Discrete Mathematics 310 (2010) 3267–3275

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Improving bounds on the minimum Euclidean distance for block codes by inner distance measure optimization

Efraim Laksman [a,1], Håkan Lennerstad [a,*], Magnus Nilsson [b,2]

[a] Mathematics and Natural Sciences, School of Engineering, Blekinge Institute of Technology, S-371 79 Karlskrona, Sweden

[b] Telecommunications, School of Computing, Blekinge Institute of Technology, S-371 79 Karlskrona, Sweden

ARTICLE INFO

Article history:
Available online 16 June 2010

Keywords:
Block code
Phase shift keying
Metric
Elias' bound
Minimal Euclidean distance

ABSTRACT

The minimum Euclidean distance is a fundamental quantity for block coded phase shift keying (PSK). In this paper we improve the bounds for this quantity that are explicit functions of the alphabet size q, block length n and code size $|C|$. For $q = 8$, we improve previous results by introducing a general inner distance measure allowing different shapes of a neighborhood for a codeword. By optimizing the parameters of this inner distance measure, we find sharper bounds for the outer distance measure, which is Euclidean.

The proof is built upon the Elias critical sphere argument, which localizes the optimization problem to one neighborhood. We remark that any code with $q = 8$ that fulfills the bound with equality is best possible in terms of the minimum Euclidean distance, for given parameters n and $|C|$. This is true for many multilevel codes.

1. Introduction

We intend to improve bounds for the minimum squared Euclidean distance for block coded phase shift keying (PSK). For error correction with respect to maximum likelihood, when using a channel with additive white Gaussian noise, the squared Euclidean distance of the code is a highly relevant measure of the efficiency of a code for fixed block length n, code size $|C|$ and alphabet size q.

On the set $\mathbf{Z}_q^n$, the squared Euclidean distance is defined as

$$d_E^2(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{n} d_E^2(x_j, y_j), \tag{1}$$

where $d_E^2(x_j, y_j)$ is

$$d_E^2(x_j, y_j) = d_E^2(x_j - y_j, 0) = 4 \sin^2 \frac{(x_j - y_j)\pi}{q}. \tag{2}$$

Note that this distance measure is translation invariant, so that the arguments can be written in such a way that one of them is zero. To simplify notation, we will write $d(x) = d(x, 0)$ for any distance measure. Now a relevant model for the words is points in the group $(\mathbf{Z}_q^n, +)$, with the squared Euclidean distance used for measuring distance; see for example [1,4].

* Corresponding author. Tel.: +46 455385455, +46 733800148 (Mob.); fax: +46 455385207.
E-mail addresses: hln@bth.se, Hakan.Lennerstad@bth.se (H. Lennerstad).
1 Tel.: +46 455385684.
2 Tel.: +46 455385660, +46 733856004 (Mob.).

0012-365X/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2010.04.025

We consider an arbitrary subset C of $\mathbf{Z}_q^n$, corresponding to a block code having $|C|$ codewords $\mathbf{x} = (x_1, \ldots, x_n)$ of length n in an alphabet of q letters. The minimum squared Euclidean distance for the code is then

$$d_{E\,\min}^2(C) = \min_{\substack{\mathbf{x},\mathbf{y}\in C \\ \mathbf{x}\neq\mathbf{y}}} d_E^2(\mathbf{x}, \mathbf{y}). \tag{3}$$

Bounds on the minimum Euclidean distance are fundamental for the geometry of $\mathbf{Z}_q^n$: what is the largest possible distance between the two closest members in a subset of $\mathbf{Z}_q^n$ with $|C|$ members?

As is well known, the minimum Euclidean distance is essential to determine the error correction capabilities of a code. We define the rate of a block code as

$$R(q, n, |C|) = \frac{\log_q |C|}{n}. \tag{4}$$

For several combinations of q, n, and $|C|$, mostly for high rates, there are known codes whose minimum squared Euclidean distances fulfil our bound with equality. For these combinations of q, n and $|C|$, neither the codes nor the bound can be improved.

For other combinations of q, n and $|C|$, there is a gap between the bound and the minimum squared Euclidean distances for the best known codes. The size of this gap differs from case to case. Especially for medium and low rates, it is unknown whether there exist better codes to discover, or if it is possible to improve the bound, or a combination of both.

Many of the best known block codes, in the sense of minimum squared Euclidean distance, are constructed as multilevel codes; see for example [3,9,10]. There are also other code constructions providing some of the best known block codes.

The results of this paper are derived by using different kinds of distance measures and metrics. Both the distance measure and the metric are functions $d(\mathbf{x}, \mathbf{y})$ from pairs of codewords to non-negative numbers with the symmetry property $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ for all $\mathbf{x}$ and $\mathbf{y}$, and $d(\mathbf{x}, \mathbf{y}) = 0$ if and only if $\mathbf{x} = \mathbf{y}$. Unlike a distance measure, a metric is also required to satisfy the triangle inequality: $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{y}, \mathbf{z})$ for all $\mathbf{x}$ and $\mathbf{y}$. Note that the *squared* Euclidean distance measure $d_E^2(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^n d_E^2(x_j - y_j)$ is not a metric in general. For $q = 8$, we have $2 = d_E^2(2) > 2d_E^2(1) = 2(2 - \sqrt{2})$, which may be the reason why the optimal inner distance measure of Theorem 4 differs from $d_E^2(i) \cdot (K - 1)$ only for $i = 1, 2$ (K is a constant, defined later).

