Matching Euclidean Signal Sets to Extensions of Cyclic Groups and Quotient Groups

Jorge Pedraza Arpasi and Bartolomeu F. Uchôa-Filho

***Resumo*— Apresentamos uma técnica para construção de extensões de grupos cícilicos. Então, fazendo uso destas extensões, encontramos novos exemplos de mapeamentos casados entre grupos e conjuntos de sinais. Como contribuição final, propomos uma nova técnica de casamento que é baseada na decomposição de um grupo em um produto Cartesiano de grupos quociente menores, cada um casado a um conjunto de sinais pequeno.**

***Palavras-Chave*— Códigos para o espaço Euclidiano, códigos de grupo, conjuntos de sinais casados a grupos.**

***Abstract*— We present a technique to construct extensions of cyclic groups. Then, by using the parameters of these extensions, we find new examples of matched mappings between groups and signal sets. As a final contribution, we propose a new technique of matching that is based on the decomposition of a group in a Cartesian product of quotient and small groups, each of them matched to a small signal set.**

***Keywords*— Euclidean space codes, group codes, signal sets matched to groups.**

I. INTRODUCTION

Matching signal sets to abstract groups is a coding technique that has received a great deal of attention since the pioneering work of Ungerboeck [1], wherein the outputs of binary convolutional encoders with encoding rate $r/(r+1)$ were matched to $(r+1)$-ary PSK or QAM signal sets by a method called *mapping by set partitioning*. He noticed that the outputs of a (n,k,m) binary convolutional encoder, i.e., with encoding rate k/n and memory m can be viewed as a group $\mathbb{Z}_2^n$, where $\mathbb{Z}_2=\{0,1\}$ is the binary group with the modulo-2 addition operation and $\mathbb{Z}_2^n=\{(x_1,x_2,\ldots,x_n): x_i\in\mathbb{Z}_2, i=1,2,\ldots,n\}$, for $n\geq 2$, is the direct product group with the modulo-2 addition operation induced componentwise.

Ungerboeck's technique, also known as Trellis Coded Modulation (TCM), is very important for bandlimited channels. Theoretically, any constellation of signal sets S has its group of symmetries $\Gamma(S)$, which is a group of isometrical mappings leaving S invariant, that is, $\gamma(S)=S$, for all $\gamma\in\Gamma(S)$ [2], [3], [4], [5]. Any constellation S can be naturally matched to $\Gamma(S)$, and this would give a good generalization of TCM. But the problem is that for the majority of constellations S there are no practical methods to find their groups of symmetries $\Gamma(S)$. Thus, for a given signal set S, a generalized definition of matching, which is not restricted to $\Gamma(S)$, is given by Loeliger in [4].

J. P. Arpasi is with the Departamento de Engenharias e Ciência da Computação, Universidade Regional Integrada Frederico Westphalen - URI/FW, Rio Grande do Sul, Brazil. Email: arpasi@fw.uri.br

B. F. Uchôa-Filho is with GPqCom/EEL/CTC/UFSC, Florianopolis, SC, Brazil. Email: uchoa@eel.ufsc.br

Definition 1: Let S be a set of points (signals) of an Euclidean space with a metric d. Let G be a group with a unit element e. It is said that S is matched to G if there exists a mapping $\mu: G\rightarrow S$ such that

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

for all $g,h\in G$.

For the case of the finite dimensional Euclidean space $\mathbb{R}^n$, $n\in\mathbb{N}$, where $\mathbb{R}$ is the set of real numbers and $\mathbb{N}$ the set of natural numbers, d is usually the canonical metric $d(x,y)=\|x-y\|=\sqrt{<x-y,x-y>}$, where $<u,v>$ is the inner product $<u,v>=\Sigma_{i=1}^{p}u_iv_i$. Note that if $\|\mu(g)\|=c$, for all $g\in G$, then the left side of (1) becomes $\sqrt{2c^2-2<\mu(g),\mu(h)>}$, whereas the right side becomes $\sqrt{2c^2-2<\mu(g^{-1}h),\mu(e)>}$. Therefore, for this case, in which all the points $\mu(g)$ are on the same sphere of radius c, the matching map (1) holds if

$$<\mu(g),\mu(h)>=<\mu(g^{-1}h),\mu(e)>. \tag{2}$$

The sphere with $c=1$, which is the unitary sphere of $\mathbb{R}^n$, is denoted by S^{n-1}. For instance, the unitary sphere of $\mathbb{R}^3$ is $S^2=\{(x,y,z): x^2+y^2+z^2=1\}$ and the unitary circle is $S^1=\{(x,y): x^2+y^2=1\}\subset\mathbb{R}^2$.

The most known matching, over 2-dimensional n-PSK signal sets, satisfying (2), is the group homomorphism between the cyclic group $\frac{\mathbb{Z}}{n\mathbb{Z}}=\mathbb{Z}_n=\{0,1,\ldots,n-1\}$, $n\geq 2$, which is the n-ary group with the modulo-n addition operation, and the group of n-roots of the unity $\mathcal{U}_n=\{e^{\frac{2\pi j}{n}k}\}_{k=0}^{n-1}\subset S^1$, $j=\sqrt{-1}$, with the complex product operation.

While the groups $(\mathbb{Z}_n,+)$ and $(\mathcal{U}_n,*)$ are the same thing, the matching map being the group isomorphism $\mu:\mathbb{Z}_n\rightarrow\mathcal{U}_n$ given by

$$\mu(k)=e^{\frac{2\pi j}{n}k}=(\cos(2\pi k/n),\sin(2\pi k/n)), \tag{3}$$

a generalization of this matching, which by itself is another outstanding example of matched signal sets, satisfying (2), over n-dimensional real signal sets, is the *group code* $S=\{s_i\}_{i=1}^{M}\subset S^{n-1}\subset\mathbb{R}^n$, such that each $s_i=\mathcal{O}_i(s_1)$, where $\mathcal{O}_i$ is an $n\times n$ orthogonal matrix and $s_1\in S^{n-1}$ is called a initial point of the group code [6].

