

However, for the lower bound on  $d$  in Corollary 2.6, we have

$$d - d_{\text{true}} \geq \frac{q^2 - q - 3 - (2 + \log_q e)m}{4 + \log_q e} - (q - 1).$$

Therefore, our codes certainly improve the true minimum distance of the one-point Hermitian codes up to

$$\frac{q^2 - q - 3 - (4 + \log_q e)(q - 1) - (2 + \log_q e)m}{4 + \log_q e}$$

for

$$m \leq (q^2 - q - 3 - (4 + \log_q e)(q - 1))/2 + \log_q e.$$

This implies that we can improve the bound up to  $O(q^2)$  for a certain range of  $m$ .

### III. SOME TABLES

In Tables II–VI, we calculate the improved codes from Proposition 2.1 and Corollary 2.6, and compare them with the true distances of one-point Hermitian codes of [12] having the same lengths and dimensions.

In Tables II–V, some improved codes for  $q = 4, 5, 7, 8$  from Proposition 2.1 are calculated and listed. Table VI is from Corollary 2.6.

It is obvious that when  $q$  becomes larger, there are more improved codes and the difference  $d_{\text{improved}} - d_{\text{true}}$  becomes larger. This phenomenon can be easily observed from Tables IV–VI.

### REFERENCES

- [1] G.-L. Feng and T. R. N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distances," *IEEE Trans. Inform. Theory*, vol. 39, pp. 37–45, Jan. 1993.
- [2] V. D. Goppa, "Codes on algebraic curves," *Sov. Math.-Dokl.*, vol. 24, no. 1, pp. 170–172, 1981.
- [3] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1720–1732, Nov. 1995.
- [4] H. Niederreiter and C. P. Xing, "Low-discrepancy sequences and global function fields with many rational places," *Finite Fields Their Applic.*, vol. 2, pp. 241–273, 1996.
- [5] H.-G. Rück and H. Stichtenoth, "A characterization of Hermitian function fields over finite fields," *J. Reine Angew. Math.*, vol. 457, pp. 185–188, 1994.
- [6] H. Stichtenoth, "A note on Hermitian codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1345–1348, Sept. 1988.
- [7] —, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1993.
- [8] M. A. Tsfasman and S. G. Vlăduț, *Algebraic-Geometric Codes*. Dordrecht, The Netherlands: Kluwer, 1991.
- [9] H. J. Tiersma, "Remarks on codes from Hermitian curves," *IEEE Trans. Inform. Theory*, vol. 33, pp. 605–609, July 1987.
- [10] C. P. Xing, "On automorphism groups of Hermitian codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1629–1635, Nov. 1995.
- [11] —, "Algebraic geometry codes with asymptotic parameters better than the Gilbert–Varshamov and Tsfasman–Vlăduț–Zink bounds," *IEEE Trans. Inform. Theory*, vol. 47, pp. 347–352, Jan. 2002.
- [12] K. Yang and P. V. Kumar, "On the true minimum distances of Hermitian codes," in *Lecture Notes in Mathematics*. New York: Springer-Verlag, 1991, vol. 1518, pp. 99–107.

## Gilbert–Varshamov Bound for Euclidean Space Codes Over Distance-Uniform Signal Sets

B. Sundar Rajan, *Senior Member, IEEE*,  
L. Venkata Subramaniam, *Member, IEEE*, and  
Rajendar Bahl, *Member, IEEE*

**Abstract**—In this correspondence, in extension of Piret’s bound for codes over phase-shift keying (PSK) signal sets, we investigate the application of the Gilbert–Varshamov (GV) bound to a variety of distance-uniform (DU) signal sets in Euclidean space. It is shown that four-dimensional signal sets matched to binary tetrahedral, binary octahedral, and binary icosahedral groups lead to better bounds compared to the bounds for signal sets matched to dicyclic groups with the same number of signal points and comparable symmetric PSK signal sets.

**Index Terms**—Euclidean space codes, Gilbert–Varshamov (GV) bound, group codes, multilevel construction, signal sets matched to groups, uniform signal sets.

### I. INTRODUCTION

For codes designed for the Hamming distance, the asymptotic Gilbert–Varshamov (GV) bound gives an achievable lower bound on the normalized rate of the code for a specified normalized Hamming distance. For a length- $n$  code  $C$  over a  $q$ -ary alphabet with minimum Hamming distance  $d_H(C)$ , the asymptotic GV bound [21] is given by

$$R(\delta_H) = 1 - H_q(\delta_H) \tag{1}$$

where

$$R(\delta_H) = \lim_{n \rightarrow \infty} (1/n) \log_q |C|$$

is the normalized rate and

$$\delta_H = \lim_{n \rightarrow \infty} (1/n) d_H(C)$$

is the normalized distance, and  $H_q(x)$  is the generalized entropy function given by

$$H_q(x) = -x \log_q \left( \frac{x}{q-1} \right) - (1-x) \log_q (1-x)$$

where  $0 \leq x \leq \left(\frac{q-1}{q}\right)$ . In this correspondence, in extension of Piret’s bound [17] for codes over phase-shift keying (PSK) signal sets, we investigate the application of the GV bound to a variety of distance-uniform (DU) signal sets in Euclidean space [6], [14]. A signal set is said to be DU if the Euclidean distance distribution of all the points in the signal set from a particular point is the same from any signal point. Examples of DU signal sets are all binary signal sets, symmetric PSK signal sets, orthogonal signal sets, simplex signal sets, hypercubes in any dimension, and signal sets matched to groups [13], [14]. A signal

Manuscript received October 18, 1999; revised August 22, 2001. This work was supported in part by CSIR, India, under Research Grants (25(0086)/97/EMR-II) and (22(0298)/99/EMR-II) to B. S. Rajan.

B. S. Rajan is with the Department of Electrical Communication Engineering and the Department of Computer Science and Automation, Indian Institute of Science, Bangalore 560012, India (e-mail: bsrajan@ece.iisc.ernet.in).

L. V. Subramaniam is with the IBM India Research Laboratory, Indian Institute of Technology, Delhi 110016, India (e-mail: lvsufram@in.ibm.com).

R. Bahl is with the Center for Applied Research in Electronics, Indian Institute of Technology, Delhi 110016, India (e-mail: rbahl@care.iitd.ernet.in).

Communicated by F. R. Kschischeng, Associate Editor for Coding Theory. Publisher Item Identifier S 0018-9448(02)00312-7.

set  $S$  is said to be matched to a group  $G$  if there exists a mapping  $\mu$  from  $G$  onto  $S$  such that for all  $g$  and  $g'$  in  $G$

$$d_E(\mu(g), \mu(g')) = d_E(\mu(g^{-1}g'), \mu(e)) \quad (2)$$

where  $d_E(x, y)$  denotes the squared Euclidean distance (SED) between  $x, y \in S$  and  $e$  is the identity element of  $G$ . Signal sets matched to groups constitute an important ingredient in the construction of geometrically uniform codes [6] and those matched to noncommutative groups have been shown [13] to be superior to signal sets matched to commutative groups in terms of having capacity exceeding the PSK limit [3]. Existence of DU signal sets not matched to any group is shown in [20]. In terms of probability of error, if the signal set  $S = \{s_0, s_1, \dots, s_{M-1}\}$  is matched to a group then the probability of error when  $s_i$  is transmitted is independent of  $i$ , whereas if it is DU then only the union bound is independent of  $i$ .

A version of the GV bound that yields geometrically uniform codes was given by Loeliger [16]. This bound applies for signal sets matched to the additive group of a finite field (elementary Abelian groups), for example,  $M$ -PSK when  $M$  is prime and for simplex signal sets with power of a prime number of signal points. Piret [17] has obtained an asymptotic lower bound for codes over symmetric PSK signal sets for Euclidean distance of the signal space code and has shown that i) the asymptotic GV bound for  $q = 2$  and  $q = 3$  is obtainable from the bounds for 2-PSK and 3-PSK signal sets and ii) his bound for  $M = 4$  is obtainable by multiplying by 2 the corresponding values of the case for  $M = 2$ ; no such match exists with the GV bound for  $M \geq 5$ .

