

Tight Bounds on the Minimum Euclidean Distance for Block Coded Phase Shift Keying

Magnus Nilsson, Håkan Lennerstad

Abstract

We present upper and lower bounds on the minimum Euclidean distance $d_{Emin}(C)$ for block coded PSK.

The upper bound is an analytic expression depending on the alphabet size q , the block length n and the number of codewords $|C|$ of the code C . This bound is valid for all block codes with $q \geq 4$ and with medium or high rate - codes where $|C| > (q/3)^n$.

The lower bound is valid for Gray coded binary codes only. This bound is a function of q and of the minimum Hamming distance $d_{Hmin}(B)$ of the corresponding binary code B .

We apply the results on two main classes of block codes for PSK; Gray coded binary codes and multilevel codes. There are several known codes in both classes which satisfy the upper bound on $d_{Emin}(C)$ with equality. These codes are therefore best possible, given q , n and $|C|$. We can deduce that the upper bound for many parameters q , n and $|C|$ is optimal or near optimal.

In the case of Gray coded binary codes, both bounds can be applied. It follows for many binary codes that the upper and the lower bounds on $d_{Emin}(C)$ coincide. Hence, for these codes $d_{Emin}(C)$ is maximal.

Keywords

Block codes, phase shift keying, minimum Euclidean distance, multilevel codes, coded modulation, Gray code, non-linear codes.

I. INTRODUCTION

Combined coding and modulation have been discussed by many authors. One of the main problems considered in the literature is to construct codes that are efficient with respect to some

fixed modulation scheme. The most widely used measure of efficiency for such codes is the minimum Euclidean distance. The minimum Euclidean distance is a relevant measure when considering communication over an additive white Gaussian noise (AWGN) channel. In this paper we present upper and lower bounds on the minimum Euclidean distance for block coded phase shift keying (PSK).

Piret presents in [10] results which give asymptotic upper and lower bounds on the minimum Euclidean distance for block codes as $n \rightarrow \infty$. These results are essential when considering codes with very large block length. For given parameters q, n and $|C|$, however, the results can only be used as guidelines for estimating the largest possible $d_{Emin}(C)$. Since monotonicity in n is not known, bounds for finite n do not follow.

In contrast, for each set of parameters q, n and $|C|$ such that $q \geq 4$ and $|C| > (q/3)^n$, the present results gives an upper bound on $d_{Emin}(C)$. As we will see, for many choices of q, n and $|C|$, the bound is optimal.

One simple and efficient construction of block codes for PSK is that of combining conventional binary block codes with Gray coding. Gray coding has been discussed in many textbooks, for example Haykin [4] or Wilson [14]. Other constructions of block codes for PSK aiming for large minimum Euclidean distance have been presented by Caire and Biglieri [1], Chen, Chen and Loeliger [2], Ginzburg [3], Imai and Hirakawa [5], Isaksson and Zetterberg [6], Kschischang, de Buda and Pasupathy [7], Piret [9], Sayegh [11], Tanabe-Hideiko, Umeda-Hiroyuki [12] and Tanner [13]. A majority of the constructions, as those discussed in [1], [2], [3], [4], [5], [7], [11], [12] and [13], are based on the idea of using conventional block codes as tools. Especially for high rates, several known Gray coded binary codes, but also many other codes obtained from [1], [2], [3], [5], [6], [7], [11] and [13], satisfy our upper bound with equality (see Section III). Hence, for each of these codes, there does not exist a code with the same parameters q, n and $|C|$ and a larger minimum Euclidean distance.

For Gray coded binary codes we further prove a lower bound on $d_{Emin}(C)$ in terms of the minimum Hamming distance of the binary code. By using the upper and lower bounds together we can show that several known codes are optimal.

As described, the two bounds have a different degree of generality. They are also proved by entirely different methods. The key argument in the proof of the lower bound is an estimate of the squared Euclidean distance by a quantity leading to Hamming distance (Lemma IV.3). The Gray coding technique is essential for the proof.

The deduction of the upper bound is more elaborate. The remainder of this section, except the last paragraph where the organization of the paper is described, is concerned with a conceptual description of the main arguments used to prove the upper bound.

Consider a code C with $|C|$ codewords. C is a subset of the universe U of all words with alphabet size q and block length n - we have $|U| = q^n$. To each word $z \in U$ we define a neighborhood $S_t(z)$. The parameter t controls the number of words in a neighborhood. The neighborhoods $S_t(z)$ are equally shaped for each word. For example, for any two words z and y the number of words in the neighborhood is constant: $|S_t(z)| = |S_t(y)| = |S_t|$. The neighborhoods also possess the following important symmetry: $y \in S_t(z) \Leftrightarrow z \in S_t(y)$.

We remark that the neighborhoods $S_t(z)$ are used as a vehicle to transfer the problem of minimum Euclidean distance from U into one neighborhood only, and here calculate the upper bound. These neighbourhoods are not decision regions - which is a common use of neighbourhoods within coding theory.

We choose t so that $|C||S_t| > |U|$, i.e. the neighborhoods of the codewords intersect. It then follows that there is at least one word y^* contained in at least $\lceil |C||S_t|/|U| \rceil = k$ neighborhoods of codewords. Here $\lceil x \rceil$ is the ceiling function: the smallest integer not less than x . By the symmetry, the neighborhood of y^* then contains at least k codewords. Now we have arrived to a set with known structure containing at least k codewords. Note that the density of codewords in this

neighborhood ($k/|S_t|$) is never lower than the density of codewords in U ($|C|/|U|$), but sometimes higher. We prove that the Euclidean distance between the closest codewords in the neighborhood of y^* cannot exceed the bound, which gives an upper bound of the minimum Euclidean distance for the code C . The argument giving the neighborhood of y^* can be illustrated as in Figure I.1.