For any adequate initial choice of s_1, the signal set S is matched to a finite multiplicative group, $G=\{\mathcal{O}_i\}_{i=1}^{M}$, by the following matching map:

$$\mu(\mathcal{O}_i)=\mathcal{O}_i(s_1). \tag{4}$$

Indeed, by using the properties of orthogonal matrices, we have that $<\mu(\mathcal{O}_i),\mu(\mathcal{O}_j)>=<\mathcal{O}_i(x_1),\mathcal{O}_j(x_1)>=<$

$\mathcal{O}_j^{-1}\mathcal{O}_i(x_1), x_1 >= < \mu(\mathcal{O}_j^{-1}\mathcal{O}_i), \mu(I) >$, where I is the identity matrix.

The Squared Euclidean Distance (SED) for this signal set is $< x_i - x_j, x_i - x_j >$ = $2 - 2\cos(\theta_{ij})$ =$4\sin^2(\frac{\theta_{ij}}{2})$, where θ_{ij} is the angle between x_i and x_j, and the minimum SED for this case takes place when θ_{ij} is minimum and different from zero [7].

The group $G = \{\mathcal{O}_i\}_{i=1}^{M}$ is a finite subgroup of $SO(n, \mathbb{R})$, the group of real orthogonal matrices of dimension n, which is an infinite group. For dimension two all the finite subgroups of $SO(2, \mathbb{R})$ are the dihedral groups D_{2n}, $n \geq 2$, and the cyclic groups $\mathbb{Z}_n$ [8]. Of course, there may exist matchings of D_{2n} and $\mathbb{Z}_n$ for which these two classes of groups are not considered as subgroups of $SO(2, \mathbb{R})$. For instance, in [9], Bali and Rajan give a method to match two-dimensional $2n - APSK$ Euclidean signal sets $S \subset \mathbb{R}^2$ by using a especial function of an asymmetric initial angle. Other family of important finite groups, that can be matched to an Euclidean signal set, is the generalized quaternions groups Q_{2^n}, $n \geq 3$. As matrices, all the members of the family of quaternions are subgroups of $SO(4, \mathbb{R}) \cong SO(2, \mathbb{C})$, where $\mathbb{C}$ is the complex numbers field. In [10], a method is given to match any Q_{2^n} to a 4-dimensional real Euclidean constellation $S \subset \mathbb{R}^4$.

In this work, we use the theory of extension of groups to show that the group D_{2n} is a particular case of the semidirect product $\mathbb{Z}_n$ by $\mathbb{Z}_m$ with m even. Analogously, we show that the group Q_{2^n} is a particular case of the extension $\mathbb{Z}_n$ by $\mathbb{Z}_m$ with n, m even. The semidirect product is a particular case of extension, in the sense that any semidirect product is an extension but there exist many extensions that are not semidirect products. We will see that semidirect products of $\mathbb{Z}_n$ by $\mathbb{Z}_2$ generate dihedral groups, and extensions $\mathbb{Z}_n$ by $\mathbb{Z}_2$, that are not semidirect products, generate the quaternions groups. We will match semidirect products $\mathbb{Z}_n$ by $\mathbb{Z}_m$, with m even, to 4-dimensional real signal sets, and we will match generalized extensions $\mathbb{Z}_n$ by $\mathbb{Z}_m$, with both n and m even, to $2m$-dimensional real signal sets.

We also propose a new technique to matching groups to signal sets. This technique uses the decomposition of a group G into minor quotient groups $\frac{G}{N}$, where N is a normal subgroup. The smaller $\frac{G}{N}$ the easier it is to find a signal set matched to it.

This work is organized as follows. In Section II, we present some properties of extension of cyclic groups, which are necessary for the matchings we develop in the next sections. In Section III, we match cyclic extensions of groups to signal sets. The new technique to matching groups to signal sets, announced in the previous paragraph, is presented in Section IV. Finally, in Section V, we conclude the paper.

II. Extensions of Cyclic Groups

A formal definition of extension of groups is the following.

Definition 2: Given two abstract groups H and K, the extension of H by K is a group G having a normal subgroup N such that N is isomorphic to H and $\frac{G}{N}$ is isomorphic to K [11], [8].

We will give in the next section a method to construct extension of cyclic groups $H = \mathbb{Z}_n$ by $K = \mathbb{Z}_m$ in such a way that it depends on two elements $a, b \in \mathbb{Z}_n$ satisfying an n-modular system. This method allows us to construct a matching of the extension $\mathbb{Z}_n$ by $\mathbb{Z}_m$ based on the compound natural matchings based upon (3) of $\mathbb{Z}_n$ and $\mathbb{Z}_m$. For the construction of this extension, we need to consider $\mathbb{Z}_n$ as a ring, the ring of integers modulo n.

Lemma 1: Consider the rings $\mathbb{Z}_n$ and $\mathbb{Z}_m$, and $a, b \in \mathbb{Z}_n$, such that $ab = b \in \mathbb{Z}_n$. Then the mapping $\xi : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_n$ defined by

$$\xi(j,k) = \begin{cases} 0 & \text{if} \quad j+k < m \\ b & \text{if} \quad j+k \geq m \end{cases}, \tag{5}$$

satisfies the $\mathbb{Z}_n$-equation;

$$a^i \xi(j,k) + \xi(i, j+k) = \xi(i,j) + \xi(i+j,k), \tag{6}$$

for all $i, j, k \in \mathbb{Z}_m$

Proof: First, note that $a^2 b \equiv a(ab) \equiv ab \equiv b \mod n$. Thus, by induction, $a^p b \equiv b \mod n$, for all $p \in \mathbb{N}$. Now we analyze equation (6) for the following three cases:

Case 1 ($i+j+k \geq 2m$): For this case we have that $i+j \geq m$, $i+k \geq m$, and $j+k \geq m$. Letting $s < m$ be such that $s = j+k-m$, then $\xi(i, j+k) = \xi(i,s)$. If $i+s < m$ then $i+j+k-m < m$, a contradiction. Hence, $i+s \geq m$. On the other hand, letting $r < m$ be such that $r = i+j-m$, then $\xi(i+j,k) = \xi(r,k)$. If $r+k < m$ then $i+j+k < 2m$, again a contradiction. Hence, $r+k \geq m$. Therefore, in this case, (6) holds true as it becomes $a^i b + b = b + b$.

