On the performance of binary extremal self-dual codes

STEFKA BOUYUKLIEVA

Department of Mathematics and Informatics
Veliko Tarnovo University
5000 Veliko Tarnovo, Bulgaria,

ANTON MALEVICH and WOLFGANG WILLEMS

Department of Mathematics
University of Magdeburg
39016 Magdeburg, Germany

Abstract

The decoding error probability of a code C measures the quality of performance when C is used for error correction in data transmission. In this note we compare different types of codes with regard to the decoding error probability.

1 Introduction

From a pure mathematical point of view binary extremal self-dual codes of type II deserve particular attention. They are related to unimodular even lattices, provide 5-designs, and often have interesting automorphism groups. In this paper we investigate how good they perform if used for error correction in data transmission. To measure the performance we take the decoding error probability and assume that bounded distance decoding is used for correction of errors.

The notation thoughout the paper is standard and can be taken from [8]. A binary self-dual code C is called of type II if for all codewords $c \in C$ the weight $\mathrm{wt}(c)$ is divisible by 4. Otherwise, i.e., $2 \mid \mathrm{wt}(c)$ for all $c \in C$ and there is a codeword c with $4 \nmid \mathrm{wt}(c)$ we say that C is of type I. A binary self-dual code of length n and minimum distance d satisfies

$$d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + \delta$$

where $\delta = 4$ if $n \not\equiv 22 \bmod 24$ and $\delta = 6$ if $n \equiv 22 \bmod 24$ (see [11], [10]). We call C extremal if the bound is attained. Furthermore, if $24 \mid n$ then an extremal self-dual code is always of type II as Rains has shown in [11]. Finally, extremal codes of type II do not exist for large n according to a result of Mallows and Sloane [9]. More precisely, due to Zhang [13], the length n is bounded by 3928. Apart from section 2 all codes are binary.

2 Decoding error probabilities

The question of decoding error probabilities was studied in [6] for bounded distance decoding. For the reader's convenience we repeat here the main result which we shall apply below to measure the quality of performance.

Assume that a linear $[n,k,d]$ code C over a finite field $K = \mathbb{F}_q$ is used for error correction in data transmission over a non-reliable channel, say with symbol error probability p. In addition, we assume that bounded distance decoding is used, i.e., we decode only up to $t \leq \frac{d-1}{2}$ errors. Finally, for $x \in K^n$ and $r \in \mathbb{N}_0$ the set

$$\mathrm{B}_r(x) = \{y \mid y \in K^n,\, \mathrm{d}(x,y) \leq r\}$$

describes the ball around x of radius r.

Clearly, a decoding error occurs exactly if the receiver gets a vector $y \in \mathrm{B}_t(c)$ for some codeword $c \in C$ which was not transmitted. Thus the probability of a decoding error is the conditional probability

$$\mathrm{P}(C,t,p) = P(X \in C \setminus \{c\} \mid Y \in \mathrm{B}_t(c)\}$$

where the random variable X stands for the transmitted codeword and Y for the received vector. As a main result of [6] we have

Theorem 1 *Let C and C' be $[n,k,d]$ codes with weight distributions $(a_0,\ldots,a_n)$ and $(a'_0,\ldots,a'_n)$ respectively. If the symbol error probability p is small enough then for all $t \leq \frac{d-1}{2}$ the following two conditions are equivalent.*

a) $\mathrm{P}(C,t,p) < \mathrm{P}(C',t,p)$.

b) $(a_0,\ldots,a_n) \prec (a'_0,\ldots,a'_n)$, *where $\prec$ means lexicographical ordering.*

Thus for small p the quality of performance can be read off from the weight distribution. We say that C performs better than C' if $(a_0,\ldots,a_n) \prec (a'_0,\ldots,a'_n)$. In this spirit we shall study different classes of codes in the following sections.

3 Self-dual codes vs non self-dual codes

Let C be a self-dual $[n,\frac{n}{2},d]$ code of type II with weight distribution $(a_0,\ldots,a_n)$. Suppose that C' is any other non self-dual code with the same parameters as C and weight distribution $(a'_0,\ldots,a'_n)$. Since C is of type II we have $a_k = 0$ for all k with $4 \nmid k$. Thus the weight function takes generically less values on C than on C', or in other words, the codewords of C are concentrated in less weight values. Therefore we may expect that $a'_d < a_d$, i.e., C' performs better than the self-dual code C of type II. It turns out that this is not true in general.