The quantities $d_E^2(x_j, y_j) = 4 \sin^2 \frac{(x_j - y_j)\pi}{q}$ are Euclidean distances between points when the entries $0, \ldots, q - 1$ are distributed equidistantly on a unit circle. The generalized distance measures considered in this paper will be translation invariant and defined on $\mathbf{Z}_q^n$, so they will be defined by a sequence of non-negative numbers, $\delta = \delta(0) = 0, \delta(2), \ldots, \delta(q - 1)$, without any particular geometrical meaning. The distance is then

$$\delta(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^n \delta(x_j, y_j) = \sum_{j=1}^n \delta(x_j - y_j), \tag{5}$$

generalizing

$$d_E^2(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^n d_E^2(x_j, y_j) = \sum_{j=1}^n d_E^2(x_j - y_j). \tag{6}$$

Some of the numbers $\delta(i)$ may be infinite, prohibiting the corresponding differences. The Lee metric, for example, is represented by $\delta(i) = i$. Also truncated Lee metrics, where $\delta(i) = i$ for $i \leq r$ but $\delta(i) = \infty$ for $i > r$, have been considered [6].

An alternative notation is sometimes useful. For two codewords $\mathbf{x}$ and $\mathbf{y}$, the number of positions where $\mathbf{x}$ and $\mathbf{y}$ differ by i or by $q - i$ is denoted by $c_i(\mathbf{x}, \mathbf{y})$:

$$c_i(\mathbf{x}, \mathbf{y}) = |\{j \in [1, n] : (x_j - y_j) \equiv_q i \text{ or } (x_j - y_j) \equiv_q q - i\}|, \tag{7}$$

where $\equiv_q$ means equal with respect to modulo q. We are still working with a generalization of the closest distance of letters in a unit circle, so two words can in one position differ by at most $\lfloor q/2 \rfloor$. Then an alternative notation for $\delta(\mathbf{x}, \mathbf{y})$ is

$$\delta(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^n \delta(x_j - y_j) = \sum_{i=1}^{\lfloor q/2 \rfloor} \delta(i) c_i(\mathbf{x}, \mathbf{y}). \tag{8}$$

2. Previous work

Apart from the presentation in this section, Section 6 contains an overview over the arguments that to some extent requires knowledge of the technical definitions that occur in the paper. The bounds in this paper and in the previous papers in this line of research are partly based on the arguments leading to the well-known Elias bound (see also Section 6, [1, pp. 318–321] and [4, pp. 558–564]). The Elias bound arguments have been used by Piret [8], who calculated bounds for the maximum rate, $n^{-1} \ln |C|$, for codes C with given $d_{E\,\min}^2(C)/n$ as $n \to \infty$. Piret's upper bound on the rate becomes

$$\ln q - \max_{\substack{2\beta S\beta^T = d^2_{E\min}(C)/n \\ \sum_i \beta_i = 1}} (H(\beta)), \tag{9}$$

where H is the entropy function

$$H(\beta) = -\sum_{i=1}^{q} \beta_i \ln(\beta_i), \tag{10}$$

β is a vector of length q and S is the $q \times q$ matrix with elements $2\sin^2[(i-j)\pi/q]$ in position (i, j).

The maximum rate as $n \to \infty$ is a non-increasing function of $d^2_{E\min}(C)/n$. Thus we can get a bound on $d^2_{E\min}/n$ as $n \to \infty$ as a function of the rate by reflecting the graph of Piret's bound in the line $\frac{\ln|C|}{d^2_{E\min}}$.

Wyner [11] has produced another bound for the same quantity as Piret. It is independent of q, and the q points may be distributed arbitrarily, giving for larger q weaker restrictions and a tighter bound in general. Wyner's bound is

$$\lim_{n\to\infty} \frac{1}{n} \frac{nK\left(\frac{d^2_{E\min}}{2n}\right)(2\pi)^n}{V_n\left(\sqrt{2n\left(1-\sqrt{1-\frac{d^2_{E\min}}{2n}}\right)-1}\right)}, \tag{11}$$

where $V_n(r)$ is defined as the volume of a sphere with radius r in the n-dimensional torus with the Euclidean distance 2π in each dimension. Just as with Piret's bound, it is a bound on $d^2_{E\min}(C)/n$ for a given rate as $n \to \infty$.

3. Problem formulation

The first result in the present research is a general and not very explicit bound, which is valid for arbitrary values of the parameters q, n and $|C|$. The second result is an explicit bound, valid for $q = 8$ only. We next start the argument and simultaneously present results of previous papers [5–7].

Let $S_{\delta,t}(\mathbf{z})$ be a sphere induced by δ, centered at $\mathbf{z}$ with radius t, i.e.

$$S_{\delta,t}(\mathbf{z}) = \left\{ \mathbf{y} : \sum_{i=1}^{\lfloor q/2 \rfloor} \delta(i) c_i(\mathbf{z}, \mathbf{y}) \le t \right\}. \tag{12}$$

Observe that the number of words in a sphere is independent of the word that lies at its center.

We generalize Elias' argument by using a critical sphere induced by δ, instead of a critical sphere induced by d^2_E. Define $K = \left\lceil |C|\,|S_{\delta,t}|q^{-n} \right\rceil$, and assume that t is large enough so that $|C|\,|S_{\delta,t}|q^{-n} > 1$. According to Elias' argument, there now exists a sphere $S_{\delta,t}(\mathbf{y}^*)$ containing at least K codewords, and by argument of translation, we may assume that $\mathbf{y}^* = \mathbf{0}$. Now let $W = S_{\delta,t}(\mathbf{y}^*) \cap C$, so $|W| = K$. We trivially have

$$d^2_{E\min}(C) \le d^2_{E\min}(W) \le d^2_{E\text{mean}}(W), \tag{13}$$

where $d^2_{E\text{mean}}(W)$ is the average distance between the codewords in W. Elias [1, pp. 318–321] bounds $d^2_{E\text{mean}}(W)$ by

$$\frac{K^2 x(2-x)\bar{D}n}{K(K-1)}, \tag{14}$$

where $\bar{D}$ is the average distance between letters $\sum_{j=0}^{q-1} d(j)$, which when d is d^2_E results in $\bar{D} = 2$. If the radius of the critical sphere is t, then $x = t/\bar{D}n$. This then also works as a bound on $d^2_{E\min}(W)$.

