[12] O. Sharon, "On the relation between bit delay for Slot Reuse and the number of address bits in the dual bus configuration," extended version, available upon request.

Block-Coded Modulation Using Two-Level Group Codes Over Generalized Quaternion Groups

T. V. Selvakumaran and B. Sundar Rajan, *Senior Member, IEEE*

***Abstract*—A length n group code over a group G is a subgroup of G^n under component-wise group operation. Two-level group codes over the class of generalized quaternion groups, Q_{2^m}, $m \geq 3$, are constructed using a binary code and a code over $Z_{2^{m-1}}$, the ring of integers modulo 2^{m-1}, as component codes and a mapping f from $Z_2 \times Z_{2^{m-1}}$ to Q_{2^m}. A set of necessary and sufficient conditions on the component codes is derived which will give group codes over Q_{2^m}. Given the generator matrices of the component codes, the computational effort involved in checking the necessary and sufficient conditions is discussed. Starting from a four-dimensional signal set matched to Q_{2^m}, it is shown that the Euclidean space codes obtained from the group codes over Q_{2^m} have Euclidean distance profiles which are independent of the coset representative selection involved in f. A closed-form expression for the minimum Euclidean distance of the resulting group codes over Q_{2^m} is obtained in terms of the Euclidean distances of the component codes. Finally, it is shown that all four-dimensional signal sets matched to Q_{2^m} have the same Euclidean distance profile and hence the Euclidean space codes corresponding to each signal set for a given group code over Q_{2^m} are automorphic Euclidean-distance equivalent.**

***Index Terms*—Coded modulation, group codes, multilevel construction.**

I. Introduction

The concept of geometrically uniform codes introduced by Forney [1] generalizes Slepian's signal sets [2] and several other known classes of good codes like Ungerboeck's trellis codes, coset codes, and lattice codes [3], [4]. An important ingredient in the recipe given in [1] for construction of geometrically uniform codes is a group code over a group G. A group code over a group G is a subgroup, under component-wise operation of G^I, where I is an index set, finite or infinite. The case I being infinite corresponds to trellis-coded modulation and I being finite corresponds to block-coded modulation. This correspondence deals with block-coded modulation using group codes over generalized quaternion groups which are non-Abelian. The generalized quaternion group with 2^m elements, $m \geq 3$, denoted by Q_{2^m}, is given by the presentation [5]

$$Q_{2^m} = \langle x, y | x^{2^{m-1}} = 1, x^{2^{m-2}} = y^2, y^{-1}xy = x^{-1} \rangle.$$

Manuscript received June 8, 1996; revised January 19, 1998. This work was supported in part by the National Board for Higher Mathematics, India, through a fellowship to T. V. Selvakumaran. The material in this correspondence was presented in part at the 1997 IEEE International Symposium on Information Theory (ISIT'97), Ulm, Germany, June 29–July 4, 1997.

T. V. Selvakumaran is with the Department of Mathematics, Indian Institute of Technology, New Delhi-110 016, India (e-mail: selva@maths.iitd.ernet.in).

B. S. Rajan is with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore-560 012, India (e-mail: bsrajan@ece.iisc.ernet.in).

Communicated by N. Seshadri, Associate Editor for Coding Techniques.

Publisher Item Identifier S 0018-9448(99)00066-8.

Note that $m = 3$ gives the familiar quaternion group of eight elements.

A signal set is a finite set of points in an Euclidean space of finite dimension. A signal set S in $\mathbb{R}^N$ is said to be matched to a group G if there exists a mapping μ from G onto S such that for all g and g' in G

$$d_E(\mu(g), \mu(g')) = d_E(\mu(g^{-1}g'), \mu(e))$$

where $d_E(a, b)$ denotes the Euclidean distance between a, b, and e is the identity element of G [6]. For coded communication systems, the capacity of the signal set [7] is a more relevant performance index of a signal set as compared to the average probability of error of the signal set. It has been shown that the capacity of the signal sets matched to Abelian groups are upper-bounded by the so-called phase-shift keying (PSK) limit [6]. Signal sets matched to non-Abelian groups that exceed PSK limit exist [6], [8]. This motivates the study of signal sets matched to non-Abelian groups and group codes over them.

Imai and Hirakawa [9] introduced the notion of multilevel construction of codes by combining conventional error-correcting codes, called component codes. Fig. 1 shows a two-level construction of codes over Q_{2^m} with a binary code and a code over $Z_{2^{m-1}}$ as component codes. Several authors have studied multilevel construction for group codes [10], [13]. Ginzburg [14] has generalized the approach of Imai and Hirakawa. One of the important aspects in multilevel construction is the conditions on the component codes that lead to the resulting code being a group code over a group. In [11] this problem has been addressed to obtain linear codes over cyclic groups. Garello and Benedetto [13] give conditions for the multilevel constructed code to be a group code over a semidirect product group. We obtain necessary and sufficient conditions on the component codes that lead to a group code over Q_{2^m}. Note that Q_{2^m} cannot be obtained as a semidirect product of its subgroups.

Block-coded modulation schemes have been studied primarily for PSK signal sets by several authors [15]–[17]. In [18] a four-dimensional signal set with eight points has been indexed with the elements of the Quaternion group of eight elements without any mention of matching between the signal set and the group. We describe signal sets in four dimensions matched to Q_{2^m} for any m and for $m = 3$ this coincides with the one given in [18]. The two-level group codes over Q_{2^m} are used to obtain Euclidean space codes with this four-dimensional signal set as the basic signal set. Multilevel construction is closely related to the notion of set partitioning process [14], [17], [19] and for group partitioning the performance of the resulting signal space code depends on the selection of coset representative [15]. We show that, in our case, the performance is independent of the coset representative. Also, we give the minimum Euclidean distance of the multilevel group codes in terms of the minimum distance of the component codes.

The four-dimensional signal sets used can be obtained as Slepian signal sets by the action of orthogonal matrix groups, which are faithful irreducible representations of Q_{2^m}, on an initial vector. We show that the initial vector problem does not arise in the case of Q_{2^m}.

This correspondence has been organized as follows: Section II describes the four-dimensional signal set matched to Q_{2^m}. The necessary and sufficient conditions on the generator matrices of the component codes to result in a multilevel group code over Q_{2^m} is derived in Section III. The relation between the minimum Euclidean distance of the multilevel group code and the minimum Euclidean distances of the component codes is discussed in Section IV. Section

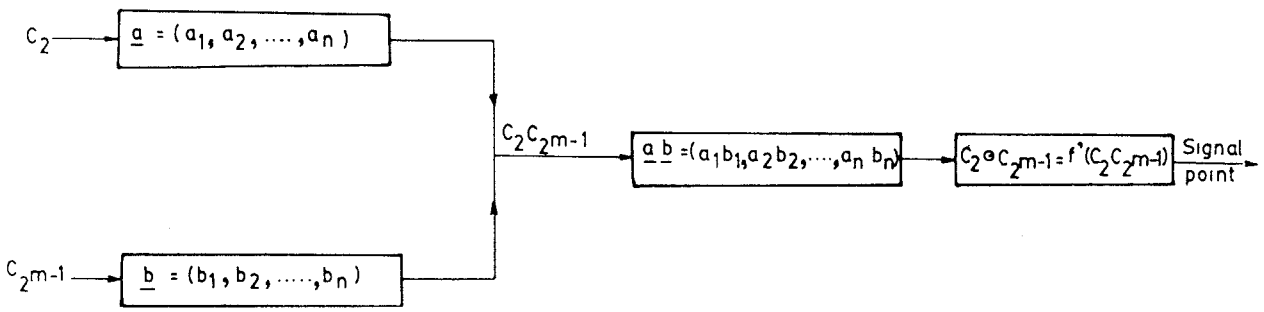


Fig. 1. Two-level construction of group codes over Q_{2m}.