Let C be any extremal self-dual [32,16,8] code of type II, for instance the extended quadratic residue code of length 31. Thus, by ([9], Theorem 2), we have $a_d = a_8 = 620$. In

[3], Cheng and Sloane contructed a $[32, 17, 8]$ code. If we delete one row in the generator matrix of C, we obtain a $[32, 16, 8]$ code C' which is not self-dual. Computing a'_d with Magma we get $a'_d = a_8 = 681$. Thus the self-dual type II code C performs better than the non self-dual code C'.

4 Experimental results

Let C and C' be extremal self-dual codes of length n and minimal distance d. Suppose that C is of type II and C' of type I. By Gleason's result [7], we know that $8 \mid n$. Furthermore, by Rains [11], an extremal self-dual code of length $n = 24m$ is always of type II. Thus we may assume that $n = 24m + 8$ or $n = 24m + 16$. Let a_d and a'_d denote the number of codewords of weight d in C resp. C'. Checking the examples of known extremal codes we find the following. For the existence of the particular codes we refer to [2], [5], [4].

n	d	a_d (type II)	a'_d (type I)
32	8	620	364
40	8	285	$125 + 16\beta$ $(0 \leq \beta \leq 26)$ (two codes are known with $A'_d = 285$ i.e. $\beta = 10$)
56	12	8 190	$\leq 4\,862$
64	12	2 976	$1\,312 + 16\beta$ $(0 \leq \beta \leq 284)$ (in all known examples $A'_d \leq 2336$ and $\beta \leq 64$)
80	16	97 565	$\leq 66\,845$
104	20	1 136 150	$\leq 739\,046$

We see that in the known examples of extremal self-dual codes the type I codes always perform better than the type II provided $n = 24m + 8 \geq 32$. The parameter β in the last column takes care of the fact that in contrast to extremal self-dual type II codes the weight distribution of type I codes is not unique in general. For $n = 56, 80$ and 104 we have computed a'_d for all possible weight distributions and the bounds are given in column four. Finally note that for $n = 40$ the two known codes of type I which satisfy $a'_d = 285$ perform worse than any extremal type II code since $a'_{d+2} \neq 0$, but $a_{d+2} = 0$.

In order to value the performance of self-dual type I codes we need the concept of a shadow.

5 The shadow of self-dual codes

Let C be a $[n, n/2, d]$ self-dual code of type I. Furthermore let C_0 denote the subcode of C consisting of all codewords whose weights are multiples of 4. If $C_2 = C \setminus C_0$ then the shadow $S = \mathrm{S}(C)$ consists of all vectors $u \in \mathbb{F}_2^n$ with the property that

$$\begin{aligned} u \cdot v = 0 \quad & \text{for all } v \in C_0, \\ u \cdot v = 1 \quad & \text{for all } v \in C_2. \end{aligned}$$

Note that ${C_0}^{\perp}$ consists of the union of four cosets of C_0, say $C_0 \cup C_1 \cup C_2 \cup C_3$. If $C = C_0 \cup C_2$ then $S = \mathrm{S}(C) = C_0^{\perp} \setminus C = C_1 \cup C_3$. For our purpose (comparing the performance with codes of type II), we may suppose that $8 \mid n$, by [7]. Using the invariants of a self-dual code of type I the weight enumerator of C can be written as

$$A(x,y) = \sum_{0 \leq j \leq \lfloor \frac{n}{2} \rfloor} a_j x^{n-2j} y^{2j} = \sum_{0 \leq i \leq \lfloor \frac{n}{8} \rfloor} c_i (x^2+y^2)^{\frac{n}{2}-4i} \{x^2 y^2 (x^2-y^2)^2\}^i \tag{1}$$

with $a_j \in \mathbb{N}_0$ and $c_i \in \mathbb{Z}$. By ([9], Theorem 5), we get

$$S(x,y) = \sum_{0 \leq j \leq 2 \lfloor \frac{n}{8} \rfloor} b_j x^{n-4j} y^{4j} = \sum_{0 \leq i \leq \lfloor \frac{n}{8} \rfloor} (-1)^i c_i 2^{\frac{n}{2}-6i} (xy)^{\frac{n}{2}-4i} (x^4-y^4)^{2i}. \tag{2}$$

for the weight enumerator of its shadow Note that in our particular case, i.e., $8 \mid n$, the weights of the shadow are always divisible by 4.

