CONSTELAÇÕES DE SINAIS CASADAS A GRUPOS NÃO-COMUTATIVOS

Antonio de Andrade e Silva* **e Reginaldo Palazzo Jr.**†
Departamento de Matemática - CCEN-UFPb
Departamento de Telemática - FEEC-UNICAMP

Resumo - Neste trabalho consideramos a caracterização de constelações de sinais casadas a grupos não-comutativos, estes como sendo resultantes do produto semidireto de um grupo comutativo por um grupo cíclico de ordem par. Como consequência, propomos um algoritmo para a determinação das constelações de sinais casadas a tais grupos.

Abstract - In this paper we consider signal constellations matched to noncommutative groups. These groups are characterized as the semidirect product of a commutative group by a cyclic group of order even. As a consequence, we propose an algorithm to determine the signal constellations matched to such groups.

Palavras Chaves: Constelações de sinais casadas a grupos não-comutativos, códigos de Slepian, rotulamento isométrico, casamento de sinais a grupos.

1. INTRODUÇÃO

Forney [2] mostrou que a maioria das classes de bons códigos de espaço de sinais são geometricamente uniformes. Uniformidade geométrica, além de ser um tipo forte de simetria, inclui propriedades desejáveis tais como: todas as regiões de Voronoi são congruentes; o espectro de distância é o mesmo independente da palavra-código; as palavras-código possuem a mesma probabilidade de erro; e o grupo gerador é isomorfo a um grupo de permutação transitivo.

Um dos problemas de pesquisa relacionado aos códigos geometricamente uniformes tem a ver com a estrutura de grupo do grupo gerador $G(S)$ pertencente ao grupo de simetrias $\Gamma(S)$, isto é, se $G(S)$ é o grupo gerador de S (conjunto de sinais) e $s_0 \in S$, s_0 um ponto inicial, então S é a órbita de s_0 sob $G(S)$, e o mapeamento $\mu : G(S) \longrightarrow S$ definido por $\mu(g) = g(s_0)$, é um-a-um, onde $g \in G(S)$ e $g(s_0)$ denota a ação de g no ponto inicial s_0. Este mapeamento induz uma estrutura de grupo em S que é isomorfa ao grupo gerador $G(S)$.

Desse modo, o procedimento de determinação do mapeamento $\mu(.)$ resulta no procedimento de casamento de sinais a grupos. Consequentemente, é uma maneira alternativa de se determinar códigos geometricamente uniformes.

O objetivo deste trabalho é estender o resultado de Loeliger [3], o casamento de conjunto de sinais a grupos abelianos cíclicos, no sentido de se estabelecer as condições em que um conjunto de sinais está casado a um grupo não-comutativo.

Este trabalho está organizado da seguinte maneira. Na Seção 2, estabelecemos os conceitos necessários para o entendimento das seções que se seguem. Na Seção 3, caracterizamos as constelações de sinais que são casadas a um grupo não-comutativo resultante do produto semidireto de um grupo comutativo por um grupo cíclico de ordem par. Na Seção 4, são apresentados resultados relativos aos conceitos de d-caminho e de d-cadeia. Na Seção 5, apresentamos um algoritmo para a obtenção de constelações de sinais casadas a grupos, grupos estes formados pela extensão de dois outros grupos. Finalmente, na Seção 6, apresentamos as conclusões.

2. PRELIMINARES

Uma *constelação de sinais* S é qualquer subconjunto discreto do $\mathbb{R}^N$. Os elementos de uma constelação de sinais S são chamados *pontos de sinais*. Um *código do espaço euclidiano* é um subconjunto de $S^{\mathbb{I}}$, onde $\mathbb{I} \subseteq \mathbb{Z}$, e $S^{\mathbb{I}}$ denota o produto cartesiano de S, $\mathbb{I}$ vezes.

Uma *isometria* φ é uma aplicação que preserva distância, isto é, $d(\varphi(s_i), \varphi(s_j) = d(s_i, s_j)$.

Uma constelação de sinais S é *geometricamente uniforme* [2] se dados $\mathbf{s}_1, \mathbf{s}_2 \in S$ existe uma isometria φ, $\varphi \in Isom(\mathbb{R}^N)$, o conjunto de isometrias, tal que

$$\varphi(\mathbf{s}_1) = \mathbf{s}_2 \text{ e } \varphi(S) = S.$$

Se $\Gamma(S) = \{\varphi \in Isom(\mathbb{R}^N) : \varphi(S) = S\}$, o conjunto de simetrias de S, isto é, o conjunto de todas as isometrias que deixam S invariante, então S é a órbita de qualquer ponto $\mathbf{s}_0 \in S$ sob $\Gamma(S)$, isto é,

$$S = \{\varphi(\mathbf{s}_0) : \varphi \in \Gamma(S)\} = \bigcup_{\varphi \in \Gamma(S)} \{\varphi(\mathbf{s}_0)\}.$$