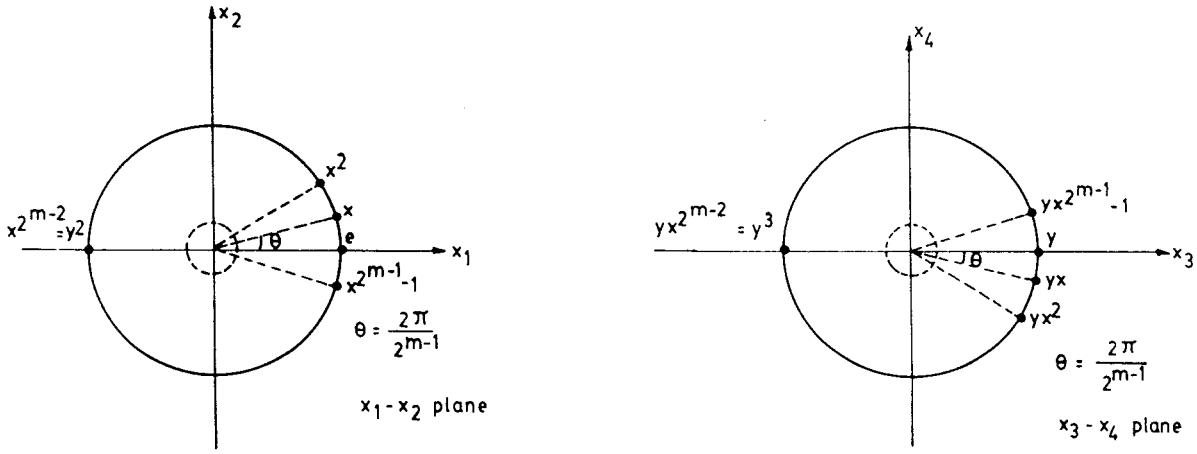


Fig. 2. A signal set matched to Q_{2m}.

V discusses the initial vector problem and the automorphic Euclidean distance equivalence [20] of the Euclidean space codes obtained from the group codes over Q_{2^m}. Some general remarks and possible directions for further work are given in Section VI.

II. Signal Sets Matched to the Generalized Quaternion Group

In this section we describe four-dimensional signal sets matched to Q_{2^m} for all $m \geq 3$ and demonstrate that these signal sets can be obtained as Slepian signal sets. In Section V, these signal sets will be viewed as Slepian signal sets and the initial vector problem will be discussed.

Fig. 2 shows a signal set S in $\mathbb{R}^4$ matched to Q_{2^m}, where

$$S = \Big\{(\cos k\theta, \sin k\theta, 0, 0), (0, 0, \cos k\theta, -\sin k\theta), \quad 0 \leq k \leq 2^{m-1} - 1, \theta = \frac{2\pi}{2^{m-1}}\Big\}. \tag{1}$$

The mapping $\mu: Q_{2^m} \longrightarrow S$ is given by

$$\mu(x^k) = (\cos k\theta, \sin k\theta, 0, 0)$$
$$\mu(yx^k) = (0, 0, \cos k\theta, -\sin k\theta), \qquad 0 \leq k \leq 2^{m-1} - 1.$$

It is a straightforward calculation to check that S is matched to Q_{2^m}.

The mapping μ naturally extends to $\mu^n: Q_{2^m}^n \longrightarrow S^n$ componentwise. This associates to every length n code over Q_{2^m} a signal set in $4n$ dimensions.

The Euclidean weight of an element $y^j x^k$ in Q_{2^m}, is defined as

$$w_E(y^j x^k) = \begin{cases} |\exp(2\pi ki/2^{m-1}) - 1|^2, & \text{if } j = 0 \\ 2, & \text{if } j = 1. \end{cases}$$

The Euclidean weight of an n-tuple in $Q_{2^m}^n$ is then the sum of the Euclidean weight of its components. For a group code over Q_{2^m} the Euclidean distance distribution is the Euclidean weight distribution of the code [1].

Slepian [2] describes a class of signal sets which he called "group codes" as a signal set in $\mathbb{R}^N$ which is the orbit of a point in $\mathbb{R}^N$ under a finite group of orthogonal transformations of $\mathbb{R}^N$. Loeliger [6] has shown that a signal set is matched to a group, if and only if it is a translate of a Slepian signal set. To be specific, if a Slepian signal set has its centroid at the origin then it is a signal set matched to its generating group.

Note that the signal set S defined in (1) can be obtained as the orbit of the point $(1, 0, 0, 0)$ under the group of orthogonal matrices of $\mathbb{R}^4$ given by

$$G = \left\{ \begin{bmatrix} \cos kp & -\sin kp & 0 & 0 \\ \sin kp & \cos kp & 0 & 0 \\ 0 & 0 & \cos kp & \sin kp \\ 0 & 0 & -\sin kp & \cos kp \end{bmatrix}, \begin{bmatrix} 0 & 0 & -\cos kp & \sin kp \\ 0 & 0 & -\sin kp & -\cos kp \\ \cos kp & \sin kp & 0 & 0 \\ -\sin kp & \cos kp & 0 & 0 \end{bmatrix}, \quad 0 \leq k \leq 2^{m-1} - 1 \right\}.$$

III. Multilevel Codes over Q_{2^m}

In this section, we characterize two-level group codes over Q_{2^m} that are obtained from the component codes over Z_2 and $Z_{2^{m-1}}$.

TABLE I
DEFINITION OF THE MAPPING f

$Z_2 \backslash Z_{2^{m-1}}$	0	1	$\cdots$	2^{m-2}	$\cdots$	$2^{m-1}-1$
0	1	x	$\cdots$	$x^{2^{m-1}}$	$\cdots$	$x^{2^{m-1}-1}$
1	y	yx	$\cdots$	$yx^{2^{m-2}}$	$\cdots$	$yx^{2^{m-1}-1}$

We define a one–one, onto mapping $f: Z_2 \times Z_{2^{m-1}} \longrightarrow Q_{2^m}$ as $f(a, b) = y^a x^b$ where $a \in Z_2$ and $b \in Z_{2^{m-1}}$ as shown in Table I.

Let the component codes be a code C_2 of length n over Z_2 and a code $C_{2^{m-1}}$ of length n over $Z_{2^{m-1}}$. We construct a set denoted by $C_2 C_{2^{m-1}}$ called an extension of C_2 and $C_{2^{m-1}}$ given by

$$\begin{aligned} C_2 C_{2^{m-1}} = \{\underline{ab} = (a_1 b_1, a_2 b_2, \cdots, a_n b_n) | \\ \cdot \underline{a} = (a_1, a_2, \cdots, a_n) \in C_2, \\ \underline{b} = (b_1, b_2, \cdots, b_n) \in C_{2^{m-1}}\}. \end{aligned}$$

That is, an element $\underline{ab}$ in $C_2 C_{2^{m-1}}$ is obtained by component-wise juxtaposition of an element $\underline{a}$ in C_2 and an element $\underline{b}$ in $C_{2^{m-1}}$. Notice that, for each component $a_i b_i$ of $\underline{ab}$, a_i and b_i are just two symbols placed next to each other.

By extending the mapping f to f' as shown below, from $C_2 C_{2^{m-1}}$ to $Q_{2^m}^n$

$$f': C_2 C_{2^{m-1}} \longrightarrow Q_{2^m}^n$$

$$\begin{aligned} \underline{ab} = (a_1 b_1, a_2 b_2, \cdots, a_n b_n) \longrightarrow \\ (f(a_1, b_1), f(a_2, b_2), \cdots, f(a_n, b_n)) \in Q_{2^m}^n \end{aligned}$$

we associate a subset of $Q_{2^m}^n$ with $C_2 C_{2^{m-1}}$. Let this subset, image of $C_2 C_{2^{m-1}}$ under f', be $C_2 \odot C_{2^{m-1}}$. In general, $C_2 \odot C_{2^{m-1}}$ need not be a subgroup of $Q_{2^m}^n$, i.e., it need not be a group code over Q_{2^m}. Fig. 1 describes this construction.

