PAPER

On Asymptotic Elias Bound for Euclidean Space Codes over Distance-Uniform Signal Sets

Balaji Sundar RAJAN[†a)], ***Regular Member and*** **Ganapathy VISWANATH**[†], ***Student Member***

SUMMARY The asymptotic Elias upper bound of codes designed for Hamming distance is well known. Piret and Ericsson have extended this bound for codes over symmetric PSK signal sets with Euclidean distance and for codes over signal sets that form a group, with general distance function respectively. The tightness of these bounds depend on a choice of a probability distribution, and finding the distribution (optimum distribution) that leads to the tightest bound is difficult in general. In this paper we point out that these bounds are valid for codes over the wider class of distance-uniform signal sets (a signal set is referred to be distance-uniform if the Euclidean distance distribution is same from any point of the signal set). We show that optimum distributions can be found for (i) simplex signal sets, (ii) Hamming spaces and (iii) biorthogonal signal set. The classical Elias bound for arbitrary alphabet size is shown to be obtainable by specializing the extended bound to simplex signal sets with optimum distribution. We also verify Piret's conjecture for codes over 5-PSK signal set.
key words: *Euclidean space codes, group codes, uniform signal sets, signal sets matched to groups*

1. Introduction

Hamming distance of a binary code is the appropriate performance index when the code is used on a binary symmetric channel. For other channels Hamming distance may not be an appropriate performance index. For instance, when used in Additive White Gaussian noise ($AWGN$) channel the minimum squared Euclidean distance ($MSED$) of the resulting signal space code is the appropriate performance index [1]–[3]. For codes designed for the Hamming distance, Elias bound gives an asymptotic upper bound on the normalized rate of the code for a specified normalized Hamming distance. To be precise, let C be a length n code over a q-ary alphabet with minimum Hamming distance $d_H(C)$. The asymptotic Elias bound [4]–[6] is given by

$$\begin{aligned} &R(\delta_H) \leqq 1 - H_q(\theta - \sqrt{\theta(\theta-\delta_H)}) \ \text{ if } \ 0 \leqq \delta < \theta \\ &R(\delta_H) = 0 \ \ if \ \ \theta \leqq \delta < 1 \end{aligned} \qquad (1)$$

where $\theta = (q-1)/q$, $R = \lim_{n\to\infty} \frac{1}{n}\log_q \mid C \mid$ is the normalized rate, $\delta_H = \lim_{n\to\infty}\frac{1}{n} d_H(C)$ is the normalized Hamming distance and $H_q(x)$ is the generalized entropy function given by

$$H_q(x) = -x\log_q\left[\frac{x}{q-1}\right] - (1-x)\log_q(1-x) \quad \text{if } \ 0 \leqq x \leqq \left[\frac{q-1}{q}\right] \qquad (2)$$

Piret [11] has extended this bound for codes over symmetric PSK signal sets for Euclidean distance and Ericsson [13] for codes over any signal set that forms a group for the general distance function. These bounds and their tightness depend on the choice of a probability distribution. In this paper we point out that these bounds hold for the wider class of signal sets, namely the distance-uniform signal sets. The existence of distance-uniform signal sets that are not matched to any group was shown in [14]. We show that the tightest bound (optimum distribution) is obtainable for simplex, Hamming spaces and biorthogonal signal sets. Also, we verify the conjecture of Piret regarding the optimum distribution for codes over symmetric 5-PSK signal set.

A signal set is said to be distance-uniform if the Euclidean distance distribution of all the points in the signal set from a particular point in the signal set is same from any point, i.e., if the signal set is $S = \{s_0, s_1, \ldots, s_{M-1}\}$ and $D_i = \{d_{ij}, j = 0, 1, \ldots, M-1\}$ is the Euclidean distance distribution from the signal point s_i, then D_i is the same for all $i = 0, 1, ..., M-1$. Examples of uniform signal sets are all binary signal sets, symmetric PSK Signal sets, orthogonal signal sets, simplex signal sets [1]–[3] and hypercubes in any dimension. The class of signal sets matched to groups [7], [9] form an important class of distance-uniform signal sets. 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,

$$d_E(\mu(g), \mu(g')) = d_E(\mu(g^{-1}g'), \mu(e)) \qquad (3)$$

where $d_E(x, y)$ denotes the squared Euclidean distance 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 [8] which include important classes of codes as special cases. Moreover, it has been shown that signal sets matched to non-commutative groups have the capacity of exceeding the PSK limit [10], whereas the

Manuscript received February 12, 2002.
Manuscript revised July 11, 2002.
Final manuscript received September 9, 2002.
[†]The authors are with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore, India.
a) E-mail: bsrajan@ece.iisc.ernet.in

capacity of signal sets matched to commutative groups are upper-bounded by the PSK limit [7], [9].