By considering intersecting neighborhoods, we are thus able to reduce the problem of $|C|$ codewords in U into a problem about k codewords in one neighborhood. The main part of the proof is concerned with the calculation of the bound in the reduced problem. Here we first note that the minimum Euclidean distance certainly is bounded from above by the *mean* Euclidean distance. It turns out that in this case the mean is maximal when all possible distances are practically equal. Then the minimum and the mean differ very little, hence the estimate of a minimum by a mean is

quantitatively efficient. By mathematical methods, involving certain reformulations of the problem, we calculate the upper bound on the mean Euclidean distance for the k codewords in the neighborhood.

We need neighborhoods with a structure simple enough in order to calculate explicit bounds. Further, since we want to establish an upper bound on the mean Euclidean distance, we also prefer neighborhoods where all distances within a neighborhood are small. These requirements are well fulfilled in the type of neighborhood which is used.

The paper is organized as follows. Section II presents the mathematical formulation of the bounds on $d_{Emin}(C)$. Section III provides tables of Gray coded binary codes and multilevel codes which turn out to be optimal. Section IV contains the proofs of the bounds.

II. FORMULATION OF THE BOUNDS

A. The Upper Bound

In this section the upper bound on the minimum Euclidean distance, $d_{Emin}(C)$, is formulated in Theorems II.1, II.2 and II.3. The theorems are proved in Section IV. We begin with definitions that are needed for the formulation and for the application of the result.

A block code for q -ary PSK is referred to as a block code over \mathbf{Z}_q , where \mathbf{Z}_q is the ring of integers $0, 1, 2, \dots, q \Leftrightarrow 1$ (modulo q). A block code C over \mathbf{Z}_q of block length n is a subset of \mathbf{Z}_q^n . Here \mathbf{Z}_q^n is the set of all n -tuples over \mathbf{Z}_q . The n -tuples in \mathbf{Z}_q^n are called words, and the n -tuples in C are called codewords.

Let $x = (x_1, x_2, x_3, \dots, x_n)$ and $y = (y_1, y_2, y_3, \dots, y_n)$ be two words in \mathbf{Z}_q^n . The elements of \mathbf{Z}_q may be regarded as equidistant points on a circle with radius one, as depicted together with Gray coding in Figure II.2. It follows from elementary geometrical considerations that the Euclidean distance between the points $x_i, y_i \in \mathbf{Z}_q$ on the circle is $2|\sin \frac{(x_i - y_i)\pi}{q}|$. A distance associated with

$j = |x_i \leftrightarrow y_i| \in \{0, 1, \dots, q \leftrightarrow 1\}$ steps on this circle is denoted by d_j :

$$d_j = 2 \sin \frac{j\pi}{q}. \quad (1)$$

The squared Euclidean distance between the words x and y is then defined as

$$d_E^2(x, y) = \sum_{i=1}^n d_{|x_i - y_i|}^2 = \sum_{i=1}^n 4 \sin^2 \frac{(x_i \leftrightarrow y_i)\pi}{q}, \quad (2)$$

i.e. the sum of the squared Euclidean distances between corresponding letters.

Note that this distance is consistent with the modulo q structure, since

$$\sin^2 \frac{(\pm x + mq)\pi}{q} = \sin^2 \frac{x\pi}{q}. \quad (3)$$

for all integers x and m .

Only the two smallest of the d_j 's appear explicitly in the bounds. These are

$$d_1^2 = 4 \sin^2 \frac{\pi}{q} \text{ and } d_2^2 = 4 \sin^2 \frac{2\pi}{q}. \quad (4)$$

Note that $d_2^2 = d_1^2 \cos^2 \frac{\pi}{q}$, hence if $q \geq 4$ we have

$$2d_1^2 \leq d_2^2 \leq 4d_1^2. \quad (5)$$

These relations are crucial in the proofs.

The minimum squared Euclidean distance $d_{Emin}^2(C)$ for a code C is

$$d_{Emin}^2(C) = \min_{x, y \in C, x \neq y} d_E^2(x, y). \quad (6)$$

Assume now that $q \geq 4$, and consider a block code $C \subset \mathbf{Z}_q^n$ with $|C|$ codewords.

Let $t \leq n$ be a positive integer large enough so that

$$q^{-n} |C| \sum_{i=0}^t \binom{n}{i} 2^i > 1. \quad (7)$$

Since $t \leq n$, the existence of such a t requires that

$$|C| > \left(\frac{q}{3}\right)^n. \quad (8)$$

Condition (8) means that the upper bound to be presented applies only for codes with sufficiently high rate. Usually the smallest t satisfying (7) gives the tightest bound.

We denote by $\lceil x \rceil$ the ceiling function: the smallest integer not less than x . Similarly, by $\lfloor x \rfloor$ we denote the floor function: the largest integer not larger than x .

We next define k :

$$k = \lceil q^{-n} |C| \sum_{i=0}^t \binom{n}{i} 2^i \rceil. \quad (9)$$

The requirement (7) on t clearly implies that $k \geq 2$.

We first present the preliminary bound Theorem II.1. The main part of the proofs presented in Section IV is devoted to this theorem, here the main difficulties are overcome. Theorem II.2 improves the bound of Theorem II.1. Theorem II.3 does not improve the bound but simplifies the use of it - in particular when the parameters are large.