In [5], the use of a critical sphere induced by the distance measure δ, where $\delta(1) = 1$ and $\delta(i) = \infty$ for $i > 1$, allowing at most t non-zeros in a sphere, resulted in the bound

$$d^2_{E\min}(C) \le \frac{t}{K-1} d^2_E(2) + 2\left(t - \frac{t}{K-1}\right) d^2_E(1). \tag{15}$$

This bound is applicable for $|C| > (q/3)^n$ only, so it cannot be used for low rates, but it is tight in many cases for high rates.

In [6], a two-parameter (t, r)-Lee metric $\delta(i) = i$ if $i \le r$ and $\delta(i) = \infty$ if $i > r$ was tried for $q = 8$. It was shown that $r = 2$ improves the bound for medium rates, while $r = 4$ is preferable for low rates.

The idea of considering a general inner distance measure δ and designing it to optimize the bound for the outer distance measure, which is a squared Euclidean, was first presented in [7]. Here a K-dependent inner distance measure was presented, as well as columns that appear to be extremal by sampling the space of all possible distance measures. Compared to that paper, the present paper presents an improved K-dependent distance measure. Furthermore, in this paper a partial optimality of this distance measure is proven.

4. General results

Continuing the argument of the previous section, we have a sphere $S_{\delta,t}(\mathbf{w})$ containing at least $K = \lceil |C|\,|S_{\delta,t}|q^{-n}\rceil$ codewords, $W = S_{\delta,t}(\mathbf{w}) \cap C$, and we assume that $\mathbf{w} = \mathbf{0}$.

Theorem 1. *For any code C in $\mathbf{Z}_q^n$, we have the bound*

$$d^2_{E\,\min}(C) \le \min_{K\in[2,|C|]} \min_{\delta} \frac{2\widetilde{t}_K f_\delta(\widehat{\mathbf{y}})}{K-1}, \tag{16}$$

where

$$\widetilde{t}_K(\delta) = \min\left(\left\{t : K \le \lceil |C|\,|S_{\delta,t}|q^{-n}\rceil\right\}\right), \tag{17}$$

$$f_\delta(\mathbf{y}) = \frac{\sum_{j_1=2}^{K}\sum_{j_2=1}^{j_1-1} d_E^2(y_{j_1}, y_{j_2})}{\sum_{j=1}^{K}\delta(y_j)}, \tag{18}$$

and $\widehat{\mathbf{y}}$ is a vector maximizing $f_\delta(\mathbf{y})$.

Even though $\widetilde{t}_K$ is a function not only of δ, but also of n, $|C|$ and q, we usually omit those parameters as we assume that they are fixed. The same is true for the dependence that $f_\delta(\widehat{\mathbf{y}})$ has on q. We also remark that the minimum over t always exists since the sphere $S_{\delta,t}$ is defined with an inclusive inequality.

Proof. We start by representing the codewords in W as rows in a matrix M of type $K \times n$. Then we may write the average distance between the codewords as

$$d^2_{E\text{mean}}(W) = \frac{1}{\binom{K}{2}} \sum_{i=1}^{n}\sum_{j_1=2}^{K}\sum_{j_2=1}^{j_1-1} d_E^2(m_{j_1,i}, m_{j_2,i}), \tag{19}$$

with the restriction

$$\sum_{i=1}^{n}\sum_{j=1}^{K}\delta(m_{j,i}) \le Kt, \tag{20}$$

where $m_{j,i}$ is the element on row j and column i of M. The restriction comes from the weight of each codeword being at most t.

Using (18), where $\mathbf{y}$ is a column of M, we have

$$d^2_{E\text{mean}}(W) = \frac{1}{\binom{K}{2}} \sum_{i=1}^{n}\sum_{j_1=2}^{K}\sum_{j_2=1}^{j_1-1} d_E^2(m_{j_1,i}, m_{j_2,i}) = \frac{1}{\binom{K}{2}} \sum_{i=1}^{n} f_\delta(m_{\cdot,i}) \sum_{j=1}^{K}\delta(m_{j,i}), \tag{21}$$

where $m_{\cdot,i}$ is the ith column vector of M.

Let $\widehat{\mathbf{y}}$ be a column vector such that $f_\delta(\widehat{\mathbf{y}})$ achieves its maximum value. We then have

$$\begin{aligned} d^2_{E\text{mean}}(W) &= \frac{1}{\binom{K}{2}} \sum_{i=1}^{n} f_\delta(m_{\cdot,i}) \sum_{j=1}^{K}\delta(m_{j,i}) \\ &\le \frac{1}{\binom{K}{2}} f_\delta(\widehat{\mathbf{y}}) \sum_{i=1}^{n}\sum_{j=1}^{K}\delta(m_{j,i}) \le \frac{Kt}{\binom{K}{2}} f_\delta(\widehat{\mathbf{y}}) = \frac{2tf_\delta(\widehat{\mathbf{y}})}{K-1}, \end{aligned} \tag{22}$$

where the second inequality comes from (20). Note that this holds for any additive distance measure δ and any integer $K \in [2, |C|]$. We have proved the theorem. □

We next find vectors $\widehat{\mathbf{y}}$ by which δ may be chosen to optimize the bound. We start with a lemma to show that the bound is independent of the scaling of δ.