Note que $\Gamma(S)$ sob a operação de composição forma um grupo. Em geral, o grupo de simetrias $\Gamma(S)$ de uma constelação de sinais geometricamente uniforme é mais do que o necessário para gerar S. Assim, um *grupo gerador* $G(S)$ de S é um subgrupo de $\Gamma(S)$ que é minimamente suficiente para gerar S a partir de qualquer ponto $\mathbf{s}_0 \in S$ ou, equivalentemente, o conjunto $\{\mathbf{s} \in S : \varphi(\mathbf{s}) = \mathbf{s}\}$ tem cardinalidade nula, $\forall \varphi \in G(S)$, $\varphi \neq I_S$, onde I_S é o elemento identidade de $\Gamma(S)$. Note que o grupo gerador $G(S)$ de uma constelação de sinais geometricamente uniforme pode não existir [2]. Se

*O autor está no Departamento de Matemática, CCEN-UFPb, 58.059-900, J. Pessoa, Pb.

†O autor está no Departamento de Telemática, FEEC-UNICAMP, CP 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 tem recebido apoio financeiro do Conselho Nacional de Desenvolvimento Científico e Tecnológico, CNPq, No. 301416/85-0. email:palazzo@dt.fee.unicamp.br

$G(S)$ é o grupo gerador de uma constelação de sinais geometricamente uniforme S e $s_0 \in S$, então

$$S = \bigcup_{\varphi \in G(S)} \{\varphi(s_0)\},$$

e o mapeamento $\mu : G(S) \longrightarrow S$ definido por $\mu(\varphi) = \varphi(s_0)$ é bijetivo. O mapeamento μ induz uma estrutura de grupo em S, isto é, dados $s_1, s_2 \in S$, a operação $s_1 * s_2 = \mu(\mu^{-1}(s_1)\mu^{-1}(s_2))$ define uma estrutura de grupo em S e, neste caso, $(S, *)$ é isomorfo a $G(S)$. Assim, se o grupo S não é simples, então cada subgrupo normal S' de S induz em S uma fatoração de S' por S/S'. Isto sugere o estudo de uma constelação de sinais S através de constelações de sinais S' e S/S' cada com cardinalidade menor do que a cardinalidade de S. Este fato será apresentado na Seção 3.

Um *código de bloco cujas palavras-código possuem a mesma energia* ou um *código esférico* S, é qualquer constelação finita de sinais sobre uma esfera que gera $\mathbb{R}^N$ como um espaço vetorial, [7]. Em particular, quando um código esférico S é geometricamente uniforme dizemos que S é uma *constelação uniforme*. Constelações uniformes foram introduzidas por Slepian, [7], sob o nome de *códigos de grupo para o canal gaussiano* e generalizadas por Forney para qualquer constelação de sinais, [2].

Seja H um subgrupo normal de $G(S)$. Então,

$$S_g = \bigcup_{\phi \in \varphi_g H} \{\phi(s_0)\} = \bigcup_{\varphi \in H} \{\varphi_g(\varphi(s_0))\},\ \varphi_g \in G(S)$$

é a órbita de s_0 sob a classe lateral $\varphi_g H$. Assim,

$$S = \bigcup S_g.$$

Se S' é a órbita de s_0 sob H, então a partição S/S' de S induzida por H é chamada uma *partição geometricamente uniforme*.

Um *grupo de rótulos* G para uma partição geometricamente uniforme S/S' é um grupo isomorfo ao grupo quociente $G(S)/G(S')$. Um *rotulamento isométrico* [2] da partição geometricamente uniforme S/S' é um mapeamento $\mu : G \longrightarrow S/S'$ definido por

$$\mu(g) = \varphi_g(S').$$

Em [3] Loeliger generaliza, para um grupo finito, a idéia de rotulamento isométrico, definindo um mapeamento casado de um grupo sobre uma constelação de sinais e mostra que toda constelação de sinais casada a um grupo é, a menos de translação, uma constelação uniforme, [3, Corolário 1], e caracteriza todas as constelações de sinais casadas a um grupo comutativo cíclico, [3, Teorema 10]. Este resultado é generalizado por Palazzo *et al.* [4] através de um algoritmo heurístico. Em todos estes casos, a motivação foi a introdução de alguma "*linearidade*" no estudo de códigos do espaço euclidiano via um grupo.

3. CONSTELAÇÕES DE SINAIS CASADAS A GRUPOS

Nesta seção iremos caracterizar as constelações de sinais que são casadas a um grupo não comutativo que é fatorável como o produto semi-direto de um grupo comutativo por um grupo cíclico de ordem par.