Case 2 ($m \leq i+j+k < 2m$): For this case consider the following four subcases: 2.a) $i+j \geq m$ and $j+k \geq m$, 2.b) $i+j < m$ and $j+k \geq m$, 2.c) $i+j \geq m$ and $j+k < m$, and 2.d) $i+j < m$ and $j+k < m$. For subcase 2.a), let $s < m$ be such that $s = j+k-m$. Then $\xi(i, j+k) = \xi(i,s)$. If $i+s \geq m$ then $i+j+k \geq 2m$, a contradiction. Hence, $i+s < m$. Now let $r < m$ be such that $r = i+j-m$. Then $\xi(i+j,k) = \xi(r,k)$. If $r+k \geq m$ then $i+j+k \geq 2m$, again a contradiction. Hence, $r+k < m$. Therefore, for this subcase (6) holds true as it becomes $a^i b + 0 = b + 0$. For the subcase 2.b), let $s < m$ be such that $s = j+k-m$. Then $\xi(i, j+k) = \xi(i,s)$. If $i+s \geq m$ then $i+j+k \geq 2m$, a contradiction. Hence, $i+s < m$. Now let $r < m$ be such that $r = i+j-m$. Then $\xi(i+j,k) = \xi(r,k)$. If $r+k < m$ then $i+j+k < m$, another contradiction. Hence, $r+k \geq m$. Therefore, for this subcase too, (6) holds true as it becomes $a^i b + 0 = 0 + b$. The proofs for the remaining two subcases follow the same lines.

Case 3 ($0 \leq i+j+k < m$): For this case (6) becomes $a^i 0 + 0 = 0 + 0$, which is clearly true. ■

Proposition 1: Consider the rings of integers $\mathbb{Z}_n$ and $\mathbb{Z}_m$, and $a, b \in \mathbb{Z}_n$ satisfying (6) as well as

$$\begin{array}{c} a^m = 1 \in \mathbb{Z}_n \\ ab = b \in \mathbb{Z}_n \end{array} \tag{7}$$

Then the Cartesian $G = \mathbb{Z}_n \times \mathbb{Z}_m$ with the operation

$$(i,j) * (h,k) = (i + ha^j + \xi(j,k), j+k) \tag{8}$$

is an extension of $\mathbb{Z}_n$ by $\mathbb{Z}_m$, where ξ is defined in (5).

Proof: The operation (8) is closed. The associative equation $((i,j)(h,k))(u,v) = (i,j)((h,k)(u,v))$ holds by

applying the property of ξ given in equation (6). The unique inverse of $(i,0)$ is $(-i,0)$. For $j \neq 0$, consider $x=(i,j)$ and $y=(-(b+ia^{m-j}), m-j)$. Since $a^m \equiv 1 \mod n$ and $ab \equiv b \mod n$, then $xy=(i,j)(-(b+ia^{m-j}), m-j)$ = $(i-(b+i)a^{m-j}a^j+b), j+m-j)$ =$(0,0)$. Analogously, $yx=(0,0)$, thus y is the unique inverse of x. Therefore, $\mathbb{Z}_n \times \mathbb{Z}_m$ is a group with the operation in (8). Now consider $N = \mathbb{Z}_n \times \{0\} = \{(u,0) : u = 0,1,2,\ldots,n-1\} \subset \mathbb{Z}_n \times \mathbb{Z}_m$. For each pair $(i,j) \in \mathbb{Z}_n \times \mathbb{Z}_m$, we have that $(i,j)(u,0)(i,j)^{-1}$ = $(ua^j,0) \in N$. Thus, N is a normal subgroup of $\mathbb{Z}_n \times \mathbb{Z}_m$, with $\mathbb{Z}_n \cong N$. On the other hand, considering the canonical projection $\pi : \frac{\mathbb{Z}_n \times \mathbb{Z}_m}{N} \to \mathbb{Z}_m$, defined by $\pi((i,j)) = j$, we conclude that $\frac{\mathbb{Z}_n \times \mathbb{Z}_m}{N} \cong \mathbb{Z}_m$ and therefore $\mathbb{Z}_n \times \mathbb{Z}_m$ is an extension of $\mathbb{Z}_n$ by $\mathbb{Z}_m$ with the group operation defined in (8). ■

Remarks:

- When $b=0$ and $a^m \equiv 1 \mod n$, we have a semidirect product that often is denoted by $\mathbb{Z}_n \rtimes \mathbb{Z}_m$. Indeed, define $\phi : \mathbb{Z}_m \to Aut(\mathbb{Z}_n)$ such that $\phi(j)(i) = ia^j$. Then ϕ is a group homomorphism and the group operation on $\mathbb{Z}_n \rtimes \mathbb{Z}_m$ given in (8) becomes $(i,j)(h,k) = (i+ha^j, j+k)$.
- The inverse of any pair (i,j), for this semidirect product, is $(-ia^{-j}, -j)$. And if the homomorphism ϕ is not the trivial one, that is, $a \neq 1$, then $\mathbb{Z}_n \rtimes \mathbb{Z}_m$ is always a non-abelian group.
- If $a=1$ and $b=0$, then we have a direct product $\mathbb{Z}_n \times \mathbb{Z}_m$.

Since each pair (a,b) satisfying (7) determines a unique extension $\mathbb{Z}_n$ by $\mathbb{Z}_m$, we will henceforth denote it by $\mathbb{Z}_n \times_{a,b} \mathbb{Z}_m$. Note that $\mathbb{Z}_n \times_{a,0} \mathbb{Z}_m$ will always be a semidirect product and $\mathbb{Z}_n \times_{1,0} \mathbb{Z}_m$ = $\mathbb{Z}_n \times \mathbb{Z}_m$.