In the following theorem, we characterize the component codes C_2 and $C_{2^{m-1}}$ for which $C_2 \odot C_{2^{m-1}}$ is a group code over Q_{2^m}.

Theorem 1: (A preliminary version of this theorem appears in [21]). Given a code C_2 over Z_2 and a code $C_{2^{m-1}}$ over $Z_{2^{m-1}}$, the set $C_2 \odot C_{2^{m-1}}$ is a group code over Q_{2^m}, if and only if

1) C_2 is a group code over Z_2;
2) $C_{2^{m-1}}$ is a group code over $Z_{2^{m-1}}$;
3) $2C_2 \cdot (2^{m-3} C_2 \oplus_{2^{m-1}} C_{2^{m-1}}) \subseteq C_{2^{m-1}}$
where $\oplus_{2^{m-1}}$ denotes component-wise addition modulo 2^{m-1} and $\cdot$ denotes component-wise integer multiplication.

Proof: ($\Longrightarrow$) Let

1) C_2 be a group code over Z_2;
2) $C_{2^{m-1}}$ be a group code over $Z_{2^{m-1}}$;
3) $2C_2 \cdot (2^{m-3} C_2 \oplus_{2^{m-1}} C_{2^{m-1}}) \subseteq C_{2^{m-1}}$,
i.e.,
$2\underline{a} \cdot (2^{m-3} \underline{b} \oplus_{2^{m-1}} \underline{c}) \in C_{2^{m-1}}$
for all codewords $\underline{a}, \underline{b} \in C_2$ and $\underline{c} \in C_{2^{m-1}}$.

Let

$$\begin{aligned} \underline{r_1} &= (r_{11}, r_{12}, \cdots, r_{1n}) \\ \underline{r_2} &= (r_{21}, r_{22}, \cdots, r_{2n}) \in C_2 \end{aligned}$$

and

$$\begin{aligned} \underline{s_1} &= (s_{11}, s_{12}, \cdots, s_{1n}) \\ \underline{s_2} &= (s_{21}, s_{22}, \cdots, s_{2n}) \in C_{2^{m-1}} \end{aligned}$$

so that

$$f'(\underline{r_1 s_1}),\ f'(\underline{r_2 s_2}) \in C_2 \odot C_{2^{m-1}}$$

.

Since $Q_{2^m}^n$ is a finite group, if

$$f'(\underline{r_1 s_1}) \star f'(\underline{r_2 s_2}) \in C_2 \odot C_{2^{m-1}}$$

for all $\underline{r_1}, \underline{r_2} \in C_2$ and $\underline{s_1}, \underline{s_2} \in C_{2^{m-1}}$, where $\star$ denotes the group operation of $Q_{2^m}^n$ then $C_2 \odot C_{2^{m-1}}$ is a subgroup of $Q_{2^m}^n$ and hence, a group code over Q_{2^m}.

We have

$$\begin{aligned} \underline{r_1}\ \underline{s_1} &= (r_{11}s_{11}, r_{12}s_{12}, \cdots, r_{1n}s_{1n}) \\ &= (r_{1i}s_{1i})_{i=1}^n \in C_2 C_{2^{m-1}} \\ \underline{r_2}\ \underline{s_2} &= (r_{21}s_{21}, r_{22}s_{22}, \cdots, r_{2n}s_{2n}) \\ &= (r_{2i}s_{2i})_{i=1}^n \in C_2 C_{2^{m-1}} \\ f'(\underline{r_1}\ \underline{s_1}) &= (f(r_{11}, s_{11}), f(r_{12}, s_{12}), \cdots, f(r_{1n}, s_{1n})) \in Q_{2^m}^n \\ f'(\underline{r_2}\ \underline{s_2}) &= (f(r_{21}, s_{21}), f(r_{22}, s_{22}), \cdots, f(r_{2n}, s_{2n})) \in Q_{2^m}^n. \end{aligned}$$

Now, any element in Q_{2^m} is of the form

$$y^a x^b,\ a = 0, 1\ b = 0, 1, \cdots, 2^{m-1} - 1.$$

Let

$$y^{a_1} x^{b_1},\ y^{a_2} x^{b_2},\ a_1,\ a_2 = 0, 1, b_1, b_2 = 0, 1, \cdots, 2^{m-1} - 1$$

be any two elements in Q_{2^m}. Checking the four different cases of (a_1, a_2) separately, one easily obtains the formula

$$\begin{aligned} &(y^{a_1} x^{b_1})(y^{a_2} x^{b_2}) \\ &\qquad = y^{a_1 \oplus_2 a_2} x^{b_1 \oplus_{2^{m-1}} b_2 \ominus_{2^{m-1}} 2a_2(2^{m-3} a_1 \oplus_{2^{m-1}} b_1)} \end{aligned}$$

for all $a_1, a_2 = 0, 1, b_1, b_2 = 0, 1, \cdots, 2^{m-1} - 1$. Hence (see equations at the bottom of this page). Since C_2 and $C_{2^{m-1}}$ are group codes over Z_2 and $Z_{2^{m-1}}$, we have $\underline{s_1} \oplus_{2^{m-1}} \underline{s_2} \in C_{2^{m-1}}$ and $\underline{r_1} \oplus_2 \underline{r_2} \in C_2$.

Also, we are given that,

$$2C_2 \cdot (2^{m-3} C_2 \oplus_{2^{m-1}} C_{2^{m-1}}) \subseteq C_{2^{m-1}}$$

for all codewords in C_2 and $C_{2^{m-1}}$. In particular,

$$2\underline{r_2} \cdot (2^{m-3} \underline{r_1} \oplus_{2^{m-1}} \underline{s_1}) \in C_{2^{m-1}}.$$

That is,

$$\underline{s_1} \oplus_{2^{m-1}} \underline{s_2} \ominus_{2^{m-1}} 2\underline{r_2} \cdot (2^{m-3} \underline{r_1} \oplus_{2^{m-1}} \underline{s_1}) \in C_{2^{m-1}}$$

i.e.,

$$\overline{\underline{r_1} \oplus_2 \underline{r_2}}\ \overline{\underline{s_1} \oplus_{2^{m-1}} \underline{s_2} \ominus_{2^{m-1}} 2\underline{r_2} \cdot (2^{m-3} \underline{r_1} \oplus_{2^{m-1}} \underline{s_1})} \in C_2 C_{2^{m-1}}$$

$$\begin{aligned} f'(\underline{r_1}\ \underline{s_1}) \star f'(\underline{r_2}\ \underline{s_2}) &= (f(r_{1i}, s_{1i}))_{i=1}^n (f(r_{2i}, s_{2i}))_{i=1}^n \\ &= \left(f(\overline{r_{1i} \oplus_2 r_{2i}}, \overline{s_{1i} \oplus_{2^{m-1}} s_{2i} \ominus_{2^{m-1}} 2r_{2i}(2^{m-3} r_{1i} \oplus_{2^{m-1}} s_{1i})})\right)_{i=1}^n \\ &= f'(\overline{\overline{r_1 \oplus_2 r_2}\ \overline{s_1 \oplus_{2^{m-1}} \underline{s_2} \ominus_{2^{m-1}} 2\underline{r_2} \cdot (2^{m-3} \underline{r_1} \oplus_{2^{m-1}} \underline{s_1})}}) \end{aligned}$$

i.e.,

$$f'(\underline{r_1}\ \underline{s_1}) \star f'(\underline{r_2}\ \underline{s_2}) \in C_2 \odot C_{2^{m-1}}$$

for all $\underline{r_1}, \underline{r_2} \in C_2$ and $\underline{s_1}, \underline{s_2} \in C_{2^{m-1}}$ which implies that $C_2 \odot C_{2^{m-1}}$ is a subgroup of $Q_{2^m}^n$ and hence, a group code over Q_{2^m}.

