Designs and self-dual codes with long shadows

Christine Bachoc *and Philippe Gaborit †

Abstract

In this extended abstract we introduce the notion of s-extremal codes for self-dual binary codes and we relate this notion to the existence of 1-designs or 2-designs in these codes. We extend the classification of codes with long shadows of [13] to codes with minimum distance 6, for which we give partial classification. Complete proofs of these results and more can be found in [3].

1 Introduction

One important parameter of binary codes is their minimum weight d. In the case of singly-even self-dual codes, only unsatisfactory bounds were known until the notion of the shadow was introduced by Conway and Sloane in [10]. Let C be a singly-even self-dual code and C_0 its doubly-even subcode, then the shadow S of C is defined as $S := {C_0}^{\perp} \setminus C$. One uses the additional information contained in the weight enumerator of S, which is obtained by a linear transformation of the one of C. The best achievement of this idea is the result by Rains [26] extending the well known bound of Type II codes to Type I codes.

On the other hand, Elkies has studied in [13] the minimum weight (respectively the minimum norm) of the shadow of self-dual codes (respectively of unimodular lattices), especially in the cases where it attains a high value. In the case of codes, let s denote the minimum weight of S, then $s \equiv \frac{n}{2} \pmod 4$; Elkies shows that $s \leq \frac{n}{2}$ and that $s = \frac{n}{2}$ if and only if C is the direct sum of $\frac{n}{2}$ $[2, 1, 2]$ binary self-dual codes. He also classifies the self-dual codes such that $s = \frac{n}{2} - 4$, and shows in particular that their length cannot exceed 22.

In this paper, we propose to study the parameters d and s simultaneously. We prove that $2d + s \leq \frac{n}{2} + 4$, except in the case where $n \equiv 22 \pmod{24}$ where $2d + s \leq \frac{n}{2} + 8$, and we call s-extremal the codes for which equality holds. We prove the existence of 1-designs and sometimes 2-designs in s-extremal codes. The cases considered by Elkies correspond to s-extremal codes with $d = 2$ and $d = 4$. We study s-extremal codes for $d = 6$ and we show in particular that such codes can only exist for lengths $22 \leq n \leq 44$, that there is a unique such code for lengths $40, 42$ and 44 and we provide partial classification for the other lengths. (Note that analogous results for lattices can be found in [5]). We also construct an isodual $[42, 21, 8]$ code with covering radius 6 related to a particular s-extremal code. The paper is organized as follows : in sections 2 and 3 we define the notion of s-extremal codes and we prove the existence of 1-designs and sometimes 2-designs in these codes. In sections 4 and 5 we consider the case of s-extremal codes with $s = \frac{n}{2} - 8$, we show that their length n satisfies

*Laboratoire A2X, Université Bordeaux I, 351, cours de la Libération, 33405 Talence France, **Email:** bachoc@math.u-bordeaux.fr

†LACO, Université de Limoges, 123, av A. Thomas, 87000 Limoges, France, **Email:** gaborit@unilim.fr

$22 \leq n \leq 44$, and give partial classification results. At last in section 6 we give examples of s-extremal codes.

2 s-extremal codes

Let C be a self-dual binary code, which is assumed not to be doubly even and let S be its shadow. We denote W_C and W_S the weight enumerators of C and S. From [10], there exists $c_0, \ldots, c_{[n/8]} \in \mathbb{R}$ such that:

$$\begin{cases} W_C(x,y) & = \sum_{i=0}^{[n/8]} c_i (x^2+y^2)^{\frac{n}{2}-4i} \{x^2y^2(x^2-y^2)^2\}^i \\ W_S(x,y) & = \sum_{i=0}^{[n/8]} c_i (-1)^i 2^{\frac{n}{2}-6i} (xy)^{\frac{n}{2}-4i} (x^4-y^4)^{2i} \end{cases} \quad (1)$$

We denote d the minimum weight of C and s the minimum weight of its shadow. This section is devoted to the proof of the following theorem:

Theorem 2.1 *Let C be a self-dual binary code, assumed not to be doubly even, of minimum weight d, and let S be its shadow, of minimum weight s. Then, $2d+s \leq 4+\frac{n}{2}$, unless $n \equiv 22 \mod 24$ and $d = 4[n/24]+6$, in which case $2d+s = 8+\frac{n}{2}$.*

Definition 2.2 *A code which parameters (d,s) satisfy equality in the previous bounds is said to be s-extremal. In that case, the polynomials W_C and W_S are uniquely determined.*

Examples: The s-extremal codes with $d = 4$ correspond to the codes with long shadows which have been classified in [13]. For $d = 6$, the unique binary self-dual $[26, 13, 6]$ code and the two binary self-dual $[28, 14, 6]$, from the classification of self-dual codes [9] are examples of s-extremal codes. The exceptionnal case in the theorem is the case of extremal codes (in the sense of [26]) of length $n \equiv 22 \mod 24$, obtained by shortening of doubly even extremal ones of length a multiple of 24.