Example 1: Consider the cyclic groups $\mathbb{Z}_n$ and $\mathbb{Z}_m$ such that m is even, with $a=n-1$ and $b=0$. Since m is even, then $a^m = (n-1)^m \equiv (-1)^m \equiv 1 \mod n$. Hence $\{a = n-1, b=0\}$ is a solution of the modular equations (7). In this case we have the semidirect product $\mathbb{Z}_n \times_{(n-1),0} \mathbb{Z}_m$. Its group operation is

$$\begin{aligned}(i,j)(h,k) &= (i+ha^j, j+k)\\ &= (i+h(n-1)^j, j+k)\\ &= \begin{cases}(i+h, j+k), & \text{if } j \text{ is even}\\ (i-h, j+k), & \text{if } j \text{ is odd,}\end{cases}\end{aligned}$$

and for any pair (i,j) the inverse is given by $(i,j)^{-1} = (i(-1)^{j+1}, -j)$. For $m=2$, we have the dihedral group $D_{2n} = \mathbb{Z}_n \times_{(n-1),0} \mathbb{Z}_2$, and the mapping $\phi : \mathbb{Z}_2 \to Aut(\mathbb{Z}_n)$ is given by $\phi(j)(i) = i(n-1)^j$.

Example 2: Consider the cyclic groups $\mathbb{Z}_n$ and $\mathbb{Z}_m$ such that both n and m are even, and $a=n-1$, $b=\frac{n}{2}$. Since m is even, then $a^m = (n-1)^m \equiv (-1)^m \equiv 1 \mod n$. On the other hand, n even implies $\frac{n}{2} \equiv -\frac{n}{2} \mod n$. Hence, $(n-1)\frac{n}{2} = n\frac{n}{2} - \frac{n}{2} \equiv -\frac{n}{2} \mod n$. Therefore, $\{a=n-1, b=\frac{n}{2}\}$ is solution of (7), and we have an extension, $\mathbb{Z}_n \times_{(n-1),n/2} \mathbb{Z}_m$, which is not a semidirect product. The group operation on the pairs of this extension is $(i,j)(h,k) = (i+ha^j+\xi(j,k), j+k) = (i+h(n-1)^j+\xi(j,k), j+k)$. Hence,

$$(i,j)(h,k) = \begin{cases}(i+h, j+k), & \text{if } j+k<m,\ j \text{ even}\\ (i-h, j+k), & \text{if } j+k<m,\ j \text{ odd}\\ (i+h+\frac{n}{2}, j+k), & \text{if } j+k \geq m,\ j \text{ even}\\ (i-h+\frac{n}{2}, j+k), & \text{if } j+k \geq m,\ j \text{ odd.}\end{cases}$$

From the above, the inverse $(i,j)^{-1}$ is given by

$$(i,j)^{-1} = \begin{cases}(-i,0), & \text{if } j=0\\ (\frac{n}{2}+i(-1)^{j+1}, -j), & \text{if } j \neq 0.\end{cases}$$

For the particular case where $n=2^{p-1}$, $m=2$, $a=2^{p-1}-1$, and $b=2^{p-2}$, we have the generalized quaternions groups $Q_{2^p} = \mathbb{Z}_{2^{p-1}} \times_{(2^{p-1}-1),2^{p-2}} \mathbb{Z}_2$. The group operation for this family of groups is $(i,j)(h,k)$ = $(i+ha^j+\xi(j,k), j+k)$ = $(i+h(2^{p-1}-1)^j+\xi(j,k), j+k)$. Hence, the inverse $(i,j)^{-1}$ is given by

$$(i,j)^{-1} = \begin{cases}(-i,0), & \text{if } j=0\\ (i+2^{p-2}, -j), & \text{if } j=1.\end{cases}$$

It is clear that when $nm = n'm'$ and when there are pairs (a,b) and (a',b') satisfying the condition in (7), then $\mathbb{Z}_n \times_{a,b} \mathbb{Z}_m$ = $\mathbb{Z}_{n'} \times_{a',b'} \mathbb{Z}_{m'}$. For instance, $\mathbb{Z}_3 \times_{2,0} \mathbb{Z}_8$ = $\mathbb{Z}_{12} \times_{2,9} \mathbb{Z}_2$, as shown in [12].

III. Matching Cyclic Extensions of Groups to Signal Sets

Consider the semidirect product $\mathbb{Z}_n \times_{a,0} \mathbb{Z}_m$ and the map $\mu : \mathbb{Z}_n \times_{a,0} \mathbb{Z}_m \to S^3 \subset \mathbb{R}^4$, induced by (3), given as

$$\mu(i,j) = (\mu(i), \mu(j)) = \frac{1}{\sqrt{2}}\left(e^{\frac{2\pi\sqrt{-1}}{n}i}, e^{\frac{2\pi\sqrt{-1}}{m}j}\right) \quad (9)$$

If $a^{-j} = \pm 1$ then the matching (9) satisfies the condition in (2). Indeed, given the pairs $(i,j),(h,k) \in \mathbb{Z}_n \times_{a,0} \mathbb{Z}_m$ we have $(i,j)^{-1}(h,k)$= $((h-i)(a)^{-j}, k-j)$. From this, $< \mu((i,j)^{-1}(h,k)), \mu(0,0) > = < \mu((h-i)a^{-1}, k-j), \mu(0,0) > = \frac{1}{2}\left(\cos\left(\frac{2\pi(h-i)a^{-j}}{n}\right) + \cos\left(\frac{2\pi(k-j)}{m}\right)\right)$. On the other hand, by using the trigonometric relation $\cos(a-b) = \cos(a)\cos(b)+\sin(a)\sin(b)$, we have that $< \mu(i,j), \mu(h,k) >$ becomes

$$\frac{1}{2}\left(\cos\left(\frac{2\pi(i-h)}{n}\right) + \cos\left(\frac{2\pi(k-j)}{m}\right)\right),$$

which shows that (9) is a matching map if $a^{-j} = \pm 1$, for all $1 \leq j \leq m$. That is right for the case $a=n-1$ in Example 1. For the particular case $m=2$, which implies the dihedral group $D_{2n} = \mathbb{Z}_n \times_{(n-1),0} \mathbb{Z}_2$, the matching (9) becomes

$$\begin{aligned}\mu(i,j) &= \frac{1}{\sqrt{2}}\left(\cos\left(\frac{2\pi i}{n}\right), \sin\left(\frac{2\pi i}{n}\right), \cos(\pi j), 0\right)\\ &= \begin{cases}\frac{1}{\sqrt{2}}\left(\cos\left(\frac{2\pi i}{n}\right), \sin\left(\frac{2\pi i}{n}\right), 1, 0\right), & \text{if } j=0\\ \frac{1}{\sqrt{2}}\left(\cos\left(\frac{2\pi i}{n}\right), \sin\left(\frac{2\pi i}{n}\right), -1, 0\right), & \text{if } j=1.\end{cases}\end{aligned}$$

