Rotational invariance of two-level group codes over dihedral and dicyclic groups

JYOTI BALI¹ and B SUNDAR RAJAN²

¹Department of Electrical Engineering, Indian Institute of Technology, Hauz Khas, New Delhi 110016, India

²Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012, India

e-mail: jbali@ee.iitd.ernet.in; bsrajan@ece.iisc.ernet.in

Abstract. Phase-rotational invariance properties for two-level constructed, (using a binary code and a code over a residue class integer ring as component codes) Euclidean space codes (signal sets) in two and four dimensions are discussed. The label codes are group codes over dihedral and dicyclic groups respectively. A set of necessary and sufficient conditions on the component codes is obtained for the resulting signal sets to be rotationally invariant to several phase angles.

Keywords. Multilevel codes; group codes; dihedral groups; coded modulation.

1. Introduction

It is well known (Viterbi & Omura 1979; Benedetto *et al* 1987) that digital communication over Additive White Gaussian Noise (AWGN) channel can be modelled as transmission of a point from a finite set of points, called signal set, of a finite dimensional vector space and the Maximum Likelihood soft decoding then becomes choosing the closest point in the signal set, in the sense of Euclidean distance, from the received point in the space. The probability of error performance to a large extent is dominated by the minimum of the pairwise distances of the signal points. The problem of signal set design for AWGN channel then is choosing a specified number of points in a space of specified dimensions in such a way that the minimum distance is the maximum possible.

A recipe for obtaining good signal sets in large dimensions starting from a signal set of small dimension using group codes is discussed by Forney (1991). A group code over a group G is a subgroup C of G^n , n -fold direct product of G , with component-wise group operation. A signal set S 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 ,

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

where, $d_E(a, b)$ denotes the squared Euclidean distance between $a, b \in S$ and e is the identity element of G . If G and S have the same number of elements then the elements of S can be labelled with the elements of G , and such a labelling satisfying the condition (1) is referred as a matched labelling (Loeliger 1991, 1992). A signal set matched to a group has the property that the Euclidean distance distribution of the points of the signal set from any point is same, known as Uniform Error property (UEP). If S is a signal set of dimension N matched to a group G and μ is a matched labelling, then under the extended mapping

$\mu^n: G^n \rightarrow S^n$ given by $\mu^n(g_0, g_1, \dots, g_{n-1}) = (\mu(g_0), \mu(g_1), \dots, \mu(g_{n-1}))$, $\mu^n(C)$ gives a signal set in Nn dimensions, called the signal space code and this is matched to the group C . Forney (1991) has shown that such signal space codes are special cases of general class of codes known as geometrically uniform codes which have UEP. C is referred as label code of the signal space code.

Recently 'multilevel constructions' have been reported using binary codes as component codes and suitable mapping of coded bits onto a signal set of small dimension, for example a phase shift keying (PSK) signal set (Cusack 1984; Sayegh 1986; Pottie & Taylor 1989; Kschischang *et al* 1989; Kasami *et al* 1991; Calderbank & Seshadri 1993; Biglieri & Caire 1994; Garelo & Benedetto 1995; Imai & Hirakawa 1997). Multilevel construction has attracted wide spread research because of their amenability for efficient suboptimal multistage decoding (Calderbank 1989; Takata *et al* 1993; Kofman *et al* 1994). A multilevel block code of L levels uses L block codes, called component codes, of the same length n , over finite alphabets of possibly different sizes. A signal set S , called basic signal set, of dimension N , has $\prod_{i=1}^L m_i$ points, where $m_i, i = 1, 2, \dots, L$, are the size of the alphabets, with each point labelled by an ordered L -tuple with one entry from each alphabet. With this labelling, a set of L codewords, one from each code, corresponds to a point in Nn dimensions, with each coordinate of L codewords choosing a point in S . The collection of all such points corresponding to all possible combinations of codewords of the component codes is the multilevel constructed signal space code or Euclidean space code.