In this paper we discuss the asymptotic upper bound on the normalized rate of Euclidean space codes [7], [8] over distance-uniform signal sets, for given normalized squared Euclidean distance. However, the arguments are valid for any distance function. We show that

- The Piret's and Ericsson's bound are valid for codes over any uniform-signal set.
- The distribution that gives the tightest bound (optimum distribution) for codes over simplex signal sets, Hamming spaces and biorthogonal signal sets are easily obtained.
- The bound for codes over simplex signal sets with optimum distribution is essentially the classical Elias bound. We also verify Piret's conjecture regarding the optimum distribution for codes over 5-PSK signal sets.

The content of this paper is organized as follows: The validity of Piret's and Ericsson's bound for codes over the wider class of distance-uniform signal sets is given in Sect. 2. Also, the optimum distribution for codes over simplex, Hamming spaces and biorthogonal signal sets are obtained. The relation between classical asymptotic Elias bound and the extended bound is established by specializing to the codes over simplex signal sets. Further we verify Piret's conjecture on the optimum distribution for codes over 5-PSK signal sets. Section 3 contains directions for further research and concluding remarks.

2. Extended Upper Bound (EUB)

Following the arguments in the spirit of Elias bound [4], Piret [11] has obtained an asymptotic upper bound in the parametric form on the rate of Euclidean space codes over symmetric PSK signal sets from which the Elias bound for $q = 2$ is obtainable and not for $q \geqq 4$. Ericsson [13] has shown that this bound is valid for codes over any signal set that forms a group and for any general distance function. We point out in the following that the validity of this bound extends to codes over the wider class of distance-uniform signal sets. Theorem 1 gives the extended upper bound (EUB), the proof of which is same as that of Piret [11].

Theorem 1: Let A be a distance-uniform signal set with M signal points $\{a_0, a_1, \ldots, a_{M-1}\}$ and S be a $M \times M$ matrix with (i, j)th entry s_{ij} equal to $d^2_{i,j}$, the squared Euclidean distance between a_i and a_j. For C, a length n code over A, let

$$\delta(C) = \frac{1}{n} d^2(C), \quad R(C) = \frac{1}{n} \ln \mid C \mid \quad \text{and}$$
$$R(M, \delta) = \lim_{n\to\infty} sup_{\substack{|C| \geqq n \\ \delta(C) \geqq \delta}} R(C) \tag{4}$$

$d^2(C)$ is the minimum squared Euclidean distance ($MSED$) of the code. The asymptotic upper bound $R_U(M, \delta)$ on $R(C)$ is given in terms of a probability distribution $\underline{\beta} = (\beta_0, \beta_1, \cdots, \beta_{M-1})$, by

$$R_U(M, \delta) = \ln(M) - H(\underline{\beta}) \quad \text{and} \quad \delta = \underline{\beta} S \underline{\beta}^T \tag{5}$$

where $H(\underline{\beta}) = -\Sigma_{i=0}^{M-1} \beta_i \ln(\beta_i)$.

Proof: The proof is essentially same as that of Piret [11]. We give below the minor adjustments that are needed in the initial part of Piret's proof to make it valid for codes over distance-uniform signal sets:

Let $\{s_0, s_1, ..., s_{M-1}\}$ be the signal set S, and let the ordered vector $d = (d(0), d(1), ..., d(M-1))$ denote the Euclidean distance profile of S from s_0. Let Φ_r, $r = 0, 1, ..., M-1$, be a permutation on S such that $\Phi_r(s_r) = s_0$ and $\Phi_r(s_u) = s_v$, $u, v = 1, 2, ..., M-1$, where the squared Euclidean distance between s_r and s_u is $d^2(v)$. Such a permutation exists since S is distance-uniform. For any $\underline{x} = (x_1, x_2, ..., x_n)$ and $\underline{y} = (y_1, ..., y_n) \in S^n$, define $\Phi_{\underline{y}}(\underline{x}) = (\Phi_{y_1}(x_1), ..., \Phi_{y_n}(x_n))$ and call $b(\underline{x}) = (b_0(\underline{x}), b_1(\underline{x}), ..., b_{M-1}(\underline{x}))$, where $b_r(\underline{x})$ denotes the number of coordinates in $\underline{x}$ that are equal to s_r, as in [11], the composition of $\underline{x}$. For an arbitrary $\underline{u} \in S^n$ and a specified composition $\underline{b} = (b_0, b_1, ..., b_{M-1})$ denote by $B - \underline{b}(\underline{u})$ the set of all $\underline{x} \in S^n$ for which composition of $\Phi_{\underline{u}}(\underline{x}) = \underline{b}$.