The present correspondence begins by stating a general version of the GV bound that is applicable to any DU signal set. We then use this bound to investigate a variety of DU signal sets in Euclidean space like Hamming spaces [12] and signal sets matched to groups. In particular, we consider two-, three-, and four-dimensional signal sets matched to groups and compare them in terms of this bound. Among symmetric PSK and asymmetric PSK we show that the symmetric PSK signal set leads to a better bound. In three dimensions, we consider the Massey signal set [13] and obtain the GV bound for different parameters. We also show that, among the four-dimensional signal sets matched to dicyclic, binary tetrahedral, binary octahedral, and binary icosahedral groups, signal sets matched to dicyclic groups lead to smaller GV bound compared to signal sets matched to the remaining three groups for the same number of signal points. Also, we compare signal sets in different dimensions in terms of this bound based on spectral rate.

A class of Euclidean space codes is said to be asymptotically good if, for a fixed normalized SED, the normalized rate of the code is bounded away from zero as the length of the code approaches infinity. Using the well-known distance bound due to Ginzburg [9], we point out (Theorem 2) that certain multilevel constructions [10], [11] give good classes of Euclidean space codes.

The correspondence is organized as follows. In Section II, we present a version of the GV bound (Theorem 1) applicable to any DU signal set and specialize it to simplex signal sets and Hamming spaces. Application of the GV for various signal sets in two, three, and four dimensions matched to groups and their comparison based on the bound normalized with respect to dimension constitute Section III. Section IV deals with construction of good Euclidean space codes by multilevel construction. Concluding remarks constitute Section V and the modifications of the Piret's proof leading to the bound of Theorem 1 are presented in the Appendix.

## II. GV BOUND FOR DU SIGNAL SETS

The following theorem is a version of the GV bound that applies to any DU signal set.

*Theorem 1:* Let  $S$  be an  $M$ -point DU signal set. Let the set of SEDs, called SED distribution, of all the signal points from any particular point be  $\{d^2(r), r = 0, 1, \dots, M-1\}$ . Then, the number of codewords  $|C|$  in the largest code  $C \subset S^n$  with minimum squared Euclidean distance (MSED) at least  $n\delta^2$  satisfies

$$\frac{1}{n} \ln |C| \geq \ln M - H(\underline{\beta}(\mu)) \quad (3)$$

where  $\underline{\beta}(\mu)$  is the distribution  $\{\beta_r(\mu), r = 0, 1, \dots, M-1\}$  given by

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}} \quad (4)$$

and the parameter  $\mu$  is determined by the condition

$$\delta^2 = \sum_{s=0}^{M-1} \beta_s(\mu) d^2(s). \quad (5)$$

*Proof:* Let

$$V_n(\lambda^2) = |\{x \in S^n : |x - x_0|^2 < \lambda^2\}|$$

be the number of points inside a sphere of radius  $\lambda$  around some fixed point  $x_0 \in S^n$ . Then

$$|C| V_n(n\delta^2) \geq |S|^n \quad (6)$$

which is the Gilbert bound: if the balls of radius  $n\delta^2$  around all codewords do not cover the whole signal space, the code could be augmented by at least one codeword. As shown in [15], we also have

$$V_n(n\delta^2) \leq b^{nH(\underline{\beta})} \quad (7)$$

where  $\underline{\beta}$  is the probability distribution defined in (4) and (5) and  $b$  is the base of the logarithm in the definition of  $H(\underline{\beta})$ . Combining (6) and (7) yields (3).  $\square$

The asymptotic version of Theorem 1 along with the proof obtained by using modifications in Piret's proof [17] is given in the Appendix. Henceforth, we refer to the bound given by (3) as the extended GV (EGV) bound.

For simplex signal sets of size  $q$ , for any given point, the remaining  $(q-1)$  signal points are at the same SED. If a  $q$ -ary alphabet is used to designate the  $q$  points then for any chosen point the remaining  $(q-1)$  points are at the same Hamming distance. This suggests that the EGV bound for simplex signal sets and the classical GV bound are the same up to scaling of the distance.

*Corollary 1 (Simplex Signal Sets):* For all values of  $q$ , the GV bound given in (1) can be obtained from the EGV bound when specialized to codes over simplex signal sets up to a scaling factor.

*Proof:* For simplex signal sets we have  $d^2(r) = K$  if  $r \neq 0$ , and moreover

$$\sum_{r=0}^{M-1} e^{-\mu d^2(r)} = 1 + \sum_{r=1}^{M-1} e^{-\mu K} = 1 + (M-1)e^{-\mu K}. \quad (8)$$

Using (8) in (4) we have

$$\begin{aligned} \beta_0(\mu) &= \frac{1}{1 + (M-1)e^{-\mu K}}; \\ \beta_r(\mu) &= \frac{e^{-\mu K}}{1 + (M-1)e^{-\mu K}} \\ &= e^{-\mu K} \beta_0(\mu), \quad \text{if } r \neq 0. \end{aligned} \quad (9)$$

Moreover, (5) gives, utilizing that  $\sum_{r=0}^{M-1} \beta_r(\mu) = 1$

$$\beta_0(\mu) = 1 - \frac{\delta}{K}, \quad \beta_r(\mu) = \left( \frac{1}{M-1} \right) \frac{\delta}{K}; \quad r \neq 0. \quad (10)$$

Using (10) in (3) and choosing

$$K = 2M/(M-1) \quad (11)$$

and after substituting

$$\delta/K = \delta_H \quad (12)$$

(3) coincides with (1) but for the base of the logarithm. Note that the ranges also coincide, since

$$\begin{aligned} 0 \leq \delta_H &\leq \frac{(M-1)}{M} \\ \Rightarrow 0 \leq \frac{\delta}{K} &\leq \frac{(M-1)}{M} \\ \Rightarrow 0 \leq \delta &\leq \frac{(M-1)}{M} K = 2. \quad \square \end{aligned}$$

The substitutions given by (11) and (12) can be combined to obtain the relation between the normalized SED in the EGV bound and the normalized Hamming distance in the classical GV bound to give  $\delta[\frac{(M-1)}{2M}] = \delta_H$ . This is the scaling factor by which the plot of classical GV bound can be obtained from the EGV bound and *vice versa*.

A signal set is said to form an  $m$ th-order  $q$ -ary Hamming space [12] if there exists a labeling of the signal set with  $q$ -ary  $m$ -tuples with the property that the SED between any two signal points is proportional to the Hamming distance between the corresponding labels. Notice that the symmetric 4-PSK set forms a second-order binary Hamming space and, more generally, the  $N$ -dimensional cube is an  $N$ th-order binary Hamming space. In Corollary 2, we obtain the EGV bound for Hamming spaces.

*Corollary 2 (Hamming Spaces):* Let  $S$  be an  $m$ th-order  $q$ -ary Hamming space. Then

$$R_L(S, \delta) = m(1 - H_q(\delta[(q-1)/2q])). \quad (13)$$

*Proof:* Since  $S$  is an  $m$ th-order  $q$ -ary Hamming space, it has  $q^m$  points. Let  $S'$  be the subset of  $S$  such that the labels of elements of  $S'$  differ only in one fixed coordinate.  $S'$  is a simplex signal set consisting of  $q$  signal points. Codes of length  $n$  over  $S$  can be considered as codes of length  $mn$  over  $S'$ . Hence, we have

$$R_L(S, \delta) = mR_L(S', \delta) = \text{right-hand side of (13)}.$$

Note that  $S'$  is a simplex signal set consisting of  $q$  points, hence  $R_L(S', \delta)$  is given by Corollary 1.  $\square$

Since a simplex signal set with  $M$  points is a first-order  $M$ -ary Hamming space, Corollary 2 is a generalization of Corollary 1. Applying Corollary 2 to the  $N$ -dimensional hypercube, the EGV bound obtained is  $R_L(S, \delta) = NR_L(S'', \delta)$ , where  $S''$  is a one-dimensional hypercube, i.e., the binary antipodal signal set.

*Example 1:* The three-dimensional cube is a third-order binary Hamming space. Taking the points to be on a unit sphere the SED distribution from (000) is  $\{0, 4/3, 4/3, 8/3, 4/3, 8/3, 8/3, 4\}$ . The EGV bound for codes over this cube is  $3(1 - H_2(\delta/4))$ . Similarly, for the four-dimensional cube the EGV bound is  $4(1 - H_2(\delta/4))$ .