($\Longleftarrow$) Conversely, given that $C_2 \odot C_{2^{m-1}} = f'(C_2 C_{2^{m-1}})$ is a subgroup of $Q_{2^m}^n$. We have

$$f'(\underline{r_1}\ \underline{s_1}) \star f'(\underline{r_2}\ \underline{s_2}) = f'(\overline{\underline{r_1} \oplus_2 \underline{r_2}}\ \overline{\underline{s_1} \oplus_{2^{m-1}} \underline{s_2} \ominus_{2^{m-1}} 2\underline{r_2} \cdot (2^{m-3}\underline{r_1} \oplus_{2^{m-1}} \underline{s_1})}) \in C_2 \odot C_{2^{m-1}}$$

for all $\underline{r_1}, \underline{r_2} \in C_2$ and $\underline{s_1}, \underline{s_2} \in C_{2^{m-1}}$. That is, $\underline{r_1} \oplus_2 \underline{r_2} \in C_2$ and

$$\underline{s_1} \oplus_{2^{m-1}} \underline{s_2} \ominus_{2^{m-1}} 2\underline{r_2} \cdot (2^{m-3}\underline{r_1} \oplus_{2^{m-1}} \underline{s_1}) \in C_{2^{m-1}}$$

for all $\underline{r_1}, \underline{r_2} \in C_2$ and $\underline{s_1}, \underline{s_2} \in C_{2^{m-1}}$.

We now observe that the identity element of $Q_{2^m}^n$ belongs to $C_2 \odot C_{2^{m-1}}$. So, $f'(\underline{0}\,\underline{0})$ belongs to $C_2 \odot C_{2^{m-1}}$. Therefore, both C_2 and $C_{2^{m-1}}$ contain the all-zero vector. Putting $\underline{r_2} = \underline{0}$ in the expression

$$\underline{s_1} \oplus_{2^{m-1}} \underline{s_2} \ominus_{2^{m-1}} 2\underline{r_2} \cdot (2^{m-3}\underline{r_1} \oplus_{2^{m-1}} \underline{s_1}) \in C_{2^{m-1}}$$

we get that $\underline{s_1} \oplus_{2^{m-1}} \underline{s_2} \in C_{2^{m-1}}$ for all $\underline{s_1}, \underline{s_2} \in C_{2^{m-1}}$. We already know that $\underline{r_1} \oplus_2 \underline{r_2} \in C_2$ for all $\underline{r_1}, \underline{r_2} \in C_2$. Thus C_2 is a subgroup of Z_2^n and $C_{2^{m-1}}$ is a subgroup of $Z_{2^{m-1}}^n$. That is, C_2 and $C_{2^{m-1}}$ are group codes over Z_2 and $Z_{2^{m-1}}$, respectively.

Now

$$\overline{\underline{s_1} \oplus_{2^{m-1}} \underline{s_2} \ominus_{2^{m-1}} 2\underline{r_2} \cdot (2^{m-3}\underline{r_1} \oplus_{2^{m-1}} \underline{s_1})} \ominus_{2^{m-1}} \overline{\underline{s_1} \oplus_{2^{m-1}} \underline{s_2}} \in C_{2^{m-1}}$$

i.e.,

$$-2\underline{r_2} \cdot (2^{m-3}\underline{r_1} \oplus_{2^{m-1}} \underline{s_1}) \in C_{2^{m-1}}$$

for all $\underline{r_1}, \underline{r_2} \in C_2$ and $\underline{s_1}, \underline{s_2} \in C_{2^{m-1}}$. That is,

$$2C_2 \cdot (2^{m-3}C_2 \oplus_{2^{m-1}} C_{2^{m-1}}) \subseteq C_{2^{m-1}}. \qquad \square$$

Example 1: For $m = 3$, let $C_2 = \{(00), (11)\}$, $C_4 = \{(00), (01), (02), (03), (20), (21), (22), (23)\}$ be length-2 block codes over Z_2 and $Z_{2^{m-1}}$, respectively. Then the extension code $C_2 \odot C_{2^{m-1}} = \{(1\,1), (1\,x), (1\,x^2), (1\,x^3), (x^2\,1), (x^2\,x), (x^2\,x^2), (x^2\,x^3), (y\,y), (y\,yx), (y\,yx^2), (y\,yx^3), (yx^2\ \ y), (yx^2\ \ yx), (yx^2\ yx^2), (yx^2\ yx^3)\} \subset Q_8^2$ is a group code over Q_8. Under the mapping f this code gives an eight-dimensional signal set with 16 codewords with squared Euclidean distances 2, 4, 6, and 8, with multiplicities, respectively, 4, 6, 4, and 1.

A. Selection of Coset Representative

In our definition of f: $Z_2 \times Z_{2^{m-1}} \longrightarrow Q_{2^m}$ the elements $f(0, i) = x^i, 0 \le i \le 2^{m-1}$ form a subgroup of Q_{2^m}, say H. The elements $f(1, i), 0 \le i \le 2^{m-1}$ then form a coset of H, namely, yH. In our definition of f, we have chosen y as the coset representative, i.e.,

$$f(1, i) = yf(0, i) = yx^i, \qquad 0 \le i \le 2^{m-1}.$$

Suppose had we chosen any other element of yH as the coset representative, would the necessary and sufficient condition for $C_2 \odot C_{2^{m-1}}$ be still the same as in the above theorem? The answer is yes. This becomes clear when we note that every element in the coset yH is of order 4. Moreover, if z is any other element in yH then z is of the form yx^j for some j and so $z^{-1}xz = (yx^j)^{-1}x(yx^j) = x^{-1}$. Thus x and z generate Q_{2^m} and hence, redefining the function f in terms of x and z would not alter the necessary and sufficient conditions.

Suppose $C_2 \odot C_{2^{m-1}}$ is a group code over Q_{2^m}. Is its Euclidean distance distribution independent of the coset representative we choose in the definition of f? The answer is again yes. This is clear when we observe that if a codeword $\underline{c}$ in $C_2 \odot C_{2^{m-1}}$ has a component from yH, then in that component the squared Euclidean distance from the identity element of Q_{2^m} is 2. Thus the Euclidean weight of the codeword is independent of the coset representative we choose in the definition of f.

B. Computational Complexity

Now, suppose we are given a group code C_2 of length n over Z_2 and a group code $C_{2^{m-1}}$ of length n over $Z_{2^{m-1}}$. Let their generator matrices be of order $k \times n$ and $k' \times n$, respectively. Then, clearly, $|C_2| = 2^k$ and $|C_{2^{m-1}}| \ge 2^{k'}$. To check if $C_2 \odot C_{2^{m-1}}$ is a group code over Q_{2^m}, we need to check that the condition $2C_2 \cdot (2^{m-3}C_2 \oplus_{2^{m-1}} C_{2^{m-1}})$ is true, i.e.,

$$2\underline{a} \cdot (2^{m-3}\underline{b} \oplus_{2^{m-1}} \underline{c}) \in C_{2^{m-1}}, \qquad \forall \underline{a}, \underline{b} \in C_2, \underline{c} \in C_{2^{m-1}}.$$

If checking $2\underline{a} \cdot (\underline{b} \oplus_{2^{m-1}} \underline{c}) \in C_{2^{m-1}}$ is taken to be a single operation for a given $\underline{a}, \underline{b} \in C_2$ and $\underline{c} \in C_{2^{m-1}}$, then to check the condition for all codewords would take at least $2^{k+k'}$ operations. We now show that we require far less.

Let A be the generator matrix of a group code C_2 of length n over Z_2 and B be the generator matrix of a group code $C_{2^{m-1}}$ of length n over $Z_{2^{m-1}}$. We augment the generator matrices A and B each by a row of all-zero entries. We denote these augmented matrices by A' and B', respectively.

Lemma 1: Let $2\underline{a} \cdot (2^{m-3}\underline{b} \oplus_{2^{m-1}} \underline{c}) \in C_{2^{m-1}}$, for all $\underline{a}, \underline{b}, \underline{c}$ where $\underline{a}, \underline{b}$ are rows of A' and $\underline{c}$ is a row of B'. Then $2\underline{g} \cdot (2^{m-3}\underline{f}) \in C_{2^{m-1}} \forall \underline{g}, \underline{f} \in C_2$.