Uma constelação de sinais S é *casada* a um grupo G, [3], se existe um mapeamento sobrejetivo μ de G em S tal que

$$d(\mu(g), \mu(h)) = d(\mu(e), \mu(g^{-1}h)),$$

para todo $g, h \in G$, onde $d(.,.)$ é a distância euclidiana quadrática e e é a identidade de G. O mapeamento μ é chamado de *mapeamento casado*. Quando o mapeamento μ é injetivo dizemos que μ^{-1} é um *rotulamento casado*, isto é, se G é isomorfo a $G(S)$ então μ^{-1} é um rotulamento isométrico. Salvo menção explicita em contrário, todos os mapeamentos casados deste trabalho são rotulamentos casados. Neste caso, se C é um código linear de comprimento n sobre G, isto é, C é um subgrupo de G^n, então $\mu(C)$ é um código do espaço euclidiano sobre S. Assim, as regiões de decisões de $\mu(C)$ são todas congruentes.

Sejam H e K dois grupos, com H um subgrupo normal em $H \times_\theta K$, e seja $\theta : K \longrightarrow Aut(H)$ um homomorfismo de grupo. Então o *produto semidireto* de H por K via θ é o conjunto $H \times_\theta K = \{(h,k) : h \in H,\ k \in K\}$ junto com a operação binária

$$\begin{aligned} (h_1, k_1)(h_2, k_2) &= (\theta(k_1)h_2, k_1k_2), \\ \forall\ h_1, h_2 &\in H \text{ e } k_1, k_2 \in K. \end{aligned}$$

O próximo teorema caracteriza as constelações de sinais que são casadas a um grupo não-comutativo.

Teorema 1 *Sejam H e K grupos isomorfos a $\mathbb{Z}_n$ e $\mathbb{Z}_{2m}$, respectivamente, e denotados por $H = \langle h \rangle \simeq \mathbb{Z}_n$ e $K = \langle k \rangle \simeq \mathbb{Z}_{2m}$, onde $\langle x \rangle$ denota o gerador do grupo X. Então, uma constelação de sinais S é casada a um grupo $G = H \times_\theta K$ se, e somente se, $S = S_1 \times_\varphi S_2$, para $\varphi(\mu_2(k)) = \mu_1\theta(k)\mu_1^{-1}$, onde $\mu_1 : H \longrightarrow S_1$, e $\mu_2 : K \longrightarrow S_2$ são rotulamentos casados, $\theta(k) \in Aut(H), \forall\ k \in K$ e $\theta(k)(h) = h^{-1}, \forall\ h \in H$.*

Prova: Suponha que S seja uma constelação de sinais casada a G. Seja μ o rotulamento casado de G sobre S. Então μ induz uma estrutura de grupo em S. Definindo

$$S_1 \triangleq \mu(H \times_\theta \{e\}) \text{ e } S_2 \triangleq \mu(\{e\} \times_\theta K)$$

temos que S_1 e S_2 são subgrupos de S, tal que S_1 é normal em S. Agora, defina $\mu_1 : H \longrightarrow S_1$ e $\mu_2 : K \longrightarrow S_2$ por

$$\mu_1(h) \triangleq \mu(h, e) \text{ e } \mu_2(k) \triangleq \mu(e, k).$$

Então é claro que μ_1, μ_2 são isomorfismos e $S = S_1 \times_\varphi S_2$, onde $\varphi(\mu_2(k)) = \mu_1\theta(k)\mu_1^{-1}, \forall\ k \in K$. Além disso, dados $h_1, h_2 \in H$,

$$d(\mu_1(h_1), \mu_1(h_2)) = d(\mu_1(e), \mu_1(h_1^{-1}h_2)).$$

De modo análogo, podemos mostrar que μ_2 é um rotulamento casado.

Reciprocamente, sejam $\mu_1 : H \longrightarrow S_1$ e $\mu_2 : K \longrightarrow S_2$ rotulamentos casados. Então é claro que μ_1 e μ_2 induzem estruturas de grupos em S_1 e S_2, respectivamente. Assim, $S = S_1 \times_\varphi S_2$ é um grupo, onde $\varphi(s_2) \in Aut(S_1), \forall\ s_2 \in S_2$,

com $\varphi(s_2)(s_1) = s_1^{-1}, \forall\ s_1 \in S_1$. Uma vez que $\mu_1^{-1}\tau\mu_1 \in Aut(H)$, para todo $\tau \in Aut(S_1)$ segue que $G = H \times_\theta K$ é um grupo com $\theta(k) = \mu_1^{-1}\varphi(\mu_2(k))\mu_1, \forall\ k \in K$. Defina $\mu : G \longrightarrow S$ como

$$\mu(h,k) \triangleq (\mu_1(h), \mu_2(k)).$$

Então é fácil verificar que μ é um isomorfismo de G sobre S. Além disso, dados $(h_1,k_1),(h_2,k_2) \in G$, temos que

$$\begin{aligned} &d(\mu(h_1,k_1),\mu(h_2,k_2)) = \\ &d((\mu_1(h_1),\mu_2(k_1)),(\mu_1(h_2),\mu_2(k_2))) = \\ &d(\mu_1(h_1),\mu_1(h_2)) + d(\mu_2(k_1),\mu_2(k_2)) = \\ &d(\mu_1(e),\mu_1(h_1^{-1}h_2)) + d(\mu_2(e),\mu_2(k_1^{-1}k_2)), \end{aligned}$$