Definition 2 A self-dual code C of type I is called a *code with minimal shadow* if $b_1 = 1$ in (2), i.e., the shadow of C has minimum weight 4 and contains exactly one vector of weight 4.

Apart from minimal shadows we need the concept of s-extremality, a notion which was introduced in [1] by Bachoc and Gaborit.

Lemma 3 ([1], Theorem 1) *If C is a self-dual code of type I with minimum distance d and minimum weight s of the shadow then $2d + s \leq \frac{n}{2} + 4$ unless $n \equiv 22 \bmod 24$ and $d = \lfloor \frac{n}{24} \rfloor + 6$, in which case $2d + s = \frac{n}{2} + 8$.*

Definition 4 Under the assumptions of Lemma 3 a code C is called *s-extremal* if the bounds are reached, i.e., if $2d + s = \frac{n}{2} + 4$ or $2d + s = \frac{n}{2} + 8$.

In both cases, i.e., C s-extremal or C with minimal shadow it has been shown that the weight enumerator of C and its shadow are uniquely determined (see ([1], Definition 2.2) and ([12], Lemma 1)).

6 The performance of extremal self-dual codes of type I

In this section we prove

Theorem 5 *In the set of self-dual extremal codes of type I and length $n = 24m + 8$ the s-extremal codes perform best.*

Let C be as in the theorem. Since all weights of the shadow $S = \mathrm{S}(C)$ are divisible by 4 the minimum weight of the shadow can be written as $4s$ with $s \geq 1$. We express this dependency on s in the formulas for the weight enumerators.

Setting $x = 1$ in (1) and (2) we obtain

$$\begin{aligned} A^{(s)}(y) &= \sum_{j=0}^{12m+4} a_j^{(s)} y^{2j} = \sum_{i=0}^{3m+1} c_i^{(s)} (1+y^2)^{12m+4-4i} (y^2(1-y^2)^2)^i, \\ S^{(s)}(y) &= \sum_{j=0}^{6m+2} b_j^{(s)} y^{4j} = \sum_{i=0}^{3m+1} (-1)^i c_i^{(s)} 2^{12m+4-6i} y^{12m+4-4i} (1-y^4)^{2i}. \end{aligned} \tag{3}$$

Note that $a_j^{(s)}, b_j^{(s)} \in \mathbb{N}_0$ and $c_j^{(s)} \in \mathbb{Z}$. As in [11] we may write

$$c_i^{(s)} = \sum_{j=0}^{i} \alpha_{ij} a_j^{(s)} = \sum_{j=0}^{3m+1-i} \beta_{ij} b_j^{(s)}$$

with $\alpha_{ij}, \beta_{ij} \in \mathbb{Q}$. We would like to mention here that both α_{ij} and β_{ij} do not depend on the parameter s. For β_{ij}, we have

$$\beta_{ij} = (-1)^i 2^{-12m-4+6i} \cdot \frac{3m+1-j}{i} \binom{3m+i-j}{3m+1-i-j} \quad (j > 0), \tag{4}$$

which is proved in [11]. That the α_{ij} do not depend on s can be seen similarly as for β_{ij} using the Bürmann-Lagrange Theorem (see for instance [11]).

Furthermore, we know that

$$\begin{aligned} &a_0^{(s)} = 1,\ a_j^{(s)} = 0 \text{ for } j = 1, \ldots, 2m+1 \quad (\text{since } C \text{ is extremal}), \\ &b_j^{(s)} = 0 \text{ for } j = 0, \ldots, s-1 \quad (\text{since } 4s \text{ is the minimum weight of } S). \end{aligned}$$

This implies immediately $c_i^{(s)} = \alpha_{i,0}$ for $i = 1, 2, \ldots, 2m+1$. For the coefficient $c_{2m+2}^{(s)}$ we obtain the equation

$$c_{2m+2}^{(s)} = \alpha_{2m+2,0} + \alpha_{2m+2,2m+2} a_{2m+2}^{(s)} = \sum_{j=0}^{m-1} \beta_{2m+2,j} b_j^{(s)}. \tag{5}$$

The formula (4) yields

$$\beta_{2m+2,j} = 2^8 \cdot \frac{3m+1-j}{2m+2} \binom{5m+2-j}{m-1-j}. \tag{6}$$

