*IMA Journal of Mathematical Control and Information* (2014) Page 1 of 23 doi:10.1093/imamci/dnt047

# Generalized upper bounds on the minimum distance of PSK block codes

EFRAIM LAKSMAN\* AND HÅKAN LENNERSTAD

School of Engineering, Blekinge Institute of Technology, Campus Gräsvik, Valhallavägen 1, Karlskrona, Sweden \*Corresponding author. Email: efraim.laksman@bth.se

AND

MAGNUS NILSSON

Linnæus University, Kalmar Maritime Academy, Nygatan 18 B, Kalmar, Sweden

[Received on 2 October 2012; revised on 25 June 2013; accepted on 23 November 2013]

This paper generalizes previous optimal upper bounds on the minimum Euclidean distance for phase shift keying (PSK) block codes, that are explicit in three parameters: alphabet size, block length and code size. The bounds are primarily generalized from codes over symmetric PSK to codes over asymmetric PSK and also to general alphabet size. Furthermore, block codes are optimized in the presence of other types of noise than Gaussian, which induces also non-Euclidean distance measures. In some instances, codes over asymmetric PSK prove to give higher Euclidean distance than any code over symmetric PSK with the same parameters. We also provide certain classes of codes that are optimal among codes over symmetric PSK.

Keywords: asymmetric PSK; symmetric PSK; Elias bound.

### 1. Introduction

Phase shift keying (PSK) is a commonly used signal constellation in data transmission and communication systems, where often Euclidean distance is the preferred distance measure. The purpose of the present paper is to show how previously known bounds on the minimum Euclidean distance can be generalized and improved in several ways. The bounds are dependent only on the alphabet size q, word size n and code size |C|.

The PSK signal constellation corresponds to a rather fundamental mathematical-geometrical optimization problem, in finding the minimum distance of a set of points in a universe equipped with a specific multidimensional metric. This paper belongs to a line of research that develops the underlying geometrical problem by extending Elias' sphere argument in different ways. We claim that the approach used allows a larger flexibility in how performance questions may be stated, investigated and improved, as, for example, being useful for any distance measure—in this report we go beyond Euclidean distance measure. A different distance measure simply gives different coefficients in the optimization. In this paper, we present some improvements of this extension of Elias' sphere argument alongside with the main results, which are generalizations and improvements of upper bounds for the minimum Euclidean distance.

Strictly, PSK means only that the signals used differ in phase, but neither in amplitude nor frequency. If the phases used are evenly spread on the interval  $(-\pi, \pi]$ , i.e. the symbols are evenly spread on the unit circle, we will refer to this constellation as symmetric PSK, as is common in the literature. Some



FIG. 1. Illustration of symmetric PSK and asymmetric PSK signal constellations.

research has been done on signal constellations where the symbols are unevenly spread on the unit circle. In this paper, we consider distance uniform signal sets, i.e. signal constellations for which the set of distances from one symbol to the others is the same for all symbols; which we refer to as asymmetric PSK (sometimes the term 'unbalanced' is used). Note that the set of codes over symmetric PSK is a subset of the set of codes over asymmetric PSK. The two signal constellations are illustrated in Fig. 1.

Elias has formed a method to find upper bounds on the minimum distance of block codes over distance uniform signal sets, where minimum distance is measured by an additive, translation-invariant distance measure. This method has been used for several signal constellations, in particular for symmetric PSK, see Piret (1986). Note that for PSK, the distance of interest is often squared Euclidean distance, since when assuming additive white Gaussian noise (AWGN), finding the codeword closest to a signal will correspond to maximum likelihood (ML) decoding. For noise of some other distribution, ML decoding will correspond to minimum distance decoding for some other distance measure. The distribution of noise may be unknown, and even if it is known, the appropriate distance measure may be impossible to find. In such cases, as an approximation of ML decoding, minimum distance decoding may be used for some distance which does not give true ML decoding.

Elias' method has been extended by the present authors in a series of reports (see Section 3). In the extended results, the bounds are explicit in the parameters block length, alphabet size and code size, and are tight in many cases, i.e. show several code classes to be optimal with respect to minimum squared Euclidean distance.

The extension of Elias' sphere argument for forming upper bounds on codes works when applied to block codes over asymmetric PSK with additive and white noise; note that this noise does not need to be Gaussian. This establishes previous results for symmetric PSK with AWGN in a far more general setting (Theorems 4.3–4.5), as well as yields some qualitative results which are more than just generalizations of previous results (Theorems 4.1, 4.2, Corollaries 4.1, 4.2). Secondly, a theorem which cannot be generalized with respect to noise is generalized to the case of asymmetric PSK, while maintaining the restriction of AWGN (Theorem 4.6).

The purpose of the paper is more theoretical than practical: to demonstrate new ways to improve the bound. Even so there may be some future practical relevance. Improvements of minimum Euclidean distance for PSK trellis codes by asymmetric modulation has been presented in Divsalar *et al.* (1987) and Stüber & Katz (1995). For PSK block codes, it was shown in Bali & Rajan (1998) that there are multilevel codes with two levels for which minimum Euclidean distance can be increased by asymmetric modulation. Bali & Rajan (1998, Example 6) shows an 8-PSK code of length 30 which is improved by asymmetric modulation. To show that asymmetric modulation can be better than symmetric modulation in general, not only for specific codes, two examples (Examples 5.1 and 5.2) are given of optimal block codes over asymmetric PSK. Compared with any block code over symmetric PSK with the same block length, code size and alphabet size, these codes have higher minimum Euclidean distance. These two examples are only of theoretical interest, as the codes are too short for practical use. While finding optimal codes for symmetric as well as asymmetric modulation may be beyond reach, and thus difficult to compare, these examples indicate that asymmetric modulation should not be outright spurned.

Asymmetric modulation has also been discussed for other purposes than achieving high minimum Euclidean distance. In Isaka *et al.* (2000), asymmetric modulation is used for unequal error protection and in Zhang *et al.* (2009) asymmetric modulation is used for minimizing the bit error rate.

Bounds for minimum Euclidean distance of codes over asymmetric PSK, which are asymptotic in n are described in Rajan & Viswanath (2003) and Viswanath (2004), while the present bound is explicit in n. The assumption of Euclidean distance is motivated by the AWGN-channel assumption.

An asymptotic bound on the minimum distance of codes over asymmetric PSK (without the restriction that the signal set is distance uniform) was presented in Wyner (1987).

The following improvements are presented for the bound on the minimum Euclidean distance for PSK coding, compared with previous work (Nilsson & Lennerstad, 2000, 2005; Nilsson *et al.*, 2008; Laksman *et al.*, 2009a,b, 2010):

- 1. Bounds are generalized to codes over more general modulation: from symmetric PSK to also include asymmetric PSK (Theorem 4.4).
- 2. The bound is tightened in Theorem 4.5 by using the bound of Theorem 4.4 as an upper limit and exploiting symmetry properties.
- 3. For all types of PSK considered, the bounds are generalized from squared Euclidean distance to additive translation-invariant distance measures (Theorems 4.4 and 4.5). This provides an upper bound on the minimum distance for codes that more efficiently exploit the statistical properties of the noise.
- 4. Specific codes over asymmetric PSK are provided that have higher minimum Euclidean distance than any comparable codes over symmetric PSK, although they are codes of very short block lengths (Example 5.1 and Example 5.2), and of theoretical value only.
- 5. In the set of codes over symmetric PSK, we demonstrate for certain code classes that they are optimal in the sense that they have highest possible minimum Euclidean distance with given parameter values q, n and |C|, since their minimum Euclidean distance in these cases coincides with the bound (see Examples 5.3–5.7).

This means that results 1 and 3 are generalizations of the bound in previous papers, while 2 is an improvement of the bound. The results 4 and 5 demonstrate the relation between concrete codes and the bound.

Elias' sphere argument has been modified by allowing a different distance measure in the critical sphere—a so-called inner distance measure. It has turned out that a tighter bound on the Euclidean distance measure—the outer distance measure—can be derived by optimizing the inner distance measure. As Elias did, we regard the set of codewords in the critical sphere as rows in a matrix, and then switch to column view. Finding extremal codeword sets then translates into finding extremal columns.

This paper contributes to the extension of Elias' sphere argument with the following results:

- 1. If the outer distance measure is a metric, then the inner distance measure which yields the best bound is the outer distance measure (Corollary 4.1).
- 2. We present simple conditions to check whether a generalized *p*-Gaussian induced distance measure (see Definition 2.2 and the comments following it) is a metric on a PSK signal constellation. We get one condition for asymmetric PSK (Theorem 4.2) and an easier one for symmetric PSK (Corollary 4.2).
- 3. For an extremal column **x**, we always have  $d_E^2(\mathbf{x}) \leq 4$  (Theorem 4.6). This simple and general condition reduces dramatically the set of candidate columns.

In Section 2, definitions and notation are fixed. In Section 3, related papers are mentioned and Elias' sphere argument is explained, as well as the improvements made of it. In Section 4, the theoretical results of this paper may be found. In Section 5, examples of codes over asymmetric PSK which are better than their counterparts on symmetric PSK are presented, as well as proof that several classes of codes are optimal among codes over symmetric PSK. Section 6 concludes the paper with conclusions and possible continuations.

## 2. Definitions and notation

Some of the definitions below are more general than what is needed to obtain the results of this paper. To give a description of Elias' sphere argument which is as general as possible, general definitions are necessary.

NOTATION 2.1 We will use X to denote an arbitrary space. To denote a finite distance uniform space we will use U. Note also  $U^n$  becomes distance uniform. We will let T denote the space of points on the unit circle, represented by their angle. We identify an angle  $\alpha$  with all angles  $\alpha + n2\pi$ ,  $n \in \mathbb{Z}$ . Whenever we speak of the sign of an angle, we consider the sign of its representative in the interval  $(-\pi, \pi]$ . The sign function,  $\theta/|\theta|$  for  $\theta \neq 0$ , and 0 otherwise, will be denoted by  $\langle \theta \rangle$ . We will use Q to denote a finite distance uniform subspace of T, and denote the q = |Q| elements of Q by their angle. We name those symbols  $\gamma_0, \ldots, \gamma_{q-1}$ , and by an argument of rotation, we will assume  $\gamma_0 = 0$ .