These points replace the arguments used in [11] for PSK with cyclic group structure. Also, Lemmas (4.1) and (4.2) in [11], which are specifically for PSK signal sets can be replaced by the following two lemmas to make the proof valid for codes over any distance-uniform signal set.

Lemma 1: $\beta_i^t = \beta_i \ \forall i = 0, 1, 2, \cdots, M-1, \quad t = 1, 2, \cdots, n$, where β_i^t is the normalized number of occurrences of the i-th symbol in the t-th co-ordinate as n tends to ∞.

Proof: The normalized number of occurrences of i-th symbol from among M possible symbols is

$$b_i = \frac{N_i}{\sum_{j=0}^{M-1} N_j} \tag{6}$$

where N_i indicates the number of times the i-th symbol occurs. The normalized number of occurrences of the i-th symbol in the t-th co-ordinate b_i^t is obtained as

$$b_i^t = \frac{\left((\sum_{j=0}^{Q-1} N_j - 1)! \right) \Big/ \left(\prod_{j=0, j\neq i}^{Q-1} N_j! \right)}{\left(\sum_{j=0}^{Q-1} N_j \right)! \Big/ \left(\prod_{k=0, k\neq i}^{Q-1} N_k! \right)} \tag{7}$$

The above equation can be simplified to obtain the following result

$$b_i^t = \frac{N_i}{\sum_{j=0}^{Q-1} N_j} = b_i \tag{8}$$

Therefore the number of occurrences of any symbol at any co-ordinate is same. As $n \to \infty$, we have b_r tends to β_r and b_r^t tends to β_r^t. Hence we have $\beta_r^t = \beta_r$. □

Lemma 2: For $n \to \infty$ the Q-tuples β^j satisfy

$$\sum_{t=1}^{n} \beta^{(t)} S \beta^{(t)T} = n(\underline{\beta} S \underline{\beta}^T) \tag{9}$$

Proof: Follows from Lemma 1. □

In the following three theorems we obtain the optimum distribution that gives the tightest bound for simplex, Hamming spaces and biorthogonal signal sets respectively.

Theorem 2 (Simplex signal sets): The distribution $\underline{\beta} = (\beta_0, \beta_1, \beta_2, \cdots, \beta_{M-1})$ that gives the best bound for codes over M-ary simplex signal set is given by

$$\beta_r = \frac{1}{M}\left[1 - \sqrt{1 - M\frac{\delta}{K(M-1)}}\right],\ r = 1, \ldots, M-1 \tag{10}$$

where K is the squared Euclidean distance between any two signal points. Moreover for all values of q the asymptotic Elias bound given in Eq. (1), can be obtained from this bound.

Proof: For simplex signal sets, the squared Euclidean distance between any two signal points is the same. Let K denote this squared Euclidean distance, i.e.,

$$\begin{aligned} d^2(i,j) &= 0 \ \text{ if } \ i = j \\ &= K \text{ (a constant)}, \ \text{ if } \ i \neq j, \\ &\quad i,j = 0,1,2,\cdots,M-1 \end{aligned} \tag{11}$$

then

$$S = \begin{bmatrix} 0 & K & K & \ldots & K & K \\ K & 0 & K & \ldots & K & K \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ K & K & K & \ldots & 0 & K \\ K & K & K & \ldots & K & 0 \end{bmatrix} \tag{12}$$

Let $\underline{\beta} = (\beta_0, \beta_1, \ldots, \beta_{M-1})$ be any probability distribution. We find the best distribution by using Lagrange multipliers. Let

$$\begin{aligned} \Phi(\underline{\beta}, \lambda) &= H(\underline{\beta}) - \lambda\left[\delta - \underline{\beta} S \underline{\beta}^T\right] \\ &= H(\underline{\beta}) - \lambda\left[\delta - K\sum_{i=0}^{M-1}\sum_{j=0, j\neq i}^{M-1}\beta_i\beta_j\right] \end{aligned} \tag{13}$$

Using $\sum_{i=0}^{M-1}\beta_i = 1$ in the inner summation, the above becomes

$$\Phi(\underline{\beta}, \lambda) = H(\underline{\beta}) - \lambda\left[\delta - K\left\{\sum_{i=0}^{M-1}\beta_i(1-\beta_i)\right\}\right] \tag{14}$$