por outro lado,

$$\begin{aligned} &d(\mu(e,e),\mu((h_1,k_1)^{-1}(h_2,k_2)) = \\ &d((\mu_1(e),\mu_2(e)),(\mu_1(h_1),\mu_2(k_1))^{-1}(\mu_1(h_2),\mu_2(k_2))) = \\ &d((\mu_1(e),\mu_2(e)),(\varphi(\mu_2(k_1^{-1}))\mu_1(h_1^{-1}h_2),\mu_2(k_1^{-1}k_2))) = \\ &d((\mu_1(e),\mu_2(e)),(\mu_1(\theta(k_1^{-1}))(h_1^{-1}h_2),\mu_2(k_1^{-1}k_2))) = \\ &d(\mu_1(e),\mu_1(h_1h_2^{-1})) + d(\mu_2(e),\mu_2(k_1^{-1}k_2)). \end{aligned}$$

Das expressões acima vemos que

$$d(\mu(h_1,k_1),\mu(h_2,k_2)) = d(\mu(e,e),\mu((h_1,k_1)^{-1}(h_2,k_2))),$$

pois $d(\mu_1(e),\mu_1(h_1^{-1}h_2)) = d(\mu_1(e),\mu_1(h_1h_2^{-1}))$. Portanto, μ é um rotulamento casado. ■

Corolário 2 *Sejam H um grupo comutativo e $K = \langle k \rangle \simeq \mathbb{Z}_{2m}$. Então, uma constelação de sinais S é casada a um grupo $G = H \times_\theta K$ se, e somente se, $S = S_1 \times_\varphi S_2$, para $\varphi(\mu_2(k)) = \mu_1\theta(k)\mu_1^{-1}$, onde $\mu_1 : H \longrightarrow S_1$, e $\mu_2 : K \longrightarrow S_2$ são rotulamentos casados, $\theta(k) \in Aut(H), \forall\ k \in K$ e $\theta(k)(h) = h^{-1}, \forall\ h \in H$.* ■

Note que, quando $\theta(k) = I,\ \forall\ k \in K$, com I o elemento identidade do grupo $Aut(H)$, o produto semidireto $H \times_\theta K$ reduz-se ao produto direto. Portanto, o Teorema 1 pode ser usado para caracterizar constelações de sinais casadas a grupos comutativos.

Exemplo 3 *Sejam $H = \mathbb{Z}_3 = \{0,1,2\}$, $K = \mathbb{Z}_2 = \{0,1\}$ e o homomorfismo $\theta : K \longrightarrow Aut(H)$ definido por $\theta(k) = \tau^k$, $k = 0,1$, onde $\tau(h) = -h,: h = 0,1,2$. Então $G = H \times_\theta K$ é um grupo não comutativo de ordem 6 com a operação*

$$\begin{aligned} &(h,k) +_\theta (h',k') = (h +_3 \theta(k)(h'), k +_2 k'), \\ &\forall h,h' \in H \text{ e } k,k' \in K, \end{aligned}$$

onde $+_3$ e $+_2$ denotam soma mod 3 e soma mod 2, respectivamente. Assim, G é isomorfo ao grupo diedral D_3. Seja $A = \{0,1,2,3,4,5\}$ um conjunto de rótulos para G. A tabela de Cayley de A é mostrada na Tabela 1. Portanto, pelo Teorema 1, a constelação de sinais

$$\begin{aligned} S = \Big\{ &(1,0,1),(-\frac{1}{2},\frac{\sqrt{3}}{2},1),(-\frac{1}{2},-\frac{\sqrt{3}}{2},1),(1,0,-1), \\ &(-\frac{1}{2},\frac{\sqrt{3}}{2},-1),(-\frac{1}{2},-\frac{\sqrt{3}}{2},-1)\Big\} \end{aligned}$$

$+_\theta$	0	1	2	3	4	5	G
0	0	1	2	3	4	5	(0,0)
1	1	2	0	4	5	3	(1,0)
2	2	0	1	5	3	4	(2,0)
3	3	5	4	0	2	1	(0,1)
4	4	3	5	1	0	2	(1,1)
5	5	4	3	2	1	0	(2,1)

Tabela 1. Tabela Cayley do grupo $\mathbb{Z}_3 \times_\theta \mathbb{Z}_2 \simeq D_3$.