DEFINITION 2.1 (Kschischang *et al.* (1989)) Let *X* be a space. A *distance measure* is a bivariate function *d* from  $X \times X$  to  $\mathbb{R}$  such that

- 1.  $d(x, y) \ge 0$  for all  $x, y \in X$  with equality if and only if x = y and
- 2. d(x, y) = d(y, x) for all  $x, y \in X$ .

A distance measure which satisfies the triangle inequality, i.e.  $d(x, z) \le d(x, y) + d(y, z)$  for all  $x, y, z \in X$  is a *metric*.

The distance measure d will be said to be additive if

$$d(\mathbf{x},\mathbf{y}) = \sum_{i=1}^{m} d(x_i, y_i),$$

for all  $\mathbf{x}, \mathbf{y} \in X^m$  for all m.

The distance measure d will be said to be translation-invariant if

$$d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x} + \mathbf{z}, \mathbf{y} + \mathbf{z}),$$

for all  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in X^m$  for all m.

Note that by saying that a distance measure is additive, one extends it from  $X \times X$  to  $X^m \times X^m$  for all *m*.

NOTATION 2.2 For any distance measure d, we will denote  $d(0, \mathbf{x})$  by  $d(\mathbf{x})$ . Also, we will refer to  $d(\mathbf{x})$  as the weight of  $\mathbf{x}$  with respect to d.

DEFINITION 2.2 We define a family of additive and translation-invariant distance measures  $\{d_p\}_{p>0}$  on T or Q by

$$d_p(\gamma) = 2^p \left| \sin\left(\frac{\gamma}{2}\right) \right|^p.$$
(2.1)

Note that using phase-modulated sine-waves for communication and performing ML decoding while experiencing white noise X with density

$$f_X(x) = \frac{\lambda p}{2\Gamma(p^{-1})} \exp(-\lambda^p |x|^p), \qquad (2.2)$$

for  $p, \lambda > 0$ , a correct way of measuring distance between symbols as well as words is by  $d_p$ . The density function (2.2) was introduced by Subbotin (1923), who suggested it to be used for modelling measurement errors. Subbotin found this density from the two properties:

- 1. The probability of an error depends only on the magnitude of this error, and may be expressed as a function  $f_X(x)$  having the first derivative in general continuous.
- 2. The most probable value of a quantity, from which direct measures are known, must not depend on the unit employed.

Regarding the differentiability of  $f_X(x)$ —Subbotin's derivation of  $f_X(x)$  appears to rely on  $f_X(x)$  being everywhere right differentiable (or left differentiable), but not on the derivative of  $f_X(x)$  being continuous. The density in (2.2) is called generalized *p*-Gaussian density, and has been analysed further in, for example, Pham & DeFiueiredo (1989) and Taguchi (1978).

NOTATION 2.3 In the special case p = 2, the noise described in (2.2) is AWGN, and  $d_2$  is commonly known as squared Euclidean distance. We signify the importance of this distance measure by denoting it  $d_E^2$ . Note that  $d_E^2$  is not a metric.

Euclidean distance,  $\sqrt{d_E^2}$ , which will be denoted by  $d_E$ , is a translation-invariant metric, but it is not additive. We will use that

$$d_E(\gamma) = 2\left\langle \frac{\gamma}{2} \right\rangle \sin\left(\frac{\gamma}{2}\right).$$

Remark that  $\gamma/2$  is not well defined as it has two possible values, one positive and one negative. To get unique division in *T*, we lift the angle—i.e. its representative in  $(-\pi, \pi]$  – to  $\mathbb{R}$ , perform the division and bring the result back into *T*. For division by 2, this means that among the two possible values, we always choose the one which maintains the sign.

DEFINITION 2.3 The minimum distance between points in a space X with respect to the distance measure d is denoted as  $d_{\min}(X)$  and defined as

$$d_{\min}(X) = \min_{x, y \in X, x \neq y} d(x, y).$$

The average distance between points in a space X with respect to the distance measure d is denoted as  $d_{\text{average}}(X)$  and defined as infinity if  $|X| \leq 1$  and as

$$d_{\text{average}}(X) = \frac{1}{|X|(|X|-1)} \sum_{x,y \in X, x \neq y} d(x,y),$$

otherwise.

NOTATION 2.4 A set of consecutive integers  $\{i, i + 1, ..., j\}$  will often be denoted by [i, j].

NOTATION 2.5 By  $\mathbb{Z}_+$ , we refer to the set of positive integers.

### 3. Previous results

In this paper, we work with distance uniform signal constellations.

Elias did not publish his sphere argument, but the method may be found in Berlekamp (1968, pp. 318–321) and MacWilliams & Sloane (1977, pp. 558–564). We give an overview of Elias' sphere argument for forming a bound on performance for codes over distance uniform spaces together with generalizations.

Consider the code *C* on the space  $U^n$ , i.e. let  $C \subseteq U^n$  be a code. Let *d* and  $\delta$  be two additive and translation-invariant distance measures, where we seek  $d_{\min}(C)$ . Let

$$S_{\delta,t}(\mathbf{x}) = \{\mathbf{y} \in U^n | \delta(\mathbf{x}, \mathbf{y}) \leq t\}$$

be a sphere with respect to  $\delta$ , with centre **x** and radius *t*. We note that since we have a distance uniform space and a translation-invariant distance measure, the number of words in the sphere  $S_{\delta,t}(\mathbf{x})$  is independent on **x**.

Now, centred at each codeword, place a sphere with respect to  $\delta$  and radius *t*. The spheres contain a total of  $|C||S_{\delta,t}|$  words, but only  $|U|^n$  words exist. So at least one word, **w**, belong to at least  $K = \lceil |C||S_{\delta,t}||U|^{-n}\rceil$  spheres. Call the sphere  $S_{\delta,t}(\mathbf{w})$  the critical sphere. Note that the critical sphere contains at least *K* codewords. Let  $W = C \cap S_{\delta,t}(\mathbf{w})$ . Now, the chain of inequalities

$$d_{\min}(C) \leqslant d_{\min}(W) \leqslant d_{\operatorname{average}}(W)$$

is trivial, so  $d_{\text{average}}(W)$  will work as an upper bound on  $d_{\min}(C)$ .

Since we have a distance uniform signal constellation it may as well be assumed that  $\mathbf{w} = \mathbf{0}$ , as the code can be translated without changing any distances. With the assumption  $\mathbf{w} = \mathbf{0}$ , we may speak of the weight with respect to  $\delta$  of codewords in the critical sphere, rather than of their distance to  $\mathbf{w}$ , and this weight is at most *t*.

Elias defined  $\delta$  to be the distance measure in which the performance of the code was measured, i.e.  $\delta = d$ , but this is not necessary. Improvements that have been made in Nilsson & Lennerstad (2000, 2005), Nilsson *et al.* (2008) and Laksman *et al.* (2009a,b, 2010) are based on that while there is one distance measure (which we call outer distance measure) used for measuring the minimum distance of

the code, another distance measure (which we call inner distance measure) can be used for determining the shape of the spheres, i.e. the one called  $\delta$ . For PSK codes with AWGN, it is squared Euclidean distance which is the relevant outer distance measure. The signal constellations symmetric 2-PSK, 3-PSK and 4-PSK are special cases, where squared Euclidean distance can be reduced to Hamming distance. The inner distance measure ought to be chosen such that it minimizes the bound in the outer distance measure.

Based on Elias' sphere argument, but by allowing different inner distance measures, in Laksman *et al.* (2010) the following theorem and lemma were proved.

THEOREM 3.1 For any code C in  $Q^n$ , we have the bound

$$d_{\min}(C) \leq \min_{K \in [2,|C|]} \min_{\delta} \frac{2t_K(\delta)f_{\delta}(\hat{\mathbf{y}})}{K-1},$$

where

$$\tilde{t}_{K}(\delta) = \min(\{t : K \leq \lceil |C| | S_{\delta,t} | q^{-n} \rceil\})$$
$$f_{\delta}(\mathbf{y}) = \frac{\sum_{j_{1}=2}^{K} \sum_{j_{2}=1}^{j_{1}-1} d(y_{j_{1}}, y_{j_{2}})}{\sum_{j=1}^{K} \delta(y_{j})}$$

and

$$\hat{\mathbf{y}} = \operatorname{argmax}_{\mathbf{y} \in O^K} f_{\delta}(\mathbf{y}).$$

Remark that **y** in the theorem has length *K*, not *n*. The vector **y** is not a codeword, but a 'column', stemming from the construction in Berlekamp (1968) of forming a matrix of all codewords in a neighbourhood of radius  $\tilde{t}_K$ , where the codewords are rows, so that column *i* consists of the *i*th symbols from the codewords in the critical sphere. Also, even though  $\tilde{t}_K$  is a function not only of  $\delta$ , but also of *n*, |C| and *Q*, we usually omit those parameters as they are assumed to be fixed. The same is true for the dependence  $f_{\delta}(\hat{\mathbf{y}})$  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.

LEMMA 3.1 The bound in Theorem 3.1 is scale invariant in the distance measure  $\delta$ , i.e. for any s > 0, let  $\lambda(x) = s\delta(x)$  for every *x*. Then

$$\frac{2\tilde{t}_K(\delta)f_\delta(\hat{\mathbf{y}})}{K-1} = \frac{2\tilde{t}_K(\lambda)f_\lambda(\hat{\mathbf{y}})}{K-1}$$

holds.

While both Theorem 3.1 and Lemma 3.1 in Laksman *et al.* (2010) were considered only for symmetric PSK and for squared Euclidean distance d, proofs for asymmetric PSK and general additive translation-invariant d remain nearly identical. Note, however, that Theorem 3.1 does not in general hold if the PSK signal set is not distance uniform.