Now for $r = 1, 2, \ldots, M-1$, we have

$$\begin{aligned} \frac{\partial\Phi(\underline{\beta}, \lambda)}{\partial\beta_r} &= 1 - \log(\beta_r) - 1 + \log(\beta_0) \\ &\quad + K\lambda\left[1 - 2\beta_r - 1 + 2\beta_0\right] \\ &= \log\beta_0 - \log\beta_r + 2K\lambda(\beta_0 - \beta_r). \end{aligned} \tag{15}$$

Now the solution of the equation

$$\frac{\partial\Phi(\underline{\beta}, \lambda)}{\partial\beta_r} = 0 \tag{16}$$

for β_r will be the same for all $r = 1, 2, \ldots, M-1$, since the form of Eq. (15) is same for all $r = 1, 2, \ldots, M-1$. Let p be the solution of Eq. (16), i.e., $\beta_r = p$, for all $r = 1, 2, \ldots, M-1$. Now substituting $\beta_r = p$ in Eq. (15), gives

$$\begin{aligned} \delta &= K\left[2\beta_0(1-\beta_0) + \sum_{i=1}^{M-1}\sum_{\substack{j=1 \\ j\neq i}}^{M-1} p^2\right] \\ &= 2K\left[\{1-(M-1)p\}(M-1)p\right] \\ &\quad + K(M-1)(M-2)p^2 \end{aligned} \tag{17}$$

which is the same as the quadratic equation

$$KM(M-1)p^2 - 2K(M-1)p + \delta = 0 \tag{18}$$

The solutions of the quadratic equation after simplification are

$$\frac{1}{M}\left[1 \pm \sqrt{1 - \frac{\delta}{K\theta}}\right] \tag{19}$$

where $\theta = \frac{(M-1)}{M}$. It can be checked that, $H(\underline{\beta})$ is minimum for

$$\begin{aligned} \underline{\beta} = \Bigg\{ & 1 - \left[\theta - \sqrt{\theta^2 - \frac{\delta\theta}{K}}\right], \frac{1}{M}\left[1 - \sqrt{1 - \frac{\delta}{K\theta}}\right], \\ & \ldots, \frac{1}{M}\left[1 - \sqrt{1 - \frac{\delta}{K\theta}}\right]\Bigg\} \end{aligned} \tag{20}$$

For the above distribution

$$\ln M - H(\underline{\beta}) = \ln M + \beta_0\ln\beta_0 + (M-1)\beta_r\ln\beta_r \tag{21}$$

Changing the base of the logarithm to M, the above expression becomes,

$$1 - H_M\left(\theta - \sqrt{\theta^2 - \frac{\theta\delta}{K}}\right) \tag{22}$$

Substituting $\delta_H = \delta/K$ in Eq. (22) we get

$$1 - H_M\left(\theta - \sqrt{\theta(\theta - \delta_H)}\right) \tag{23}$$

which is the same as the classical asymptotic Elias bound. It remains to show that the range for δ_H on the Elias bound is $0 \leqq \delta_H < (M-1)/M$. With the substitution $\delta_H = \delta/K$, the range for δ becomes $0 \leqq \delta < K\theta$. Choosing $K = 2/\theta$ and hence the range for δ is $0 \leqq \delta < 2$ consistent with Theorem 1.

The substitution given by $K = 2M/M-1$ and $\delta = \delta/K$, can be combined to obtain the relation between normalized squared Euclidean distance in the extended bound and the normalized Hamming distance in Elias bound as

$$\delta \left[\frac{(M-1)}{2M} \right] = \delta_H \tag{24}$$

The term $\frac{M-1}{2M}$ is the factor by which the plot of Elias bound can be obtained from the plot of the bound of Theorem 2.

Example 1: Figure 1 shows binary, ternary and quaternary simplex signal set on a unit radius *sphere*. Figure 2 shows the classical *Elias* bound (with natural logarithm) for simplex signal set of size $2, 3$ and 4 and the corresponding bounds for Euclidean distance.

Theorem 3 (Hamming spaces): Let A be a signal set which is an m-th order q-ary Hamming space. Then

$$R_U(q^m, \delta) = m \left(1 - H_q \left(\theta - \sqrt{\theta^2 - \frac{\theta\delta}{K}} \right) \right) \tag{25}$$

where $\theta = \frac{(q-1)}{q}$ and K is the squared Euclidean distance between any two points differing in only one position in the label.