$+_\theta$	0	1	2	3	4	5	6	7	G
0	0	1	2	3	4	5	6	7	(0,0)
1	1	2	3	0	5	6	7	4	(1,0)
2	2	3	0	1	6	7	4	5	(2,0)
3	3	0	1	2	7	4	5	6	(3,0)
4	4	7	6	5	0	3	2	1	(0,1)
5	5	4	7	6	1	0	3	2	(1,1)
6	6	5	4	7	2	1	0	3	(2,1)
7	7	6	5	4	3	2	1	0	(3,1)

Tabela 2. Tabela Cayley do grupo $\mathbb{Z}_4 \times_\theta \mathbb{Z}_2 \simeq D_4$.

ou a constelação de sinais normalizada $\tilde{S} = \frac{1}{\sqrt{2}}S$ é casada ao grupo D_3. O conjunto S formado pelas 6 triplas (a,b,c) foi obtido através do algoritmo apresentado na Seção 5. ■

Exemplo 4 *Sejam $H = \mathbb{Z}_4 = \{0,1,2,3\}$, $K = \mathbb{Z}_2 = \{0,1\}$ e o homomorfismo $\theta : K \longrightarrow Aut(H)$ definido por $\theta(k) = \tau^k, k = 0,1$, onde $\tau(h) = -h,\ h = 0,1,2,3$. Então $G = H \times_\theta K$ é um grupo não comutativo de ordem 8 com a operação*

$$\begin{aligned} &(h,k) +_\theta (h',k') = (h +_4 \theta(k)(h'), k +_2 k'), \\ &\forall h,h' \in H \text{ e } k,k' \in K. \end{aligned}$$

onde $+_4$ e $+_2$ denotam soma mod 4 e soma mod 2, respectivamente. Seja $A = \{0,1,2,3,4,5,6,7\}$ um conjunto de rótulos para G. A tabela de Cayley de A é mostrada na Tabela 2, da qual podemos concluir que $G = \langle 1,4 \rangle$, onde 1 e 4 denotam os geradores de G, é isomorfo ao grupo diedral D_4. Portanto, pelo Teorema 1, a constelação de sinais

$$\begin{aligned} S = \{&(1,0,1),(0,1,1),(-1,0,1),(0,-1,1), \\ &(1,0,-1),(0,1,-1),(-1,0,-1),(0,-1,-1)\} \end{aligned}$$

ou a constelação de sinais normalizada $\tilde{S} = \frac{1}{\sqrt{2}}S$ é casada ao grupo D_4. O conjunto S formado pelas 8 triplas (a,b,c) foi obtido através do algoritmo apresentado na Seção 5. ■

4. D-CAMINHO

Nesta seção apresentamos uma construção de constelações de sinais a partir de um grupo qualquer via o conceito de d-caminho em uma d-cadeia baseado na construção proposta em [4].

Seja $S = \{\mathbf{x}_{g_i} : 0 \leq i \leq N-1\} \subset \mathbb{R}^N$, onde $\mathbf{x}_{g_i} = (x_{\sigma_{g_i}(0)}, \cdots, x_{\sigma_{g_i}(N-1)}) \in \mathbb{R}^N$, com $g_i \in G, g_0 = e$ e σ_{g_i}, denota a permutação associada a g_i, $0 \leq i \leq N-1$. Suponha que todos os vetores distantes d de $\mathbf{x}_{g_0}$ são $\mathbf{x}_{g_1}, \ldots, \mathbf{x}_{g_\tau}$. Vamos construir uma tabela dos elementos do grupo associados

com os vetores $\mathbf{x}_{g_i}, 0 \leq i \leq r$, da seguinte forma: a primeira linha da tabela será $g_0, \ldots, g_r$. O primeiro elemento a ser localizado na primeira coluna da tabela na $(k+1)$-ésima linha será o primeiro elemento na k-ésima linha que ainda não apareceu na primeira coluna da tabela. Seja g o primeiro elemento na k-ésima linha que ainda não apareceu na primeira coluna da tabela. Então a $(k+1)$-ésima linha será $g, gg_1, \ldots, gg_r$. Portanto, temos a seguinte tabela:

	g_0	g_1	$\cdots$	g_r
g_0	g_0	g_1	$\cdots$	g_r
g_1	g_1	g_1^2	$\cdots$	$g_1 g_r$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
g	g	gg_1	$\cdots$	gg_r
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$

Quando a j-ésima linha tiver sido escrita e todo elemento nessa j-ésima linha tenha aparecido uma vez na primeira coluna da tabela, o processo é interrompido e a tabela é considerada completa. Note que a tabela tem no máximo $|G|$ linhas. Agora, de $d(\mathbf{x}_{g_i}, \mathbf{x}_{g_0})$ temos que $d(\mathbf{x}_{g_i}, \mathbf{x}_{g_0}) = d(\mathbf{x}_{g_j g_i}, \mathbf{x}_{g_j})$, $0 \leq i, j \leq N-1$, segue-se que os vetores representados pelos elementos do grupo na $2^{\underline{a}}, \ldots, r$-ésima coluna na k-ésima linha estão distantes d do vetor representado pelo elemento do grupo na primeira coluna dessa linha. Assim, os elementos do grupo na primeira coluna da tabela representam vetores com a propriedade de que todo vetor na correspondente linha está à distância d dele. O conjunto de vetores que podem ser alcançados de $\mathbf{x}_{g_0}$ dessa maneira é chamado de *d-cadeia* iniciando em $\mathbf{x}_{g_0}$, [7]. Agora, se a distância entre os elementos do grupo na primeira coluna também estão à distância d na sequência apresentada, então tem-se um *d-caminho* nesta d-cadeia. Note que o vetor $\mathbf{x}_{g_0}$ está incluído nesse d-caminho e todos os d-caminhos iniciando de $\mathbf{x}_{g_0}$ são obtidos da tabela. Com isso, provamos o seguinte teorema.