### III. EGV BOUND FOR SIGNAL SETS MATCHED TO GROUPS IN TWO, THREE, AND FOUR DIMENSIONS

In this section, we apply the EGV bound to investigate two-, three-, and four-dimensional signal sets matched to groups.

#### A. Two-Dimensional Signal Sets Matched to Groups

The two classes of signal sets in two dimensions matched to groups are those matched to cyclic groups (symmetric PSK (SPSK)) and those matched to dihedral groups (asymmetric PSK (APSK)). Several authors have studied codes over APSK signal sets [1], [2], [5], [7]. The dihedral group  $D_{2M}$  with  $2M$  elements generated by two of its elements  $r$  and  $s$  with identity element  $e$  is

$$D_{2M} = \left\{ r^i s^j \mid r^M = s^2 = e, r^i s = s r^{-i}, 0 \leq i < M, j = 0, 1 \right\}$$

and the group operation can be expressed as

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

In general, such signal sets are matched to  $D_{2M}$  under the mapping

$$\mu(r^i s^j) = e^{\sqrt{-1}(j\pi/M + \theta + 2\pi i/M)}$$

where  $\theta$  is the angle of asymmetry. Fig. 1(a) shows the general  $2M$ -APSK signal set matched to  $D_{2M}$ . Fig. 1(b) shows the EGV bound for codes over 8-SPSK as well as 8-APSK signal sets for seven different angles of asymmetry. The uppermost curve in the bundle of curves in Fig. 1(b) corresponds to 8-SPSK and the bottom-most to 8-APSK with angle of asymmetry  $10^\circ$ . The intermediate curves correspond to values of angle of asymmetry as listed in the figure. As the angle of asymmetry is increased the curve moves up toward the 8-SPSK curve. Notice also that as the angle of asymmetry increases the APSK signal set tends more and more toward SPSK signal set. The corresponding plots for 16-SPSK and 16-APSK were seen to have similar patterns. Three observations from these plots are as follows:

- 1) signal sets matched to cyclic groups (SPSK) give better bound than signal sets matched to dihedral groups (APSK) with the same number of elements;
- 2) for APSK signal sets, the EGV bound gives a better distance as the angle of asymmetry increases; and
- 3) as the number of points in the signal set increases, the bounds differ only for smaller values of normalized distance, i.e., the range of values of  $\delta$  for which the bounds for symmetric and asymmetric PSK are the same increases.

Although these observations are based on 8- and 16-point signal sets it is conjectured that these are true for PSK signal sets with any even number of points.

#### B. Three-Dimensional Signal Sets Matched to Groups

Loeliger [13] has discussed a class of three-dimensional signal sets observed by Massey with points on a unit sphere matched to cyclic groups with even number of elements which we refer as Massey signal sets. Fig. 2(a) shows a Massey signal set, with parameter  $r$ , matched to a cyclic group with eight elements. In general, a Massey signal set with  $2M$  points has its points on two circles parallel to the  $x$ - $y$  plane separated by a distance  $2r$  along the  $z$ -axis, with  $M$  points on each circle. The points on each circle constitute an  $M$ -SPSK signal set with one  $M$ -SPSK signal set when projected onto the other circle forming another  $M$ -SPSK signal set which is a rotated version of the other one by  $\pi/M$ . The points on each circle are indexed by  $\{0, 2, \dots, 2M-2\}$  and  $\{1, 3, \dots, 2M-1\}$  in the anticlockwise direction. It is easy to check that this signal set is matched to the cyclic group of integers modulo  $2M$  under the natural mapping. In the next section, we show

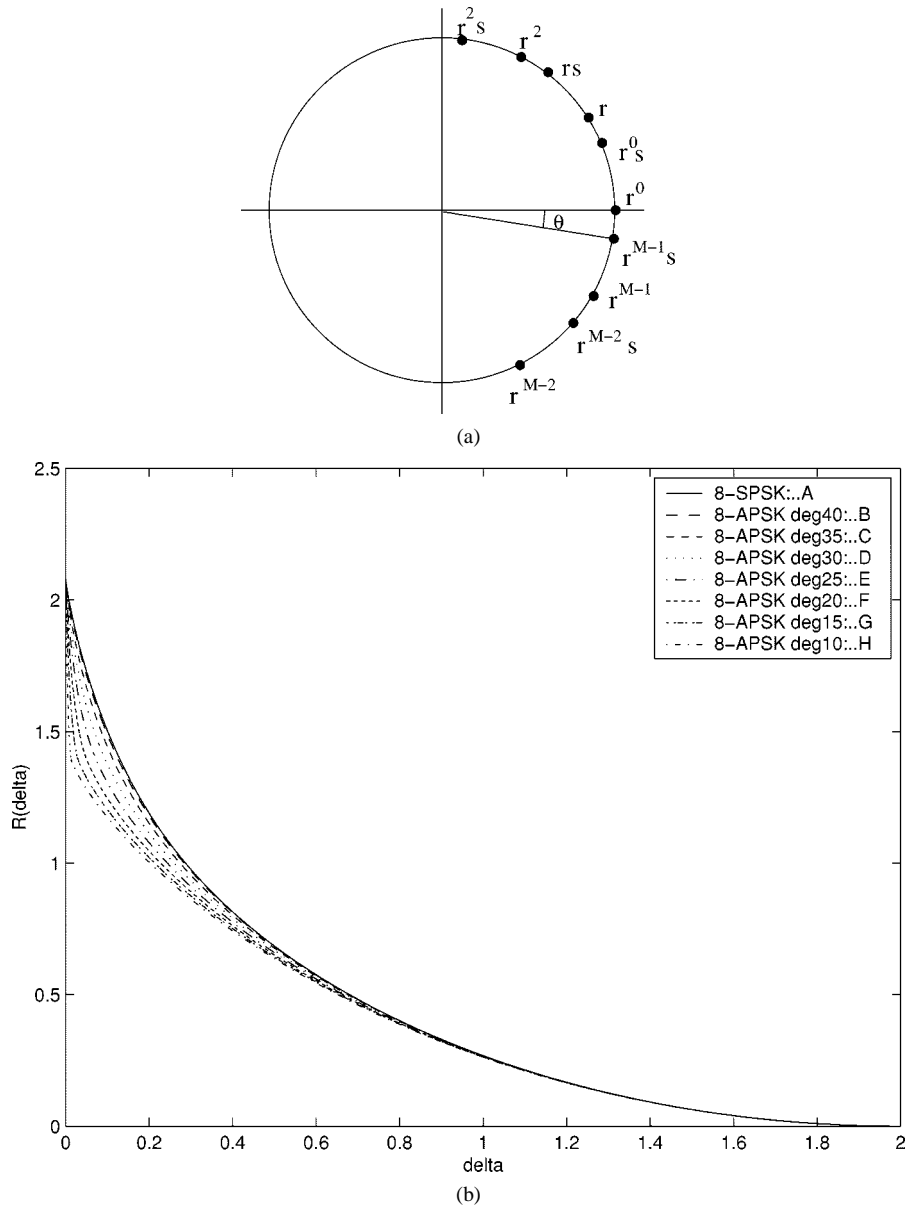


Fig. 1. (a) The general  $2M$ -APSK signal set matched to  $D_{2M}$ . (b) EGV bound for codes over 8-SPSK and 8-APSK (for different angles).

that the Massey signal set with eight points is superior to 8-SPSK and three-dimensional cube in terms of having a better bound.

For  $M = 64$ , Fig. 2(b) shows the EGV bound for several values of  $r$ . From Fig. 2(b), it is seen that the best bound depends on the normalized distance. For instance, the curve for  $r = 0.5$  intersects with the curves for all other values shown in the figure. For  $M = 8$ , also there is no unique value of  $r$  for which the bound is tighter than for all other values of  $r$ . For this case, it was observed that the bounds for values of  $r$  between 0.53 and 0.58, in steps of 0.01, intersect pairwise. However, for values  $r = 0.2, 0.4, 0.6$ , and  $0.8$  it was observed that for any pair of values of  $r$ , one bound lies above the other for the entire range of the normalized distance. For  $M = 8$ , with  $r = 0.6$  the curve appears in Fig. 5.