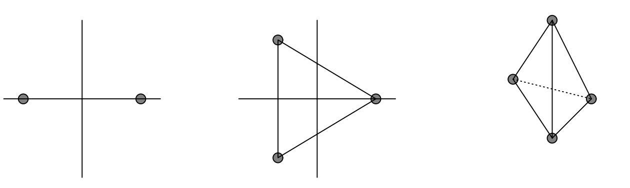


Fig. 1 Binary, ternary and quaternary simplex signal sets.

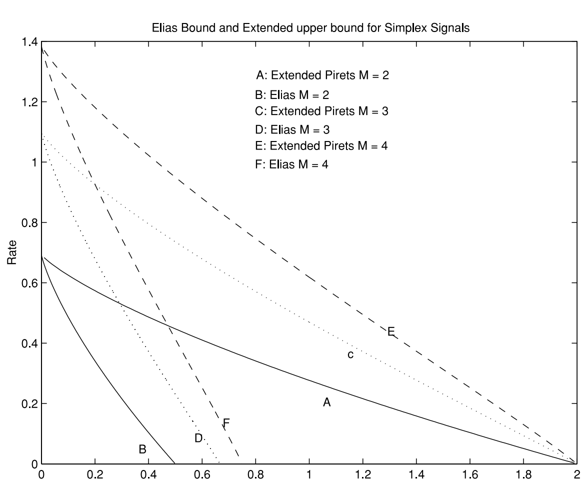


Fig. 2 The Elias and extended upper bounds for binary, ternary and quaternary simplex signal sets.

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

$$R_U(q^m, \delta) = m R_U(q, \delta) \tag{26}$$

Note that A' is a simplex signal set consisting of q points. Hence $R_U(q, \delta)$ is given by Theorem 10. □

Observe that a simplex signal set with M points is a first order M-ary Hamming space. In this sense Theorem 3 is a generalization of Theorem 2.

Corollary 1: For N-dimensional cube, the extended Piret's bound is given by

$$R_U(2^N, \delta) = N \left(1 - H_2 \left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - \frac{\delta}{2}} \right) \right) \tag{27}$$

Proof: Straightforward application of Theorem 3. □

Example 2: The 3-dimensional cube shown in Fig. 3 is a third order binary Hamming space with labeling as shown. The bound for this cube is given by

$$R_U(8, \delta) = 3 \left(1 - H_2 \left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - \frac{\delta}{2}} \right) \right) \tag{28}$$

Theorem 4 (Biorthogonal signal sets): The optimum distribution $\underline{\beta} = (\beta_0, \beta_1, \beta_2, \cdots, \beta_{M-1})$ giving the tightest bound for codes over biorthogonal signal set is given in terms of a parameter $\mu > 0$, as

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}}, \quad r = 0, 1, 2, \cdots, M-1 \tag{29}$$

where $d^2(r)$ is the squared Euclidean distance between 0th point and the rth point of the M point biorthogonal signal set.

Proof: The squared Euclidean distance profile of a M point biorthogonal signal set is as follows

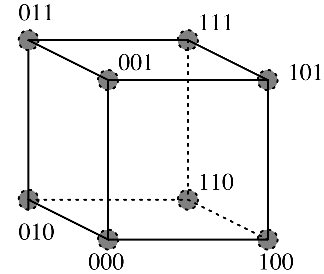


Fig. 3 3-dimensional cube.

$$\begin{aligned} d^2(r) &= 0 \text{ if } r=0 \\ &= K \text{ (a constant), if } r \neq 0 \text{ and } r \neq \frac{M}{2} \\ &= 2K \text{ if } r = \frac{M}{2} \end{aligned} \tag{30}$$

$$S = \begin{bmatrix} 0 & K & K & \dots & K & 2K & K & \dots & K \\ K & 0 & K & \dots & K & K & 2K & \dots & K \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 2K & K & K & \dots & K & 0 & K & \dots & K \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ K & K & K & \dots & 2K & K & K & \dots & 0 \end{bmatrix} \tag{31}$$

Here S is a circulant matrix. Therefore the second row of the S matrix is obtained by circularly shifting the first row to the right once. All the M rows of the S matrix can be obtained similarly.