Proof: Let the order of the augmented generator matrices A' and B' be $k \times n$ and $k' \times n$, respectively. Let

$$\underline{g} = l_1\underline{v_1} \oplus_2 l_2\underline{v_2} \oplus_2 \cdots \oplus_2 l_k\underline{v_k}, \qquad l_i = 0, 1$$
$$\underline{f} = m_1\underline{v_1} \oplus_2 m_2\underline{v_2} \oplus_2 \cdots \oplus_2 m_k\underline{v_k}, \qquad m_i = 0, 1$$

where $\underline{v_i}$'s are the rows of A'.

$$\begin{aligned} 2\underline{g} \cdot (2^{m-3}\underline{f}) &= 2(l_1\underline{v_1} \oplus_2 \cdots \oplus_2 l_k\underline{v_k}) \\ &\quad \cdot \{2^{m-3}(m_1\underline{v_1} \oplus_2 \cdots \oplus_2 m_k\underline{v_k})\} \\ &= 2^{m-2}(\oplus_2{}_{i=1}^{k}(\oplus_2{}_{j=1}^{k}(l_i\underline{v_i}) \cdot (m_j\underline{v_j}))) \\ &= \oplus_{2^{m-1}}{}_{i=1}^{k}(\oplus_{2^{m-1}}{}_{j=1}^{k}(l_i m_j) \\ &\quad \cdot \{2\underline{v_i} \cdot (2^{m-3}\underline{v_j} \oplus_{2^{m-1}} \underline{0})\}). \end{aligned}$$

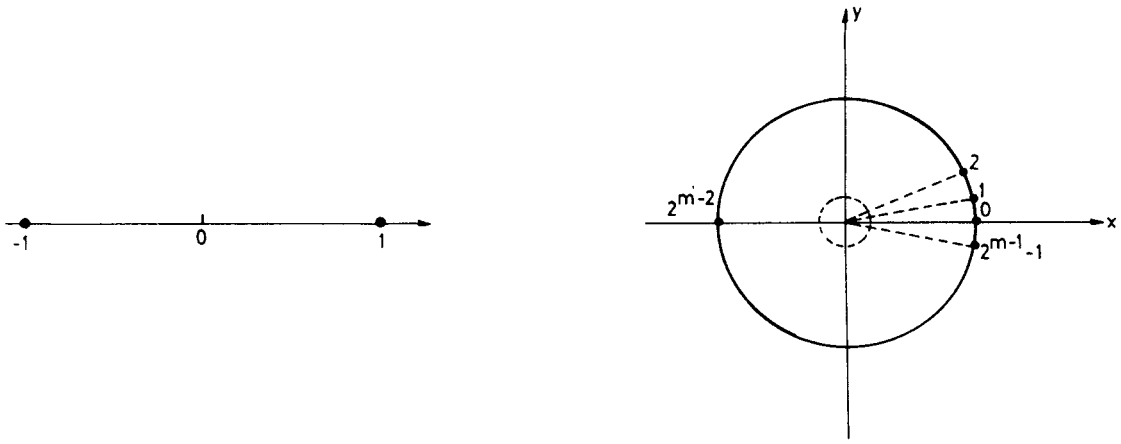
But, $2\underline{v_i} \cdot (2^{m-3}v_j \oplus_{2^{m-1}} \underline{0}) \in C_{2^{m-1}}$ for each i, j. So,

$$2\underline{g} \cdot (2^{m-3}\underline{f}) = \oplus_{2^{m-1}}{}_{i=1}^{k}(\oplus_{2^{m-1}}{}_{j=1}^{k}(l_i m_j)\{2\underline{v_i} \cdot (2^{m-3}\underline{v_j} \oplus_{2^{m-1}} \underline{0})\}) \in C_{2^{m-1}}. \qquad \square$$

Lemma 2: Let $2\underline{a} \cdot (2^{m-3}\underline{b} \oplus_{2^{m-1}} \underline{c}) \in C_{2^{m-1}}$ for all $\underline{a}, \underline{b}, \underline{c}$, where $\underline{a}, \underline{b}$ are rows of A' and $\underline{c}$ is a row of B'. Then, $2\underline{g} \cdot (\underline{f}) \in C_{2^{m-1}}$, where $\underline{g}$ is a row of A' and $\underline{f}$ is any codeword in $C_{2^{m-1}}$.

Proof: Let the order of the augmented generator matrices A' and B' be $k \times n$ and $k' \times n$, respectively. Let

$$\underline{f} = n_1\underline{u_1} \oplus_{2^{m-1}} n_2\underline{u_2} \oplus_{2^{m-1}} \cdots \oplus_{2^{m-1}} n_{k'}\underline{u_{k'}}, \qquad 0 \le n_i \le 2^{m-1} - 1$$



(a) (b)

Fig. 3. (a) The binary signal set and (b) the 2^{m-1}-PSK signal set.

where $\underline{u_i}$'s are the rows of B'. Then

$$\begin{aligned}2\underline{g}\cdot\underline{f} &= 2\underline{g}\cdot(n_1\underline{u_1}\oplus_{2^{m-1}}\cdots\oplus_{2^{m-1}} n_{k'}\underline{u_{k'}})\\ &= 2\underline{g}\cdot(n_1\underline{u_1})\oplus_{2^{m-1}}\cdots\oplus_{2^{m-1}} 2\underline{g}\cdot(n_{k'}\underline{u_{k'}})\\ &= n_1\{2\underline{g}\cdot(2^{m-3}\underline{0}\oplus_{2^{m-1}}\underline{u_1})\}\oplus_{2^{m-1}}\\ &\qquad\cdots\oplus_{2^{m-1}} n_{k'}\{2\underline{g}\cdot(2^{m-3}\underline{0}\oplus_{2^{m-1}}\underline{u_{k'}})\}.\end{aligned}$$

But, $2\underline{g}\cdot(2^{m-3}\underline{0}\oplus_{2^{m-1}}\underline{u_i})\in C_{2^{m-1}}$ for each i by Lemma 1. So

$$\begin{aligned}2\underline{g}\cdot\underline{f} &= n_1\{2\underline{g}\cdot(2^{m-3}\underline{0}\oplus_{2^{m-1}}\underline{u_1})\}\oplus_{2^{m-1}}\cdots\oplus_{2^{m-1}} n_{k'}\\ &\quad\cdot\{2\underline{g}\cdot(2^{m-3}\underline{0}\oplus_{2^{m-1}}\underline{u_{k'}})\}\in C_{2^{m-1}}.\end{aligned}$$

Hence, proved. □

Theorem 2: The condition $2C_2\cdot(2^{m-3}C_2\oplus_{2^{m-1}}C_{2^{m-1}})$ is true, if and only if, $2\underline{x}\cdot(2^{m-3}\underline{y}\oplus_{2^{m-1}}\underline{z})\in C_{2^{m-1}}$ for all $\underline{x}$, $\underline{y}$, and $\underline{z}$ where $\underline{x}$, $\underline{y}$ are rows of the augmented generator matrix A' and $\underline{z}$ is a row of the augmented generator matrix B'.

Proof:

($\Longrightarrow$) If the condition $2C_2\cdot(2^{m-3}C_2\oplus_{2^{m-1}}C_{2^{m-1}})$ is satisfied by all codewords of C_2 and $C_{2^{m-1}}$, then it is trivially satisfied for rows of the augmented generator matrices of C_2 and $C_{2^{m-1}}$, because the rows of the augmented generator matrices of C_2 and $C_{2^{m-1}}$ are codewords of C_2 and $C_{2^{m-1}}$.

($\Longleftarrow$) Conversely, let us be given that $2\underline{x}\cdot(2^{m-3}\underline{y}\oplus_{2^{m-1}}\underline{z})\in C_{2^{m-1}}$ for all $\underline{x}$, $\underline{y}$, and $\underline{z}$, where $\underline{x}$, $\underline{y}$ are rows of the augmented generator matrix A' and $\underline{z}$ is a row of the augmented generator matrix B'.