In Nilsson & Lennerstad (2000, 2005), Nilsson *et al.* (2008) and Laksman *et al.* (2009a,b, 2010), the idea of using an inner distance measure different from the outer distance measure has been developed. Note that while some partial results from these papers may hold for a general outer distance measure, they were all developed with the restriction to squared Euclidean distance as outer distance measure. In Nilsson & Lennerstad (2000, 2005), particular inner distance measures which improved the Elias'

8 of 23

#### E. LAKSMAN ET AL.

bound for some code parameters were presented, while in Nilsson *et al.* (2008) the idea of letting the inner distance measure depend on *K* appeared, using symmetric 8-PSK to exemplify. How  $\delta$  ought to depend on *K* for symmetric 8-PSK was studied in Laksman *et al.* (2010), which in Laksman *et al.* (2009b) was generalized to symmetric *q*-PSK. In Laksman *et al.* (2009a), it was shown that the work in Laksman *et al.* (2010), somewhat limited by the method, gave the actual optimum, but this was only for *q* = 8, and failed to extend to general *q*. This extension is provided in the present paper, besides the generalizations to general outer distance measures and asymmetric PSK.

# 4. Results

Generalizations built upon Elias' sphere argument have earlier been made for block codes over symmetric PSK with squared Euclidean distance, Nilsson & Lennerstad (2000, 2005), Nilsson *et al.* (2008) and Laksman *et al.* (2009a,b, 2010). The main methods in this section are further generalizations built on the generalizations previously made. In the present paper, the earlier generalizations are shown to work for block codes over asymmetric PSK. Furthermore, it is shown that any additive and translation-invariant outer distance measure can be used. The end of the section, however, deals explicitly with the case where the outer distance measure is squared Euclidean distance.

Let  $a_i(\mathbf{y})$  be the function counting the number of symbols equal to  $\gamma_i$  in a vector  $\mathbf{y}$ . Now write  $f_{\delta}$  from Theorem 3.1 as

$$f_{\delta} = \frac{\sum_{i=0}^{q-1} \sum_{j>i} a_i a_j d(\gamma_i, \gamma_j)}{\sum_{i=0}^{q-1} a_i \delta(\gamma_i)}$$

.

Rewriting the expression, using  $a_0 = K - \sum_{i=1}^{q-1} a_i$  as a way of eliminating  $a_0$ , we find that numerator has the following coefficients:

$$\operatorname{coeff}(a_i) = Kd(\gamma_i),$$
  

$$\operatorname{coeff}(a_i^2) = -d(\gamma_i) \quad \text{and}$$
  

$$\operatorname{coeff}(a_ia_i) = d(\gamma_i, \gamma_i) - (d(\gamma_i) + d(\gamma_i)), \quad i \neq j.$$

Now we may write

$$f_{\delta} = \frac{T_{1} + T_{2} + T_{3}}{D} \quad \text{with}$$

$$T_{1} = K \sum_{i=1}^{q-1} a_{i} d(\gamma_{i}),$$

$$T_{2} = -\sum_{i=1}^{q-1} a_{i}^{2} d(\gamma_{i}),$$

$$T_{3} = \sum_{i=1}^{q-1} \sum_{j>i} a_{i} a_{j} (d(\gamma_{i}, \gamma_{j}) - (d(\gamma_{i}) + d(\gamma_{j}))),$$

$$D = \sum_{i=1}^{q-1} a_{i} \delta(\gamma_{i}).$$
(4.1)

DEFINITION 4.1 Columns **y** which maximize  $f_{\delta}(\mathbf{y})$  for at least some  $\delta$  will be called *extremal columns*. A column **y** which maximizes  $f_{\delta}(\mathbf{y})$  for a particular  $\delta$  will be called a *critical column* for that  $\delta$ .

Note that which columns are extremal, and which column is critical for a particular  $\delta$ , depends on the outer distance measure, which we, however, assume to be fixed.

THEOREM 4.1 Let y be a column such that  $T_3(y) < 0$ , then y is not an extremal column.

*Proof.* Let  $Q_{\mathbf{y}}$  be the set of symbols in  $\mathbf{y}$  except  $\gamma_0$ . Let

$$m = \arg \max_{\{i:\gamma_i \in Q_y\}} \left(\frac{d(\gamma_i)}{\delta(\gamma_i)}\right).$$

Let **z** be a column with  $a_0(\mathbf{z}) = K - 1$  and  $a_m(\mathbf{z}) = 1$ . As  $T_3(\mathbf{z}) = 0$ , it follows that

$$f_{\delta}(\mathbf{z}) = \frac{T_1 + T_2}{D}(\mathbf{z}) = \frac{(K-1)d(\gamma_m)}{\delta(\gamma_m)}$$

As  $T_3(\mathbf{y}) < 0$ , it follows that

$$f_{\delta}(\mathbf{y}) < \frac{T_1 + T_2}{D}(\mathbf{y}) = \frac{\sum_{i=1}^{q-1} a_i(\mathbf{y})(K - a_i(\mathbf{y}))d(\gamma_i)}{\sum_{i=1}^{q-1} a_i(\mathbf{y})\delta(\gamma_i)} \leqslant \frac{\sum_{i=1}^{q-1} a_i(\mathbf{y})(K - 1)d(\gamma_i)}{\sum_{i=1}^{q-1} a_i(\mathbf{y})\delta(\gamma_i)} \leqslant \frac{(K - 1)d(\gamma_m)}{\delta(\gamma_m)}.$$

The last inequality follows from the left-hand side being a weighted average of several terms, where the right-hand side is the largest of those terms. In total, we have shown that  $f_{\delta}(\mathbf{y}) < f_{\delta}(\mathbf{z})$ , so  $\mathbf{y}$  cannot be an extremal column.

Finding the optimal inner distance measure is simplified a great deal when the outer distance measure is a metric, as shown by a corollary to Theorem 4.1.

COROLLARY 4.1 If the outer distance measure d is a metric, then an optimal inner distance measure  $\delta$  is the same as the outer distance measure.

*Proof.* If *d* is a metric, then  $T_3 \leq 0$ . Following the proof of Theorem 4.1, we see that columns of the form  $(i, 0, ..., 0)^{\top}$  for all *i* are extremal, and for any  $\delta$  one of these columns will be critical, even if other extremal columns which may be simultaneously critical may exist. Since interest lies in the maximal value of *f*, and not in extremal columns as such, the set of columns  $(i, 0, ..., 0)^{\top}$  will be sufficient.

For any given  $\delta$ , one of these columns will be  $\hat{\mathbf{y}}$  in Theorem 3.1, so the bound is

$$\min_{K,\delta} \frac{2\tilde{t}_K(\delta)}{K-1} \max_i \left( (K-1) \frac{d(\gamma_i)}{\delta(\gamma_i)} \right) = \min_{K,\delta} 2\tilde{t}_K(\delta) \max_i \left( \frac{d(\gamma_i)}{\delta(\gamma_i)} \right).$$

Consider an inner distance measure  $\delta_0$  with

$$m = \arg \max_{i} \left( \frac{d(\gamma_i)}{\delta_0(\gamma_i)} \right).$$

Lemma 3.1 allows us to rescale  $\delta_0$  so that  $\delta_0(\gamma_m) = d(\gamma_m)$ . If  $\delta_0(\gamma_i) > d(\gamma_i)$  for some *i*, consider  $\delta_1$  such that  $\delta_1(\gamma_i) = d(\gamma_i)$  and  $\delta_1(\gamma_j) = \delta_0(\gamma_j)$  for  $j \neq i$ . Clearly, the bound resulting from using  $\delta_1$  as inner distance measure does not give a worse bound than using  $\delta_0$  as inner distance measure. The process may be repeated until we have an inner distance measure  $\delta = d$ .

When an optimal inner distance measure is known, Theorem 3.1 can be applied directly. The last corollary applies to, e.g. Hamming metric

$$d_H(\gamma_i, \gamma_j) = \begin{cases} 0 & \text{if } \gamma_i = \gamma_j, \\ 1 & \text{if } \gamma_i \neq \gamma_j, \end{cases}$$

and to Lee metric

 $d_L(\gamma_i, \gamma_i) = \arcsin(d_1(\gamma_i, \gamma_i)/2),$ 

both of which are commonly used for determining performance of error-correcting codes. However, for these distance measures other upper bounds are known. We recommend van Lint (1992) and Roth (2006) for the Hamming metric and Quistorff (2006) for the Lee metric.

Note that it is enough for d to be a metric on Q for Corollary 4.1 to hold, there is no need for d to be a metric on the whole interval  $(-\pi, \pi]$ . For example, squared Euclidean distance is a metric for symmetric 4-PSK, but not in general. Also, for  $p \in (0, 1]$ ,  $d_p$  (from (2.1)) is a metric on the whole interval  $(-\pi, \pi]$ . It is possible to formulate a relation between the sizes of p which yield a metric and the angle of the two symbols closest to zero.

THEOREM 4.2 For p > 1, the distance measure  $d_p$  from (2.1) is a metric on an asymmetric PSK signalset Q if and only if

$$\left|\sin\left(\frac{\gamma_{i_1}-\gamma_{i_{q-1}}}{2}\right)\right|^p \leqslant \left|\sin\left(\frac{\gamma_{i_1}}{2}\right)\right|^p + \left|\sin\left(\frac{\gamma_{i_{q-1}}}{2}\right)\right|^p,\tag{4.2}$$

where  $\gamma_{i_1}$  and  $\gamma_{i_{a-1}}$  are the two smallest angles of Q, see Fig. 1(b).

*Proof.* Note that (4.2) is in fact the triangle inequality for three particular elements in Q. If we identify it with Definition 2.1, we have  $x = \gamma_{i_1}, y = \gamma_0, z = \gamma_{i_{q-1}}$ . By a rotational argument, we can choose  $y = \gamma_0$ , no matter which three elements we intend to 'test' the triangle inequality on.

Based on the observation that (4.2) is an instance of the triangle inequality, it is clear that  $d_p$  is not a metric if (4.2) is false.