The SEDs between the points $\mu(i,j)$ and the point $\mu(0,0)$ are given by $\|\mu(i,j) - \mu(0,0)\|^2$ = $2(1- < \mu(i,j), \mu(0,0) >)$. For $m=2$, and denoting by SED_9 the SED associated with the matching (9), we have that

$$\begin{aligned}\text{SED}_9 &= 2 - \cos(\pi j) - \cos(\frac{2\pi i}{n})\\ &= \begin{cases}1 - \cos(\frac{2\pi i}{n}), & \text{if } j=0\\ 3 - \cos(\frac{2\pi i}{n}), & \text{if } j=1.\end{cases}\end{aligned}$$

Clearly, SED_9 will be minimal if $j=0$ and for the minimal value of the set $\{1-\cos(\frac{2\pi i}{n}) : i=1,2,\ldots,n-1\}$. The function $f(x)=1-\cos(\frac{2\pi x}{n})$ is crescent in the interval $(0,\frac{n}{2})$. Also, $f(\frac{n}{2}-1)=f(\frac{n}{2}+1)$ for n even, and $f(\frac{n-1}{2}-1)=f(\frac{n+1}{2}+1)$ for n odd. From this, among the points $x=1,2,\ldots,n-1$, $f(x)$ is minimal for $x=1$, and $\text{SED}_{9,min}=1-\cos(\frac{2\pi}{n})$.

Let us now consider the matching of Bali and Rajan [9], which is the following two dimensional mapping for dihedral groups D_{2n} over signal sets $2n$-APSK $\subset S^1 \subset \mathbb{R}^2$:

$$\mu(i,j)=(\cos(\varphi(i,j)),\sin(\varphi(i,j))), \tag{10}$$

where φ is the angle $\varphi(i,j)=j\left(\frac{(2u+1)\pi}{n}+\phi\right)+i\frac{2\pi l}{n}$, with $u\in\{0,1,\ldots,n-1\}$, and l is such that $gcd(l,n)=1$, and ϕ is the asymmetry phase with $-\frac{\pi}{2n}<\phi<\frac{\pi}{2n}$.

Let SED_{10} be the SED for (10). Then $SED_{10}=4\sin^2(\frac{\varphi(i,j)}{2})$. In particular, for $\phi=0$, we have that

$$\text{SED}_{10}=\begin{cases} 4\sin^2\left(\frac{\pi i l}{n}\right), & \text{if } j=0 \\ 4\sin^2\left(\frac{2\pi(u+il)+1}{2n}\right), & \text{if } j=1. \end{cases}$$

Hence, the minimal SED_{10} is reached for $j=1$ and $2(u+il)+1\equiv\pm1 \mod n$. Thus, the minimal SED_{10} is $\text{SED}_{10,min}=4\sin^2(\frac{\pi}{2n})$. Since

$$\frac{1+\cos\left(\frac{2\pi}{n}\right)}{2}=\cos^2\left(\frac{\pi}{n}\right)<\cos\left(\frac{\pi}{n}\right), \text{ for all } n\geq 3,$$

we have that

$$1-\cos\left(\frac{2\pi}{n}\right)>2-2\cos\left(\frac{\pi}{n}\right)=4\sin^2\left(\frac{\pi}{2n}\right).$$

Therefore, $\text{SED}_9>\text{SED}_{10}$ for all Dihedral groups D_{2n}, with $n\geq 3$.

Example 3: Consider the group extension $\mathbb{Z}_n\times_{(n-1),n/2}\mathbb{Z}_m$ of Example 2. Consider the Euclidean space $\mathbb{R}^{2m}$ and, for $i=0,1,2,\ldots,n-1$, the points of $E_{ij}\in\mathbb{R}^{2m}$ given by

$$\begin{array}{rcl} E_{i0} & = & \left(\cos(\frac{2\pi i}{n}),\sin(\frac{2\pi i}{n}),0,0,\ldots,0\right) \\ E_{i1} & = & \left(0,0,\cos(\frac{2\pi i}{n}),\sin(\frac{2\pi i}{n}),0,0,\ldots,0\right) \\ E_{i2} & = & \left(0,0,0,0,\cos(\frac{2\pi i}{n}),\sin(\frac{2\pi i}{n}),0,0,\ldots,0\right) \\ \vdots & \vdots & \vdots \\ E_{i(m-1)} & = & \left(0,0,0,0,\ldots,\cos(\frac{2\pi i}{n}),\sin(\frac{2\pi i}{n})\right) \end{array}$$

Clearly, $\|E_{ij}\|=1$ for all $0\leq j\leq m-1$, and $<E_{ij},E_{ik}>=0$ if $j\neq k$. We match injectively these points to the group by defining the matching map as

$$\mu(i,j)=E_{ij} \tag{11}$$

Hence,

$$<\mu(i,j),\mu(h,k)>=\begin{cases} 0, & \text{if } j\neq k \\ \cos\left(\frac{2\pi(i-h)}{n}\right), & \text{if } j=k. \end{cases}$$

On the other hand, $(i,j)^{-1}(h,k)$ equals

$$\begin{cases} (h-i,k), & \text{if } j=0 \\ ((h-i)a^{-j}-\frac{n}{2}+\xi(m-j,k),k-j), & \text{if } j\neq 0. \end{cases}$$

Then,

$$<\mu((i,j)^{-1}(h,k)),\mu(0,0)>=\begin{cases} 0, & \text{if } j\neq k \\ \cos\left(\frac{2\pi(i-h)}{n}\right), & \text{if } j=k. \end{cases}$$

For the case of the quaternions $Q_{2^p}=\mathbb{Z}_{2^{p-1}}\times_{(2^{p-1}-1),2^{p-2}}\mathbb{Z}_2$, the above matching becomes

$$\mu(i,j)=\begin{cases} \left(\cos\left(\frac{2\pi i}{n}\right),\sin\left(\frac{2\pi i}{n}\right),0,0\right), & \text{if } j=0 \\ \left(0,0,\cos\left(\frac{2\pi i}{n}\right),\sin\left(\frac{2\pi i}{n}\right)\right), & \text{if } j=1, \end{cases}$$

which is exactly as the one proposed in [10].