This paper reports rotational invariance properties of coded signal sets obtained by two-level ($L = 2$) construction for a class of two-dimensional ($N = 2$) Symmetric PSK (SPSK) and four-dimensional ($N = 4$) signal sets. Four-dimensional signal sets have been studied by several authors (Welti & Lee 1974; Zetterberg & Brandstrom 1977; Saha & Birdsall 1989; Visintin *et al* 1992). Gersho & Lawrence (1984) describe the basic theory and implementation for a particular 2-bits per dimension four-dimensional encoding which readily lends itself to simple encoding and decoding. For this encoding they predict a 1.2 dB gain in noise margin over conventional 16-point(two-dimensional) quadrature amplitude modulation (QAM) signalling. In our two-level construction the component codes used are a binary code and a linear code over a residue class integer ring. The class of SPSK signal sets considered are those matched to dihedral groups and the class of four-dimensional signal sets considered are those matched to dicyclic groups. (dihedral and dicyclic groups are described in § 2). The main results are a set of necessary and sufficient conditions on the component codes for the two-level construction to result in rotationally invariant signal sets and identification of two situations under which a label code when seen as a group code over dicyclic group results in better performance compared to when seen as group code over dihedral group.

2. Dihedral and dicyclic groups and matched labellings

The class of dihedral groups is defined by

$D_M = \{r^i s^j | r^M = s^2 = e, r^i s = s r^{-i}, 0 \leq i < M, j = 0, 1\}$ where e is the identity of D_M . The group operation can be expressed as

$$(r^{i_1} s^{j_1})(r^{i_2} s^{j_2}) = r^{i_1+i_2(1-2j_1)} s^{j_1+j_2},$$

and the inverse of an element is given by

$$(r^i s^j)^{-1} = r^{i(2j-1)} s^j.$$

This group has $2M$ elements, where M is an arbitrary integer and r and s are called the generators of D_M .

DEFINITION 1

Let S denote a unit circle in 2-dimensions. A matched labelling $\mu : D_M \rightarrow S$, for a $2M$ -asymmetric PSK signal set matched to D_M is said to be an m -labelling, $0 \leq m \leq M-1$, with angle of asymmetry ϕ , $-\pi/2M < \phi < \pi/2M$, and denoted by mL_ϕ , if

$$\begin{aligned} \mu(r^i s^j) &= \exp\{\sqrt{-1}[j((2m+1)(\pi/M)+\phi)+il2\pi/M]\}, \\ i &= 0, 1, \dots, M-1, \quad j = 0, 1, (l, M) = 1 \end{aligned}$$

Definition 1 is general and includes Asymmetric PSK(PSK) signal sets. It is shown (Bali & Rajan 1997b) that for a given group code APSK performs better than SPSK under certain conditions. In this paper, however, we will be considering only SPSK signal sets i.e., $\phi = 0$ throughout. Observe that various values of the parameter m gives different labellings of the SPSK signal set with $m = 0$ corresponding to labelling the signal points in natural order in the anticlockwise direction. Our results in this paper hold even if $m \neq 0$.

The class of dicyclic groups is defined by

$$DC_{2M} = \{r^i s^j | r^M = s^2 = (rs)^2, 0 \leq i < 2M, j = 0, 1\}.$$

This group has $4M$ elements, M being any positive integer and is generated by r and s where, $r^{2M} = e$, the identity element. The group operation can be expressed as

$$(r^{i_1} s^{j_1})(r^{i_2} s^{j_2}) = r^{(i_1+i_2+j_1(Mj_2-2i_2)) \bmod 2M} s^{(j_1+j_2) \bmod 2}$$

and the inverse of an element is given by

$$(r^i s^j)^{-1} = r^{-i+j(M+2i)} s^j$$

DEFINITION 2 (Bali & Rajan 1997b)

Let S denote the unit sphere in 4 dimensions. The matched labelling we consider is the subset of S (shown in figure 1 – the $x_1 - x_2$ plane constitutes the first two dimensions and the $x_3 - x_4$ plane constitutes the remaining two),

$$(\cos k\theta, \sin k\theta, 0, 0), (0, 0, \cos k\theta, -\sin k\theta), \quad 0 \leq k \leq 2M-1, \theta = \pi/M$$

Figure 1. A signal set matched to DC_2 .

consisting of $4M$ points and the matched labelling $\mu : DC_{2M} \rightarrow S$, is

$$\begin{aligned} \mu(r^k s^l) &= (1-l) \cos(k\pi/M), (1-l) \sin(k\pi/M), \\ &\quad l \cos(k\pi/M), -l \sin(k\pi/M). \end{aligned}$$

It is routine calculation to check that the mappings of definitions 1 and 2 indeed satisfy the conditions for matched labelling given in (1).