For the other direction, we first note that if x and z have the same sign (note that  $|x|, |z| \leq \pi$ ), then clearly

$$\left|\sin\left(\frac{x-z}{2}\right)\right|^{p} \leq \left|\sin\left(\frac{x}{2}\right)\right|^{p} + \left|\sin\left(\frac{z}{2}\right)\right|^{p}.$$
(4.3)

Hence, it is enough to show that (4.3) holds for all  $x \in [\gamma_{i_1}, \pi]$  and  $z \in (-\pi, \gamma_{i_{q-1}}]$ . With x and z in those intervals, (4.3) can be written as

$$0 \leq \sin^p\left(\frac{x}{2}\right) + \sin^p\left(\frac{-z}{2}\right) - \sin^p\left(\frac{x-z}{2}\right).$$

It is an easy analytic exercise to show that the right-hand side is increasing with respect to x and decreasing with respect to z, for x and z in the given intervals, so knowing that the inequality is true for the minimum x and the maximum z is enough. Hence,  $d_p$  must be a metric on Q when (4.2) is true.

When the signal constellation comes from symmetric PSK, (4.2) can be rewritten in a much cleaner form.

 $\Box$ 

COROLLARY 4.2 The distance measure  $d_p$  from (2.1) is a metric on the symmetric PSK constellation Q if and only if

$$p\log_2\left(\frac{\sin(\gamma_{i_1})}{\sin(\gamma_{i_1}/2)}\right) \leqslant 1,$$

where  $\gamma_{i_1}$  is the smallest angle of Q, see Fig. 1(a).

*Proof.* The corollary is a matter of rewriting (4.2) with  $\gamma_{i_1} = -\gamma_{i_{q-1}}$ .

For the next theorem—which helps in reducing the set of possibly extremal columns—denoting

$$\mathbf{a}_+(\mathbf{x}) = (a_1(\mathbf{x}), \dots, a_{q-1}(\mathbf{x}))$$

and

$$N(\mathbf{x}) = f_{\delta}(\mathbf{x})\delta(\mathbf{x}) = \sum_{i=0}^{q-1} \sum_{j>i} a_i(\mathbf{x})a_j(\mathbf{x})d(\gamma_i, \gamma_j)$$

will be helpful. The following theorem was presented in a less general setting already in Laksman *et al.* (2010).

THEOREM 4.3 If a column z is extremal, then

$$\frac{N(\mathbf{z})}{\delta(\mathbf{z})} \ge \frac{\sum_{i=1}^{m} u_i N(\mathbf{y}_i)}{\sum_{i=1}^{m} u_i \delta(\mathbf{y}_i)},\tag{4.4}$$

for all  $\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_m$ , for all *m*, such that for at least some  $v, u_i \in \mathbb{Z}_+$ ,

$$\sum_{i=1}^m u_i \mathbf{a}_+(\mathbf{y}_i) = v \mathbf{a}_+(\mathbf{z}),$$

for all finite  $\delta$ .

Note that the denominator will be the same on both sides in (4.4), at least once the left-hand side has been extended by v, so  $\delta$  will play no part in the evaluation of the inequality. Also the different  $T_1$ -terms will cancel, so the parameter K will disappear, and affect (4.4) only by limiting the number of symbols different from  $\gamma_0$  in each column, so it is only a comparison of constants.

*Proof.* Assume that for some *m*, a set of columns  $\mathbf{y}'_1, \mathbf{y}'_2, \dots, \mathbf{y}'_m$  exist such that for some *v*,  $u_i$  in  $\mathbb{Z}_+$ ,  $\sum_{i=1}^m u_i \mathbf{a}_+(\mathbf{y}'_i) = v \mathbf{a}_+(\mathbf{z})$  and  $N(\mathbf{z}) \sum_i u_i \delta(\mathbf{y}'_i) - \delta(\mathbf{z}) \sum_i u_i N(\mathbf{y}'_i) < 0$ . Then for any  $\delta$ , we must have  $N(\mathbf{z}) \delta(\mathbf{y}'_i) - \delta(\mathbf{z}) N(\mathbf{y}'_i) < 0$  for at least some *i*, which is the same as saying that  $\mathbf{z}$  is not extremal.  $\Box$ 

Let  $\hat{\mathbf{y}}_1, \ldots, \hat{\mathbf{y}}_{c(K)}$  be a list containing all extremal columns. It may also contain other columns, but for computational purposes it is preferable if it does not. Note that this list may depend somewhat on K, as the length of the columns is limited by K.

To be able to truly utilize the previous theorem, it would be good to have a set of extremal columns to use for the further reduction. Let  $\gamma_i$  be a symbol in Q. We consider two cases, depending on whether  $\gamma_i$  has an additive inverse in Q or not.

*Case* 1:  $-\gamma_i \notin Q$ . Consider now the inner distance measure  $\delta$  defined by

$$\delta(x) = \begin{cases} 0, & x = \gamma_0, \\ 1, & x = \gamma_i, \\ \infty, & \text{otherwise.} \end{cases}$$

This  $\delta$  shows that an extremal column  $\mathbf{x}$  with  $a_j(\mathbf{x}) = 0$  for all  $j \notin \{0, i\}$  exists. With this condition on  $\mathbf{x}$ , it can be seen that  $f_{\delta}$  is maximized if  $a_i(\mathbf{x}) = 1$ , as  $T_1(\mathbf{x})/D(\mathbf{x})$  is constant with respect to  $a_i(\mathbf{x}), T_2(\mathbf{x})/D(\mathbf{x})$  is decreasing with respect to  $a_i(\mathbf{x})$  and  $T_3(\mathbf{x}) = 0$ . Thus, if  $-\gamma_i \notin Q$ , then  $(\gamma_i, 0, \dots, 0)^{\top}$  is an extremal column.

*Case* 2:  $-\gamma_i \in Q$ . Consider now the inner distance measure  $\delta$  defined by

$$\delta(x) = \begin{cases} 0, & x = \gamma_0, \\ 1, & x = \pm \gamma_i, \\ \infty, & \text{otherwise.} \end{cases}$$
(4.5)

This  $\delta$  shows that an extremal column **x** with  $a_k(\mathbf{x}) = 0$  for all  $k \notin \{0, i, j\}$  exists, where  $\gamma_j = -\gamma_i$ . With this condition on **x**,  $f_\delta$  must be maximized with respect to  $a_i$  and  $a_j$ . As  $T_1/D$  is constant with respect to  $a_i$  and  $a_j$ , the value of  $T_1$  causes no concern. Instead we observe that  $a_i^2 + a_j^2 \ge 2a_ia_j$ , with equality when  $a_i = a_j$ , and that  $d(\gamma_i) = d(\gamma_j)$ , so that

$$T_2 + T_3 \leq a_i a_i (d(\gamma_i, \gamma_i) - 2(d(\gamma_i) + d(\gamma_i))) = a_i a_i (d(2\gamma_i) - 4d(\gamma_i)).$$

This means that if  $d(2\gamma_i) > 4d(\gamma_i)$ , then a column maximizing  $f_{\delta}$  yield  $a_i + a_j \in \{K - 1, K\}$  and  $|a_i - a_i| \leq 1$ . Otherwise,  $a_i$  and  $a_i$  should be kept as small as possible, so that  $a_i + a_i \in \{1, 2\}$  and  $|a_i - a_i| \leq 1$ .

Case 2 indicates that for certain distance measures some extremal columns will contain zeroes in all but at most two positions, whereas for other distance measures extremal columns consisting of at most one zero exist.

Now follows a theorem which allows the optimization of  $\delta$ , which is non-enumerable, to be calculated as a finite number of linear programming problems (LPPs). The idea of this theorem was used in Laksman *et al.* (2009a), albeit in a far more restricted setting.

THEOREM 4.4 The value of

$$\min_{\delta \in \Delta} \frac{2}{K-1} \tilde{t}_K(\delta) \max_{i \in [1, c(K)]} f_{\delta}(\hat{\mathbf{y}}_i),$$
(4.6)

where  $K \ge 2$  is an integer and  $\Delta$  is the set of additive translation-invariant distance measures, is the same as the value of

$$\min_{i\in[1,c(K)]}\min_{\delta\in\Delta_i}\frac{2}{K-1}\tilde{t}_K(\delta)f_\delta(\hat{\mathbf{y}}_i),\tag{4.7}$$

where  $\Delta_i$  is the set of additive translation-invariant distance measures which solves the LPP

$$\max_{\delta} \quad \delta(\hat{\mathbf{y}}_i)$$
s.t. 
$$\sum_{j=0}^{q-1} \delta(\gamma_j) = A_i,$$

$$N(\hat{\mathbf{y}}_i) \delta(\hat{\mathbf{y}}_j) - N(\hat{\mathbf{y}}_j) \delta(\hat{\mathbf{y}}_i) \ge 0, \quad j \neq i,$$

where  $A_i$  is any positive constant.

*Proof.* For now, assume that for the  $\delta$  which is the minimizing argument in (4.6), a critical column, i.e. a column  $\hat{\mathbf{y}}_i$  which maximizes  $f_{\delta}$ , is  $\hat{\mathbf{y}}_1$ .

We have

$$f_{\delta}(\hat{\mathbf{y}}_i) = \frac{N(\hat{\mathbf{y}}_i)}{\delta(\hat{\mathbf{y}}_i)}.$$

By the lemma of scale invariance, Lemma 3.1, we see that to perform the  $\delta$ -minimization in (4.6) we should maximize  $\delta(\hat{y}_1)$  subject to the constraints

$$f_{\delta}(\hat{\mathbf{y}}_1) \ge f_{\delta}(\hat{\mathbf{y}}_i) \quad \forall i \in [2, c(K)],$$

which may also be expressed as

$$N(\hat{\mathbf{y}}_1)\delta(\hat{\mathbf{y}}_i) - N(\hat{\mathbf{y}}_i)\delta(\hat{\mathbf{y}}_1) \ge 0 \quad \forall i \in [2, c(K)].$$

$$(4.8)$$

But to maximize  $\delta(\hat{\mathbf{y}}_i)$  under the conditions (4.8) is just an LPP.