IV. Matching Quotient Groups to Signal Sets

In this section we introduce a method based on the splitting of a given group into small quotient groups. Given a group G, instead of matching it directly to a signal set S, our method takes into account normal subgroups $N_1,N_2,\ldots,N_n$, of G, in such a way that the quotient groups $\frac{G}{N_1},\frac{G}{N_2},\ldots,\frac{G}{N_n}$ are matched to small signal sets $S_1,S_2,\ldots,S_n$. Then under a couple of additional conditions this method allows us to match G to the cartesian product $S_1\times S_2\times\ldots\times S_n$.

Theorem 1: Let G be a group with non-trivial normal subgroups $N_1,N_2,\ldots,N_n$. Let $S_1,S_2,\ldots,S_n$ be signal sets injectively matched to the quotient groups $\frac{G}{N_1},\frac{G}{N_2},\ldots,\frac{G}{N_n}$. Then,
1) the Cartesian product $S_1\times S_2\times\ldots\times S_n$ is matched to G;
2) $\bigcap_{i=1}^n N_i=\{e\}$, with $n>1$, if and only if the matching is injective.

Proof: In order to prove 1), let $\mu_i:\frac{G}{N_i}\to S_i$ be the i-matching mapping, for $i=1,2,\ldots,n$. This means that if d_i is the metric over S_i then $d_i(\mu_i(gN_i),\mu_i(hN_i))=d_i(\mu_i(gh^{-1}N_i),\mu_i(N_i))$. Define the mapping $\mu:G\to S_1\times S_2\times\ldots\times S_n$ as

$$\mu(g)=(\mu_1(gN_1),\mu_2(gN_2),\ldots,\mu_n(gN_n)) \tag{12}$$

Then, considering the induced metric over $S_1\times S_2\times\ldots\times S_n$, namely, $d(s,t)=\Sigma_{i=1}^n d_i(s_i,t_i)$, where $s=(s_1,s_2,\ldots,s_n)$ and $t=(t_1,t_2,\ldots,t_n)$, we have that

$$\begin{array}{rcl} d(\mu(g),\mu(h)) & = & \Sigma_{i=1}^n d_i(\mu_i(gN_i),\mu_i(hN_i)) \\ & = & \Sigma_{i=1}^n d_i(\mu_i(gh^{-1}N_i),\mu_i(N_i)) \\ & = & d(\mu(gh^{-1}),\mu(e)), \end{array}$$

which shows that μ is a matching mapping.

To prove 2), suppose that $\mu(g)=\mu(h)$. Then $\mu_i(gN_i)=\mu_i(hN_i)$, for all $i=1,2,\ldots,n$. Since each μ_i is injective, we have that $gN_i=hN_i$, which means that $gh^{-1}\in\bigcap_{i=1}^n N_i=\{e\}$. Hence, $g=h$. Therefore, μ is injective. On the other hand, suppose the matching is injective and $n_0\neq e\in\bigcap_{i=1}^n N_i$. Then $\mu(e)$ must be different from $\mu(n_0)$. But $\mu(e)=(\mu_1(N_1),\ldots,\mu_n(N_n))=\mu(n_0)$, and we have a contradiction. ∎

Suppose that each S_i is a unitary sphere of $\mathbb{R}^{m_i}$, that is, $\|s_i\|=1$ for each $s_i\in S_i$ and $d_i^2(s_i,t_i)=<s_i-t_i,s_i-t_i>$. Then $d^2(s,t)=\sum_{i=1}^n<s_i-t_i,s_i-t_i>=\sum_{i=1}^n 2-2\cos(\theta_{s_it_i})$ and (12) can be adapted for the unitary sphere of $\mathbb{R}^{m_1}\times\mathbb{R}^{m_2}\times\ldots\mathbb{R}^{m_n}\times$ by

$$\mu(g)=\frac{1}{\sqrt{n}}(\mu_1(gN_1),\mu_2(gN_2),\ldots,\mu_n(gN_n)). \tag{13}$$

If any one of the matching maps (12) or (13) is injective, then we must have that $|G|\leq|S_1|\cdot|S_2|\cdot\cdots\cdot|S_{n-1}|\cdot|S_n|=$

$|\frac{G}{N_1}|\cdot|\frac{G}{N_2}|\cdot\cdots\cdot|\frac{G}{N_{n-1}}|\cdot|\frac{G}{N_n}|$. From this, $\Pi_{i=1}^{n}|N_i| \leq |G|^{n-1}$. In particular, for $n=2$, $|N_1||N_2| \leq |G|$.

On the other hand, it is known that the group $\mathbb{Z}_2$ is the only one that is matched to 1-dimensional signal sets such as $\{-1,1\} \subset \mathbb{R}$. All the other cyclic groups $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$, $n > 1$, can not be matched to 1-dimensional signal sets in the sense of the equation (1). The minimal dimension of the sets that they are matched to is two, and the canonical matching map μ for $\mathbb{Z}_n$, $n \geq 3$, is given by (3), i.e., $\mu(i) = e^{\frac{2\pi\sqrt{-1}}{n}i}$, $i = 0,1,\ldots,n-1$.