Let $\underline{\beta} = (\beta_0, \beta_1, \dots, \beta_{M-1})$ be any probability distribution. We find the best bound using Lagrange multipliers. Let

$$\begin{aligned} \Phi(\underline{\beta}, \lambda) &= H(\underline{\beta}) - \lambda \left[\delta - \underline{\beta} S \underline{\beta}^T\right] \\ &= H(\underline{\beta}) - \lambda \left[\delta - \sum_{i=0}^{M-1} \sum_{j=0, j\neq i}^{M-1} \beta_i s_{ij} \beta_j\right] \end{aligned} \tag{32}$$

Here β_r will be the same for $\{r = 1, 2, \dots, \frac{M}{2} - 1, \frac{M}{2} + 1, \dots, M-1\}$. Hence we have to find the optimum values for β_1 and $\beta_{\frac{M}{2}}$. These correspond to

$$\frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_1} = \log(\beta_0) - \log(\beta_1) + 2K\lambda\beta_0 - 2K\lambda\beta_{\frac{M}{2}} \tag{33}$$

and

$$\frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_{\frac{M}{2}}} = \log(\beta_0) - \log(\beta_{\frac{M}{2}}) + 4K\lambda\beta_0 - 4K\lambda\beta_{\frac{M}{2}} \tag{34}$$

Equations (33) and (34) to zero and simplifying we get

$$\beta_0 \beta_{\frac{M}{2}} = \beta_1^2 \tag{35}$$

It is easily verified that

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}}, \quad r = 0, 1, 2, \cdots, M-1 \tag{36}$$

constitute a solution of Eq. (35) with parameter μ. □

Example 3: Consider the biorthogonal signal set for $M = 4$. Biorthogonal signal with $M = 4$ is same as $4 - PSK$ signal set (Fig. 4). The optimum distribution achieving the tightest bound is given by following equations

$$\begin{aligned} &\beta_1(\mu) = \frac{e^{-2\mu}}{\sum_{s=0}^{3} e^{-\mu d^2(s)}}, \; \beta_2(\mu) = \frac{e^{-4\mu}}{\sum_{s=0}^{3} e^{-\mu d^2(s)}} \\ &\beta_3(\mu) = \beta_1(\mu), \; \beta_0(\mu) = 1 - 2\beta_1(\mu) - \beta_2(\mu) \end{aligned} \tag{37}$$

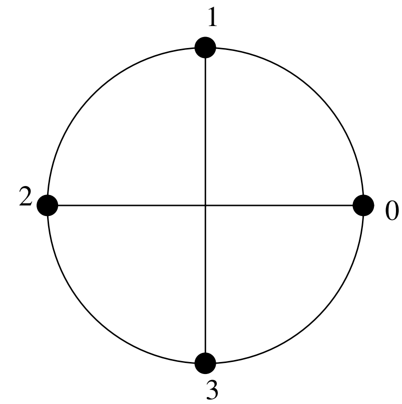


Fig. 4 Biorthogonal signal set with $M = 4$. This is same as 4-PSK with points uniformly distributed on the unit circle.

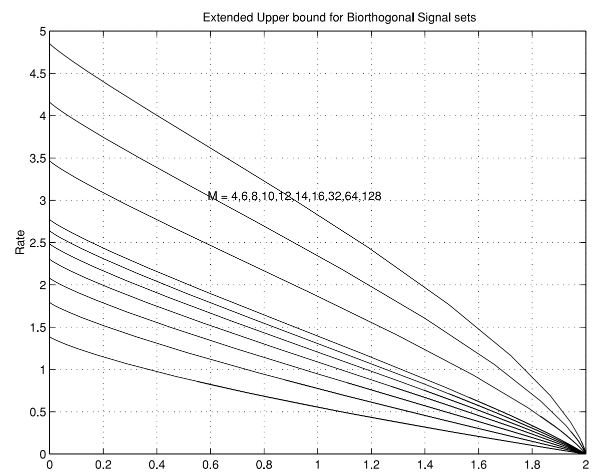


Fig. 5 The extended upper bounds for M-point biorthogonal signal set.

The above distribution for 4-PSK signal set is same as optimal distribution conjectured by Piret for PSK signal sets. The EUB for 4-point biorthogonal signal set is shown in Fig. 5. In Fig. 5 EUB for biorthogonal signal sets is plotted for different values of M. First curve from the bottom is for $M = 4$ and the top curve is for $M = 128$. □

2.1 Piret's Conjecture for Codes over 5-PSK Signal Sets

Piret has obtained both asymptotic lower and upper bounds for codes over symmetric PSK signal sets. Both the bounds are obtained in terms of a probability distribution. However, for lower bound the distribution giving the best lower bound is obtained whereas, as mentioned in the previous section, the distribution giving the best upper bound is not given but it is conjectured that the distribution which gives the optimum lower bound also gives the best upper bound. For 5-PSK we check the conjecture.