We assumed that  $\hat{\mathbf{y}}_1$  was a critical column, but we have to solve the LPP for any column being critical, so to optimize the bound for a given *K* we must solve c(K) LPPs. For any fixed critical column, we may choose the distance measure resulting in the lowest bound. To get the best bound possible, we must try for each extremal column being critical, and pick the smallest one. This is expressed by the minimization over *i*.

The condition  $\sum_{j} \delta(\gamma_j) = A_i$  is just to fix the scaling, and can be added without loss of generality, as the problem we wish to solve is invariant with respect to scaling. Without this condition, the feasible region (when  $\hat{\mathbf{y}}_i$  is an extremal column) would be unbounded and the solution to the LPPs would tend to infinity.

Note that we get no real problem from the LPPs where columns  $\hat{\mathbf{y}}_i$  which are not extremal are included in our list, because the feasible region for such columns will be empty.

Note that while the outer distance measure d does not appear explicitly in either Theorem 4.3 or 4.4, it appears implicitly in both  $N(\mathbf{x})$  and in  $f_{\delta}(\mathbf{x})$ , so both theorems are generalized with respect to the shape of the noise.

Now a theorem reducing the bound from Theorem 3.1 is presented. The set of words is restricted to those that are close to the radius of the sphere only, introducing a benevolent cancellation in at least one

case. For the theorem, we denote

$$B_K(\delta) = \frac{2\tilde{t}_K(\delta) \max_{\mathbf{y}} f_{\delta}(\hat{\mathbf{y}})}{K-1},$$

and observe that for any q, n, |C| and any K and  $\delta$ ,  $B_K(\delta)$  is a bound on the maximal minimum squared Euclidean distance for a code with parameters q, n and |C|.

This improvement exploits cancellation in the differences and the fact that the bound is not dependent on the block length.

THEOREM 4.5 We have the bound

$$d_{\min}(C) \leqslant \max_{(\mathbf{x},\mathbf{y})\in R} d(\mathbf{x},\mathbf{y}),$$

where

$$R = \{ (\mathbf{r}_1, \mathbf{r}_2) \in Q^{\infty} \times Q^{\infty} : \tilde{t}_K(\delta) - \delta(\gamma_m) < \delta(\mathbf{r}_i) \leq \tilde{t}_K(\delta), i = 1, 2 \text{ and } d(\mathbf{r}_1, \mathbf{r}_2) \leq B_K(\delta) \},\$$

for  $\gamma_m$  such that  $\delta(\gamma_m) = \min_{i \neq 0} \delta(\gamma_i)$ .

The theorem is an extension of in Nilsson & Lennerstad (2000, Theorem II.2), where the quantity  $ad_E^2(\pi/2) + bd_E^2(\pi/4)$  was to be maximized constrained by the bound of the paper, similarly to Theorem 4.5. The reformulation changed the quantity to  $ad_E^2(\pi/2) + 2bd_E^2(\pi/4)$ , introducing a factor 2 in the second term. The basic idea is to demand that minimum distance can be written as the distance between two codewords being sufficiently close to the edge of the critical sphere.

Before proving Theorem 4.5, an example of how it can be used is given.

EXAMPLE 4.1 Consider the signal constellation of symmetric 8-PSK and  $d = d_E^2$ . Let *t* and  $\delta$  be such that  $S_{\delta,t}(\mathbf{0})$  contains only words consisting of zeros and at most two  $\pm \pi/4$ 's. Obviously,  $\delta(\pi/4) = \min_{\gamma_i \neq 0} \delta(\gamma_i)$ , otherwise some other words would be included in the sphere. Also, *t* must be at least  $2\delta(\pi/4)$ , implying that the set *R* described in Theorem 4.5 contains only all words with exactly two  $\pm \pi/4$ 's and all other symbols zero. The only differences which can appear between two words in *R* are  $2d_E^2(\pi/2), d_E^2(\pi/2) + 2d_E^2(\pi/4), 4d_E^2(\pi/4), d_E^2(\pi/2), 2d_E^2(\pi/4)$  and 0.

Assuming

$$4d_E^2\left(\frac{\pi}{4}\right) < d_E^2\left(\frac{\pi}{2}\right) + d_E^2\left(\frac{\pi}{4}\right) \leq B_K(\delta) < d_E^2\left(\frac{\pi}{2}\right) + 2d_E^2\left(\frac{\pi}{4}\right),$$

we could conclude that the bound is as low as  $4d_E^2(\pi/4)$ .

It is not guaranteed that the best bound is obtained by first minimizing  $B_K(\delta)$  with respect to K and  $\delta$ , as some other choice of K and  $\delta$  may allow for better use of Theorem 4.5, but it is a reasonable way to proceed in order to achieve a good bound.

*Proof.* A sequence of symbols **x** is in this proof called maximal if  $\tilde{t}_K(\delta) - \delta(\gamma_m) < \delta(\mathbf{x}) \le \tilde{t}_K(\delta)$ , nonmaximal if  $\delta(\mathbf{x}) \le \tilde{t}_K(\delta) - \delta(\gamma_m)$ , and not allowed if  $\tilde{t}_K(\delta) < \delta(\mathbf{x})$ . This theorem is possible since the bound is independent on the block length, since the function  $f_\delta$  in Theorem 3.1 represents the worst column in a matrix  $M_W$  where the rows are the words in W. So we relax the constraint that a sequence of symbols is limited to having *n* symbols. Instead we consider possibly infinite sequences. For each nonmaximal sequence in W, we add one column to the matrix with a non-zero symbol in the row of the nonmaximal sequence, so that the sequence is still allowed. This is possible, since at least  $\delta(\gamma_m)$  always can be added to a non-maximal sequence. All other entries in the column are zero. In the same way, columns are added to the matrix until all sequences are maximal, whereafter we may continue to add as many columns with only zeros as we like. This gives in the end a set W' and matrix  $M_{W'}$ . Clearly,  $d_{\min}(W) \leq d_{\min}(W')$ , as the distance between two sequences in W' are never smaller than the distance between the corresponding words in W. The theorem considers the maximum of all differences of maximal sequences fulfilling the bound  $B_K(\delta)$ , which bounds  $d_{\min}(W')$  from above. The result follows.

As a common assumption is that one operates under AWGN, it is reasonable to pay some additional attention to the case with  $d_E^2$  as outer distance measure. It turns out that a useful reformulation of  $f_{\delta}$  is possible when  $d = d_E^2$ . In particular, this reformulation permits a theorem for reducing the set of extremal columns, not completely unlike that of Theorem 4.1.

We consider the expression for  $f_{\delta}$  given in (4.1) and simplify it by using  $d = d_E^2$ , which allows writing  $-(T_2 + T_3)$  as a sum of two squares. Note that as

$$2(\sin^2(\theta - \vartheta) - \sin^2(\theta) - \sin^2(\vartheta)) = -4\sin^2(\theta)\sin^2(\vartheta) - \sin(2\theta)\sin(2\vartheta),$$
(4.9)

for any  $\theta$  and  $\vartheta$ , we get

$$4T_3 = -2\sum_{i=1}^{q-1}\sum_{j>i}a_ia_j(d_E^2(\gamma_i)d_E^2(\gamma_j) + \langle 2(\gamma_i/2)\rangle\langle 2(\gamma_j/2)\rangle d_E(2\gamma_i)d_E(2\gamma_j))$$
$$= -2\sum_{i=1}^{q-1}\sum_{j>i}a_ia_j(d_E^2(\gamma_i)d_E^2(\gamma_j) + \langle \gamma_i\rangle\langle \gamma_j\rangle d_E(2\gamma_i)d_E(2\gamma_j)).$$

Note that we may cancel the 2's in the expression  $(2(\theta/2))$  only because the division comes first (the operations are not associative in *T*). That division comes first follows from that the division is implicit already in the first equation describing  $T_3$ .

As a special case of (4.9), using  $\theta = \vartheta$ , the following equality:

$$-4\sin^2(\theta) = -4\sin^4(\theta) - \sin^2(2\theta)$$

is obtained, and yields

$$4T_2 = -\sum_{i=1}^{q-1} a_i^2 (d_E^4(\gamma_i) + d_E^2(2\gamma_i)).$$

Now observe that

$$-\left(\sum_{i=1}^{q-1} a_i d_E^2(\gamma_i)\right)^2 - \left(\sum_{i=1}^{q-1} a_i \langle \gamma_i \rangle d_E(2\gamma_i)\right)^2$$
  
=  $4T_2 - 2\sum_{i=1}^{q-1} \sum_{j>i} a_i a_j (d_E^2(\gamma_i) d_E^2(\gamma_j) + \langle \gamma_i \rangle \langle \gamma_j \rangle d_E(2\gamma_i) d_E(2\gamma_j))$   
=  $4(T_2 + T_3).$ 

Thus, we may write

$$f_{\delta} = \frac{4T_1 - \left(\sum_{i=1}^{q-1} a_i d_E^2(\gamma_i)\right)^2 - \left(\sum_{i=1}^{q-1} a_i \langle \gamma_i \rangle d_E(2\gamma_i)\right)^2}{4D}.$$

Theorem 4.1 and the following theorem may appear to be similar, but they are independent.

THEOREM 4.6 The condition

$$\sum_{i=1}^{q-1} a_i(\mathbf{x}) d_E^2(\gamma_i) = d_E^2(\mathbf{x}) \leqslant 4$$

holds for any extremal column x.

The theorem is a generalization of a result from Laksman et al. (2009b).

*Proof.* Assume that  $\mathbf{x}$  is an extremal column such that

$$\sum_{i=1}^{q-1} a_i(\mathbf{x}) d_E^2(\gamma_i) > 4,$$

i.e. a  $\delta$  exists such that  $\mathbf{x} = \operatorname{argmax}_{\mathbf{y}} f_{\delta}(\mathbf{y})$ . For such a  $\delta$ , let  $\gamma_m$  be a symbol such that

$$\frac{d_E^2(\gamma_m)}{\delta(\gamma_m)} \ge \frac{d_E^2(\gamma_i)}{\delta(\gamma_i)} \quad \forall i \in [0, q-1].$$
(4.10)

Then we have

$$\frac{d_E^2(\gamma_m)}{\delta(\gamma_m)} \geqslant \frac{\sum_{i=1}^{q-1} b_i d_E^2(\gamma_i)}{\sum_{i=1}^{q-1} b_i \delta(\gamma_i)},$$

for any non-negative constants  $b_1, \ldots, b_{q-1}$  whereof at least one is positive, as the right-hand side can be shown to be a weighted average of the quantities on the right-hand side of (4.10).