In equation (9) we proposed the matching of groups which are semidirect products $\mathbb{Z}_n \times_{a,0} \mathbb{Z}_m$, for $a^{-j} = 1$, with four dimensional signal sets. The dihedral groups D_{2n}, being particular cases of these groups, can be matched to 3-dimensional signal sets. On the other hand, Bali and Rajan in [9] have proposed the matching of these dihedral groups to 2-dimensional signal sets. Nevertheless, we have shown that the SED for the 3-dimensional case is better than the one for the 2-dimensional case. Now, for extensions that are not semidirect products, $\mathbb{Z}_n \times_{(n-1),n/2} \mathbb{Z}_m$, we proposed a matching with signal sets in $2m$ dimensional Euclidean spaces. For the particular case of quaternions groups $Q_{2^p} = \mathbb{Z}_{2^{p-1}} \times_{(2^{p-1}-1),2^{p-2}} \mathbb{Z}_2$, $n \geq 3$, our proposed matched constellation becomes a subset of a 4-dimensional Euclidean space like the one proposed in [10]. For other particular cases of groups generated by two elements, some matching maps are proposed in [12] by the method of extension of cyclic groups. The above discussion yields the following corollary of Theorem 1.

Corollary 1: Let G be a group with two non-trivial normal subgroups N_1 and N_2 such that $N_1 \cap N_2 = \{e\}$, and the quotient groups $\frac{G}{N_1}$ and $\frac{G}{N_2}$ are isomorphic to either cyclic or dihedral groups. Then G is injectively matched to a signal set of dimension less than or equal to 4.

We now discuss the case where G is abelian and finite, for which any subgroup $N \subset G$ is normal and each quotient group $\frac{G}{N}$ is abelian. By the fundamental theorem of finite abelian groups [8], G is a finite direct product of cyclic groups, that is, $G = (\mathbb{Z}_{n_1})^{m_1} \times (\mathbb{Z}_{n_2})^{m_2} \times \ldots \times (\mathbb{Z}_{n_k})^{m_k}$. If $N_1 = (\mathbb{Z}_{n_1})^{m_1} \times (\mathbb{Z}_{n_2})^{m_2} \times \ldots \times (\mathbb{Z}_{n_k})^{m_k-1}$ and $N_2 = (\mathbb{Z}_{n_1})^{m_1-1} \times (\mathbb{Z}_{n_2})^{m_2} \times \ldots \times (\mathbb{Z}_{n_k})^{m_k}$, then we have that N_1 and N_2 are normal subgroups of G with $N_1 \cap N_2 = e$, $\frac{G}{N_1} \cong \mathbb{Z}_{n_k}$, and $\frac{G}{N_2} \cong \mathbb{Z}_{n_1}$. We then have another corollary.

Corollary 2: Let G be a finite and abelian group. If G is not cyclic then it is matched to a 4-dimensional signal set. If G is cyclic then it is matched to a 2-dimensional signal set.

Example 4: Consider the abstract group G whose Cayley table is shown in Table I. This group together with the dihedral group D_{12} and the Alternant group A_4 are the three non-abelian groups of order 12 [13]. The group G has three non-trivial normal subgroups, namely, $N_1 = \{0,3\}$, $N_2 = \{0,1,2\}$, and $N_3 = \{0,1,2,3,4,5\}$. The quotient group

$$\frac{G}{N_1} = \{\{0,3\},\{1,4\},\{2,5\},\{6,9\},\{7,10\},\{8,11\}\}$$

is isomorphic to the dihedral group $D_6 = \mathbb{Z}_3 \times_{2,0} \mathbb{Z}_2$, which is best known as the group of symmetries of the triangle. For this example, we will use the 2-dimensional matching μ_1 by using (10), with $\phi = 0, l = 1, u = 1$, and by setting $\alpha = \sin(\frac{\pi}{3})$.

0	1	2	3	4	5	6	7	8	9	10	11
1	2	0	4	5	3	8	6	7	11	9	10
2	0	1	5	3	4	7	8	6	10	11	9
3	4	5	0	1	2	9	10	11	6	7	8
4	5	3	1	2	0	11	9	10	8	6	7
5	3	4	2	0	1	10	11	9	7	8	6
6	7	8	9	10	11	3	4	5	0	1	2
7	8	6	10	11	9	5	3	4	2	0	1
8	6	7	11	9	10	4	5	3	1	2	0
9	10	11	6	7	8	0	1	2	3	4	5
10	11	9	7	8	6	2	0	1	5	3	4
11	9	10	8	6	7	1	2	0	4	5	3

TABELA I

CAYLEY TABLE FOR THE GROUP G

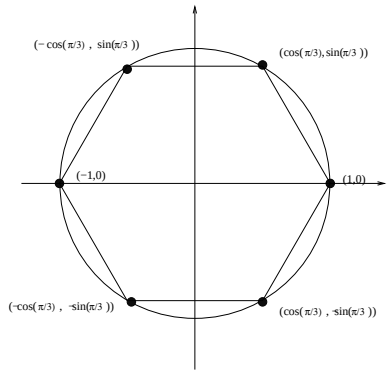

Fig. 1. Signal set matched to the group S_3

The matched signal set is shown in the Figure 1. The matching μ_1 is given in the following chart:

Coset of N_1		$D_6 = \mathbb{Z}_3 \times_{2,0} \mathbb{Z}_2$		Matched signal
$\{0,3\}$	$\mapsto$	$(0,0)$	$\overset{\mu_1}{\mapsto}$	$(1,0)$
$\{1,4\}$	$\mapsto$	$(1,0)$	$\overset{\mu_1}{\mapsto}$	$(-0.5,\alpha)$
$\{2,5\}$	$\mapsto$	$(2,0)$	$\overset{\mu_1}{\mapsto}$	$(-0.5,-\alpha)$
$\{6,9\}$	$\mapsto$	$(0,1)$	$\overset{\mu_1}{\mapsto}$	$(-1,0)$
$\{8,11\}$	$\mapsto$	$(1,1)$	$\overset{\mu_1}{\mapsto}$	$(0.5,-\alpha)$
$\{7,10\}$	$\mapsto$	$(2,1)$	$\overset{\mu_1}{\mapsto}$	$(0.5,\alpha)$.