3 Designs in s-extremal codes

In this section, we study the designs contained in the set of words of fixed weight in an s-extremal code and in its shadow. Therefore, we make use of the *harmonic weight enumerators* $W_{C,f}$ introduced in [2]. We recall that, if f is harmonic of degree k, and if C is self-dual, the polynomial $W_{C,f}$ is divisible by $(xy)^k$, and, if $Z_{C,f} := (xy)^{-k} W_{C,f}$, one has: if $k \equiv 0 \mod 2$, $Z_{C,f} \in \mathbb{C}[x^2+y^2, x^2y^2(x^2-y^2)^2]$ (respectively if $k \equiv 1 \mod 2$, $Z_{C,f} \in Q_8 \mathbb{C}[x^2+y^2, x^2y^2(x^2-y^2)^2]$, where $Q_8 = xy(x^6-7x^4y^2+7x^2y^4-y^6)$).

Theorem 3.1 *Let C be an s-extremal code. Let C_i, respectively S_i denote the set of words of weight i in C, respectively S.*

1. *For all i, C_i and S_i hold a 1-design.*
2. *If $d = \frac{n+8}{6}$, for all $i \equiv d+2 \mod 4$, C_i holds a 2-design.*
3. *If $d = \frac{n+8}{6}$, and $d \equiv 2 \mod 4$, for all i, $C_i \cup S_i$ holds a 2-design.*

Remark 3.2 *In the exceptionnal case of the extremal codes of length $n \equiv 22 \mod 24$, the sets C_i and S_i hold 3-designs (see [21]).*

4 Codes with long shadows

In [13], the codes with shadows of minimum weight equal to $n/2$ and $n/2-4$ are classified. In this section, we consider the case of weight $n/2-8$. Such codes are s-extremal if their minimum weight equals 6. The corresponding problem for lattices is handled in [22]. We prove here the following theorem:

Theorem 4.1 *Let C be a s-extremal code of length n and distance $d=6$. Then $22 \leq n \leq 44$.*

In the following, we freely identify a word x of F_2^n and its support, and we denote by $\bar{x}$ the complement of x over F_2^n.

From now on, we assume that C is a code of length n, distance $d=6$ and of shadow S with minimum weight $s=n/2-8$. A direct computation from the coefficients of W_S and W_C leads to: $c_1=-n/2$, $c_2=n(n-22)/8$,

$$\begin{aligned} W_S =& 2^{n/2-15}n(n-22)x^{n/2+8}y^{n/2-8}+2^{n/2-13}n(86-n)x^{n/2+4}y^{n/2-4} \\ &+2^{n/2-14}(3n^2-322n+2^{14})x^{n/2}y^{n/2}, \end{aligned}$$

and

$$a_6=n(n^2-66n+1136)/48,$$

$$a_8=n(n^3-92n^2+2684n-23248)/128.$$

Remark 4.2 *The expression of W_S shows already that $n \leq 86$. On the other hand, the bound announced in the theorem $n \leq 44$ is optimal since the code of lenth 44 which is the direct sum of two copies of the $[22,11,6]$ is s-extremal.*

For any $y \in \mathbb{F}_2^n$, let

$$N_{i,j}(y) := \{x : x \in C_i \mid |x \cap y| = j\}$$

and

$$n_{i,j}(y) := |N_{i,j}(y)|.$$

Since the sets C_i are 1-designs, the numbers $n_{i,j}(y)$ satisfy a linear equation (see Theorem 3 of [21]):

$$\sum_j j n_{i,j}(y) = \frac{i a_i wt(y)}{n}. \tag{2}$$

Let y be a word of C_6. Then, for all $x \in C_6$, $|x \cap y| = 0, 2$, and Equation (2) leads to