THEOREM II.1: If C is a block code over \mathbf{Z}_q with $q \geq 4$, block length n and $|C| > \left(\frac{q}{3}\right)^n$ codewords, then

$$d_{Emin}^2(C) \leq \frac{t}{k \Leftrightarrow 1} d_2^2 + 2(t \Leftrightarrow \frac{t}{k \Leftrightarrow 1}) d_1^2.$$

When $\frac{t}{k-1}$ is not an integer, the bound can be improved by the next theorem:

THEOREM II.2: If C is a block code over \mathbf{Z}_q with $q \geq 4$, block length n and $|C| > \left(\frac{q}{3}\right)^n$ codewords, then

$$d_{Emin}^2(C) \leq \max_{a,b} (ad_2^2 + 2bd_1^2),$$

where the maximum is taken over non-negative integers a and b such that

$$\begin{cases} a + b \leq t \\ ad_2^2 + 2bd_1^2 \leq \frac{t}{k-1} d_2^2 + 2(t \Leftrightarrow \frac{t}{k-1}) d_1^2. \end{cases}$$

Theorem II.2 is equivalent to the following one parameter formulation, which leaves fewer points (a, b) to check than in Theorem II.2.

THEOREM II.3: If C is a block code over \mathbf{Z}_q with $q \geq 4$, block length n and $|C| > (\frac{q}{3})^n$ codewords, then

$$d_{Emin}^2(C) \leq \max_a (ad_2^2 + 2d_1^2 \min(\lfloor (\frac{t}{k \Leftrightarrow 1} \Leftrightarrow a) \frac{d_2^2}{2d_1^2} + t \Leftrightarrow \frac{t}{k \Leftrightarrow 1} \rfloor, t \Leftrightarrow a))$$

where

$$a = \lfloor \frac{t}{k \Leftrightarrow 1} \rfloor, \dots, \lfloor \frac{t}{k \Leftrightarrow 1} + 2 \frac{d_1^2}{d_2^2} (t \Leftrightarrow \frac{t}{k \Leftrightarrow 1}) \rfloor.$$

Theorem II.3 is favorable compared to Theorem II.2 mainly when t is large. The effect of using Theorem II.3 compared to Theorem II.2 is illustrated in Figure II.1.

We next demonstrate the application of the upper bound on $d_{Emin}^2(C)$ in one simple example.

Assume $q = 8, n = 16$ and $|C| = 2^{41}$. In this case condition (7) is not satisfied for $t = 1$, but for $t = 2$ we have

$$q^{-n}|C| \sum_{i=0}^t \binom{n}{i} 2^i = 8^{-16} \times 2^{41} \times \left(1 + 2 \times 16 + \frac{4 \times 16 \times (16 \Leftrightarrow 1)}{2}\right) \approx 4.05 \quad (10)$$

Since we have found a $t \leq n = 16$, the condition $|C| > (\frac{q}{3})^n$ is true.

Thus $k = 5$. We insert $k = 5$ and $t = 2$ into Theorem II.1:

$$d_{Emin}^2(C) \leq \frac{2}{5 \Leftrightarrow 1} d_2^2 + 2(2 \Leftrightarrow \frac{2}{5 \Leftrightarrow 1}) d_1^2 = 2 \sin^2 \frac{\pi}{4} + 12 \sin^2 \frac{\pi}{8} \approx 2.76 \quad (11)$$

Since $\frac{t}{k-1} = \frac{2}{4}$ is not an integer we will get a sharper bound by using Theorem II.2. There are four points (a, b) satisfying the conditions in the theorem: $(0, 0)$, $(0, 1)$, $(0, 2)$ and $(1, 0)$. Among these, $(a, b) = (0, 2)$ maximizes $ad_2^2 + 2bd_1^2$. We get

$$d_{Emin}^2(C) \leq 0d_2^2 + 4d_1^2 = 16 \sin^2 \frac{\pi}{8} \approx 2.34. \quad (12)$$

Codes that satisfy this bound with equality can be found in Table III.1, row 5 and in Table III.2, row 5.

B. The Lower Bound

In this subsection we formulate the lower bound on $d_{Emin}^2(C)$ for Gray coded binary block codes.

We start the subsection by defining Gray coding to an extent necessary for our results. For more details on Gray coding, see for example Haykin [4] or Wilson [14]. For the basic definitions on block codes we refer to Section II-A.

Consider a binary block code B with block length $n_B = nr$. Gray coding converts the binary code B into a specific 2^r -ary code C .

Each codeword in B is divided in n binary r -tuples. Each r -tuple is converted into one 2^r -ary letter. The code B thus gives a 2^r -ary code C with block length n .

The Gray code is constructed in such a way that if two elements in \mathbf{Z}_q are at squared Euclidean distance d_1^2 from each other, i.e. are neighbors, then the corresponding binary r -tuples differ in exactly one bit. Figure II.2 illustrates Gray coding for $q = 8$. We remark that this coding is different from the commonly known transcription between binary numbers and 2^r -ary numbers, where the binary number $b_1b_2\dots b_k$, $b_i \in \mathbf{Z}_2$, represents the 2^r -ary number $\sum_{i=1}^k b_i 2^{k-i}$.

We summarize the quantitative relations: $C \subset \mathbf{Z}_q^n$, $B \subset \mathbf{Z}_2^{nr}$, $q = 2^r$ and $|C| = |B|$.

C has a squared minimum Euclidean distance $d_{Emin}^2(C)$ which is bounded from below by the minimum Hamming distance $d_{Hmin}(B)$ of the corresponding binary code B :

THEOREM II.4:

$$d_{Emin}^2(C) \geq d_{Hmin}(B)d_1^2.$$

The quantity d_1 is defined in Section II-A. Applications of the Theorem are presented in Section III, and the proof is given in Section IV.