Lemma 2. *The bound in Theorem 1 is scale invariant in the distance measure δ; i.e. for any $s > 0$, let $\lambda(x, y) = s\delta(x, y)$ for every pair x, y. Then*

$$\frac{2\widetilde{t}_K(\delta)f_\delta(\widehat{\mathbf{y}})}{K-1} = \frac{2\widetilde{t}_K(\lambda)f_\lambda(\widehat{\mathbf{y}})}{K-1} \tag{23}$$

holds.

Proof. We remark that $f_\lambda(\widehat{\mathbf{y}}) = f_\delta(\widehat{\mathbf{y}})/s$ follows from the definition of f_δ in (18). Furthermore, $S_{\lambda,t}(\mathbf{z}) = S_{\delta,t/s}(\mathbf{z})$ follows from the definition of $S_{\delta,t}$ in (12). Hence, $\widetilde{t}_K(\lambda) = s\widetilde{t}_K(\delta)$. It follows that

$$\widetilde{t}_K(\lambda)f_\lambda(\widehat{\mathbf{y}}) = s\widetilde{t}_K(\delta)f_\delta(\widehat{\mathbf{y}})/s = \widetilde{t}_K(\delta)f_\delta(\widehat{\mathbf{y}}). \quad \square \tag{24}$$

In the proof of the following lemma we will need the so-called mediant addition:

$$\frac{a_1}{b_1} \oplus \frac{a_2}{b_2} = \frac{a_1+a_2}{b_1+b_2}, \tag{25}$$

presented in [2]. The number $\frac{a_1+a_2}{b_1+b_2}$ is called the *mediant* of $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$. It is similarly defined for c ratios $\frac{a_1}{b_1}, \ldots, \frac{a_c}{b_c}$, and is a weighted mean value of the ratios, as can be seen by the identity

$$\frac{a_1}{b_1} \oplus \cdots \oplus \frac{a_c}{b_c} = \frac{b_1}{b_1+\cdots+b_c}\frac{a_1}{b_1} + \cdots + \frac{b_c}{b_1+\cdots+b_c}\frac{a_c}{b_c}. \tag{26}$$

As a weighted mean, the weights are strictly between 0 and 1, and are determined by the denominators only. We thus have $\frac{a_1}{b_1} < \frac{a_1+a_2}{b_1+b_2} < \frac{a_2}{b_2}$ if $\frac{a_1}{b_1} < \frac{a_2}{b_2}$, and $\frac{a_1}{b_1} = \frac{a_1+a_2}{b_1+b_2} = \frac{a_2}{b_2}$ if $\frac{a_1}{b_1} = \frac{a_2}{b_2}$.

Next, we intend to find vectors $\widehat{\mathbf{y}}$ such that $f_\delta(\widehat{\mathbf{y}})$ achieves its maximum. This we do only in the case $q = 8$, so from here and onwards the results are restricted to $q = 8$.

5. Results for $q = 8$

Lemma 3. *For any additive distance measure δ and for any K, one of the columns*

$$\begin{aligned} &\widehat{\mathbf{y}}_1 = (1, -1, 0, \ldots, 0), \quad \widehat{\mathbf{y}}_2 = (2, 0, \ldots, 0), \quad \widehat{\mathbf{y}}_3 = (3, 0, \ldots, 0), \\ &\widehat{\mathbf{y}}_4 = (4, 0, \ldots, 0), \quad \widehat{\mathbf{y}}_5 = (1, -2, 0, \ldots, 0), \quad \widehat{\mathbf{y}}_6 = (2, -2, 0, \ldots, 0) \end{aligned} \tag{27}$$

provides a maximum for

$$f(\mathbf{y}) = \frac{\sum_{j=2}^{K}\sum_{i=1}^{j-1} d_E^2(y_i, y_j)}{\sum_{i=1}^{K}\delta(y_i)}. \tag{28}$$

Furthermore, $f(\widehat{\mathbf{y}}_2) = f(\widehat{\mathbf{y}}_6)$.

Proof. Maximization of the function $f_\delta(\mathbf{y})$ is done by a sequence of transformations of the variables. We first introduce the functions $a_i(\mathbf{y})$ that counts the number of occurrences of i in the column $\mathbf{y}$. That is, $a_0(\mathbf{y})$ is the number of zeros, $a_1(\mathbf{y})$ the number of 1s, $a_7(\mathbf{y})$ the number of -1s (as $-1 \equiv_8 7$), and so on. Since the length of the column $\mathbf{y}$ is K, we know that $K = \sum_{i=0}^{7} a_i(\mathbf{y})$.

The function $f_\delta(\mathbf{y})$ can then be rewritten as follows:

$$\begin{aligned} f_\delta(\mathbf{y}) &= \frac{\sum_{i=2}^{K}\sum_{j=1}^{i-1} d_E^2(y_i, y_j)}{\sum_{i=1}^{K}\delta(y_i)} \\ &= \frac{\sum_{i=1}^{3}\sum_{j=0}^{7} d_E^2(i)a_j a_{j+i} + \sum_{i=0}^{3} d_E^2(4)a_i a_{i+4}}{\sum_{i=1}^{3}\delta(i)(a_i + a_{-i}) + \delta(4)a_4}. \end{aligned} \tag{29}$$

The main objective is to maximize f_δ with respect to $a_0, \ldots, a_7$. Note that, while there are 8^K different columns $(y_1, \ldots, y_K)$, there are only $\binom{8+K-1}{K}$ different vectors $(a_0, \ldots, a_7)$. This is the number of selections of K objects out of eight

alternatives with repetition but without order, since by going from $(y_1, \ldots, y_K)$ to $(a_0(\mathbf{y}), \ldots, a_7(\mathbf{y}))$ we have removed order changes that are insignificant for the value of f_δ. It is independent of rearrangements as $(y_1, y_2, \ldots, y_K) \to (y_2, y_1, \ldots, y_K)$.