2.1.1 Piret's Lower Bound

Let A be a M point uniform signal set with Euclidean distance distribution $\{d(r), r = 0, 1, \ldots, M-1\}$. For C, a length n code over S, let

$$\delta(C) = \frac{1}{n} d^2(C)$$
$$R(C) = \frac{1}{n} \ln \mid C \mid$$
$$R(M, \delta) = \lim_{n\to\infty} sup_{\substack{|C| \geqq n \\ \delta(C) \geqq \delta}} R(C) \tag{38}$$

where $d^2(C)$ is the $MSED$ of C and $R(C)$ is the rate of the code. Then a lower bound $R_L(M, \delta)$ on $R(C)$ is given in terms of a parameter μ by

$$R_L(M, \delta) = \ln M - H(\underline{\beta}(\mu)) \quad 0 \leqq \delta \leqq 2 \tag{39}$$

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

$$\beta_r(\mu) = \frac{e^{-\mu d^2(r)}}{\sum_{s=0}^{M-1} e^{-\mu d^2(s)}} \tag{40}$$
$$\delta = \sum_{s=0}^{M-1} \beta_s(\mu) d^2(s) \tag{41}$$

Note that bound is not given in terms of an arbitrary distribution-instead the distribution given above is optimum for the lower bound. Equation (39) is counterpart of the equation for the upper bound (Eq. (5)). Piret conjectures that the distribution given in Eq. (40) is the optimum distribution for the upper bound also.

If Piret's conjecture was true then the distribution given in Eq. (40) should satisfy the set of equations to get the optimal distribution for $5 - PSK$ signal set (Lagrange multiplier method is used to get optimum distribution).

$$\Phi(\underline{\beta}, \lambda) = H(\underline{\beta}) - \lambda \left[\delta - \underline{\beta} S \underline{\beta}^T\right]$$
$$= H(\underline{\beta}) - \lambda \left[\delta - \sum_{i=0}^{4} \sum_{j=0, j\neq i}^{4} \beta_i s_{ij} \beta_j\right] \tag{42}$$

where s_{ij} is of the form $4\sin^2[(i-j)\pi/M]$. Now for $r = 1, 2$ we obtain the partial derivatives,

$$\frac{\partial \Phi(\underline{\beta}, \lambda)}{\partial \beta_r} = \log(\beta_0) - \log(\beta_r) - 2\lambda \sum_{j=1}^{4} s_{0,j}\beta_j$$
$$+ 2\lambda \sum_{j=0, j\neq r}^{4} s_{r,j}\beta_j \tag{43}$$

Since the above expression is identical for $r = 1, 4$ and $r = 2, 3$ we have $\beta_1 = \beta_4$ and $\beta_2 = \beta_3$. Taking $r = 1$ we solve for λ in terms of β_1 and β_2.

$$\lambda = \frac{\log \beta_1 - \log \beta_0}{2(a + (b-4a)\beta_1 - (a+b)\beta_2)} \tag{44}$$

where $a = 4\sin^2(\pi/5)$ and $b = 4\sin^2(2\pi/5)$. From the optimal distribution for lower bound [11] we have $\beta_1 = \beta_0 e^{-\mu a}$ and $\beta_2 = \beta_0 e^{-\mu b}$. Substituting for β_1 and β_2 in Eq. (44) we get

$$\lambda = \frac{-\mu a}{2(a + (b-4a)\beta_0 e^{\mu a} - (a+b)\beta_0 e^{-\mu b})} \tag{45}$$

The partial derivative of the Lagrangian for $r = 2$ is

$$\log\beta_0 - \log\beta_2 + 2\lambda\left[b - (a+b)\beta_1 + (a-4b)\beta_2\right] \tag{46}$$

Substituting for λ, β_1 and β_2 in Eq. (46) we get the following

$$b - a\frac{\left[b - (a+b)\beta_0 e^{-(\mu a)} + (a-4b)\beta_0 e^{-(\mu b)}\right]}{\left[a + (b-4a)\beta_0 e^{-(\mu a)} - (a+b)\beta_0 e^{-(\mu b)}\right]} = 0 \tag{47}$$

Simplifying these equations we get

$$\frac{b}{a} = \frac{\left[-(a+b)\beta_0 e^{-(\mu a)} + (a-4b)\beta_0 e^{-(\mu b)}\right]}{\left[(b-4a)\beta_0 e^{-(\mu a)} - (a+b)\beta_0 e^{-(\mu b)}\right]} \tag{48}$$

The right hand side of the above equation was computed by varying μ (here μ is any non-negative real number). The right hand side was equal to 2.6180 for every value of μ. This is same as $\frac{b}{a}$. Therefore we conclude that Piret's conjecture for 5-PSK is correct.