$$m_2 := n_{6,2}(y) = 3(n^2-66n+1128)/8.$$

For all $x \in C_8$, $|x \cap y| = 0, 2, 4$; moreover, $|x \cap y| = 4$ if and only if $|(x+y) \cap y| = 2$, so $n_{8,4}(y) = n_{6,2}(y) = m_2$. With Equation (2) we can also calculate $n_{8,2}(y)$:

$$n_{8,2}(y) = 3(n^3 - 96n^2 + 2948n + 27760)/16.$$

Now we assume that $wt(y) = 8$. Again, for $x \in C_6$, we have $|x \cap y| = 0, 2, 4$; but (2) is not enough to calculate the values of $n_{6,j}(y)$. From now on, we set $N_j(y) := N_{6,j}(y)$ and $n_j(y) := n_{6,j}(y)$. Counting in two ways the number of elements of the set

$$\{(x, y) : x \in C_6, y \in C_8 \mid |x \cap y| = 4\}$$

leads to the calculation of the *mean value* mv of $n_4(y)$:

$$mv = \frac{1}{a_8} \sum_{y \in C_8} n_4(y) = \frac{a_6}{a_8} m_2 = \frac{(n^2 - 66n + 1136)(n^2 - 66n + 1128)}{n^3 - 92n^2 + 2684n - 23248}. \tag{3}$$

One notices that, if $x \in N_4(y)$, also $x + y \in N_4(y)$, so $n_4(y)$ is even of size say $2k$ with:

$$N_4(y) = \{x_1, \cdots, x_k\} \cup \{y + x_1, \cdots, y + x_k\}.$$

In order to prove the theorem, we first prove two lemmas.

Lemma 4.3 *Let x_i and x_j be elements of $N_4(y)$ with $i \neq j$ then x_i and x_j do not intersect on $\bar{y}$.*

Lemma 4.4 *The set $N_4(y)$ is, up to a permutation of the coordinates, contained in the set $S_4 = \{t_1, \ldots, t_7\} \cup \{t_1 + y, \ldots, t_7 + y\}$:*

y	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
t_1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
t_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0
t_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0
t_4	1	0	1	0	1	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0
t_5	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0
t_6	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0
t_7	1	0	0	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	1	1

In particular, $n_4(y) \leq 14$. Moreover, if $n_4(y) = 10, 12$ or 14, the set $N_4(y)$ is unique up to a permutation of the coordinates leaving y invariant.

We now prove the theorem:

Proof of theorem 4.1: First, by the classification of self-dual codes, we have $n \geq 22$ because $d \geq 6$. Suppose $n \geq 46$. Then, $a_8 > 0$, so let $y \in C_8$. Then, from lemma 4.4, $n_4(y) \leq 14$, which gives $mv \leq 14$. But, from (3),

$$mv - 14 = \frac{(n - 22)(n - 44)(n^2 - 80n + 1660)}{(n^3 - 92n^2 + 2684n - 23248)}$$

is strictly positive for $n \geq 46$, a contradiction.

□

n	mv	n	mv
22	14	34	2
24	7.68	36	3.36
26	4.40	38	6
28	2.67	40	9.26
30	1.82	42	12
32	1.60	44	14

Table 1: The value of mv for $d = 6$

5 Classification results

We now prove some results on the classification of the s-extremal codes of distance $d = 6$; we assume that the length n is at least equal to 34. We introduce a few more definitions:

Definition 5.1 *Let C be an s-extremal code of minimum distance 6. Let n_4^{max} denote the maximal value of $n_4(y)$ when y runs over the set of codewords of weight 8, and let $N_4^{max} := \{y : y \in C_8 \mid n_4(y) = n_4^{max}\}$.*

We have already seen (Lemma 4.4) that $n_4^{max} \leq 14$. It turns out that a high value of this number is a strong constraint on the code. We shall completely classify the codes with $n_4^{max} = 10, 12, 14$.

Theorem 5.2

- *Assume $n_4^{max} = 14$. Then, $n = 36, 38, 44$, and in each case there is a unique code up to equivalence. In the case $n = 44$, it is the orthogonal sum of two copies of the shorter Golay code with parameters $[22, 11, 6]$.*
- *Assume $n_4^{max} = 12$. Then, $n = 34, 36, 40, 42$, and in each case there is a unique code up to equivalence.*
- *Assume $n_4^{max} = 10$. Then, $n = 34, 36, 38$, there are up to equivalence 3 codes of length 34, and a unique code of length respectively 36 and 38.*

Before giving a proof of this theorem, we derive from it a classification of the s-extremal codes of minimum weight 6, for the lengths 40, 42, 44.

