)$	0	0	1
$(1/2, \sqrt{3}/2)$	1	1	8
$(-1,0)$	2	1	4
$(-1/2, \sqrt{3}/2)$	3	1	8
$(0, \sqrt{3})$	4	3	2
$(1/2, -\sqrt{3}/2)$	5	1	8
$(1,0)$	6	1	4
$(-1/2, -\sqrt{3}/2)$	7	1	8

Tabela 6: Tabela de Cayley

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

No subconjunto representado pela GN dada, é encontrada a matriz dos rótulos:

$$GR = [\ 4 \quad 1 \quad 3 \quad 1 \quad 1 \quad 4\ ],$$

obtida com a utilização do algoritmo de busca dos códigos de treliça ótimos.

Aplicando os Operadores Lineares do grupo $\mathcal{G}$, tem-se 4 matrizes geradoras $\mathcal{G}(GR)$ distintas, correspondentes a 4 códigos equivalentes:

$\mathcal{G}(GR) = \{I(GR), \rho(GR), \phi(GR), \rho\phi(GR)\} =$

$\{[\ 4 \quad 1 \quad 3 \quad 1 \quad 1 \quad 4\ ], [\ 4 \quad 5 \quad 7 \quad 5 \quad 5 \quad 4\ ],$

$[\ 4 \quad 3 \quad 7 \quad 3 \quad 3 \quad 4\ ], [\ 4 \quad 6 \quad 5 \quad 6 \quad 6 \quad 7\ ]\},$

nesta ordem.

Analizando as colunas da matriz G, observa-se que existem 4 possibilidades para as colunas 2, 3, 4 e 5, mostrando a existência de 256 possíveis grupos para a GN, geradoras de códigos ótimos. Portanto, tem-se 1024 matrizes geradoras distintas com códigos de treliça equivalentes.

5 Conclusão

Uma classe de equivalência foi obtida, através da aplicação de operadores lineares que apresentam estruturas de grupos, reafirmando a ligação entre Estruturas Algébricas e Teoria de Código. A aplicação das propriedades de grupo ao conjunto de matrizes geradoras de códigos de treliça é uma ferramenta para determinação das matrizes que geram códigos distintos com relação ao espectro de peso. Essa classe de equivalência sendo implementada em um algoritmo de busca de códigos de treliça ótimos, dentre os subconjuntos especiais, diminui consideravelmente a quantidade de matrizes geradoras a serem investigadas pelo algoritmo.

Referências

[1] A. A. Calderbank and N. J. A. Sloane *New Trellis Codes Based on Lattices and Cosets* . IEEE Transf. Inform. Theory, IT-33 : 177 – 195, 1987.

[2] A. Garcia e Y. Lequain *Introdução a Álgebra*. IMPA, Rio de Janeiro, 2004.

[3] E. M. Rosa, W. C. Borelli and P. G. Farrell, *A Formalized Optimum Code Search for q-ary Trellis Codes*. IEEE Global Telecommunications Conference (GLOBECOM 97). vol. 2, pp. 948–952, Phoenix, USA.

[4] E. M. Rosa, *Códigos Treliça Baseados em partições de Reticulados: Propriedades Estruturais e Determinação de Códigos Ótimos*. Tese de Doutorado - UNICAMP, Campinas. 1999.

[5] J. C. Silva Filho, W. C. Borelli e E. M. R. Marques, *Partições de Reticulados Aplicadas aos Códigos de Treliça*. XXX CNMAC, Florianópolis, 2007.

[6] J. C. Silva Filho, W. C. Borelli e E. M. R. Marques, *Códigos Treliça Baseados em Reticulados Quocientes*. VI ERMAC, João Pessoa, 2006.