Hence $\beta_{2m+2,j} > 0$ for $j = 1, 2, \ldots, m-1$ and therefore, by (5), $c_{2m+2}^{(s)} \geq 0$ since $b_j^{(s)} \geq 0$. Moreover, $c_{2m+2}^{(s)} = 0$ if and only if $b_1^{(s)} = \cdots = b_{m-1}^{(s)} = 0$. By Lemma 3, we get $4s \leq 4m$ since $d = 4m+4$, and in case $s = m$ the code C is s-extremal. This shows that $c_{2m+2}^{(s)} = 0$ if and only if C is s-extremal. In that case we have

$$a_{2m+2}^{(m)} = -\frac{\alpha_{2m+2,0}}{\alpha_{2m+2,2m+2}}. \tag{7}$$

Now, by (5), we obtain

$$a_{2m+2}^{(s)} = \frac{c_{2m+2}^{(s)} - \alpha_{2m+2,0}}{\alpha_{2m+2,2m+2}} = \frac{c_{2m+2}^{(s)}}{\alpha_{2m+2,2m+2}} + a_{2m+2}^{(m)}. \tag{8}$$

Thus, to prove Theorem 5, we only have to show that

$$a_{2m+2}^{(s)} > a_{2m+2}^{(m)} \quad \text{for } 1 \le s \le m-1.$$

This is obviously equivalent to proving that $\alpha_{2m+2,2m+2} > 0$ since $c_{2m+2}^{(s)} > 0$ for $s < m$.

By [11], we have

$$\begin{aligned} \alpha_{i,0} &= -\frac{n}{2i}\left[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-n/2-1+4i}(1-y)^{-2i}\right] \\ &= -\frac{12m+4}{i}\left[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-12m-5+4i}(1-y)^{-2i}\right]. \end{aligned}$$

For $i = 2m+2$ we compute

$$\begin{aligned} \alpha_{2m+2,0} &= -\frac{12m+4}{2m+2}\left[\text{coeff. of } y^{2m+1} \text{ in } (1+y)^{-12m-5+8m+8}(1-y)^{-4m-4}\right] \\ &= -\frac{6m+2}{m+1}\left[\text{coeff. of } y^{2m+1} \text{ in } (1+y)^{-4m+3}(1-y)^{-4m-4}\right] \\ &= -\frac{6m+2}{m+1}\left[\text{coeff. of } y^{2m+1} \text{ in } (1+y)^{7}(1-y^2)^{-4m-4}\right] < 0 \end{aligned}$$

since $[\ldots] > 0$ because of $(1-y^2)^{-1} = 1 + y^2 + y^4 + \ldots$.

Since $a_{2m+2}^{(m)} \ge 0$ we obtain from (7) that $\alpha_{2m+2,2m+2} > 0$ which completes the proof of Theorem 5.

Remark 1 We would like to mention that we do not have $a_{2m+2}^{(s-1)} \ge a_{2m+2}^{(s)}$ in general. In particular it may happen that $a_{2m+2}^{(1)} < a_{2m+2}^{(s)}$ for some $s > 1$.

Remark 2 The statement in Theorem 5 holds also true if $n = 24m + 16$.

7 Type I codes with minimal shadow vs type II codes

The aim of this section is to show

Theorem 6 *Extremal self-dual codes of type I with minimal shadow and of length $n = 24m+8$ perform better than extremal self-dual codes of type II and of the same length n. In particular, according to the last section, s-extremal codes perform better than extremal self-dual codes of type II.*

Keeping the notation of the previous section we consider an extremal code C of type I with minimal shadow S and of length $n = 24m + 8$. As mentioned earlier C contains exactly one vector, say v, of weight $4 = 4s$, i.e., $s = 1$. Suppose that S contains another vector w with $\mathrm{wt}(w) = i$ for some $i \in \{8, 12, \ldots, 4m - 4\}$. Since the sum of two vectors in S is a codeword in C [4] we have $v + w \in C$ with $0 \neq \mathrm{wt}(v + w) \leq 4m$, a contradiction to the assumption that C is extremal, i.e. $d = 4m + 4$. This shows that

$$b_1^{(1)} = 1, b_2^{(1)} = \cdots = b_{m-1}^{(1)} = 0.$$

Rewriting equation (5) we get

$$c_{2m+2}^{(1)} = \alpha_{2m+2,0} + \alpha_{2m+2,2m+2} a_{2m+2}^{(1)} = \beta_{2m+2,1}.$$