3. Two-level group codes and their characterization

The block diagram of a two-level block-coded modulation is shown in figure 2a. C_r and C_s are length n codes over alphabets $X = \{x_1, x_2, x_3, x_4\}$, ($m_1 = 4$) and $Y = \{y_1, y_2\}$, ($m_2 = 2$). Figure 2b shows a labelling of S consisting of eight points on the circle, with elements of X and Y . For codewords $a = (a_0, \dots, a_{n-1}) \in C_1$ and $b = (b_0, \dots, b_{n-1}) \in C_2$, each pair (a_i, b_i) , $i = 0, 1, \dots, n-1$, selects a point in S , and the pair (a, b) specifies a point in $2n$ dimensions. The collection of all such points in $2n$ dimensions corresponding to all possible pairs of codewords constitute the two-level block coded modulation code (signal set) or signal space code. This paper deals with X and Y being Z_2 and Z_λ , residue class integers modulo 2 and modulo λ respectively, where $\lambda = M$ for codes over D_M and $\lambda = 2M$ for codes over DC_{2M} .

DEFINITION 3

Let C_s and C_r be length n codes over respectively, $Z_2 = \{0, 1\}$ and $Z_\lambda = \{0, 1, \dots, \lambda-1\}$, and $a = (a_0, \dots, a_{n-1}) \in C_s$, $b = (b_0, \dots, b_{n-1}) \in C_r$. Let $c_{a,b}$ denote

$$(r^{b_0} s^{a_0}, r^{b_1} s^{a_1}, \dots, r^{b_{n-1}} s^{a_{n-1}}) \in D_\lambda^n (\text{or } DC_\lambda^n)$$

The subset $\{c_{a,b} | a \in C_s, b \in C_r\}$ of D_λ^n (or DC_λ^n), denoted by $r^{C_r} s^{C_s}$, is called the two level code over D_λ (or DC_λ) with component codes C_s and C_r . If $r^{C_r} s^{C_s}$ is a subgroup of D_λ^n (or DC_λ^n) then it is called a two-level group code and is denoted by C . The signal space code obtained with C as the label code and a matched labelling μ will be denoted by $\mu^n(C)$.

Figure 2. (a) Block diagram of a two-level block coded modulation. (b) Labelling of an 8-PSK signal set with X and Y .

Bigleiri & Caire (1994) have studied the Geometrical Uniformity properties of signal space codes obtained by L -level construction. The component codes used are L linear binary codes with the 2^L -ary SPSK as the basic signal set. The points of the PSK signal set can be designated with either the cyclic group with 2^L elements or with the dihedral group with 2^L elements. They derive conditions under which the resulting multilevel code is a group code over the cyclic or dihedral group.

In the rest of the section we give the necessary and sufficient conditions on the component codes of the two-level construction shown in figure 2a to result in a group code over D_M and DC_{2M} .

Theorem 1 (Bali & Rajan 1997a, 1998). *The two-level code $C = r^{C_r} s^{C_s}$ is a group code over D_M if and only if*

- (i) C_s and C_r are linear codes over Z_2 and Z_M respectively, and
- (ii) $C_s \odot 2C_r \subseteq C_r$ if M is even and $C_s \odot C_r \subseteq C_r$, if M is odd, where, $\odot$ denotes pointwise product.

In theorem 1, M is an arbitrary integer. When M is a power of 2, say, $M = 2^{L-1}$, and C_r is decomposable in terms of $L-1$ linear binary codes $C_1, C_2, \dots, C_{L-1}$, i.e., it can be

obtained as

$$C_r = C_1 + 2C_2 + \cdots + 2^{L-2}C_{L-1},$$

then theorem 1 coincides with theorem 1 of Bigleiri & Caire (1994).