We now proceed to the next transformation. The function can be expanded as

$$f_\delta = \frac{g_1 d_E^2(1) + g_2 d_E^2(2) + g_3 d_E^2(3) + g_4 d_E^2(4)}{\delta(1)\,(a_1 + a_7) + \delta(2)\,(a_2 + a_6) + \delta(3)\,(a_3 + a_5) + \delta(4) a_4}, \tag{30}$$

where

$$\begin{aligned} g_1 &= (a_0 a_1 + a_1 a_2 + a_2 a_3 + a_3 a_4 + a_4 a_5 + a_5 a_6 + a_6 a_7 + a_7 a_0) \\ g_2 &= (a_0 a_2 + a_1 a_3 + a_2 a_4 + a_3 a_5 + a_4 a_6 + a_5 a_7 + a_6 a_0 + a_7 a_1) \\ g_3 &= (a_0 a_3 + a_1 a_4 + a_2 a_5 + a_3 a_6 + a_4 a_7 + a_5 a_0 + a_6 a_1 + a_7 a_2) \\ g_4 &= (a_0 a_4 + a_1 a_5 + a_2 a_6 + a_3 a_7)\,. \end{aligned} \tag{31}$$

Now, rewriting f_δ in terms of the functions α_i, $i = 0, \ldots, 7$, where

$$\begin{aligned} \alpha_0 &= a_0 & \alpha_4 &= a_4 \\ \alpha_1 &= a_1 + a_7 & \alpha_5 &= a_3 - a_5 \\ \alpha_2 &= a_2 + a_6 & \alpha_6 &= a_2 - a_6 \\ \alpha_3 &= a_3 + a_5 & \alpha_7 &= a_1 - a_7, \end{aligned} \tag{32}$$

exploits the symmetries of the problem, and leaves us with a denominator which is far easier to handle. It has inverse relations

$$\begin{aligned} a_0 &= \alpha_0 & a_4 &= \alpha_4 \\ a_1 &= \frac{\alpha_1 + \alpha_7}{2} & a_5 &= \frac{\alpha_3 - \alpha_5}{2} \\ a_2 &= \frac{\alpha_2 + \alpha_6}{2} & a_6 &= \frac{\alpha_2 - \alpha_6}{2} \\ a_3 &= \frac{\alpha_3 + \alpha_5}{2} & a_7 &= \frac{\alpha_1 - \alpha_7}{2}. \end{aligned} \tag{33}$$

Pure calculation proves that

$$f_\delta = \frac{h_1 d_E^2(1) + h_2 d_E^2(2) + h_3 d_E^2(3) + h_4 d_E^2(4)}{4\,(\delta(1)\alpha_1 + \delta(2)\alpha_2 + \delta(3)\alpha_3 + \delta(4)\alpha_4)}, \tag{34}$$

where

$$\begin{aligned} h_1 &= 4\alpha_0\alpha_1 + 2\alpha_1\alpha_2 + 2\alpha_2\alpha_3 + 4\alpha_3\alpha_4 + 2\alpha_5\alpha_6 + 2\alpha_6\alpha_7 \\ h_2 &= 4\alpha_0\alpha_2 + \alpha_1^2 + 2\alpha_1\alpha_3 + 4\alpha_2\alpha_4 + \alpha_3^2 - \alpha_5^2 + 2\alpha_5\alpha_7 - \alpha_7^2 \\ h_3 &= 4\alpha_0\alpha_3 + 4\alpha_1\alpha_4 + 2\alpha_1\alpha_2 + 2\alpha_2\alpha_3 - 2\alpha_5\alpha_6 - 2\alpha_6\alpha_7 \\ h_4 &= 4\alpha_0\alpha_4 + 2\alpha_1\alpha_3 + \alpha_2^2 - 2\alpha_5\alpha_7 - \alpha_6^2. \end{aligned} \tag{35}$$

Recall that $a_0 = K - \sum_{i=1}^{7} a_i$, which gives $\alpha_0 = K - \sum_{i=1}^{4} \alpha_i$. Also, since we have the restriction $q = 8$, which is studied here, we have

$$\begin{aligned} &d_E^2(0) = 0, \\ &d_E^2(1) = d_E^2(7) = 4\sin^2\frac{\pi}{8} = 2 - \sqrt{2}, \\ &d_E^2(2) = d_E^2(6) = 4\sin^2\frac{2\pi}{8} = 2, \\ &d_E^2(3) = d_E^2(5) = 4\sin^2\frac{3\pi}{8} = 2 + \sqrt{2}, \quad \text{and} \\ &d_E^2(4) = 4\sin^2\frac{4\pi}{8} = 4. \end{aligned} \tag{36}$$

This makes it possible to rewrite f_δ as

$$f_\delta = \frac{4K\sum_{i=1}^{4}\alpha_i d_E^2(i) - \left(\sum_{i=1}^{4}\alpha_i d_E^2(i)\right)^2 - \left(\sqrt{2}\alpha_5 + 2\alpha_6 + \sqrt{2}\alpha_7\right)^2}{4\sum_{i=1}^{4}\delta_i\alpha_i}. \tag{37}$$

By construction, for any $\mathbf{x}$, the quantities $\alpha_1(\mathbf{x})$, $\alpha_2(\mathbf{x})$, $\alpha_3(\mathbf{x})$ and $\alpha_4(\mathbf{x})$ are non-negative integers, at least one greater than

zero, while $\alpha_5(\mathbf{x})$, $\alpha_6(\mathbf{x})$ and $\alpha_7(\mathbf{x})$ are integers, possibly negative. Furthermore, we know that $\alpha_1(\mathbf{x})+\alpha_7(\mathbf{x})$, $\alpha_2(\mathbf{x})+\alpha_6(\mathbf{x})$ and $\alpha_3(\mathbf{x})+\alpha_5(\mathbf{x})$ are even numbers.