### C. Bounds for Four-Dimensional Signal Sets Matched to Groups

Modulation schemes with four-dimensional signal sets have been studied by several authors [13], [24], [4], [19], [8], [18], [22], [23]. Gersho and Lawrence [8] describe the basic theory and implementation for a particular lattice type, four-dimensional signal set, which readily

lends itself to simple encoding and decoding with around 1.2-dB gain in noise margin over the conventional two-dimensional 16-point QAM signaling. Moreover, a four-dimensional signal set matched to a non-commutative group with 7200 signal points has been observed to have higher capacity than the PSK limit [13]. In this subsection, we apply the EGV bound for four-dimensional signal sets matched to dicyclic, binary tetrahedral, binary octahedral, and binary icosahedral groups. The class of signal sets matched to dicyclic groups includes those matched to the quaternion group and generalized quaternion groups since these two are special cases of dicyclic groups. These groups are simply described in terms of the quaternions as follows. The elements of the set

$$H = \{\sigma = a\underline{e} + b\underline{j} + c\underline{k} + d\underline{l} \mid a, b, c, d \in R : a^2 + b^2 + c^2 + d^2 = 1\}$$

where  $R$  denotes the field of real numbers and  $\underline{e}$ ,  $\underline{j}$ ,  $\underline{k}$ , and  $\underline{l}$  are the vectors satisfying

$$\begin{aligned} \underline{i}^2 = \underline{j}^2 = \underline{k}^2 = -\underline{e}, \quad \underline{j}\underline{k} = -\underline{k}\underline{j} = \underline{l}, \quad \underline{k}\underline{l} = -\underline{l}\underline{k} = \underline{j}, \\ \underline{l}\underline{j} = -\underline{j}\underline{l} = \underline{k}, \quad \text{and} \quad \sigma \cdot \underline{e} = \underline{e} \cdot \sigma = \sigma, \quad \forall \sigma \in H. \end{aligned}$$

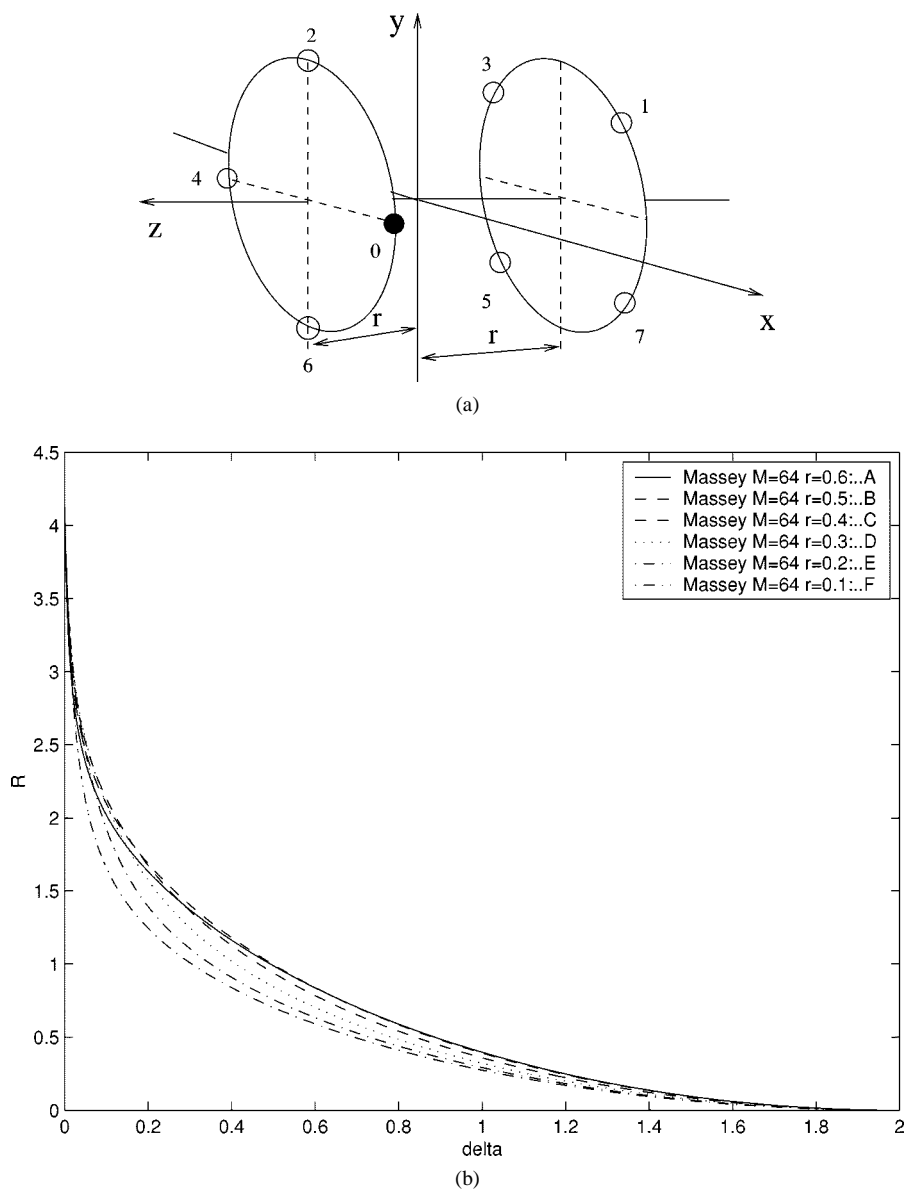


Fig. 2. (a) The Massey signal set for  $M = 8$ . (b) EGV bound for codes over Massey signal sets for  $M = 64$ .

In the infinite noncommutative group  $H$ , multiplication of two elements  $(a_1\underline{e} + b_1\underline{j} + c_1\underline{k} + d_1\underline{l})$  and  $(a_2\underline{e} + b_2\underline{j} + c_2\underline{k} + d_2\underline{l})$  results in  $(a_3\underline{e} + b_3\underline{j} + c_3\underline{k} + d_3\underline{l})$  where

$$[a_3 \ b_3 \ c_3 \ d_3] = [a_1 \ b_1 \ c_1 \ d_1] \begin{bmatrix} a_2 & b_2 & c_2 & d_2 \\ -b_2 & a_2 & -d_2 & c_2 \\ -c_2 & d_2 & -a_2 & b_2 \\ -d_2 & -c_2 & -b_2 & -a_2 \end{bmatrix}.$$

The groups of interest to us are the following finite subgroups of  $H$ .

- 1) **Dicyclic Groups  $DC_{4M}$** : The subgroup of  $H$  with  $4M$  elements, ( $M$ -arbitrary positive integer)

$$\sigma_v = (\cos(\pi v/M), \sin(\pi v/M), 0, 0),$$

$$v = 0, 1, \dots, 2M - 1$$

and

$$\tau_v = (0, 0, \cos(\pi v/M), \sin(\pi v/M)),$$

$$v = 2M, 2M + 1, \dots, 4M - 1.$$

The special case  $M = 2$  gives the quaternion group  $Q_8 = \{\pm\underline{e}, \pm\underline{j}, \pm\underline{k}, \pm\underline{l}\}$  with eight elements.