Proof of theorem 1 and the Euclidean distance properties of the resulting symmetric and asymmetric PSK signal space codes can be seen in Bali & Rajan (1998).

Example 1. If $C_r = Z_M^n$, i.e., if C_r is the trivial code consisting of all possible n -tuples over Z_M , then for any binary linear code C_s , conditions of theorem 1 are satisfied and hence the resulting code is a group code over D_M .

Example 2. If C_s is a repetition code consisting of all zero and all one vectors only and C_r is any linear code over Z_M , then conditions of theorem 1 are satisfied and hence the code is a group over D_M .

Example 3. Let $C_s = \{000, 111\}$ and $C_r = \{000, 220, 132, 312, 200, 020, 332, 112\}$ over Z_4 . Then the resulting two-level code is a group code over D_4 and has the following 16 codewords

$$\begin{aligned} & \{(r^0, r^0, r^0), (r^2, r^2, r^0), (r^1, r^3, r^2), (r^3, r^1, r^2), \\ & (r^2, r^0, r^0), (r^0, r^2, r^0), (r^3, r^3, r^2), (r^1, r^1, r^2), \\ & (s, s, s), (r^2s, r^2s, s), (r^1s, r^3s, r^2s), (r^3s, r^1s, r^2s), \\ & (r^2, s, s), (s, r^2s, s), (r^3s, r^3s, r^2s), (r^1s, r^1s, r^2s)\}. \end{aligned}$$

Observe that in this example, M is a power of 2, but C_r is a non-decomposable code.

Example 4. Let $C_r = \{0000, 1233, 3211, 0222, 1011, 2022, 3033, 2200\}$ over Z_4 and $C_s = \{0000, 1111\}$. For these codes $C_s \odot 2C_r = \{0000, 2022\} \subseteq C_r$. Therefore, the two-level code $r^{C_r} s^{C_s}$ is a group code over D_4 and the codewords are:

$$\begin{aligned} & (1111), (1, r^2, r^2, r^2), (r^3, r^2, r, r), (r, r^2, r^3, r^3), \\ & (r, 1, r, r), (r^2, r^2, 1, 1), (r^3, 1, r^3, r^3), (r^2, 1, r^2, r^2), \\ & (s, s, s, s), (s, r^2s, r^2s, r^2s), (r^3s, r^2s, rs, rs), \\ & (rs, r^2s, r^3s, r^3s), (rs, s, rs, rs), (r^2s, r^2s, s, s), \\ & (r^3s, s, r^3s, r^3s), (r^2, 1, r^2, r^2), \end{aligned}$$

The following theorem gives the necessary and sufficient conditions on the component codes of the two-level construction shown in figure 2a to result in a group code over DC_{2M} .

Theorem 2 (Bali & Rajan 1997b). *The two-level code $C = r^{C_r} s^{C_s}$ is a group code over DC_{2M} if and only if*

- (i) C_s and C_r are linear codes over Z_2 and Z_M respectively.
- (ii) $C_s \odot 2C_r \subseteq C_r$, where $\odot$ denotes pointwise product.
- (iii) $M(C_s \odot C_s) \subseteq C_r$.

The proof is similar to that of theorem 1 and is omitted. We list below a few classes of group codes over DC_λ .

Example 5. If $C_r = Z_{2\lambda}^n$, i.e., if C_r is the trivial code consisting of all possible n -tuples over $Z_{2\lambda}$, then for any binary linear code C_s , conditions of theorem 1 are satisfied and hence the resulting code is a group code over DC_λ .

Example 6. If C_s is a repetition code consisting of all zero and all one vectors only then conditions of theorem 1 are satisfied for any linear code over $Z_{2\lambda}$ containing all $-\lambda$ codeword, as C_r code.

Example 7. Let C_s be any binary code with the property $C_s \odot C_s \subseteq C_s$ and C_r is the parity check code over $Z_{2\lambda}$. Then the resulting two-level code is a group code over DC_λ .