Next, we consider the function

$$\varphi_\delta = \frac{4K\sum_{i=1}^{4}\alpha_i d_E^2(i) - \left(\sum_{i=1}^{4}\alpha_i d_E^2(i)\right)^2}{4\sum_{i=1}^{4}\delta(i)\alpha_i}. \tag{38}$$

Obviously we have $f_\delta(\mathbf{x}) \le \varphi_\delta(\mathbf{x})$ for any $\mathbf{x}$.

Let $\mathbf{y}_1 = (1, 0, \ldots, 0)$, $\mathbf{y}_2 = (2, 0, \ldots, 0)$, $\mathbf{y}_3 = (3, 0, \ldots, 0)$, $\mathbf{y}_4 = (4, 0, \ldots, 0)$, and observe that we have

$$\begin{aligned} f_\delta(\mathbf{y}_1) &= \frac{4Kd_E^2(1) - d_E^4(1) - 2}{4\delta(1)} \qquad f_\delta(\mathbf{y}_2) = \frac{4Kd_E^2(2) - d_E^4(2) - 4}{4\delta(2)} \\ f_\delta(\mathbf{y}_3) &= \frac{4Kd_E^2(3) - d_E^4(3) - 2}{4\delta(3)} \qquad f_\delta(\mathbf{y}_4) = \frac{4Kd_E^2(4) - d_E^4(4)}{4\delta(4)}. \end{aligned} \tag{39}$$

Now, any column $\mathbf{x}$ where

$$\begin{aligned} f_\delta(\mathbf{x}) &\le \frac{\alpha_1(\mathbf{x})f_\delta(\mathbf{y}_1)}{\alpha_1(\mathbf{x})} \oplus \frac{\alpha_2(\mathbf{x})f_\delta(\mathbf{y}_2)}{\alpha_2(\mathbf{x})} \oplus \frac{\alpha_3(\mathbf{x})f_\delta(\mathbf{y}_3)}{\alpha_3(\mathbf{x})} \oplus \frac{\alpha_4(\mathbf{x})f_\delta(\mathbf{y}_4)}{\alpha_4(\mathbf{x})} \\ &\le \max(f_\delta(\mathbf{y}_1), f_\delta(\mathbf{y}_2), f_\delta(\mathbf{y}_3), f_\delta(\mathbf{y}_4)) \end{aligned} \tag{40}$$

cannot be extremal. There are still many columns that must be compared, so we start by discarding a large set of columns which cannot be extremal.

Since we have $f_\delta \le \varphi_\delta$, we may first discard all $\mathbf{x}$ where

$$\varphi_\delta(\mathbf{x}) \le \frac{\alpha_1(\mathbf{x})f_\delta(\mathbf{y}_1)}{\alpha_1(\mathbf{x})} \oplus \frac{\alpha_2(\mathbf{x})f_\delta(\mathbf{y}_2)}{\alpha_2(\mathbf{x})} \oplus \frac{\alpha_3(\mathbf{x})f_\delta(\mathbf{y}_3)}{\alpha_3(\mathbf{x})} \oplus \frac{\alpha_4(\mathbf{x})f_\delta(\mathbf{y}_4)}{\alpha_4(\mathbf{x})}. \tag{41}$$

This condition is equivalent to

$$\frac{4K\sum_{i=1}^{4}\alpha_i(\mathbf{x})d_E^2(i) - \left(\sum_{i=1}^{4}\alpha_i(\mathbf{x})d_E^2(i)\right)^2}{4\sum_{i=1}^{4}\delta(i)\alpha_i(\mathbf{x})} \le \frac{4K\sum_{i=1}^{4}\alpha_i(\mathbf{x})d_E^2(i) - \sum_{i=1}^{4}\alpha_i(\mathbf{x})d_E^4(i) - 2\alpha_1(\mathbf{x}) - 4\alpha_2(\mathbf{x}) - 2\alpha_3(\mathbf{x})}{4\sum_{i=1}^{4}\delta(i)\alpha_i(\mathbf{x})}, \tag{42}$$

which can also be expressed as

$$\sum_{i=1}^{4}\alpha_i(\mathbf{x})d_E^4(i) + 2\alpha_1(\mathbf{x}) + 4\alpha_2(\mathbf{x}) + 2\alpha_3(\mathbf{x}) \le \left(\sum_{i=1}^{4}\alpha_i(\mathbf{x})d_E^2(i)\right)^2. \tag{43}$$