- 2) **The Binary Tetrahedral Group  $G_{24}$** : This group with 24 elements consists of  $Q_8$  and the two cosets  $\omega Q_8$  and  $\omega^2 Q_8$  of  $Q_8$ , where

$$\omega = \frac{1}{2}(\underline{e} + \underline{j} + \underline{k} + \underline{l}).$$

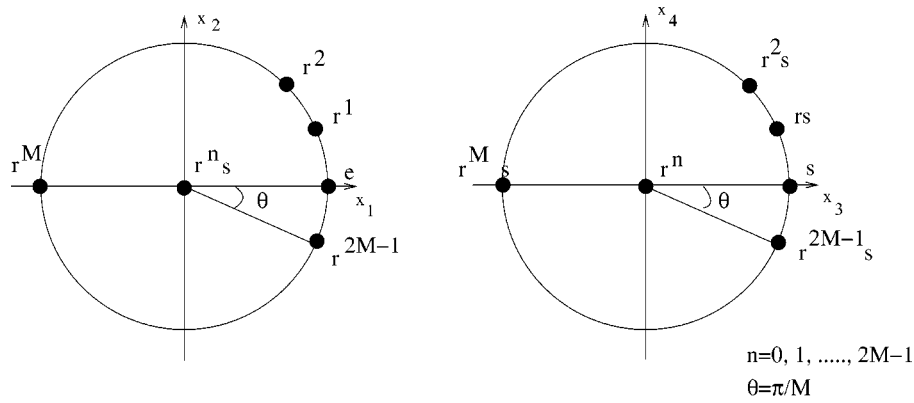
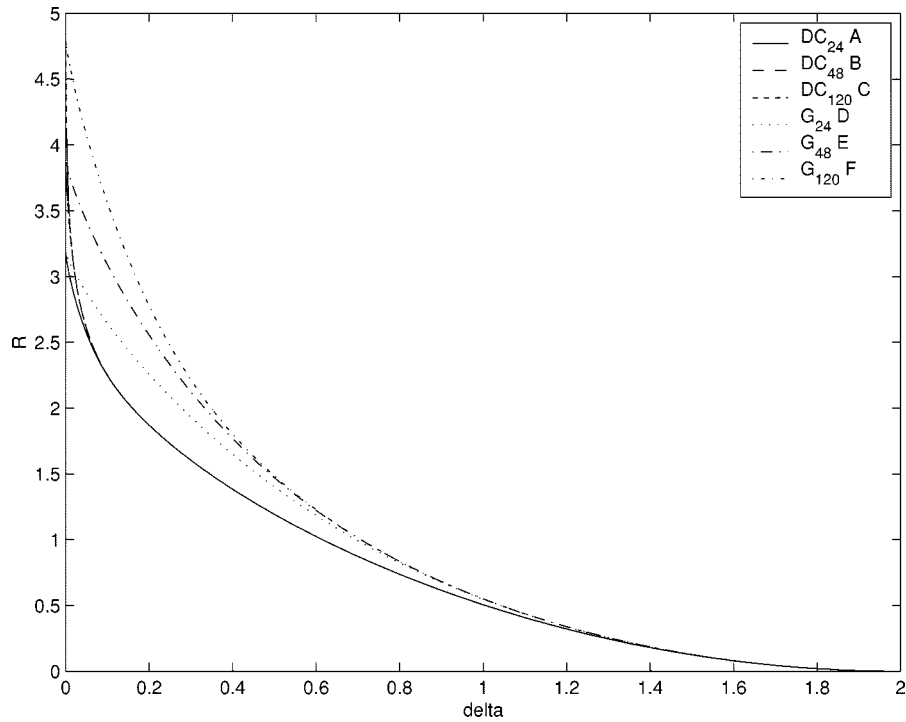
Note that  $\omega^3 = (-\underline{e}) \in Q_8$ . Explicitly, we have  $G_{24} = Q_8 \cup \omega Q_8 \cup \omega^2 Q_8$ .

- 3) **The Binary Octahedral Group  $G_{48}$** : This group with 48 elements is obtained by adding  $G_{24}$  and its coset  $\omega_1 G_{24}$  where

$$\omega_1 = \frac{1}{\sqrt{2}}(\underline{e} + \underline{j})$$

i.e.,  $G_{48} = G_{24} \cup \omega_1 G_{24}$ .

- 4) **The Binary Icosahedral Group  $G_{120}$** : This group consists of 120 elements and is obtainable as elements generated by

Fig. 3. Signal set matched to  $DC_{4M}$ .Fig. 4. EGV bound for the signal sets,  $DC_{24}$  (A),  $DC_{48}$  (B),  $DC_{120}$  (C),  $G_{24}$  (D),  $G_{48}$  (E),  $G_{120}$  (F).

the following three generators:  $\sigma_1 = \frac{1}{2}(\gamma \underline{e} + \gamma^{-1} \underline{j} + \underline{l})$ ,  $\sigma_2 = \frac{1}{2}(\underline{e} + \gamma^{-1} \underline{k} + \gamma \underline{l})$  and  $\sigma_3 = \underline{l}$ , where  $\gamma = \frac{1}{2}(1 + \sqrt{5})$ .

Fig. 3 shows four-dimensional signal sets matched to  $DC_{4M}$ . Figures for four-dimensional signal sets matched to binary tetrahedral group with 24 elements, binary octahedral group with 48 elements, binary icosahedral group with 120 elements, and other numerous groups can be seen in [4]. Note that a signal point is specified by four coordinates with the first two coordinates in the  $x_1$ - $x_2$  plane and the other two in the  $x_3$ - $x_4$  plane. The mapping that matches these signal sets to the respective groups is the common mapping  $\mu(a\underline{e} + b\underline{j} + c\underline{k} + d\underline{l}) = (a, b, c, d)$ , which can be easily verified to satisfy (2).

From the EGV bound for signal sets matched to dicyclic groups of different order (curves not shown in the correspondence), it was observed that for larger values of the normalized distance the number of points in the signal set does not matter and when a smaller normalized distance is the requirement, a larger number of points in the signal set are desirable; an observation which is true for SPSK signal sets as pointed out in [17]. The existence of  $DC_{24}$ ,  $DC_{48}$ , and  $DC_{120}$  makes these directly comparable with  $G_{24}$ ,  $G_{48}$ , and  $G_{120}$ , respectively, in terms of their bounds, as shown in Fig. 4. The bounds for codes over

$DC_{48}$  and  $DC_{120}$  appear indistinguishable. As seen from this set of bounds, signal sets matched to a binary tetrahedral group, a binary octahedral group, and a binary icosahedral group give better bounds than signal sets matched to dicyclic groups with the same number of signal points.

#### D. Comparison of Signal Sets Based on Spectral Rate

For band-limited applications, the rate of the code per dimension is the appropriate parameter based on which signal sets are to be compared. To facilitate this we measure the rate of the code per two dimensions, i.e.,

$$\frac{2}{N} R(C) = \frac{2}{Nn} \ln |C|$$

and call it the spectral rate (rate in bits per symbol per two dimensions) of the code. In this subsection, we compare the signal sets based on the spectral rate.

It immediately follows from the closed-form expression for the bound (given following Corollary 2), for any  $N$ -dimensional cube that for all values of  $N$ , the  $N$ -dimensional cube has the same spectral rate

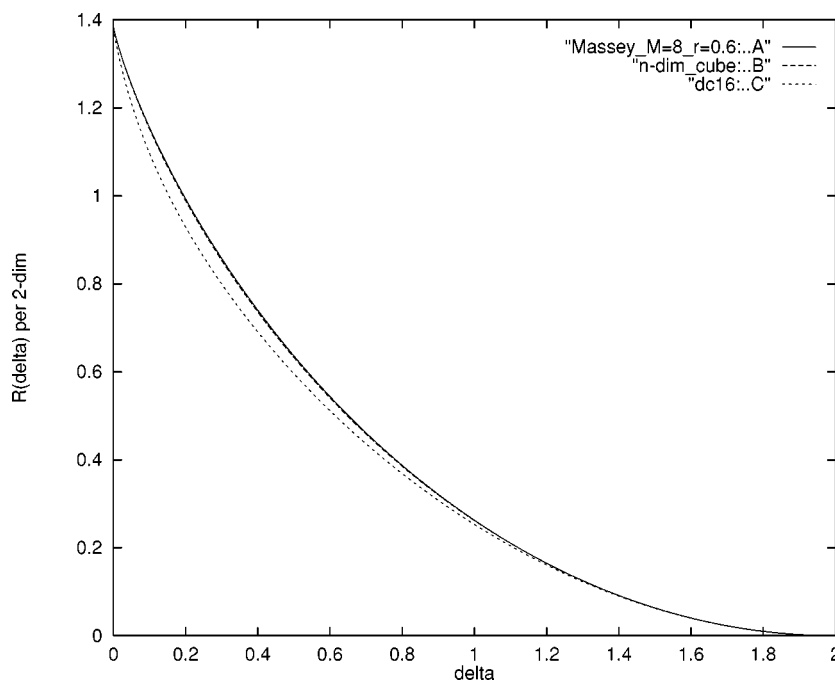


Fig. 5. EGV bound for the signal sets, Massey  $r = 0.6$  with eight elements in three dimensions (A), the  $n$ -dimensional cube (B), and dicyclic with 16 elements (C).