Notice that when all the three conditions of theorem 1 are satisfied for a set of component codes then these can be used to construct both group codes over the dihedral group as well as group codes over the dicyclic group. The resulting coding gain when used as dihedral group code is given by

$$G_D = d_D/4 \sin^2(\pi/2^R),$$

and when used as dicyclic group code is given by

$$G_\lambda = d_{DC}/4 \sin^2(\pi/2^{R/2})$$

where d_D and d_{DC} denote the MSED of the signal space codes of dihedral and dicyclic group codes respectively and R denotes the rate of the code in bits per channel use (Kschischang *et al* 1989).

Theorems 3 and 4 below identify two situations for component codes satisfying conditions of both theorems 1 and 2; labelling with dicyclic groups gives better performance compared to labelling with dihedral groups.

Theorem 3. *If C_s is a (n, k, d_s) binary linear code with $C_s \odot C_s \subseteq C_s$ and $C_r = Z_{2M} \cdot C_s$, then, the two-level code construction will give group code over both D_M and DC_{2M} . For such a pair of component codes*

$$(i) \quad \text{If } 2 \cos(\pi/4M) > \Gamma(R), \quad (2)$$

where $\Gamma(R) = \sin(\pi/2^{R/2})/\sin(\pi/2^R)$ then, $G_\lambda > G_D$.

$$(ii) \quad \text{If } R > 2.68 \text{ then, } G_D > G_\lambda.$$

Proof. (i) We have the Hamming distance of $C_r = d_s$. Using this, $d_D = 4d_s \sin^2(\pi/4M)$ and $d_{DC} = 4d_s \sin^2(\pi/2M)$ Using these values in the expressions for gain above, it is easy to check that $G_\lambda > G_D$ translates to (2).

(ii) Cosine function is upper bounded by 1 therefore, the LHS of (2) can be at most equal to 2. $G_D > G_\lambda$ if $\Gamma(R) > 2 \cos(\pi/4M)$. If $R > 2.68$ then $\Gamma(R) > 2$, hence $G_D > G_\lambda$.

Theorem 4. If C_s is a $(n, n/2, 2)$ binary code (n even) with generator matrix of the form

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 1 & 1 \end{bmatrix}$$

and C_r is $(n, n-1, 2)$ $2M$ -ary parity check code then, $G_\lambda > G_D$ if $2 \cos(\pi/4M) > \sin(\pi/2^{R/2})/\sin(\pi/2^R)$.

Proof. It is easy to verify that the component codes in the statement of the theorem satisfy conditions of both theorems 1 and 2. The rest of the proof is similar to that of part (i) of theorem 3. $\square$

Example 8. Consider the case $n = 8$, $M = 2$ in theorem 4. Then, $R = 9/4 = 2.25$ bits/symbol,

$G_D = 2 \sin^2(\pi/8)/\sin^2(\pi/2^{2.25}) = 0.7782735$ (-1.0886775 dB) and $G_\lambda = 2 \sin^2(\pi/4)/\sin^2(\pi/2^{2.25/2}) = 1.0171907$ (0.0740239 dB) $> G_D$.

4. Phase rotational invariance

For L-level codes with binary component codes phase invariance properties have been reported (Kasami *et al* 1994a). In this section we discuss phase rotational invariance properties of two-level group codes over D_M and DC_{2M} .

For mL of a $2M$ -SPSK signal set, a codeword

$$(r^{y_0} s^{x_0}, r^{y_1} s^{x_1}, \dots, r^{y_i} s^{x_i}, \dots, r^{y_{n-1}} s^{x_{n-1}}) \in C, \quad (3)$$

is mapped onto the point

$$\begin{aligned} & \exp\{\sqrt{-1}[x_0((2m+1)\pi/M) + y_0 2\pi/M]\}, \dots, \\ & \exp\{\sqrt{-1}[x_i((2m+1)\pi/M) + y_i 2\pi/M]\}, \dots, \\ & \exp\{\sqrt{-1}[x_{n-1}((2m+1)\pi/M) + y_{n-1} 2\pi/M]\}, \end{aligned} \quad (4)$$