Teorema 5 *Seja $\mathbf{x}_{g_0}, \mathbf{x}_{g_1}, \ldots, \mathbf{x}_{g_k}$ um d-caminho em uma d-cadeia iniciando de $\mathbf{x}_{g_0}$. Então*

(1) *$H = \{g_0, g_1, \ldots, g_k\}$ é um subgrupo de G gerado pelos elementos da primeira linha da tabela.*

(2) *Se $H \neq G$, então para todo $g \in G - H$ existe um novo d-caminho iniciando em $\mathbf{x}_g$ e os elementos do grupo desse novo d-caminho formam as classes laterais à esquerda gH de H em G.* ■

Sejam S uma constelação de sinais e $P(S) = \{S' : S' \subset S,\ S' \neq \emptyset\}$ uma partição de S. Note que cada S' pertencente à partição $P(S)$ resulta de uma classe lateral à esquerda de H, isto é, gH em G. Assim, dizemos que S está *casada* a G se existe um mapeamento μ de G sobre $P(S)$ tal que

$$d(\mu(g), \mu(h)) = d(\mu(e), \mu(g^{-1}h)),$$

para todos $g, h \in G$, tal que gH e hH são classes laterais à esquerda de H em G, onde $d(.,.)$ é a distância euclidiana quadrática interclasses laterais.

Teorema 6 *Seja G um grupo e seja H um subgrupo de G como no Teorema 5. Se $S = \bigcup_{g \in G} S_g$, onde S_g são constelações de sinais associadas às classes laterais de H em G, então S está casada a G.*

Prova. Por construção cada S_g tem a mesma distância euclidiana quadrática intraclasses laterais e, assim, cada S_g tem a mesma lista ordenada de distâncias euclidianas interclasses laterais, pois todas as constelações S_g são formadas de d-caminhos fechados. Portanto, $\mu : G \longrightarrow P(S)$, dado por $\mu(g) = S_g$, é um mapeamento casado. ■

Pelo Teorema 6, observamos que a constelação de sinais S casada a G têm a seguinte propriedade: o perfil de distância de qualquer ponto de sinal independe do ponto de sinal a ser considerado. Portanto, G tem uma medida de distância invariante por translação. Assim, um código linear C projetado sobre este grupo é invariante por translação (independe da palavra-código), e mais, para um canal gaussiano a probabilidade de erro condicional independe da palavra-código.

O próximo resultado considera a forma geral de decomposição de um grupo G como o produto de dois grupos sendo que um deles, digamos H, é um subgrupo normal em G. Com isso, se G/H é isomorfo a um grupo K, então G é isomorfo a $H * K$ denotado por $G \simeq H * K$, segundo uma operação apropriada $*$. Portanto, diz-se que G é uma extensão de H por K, [1].

Lema 7 *Seja G um grupo que é uma extensão de H por K. Então,*

(1) *Se S é uma constelação de sinais casada a H, então S é casada a G.*

(2) *Se S é uma constelação de sinais casada a K, então S é casada a G.*

Prova. (1) Caso particular do Teorema 3.1.

(2) Seja $\mu : G \longrightarrow S$ definida por $\mu(g) = \mu(aH)$, se $g \in aH$, para todo $g \in G$, onde μ é o rotulamento casado de $K \simeq G/H$ sobre S. É claro que μ está bem definida e é sobrejetiva. Dados $g_1, g_2 \in G$, existem únicos $a_1, a_2 \in [G/H]$ e $h_1, h_2 \in H$ tais que $g_1 = a_1 h_1$ e $g_2 = a_2 h_2$. Como $g_1^{-1} g_2 = h_1^{-1} a_1^{-1} a_2 h_2$ e

$$h_1^{-1} a_1^{-1} a_2 h_2 = a_1^{-1}(a_1 h_1^{-1} a_1^{-1}) a_2 h_2 = a_1^{-1} h_3 a_2 h_2,\ h_3 = a_1 h_1^{-1} a_1^{-1} \in H,$$
$$h_3 a_2 h_2 = a_2(a_2^{-1} h_3 a_2 h_2) = a_2 h_4,\ h_4 = a_2^{-1} h_3 a_2 h_2 \in H$$

temos que $g_1^{-1} g_2 = a_1^{-1} a_2 h_4$, isto é, $g_1^{-1} g_2 \in a_1^{-1} a_2 H$. Portanto,

$$d(\mu(g_1), \mu(g_2)) = d(\mu(a_1 H), \mu(a_2 H)) =$$
$$d(\mu(H), \mu(a_1^{-1} a_2 H)) = d(\mu(e), \mu(g_1^{-1} g_2)).$$

Logo, μ é um mapeamento casado. ■

Note que para o mapeamento casado do Lema 7, μ^{-1}, não é um rotulamento casado, pois μ não é injetivo.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	0	4	5	3
2	2	0	1	5	3	4
3	3	5	4	0	2	1
4	4	3	5	1	0	2
5	5	4	3	2	1	0

Tabela 3. Tabela de Cayley do grupo $\mathbb{D}_3$.