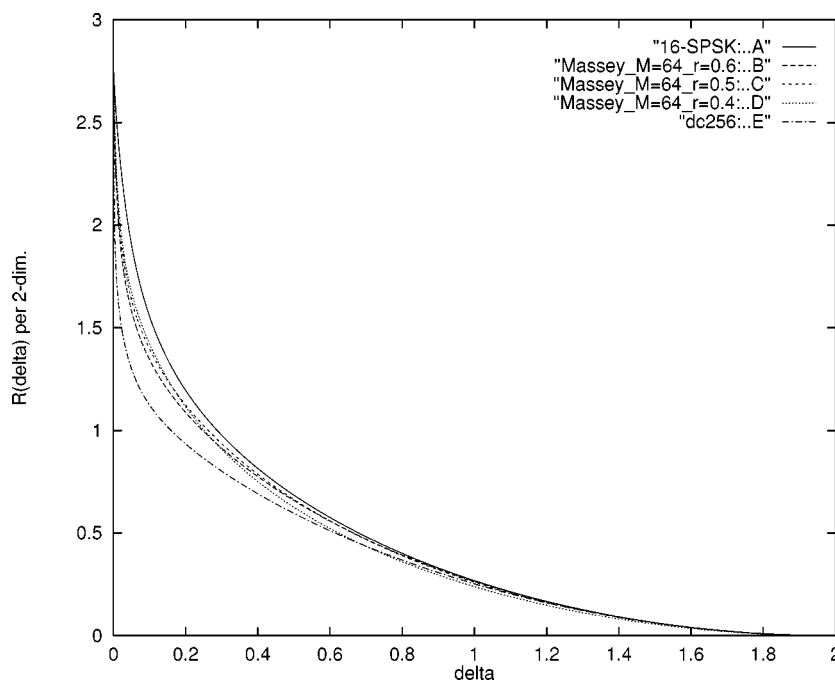


Fig. 6. EGV bound for the signal sets, Massey with 64 elements in three dimensions ( $r = 0.6$  (B),  $r = 0.5$  (C),  $r = 0.4$  (D)), cyclic with 16 elements (16-SPSK) (A), and dicyclic with 256 elements (E).

as that of 4-SPSK. Fig. 5 shows the normalized EGV bound for the Massey signal set with eight elements, any  $N$ -dimensional cube, and the signal set matched to  $DC_{16}$ . Notice that the comparison is made among signal sets of different sizes in different dimensions but having the same number of signal points per dimension. For the Massey signal set, the parameter  $r$  is chosen to be 0.6. It is seen from Fig. 5 that the Massey signal set gives a better normalized bound compared to the other two. In particular, the Massey signal set with eight points has a better bound than 4-SPSK. However, this superiority of the Massey signal set over the corresponding SPSK signal set is not true in general.

For instance, the Massey signal set with 64 points is not superior in comparison to the 16-SPSK signal set. This is demonstrated in Fig. 6. However, the supremacy of both the Massey signal set and the SPSK signal set over the corresponding signal set matched to dicyclic groups holds in this case as well. Note that the value of  $r$  that gives the best bound for the 64-point Massey signal set is not unique; depending on the value of  $\delta$ , values between 0.4 and 0.6 for  $r$  gives the best bound. The 16-SPSK gives a larger value for spectral rate for all values of  $\delta$ .

Fig. 7 shows the EGV bound for a spectral rate of signal sets matched to  $G_{24}$  and  $DC_{24}$ . The bound corresponding to 5-SPSK is also shown.

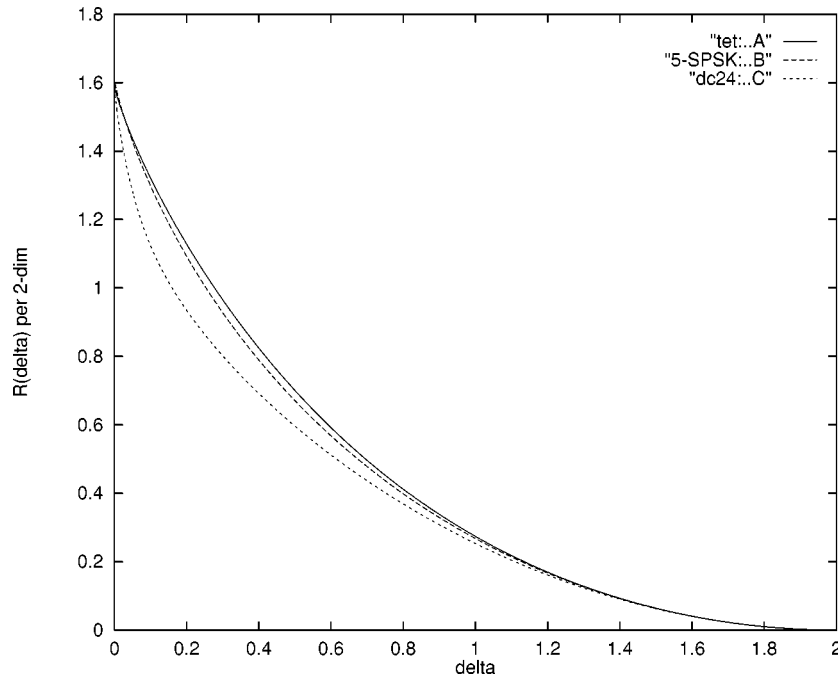


Fig. 7. EGVB bound for the signal sets,  $G_{24}$  in four dimensions (A), dicyclic with 24 elements in four dimensions (C), and cyclic with five elements (5-SPSK) (B).

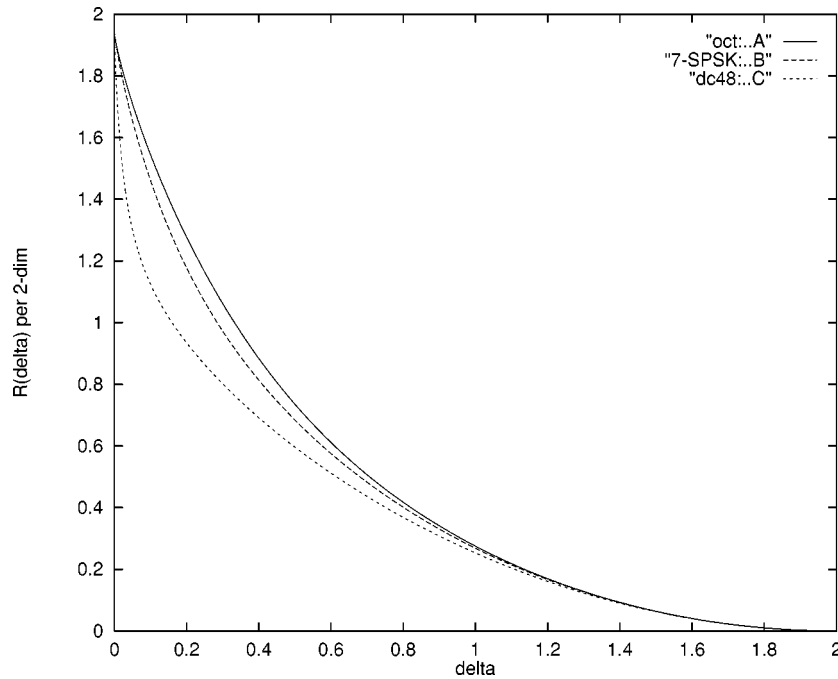


Fig. 8. EGVB bound for the signal sets,  $G_{48}$  in four dimensions (A), dicyclic with 48 elements in four dimensions (C), and cyclic with seven elements (7-SPSK) (B).