We need to show that for any arbitrary $\underline{a}$, $\underline{b}\in C_2$ and $\underline{c}\in C_{2^{m-1}}$, $2\underline{a}\cdot(2^{m-3}\underline{b}\oplus_{2^{m-1}}\underline{c})\in C_{2^{m-1}}$. In light of Lemma 1, it is enough to show that,

$$2\underline{a}\cdot\underline{c}\in C_{2^{m-1}}.$$

We show it by induction. Let the order of the augmented generator matrix A' and B' be $k\times n$ and $k'\times n$, respectively. Let

$$\underline{a}=m_1\underline{v_1}\oplus_2 m_2\underline{v_2}\oplus_2\cdots\oplus_2 m_k\underline{v_k},\qquad m_i=0,\,1.$$

We can view $(m_1,\,m_2,\,\cdots,\,m_k)$, $m_i=0,\,1$ as an ordered n-tuple with decreasing order of significance from m_1 to m_k. Clearly, for the base case $(0,\,0,\,\cdots,\,0,\,1)$ we have $2\underline{v_k}\cdot\underline{c}\in C_{2^{m-1}}$ by Lemma 2. Now, we assume that $2\underline{a'}\cdot\underline{c}\in C_{2^{m-1}}$ for all $\underline{a'}$ such that,

$$\underline{a'}=m_1'\underline{v_1}\oplus_2 m_2'\underline{v_2}\oplus_2\cdots\oplus_2 m_k'\underline{v_k}$$

and

$$(m_1',\,m_2',\,\cdots,\,m_k')<(m_1,\,m_2,\,\cdots,\,m_k).$$

Let the least significant nonzero of $(m_1,\,m_2,\,\cdots,\,m_k)$ be at position t, i.e.,

$$\begin{aligned}(m_1,\,m_2,\,\cdots,\,m_k) &= (m_1,\,m_2,\,\cdots,\,m_{t-1},\,0,\,0,\,\cdots,\,0)\\ &\quad+(\underbrace{0,\,0,\,\cdots,\,0,\,1}_{t},\,\underbrace{0,\,0,\,\cdots,\,0}_{n-t}).\end{aligned}$$

Let $\underline{v}=m_1\underline{v_1}\oplus_2 m_2\underline{v_2}\oplus_2\cdots\oplus_2 m_{t-1}\underline{v_{t-1}}$. Then,

$$\begin{aligned}2\underline{a}\cdot\underline{c} &= 2(\underline{v}\oplus_2\underline{v_t})\cdot\underline{c}\\ &= 2(\underline{v}\oplus_{2^{m-1}}\underline{v_t}\ominus_{2^{m-1}}2\underline{v}\cdot\underline{v_t})\cdot\underline{c}\\ &= 2\underline{v}\cdot\underline{c}\oplus_{2^{m-1}}2\underline{v_t}\cdot\underline{c}\ominus_{2^{m-1}}2\underline{v_t}\cdot(2\underline{v}\cdot\underline{c}).\end{aligned}$$

Now, $2\underline{v}\cdot\underline{c}\in C_{2^{m-1}}$ by the induction hypothesis. So, $2\underline{v_t}\cdot(2\underline{v}\cdot\underline{c})$, $2\underline{v_t}\cdot\underline{c}\in C_{2^{m-1}}$ by Lemma 2, i.e.,

$$2\underline{a}\cdot\underline{c}=2\underline{v}\cdot\underline{c}\oplus_{2^{m-1}}2\underline{v_t}\cdot\underline{c}\ominus_{2^{m-1}}2\underline{v_t}\cdot(2\underline{v}\cdot\underline{c})\in C_{2^{m-1}}.$$

Hence, proved. □

Example 2: For $m=3$, let C_2 and C_4 be length-3 block codes with generators $[0\,0\,0]$ and $[1\,1\,2]$, respectively. Then, the extension code $C_2\odot C_4$ is a group code over Q_8.

Example 3: For $m=5$, let C_2 and C_{16} be length-2 block codes with generators $[1\,0]$ and $[0\,1]$, $[4\,1]$, respectively. Then, the extension code $C_2\odot C_{16}$ is a group code over Q_{32} with 128 codewords.

IV. Minimum Euclidean Distance

Given the minimum Hamming distance of the component codes, a lower bound for the minimum Euclidean distance for the resultant multilevel group code is well known [15], [17]. In this section, we derive the minimum Euclidean distance of the group code over Q_{2^m} given the minimum Euclidean distances of the component codes C_2 and $C_{2^{m-1}}$.

Let us now assume binary signal set for Z_2 and the 2^{m-1}-PSK signal set for $Z_{2^{m-1}}$. The *Euclidean weight* of an element a of $Z_{2^{m-1}}$ is defined as $w_E(a)=|\exp(2\pi ai/2^{m-1})-1|^2$, which is the squared Euclidean distance from the point a to the point 0 as shown in Fig. 3, and the weight of an n-tuple $\underline{v}\in Z_{2^{m-1}}^n$ is defined as the sum of the weights of the components. The minimum squared Euclidean distance of group codes over Z_2 and $Z_{2^{m-1}}$ are then the weights of codewords with minimum Euclidean weight [17].

Theorem 3: Let C_2 and $C_{2^{m-1}}$ be group codes over Z_2 and $Z_{2^{m-1}}$, respectively, that satisfy the conditions of Theorem 1. Let $d_{E_1}^2$ and $d_{E_2}^2$ be the minimum squared Euclidean distance of the group codes C_2 and $C_{2^{m-1}}$, respectively, of length n. Then the

minimum squared Euclidean distance of the group code $C_2 \odot C_{2^{m-1}}$ over Q_{2^m} of length n is given by

$$d_E^2 = \min \cdot \left\{ \frac{d_{E_1}^2}{2},\, d_{E_2}^2 \right\}.$$

Proof: Let $\underline{c} = (x_1y_1,\, x_2y_2,\, \cdots,\, x_ny_n)$ be any codeword in $C_2 \odot C_{2^{m-1}}$ formed from $\underline{x} = (x_1,\, x_2,\, \cdots,\, x_n) \in C_2$ and $\underline{y} = (y_1,\, y_2,\, \cdots,\, y_n) \in C_{2^{m-1}}$ with $\underline{x} \neq \underline{0}$.

Let the Euclidean distance of $\underline{x}$ from $\underline{0}$ be d. Then the Hamming distance of $\underline{x}$ from $\underline{0}$ is $d^2/4$. That is, the codeword $\underline{x}$ has 1's in exactly $d^2/4$ places. So, exactly $d^2/4$ components in the codeword $\underline{c}$ of $C_2 \odot C_{2^{m-1}}$ would lie in the X_3–X_4 plane (see Fig. 1) and the remaining $(n - d^2/4)$ components would lie in the X_1–X_2 plane. So, the squared Euclidean distance of $\underline{c}$ from $\underline{0}$ in $\mathbb{R}^4$ is at least $2d^2/4 = d^2/2$.

Thus the squared minimum Euclidean distance of any codeword $\underline{c}$ in $C_2 \odot C_{2^{m-1}}$ (formed from a nonzero codeword $\underline{x}$ in C_2) from $\underline{0}$ is at least $d_{E_1}^2/2$.

Now, we take the codeword $\underline{y} = \underline{0} \in C_{2^{m-1}}$ and a codeword $\underline{x} = (x_1,\, x_2,\, \cdots,\, x_n)$ in C_2 with Euclidean weight d_{E_1}. Then clearly, the codeword $\underline{c} = (x_10,\, x_20,\, \cdots,\, x_n0)$ has Euclidean weight $d_{E_1}^2/2$. Thus the minimum squared Euclidean distance of any codeword $\underline{c}$ in $C_2 \odot C_{2^{m-1}}$ (formed from a nonzero codeword in C_2) is $d_{E_1}^2/2$.