III. OPTIMAL CODES

In this section we discuss two main classes of block codes for PSK; Gray coded binary block codes and multilevel codes. Especially for high rates, both classes provide several codes that are optimal in the sense that they satisfy our upper bound on $d_{Emin}^2(C)$, presented in Section II-A with equality.

A. Gray coded binary block codes

Let B be a binary block code of block length $n_B = nr$, minimum Hamming distance $d_{Hmin}(B)$ and $|B|$ codewords. From Section II-B we conclude that Gray coding gives a 2^r -ary code C of block length n with $|C| = |B|$ codewords. The squared minimum Euclidean distance $d_{Emin}^2(C)$ is bounded from below by Theorem II.4. If $|C| > (q/3)^n$, $d_{Emin}^2(C)$ is bounded from above by Theorem II.2.

It is easy to check that if B is a single-parity code, referred to as $B2$ in the tables below, with $d_{Hmin}(B2) = 2$, then the upper and lower bounds on $d_{Emin}(C)$ coincide. Also in many cases when B is an extended Hamming code, called $B4$ in the tables ($d_{Hmin}(B4) = 4$), or an extended double error correcting BCH-code denoted by $B6$ ($d_{Hmin}(B6) = 6$), the upper and lower bounds coincide.

Hence, the corresponding 2^r -ary codes are optimal. Since $B4$ and $B6$ only exist for certain values on n_B , we have also considered shortened versions of these codes. Table III.1 shows the parameters for optimal Gray coded binary block codes.

For more details on the binary codes, $B2$, $B4$ and $B6$, including the calculation of $|B|$, we refer to textbooks as [4] or [14].

Table III.1. Optimal Gray coded binary codes.

B. Multilevel codes

Multilevel codes for PSK were introduced by Imai and Hirakawa [5], and have later been discussed by many authors: [1], [2], [3], [6], [7], [9], [11], [13] and [14].

Let $B_0, B_1, B_2, \dots, B_{r-1}$ be r binary block codes, all with the same block length n . Then

$$C = \sum_{i=0}^{r-1} 2^i B_i \quad (13)$$

is a 2^r -ary multilevel code with component codes $B_0, B_1, B_2, \dots, B_{r-1}$. The number of codewords in C is

$$|C| = \prod_{i=0}^{r-1} |B_i|, \quad (14)$$

and the squared minimum Euclidean distance is

$$d_{Emin}^2(C) = \min_{i=0, \dots, r-1} \{d_{2^i}^2 d_{Hmin}(B_i)\}. \quad (15)$$

Here d_{2^i} is defined in equation 1, in Section II-A. To avoid any misconception of the notation we point out that the index here has an exponent - we have d_k^2 where $k = 2^i$.

For a proof of (15), see for example [1].

By using the binary codes $B2$, $B4$ and $B6$ of Subsection III-A as component codes, we obtain several multilevel codes C where the value of $d_{Emin}^2(C)$ equals our upper bound. Hence, these codes are optimal. Table III.2 shows the parameters for optimal multilevel codes.

Contrary to Gray coded binary codes, multilevel codes are not restricted to the case of q being a power of 2, although we only consider this case here.

Table III.2. Optimal multilevel codes.

IV. PROOFS

A. Proof of the Upper Bound

In this subsection the Theorems II.1, II.2 and II.3 are proved. We begin with some notation.

Let z be a word in \mathbf{Z}_q^n and let $r = \lfloor \frac{q}{2} \rfloor$, i.e. r is the largest integer not larger than $\frac{q}{2}$. For $i = 0, 1, 2, \dots, r$, let $c_i(z)$ be the number of letters in z which are equal to i (modulo q) or $\Leftrightarrow i$ (modulo q). For example, $c_0(z)$ is the number of zeros in z , $c_1(z)$ the number of 1:s and -1:s, $c_2(z)$ the number of 2:s and -2:s, and so on. Since we have in total n letters, for any word $z \in \mathbf{Z}_q^n$ we clearly have $\sum_{i=0}^r c_i(z) = n$.

Let t be a positive integer, where $t \leq n$. We define the t -neighborhood of z in the following way:

$$S_t(z) = \{y; c_1(y \Leftrightarrow z) \leq t \text{ and } c_i(y \Leftrightarrow z) = 0 \text{ for } i > 1\}. \quad (16)$$

$S_t(z)$ can be described as the set of words y differing from z in at most t letters. The deviation from z in any position can only be -1, 0 or 1. It is obvious from the definition that the t -neighborhood possesses symmetry in the sense of relations: $y \in S_t(z)$ if and only if $z \in S_t(y)$.

The number of words in $S_t(z)$ is a function of n and t but independent of z . It is given by the following sum:

$$|S_t(z)| = |S_t| = \sum_{i=0}^t \binom{n}{i} 2^i. \quad (17)$$

Proof of Theorem II.1. Let $\{x_m : m = 1, 2, 3, \dots, |C|\}$ be the codewords in a block code C over \mathbf{Z}_q of block length n .

Suppose that we have $|C|$ different colors and $|S_t|$ labels of each color. Onto each word in the neighborhood $S_t(x_m)$, we put a label of the m :th color. Then, totally $|C||S_t|$ labels are distributed on at most q^n different words. On average, there are $\frac{|C||S_t|}{q^n}$ different labels on each word. Assume that t is chosen such that $\frac{|C||S_t|}{q^n} > 1$. We then define k to be

$$k = \lceil q^{-n} |C| \sum_{i=0}^t \binom{n}{i} 2^i \rceil. \quad (18)$$

Since the number of labels on a word is always an integer, there must be one word y^* having at least k labels. This is a case of the pidgeonhole principle. Thus $y^* \in S_t(x_m)$ for at least k different codewords x_m . By the symmetry property of t -neighborhoods, we can conclude that there are at least k codewords in the neighborhood $S_t(y^*)$.