Note that the 5-SPSK signal set has a slightly higher rate. It has 25 points in four dimensions compared to 24 for the other two signal sets considered. This amounts to a slight advantage in favor of 5-SPSK. In spite of this, the signal set matched to  $G_{24}$  gives a tighter bound than the 5-SPSK signal set. Clearly,  $G_{24}$  gives larger values compared to signal sets matched to  $DC_{24}$ . Similar bounds for comparison between signal sets matched to  $G_{48}$ ,  $DC_{48}$ , and the closest SPSK signal set, 7-SPSK, are shown in Fig. 8, leading to a similar conclusion. The closest SPSK signal set that can be compared with signal sets matched to  $G_{120}$  and  $DC_{120}$  is the 11-SPSK signal set. Fig. 9 shows the bounds for these signal sets with an identical conclusion.

#### IV. ASYMPTOTICALLY GOOD EUCLIDEAN SPACE CODES

A class of Euclidean space codes is said to be good if, as the length of the code approaches infinity, neither the normalized rate nor the normalized distance approach zero. In this section, we show that in a multilevel construction [9]–[11] of Euclidean space codes, by choosing each component code from a class of asymptotically good Hamming distance codes, one obtains asymptotically good Euclidean space codes.

An  $L$ -level multilevel construction of a Euclidean space code over a signal set  $S$  uses a number  $L$  of block codes  $C_i$ , called component codes, of size  $M_i$  over alphabets  $A_i$  of size  $q_i$ ,  $i = 1, 2, \dots, L$ , each

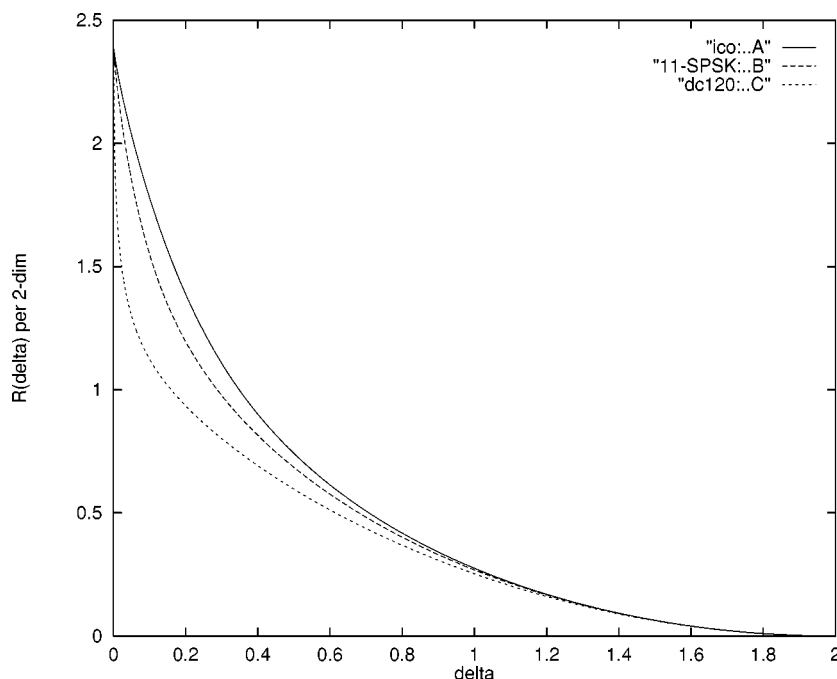


Fig. 9. EGV bound for the signal sets,  $G_{120}$  in four dimensions (A), dicyclic with 120 elements in four dimensions (C), and cyclic with 11 elements (11-SPSK) (B).

of length  $n$ . The size of the signal set is  $M = \prod_{i=1}^L q_i$ , so that each signal point can be labeled with an ordered  $L$ -tuple  $(a_1, a_2, \dots, a_L)$  where  $a_i \in A_i$ ,  $i = 1, 2, \dots, L$ . A set of  $L$  codewords, one from each of the codes  $C_i$ , specifies a signal point in the Euclidean space code as described in the following. Let  $(a_{j1}, a_{j2}, \dots, a_{jn}) \in C_j$ ,  $j = 1, 2, \dots, L$ , be the  $L$  codewords. Each of the  $n$  ordered  $L$ -tuples  $(a_{1i}, a_{2i}, \dots, a_{Li})$  specify a signal point in  $S$  and the  $L$  codewords together specify a sequence of  $n$  points from  $S$ . The collection of all such  $n$ -length sequences over  $S$  corresponding to all possible combinations of codewords from component codes constitute the Euclidean space code. Notice that the resulting Euclidean space code is in  $nN$  dimensions if the dimension of  $S$  is  $N$ . If each of the component codes are from a class of codes, then corresponding to each choice of code in that class we get a Euclidean space code—thus, a class of codes for each component code to choose from specifies a class of Euclidean space codes. Theorem 2 uses the well-known distance bound by Ginzburg [9] to show that if the class of codes from which the component codes are asymptotically good in Hamming distance, then the multilevel construction will lead to an asymptotically good class of Euclidean space codes.

*Theorem 2:* In a multilevel construction, if all the component codes are from an asymptotically good class for Hamming distance, then the resulting class of Euclidean space codes will be asymptotically good.

*Proof:* Let the component code  $C_i$  have Hamming distances  $\delta_{H_i}$ ,  $i = 1, 2, \dots, L$ . First, partition the signal space  $S$  into  $q_1$  subsets where each subset consists of the signal points whose first component in the label is the same. Recall that each signal point in  $S$  is labeled with an ordered  $L$ -tuple  $(a_1, a_2, \dots, a_L)$  where the  $i$ th component  $a_i$  is from  $A_i$  of size  $q_i$ ,  $i = 1, 2, \dots, L$ . Let the subsets of the partition be

$$\{S_{a_1=0}, S_{a_1=1}, \dots, S_{a_1=q_1-1}\}.$$

Let

$$\delta_l = \min_{\{j,k\}} \{d^2(x,y) | x \in S_{a_1=j}, y \in S_{a_1=k}, j \neq k\}$$

where  $d^2(x, y)$  denotes the SED between  $x$  and  $y$ . Notice that  $\delta_l$  is the intersubset distance of the first-level partition. Now carry out the

partition based on the second component of the label for each subset in the first-level partition as above and proceed iteratively for  $L$  levels of partition. For the  $i$ th level of partition denote the intersubset distance by  $\delta_i$ ,  $i = 1, 2, \dots, L$ . It is well known [9] that

$$\delta \geq \min_{1 \leq i \leq L} \{\delta_{H_i} \delta_i\}$$

where  $\delta$  is the MSED of the resulting Euclidean space code. From the above it follows that

$$\frac{\delta}{n} \geq \min_{1 \leq i \leq L} \left\{ \left( \frac{\delta_{H_i}}{n} \right) \delta_i \right\}.$$

The normalized rate of the Euclidean space code is

$$\frac{R}{n} = \sum_{i=1}^L \frac{\ln(M_i)}{n}.$$

Now if each component code is from an asymptotically good class of codes then both  $\frac{\delta_{H_i}}{n}$  and  $\frac{\ln(M_i)}{n}$  are bounded away from zero for all  $i$  as  $n$  tends to infinity. This implies that both  $\frac{\delta}{n}$  and  $\frac{R}{n}$  are bounded away from zero for all  $i$  as  $n$  tends to infinity.  $\square$

## V. CONCLUSION

In this correspondence, in extension of Piret's work, the application of an extended version of the GV bound to a variety of DU signal sets in Euclidean space has been investigated. Some of the possible directions for further research are as follows.

- 1) In Section III, it has been observed for 8- and 16-PSK signal sets that introduction of asymmetry of any angle matched to dihedral groups gives a smaller bound. It is conjectured that it is true for any even-number PSK signal sets. It will be interesting to attempt a proof of this conjecture.
- 2) An important direction to pursue is to identify the conditions on the component codes in the multilevel construction that will result in Euclidean space codes that exceed the EGV bound.
- 3) A natural problem to attempt is to classify the known classes of Euclidean space codes in terms of asymptotic goodness.