Now, let us consider all the codewords in $C_2 \odot C_{2^{m-1}}$ that are formed from the all-zero codeword of C_2, i.e., $\underline{c} = (0y_1,\, 0y_2,\, \cdots,\, 0y_n)$, $\underline{y} = (y_1,\, y_2,\, \cdots,\, y_n) \in C_{2^{m-1}}$. Clearly, the minimum squared Euclidean distance of all codewords from $\underline{0}$ is $d_{E_2}^2$.

Now, we observe that the set of all codewords in $C_2 \odot C_{2^{m-1}}$ may be partitioned (disjoint union) into i) the set of codewords formed from $\underline{0}$ from C_2 and any arbitrary codeword from $C_{2^{m-1}}$ and ii) the set of all codewords formed from any nonzero codeword from C_2 and any arbitrary codewords from $C_{2^{m-1}}$.

Hence, $d_{E_2}^2 = \min\{d_{E_1}^2/2,\, d_{E_2}^2\}$. □

V. Initial Vector Problem

A finite group of orthogonal transformations of $\mathbb{R}^N$ is the real representation of degree N of a group. For an introduction to the representation theory of groups one might like to read Serre [22] or Blake and Mullin [23].

Given a representation ρ of degree N of a finite group G, what is the vector $x \in \mathbb{R}^N$ that maximizes the minimum distance of the signal set? This is the initial vector problem of group codes. Biglieri and Elia [24] have solved the initial vector problem for arbitrary representations of cyclic groups. Mitelholzer and Lahtonen [25] have partially solved this problem for faithful, irreducible representations of finite reflection groups.

Moreover, even if we know the optimal initial vector for a particular representation of G, how can we be sure that no other representation of the same group G gives a better minimum distance for some initial vector? We will now show that in the case of the generalized quaternion group, this problem does not arise if we consider only faithful, irreducible representations.

The conjugacy classes of Q_{2^m} are $\{1\}$, $\{x^{2^{m-2}} = y^2\}$, $\{yx^j,\, \forall\, j \neq 0,\, 2^{m-2}\}$, $\{x^i,\, x^{-i}\} \forall\ i \neq 0,\, 2^{m-2}$. There are $2^{m-2} + 3$ conjugacy classes in all. We note that

$$1^2 + 1^2 + 1^2 + 1^2 + \underbrace{2^2 + 2^2 + \cdots + 2^2}_{(2^{m-2}-1) \text{ times}} = 2^m.$$

TABLE II
Characters of $\psi_1,\, \psi_2,\, \psi_3,\, \psi_4$

	x	y
ψ_1	1	1
ψ_2	1	−1
ψ_3	−1	1
ψ_4	−1	−1

There are four complex irreducible representations of degree 1 and $2^{m-2} - 1$ complex irreducible representations of degree 2. The four complex representations of degree 1 are obtained by letting ± 1 correspond to x and y in all possible ways. Their characters ψ_1, ψ_2, ψ_3, ψ_4 are given by Table II.

Clearly, the above representations of degree 1 are not faithful because $\rho(x^2) = \rho(1)$ in all the four cases.

Next, we consider the complex irreducible representations of degree 2. Put $\omega = e^{2\pi i/q}$, where $q = 2^{m-1}$ and let h be an arbitrary integer. We define a representation ρ^h by setting

$$[\rho^h(x^k)] = \begin{bmatrix} \omega^{hk} & 0 \\ 0 & \omega^{-hk} \end{bmatrix}$$

and

$$[\rho^h(y)] = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad \text{if } h \text{ is odd}$$

$$[\rho^h(y)] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \text{if } h \text{ is even.}$$

A direct calculation shows that this is indeed a representation. Moreover, $\rho^h = \rho^{q+h}$. The corresponding characters χ^h are given by

$$\chi^h(x^k) = \omega^{hk} + \omega^{-hk} = 2\, \cos\, \frac{2\pi hk}{q}$$

$$\chi^h(y) = 0.$$

For representations over fields of character zero, two representations are equivalent if and only if they have the same character. So, $\rho^h \cong \rho^{q-h}$. Also, for $0 \leq h \leq q/2$, we have different values of χ. But, the $h = 0$ and $h = q/2$ cases are reducible, with characters $\psi_1 + \psi_2$ and $\psi_3 + \psi_4$, respectively. On the other hand, for $0 < h < q/2$, the representation ρ^h is irreducible: since $\omega^h \neq \omega^{-h}$, the only lines stable under $\rho^h(x)$ are the coordinate axes and these are not stable under $\rho^h(y)$. Thus we have accounted for all the complex irreducible representations of Q_{2^m} (up to equivalence)—four of degree 1 and $2^{m-2} - 1$ of degree 2.

In the above representations the cases when h is even are not faithful for $\rho^h(y^2) = \rho^h(1)$. But, all the representations with h odd are faithful. We consider only these cases.

The corresponding real irreducible representations of degree 4 are

$$[\rho^h(x)] = \begin{bmatrix} \cos\, hp & -\sin\, hp & 0 & 0 \\ \sin\, hp & \cos\, hp & 0 & 0 \\ 0 & 0 & \cos\, hp & \sin\, hp \\ 0 & 0 & -\sin\, hp & \cos\, hp \end{bmatrix}$$

$$[\rho^h(y)] = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

where $p = 2\pi/q$.

Now, we note that $\rho^h(x) = \rho^1(x^h)$ and $\rho^h(y) = \rho^1(y)$ for all odd h between 0 and $q/2$. Hence, the matrices of the representation ρ^h are really the same as those of ρ^1, except that they appear in a different order. Thus the signal sets they generate for a given initial vector would be the same.

Now, if $w = (w_1, w_2, w_3, w_4)$ is any initial vector in $\mathbb{R}^4$ with norm 1 (i.e., $w_1^2+w_2^2+w_3^2+w_4^2 = 1$), such that it is not an eigenvector of any of the matrices of the representation ρ^h, we have

$$
\begin{aligned}
&[\rho^h(x^k)][w] \\
&\quad = \begin{bmatrix} \cos hkp & -\sin hkp & 0 & 0 \\ \sin hkp & \cos hkp & 0 & 0 \\ 0 & 0 & \cos hkp & \sin hkp \\ 0 & 0 & -\sin hkp & \cos hkp \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix} \\
&\quad = \begin{bmatrix} w_1 \cos hkp - w_2 \sin hkp \\ w_1 \sin hkp + w_2 \cos hkp \\ w_3 \cos hkp + w_4 \sin hkp \\ -w_3 \sin hkp + w_4 \cos hkp \end{bmatrix}
\end{aligned}
$$

and

$$
\begin{aligned}
&[\rho^h(yx^k)][w] \\
&\quad = \begin{bmatrix} 0 & 0 & -\cos hkp & \sin hkp \\ 0 & 0 & -\sin hkp & -\cos hkp \\ \cos hkp & \sin hkp & 0 & 0 \\ -\sin hkp & \cos hkp & 0 & 0 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix} \\
&\quad = \begin{bmatrix} -w_3 \cos hkp + w_4 \sin hkp \\ -w_3 \sin hkp - w_4 \cos hkp \\ w_1 \cos hkp + w_2 \sin hkp \\ -w_1 \sin hkp + w_2 \cos hkp \end{bmatrix}.
\end{aligned}
$$

Thus the distance profile of the signal set is

$$
\begin{aligned}
&d_E^2([\rho^1(x^m)][w], [\rho^1(x^n)][w]) = 2(1 - \cos(m-n)p) \\
&d_E^2([\rho^1(yx^m)][w], [\rho^1(yx^n)][w]) = 2 \\
&\quad \cdot (1 - \cos(m-n)p) \text{ for all } m \text{ and } n \\
&d_E^2([\rho^1(x^m)][w], [\rho^1(yx^n)][w]) = 2
\end{aligned}
$$

which is independent of the initial vector w, provided w is not an eigenvector of any of the matrices of the representation ρ^h. Hence, every signal set matched to Q_{2^m} would have the same Euclidean distance profile.