The quotient group

$$\frac{G}{N_2} = \{\{0,1,2\},\{3,4,5\},\{6,7,8\},\{9,10,11\}\}$$

is isomorphic to the cyclic group $\mathbb{Z}_4 = \{0,1,2,3\}$. The signal set $S_2 = \{(1,0),(0,1),(-1,0),(0,-1)\} \subset \mathbb{R}^2$, shown in Figure 2, is injectively matched to $\frac{G}{N_2} \cong \mathbb{Z}_4$ via the following chart:

Coset of N_2		$\mathbb{Z}_4$		Matched signal
$\{0,1,2\}$	$\mapsto$	e	$\overset{\mu_2}{\mapsto}$	$(1,0)$
$\{3,4,5\}$	$\mapsto$	2	$\overset{\mu_2}{\mapsto}$	$(-1,0)$
$\{6,7,8\}$	$\mapsto$	1	$\overset{\mu_2}{\mapsto}$	$(0,1)$
$\{9,10,11\}$	$\mapsto$	3	$\overset{\mu_2}{\mapsto}$	$(0,-1)$

Finally, the quotient group

$$\frac{G}{N_3} = \{\{0,1,2,3,4,5\},\{6,7,8,9,10,11\}\}$$

is isomorphic to the binary, and cyclic, group $\mathbb{Z}_2 = \{0,1\}$, and it is matched to the set $\{1,-1\}$.

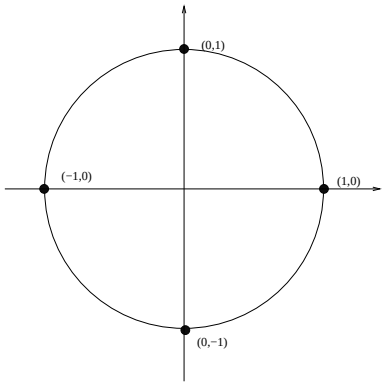

Fig. 2. Signal set matched to the group $\mathbb{Z}_4$

G	N_1, N_2	SED
0	$\frac{1}{\sqrt{2}}(1,0,1,0)$	0
1	$\frac{1}{\sqrt{2}}(-0.5,0.\alpha,1,0)$	1.5
2	$\frac{1}{\sqrt{2}}(-0.5,-\alpha,1,0)$	1.5
3	$\frac{1}{\sqrt{2}}(1,0,-1,0)$	2.0
4	$\frac{1}{\sqrt{2}}(-0.5,\alpha,-1,0)$	3.5
5	$\frac{1}{\sqrt{2}}(-0.5,-\alpha,-1,0)$	3.5
6	$\frac{1}{\sqrt{2}}(-1,0,0,1)$	3
7	$\frac{1}{\sqrt{2}}(0.5,\alpha,0,1)$	1.5
8	$\frac{1}{\sqrt{2}}(0.5,-\alpha,0,1)$	1.5
9	$\frac{1}{\sqrt{2}}(-1,0,0,-1)$	3
10	$\frac{1}{\sqrt{2}}(0.5,\alpha,0,-1)$	1.5
11	$\frac{1}{\sqrt{2}}(0.5,-\alpha,0,-1)$	1.5

TABELA II

MATCHING OF THE GROUP G TO AN EUCLIDEAN SET OF $\mathbb{R}^4$

Since $N_1 \cap N_2 = \{0\}$, then for these two subgroups we obtain an injective matching (given in (13)) of G to a 4-dimensional signal set. It is the matching $\mu : G \to S_1 \times S_2 \subset \mathbb{R}^4$ given in the Table II together with its SEDs. For N_1 and N_3 we have that $N_1 \cap N_3 = N_1$, which results in a non-injective matching. For N_2 and N_3 we have that $N_2 \cap N_3 = N_3$, which does not give an injective matching either.

V. CONCLUSIONS

Matching signal sets and groups is a useful method for encoding information in bandlimited channels. We studied extensions of cyclic groups and showed that the semidirect product is a particular case of the extension of groups. The analysis of extension of cyclic groups gave us parameters that allowed the construction of new examples of matching signal sets and groups. For instance, we found groups that are generalizations of the dihedrals D_{2n} that are matched to 4-dimensional signal sets. Similar results were obtained for the quaternions Q_{2^n}. The reduction of the dimension of the signal set, for these generalized groups, is left for future work. Finally, in the last section, we presented a new technique of matching groups and signal sets. This technique is useful for matching big and non-abelian groups other than the dihedral and the quaternion groups. Particularly, we showed that, if a group G has two normal subgroups N_1 and N_2, with $N_1 \cap N_2 = \{e\}$, then, no matter how big G is, it can be injectively matched to a signal set with dimension less than or equal to four.

REFERÊNCIAS

[1] G. Ungerboeck, "Channel coding with multilevel-phase signals," *IEEE Transactions on Information Theory*, vol. 28, pp. 55–67, 1982.

[2] A. Calderbank and N. Sloane, "New trellis codes based on lattices and cosets," *IEEE Transactions on Information Theory*, vol. 33, pp. 177–195, 1987.

[3] D. G. Forney, "Geometrically uniform codes," *IEEE Transactions on Information Theory*, vol. 37, no. 5, pp. 1241–1260, 1991.

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

[5] G. Forney and M. Trott, "The dynamics of group codes; state spaces, trellis diagrams and canonical encoders," vol. IT 39(5), pp. 1491–1513, 1993.

[6] D. Slepian, "Group codes for the gaussian channels," *Bell Systems Technical Journal*, vol. 47, pp. 575–602, 1968.

[7] R. M. de Siqueira and S. R. Costa, "Upper bounds for commutative group codes," in *Proceedings of the 2006 International Telecommunications Symposium*. Fortaleza, CE: IEEE, Setembro 2006.

[8] J. J. Rotman, *An Introduction to the Theory of the Groups*, 4th ed. New York: Springer Verlag, 1995.

[9] J. Bali and S. Rajan, "Block coded psk modulation using two-level group codes over dihedral groups," *IEEE Transactions on Information Theory*, vol. 44, pp. 1620–1631, July 1998.

[10] T. Selvakumaran and S. Rajan, "Block coded psk modulation using two-level group codes over generalized quaternion groups," *IEEE Transactions on Information Theory*, vol. 45, pp. 365–372, january 1999.

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

[12] J. P. Arpasi, "Matching signal sets and extension of cyclic groups," in *Proceedings of the 2006 International Telecommunications Symposium*. Fortaleza, CE: IEEE, Setembro 2006.

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