Now let **y** be a column such that  $a_m(\mathbf{y}) = 1$ ,  $a_0(\mathbf{y}) = K - 1$ , and thus  $a_i(\mathbf{y}) = 0$  for all  $i \notin \{0, m\}$ . Calculation shows that

$$f_{\delta}(\mathbf{y}) = (4K - 4) \frac{d_E^2(\gamma_m)}{4\delta(\gamma_m)}.$$

Next we will prove that  $f_{\delta}(\mathbf{x}) < f_{\delta}(\mathbf{y})$ , so **x** cannot be extremal. Form a bound on  $f_{\delta}(\mathbf{x})$  as

$$f_{\delta}(\mathbf{x}) \leqslant f_{\delta}(\mathbf{x}) + \frac{\left(\sum_{i=1}^{q-1} a_i(\mathbf{x}) \langle \gamma_i \rangle d_E(2\gamma_i)\right)^2}{4 \sum_{i=1}^{q-1} a_i(\mathbf{x}) \delta(\gamma_i)}$$
$$= \frac{4K \sum_{i=1}^{q-1} a_i(\mathbf{x}) d_E^2(\gamma_i) - \left(\sum_{i=1}^{q-1} a_i(\mathbf{x}) d_E^2(\gamma_i)\right)^2}{4 \sum_{i=1}^{q-1} a_i(\mathbf{x}) \delta(\gamma_i)}$$
$$= \left(4K - \sum_{i=1}^{q-1} a_i(\mathbf{x}) d_E^2(\gamma_i)\right) \frac{\sum_{i=1}^{q-1} a_i(\mathbf{x}) d_E^2(\gamma_i)}{4 \sum_{i=1}^{q-1} a_i(\mathbf{x}) \delta(\gamma_i)}.$$

But by assumption, we have

$$4K - 4 > 4K - \sum_{i=1}^{q-1} a_i(\mathbf{x}) d_E^2(\gamma_i) \quad \text{and} \quad \frac{d_E^2(\gamma_m)}{4\delta(\gamma_m)} \ge \frac{\sum_{i=1}^{q-1} a_i(\mathbf{x}) d_E^2(\gamma_i)}{4\sum_{i=1}^{q-1} a_i(\mathbf{x})\delta(\gamma_i)},$$

thus  $f_{\delta}(\mathbf{y}) > f_{\delta}(\mathbf{x})$ , which yields a contradiction. Hence, no extremal column  $\mathbf{x}$  with  $d_E^2(\mathbf{x}) > 4$  can exist.

## 5. Codes

For uncoded communication, it is trivial to see that the symmetric version of PSK maximizes the minimum distance, but for coded communication it is not so. In Examples 5.1 and 5.2, block codes with asymmetric PSK which are better than optimal block codes with symmetric PSK are presented. The codes used in these examples are very small, and presented only to show that performance can for some parameters be improved by use of asymmetric PSK rather than symmetric PSK. Longer and larger codes for which it is better to use asymmetric PSK than symmetric PSK are given in Bali & Rajan (1998), but those codes may be non-optimal.

For hard-decision decoding, a slight increase of minimum distance may not increase the errorcorrecting capability of the code. For soft-decision decoding, however, the error-correcting capability is arbitrarily close to half the minimum distance, so that any increase in minimum distance is an improvement.

The improvement of code performance gained by an increased minimum distance can be measured in terms of power saving for the transmitted signal. When using squared Euclidean distance (p = 2)an increased minimum distance by a certain factor leads approximately to a power saving by the same factor. For other distance measures of the form  $d_p(\gamma)$  an increased minimum distance still leads to power saving but for p not equal to 2 the relation between increase of minimum distance and power saving is not of the same simple form.

EXAMPLE 5.1 Consider a PSK code with q = 8, n = 2 and |C| = 3. The best such code given symmetric PSK and  $\gamma_i = 2\pi i/q$  is  $C = \{(\gamma_0, \gamma_0), (\gamma_3, \gamma_6), (\gamma_6, \gamma_3)\}$ , which results in  $d_{E\min}^2(C) \approx 5.41$ . The best such code given asymmetric PSK is obtained by using the same code, but with  $\gamma_i = 2\pi i/q$  only for even *i*, and  $\gamma_i = 2\pi (i + 0.41)/q$  for odd *i*, which results in  $d_{E\min}^2(C) \approx 5.79$ .

The columns  $\hat{\mathbf{y}}_i = (\gamma_i, \gamma_0, \dots, \gamma_0)^\top$ , for  $i = 1, \dots, 7$  and  $\hat{\mathbf{y}}_8 = (\gamma_1, \gamma_6, \gamma_0, \dots, \gamma_0)^\top$  are extremal. For K = 2, also  $\hat{\mathbf{y}}_9 = (\gamma_1, \gamma_7)^\top$  and  $\hat{\mathbf{y}}_{10} = (\gamma_2, \gamma_7)^\top$  are extremal. If  $K \ge 3$ , then  $\hat{\mathbf{y}}_9 = (\gamma_1, \gamma_7, \gamma_7, \gamma_0, \dots, \gamma_0)^\top$  and  $\hat{\mathbf{y}}_{10} = (\gamma_2, \gamma_7, \gamma_7, \gamma_0, \dots, \gamma_0)^\top$  are extremal.

With K = 2 and  $\delta(\hat{\mathbf{y}}_8)$  critical, we get

$$\begin{split} \delta(\gamma_1) &= 1.11, \quad \delta(\gamma_2) = 2.68, \\ \delta(\gamma_3) &= 3.79, \quad \delta(\gamma_4) = 4.00, \\ \delta(\gamma_5) &= 2.89, \quad \delta(\gamma_6) = 2.68, \\ \delta(\gamma_7) &= 0.89. \end{split}$$

for  $A_8 = 18.05$ . This yields the bound 7.58, which can also be obtained by some other inner distance measures, and is the best bound attainable by this method.

That the code in the example is optimal within the set of codes over asymmetric PSK has been verified by exhaustive search.

EXAMPLE 5.2 Consider a PSK code with q = 8, n = 2 and |C| = 4. The best such code given symmetric PSK and  $\gamma_i = 2\pi i/q$  is  $C = \{(\gamma_0, \gamma_0), (\gamma_1, \gamma_4), (\gamma_4, \gamma_1), (\gamma_5, \gamma_5)\}$ , which results in  $d_{E\min}^2(C) \approx 4.59$ . The best such code given asymmetric PSK is obtained by using the same code, but with  $\gamma_i = 2\pi i/q$  only for even *i*, and  $\gamma_i = 2\pi (i + 0.57)/q$  for odd *i*, which results in  $d_{E\min}^2(C) \approx 5.33$ .

With K = 2 and  $\delta(\hat{\mathbf{y}}_8)$  critical, we get

$$\begin{split} \delta(\gamma_1) &= 1.70, \quad \delta(\gamma_2) = 2.18, \\ \delta(\gamma_3) &= 3.89, \quad \delta(\gamma_4) = 4.00, \\ \delta(\gamma_5) &= 2.66, \quad \delta(\gamma_6) = 2.18, \\ \delta(\gamma_7) &= 0.48, \end{split}$$

for  $A_8 = 17.10$ . This yields the bound 5.33 which is the best bound possible, though, many other inner distance measures result in the same bound.

That the code in this example is optimal within the set of codes over asymmetric PSK has been verified by exhaustive search. That the code is optimal within the set of codes over asymmetric PSK does not follow from its minimum distance meeting the bound, as this is only a bound for one particular asymmetric PSK constellation.

Examples 5.3–5.7, based on multilevel codes (Imai & Hirakawa, 1977), consider symmetric *q*-PSK and are intended to show how to apply the bound for large *n*, and to show instances where the bound is tight with respect to  $d_E^2$ . However, the inner distance measure used to prove this is the same one presented already in Nilsson & Lennerstad (2000). In the following examples, we denote the symbols  $\gamma_i = 2\pi i/q, i \in [0, q - 1]$ .

EXAMPLE 5.3 Consider q = 3a, where  $a \ge 2$  is an integer. Then a code *C* with  $n = (3^m + 1)/2$ ,  $|C| = a^n 3^{n-m-1}$  and  $d_{E\min}^2 = 4d_E^2(\gamma_1)$  exists, for any integer  $m \ge 2$ . It can be constructed as C = C1 + 3C2 where *C*1 is a ternary extended Hamming code and *C*2 is  $\mathbb{Z}_a^n$ . The bound described in this work will be used to show that for large enough *m* the code *C* has the highest  $d_{E\min}^2$  possible.

Consider the inner distance measure  $\delta$  described in (4.5), with i = 1, and  $t = 2\delta(\gamma_1)$ . These  $\delta$  and t do not necessarily yield the lowest bound possible initially, but by use of Theorem 4.5 they will be sufficient. Theorem 4.5 gives that the bound must have the form (in order of size)  $2d_E^2(\gamma_1)$ ,  $d_E^2(\gamma_2)$ ,  $4d_E^2(\gamma_1)$ ,  $2d_E^2(\gamma_1)$ ,  $d_E^2(\gamma_2)$  or  $2d_E^2(\gamma_2)$ .