5. ALGORITMO DE CONSTRUÇÃO DE CONSTELAÇÕES DE SINAIS CASADAS A GRUPOS

Em geral, o Teorema 6 não fornece a natureza geométrica da constelação de sinais. De fato, este teorema estabelece que uma constelação de sinais deve ser encontrada como uma união de constelações de sinais. Assim, a chave para transformar o Teorema 6 em um algoritmo construtivo é proporcionado pelo conceito de d-caminho em uma d-cadeia, do Teorema 5 e do Lema 7.

O algoritmo, apresentado a seguir, permite construir de maneira sistemática as figuras geométricas associadas a grupos gerais.

Algoritmo A

Dado um grupo finito G

Passo 1 - Associe a G um conjunto qualquer de rótulos A;

Passo 2 - Construa a tabela de Cayley para A;

Passo 3 - Para cada linha da tabela de Cayley do Passo 2 associe uma permutação σ_i, $i \in A$.

Passo 4 - Selecione subconjuntos de A cujos elementos do grupo associados aos vetores $\mathbf{x}_j$ estão à mesma distância euclidiana quadrática d_j de $\mathbf{x}_0$;

Passo 5 - Para cada subconjunto A_j de A do Passo 4 associe um d_j-caminho;

Passo 6 - Associe a cada d_j-caminho do Passo 5 um subgrupo H_j de G;

Passo 7 - Faça $S_j = \bigcup_{i \in \mathbb{I}} S_{ji}$, onde S_{ji} são as constelações de sinais casadas com as classes laterais de H_j em G.

Este algoritmo pode ser facilmente implementado, possibilitando a determinação de figuras geométricas associadas a grupos mais gerais do que aqueles apresentados nos exemplos a seguir.

Exemplo 8 *Encontre as constelações de sinais casadas ao grupo diedral D_3.*

Passo 1– *Seja $A = \{0,1,2,3,4,5\}$ um conjunto de rótulos para D_3.*

Passo 2– *Ver Tabela* 3.

Passo 3– *Sejam*

$$\sigma_0 = (0),\ \sigma_1 = (012)(345),\ \sigma_2 = (021)(354),$$
$$\sigma_3 = (03)(15)(24),\ \sigma_4 = (04)(13)(25)$$
$$e\ \sigma_5 = (05)(14)(23)$$

as permutações associadas ao Passo 2.

	0	1	2	5
0	0	1	2	5
1	1	2	0	3
2	2	0	1	4
4	4	3	5	2
3	3	5	4	1
5	5	4	3	0

Tabela 4. Constelação de sinais S_1, prisma.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	0	4	5
2	2	0	1	5	3
3	3	5	4	0	2
5	5	4	3	2	1
4	4	3	5	1	0

Tabela 5. Constelação de sinais S_2, antiprisma.

Passo 4– *Sejam $A_1 = \{0,1,2\}$,: $A_2 = \{0,3,4\}$ e $A_3 = \{0,5\}$ os conjuntos com distâncias euclidianas quadráticas $d_1 = 12$, $d_2 = 58$ e $d_3 = 70$, respectivamente.*

Passo 5–

	0	*1*	*2*
0	*0*	*1*	*2*
1	*1*	*2*	*0*
2	*2*	*0*	*1*

	0	*3*
0	*0*	*3*
3	*3*	*0*

	0	*4*
0	*0*	*4*
4	*4*	*0*

	0	*3*	*4*
0	*0*	*3*	*4*
3	*3*	*0*	*2*
2	*2*	*5*	*3*
5	*5*	*2*	*1*
1	*1*	*4*	*5*
4	*4*	*1*	*0*

	0	*5*
0	*0*	*5*
5	*5*	*0*

Passo 6– *Sejam $H_1 = \{0,1,2\}$, $H_2 = \{0,3\}$, $H_3 = \{0,4\}$ e $H_4 = \{0,5\}$ os subgrupos de D_3 associados aos d_j-caminhos $j = 1,2,3,4$ do Passo* 5.