We may immediately discard all columns $\mathbf{x}$ with $\alpha_1(\mathbf{x}) \ge 7$, $\alpha_2(\mathbf{x}) \ge 3$, $\alpha_3(\mathbf{x}) \ge 2$ or $\alpha_4(\mathbf{x}) \ge 2$, as any of these inequalities being satisfied will make inequality (43) true. This leaves us with $7 \times 3 \times 2 \times 2 = 84$ columns to examine. Testing these with condition (40), we find only 14 columns which may be extremal, namely

$$\begin{aligned} &\mathbf{y}_1 = (1, 0, \ldots, 0), && \mathbf{y}_2 = (2, 0, \ldots, 0), \\ &\mathbf{y}_3 = (3, 0, \ldots, 0), && \mathbf{y}_4 = (4, 0, \ldots, 0), \\ &\mathbf{y}_5 = (1, -2, 0, \ldots, 0), && \mathbf{y}_6 = (2, -2, 0, \ldots, 0), \\ &\mathbf{y}_7 = (1, -3, 0, \ldots, 0), && \mathbf{y}_8 = (1, -1, 0, \ldots, 0), \\ &\mathbf{y}_9 = (1, 1, -2, 0, \ldots, 0), && \mathbf{y}_{10} = (1, 1, -1, -2, 0, \ldots, 0), \\ &\mathbf{y}_{11} = (1, 1, -1, 0, \ldots, 0), && \mathbf{y}_{12} = (1, 1, -1, -1, 0, \ldots, 0), \\ &\mathbf{y}_{13} = (1, 1, 1, -1, -1, 0, \ldots, 0), && \mathbf{y}_{14} = (1, 1, 1, -1, -1, -1, 0, \ldots, 0). \end{aligned} \tag{44}$$

Since

$$\begin{aligned} f_\delta(\mathbf{y}_{10}) &= f_\delta(\mathbf{y}_{10}) \oplus f_\delta(\mathbf{y}_{10}) < f_\delta(\mathbf{y}_8) \oplus f_\delta(\mathbf{y}_8) \oplus f_\delta(\mathbf{y}_8) \oplus f_\delta(\mathbf{y}_6) \\ &\le \max(f_\delta(\mathbf{y}_8), f_\delta(\mathbf{y}_6)), \end{aligned} \tag{45}$$

we may conclude that $f_\delta(\mathbf{y}_{10})$ cannot be extremal. Continuing to reduce the set of columns in our list in this manner, we end up with only the vectors given in the lemma. Also, $f_\delta(\widehat{\mathbf{y}}_2) = f_\delta(\widehat{\mathbf{y}}_6)$ follows from $f_\delta(\widehat{\mathbf{y}}_2) \oplus f_\delta(\widehat{\mathbf{y}}_2) = f_\delta(\widehat{\mathbf{y}}_6)$. Those six columns are extremal, and the set cannot be reduced further. This follows by considering different distance measures δ such that

they all cause f_δ to achieve its maximum value, which we know it does for at least one of the six columns. Considering the distance measure

$$\begin{aligned} \delta(1) &= (2-\sqrt{2})(K-1)-3+2\sqrt{2}, \quad & \delta(2) &= 2(K-1)+\sqrt{2}-1, \\ \delta(3) &= (2+\sqrt{2})(K-1), & \delta(4) &= 4(K-1), \end{aligned} \tag{46}$$

we get that $\widehat{\mathbf{y}}_1, \widehat{\mathbf{y}}_3, \widehat{\mathbf{y}}_4$ and $\widehat{\mathbf{y}}_5$ are extremal. Considering the distance measure

$$\begin{aligned} \delta(1) &= (2-\sqrt{2})(K-1)-4+3\sqrt{2}, \quad & \delta(2) &= 2(K-1), \\ \delta(3) &= (2+\sqrt{2})(K-1), & \delta(4) &= 4(K-1), \end{aligned} \tag{47}$$

we get that $\widehat{\mathbf{y}}_2, \widehat{\mathbf{y}}_3, \widehat{\mathbf{y}}_4, \widehat{\mathbf{y}}_5$ and $\widehat{\mathbf{y}}_6$ are extremal. □

Equipped with knowledge about which columns are extremal, we can specify which δ minimize $f_\delta(\widehat{\mathbf{y}})$.

Theorem 4. *A distance measure δ which minimizes $f_\delta(\widehat{\mathbf{y}})$ can in the case $q = 8$ be described as*

$$\begin{aligned} \delta(1) &= (2-\sqrt{2})(K-1)-2+2\sqrt{2}-h \\ \delta(2) &= 2(K-1)+h \\ \delta(3) &= (2+\sqrt{2})(K-1) \\ \delta(4) &= 4(K-1), \end{aligned} \tag{48}$$

for any $h \in [0, \sqrt{2}-1]$.

Furthermore, with

$$\sum_{i=1}^{4} \delta(i) = 10(K-1)-2+2\sqrt{2}, \tag{49}$$

the minimum value of $f_\delta(\widehat{\mathbf{y}})$ is 1.

Proof. Let $B = f_\delta(\widehat{\mathbf{y}})$. We then have

$$f_\delta(\widehat{\mathbf{y}}_1) \le B \Leftrightarrow \frac{(2-\sqrt{2})(K-1)-1+\sqrt{2}}{\delta(1)} \le B, \tag{50}$$

$$f_\delta(\widehat{\mathbf{y}}_2) \le B \Leftrightarrow \frac{2(K-1)}{\delta(2)} \le B, \tag{51}$$

$$f_\delta(\widehat{\mathbf{y}}_3) \le B \Leftrightarrow \frac{(2+\sqrt{2})(K-1)}{\delta(3)} \le B, \tag{52}$$

$$f_\delta(\widehat{\mathbf{y}}_4) \le B \Leftrightarrow \frac{4(K-1)}{\delta(4)} \le B, \tag{53}$$

$$f_\delta(\widehat{\mathbf{y}}_5) \le B \Leftrightarrow \frac{(4-\sqrt{2})(K-1)-2+2\sqrt{2}}{\delta(1)+\delta(2)} \le B, \tag{54}$$

where at least one of the inequalities is an equality. From (52)–(54), we get

$$\frac{10(K-1)-2+2\sqrt{2}}{\delta(1)+\delta(2)+\delta(3)+\delta(4)} \le B \tag{55}$$

by use of mediant addition. By the normalization (49) on δ, we thus have $B \ge 1$. By letting (52)–(54) all be equalities, we get $B = 1$, which is the lowest value we can get on B. (Using (50)–(53) in a similar manner only gives a less tight bound on B, and so does not determine B.)