The chosen  $\delta$  results in  $\hat{\mathbf{y}} = (\gamma_1, \gamma_{q-1}, \gamma_0, \gamma_0, \dots, \gamma_0)^\top$  and

$$f_{\delta}(\hat{\mathbf{y}}) = \frac{2Kd_{E}^{2}(\gamma_{1}) - d_{E}^{4}(\gamma_{1})}{2\delta(\gamma_{1})} = \frac{2(K-2)d_{E}^{2}(\gamma_{1}) + d_{E}^{2}(\gamma_{2})}{2\delta(\gamma_{1})}.$$

The bound becomes

$$\frac{2tf_{\delta}(\hat{\mathbf{y}})}{K-1} = 2d_E^2 + \frac{2(K-3)d_E^2(\gamma_1) + 2d_E^2(\gamma_2)}{K-1}.$$

As  $d_E^2(\gamma_2) > 2d_E^2(\gamma_1)$  for  $q \ge 5$ , we see that for  $K \ge 4$  the bound is less than  $2d_E^2(\gamma_1) + d_E^2(\gamma_2)$ , which is enough to claim that it is  $4d_E^2(\gamma_1)$ . To show that *C* is optimal with respect to  $d_{E\min}^2$ , it now suffices to show that  $K \ge 4$ .

The size of the critical sphere is  $|S_{\delta,t}| = \sum_{i=0}^{2} 2^{i} {n \choose i} = 2n^{2} + 1$ . We have

$$K = \left\lceil \frac{|S_{\delta,t}||C|}{q^n} \right\rceil \ge \left\lceil \frac{(3^m+1)^2}{2 \times 3^{m+1}} \right\rceil,$$

which is growing with respect to m. As m = 3 yields K = 4, we see that C is optimal if  $m \ge 3$ .

EXAMPLE 5.4 Let q = 2a, where  $a \ge 3$  is an integer. Then a code *C* with  $n = 2^m$ ,  $|C| = a^n 2^{n-m-1}$  and  $d_{E\min}^2 = d_E^2(\gamma_2)$  exists, for any integer  $m \ge 2$ . It can be constructed as C = C1 + 2C2 where C1 is a binary extended Hamming code and C2 is  $\mathbb{Z}_a^n$ . The bound described in this work will be used to show that *C* has the highest  $d_{E\min}^2$  possible.

Consider the inner distance measure  $\delta$  described in (4.5), with i = 1, and  $t = \delta(\gamma_1)$ . These  $\delta$  and t are not necessarily the best possible, but they will be sufficient. The size of the critical sphere is  $|S_{\delta,t}| = \sum_{i=0}^{1} 2^i {n \choose i} = 2n + 1$ . We have

$$K = \left\lceil \frac{|S_{\delta,t}||C|}{q^n} \right\rceil \geqslant \left\lceil \frac{2^{m+1}+1}{2^{m+1}} \right\rceil = 2.$$

The chosen  $\delta$  results in  $\hat{\mathbf{y}} = (\gamma_1, \gamma_{q-1}, \gamma_0, \gamma_0, \dots, \gamma_0)^\top$  and

$$f_{\delta}(\hat{\mathbf{y}}) = \frac{2Kd_E^2(\gamma_1) - d_E^4(\gamma_1)}{2\delta(\gamma_1)}.$$

The bound becomes

$$\frac{2tf_{\delta}(\hat{\mathbf{y}})}{K-1} = \frac{2Kd_{E}^{2}(\gamma_{1}) - d_{E}^{4}(\gamma_{1})}{K-1},$$

which for K = 2 simplifies to  $d_E^2(\gamma_2)$ .

Hence, C is optimal with respect to  $d_{E\min}^2$ .

EXAMPLE 5.5 Consider q = 4a, where  $a \ge 2$  is an integer. Then a code *C* with  $n = 2^m$ ,  $|C| = a^n 2^{2n-m-2}$ and  $d_{E\min}^2 = 4d_E^2(\gamma_1)$  exists, for any integer  $m \ge 2$ . It can be constructed as C = C1 + 2C2 + 4C3 where *C*1 is a binary extended Hamming code, *C*2 is a binary code with a parity check bit and *C*3 is  $\mathbb{Z}_a^n$ . The bound described in this work will be used to show that for large *m* the code *C* has the highest  $d_{E\min}^2$ possible.

Proceed as in Example 5.3, including the choice of  $\delta$  and *t* to show that  $K \ge 4$  is sufficient.

The size of the critical sphere is  $|S_{\delta,t}| = \sum_{i=0}^{2} 2^{i} {n \choose i} = 2n^{2} + 1$ . We have

$$K = \left\lceil \frac{|S_{\delta,t}||C|}{q^n} \right\rceil \geqslant \left\lceil \frac{2^{2m+1}+1}{2^{m+2}} \right\rceil,$$

which is growing with respect to m. As m = 3 yields K = 4, we see that C is optimal if  $m \ge 3$ .

EXAMPLE 5.6 Consider q = 4a, where  $a \ge 2$  is an integer. Then a code *C* with  $n = 2^m$ ,  $|C| = a^n 2^{2n-2m-1}$ and  $d_{E\min}^2 = 6d_E^2(\gamma_1)$  exists, for any even integer  $m \ge 4$ . It can be constructed as C = C1 + 2C2 + 4C3where *C*1 is a binary extended Preparata code, *C*2 is a binary code with a parity check bit and *C*3 is  $\mathbb{Z}_a^n$ .

The bound described in this work will be used to show that for large *m* the code *C* has the highest  $d_{E\min}^2$  possible.

Proceed as in Example 5.3, including the choice of  $\delta$ , but let  $t = 3\delta(\gamma_1)$ . With this value of t, Theorem 4.5 gives that the bound must be one of the following values (given in order of size):  $2d_E^2(\gamma_1)$ ,  $d_E^2(\gamma_2)$ ,  $4d_E^2(\gamma_1)$ ,  $2d_E^2(\gamma_1) + d_E^2(\gamma_2)$ ,  $6d_E^2(\gamma_1)$ ,  $2d_E^2(\gamma_2)$ ,  $4d_E^2(\gamma_1) + d_E^2(\gamma_2)$ ,  $2d_E^2(\gamma_1) + 2d_E^2(\gamma_2)$ ,  $3d_E^2(\gamma_2)$ . Note that the order of size here depends on  $q \ge 5$ . Using that  $q \ge 8$ , so that  $d_E^2(\gamma_2) \ge (2 + \sqrt{2})d_E^2(\gamma_1)$ , it can be seen that

$$f_{\delta}(\hat{\mathbf{y}}) \leqslant \frac{(2-\sqrt{2})(K-2)+1}{2\delta(\gamma_1)} d_E^2(\gamma_2),$$

so that the bound  $(2tf_{\delta}(\hat{\mathbf{y}})/(K-1))$  is less than or equal to

$$3\frac{(2-\sqrt{2})(K-2)+1}{K-1}d_E^2(\gamma_2)$$

which is less than  $2d_E^2(\gamma_2)$  when  $K \ge 7$ . Hence, whenever  $K \ge 7$ , the bound is  $6d_E^2(\gamma_1)$ .

The size of the critical sphere is  $|S_{\delta,t}| = \sum_{i=0}^{3} 2^{i} {n \choose i} \ge n^{3}$ , with equality if and only if n = 3. We have

$$K = \left\lceil \frac{|S_{\delta,t}||C|}{q^n} \right\rceil \approx \left\lceil \frac{2^{3m}}{2^{2m+1}} \right\rceil,$$

which is growing with respect to m. As m = 4 yields K = 8, we see that C is optimal if  $m \ge 4$ .

EXAMPLE 5.7 Consider q = ap, where  $p \ge 5$  is a prime and a is a positive integer. Then a code C with  $n = p^m - 1$ ,  $|C| = a^n p^{n-(r-1)m-1}$  and  $d_{E\min}^2 = 2rd_E^2(\gamma_1)$  exists, for  $m \ge 1$  and  $r \le (p-1)/2$ , both integers. It can be constructed as C = C1 + pC2 where C1 is a code from Roth & Siegel (1994) and  $C2 = \mathbb{Z}_a^n$ . Remark that the code C1 was originally developed to perform well with respect to the Leemetric. The bound described in this work will be used to show that for large enough m the code C has the highest  $d_{E\min}^2$  possible.

In the case r = 2, assume  $m \ge 2$  and proceed as in Example 5.3, including the choice of  $\delta$  and t to show that  $K \ge 4$  is sufficient. The size of the critical sphere is again  $2n^2 + 1$ , and

$$K = \left\lceil \frac{(2(p^m - 1)^2 + 1)}{p^{m+1}} \right\rceil > \left\lceil \frac{p^{2m}}{p^{m+1}} \right\rceil \ge p,$$

which is sufficient to claim  $K \ge 4$ , so that C is optimal with respect to  $d_{E\min}^2$ .

In the case r = 3, assume  $m \ge 2$  and proceed as in Example 5.6, including the choice of  $\delta$  and t to show that  $K \ge 7$  is sufficient. Note that r = 3 requires  $p \ge 7$ . The size of the critical sphere is again at least  $n^3$ , and

$$K = \left\lceil \frac{(p^m - 1)^3}{p^{2m+1}} \right\rceil = \left\lceil \frac{p^{3m}(p^m - 1)^3}{p^{3m}p^{2m+1}} \right\rceil \ge \left(\frac{p^m - 1}{p^m}\right)^3 p.$$

But  $p^m \ge 49$ , so  $((p^m - 1)/p^m)^3 \ge 0.94$ , which multiplied by *p* is at least 6.58, so  $K \ge 7$  is obtained. Hence, *C* is optimal with respect to  $d_{E\min}^2$ .

In the general case, let  $\delta$  be defined as in (4.5) with i = 1 and let  $t = rd_E^2(\gamma_1)$ .