Let $V = \{x_{i_1}, \dots, x_{i_k}\}$ be a set of k codewords contained in the t -neighborhood of y^* . We will derive an upper bound on $d_{Emin}^2(V)$. Since V is a subset of C , we clearly have

$$d_{Emin}^2(C) \leq d_{Emin}^2(V). \quad (19)$$

It is clear from the definition of $d_E^2(x, y)$ that for any three words x, z and y , we have $d_E^2(x \Leftrightarrow y, z \Leftrightarrow y) = d_E^2(x, z)$. If we subtract the word y^* from all codewords in V , the distances between the corresponding modified codewords are the same as between the original codewords in V . Since the k codewords x_{i_1}, \dots, x_{i_k} are in the t -neighborhood of y^* , the modified codewords $x_{i_1} \Leftrightarrow y^*, \dots, x_{i_k} \Leftrightarrow y^*$ in the t -neighborhood of 0 clearly consist of the letters 0, 1 and -1 only. We keep the notation V also for this modified set.

For simplicity we will from here on denote the members in the modified set V by $V = \{x_1, x_2, \dots, x_k\}$. Let $V^2 = \{(x_i, x_j) : x_i, x_j \in V, i < j\}$. The set V^2 can be viewed as the set of all subsets of V with exactly two members. The pairs of V^2 represent all distances which are compared when $d_{Emin}^2(V)$ is calculated.

We have $|V^2| = \binom{k}{2}$. Let

$$G(V) = \sum_{(x_i, x_j) \in V^2} d_E^2(x_i, x_j), \quad (20)$$

the sum of all possible squared distances in V . The *minimum* squared distance $d_{Emin}^2(V)$ can clearly not be larger than the *mean* squared distance. In formula:

$$d_{Emin}^2(V) \leq \frac{G(V)}{\binom{k}{2}}. \quad (21)$$

In the set V we have k codewords of length n , each codeword containing at most t non-zeros (1:s and -1:s). The quantity $G(V)$ will be bounded from above, which by (19) and (21) gives an upper bound on $d_{Emin}^2(C)$.

We will next regard the set V as a $k \times n$ -matrix with elements -1, 0 and 1. The j :th row in the matrix is the j :th codeword in V . Hence the i :th column in the matrix consists of the i :th letters of the codewords of V .

The contribution to $G(V)$ from a column with u 1:s, v -1:s and $(k \Leftrightarrow u \Leftrightarrow v)$ 0:s is

$$f(k, u, v) = uv d_2^2 + (k \Leftrightarrow u \Leftrightarrow v)(u + v)d_1^2. \quad (22)$$

This can be seen by taking all possible pairs of the elements in the column and adding the result. Equal entries give zero, one zero and one non-zero give d_1^2 , and 1 paired with -1 gives d_2^2 .

The contribution per non-zero from a column with u 1:s and v -1:s is $\frac{f(k, u, v)}{u+v}$. In the following we will show that this quantity is maximal for $u = v = 1$, and hence it's maximum value is $\frac{1}{2}(d_2^2 + (k \Leftrightarrow 2)d_1^2)$. Essentially, by multiplying the maximum contribution per non-zero with the maximum number of non-zeros in V , which is kt , we will be able to derive the following upper bound on $G(V)$:

$$\text{LEMMA IV.1: } G(V) \leq kt\left(\frac{1}{2}d_2^2 + (k \Leftrightarrow 2)d_1^2\right).$$

Once Lemma IV.1 is proved, we can also prove Theorem II.1 by (19), (21) and Lemma IV.1:

$$d_{Emin}^2(C) \leq d_{Emin}^2(V) \leq \frac{G(V)}{\binom{k}{2}} \quad (23)$$

$$\leq \frac{\frac{kt}{2}(d_2^2 + 2d_1^2(k \Leftrightarrow 2))}{\binom{k}{2}} = \frac{t}{k \Leftrightarrow 1}d_2^2 + 2d_1^2\left(t \Leftrightarrow \frac{t}{k \Leftrightarrow 1}\right). \quad (24)$$

We next define the quantity f_i :

$$f_i = f(k, [i], [i]). \quad (25)$$

This is the value of f when having an (almost) equal number of 1:s and -1:s. We are now in a position to prove that $\frac{f(k, u, v)}{u+v}$ is maximal for $u = v = 1$.

LEMMA IV.2:

$$\max_{u+v \geq 1} \frac{f(k, u, v)}{u+v} = \max_{k \geq i \geq 1} \frac{f_i}{i} = \frac{1}{2}d_2^2 + (k \Leftrightarrow 2)d_1^2.$$

The maximum is attained for $u = v = 1$, i.e. $i = 2$.

Proof of Lemma IV.2. We first prove that in each column, for a given number of non-zeros, we maximize by taking an equal number of 1:s and -1:s, or at least as equal as possible.