3. Conclusion

The known upper bounds [11] and [13], respectively, on the normalized rate of a code over symmetric PSK signal set for a specified $NSED$ and of a code over any signal set constituting a group for a general distance function are shown to be valid for codes over any distance-uniform signal set. In general, the tightness of these bounds depends on a choice of a probability distribution. The optimum distribution for the cases (i) simplex (ii) Hamming spaces and (iii) biorthogonal signal sets leading to tightest bounds are obtained. The classical asymptotic Elias bound is shown to be same as the bound of this paper for codes over simplex signal sets with the optimum distribution obtained. An interesting direction for further research would be to attempt to get best bounds for codes over signal sets matched to specific groups, like dihedral, quaternion and dicyclic groups.

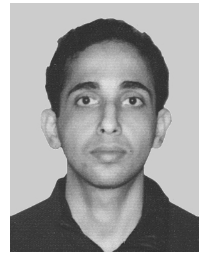
Acknowledgements

We thank Prof. T. Ericsson for his comments after going through the initial version of the paper and also sending a copy of his paper. We are grateful to anonymous referees for their valuable inputs.

References

[1] S. Benedetto, E. Bilglieri, and Castellani, Digital Transmission Theory, Prentice-Hall, 1987.
[2] A.J. Viterbi and J.K. Omura, Digital Communication and Coding, McGraw-Hill, 1979.
[3] J.M. Wozencraft and I.M. Jacobs, Principles of Communication Engineering, Wiley, N.Y., 1965.
[4] J.H. Van Lint, Introduction to Coding Theory, Springer Verlag, Heidelberg, Germany, 1982.
[5] F.J. Mac Williams, Theory of Error Correcting Codes, Amsterdam, North Hollands, The Netherlands, 1977.
[6] W.W. Peterson and E.J. Weldon, Error Correcting Codes, MIT Press, Cambridge, M.A., 1972.
[7] H.A. Loeliger, On Euclidean Space Group Codes, PhD. Thesis, Swiss Federal Institute of Technology, Zurich, 1992.
[8] G.D. Forney, Jr., "Geometrically uniform codes," IEEE Trans. Inf. Theory, vol.37, no.6, pp.1241–1260, Nov. 1991.
[9] H.A. Loeliger, "Signal sets matched to groups," IEEE Trans. Inf. Theory, vol.37, no.6, pp.1675–1682, Nov. 1991.
[10] R.E. Blahut, Principles and Practice of Information Theory, Addison Wesley, 1987.
[11] P. Piret, "Bounds for codes over the unit circle," IEEE Trans. Inf. Theory, vol.IT-32, no.6, pp.760–767, Nov. 1986.
[12] F.R. Kschischang, P.G. deBuda, and S. Pasupathy, "Block codes for M-ary parse shift keying," IEEE J. Sel. Areas Commun., vol.7, no.6, pp.900–913, Aug. 1989.
[13] T. Ericsson, "Generalizations of the Johnson and the Bassalygo-Elias bounds," Fourth Joint Swedish-Soviet International Workshop on Information Theory, Gotland, Sweden, Aug. 27–Sept. 1, 1989.
[14] D. Slepian, "On neighbor distances and symmetries in group codes," IEEE Trans. Inf. Theory, vol.IT-17, no.5, pp.630–632, Sept. 1971.

Balaji Sundar Rajan was born in Tamil Nadu, India. He received the B.Sc. degree in mathematics from Madras University, the B.Tech. degree in electronics from Madras Institute of Technology, and the M.Tech. and Ph.D. degrees in electrical engineering from the Indian Institute of Technology, Kanpur, in 1979, 1982, 1984, 1989 respectively. He was a faculty with the Department of Electrical Engineering Indian Institute of Technology in Delhi, from 1990 to 1997. Currently, he is Associate Professor in the Department of Electrical Communication Engineering, Indian Institute of Science in Bangalore. His primary research interests are in error-control coding, coded modulation, and cryptology. Prof. Rajan is a senior member of IEEE and a member of American Mathematical Society.



Ganapathy Viswanath received the MSc. (engg.) degree from Indian Institute of Science, Bangalore, India, in 1997. Since 1997, he has been a research student in the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore. His research interests are in the areas of error control coding and signal processing.