To bound the size of the critical sphere from above, some preparation is necessary. First, note that  $n = p^m - 1 \ge (2r + 1)^m - 1 > 4r^2$ . Next, we will need

$$\binom{n}{r} \ge \frac{n^r - \binom{r}{2}n^{r-1}}{r!}.$$
(5.1)

That this holds can be seen in the following manner: write  $\binom{n}{r}$  as a polynomial in *n*. The denominator is r!, while the numerator is  $n(n-1)\cdots(n-r+1)$ . When expanding this polynomial, we note that the signs are alternating. Also, we will show that  $r^2|c_k| > |c_{k-1}|$ , where  $c_k$  is the coefficient of  $n^k$  for any k.<sup>1</sup> We see this by the following equation:

$$r^{2}|c_{k}| = r^{2} \sum_{i} p_{k}^{(i)} = r \sum_{i} \sum_{j=0}^{r-1} p_{k}^{(i)} > \sum_{i} \sum_{j=0}^{r-1} jp_{k}^{(i)} > \sum_{i} p_{k-1}^{(i)} = |c_{k-1}|,$$

where  $p_k^{(i)}$  for different *i* span over all products of r - k distinct integers from the interval [0, r - 1]. As  $n > r^2$ , we get  $|c_k|n^k > |c_{k-1}|n^{k-1}$ . Now (5.1) follows easily as

$$\binom{n}{r} = \frac{\sum_{k} c_{k} n^{k}}{r!} \ge \frac{c_{r} n^{r} + c_{r-1} n^{r-1}}{r!} = \frac{n^{r} - \binom{r}{2} n^{r-1}}{r!},$$

where the inequality follows from pairing adjacent terms.

Using (5.1), the size of the critical sphere can be estimated as

$$|S_{\delta,t}| = \sum_{i=0}^{r} 2^{i} \binom{n}{i} \ge 2^{r} \binom{n}{r} \ge \frac{2^{r}}{r!} \left( n^{r} - \binom{r}{2} n^{r-1} \right).$$

Using that  $m \ge 2$  and that only cases where  $r \ge 4$  so that  $p \ge 11$  need to be dealt with,

$$\begin{aligned} |S_{\delta,t}| &\ge \frac{1.98^r}{r!} \left( p^{rm} - \binom{r}{2} p^{(r-1)m} \right) \ge \frac{1.98^r}{r!} p^{rm-2} \left( p^2 - \binom{r}{2} \right) \\ &\ge \frac{1.98^r}{r!} p^{rm-2} \left( (2r+1)^2 - \binom{r}{2} \right) > \frac{1.98^r}{(r-1)!} p^{rm-2} (3r+4). \end{aligned}$$

We get

$$K \ge \left\lceil \frac{1.98^r (3r+4)p^{rm-2}}{(r-1)!p^{(r-1)m+1}} \right\rceil = \left\lceil \frac{1.98^r (3r+4)p^{m-3}}{(r-1)!} \right\rceil$$

which is strictly increasing with respect to *m*, and  $K \to \infty$  when  $m \to \infty$  and *r* is fixed. The bound has the form

$$\frac{2tf_{\delta}(\tilde{\mathbf{y}})}{K-1} = \frac{2(K-1)d_E^2(\gamma_1) + (d_E^2(\gamma_2) - 2d_E^2(\gamma_2))}{K-1}r.$$

The bound quite clearly approaches  $2rd_E^2(\gamma_1)$  from above as *K* approaches infinity, so for any fixed *r*, the bound will be tight for large enough *m*.

<sup>&</sup>lt;sup>1</sup> In fact,  $|c_k|$  are Sterling numbers of the first kind, the number of ways in which r distinct objects can be placed in r - k cycles. The property shown for them here may be—and probably is—known.

### 22 of 23

#### E. LAKSMAN ET AL.

The code *C* is optimal with respect to  $d_{E\min}^2$  if *m* is large enough. For r = 2 and r = 3, we have seen that  $m \ge 2$  is sufficient.

## 6. Conclusion

We have considered Elias' sphere argument for forming upper bounds on codes over distance uniform signal constellations, taken an improvement of it developed for symmetric PSK with squared Euclidean distance, and generalized the improvement to work also for asymmetric PSK and other additive and translation-invariant distance measures.

Codes over asymmetric PSK may be interesting for applications since there are examples of code parameters where codes over asymmetric PSK have higher minimum Euclidean distance than codes over symmetric PSK, although the difference seem not to be large. The bound, as well as the proof of it, is a generalization of a previous result for codes over symmetric PSK. The bound is formulated in terms of extremal columns, but as the formulation is more general, less can be said about the extremal columns. Nonetheless, results to help determining the extremal columns for given parameters are presented. The results in the paper are general, valid for both symmetric PSK and asymmetric PSK block codes, and most of the results can be applied for any additive and translation-invariant distance measure.

Noise in wireless communication is often assumed to be AWGN, which leads to the codeword which has the least square Euclidean distance to the received signal being the codeword most likely sent. Typically, the error-correcting codes used are created in order to give the best error-correcting capability, i.e. the greatest minimum squared Euclidean distance, in relation to the amount of data that has to be transmitted. If the noise follows a different distribution than AWGN, ML decoding is no longer equivalent to finding the codeword or code sequence closest with respect to squared Euclidean distance to the received signal. A different distribution of noise gives rise to a different distance measure to use when measuring proximity between signals.

A method for forming upper bounds on minimum squared Euclidean distance for PSK block codes has been generalized to work for other distances as well, and special consideration has been given to the distances for which minimum distance decoding corresponds to ML-decoding when noise follows generalized *p*-Gaussian density. Several classes of codes have by use of the bound been shown to be optimal with respect to  $d_{Emin}^2$  within the set of block codes over symmetric PSK.

It is of general importance to understand the limits of minimum distance (with respect to a relevant distance measure) for a code with certain parameters in order to maximize the potential for error correction and noise independence. This approach, based on an extended version of the Elias' bound, has the advantage of being independent of the structure of the code—a code is only assumed to be a subset of the universe.

We consider the ease with which generalizations and extensions can be made, demonstrated by the results of the paper, as an important virtue of the present approach.

### References

BALI, J. & RAJAN, B. S. (1998) Block-coded PSK modulation using twolevel group codes over dihedral groups. IEEE Trans. Inf. Theory, 44, 1620–1631.

BERLEKAMP, E. R. (1968) Algebraic Coding Theory. New York: McGraw Hill.

DIVSALAR, D., SIMON, M. K. & YUEN, J. H. (1987) Trellis coding with asymmetric modulations. *IEEE Trans. Commun.*, **35**, 130–141.

IMAI, H. & HIRAKAWA, S. (1977) A new multilevel coding method using error-correcting codes. *IEEE Trans. Inf. Theory*, IT-23, 371–377.

- ISAKA, M., FOSSORIER, M. P. C., MORELOS-ZARAGOZA, R. H., LIN, S. & IMAI, H. (2000) Multilevel coded modulation for unequal error protection and multistage decoding. II. Asymmetric constellations. *IEEE Trans. Commun.*, 48, 774–786.
- KSCHISCHANG, F. R., DE BUDA, P. G. & PASUPATHY, S. (1989) Block coset codes for *M*-ary phase shift keying. *IEEE J. Sel. Areas Commun.*, **7**, 900–913.
- LAKSMAN, E., LENNERSTAD, H. & NILSSON, M. (2009a) Bounding the Euclidean minimum distance for any PSK block codes of alphabet size 8. *Proc: IEEE Information Theory Workshop*, Taormina, Italy.
- LAKSMAN, E., LENNERSTAD, H. & NILSSON, M. (2009b) Inner metric bounds on the minimal Euclidean distance for arbitrary *q*-ary block codes. *Presented at Conference: The 9th International Conference on Finite Fields and their Applications*, Dublin, Ireland.
- LAKSMAN, E., LENNERSTAD, H. & NILSSON, M. (2010) Improving bounds on the minimal Euclidean distance for block codes by inner metric optimization. *Discrete Math.*, 310, 3267–3275.
- MACWILLIAMS, F. J. & SLOANE, N. J. A. (1977) *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland.
- NILSSON, M. & LENNERSTAD, H. (2000) An upper bound on the minimum Euclidean distance for block coded phase shift keying. *IEEE Trans. Inf. Theory*, 46, 656–662.
- NILSSON, M. & LENNERSTAD, H. (2005) Improved upper bound on the minimum Euclidean distance for block coded phase shift keying. *Proc: RadioVetenskap och Kommunikation 05*. Sweden: Linköping.
- NILSSON, M., LENNERSTAD, H. & LAKSMAN, E. (2008) A two-metric approach to improve bounds on the minimum Euclidean distance for block codes. *Proc: RadioVetenskap och Kommunikation 08*, Växjö, Sweden.
- PHAM, T. T. & DEFIGUEIREDO, R. J. P. (1989) Maximum likelihood estimation of a class of non-Gaussian densities with application to deconvolution. *IEEE Trans. Acoust. Speech Signal Process.*, **37**, 73–82.
- PIRET, PH. (1986) Bounds for codes over the unit circle. IEEE Trans. Inf. Theory, IT-32, 760-767.
- QUISTORFF, J. (2006) New upper bounds on Lee codes. Discrete Appl. Math., 154, 1510–1521.
- RAJAN, B. S. & VISWANATH, G. (2003) On asymptotic Elias bound for Euclidean space codes over distance-uniform signal sets. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, E86-A, 480–486.
- ROTH, R. M. (2006) Introduction to Coding Theory. Cambridge: Cambridge University Press.
- ROTH, R. M. & SIEGEL, P. H. (1994) Lee-metric BCH codes and their application to constrained and partialresponse channels. *IEEE Trans. Inf. Theory*, **40**, 1083–1096.
- STÜBER, G. L. & KATZ, E. (1995) Systematic trellis-coded modulation with asymmetric constellations. Proc: Global Telecommunications Conference, 1995. Conference Record. Communication Theory Mini-Conference, GLOBECOM '95. IEEE.
- SUBBOTIN, M. T. (1923) On the law of frequency of errors. Mat. Sb., 31, 296-301.
- TAGUCHI, T. (1987) On a generalization of Gaussian distribution. Ann. Inst. Statis. Math., 39, 211-242.
- VAN LINT, J. H. (1992) Introduction to Coding Theory. Berlin: Springer.
- VISWANATH, G. (2004) Elias upper bound for Euclidean space codes and codes close to the singleton bound, *Ph.D. Thesis*, Indian Institute of Science, India.
- WYNER, A. D. (1987) Bounds on communication with polyphase coding. Probl. Pereda. Inform., 23, 18-26.
- ZHANG, X., ZHAO, Y. & ZOU, L. (2009) Optimum asymmetric constellation design for trellis-coded modulation over Gaussian Channels. *IEEE Commun. Lett.*, 13, 528–530.