APPENDIX  
ASYMPTOTIC VERSION OF THEOREM 1

**Theorem 3:** Let  $S$  be an  $M$ -point DU signal set with SED distribution  $\{d^2(r), r = 0, 1, \dots, M-1\}$ . For  $C$ , a length- $n$  code over  $S$  let

$$\delta(C) = \frac{1}{n} d^2(C) \quad R(C) = \frac{1}{n} \ln |C|$$

and

$$R(\delta) = \lim_{n \rightarrow \infty} \sup_{|C| \geq n; \delta(C) \geq \delta} R(C).$$

Then a lower bound  $R_L(S, \delta)$  on  $R(C)$  is given by

$$R_L(S, \delta) = \ln(M) - H(\underline{\beta}(\mu)), \quad 0 \leq \delta \leq 2 \quad (14)$$

where  $\underline{\beta}(\mu)$  is the distribution  $\{\beta_r(\mu), r = 0, 1, \dots, M-1\}$  given by (4) and the parameter  $\mu$  is determined by the condition given in (5).

*Proof:* Let  $\{s_0, s_1, \dots, s_{M-1}\}$  be the signal set  $S$ , and let the ordered vector  $\underline{d} = (d(0), d(1), \dots, d(M-1))$  denote the Euclidean distance profile of  $S$  from  $s_0$ . Let  $\phi_r, r = 0, 1, \dots, M-1$ , be a permutation on  $S$  such that  $\phi_r(s_r) = s_0$  and  $\phi_r(s_u) = s_v, u, v = 0, 1, \dots, M-1$ , where the SED between  $s_r$  and  $s_u$  is  $d^2(v)$ . Such a permutation exists since  $S$  is DU. For any  $\underline{x} = (x_0, x_1, x_2, \dots, x_n)$  and  $\underline{y} = (y_0, y_1, y_2, \dots, y_n) \in S^n$ , we define

$$\phi_{\underline{y}}(\underline{x}) = (\phi_{y_0}(x_0), \phi_{y_1}(x_1), \dots, \phi_{y_n}(x_n)).$$

Following Piret, we call

$$\underline{b}(\underline{x}) = (b_0(\underline{x}), b_1(\underline{x}), \dots, b_{M-1}(\underline{x}))$$

or simply  $\underline{b} = (\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{M-1})$ , where  $b_r(\underline{x})$  denotes the number of coordinates in  $\underline{x}$  that are equal to  $s_r$ , as in [17], the composition of  $\underline{x}$ . Also, for large values of  $n$ , we call

$$\underline{\beta}(\underline{x}) = (\beta_0(\underline{x}), \beta_1(\underline{x}), \dots, \beta_{M-1}(\underline{x}))$$

the normalized composition of  $\underline{x}$  if  $b_r(\underline{x})$  is the least integer  $\leq n\beta_r(\underline{x})$  and if  $b_0(\underline{x}) = n - \sum_{r=1}^{M-1} b_r(\underline{x})$ . Moreover, in this case we say that the  $M$ -tuple  $\underline{b}(\underline{x})$  achieves the  $M$ -tuple  $\underline{\beta}(\underline{x})$ . For an arbitrary  $\underline{u} \in S^n$  and a specified composition  $\underline{b} = (b_0, b_1, \dots, b_{M-1})$  we denote  $B_{\underline{b}}(\underline{u})$  the set of all  $\underline{x} \in S^n$  for which

$$\text{composition of } \phi_{\underline{u}}(\underline{x}) = \underline{b}.$$

For all  $\underline{x} \in B_{\underline{b}}(\underline{u})$ , the SED  $d^2(\underline{x}, \underline{u})$  between  $\underline{x}$  and  $\underline{u}$  is given by

$$d^2(\underline{x}, \underline{u}) = \sum_{r=0}^{M-1} b_r d^2(r). \quad (15)$$

Since  $S$  is a DU signal set,  $S^n$  also will have the uniformity property hence the cardinality of  $B_{\underline{b}}(\underline{u})$  is independent of  $\underline{u}$ . We denote this cardinality by  $N(\underline{b})$  given by

$$N(\underline{b}) = \frac{n!}{\prod_{r=0}^{M-1} (b_r!)} \quad (16)$$

Moreover, exhibiting the independence of the right-hand side of (16) on the choice of  $\underline{u}$ , it is denoted by

$$D^2(\underline{b}) = \sum_{r=0}^{M-1} b_r d^2(r). \quad (17)$$

Equation (17) corresponds to [17, eq. (11)]. The rest of the proof is identical to that of Piret's and hence omitted, except that we point out

the following. The arguments leading to [17, eqs. (11)–(24)] hold in our case also with  $4 \sin^2(r\pi/Q)$  in (18) and (23) replaced by  $d^2(r)$ .

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their detailed comments which considerably improved the clarity and presentation of the material. Theorem 1, along with its proof, was sharpened into its present form from Theorem 3 given in the Appendix by a reviewer. Also the authors wish to thank Hugo Brändström and Lars Zetterberg for providing the technical report [4].

REFERENCES

- [1] J. Bali and B. S. Rajan, "Block coded PSK modulation using two-level group codes over dihedral groups," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1620–1631, July 1998.
- [2] E. Biglieri, D. Divsalar, P. J. McLane, and M. K. Simon, *Introduction to Trellis-Coded Modulation With Applications*. New York: MacMillan, 1991.
- [3] R. E. Blahut, *Principles and Practice of Information Theory*. Reading, MA: Addison-Wesley, 1987.
- [4] H. Brändström, "Classification of codes for phase and amplitude modulated signals in four dimensional base space," *Telecommunication Theory*, Royal Inst. Technol., Stockholm, Sweden, Tech. Rep. 105, Jan. 1976.
- [5] G. Caire and E. Biglieri, "Linear block codes over cyclic groups," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1246–1256, Sept. 1995.
- [6] G. D. Forney, Jr., "Geometrically uniform codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1241–1260, Sept. 1991.
- [7] R. Garelo and S. Benedetto, "Multilevel construction of block and trellis group codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1257–1264, Sept. 1995.
- [8] A. Gersho and V. B. Lawrence, "Multidimensional signal constellations for voiceband data transmission," *IEEE J. Select. Areas Commun.*, vol. SAC-2, pp. 687–702, Sept. 1984.
- [9] V. V. Ginzburg, "Multidimensional signals for a continuous channel," *Probl. Inform. Transm.*, vol. 23, pp. 20–34, Jan.–Mar. 1984.
- [10] H. Imai and S. Hirakawa, "A new multilevel coding method using error correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 371–377, May 1977.
- [11] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On multilevel block modulation codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 965–975, July 1991.
- [12] F. R. Kschischang, P. G. deBuda, and S. Pasupathy, "Block codes for M-ary phase shift keying," *IEEE J. Select. Areas Commun.*, vol. 7, pp. 900–913, Aug. 1989.
- [13] H. A. Loeliger, "Signal sets matched to groups," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1675–1682, Nov. 1991.
- [14] —, "On Euclidean space group codes," Ph.D. dissertation, Swiss Federal Inst. Technol., Zurich, 1992.
- [15] —, "An upper bound on the volume of discrete spheres," *IEEE Trans. Inform. Theory*, vol. 40, pp. 2071–2073, Nov. 1994.
- [16] —, "Averaging arguments for lattices and linear codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1767–1773, Nov. 1997.
- [17] P. Piret, "Bounds for codes over the unit circle," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 760–767, Nov. 1986.
- [18] D. Saha and T. Birdsall, "Quadrature-quadrature phase-shift keying," *IEEE Trans. Commun.*, vol. 37, pp. 437–448, May 1989.
- [19] T. V. Selvakumaran and B. S. Rajan, "Block coded modulation using two-level group codes over generalized quaternion groups," *IEEE Trans. Inform. Theory*, vol. 45, pp. 365–372, Jan. 1999.
- [20] D. Slepian, "On neighbor distances and symmetries in group codes," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 630–632, Sept. 1971.
- [21] J. H. van Lint, *Introduction to Coding Theory*. Heidelberg, Germany: Springer-Verlag, 1982.
- [22] M. Visintin, E. Biglieri, and V. Casellani, "Four-dimensional signaling for bandlimited channels," *IEEE Trans. Commun.*, vol. 42, pp. 403–409, Feb./Mar./Apr. 1989.
- [23] G. R. Welty and J. S. Lee, "Digital transmission with coherent four-dimensional signaling," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 497–502, July 1974.
- [24] L. H. Zetterberg and H. Brändström, "Codes for combined phase and amplitude modulated signals in a four-dimensional space," *IEEE Trans. Commun.*, vol. COM-25, pp. 943–950, Sept. 1977.