in $2n$ -dimensional space. There is a one-one correspondence between codewords and $2n$ -dimensional points given by (3) and (4). The code is said to be rotationally invariant to an angle θ , if whenever (4) is a signal point for a codeword in C , then the vector corresponding to

$$\begin{aligned} & \exp\{\sqrt{-1}[x_0((2m+1)\frac{\pi}{M}) + y_0 2\pi/M + \theta]\}, \dots, \\ & \exp\{\sqrt{-1}[x_i((2m+1)\pi/M) + y_i 2\pi/M + \theta]\}, \dots, \\ & \exp\{\sqrt{-1}[x_{n-1}((2m+1)\pi/M) + y_{n-1} 2\pi/M + \theta]\}, \end{aligned}$$

is a codeword in C . The following theorem gives the conditions on the component codes for a two-level group code over D_M to be invariant to different angles of rotations including the minimum angle.

Theorem 5. For mL of a $2M$ -SPSK signal set, $\mathbf{C} = \mathbf{r}^{C_r} \mathbf{s}^{C_s}$ is invariant to

- (i) $k(2\pi/M)$, rotations where k divides M , iff the all- k vector $(k, k, \dots, k) \in C_r$,
- (ii) $k(2\pi/M)$, rotations where k and M are relatively prime, iff the all-1 vector $(1, 1, \dots, 1) \in C_r$,
- (iii) π/M rotations iff all-1 vector is present in C_r and C_s .

Proof.

- (i) Let $M/k = \lambda$. Then replacing y_i by $y_i + \lambda$, $i = 0, 1, \dots, n-1$, in (3) corresponds to θ in (4) getting replaced by $\lambda 2\pi/M$, and the converse.
- (ii) If k and M are relatively prime, then $k 2\pi/M$ rotations can be obtained by k successive $2\pi/M$ rotations and $2\pi/M$ rotations can be obtained by u successive $k 2\pi/M$ rotations where u is given by $uk + vM = 1$ (Bezout's Theorem). Hence it is sufficient to consider $2\pi/M$ rotations only for which all-1 vector $(1, 1, \dots, 1)$ should be in C_r , which follows from (i) with $\lambda = M$.
- (iii) Suppose all-1 vectors are present in both C_r and C_s . Presence of all-1 vector in C_s guarantees rotational invariance by $(2m+1)\pi/M = m 2\pi/M + \pi/M$. The presence of all-1 vector in C_r guarantees rotational invariance by all multiples of $2\pi/M$, including $-m 2\pi/M$. Clearly, rotational invariance for both $m 2\pi/M + \pi/M$ and $-m 2\pi/M$ implies rotational invariance for π/M . The converse is straightforward. $\square$

For a $4n$ -dimensional signal set obtained using a two level group code over DC_{2M} , a codeword

$$\mathbf{r}^{y_0} \mathbf{s}^{x_0}, \mathbf{r}^{y_1} \mathbf{s}^{x_1}, \dots, \mathbf{r}^{y_i} \mathbf{s}^{x_i}, \mathbf{r}^{y_{n-1}} \mathbf{s}^{x_{n-1}} \in C \quad (5)$$

is mapped onto the point

$$\begin{aligned} & (1 - x_0) \exp\{\sqrt{-1}[y_0\pi/M]\}, x_0 \exp\{\sqrt{-1}[-y_0\pi/M]\}, \dots \\ & (1 - x_i) \exp\{\sqrt{-1}[y_i\pi/M]\}, x_i \exp\{\sqrt{-1}[-y_i\pi/M]\}, \dots \\ & (1 - x_{n-1}) \exp\{\sqrt{-1}[y_{n-1}\pi/M]\}, x_{n-1} \exp\{\sqrt{-1}[-y_{n-1}\pi/M]\} \end{aligned} \quad (6)$$