Consider $f(k, u \Leftrightarrow x, v + x)$ as a function of a real variable, and take the derivative with respect to x :

$$\frac{d}{dx}f(k, u \Leftrightarrow x, v + x) = \frac{d}{dx}((u \Leftrightarrow x)(v + x)d_2^2 + (k \Leftrightarrow u \Leftrightarrow v)(u + v)d_1^2) = (u \Leftrightarrow v \Leftrightarrow 2x)d_2^2. \quad (26)$$

Thus $f(k, u + x, v \Leftrightarrow x)$ is increasing for $x < \frac{u-v}{2}$, decreasing for $x > \frac{u-v}{2}$, and maximal for $x = \frac{u-v}{2}$. It follows that

$$\max_{x \text{ integer}} (f(k, u \Leftrightarrow x, v + x)) = f(k, \lceil \frac{u+v}{2} \rceil, \lfloor \frac{u+v}{2} \rfloor). \quad (27)$$

Now assume that $i = 2m, m \geq 1$. Then,

$$\frac{f(k, m, m)}{2m} = \frac{m^2 d_2^2 + 2m(k \Leftrightarrow 2m)d_1^2}{2m} = (\frac{d_2^2}{2} \Leftrightarrow 2d_1^2)m + kd_1^2, \quad (28)$$

which is decreasing as a function of m since $\frac{d_2^2}{2} \Leftrightarrow 2d_1^2 < 0$. Hence, among all even $(u+v)$:s, the quantity $\frac{f(k, u, v)}{u+v}$ is maximal if $u = v = 1$.

We next compare the case $u = v = 1$ to all cases of odd $(u+v)$:s. Assume that $i = 2m+1, m \geq 0$. Then,

$$\frac{f(k, 1, 1)}{2} \Leftrightarrow \frac{f(k, m+1, m)}{2m+1} \quad (29)$$

$$= \frac{(2m+1)f(k, 1, 1) \Leftrightarrow 2f(k, m+1, m)}{2(2m+1)} \quad (30)$$

$$= \frac{(2m+1)(d_2^2 + 2d_1^2(k \Leftrightarrow 2)) \Leftrightarrow 2m(m+1)d_2^2 \Leftrightarrow 2(2m+1)(k \Leftrightarrow 2m \Leftrightarrow 1)d_1^2}{2(2m+1)} \quad (31)$$

$$= \frac{2(4d_1^2 \Leftrightarrow d_2^2)m^2 + (d_2^2 \Leftrightarrow 2d_1^2)}{2(2m+1)}. \quad (32)$$

By (5), both terms in the numerator are non-negative for any m . Hence

$$\frac{f(k, 1, 1)}{2} \Leftrightarrow \frac{f(k, m+1, m)}{2m+1} \geq 0. \quad (33)$$

Lemma IV.2 is proved.

Proof of Lemma IV.1. Considering the matrix representation of V , let a_i be the number of columns having i non-zero letters. By the first equality in Lemma IV.2, we have for any set V :

$$G(V) \leq \sum_{i=0}^k a_i f(k, [i], [i]) = \sum_{i=0}^k a_i f_i. \quad (34)$$

The total number of non-zeros in V is at most kt , i.e.

$$\sum_{i=0}^k i a_i \leq kt. \quad (35)$$

By combining Lemma IV.2 with (34) and (35) we can complete the proof of Lemma IV.1:

$$G(V) \leq \sum_{i=0}^k a_i f_i \leq \sum_{i=0}^k a_i \frac{if_2}{2} \leq \frac{f_2}{2} \sum_{i=0}^k i a_i \leq \frac{f_2 kt}{2} = \frac{kt}{2} (d_2^2 + d_1^2 (k \Leftrightarrow 2)). \quad (36)$$

By the argument given between Lemma IV.1 and Lemma IV.2, Theorem II.1 is proved.

Proof of Theorem II.2. Theorem II.2 is an improved version of Theorem II.1. The improvement is done in three steps. For any set V , defined in the proof of Theorem II.1, we construct a new set V' for which we show the following properties:

$$1. \quad d_{Emin}^2(V') \geq d_{Emin}^2(V), \quad (37)$$

$$2. \quad d_{Emin}^2(V') \leq \frac{t}{k \Leftrightarrow 1} d_2^2 + 2d_1^2 (t \Leftrightarrow \frac{t}{k \Leftrightarrow 1}), \quad (38)$$

$$3. \quad \text{If } x' \text{ and } z' \text{ are in } V', \text{ then } d_E^2(x', z') \text{ is of the form } ad_2^2 + 2bd_1^2 \quad (39)$$

The factor 2 in the term $2bd_1^2$ in (39) is the main point of Theorem II.2, it gives most of the improvement. We show that when constructing V' it is possible to modify the codewords in V so that each codeword contains exactly t non-zeros, without decreasing the minimum Euclidean

distance. Then, $d_E^2(x', z')$ will always contain an even number of d_1^2 's, where x' and z' are any of the k modified codewords.

Let V' be a set of k words of length $n' \geq n$ with exactly t non-zeros in each word. Let the first n letters of the k words in V' be equal to the k codewords in V . The remaining $n' \Leftrightarrow n$ letters of the words in V' consist of zeros, 1:s and -1:s so that each word include exactly t non-zeros. Hence, in the new columns we fill the words with non-zeros so each word of V' consists of exactly t non-zeros.

It is clear from the construction of V' that no distance between two words in V' is smaller than the distance between the corresponding codewords in V . Thus (38) follows.

Consider the proof of Theorem II.1. Since the restrictions on V , i.e. k words and at most t non-zeros per word also hold for V' , (39) is also valid.