Using equations (8) and (7) we see that

$$\begin{aligned} a_{2m+2}^{(1)} &= \frac{c_{2m+2}^{(1)} - \alpha_{2m+2,0}}{\alpha_{2m+2,2m+2}} = \frac{\beta_{2m+2,1}}{\alpha_{2m+2,2m+2}} + a_{2m+2}^{(m)} \\ &= -\frac{\beta_{2m+2,1}}{\alpha_{2m+2,0}} a_{2m+2}^{(m)} + a_{2m+2}^{(m)} = a_{2m+2}^{(m)} \left(1 - \frac{\beta_{2m+2,1}}{\alpha_{2m+2,0}}\right). \end{aligned} \tag{9}$$

Observe that all terms at the right hand side are computable as follows:

Clearly, $a_{2m+2}^{(m)}$ is the number of minimal weight vectors of an s-extremal code which is known. More presicely, by [1], we have

$$a_{2m+2}^{(m)} = \frac{n}{d} \sum_{\substack{j,k \in \mathbb{N} \\ j+k = \frac{d}{2} - 1}} (-1)^j \binom{\frac{n}{2} - 2d + j}{j} \binom{d + k - 1}{k}.$$

Furthermore, by (6),

$$\beta_{2m+2,1} = 2^8 \cdot \frac{3m}{2m+2} \binom{5m+1}{m-2}.$$

Finally, for $\alpha_{2m+2,0}$, in the previous section we found the expression

$$\alpha_{2m+2,0} = -\frac{6m+2}{m+1} \left[\text{coeff. of } y^{2m+1} \text{ in } (1+y)^7 (1-y^2)^{-4m-4}\right]$$

which turns out to be

$$\alpha_{2m+2,0} = -\frac{6m+2}{m+1} \left[7\binom{5m+3}{m} + \binom{7}{3}\binom{5m+2}{m-1} + \binom{7}{5}\binom{5m+1}{m-2} + \binom{5m}{m-3}\right].$$

Thus $a_{2m+2}^{(1)}$ can be computed explicitely.

Let C' be an extremal self-dual code of length $n = 24m + 8$ of type II with a'_{m+1} codewords of weight $4m + 4$. By [9], we have

$$a'_{m+1} = \frac{1}{4}n(n-1)(n-2)(n-4)\frac{(5m)!}{m!(4m+4)!}.$$

Furthermore, by [13], we know that $m < 159$. Using a computer one easily shows that

$$a^{(1)}_{2m+2} < a'_{m+1}$$

for $m = 1, 2, \ldots, 158$. Thus we may conclude that in case $n = 24m + 8$ extremal self-dual codes of type I with minimal shadow always perform better then extremal self-dual codes of type II.

Remark 3 For $n = 24m + 16$ extremal self-dual codes of type I with minimal shadow do in general not perform better than extremal self-dual type II codes, but s-extremal still do.

References

[1] C. Bachoc and P. Gaborit, Designs and self-dual codes with long shadows, *J. Combin. Theory A* **105** (2004), 15-34.

[2] S. Bouyuklieva and V. Yorgov, Singly-even codes of length 40, *Des. Codes Crypt.* **9** (1996), 131-141.

[3] Y. Cheng and N.J.A. Sloane, Codes from symmetry groups, and a $[32, 17, 8]$ code, *SIAM, J. Discrete Math.* **2** (1989), 28-37.

[4] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1991), 1319-1333.

[5] R. Doncheva and M. Harada, Some extremal self-dual codes with an automorphism of order 7, *Appl. Algebra Eng. Comm. Comp.* **14** (2003, 75-79.

[6] A. Faldum, J. Lafuente, G. Ochoa and W. Willems, *Error probabilities for bounded distance decoding*, **40** (2006), 237-252.

[7] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in *Actes Congrès Internat. Math.* **3** (1970), 211-215.

[8] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North Holland, Amsterdam 1977.

[9] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. and Control* **22** (1973), 188-200.

[10] E.M. Rains and N.J.A. Sloane, Self-dual codes, in Handbook of Coding Theory, V.S. Pless and W.C. Huffman, Eds., Elsevier, Amsterdam, 1998, 177-294.

[11] E.M. Rains, Shadow bounds for self-dual-codes, *IEEE Trans. Inform. Theory* **44** (1998), 134-139.

[12] V. Yorgov, On the minimal weight of some singly-even codes, *IEEE Trans. Inform. Theory* **45** (1999), 2539-2541.

[13] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.* **91** (1999), 277-286.