in $4n$ -dimensional space. There is a one-one correspondence between codewords of the group code given by (5) and $4n$ -dimensional points given by (6). The code is said to be rotationally invariant to an angle θ , if whenever (6) is a signal point for a codeword in C , then the codeword corresponding to

$$\begin{aligned} & (1 - x_0) \exp\{\sqrt{-1}[y_0\pi/M+\theta]\}, x_0 \exp\{\sqrt{-1}[-y_0\pi/M+\theta]\}, \dots \\ & (1 - x_i) \exp\{\sqrt{-1}[y_i\pi/M+\theta]\}, x_i \exp\{\sqrt{-1}[-y_i\pi/M+\theta]\}, \dots \\ & (1 - x_{n-1}) \exp\{\sqrt{-1}[y_{n-1}\pi/M+\theta]\}, x_{n-1} \exp\{\sqrt{-1}[-y_{n-1}\pi/M+\theta]\} \end{aligned}$$

is a codeword in C . The following theorem give the conditions on the component codes for a two-level group code over DC_{2M} to be invariant to different angles, the proof of which is similar to that of theorem 5 and hence omitted.

Theorem 6. A two-level group code, $C = r^{C_r} s^{C_s}$ over DC_{2M} is invariant to

- (i) $k(\pi/M)$, rotations where k divides M , iff the all k vector $(k, k, \dots, k) \in C_r$,
- (ii) $k(\pi/M)$, rotations where k and M are relatively prime, iff the all-1 vector $(1, 1, \dots, 1) \in C_r$,

Notice that the minimum angle of rotational invariance in this case is π/M whereas for 2M-SPSK it is $2\pi/M$. Moreover, the C_s code plays no role in the conditions of rotational invariance, i.e., the minimal angle of rotational invariance is completely determined by the C_r code.

5. Conclusion

Rotational invariance properties of signal space codes obtained by group codes over dihedral groups and dicyclic groups are discussed. The group codes are those obtainable by two-level construction from a binary code and a code over residue class integer ring. The signal space codes obtained from group codes over dihedral group codes are in $2n$ dimensions and those obtained from dicyclic group codes are in $4n$ dimensions where n is the length of the code. Theorem 3 includes conditions under which the codes are invariant to the minimum angle for dihedral group codes. If the component codes satisfy the conditions of the theorem then the effect of phase ambiguity in carrier recovery in multiples of $2\pi/M$ can be nullified by two-stage differential encoding as follows: After the encoder (and before the modulator) the sequence of symbols to be transmitted is of the form $(\dots, y_{i-1}x_{i-1}, y_i x_i, y_{i+1}x_{i+1}, \dots)$ where $(\dots, x_{i-1}, x_i, x_{i+1}, \dots)$ is the corresponding binary sequence and $(\dots, y_{i-1}, y_i, y_{i+1}, \dots)$ is the corresponding sequence over Z_M . (i) First differentially encode the binary sequence $\{x_i\}$ resulting in the sequence, say, $\{x'_i\}$. After this the original sequence becomes $(\dots, y_{i-1}x'_{i-1}, y_i x'_i, y_{i+1}x'_{i+1}, \dots)$. (ii) Now the above sequence can be seen as the interleaved version of two subsequences where the first subsequence, say $S_0 = \{y_j x'_j\}$, consists of those symbols with $x'_j = 0$ and the second, say $S_1 = \{y_j x'_j\}$, consists of those symbols with $x'_j = 1$. Now differentially encode modulo M , the $\{y_j\}$ parts of the each subsequence.

It is straightforward to verify that by two stage differential decoding procedure, in the reverse order of encoding, the effects of phase rotations by multiple of the angle $2\pi/M$ can be removed.

Theorem 4 includes conditions under which the codes are invariant to the minimum angle for dicyclic group codes. If the component codes satisfy the conditions of the theorem then the effect of phase ambiguity in carrier recovery in multiples of π/M can be nullified by differential encoding as in the dihedral group code case without the first stage encoding; i.e., differential encoding of binary symbols is not needed for due to rotations of the signal set binary components do not get affected.

The authors wish to thank E Biglieri, H A Loeliger, F R Kschischang and R Garello for sending the preprints of their work. This work was supported by Council of Scientific and Industrial Research through a fellowship to Jyoti Bali.