The minimum Euclidean distance between two words x' and y' is

$$d_E^2(x', z') = \sum_{i=1}^n 4 \sin^2 \frac{(x'_i \Leftrightarrow z'_i)\pi}{q}. \quad (40)$$

Since x' and z' are words in V' including only 0:s, 1:s and -1:s, the i :th term in (40) must be either d_2^2 (if x'_j and z'_j are non-zeros with different signs), d_1^2 (if exactly one of x'_j and z'_j is non-zero) or 0 (if $x'_j = z'_j$). Clearly, $d_E^2(x', z')$ is of the form $ad_2^2 + sd_1^2$, where a and s are non-negative integers. What remains to show is that s must be even and that $a + \frac{s}{2} \leq t$. Assume that x' and z' have non-zeros in exactly p common positions. Then $a \leq p$. The remaining $2(t \Leftrightarrow p)$ non-zeros ($(t \Leftrightarrow p)$ from each of x' and z') are in distinct positions giving $s = 2(t \Leftrightarrow p) = 2b$, where b is an integer. Finally, we have $a + b \leq p + b = t$, and thus (39) is shown.

Proof of Theorem II.3. The application of Theorem II.2 includes solving the following integer programming problem. Maximize $ad_2^2 + 2bd_1^2$, where a and b are integers such that

$$ad_2^2 + 2bd_1^2 \leq \frac{t}{k \Leftrightarrow 1} d_2^2 + 2d_1^2 (t \Leftrightarrow \frac{t}{k \Leftrightarrow 1}), \quad (41)$$

$$a + b \leq t \quad (42)$$

$$a \geq 0 \quad (43)$$

$$b \geq 0. \quad (44)$$

A graph of this integer programming problem is given by Figure II.1.

Since a normal to the first constraint is parallel to the gradient of the goal function, the solution must be close to this constraint. It is therefore enough to check all points with integer coordinates close to this line. We will look for integer points as close as possible on the left side to the straight line

$$ad_2^2 + 2bd_1^2 = \frac{t}{k \Leftrightarrow 1} d_2^2 + 2d_1^2 (t \Leftrightarrow \frac{t}{k \Leftrightarrow 1}). \quad (45)$$

We will check a minimum number of points if we parametrize in the variable a , essentially from the intersection with the second constraint to the b -axis. This is so since the slope of the first constraint is $\Leftrightarrow \frac{d_2^2}{2d_1^2} \leq \Leftrightarrow 1$, as shown in Figure II.1.

Solving the linear system of equations gives the intersection of the first (41) and second (42) constraints at the point $(a, b) = (\frac{t}{k-1}, t \Leftrightarrow \frac{t}{k-1})$. Hence the first value of a which need to be considered is $\lfloor \frac{t}{k-1} \rfloor$. The last value of a is given by the intersection of $b = 0$ and the first constraint. Invoking $b = 0$ in (45) gives $ad_2^2 = \frac{t}{k-1} d_2^2 + 2d_1^2 (t \Leftrightarrow \frac{t}{k-1})$ Picking the integer closest but smaller gives the maximal a as

$$a = \lfloor \frac{t}{k \Leftrightarrow 1} + 2 \frac{d_1^2}{d_2^2} (t \Leftrightarrow \frac{t}{k \Leftrightarrow 1}) \rfloor. \quad (46)$$

The next question is which values of b corresponds to each a at the points closest to the constraint.

Solving (45) for b gives similarly

$$b = \lfloor (\frac{t}{k \Leftrightarrow 1} \Leftrightarrow a) \frac{d_2^2}{2d_1^2} + t \Leftrightarrow \frac{t}{k \Leftrightarrow 1} \rfloor. \quad (47)$$

However the constraint $a + b \leq t$ will in some cases interfere, the appropriate value of b is therefore

$$b = \min(t \Leftrightarrow a, \lfloor (\frac{t}{k \Leftrightarrow 1} \Leftrightarrow a) \frac{d_2^2}{2d_1^2} + t \Leftrightarrow \frac{t}{k \Leftrightarrow 1} \rfloor). \quad (48)$$

This finishes the proof of Theorem II.3.

B. Proof of the Lower Bound

For the proof of Theorem II.4, we need the following lemma:

LEMMA IV.3: Let $n \in \mathbf{N}$ and $|nx| \leq \frac{\pi}{2}$. Then,

$$\sin^2 nx \leq n \sin^2 x.$$

Proof: Let $f(x) = \sin^2 nx \Leftrightarrow n \sin^2 x$. We have to prove that $f(x) \geq 0$ when $|nx| \leq \frac{\pi}{2}$. Since $f(x)$ is even it is enough to study $x \in (0, \frac{\pi}{2n})$. We have $f(0) = 0$ and

$$f'(x) = 2n \sin nx \cos nx \Leftrightarrow 2n \sin x \cos x = 2n(\sin 2nx \Leftrightarrow \sin 2x). \quad (49)$$

It follows that $f(x) \geq 0$ in the interval $0 \leq x \leq \frac{\pi}{4n}$, since $\sin 2nx \geq \sin 2x$ here. Furthermore,

$$f''(x) = 4n(n \cos 2nx \Leftrightarrow \cos 2x) \leq 0 \text{ if } \frac{\pi}{4n} \leq x \leq \frac{\pi}{2n}. \quad (50)$$

Hence f is concave in the interval $\frac{\pi}{4n} \leq x \leq \frac{\pi}{2n}$. It follows that the lemma is proved once we have shown that $f(\frac{\pi}{2n}) \geq 0$ for all $n \in \mathbf{N}$. Now,

$$f\left(\frac{\pi}{2n}\right) = 1 \Leftrightarrow n \sin^2\left(\frac{\pi}{2n}\right) \geq 0 \Leftrightarrow \left(\frac{\pi}{2}\right)^2 \frac{1}{n} \left(\frac{\sin \frac{\pi}{2n}}{\frac{\pi}{2n}}\right)^2 \leq 1. \quad (51)$$

By invoking $\frac{\sin x}{x} \leq 1$ we get

$$\left(\frac{\pi}{2}\right)^2 \frac{1}{n} \left(\frac{\sin \frac{\pi}{2n}}{\frac{\pi}{2n}}\right)^2 \leq \left(\frac{\pi}{2}\right)^2 \frac{1}{n} \leq 1 \quad (52)$$

where the second inequality is true if $n \geq (\frac{\pi}{2})^2 \approx 2.47$, hence we are done if $n \geq 3$. Since $f(\frac{\pi}{2}) = f(\frac{\pi}{4}) = 0$, the lemma is proved.