Passo 7– *Sejam $S_1 = S_{11} \cup S_{13}$, onde $S_{11} = \{0,1,2\}$ e $S_{13} = \{0,5\}$, $S_2 = S_{21} \cup S_{22}$, onde $S_{21} = \{0,1,2\}$ e $S_{22} = \{0,3,4\}$, onde os d-caminhos associados são mostrados nas primeiras colunas nas Tabelas 4 e 5.*

Os gráficos associados a S_2 e S_1 são o antiprisma da Figura 1 *e o prisma da Figura* 2, *respectivamente. Note das Tabelas 4 e 5 que os vizinhos de 3 são 4,5 e 1, no caso do conjunto de sinais S_1, e 5,4,0, e 2, no caso do conjunto de sinais S_2, respectivamente.Pelo Lema* 7 *as constelações de sinais $2PSK$ e $3PSK$ são também casadas com o grupo D_3.*

6. CONCLUSÕES

Neste trabalho consideramos o problema de casamento de uma constelação de sinais a um grupo, o qual é o produto semidireto de um grupo comutativo por um grupo cíclico de

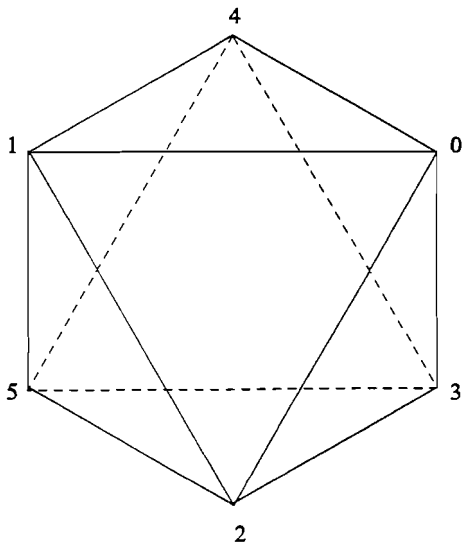

Figura 1. Antiprisma casado com D_3.

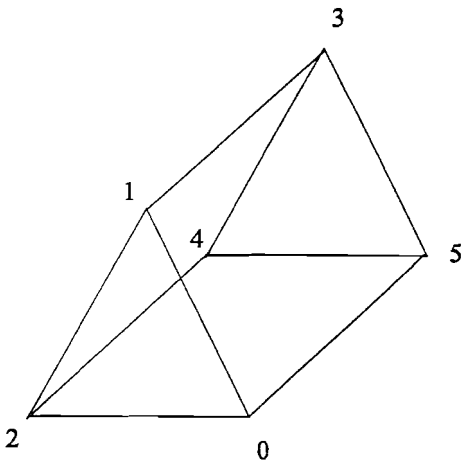

Figura 2. Prisma casado com D_3.

ordem par. Os resultados de Loeliger foram estendidos e as condições para as quais o casamento de sinais a grupos não abelianos possa ser efetivado foram estabelecidas. Um algoritmo para encontrar as correspondentes constelações de sinais casadas a tais grupos foi proposto. A extensão do Teorema 1 para um grupo mais geral pode ser considerada como uma proposta de pesquisa.

REFERÊNCIAS

[1] D. S. Dummit and R.M. Foote, *Abstract Algebra*, New Jersey, Prentice Hall, 1991.

[2] G. D. Forney Jr, "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. IT-37, pp 1241-1260, Sept. 1991.

[3] H. A. Loeliger, "Signal sets matched to groups," *IEEE Trans. Inform. Theory*, vol. IT-37, pp 1675-1682, Nov. 1991.

[4] R. Palazzo Jr, J. C. Interlando e C. Almeida, "Constructions of signals sets matched to abelian and non-abelian groups," *Proc. IEEE Internat. Symp. on Inform. Theory*, ISIT-94, Trondhein, Norway, 1994.

[5] A.A. e Silva e R. Palazzo, Jr., "Construção de reticulados via fórmula de códigos p-ários generalizado," *13 Simpósio Brasileiro de Telecomunicações*, Águas de Lindóia, São Paulo, pp. 66-70, 1995.

[6] A.A. e Silva, *Uma contribuição à classe dos códigos geometricamente uniformes*, Tese de Doutorado, FEEC-UNICAMP, 1996.

[7] D. Slepian, "Groups codes for the gaussian channel," *Bell Syst. Tech. J.*, vol 47, pp 576-602, 1968.

Antonio de Andrade e Silva é Professor no Departamento de Matemática da Universidade Federal da Paraíba, João Pessoa. Suas áreas de interesse são Teoria da Codificação e Álgebra.

Reginaldo Palazzo Jr. graduou-se em Engenharia Elétrica e obteve o título de Mestre em Engenharia Elétrica ambos pela Faculdade de Engenharia Elétrica da UNICAMP, em 1975 e 1977, respectivamente. Em seguida obteve o graus de Engineer e de Ph.D. pela University of California, Los Angeles, CA, USA, em 1981 and 1984, respectivamente. Desde maio de 1985 pertence ao quadro de docentes da Faculdade de Engenharia Elétrica e de Computação, FEEC-UNICAMP, onde obteve a Livre-Docência em 1987. Desde 1996 é Professor Titular e Coordenador do Grupo de Codificação Algébrica e Geométrica na FEEC. Suas áreas de pesquisa são teoria da codificação, da informação, de comunicações e criptografia.