References

- Bali J, Rajan B S 1997a Block coded asymmetric PSK modulation using two-level group codes over dihedral groups. *IEEE International Symposium on Information Theory*, Ulm, Germany
- Bali J, Rajan B S 1997b Two-level group codes over four dimensional signal sets. *Proc. 1997 National Conf. on Communications*, pp 101–105
- Bali J, Rajan B S 1998 Block coded PSK modulation using two-level group codes over dihedral groups. *IEEE Trans. Info. Theory* 44: (in press)
- Bendetto S, Biglieri E, Castellani V 1987 *Digital transmission theory* (Englewood Cliffs, NJ: Prentice-Hall)
- Biglieri E, Caire C 1994 Symmetry properties of multilevel coded modulation. *IEEE Trans. Info. Theory* 40: 1630–1632
- Calderbank A R 1989 Multilevel codes and multistage decoding. *IEEE Trans. Commun.* 37: 222–229
- Calderbank A R, Seshadri N 1993 Multilevel codes for unequal error protection. *IEEE Trans. Info. Theory* 39: 1234–1248
- Cusack E L 1984 Error control coding for QAM signalling. *Electron. Lett.* 20: 62–63
- Forney G D 1991 Geometrically uniform codes. *IEEE Trans. Info. Theory* 37: 1241–1260
- Garello R, Bendetto S 1995 Multilevel construction of block and trellis group codes. *IEEE Trans. Info. Theory* 41: 1257–1264
- Gershon A, Lawrence V B 1984 Multidimensional signal constellations for voiceband data transmission. *IEEE J. Selected Areas in Commun.* 2: 687–702
- Imai H, Hirakawa S 1977 A new multilevel coding method using error correcting codes. *IEEE Trans. Info. Theory* 23: 371–377
- Kasami T, Takata T, Fujiwara T, Lin S 1991a On linear structure and phase rotation invariant properties of block M-PSK modulation codes. *IEEE Trans. Info. Theory* 37: 164–167
- Kasami T, Takata T, Fujiwara T, Lin S 1991b On multilevel block modulation codes *IEEE Trans. Info. Theory* 37: 965–975
- Kofman Y, Zehavi E, Shamai S 1994 Performance analysis of a multilevel coded modulation system. *IEEE Trans. Commun.* 42: 299–312
- Kschischang F R, de Buda P G, Pasupathy S 1989 Block codes for M-ary phase shift keying. *IEEE J. Selected Areas in Commun.* 7: 900–913
- Loeliger H A 1991 Signal sets matched to groups. *IEEE Trans. Info. Theory* 37: 1675–1682
- Loeliger H A 1992 *On Euclidean space group codes*. Ph D thesis, Swiss Federal Institute of Technology, Zurich
- Pottie G J, Taylor D P 1989 Multilevel codes based on partitioning. *IEEE Trans. Info. Theory* 35: 87–98
- Saha D, Birdsall T 1989 Quadrature-quadrature phase-shift keying. *IEEE Trans. Commun.* 37: 437–448
- Sayegh S I 1986 A class of optimum block codes in signal space. *IEEE Trans. Commun.* 34: 1043–1045
- Takata T, Ujita S, Kasami T, Lin S 1993 Multistage decoding of multilevel block M-PSK modulation codes and its performance analysis. *IEEE Trans. Info. Theory* 39: 1204–1218
- Visintin M, Biglieri E, Castellani V 1992 Four-dimensional signalling for bandlimited channels. *IEEE Trans. Commun.* 40: 21–34
- Viterbi A J, Omura J K 1979 *Principles of digital communications and coding*, Int. edn (New York: McGraw-Hill)

- Welch G R, Lee J S 1974 Digital transmission with coherent four-dimensional modulation. *IEEE Trans. Info. Theory* 20: 497–502
- Zetterberg L H, Brandstrom H 1977 Codes for combined phase and amplitude modulated signals in a four-dimensional space. *IEEE Trans. Commun.* 25: 943–950