So distance measures δ which minimize B and give $B = 1$ must give equality in (52)–(54) and satisfy (50) and (51). These are exactly the distance measures described in the theorem. □

Combining Theorems 1 and 4 with Lemma 2, we get the following corollary.

Corollary 5. *For any code C in $\mathbf{Z}_8^n$, we have that*

$$d_{E\min}^2(C) \le \min_{K \in [2,|C|]} \min_{\delta \in \Delta} \frac{2\widetilde{t}_K}{K-1} \tag{56}$$

holds, where Δ is the set of distance measures with

$$\sum_{i=1}^{4} \delta(i) = 10(K-1) - 2 + 2\sqrt{2} \tag{57}$$

and

$$\widetilde{t}_K(\delta) = \min\left(\left\{t : K \leq \left\lceil |C|\,|S_{\delta,t}|q^{-n}\right\rceil\right\}\right). \tag{58}$$

6. Conclusions

In this paper, we have improved previous upper bounds for the minimum Euclidean distance. One of the bounds is valid for any combination of the three parameters $|C|$, n and q, while the other is explicit in the two parameters $|C|$ and n for the case $q = 8$.

The results develop the Elias sphere method to provide an improved bound on the minimum Euclidean distance that is non-asymptotic. The proof method is not tied to a certain structure of codes, and applies for any PSK block code with parameters $q = 8$, n and $|C|$. This means that one possible continuation is to investigate other distance measures than a Euclidean by following a similar path starting with the Elias sphere. It may be an even more challenging task to investigate if similar bounds also can be constructed for PSK Trellis codes, having a different basic structure.

Next we give an overview of the technical method of this paper. First Elias' method, [1, pp. 318–321], was followed. Here the problem was localized to a critical sphere, where codewords are at least as dense as elsewhere in the code, and the minimum distance between codewords in the critical sphere is trivially bounded by the average distance between them. However, in this line of research, the critical sphere is defined in terms of a general distance measure, δ, characterized by its values $\delta(i)$ for integers i, called the *inner distance measure*. Later, the values of the coefficients were chosen to obtain the best possible bound on the *outer distance measure*, which here is the squared Euclidean distance.

Still following Elias, the average distance between the codewords in the sphere is bounded by listing the codewords as rows in a matrix, and seeking columns of the matrix which will maximize the average distance. Elias sought columns that maximized the average distance between codewords and he considered compositions of the columns, allowing columns where each symbol may appear a continuous number of times. Allowing such compositions is an approximation which we avoid. Instead, by fixing $q = 8$, we found all columns which can give the maximal average distance between the codewords in the critical sphere, independently of the inner distance measure δ. Such columns are called extremal columns. We then chose the values of $\delta(i)$ to optimize the bound on $d^2_{E\,\min}(C)$, which gave one of the main results.

The bound is a product of two factors, both depending on the shape of the spheres. We minimized one of these factors, namely the factor which intuitively is more sensitive to the inner distance measure. While this is not certain to optimize the bound on the $d^2_{E\,\min}(C)$, consisting of two factors, the new bound is as good as previous bounds, and is strictly better for low-rate codes.

Central in the solution is that for $q = 8$ it turns out that only six columns can be singled out as extremal, independently of the inner distance measure. Of these six, for given n and $|C|$, five are used since two of them give identical values, defining an optimal inner distance measure with respect to one factor of the bound.

While there are many high-rate codes which meet the bounds (older bounds as well as the new bound), only a few medium-rate codes and no low-rate codes which meet the bound are known. It is thus of interest for low and medium rates either to improve the bound or to find codes C with higher $d^2_{E\,\min}(C)$.

References

[1] E.R. Berlekamp, Algebraic Coding Theory, McGraw Hill, New York, 1968.
[2] R. Graham, D. Knuth, O. Patashnik, Concrete Mathematics, Addison Wesley, ISBN: 0-201-14236-8, 1994.
[3] H. Imai, S. Hirakawa, A new multilevel coding method using error-correcting codes, IEEE Transactions on Information Theory 23 (3) (1997) 371–377.
[4] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, The Netherlands, 1977.
[5] M. Nilsson, H. Lennerstad, An upper bound on the minimum Euclidean distance for block coded phase shift keying, IEEE Transactions on Information Theory 46 (2) (2000) 656–662.
[6] M. Nilsson, H. Lennerstad, Improved upper bound on the minimum Euclidean distance for block coded phase shift keying, in: Proceedings of RVK05, Linköping, Sweden, 2005.
[7] M. Nilsson, H. Lennerstad, E. Laksman, A two-metric approach to improve bounds on the minimum Euclidean distance for block codes, in: Proceedings of RVK08, Växjö, Sweden, 2008.
[8] Ph. Piret, Bounds for codes over the unit circle, IEEE Transactions on Information Theory IT-32 (1986) 760–767.
[9] S. Sayegh, A class of optimum block codes in signal space, IEEE Transactions on Communications 34 (10) (1986) 1043–1045.
[10] H. Tanabe, H. Umeda, M.A. Salam, A new construction method of multilevel coded modulation with a good Euclidean minimum distance, in: 1997 IEEE International Symposium on Information Theory, 29 June–4 July, 1997, p. 437.
[11] A.D. Wyner, Bounds on communication with polyphase coding, Bell System Technical Journal 45 (1966) 523–559.