Proof of Theorem II.4. Let x_B and z_B be two codewords in B at Hamming distance $d_H(x_B, z_B)$ from each other, and let x and z be the two corresponding codewords in C . Let $x_{B,j}$ and $z_{B,j}$ be the j :th r -tuple in x_B and z_B respectively and denote by x_j and z_j be the j :th letter in x and z . Suppose that $x_{B,j}$ and $z_{B,j}$ differ in h_j bits. Clearly, $0 \leq h_j \leq r$ and

$$\sum_{j=1}^n h_j = d_H(x_B, z_B). \quad (53)$$

Let $|x_j \leftrightarrow z_j|_q = \min_{m \in \mathbf{Z}} |x_j \leftrightarrow z_j + mq|$. In the literature, $|x_j \leftrightarrow z_j|_q$ is sometimes referred to as the Lee distance between x_j and z_j [8]. It follows from the construction of the Gray code that we have

$$h_j \leq |x_j \leftrightarrow z_j|_q \leq \frac{q}{2}. \quad (54)$$

This gives

$$d_E^2(x, z) = 4 \sum_{j=1}^n \sin^2 \frac{(x_j \leftrightarrow z_j)\pi}{q} = 4 \sum_{j=1}^n \sin^2 \frac{|x_j \leftrightarrow z_j|_q \pi}{q} \geq 4 \sum_{j=1}^n \sin^2 \frac{h_j \pi}{q}. \quad (55)$$

By Lemma IV.3 together with (53) we obtain

$$d_E^2(x, z) \geq 4 \sum_{j=1}^n \sin^2 \frac{h_j \pi}{q} \geq 4 \sum_{j=1}^n h_j \sin^2 \frac{\pi}{q} = d_H(x_B, z_B) d_1^2. \quad (56)$$

We have derived

$$d_E^2(x, z) \geq d_H(x_B, z_B) d_1^2 \quad (57)$$

for any two words $x, y \in C$. Finally, take words $x, y \in C$ at closest Euclidean distance: $d_E^2(x, z) = d_{Emin}^2(C)$. We can then conclude the proof of Theorem II.4:

$$d_{Emin}^2(C) = d_E^2(x, z) \geq d_H(x_B, z_B) d_1^2 \geq d_{Hmin}(B) d_1^2. \quad (58)$$

References:

- [1] G. Caire and E. Biglieri, *Linear block codes over cyclic groups*, IEEE Trans. Inform. Theory, vol. 41, pp. 1246 - 1256, Sep. 1995.
- [2] C.- J. Chen, T.- Y. Chen and H.- A. Loeliger, *Construction of linear ring codes for 6-PSK*, IEEE Trans. Inform. Theory, vol. 40, pp. 563 - 566, March 1994.

- [3] V. V. Ginzburg, *Multidimensional signals for a continuous channel*, Probl. Inform. Transm., vol. 20, pp. 20 - 34, 1984.
- [4] S. Haykin, *Digital Communications*, Wiley, New York, 1988.
- [5] H. Imai and S. Hirakawa, *A new multilevel coding method using error-correcting codes*, IEEE Trans. Inform. Theory, vol. 23, pp. 371 - 377, 1977.
- [6] M. Isaksson and L. H. Zetterberg, *A class of block codes with expanded signal-sets for PSK-modulation*, Proc. of EUROCON 88, Stockholm, Sweden, pp. 181 - 184, June 1988.
- [7] F. R. Kschischang, P. G. de Buda and S. Pasupathy, *Block coset codes for M-ary phase shift keying*, IEEE J. Select. Areas Comm., vol. 7, pp. 900 - 913, Aug. 1989.
- [8] C. Y. Lee, *Some properties of Nonbinary Error Correcting Codes*, IRE Trans. Inform. Theory, vol. 4, pp. 77 - 82, June 1958.
- [9] Ph. Piret, *Algebraic construction of cyclic codes over Z_8 with a good minimum Euclidean distance*, IEEE Trans. Inform. Theory, vol. 41, pp. 815 - 818, May 1995.
- [10] Ph. Piret, *Bounds for Codes Over the Unit Circle*, IEEE Trans. Inform. Theory, vol. IT-32, no. 6, pp. 760-767, 1986.
- [11] S. I. Sayegh, *A class of optimum block codes in signal space*, IEEE Trans. Comm., vol. 34, pp. 1043 - 1045, Oct. 1986.
- [12] Tanabe-Hideiko, Umeda-Hiroyuki, *Expanding Channel Signal-set and Multilevel Coding over $GF(M)$ for block coded PSK modulation scheme*, Proceedings of the International Symposium on Information Theory and Its Applications, Part 1, Sidney, Australia, 1994.
- [13] R. M. Tanner, *Algebraic construction of large euclidean distance combined coding modulation systems*, Abstracts of Papers from 1986 IEEE ISIT, Ann Arbor, Oct. 1986.
- [14] S. G. Wilson, *Digital Modulation and Coding*, Prentice Hall, New Jersey, 1996.