We have shown that, except for labeling the signal points with the elements of the group Q_{2^m}, two four-dimensional signal sets matched to Q_{2^m} are equivalent from the Euclidean distance point of view.

Caire and Biglieri [20] have defined a notion of equivalence of Euclidean distance for codes over cyclic groups. Here, we extend their notion of equivalence for the case of codes over Q_{2^m}.

Definition 1: Automorphic Euclidean-Distance (AED) equivalence: let S be a signal set matched to a generalized quaternion group Q_{2^m}, and let μ: $Q_{2^m} \longrightarrow S$ denote the matching function. Two codes C and C' over Q_{2^m} are called AED-equivalent if there exists an automorphism f of the group Q_{2^m} which maps C to C' such that the composition map $(\mu^n \circ f(\mu^n)^{-1})$ is a symmetry of S^n.

If $C' = f(C)$, then the two codes $C = \mu(C)$ and $C' = \mu(C')$ are equivalent from the Euclidean distance point of view.

It is easy to check that if S_1 and S_2 are two signal sets matched to Q_{2^m} obtained from two different initial vectors, where $\mu_1(Q_{2^m}) = S_1$, $\mu_2(Q_{2^m}) = S_2$, and C is a group code over Q_{2^m} of length n then $\mu_1^n(C)$ and $\mu_2^n(C')$ are AED-equivalent [26].

VI. Discussion

We have characterized group codes over Q_{2^m} that are obtainable as multilevel codes and discussed certain aspects of the Euclidean distance of the resulting Euclidean space codes. The characterization is the counterpart of results available in [26]–[28] for the case of multilevel group codes over dihedral groups.

It will be interesting to obtain the capacity curves by simulation for the signal sets matched to Q_{2^m} that have been described in this correspondence in line with those described in [6]–[8]. For the case of multilevel group codes over semidirect product groups an algebraic characterization is given in [13, Theorem 2]. Similar algebraic characterization for the codes discussed in this correspondence would help in understanding the algebraic structure of the codes.

References

[1] G. D. Forney, Jr., "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1241–1260, 1991.

[2] D. Slepian, "Group codes for the Gaussian channel," *Bell Syst. Tech. J.*, vol. 47, pp. 575–602, 1968.

[3] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 55–67, 1982.

[4] G. D. Forney, Jr., "Coset codes—Part I: Introduction and geometric classification," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1123–1151, 1988.

[5] D. J. S. Robinson, *A Course in the Theory of Groups.* New York: Springer-Verlag, 1982.

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

[7] R. E. Blahut, *Principles and Practice of Information Theory.* Reading, MA: Addison-Wesley, 1987, ch. 7.

[8] H. A. Loeliger, "On Euclidean space group codes," Ph.D. dissertation, Swiss Federal Inst. Technol., Zurich, Switzerland, 1992.

[9] H. Imai and S. Hirakawa, "A new multilevel coding method using error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 371–376, 1977.

[10] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On multilevel block modulation codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 965–975, 1991.

[11] ——, "On linear structure and phase rotation invariant properties of M-PSK modulation codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 164–167, 1991.

[12] G. J. Pottie and D. P. Taylor, "Multilevel codes based on partitioning," *IEEE Trans. Inform. Theory*, vol. 35, pp. 87–98, 1989.

[13] R. Garello and S. Benedetto, "Multilevel construction of block and trellis group codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1257–1264, 1995.

[14] V. V. Ginzburg, "Multidimensional signals for a continuous channel," *Probl. Pered. Inform.*, vol. 20, pp. 28–46, 1984.

[15] F. R. Kschischang, P. G. de Buda, and S. Pasupathy, "Block coset codes for M-ary phase shift keying," *IEEE J. Select. Areas Commun.*, vol. 7, pp. 900–913, 1989.

[16] M. Isaksson and L. H. Zetterberg, "Block-coded M-PSK modulation over GF (M)," *IEEE Trans. Inform. Theory*, vol. 39, pp. 337–346, 1993.

[17] C. Chen, T. Chen, and H. A. Loeliger, "Construction of linear ring codes for 6-PSK," *IEEE Trans. Inform. Theory*, vol. 40, pp. 563–566, 1994.

[18] L. H. Zetterberg and H. Brandstorm, "Codes for combined phase and amplitude modulated signals in a four-dimensional space," *IEEE Trans. Commun.*, vol. COM-25, pp. 943–950, 1977.

[19] S. I. Sayegh, "A class of optimum block codes in signal space," *IEEE Trans. Commun.*, vol. COM-34, pp. 1043–1045, 1986.

[20] G. Caire and E. Biglieri, "Linear block codes over cyclic groups," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1246–1256, 1995.

[21] T. V. Selvakumaran and N. Venkatasubramanian, "Multi-level group codes over the quaternion group and its generalizations," Masters' thesis, Indian Inst. Technol., New Delhi, India, 1996.

[22] J. P. Serre, *Linear Representations of Finite Groups.* New York: Springer-Verlag, 1977.

[23] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding.* New York: Academic, 1975.

[24] E. Biglieri and M. Elia, "Cyclic group codes for the Gaussian channel," *IEEE Trans. Inform. Theory*, vol. IT-38, pp. 624–629, 1972.

[25] T. Mittelholzer and J. Lahtonen, "Group codes generated by finite reflection groups," *IEEE Trans. Inform. Theory*, vol. 42, pp. 519–527,

1996.
[26] J. Bali and B. Sundar Rajan, "Block-coded PSK modulation using two-level group codes over dihedral groups," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1620–1631, July 1998.
[27] ____, "A class of multilevel group codes over dihedral groups with good Euclidean distance properties," presented at the Mediterranean Workshop on Coding Applications, Palma, Spring, Feb. 28–Mar. 1, 1996.
[28] ____, "On multilevel group codes over dihedral groups," in *Proc.: Nat. Conf. Communications, NCC '96* (IIT Bombay, India, Feb. 1996).

Comment on "Relations Between Entropy and Error Probability"

Jovan Dj. Golić

The first part of the above correspondence[1] contains the tight upper and lower bounds on the equivocation in terms of the Bayes error probability. The upper bound is said to be known, whereas the lower bound is claimed to be new. However, the lower bound is also known and has been independently determined in [5] and [6]. Unlike the remark from the above correspondence,[1] it is the upper bound that follows from the Kuhn–Tucker conditions, whereas the lower bound is derived from the set of extremal points of the corresponding polyhedron. The lower bound can also be found in [2], where the relationship between an arbitrary uncertainty measure and the Bayes error probability is investigated in more detail and optimal information measures with respect to certain similarity criteria are established. Other related concepts and results are given in [1] and [3]. Note that various relationship problems have been extensively studied in many papers in the area of statistical pattern recognition dealing with feature selection and extraction criteria, see [4], for example.

Manuscript received June 30, 1997; revised May 26, 1998.

The author is with the School of Electrical Engineering, University of Belgrade, 11001 Belgrade, Yugoslavia.

Communicated by A. R. Calderbank, Editor-in-Chief.
Publisher Item Identifier S 0018-9448(99)00070-X.

[1] M. Feder and N. Merhav, *IEEE Trans. Inform. Theory*, vol. 40, pp. 259–266, Jan. 1994.

References

[1] J. Dj. Golić, "On the relationship between the efficiency measures of multicategory information systems," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 531–538, July 1987.
[2] ____, "On the relationship between the information measures and the Bayes probability of error," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 681–693, Sept. 1987.
[3] ____, "On the relationship between the separability measures and the Bayes probability of errors," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 694–701, Sept. 1987.
[4] ____, "Uncertainty and similarity measures in pattern recognition," in *Proc. 26th Allerton Conf. Communication, Control, and Computing* (Monticello, IL, Sept. 1988), pp. 639–646.
[5] V. A. Kovalevsky, "The problem of character recognition from the point of view of mathematical statistics," in *Character Readers and Pattern Recognition*. New York: Spartan, 1968.
[6] D. L. Tebbe and S. J. Dwyer III, "Uncertainty and probability of error," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 516–518, May 1968.