Corollary 5.3 *There is up to equivalence a unique s-extremal code of minimum weight 6 at length 44, respectively 42 and 40.*

□

We give in Table 1 the value of mv computed from (3) for $d = 6$ and $22 \leq n \leq 44$.

If the length of C equals 40, 42, 44, we have $n_4^{max} \geq 10$. Hence Theorem 5.2 exhausts all the possibilities. □

For $C = C_0 \cup C_2$ and $S = C_1 \cup C_3$, the neighbors of C are defined as $C_0 \cup C_1$ and $C_0 \cup C_3$.

Remark 5.4 *In [18], the authors point out a doubly-even $[40, 20, 8]$ code with covering radius 7, which turns out to be equivalent to the two equivalent doubly-even neighbors of the unique*

s-extremal $[40,20,6]$ *code. The neighbor of a self-dual Analogously, the s-extremal* $[34,17,6]$ *codes for* $n_4^{max} = 10, 12$*, have each, two equivalent isodual* $[34,17,8]$ *neighbors with covering radius* 6*; the s-extremal* $[36,18,6]$ *code for* $n_4^{max} = 14$ *has two equivalent self-dual* $[36,18,8]$ *neighbors with covering radius* 6*; the two s-extremal* $[38,19,6]$ *codes for* $n_4^{max} = 12, 14$ *have each two equivalent isodual* $[38,19,8]$ *neighbors with covering radius* 7*; the s-extremal* $[42,21,6]$ *code for* $n_4^{max} = 10$ *has two equivalent isodual* $[42,21,8]$ *neighbors with covering radius* 6 *and the unique s-extremal* $[44,22,6]$ *code has two equivalent self-dual* $[44,22,8]$ *neighbors with covering radius* 7*.*

Remark 5.5 *The unique* $[40,20,6]$ *code also leads to a* 40*-dimensional unimodular lattice of norm* 3 *with a long shadow in the sense of [22]. The construction is the standard Construction A followed by a neighboring procedure using the all-one vector*

6 Number and examples of s-extremal codes

We now consider examples of s-extremal codes. The s-extremal codes with $d = 4$ have been classified in [13]. We now list the known s-extremal codes corresponding to a given d. First note that from Theorem 3.1 the unique singly-even $[16,8,4]$ holds 2-designs.

- $d = 6$

For this minimum distance, from section 4 codes are known to exist for length $22 \leq n \leq 44$. The two codes of length 28 hold 2-designs. Existing codes are given in the following table :

n	num	ref	n	num	ref
22	1	[24]	34	≥ 2	[10],§5
24	1	[25]	36	≥ 3	§5
26	1	[9]	38	≥ 2	§5
28	2	[9]	40	1	§5
30	9	[9]	42	1	§5
32	19	[5]	44	1	§5

- $d = 8$

In that case it is not known for up to which length s-extremal codes do exist. The codes of length 40 hold 2-designs. We list known codes for $d = 8$:

n	num	ref
32	3	[10]
36	≥ 3	[20],[16]
38	≥ 8	[20],[16]
40	≥ 4	[10],[7]
42	≥ 17	[10],[8]
44	≥ 1	[10]

- $d = 10$

The codes of length 52 hold 2-designs, the cod $sub(XQ_{47})$ is the code obtained by subtractio of the (11) trivial code from the extended quadratic residu code of length 47. Codes are only known for the following lengths :

n	num	ref
46	≥ 1	$sub(XQ_{47})$
50	≥ 1	[10]
52	≥ 460	[19]
54	≥ 166	[27], §3
58	≥ 1	[10]

- $d = 12$

In that case it is not known whether a s-extremal $[64, 32, 12]$ code exists, such a code would hold 2-designs. For length 68, although many codes are known, none of them is s-extremal. The only known codes are :

n	num	ref
60	≥ 3	[28],[12]
62	≥ 8	[12]
66	≥ 2	[10],[17]

- $d \geq 14$

For $d = 14$, two codes are known for length 76 ([15],[1]), which contain 2-designs, and more than 50 codes are known for length 78 from [14] and [1]. For $d = 16$ only one s-extremal code is known for length 86 from [11] and for $d = 18$ one code is obtained for length 102 from the extended quadratic residue code of length 104.

References

[1] A. Baartmans and V. Yorgov, Some new extremal codes of length 76 and 78, *Proc. 7th Int. Workshop Alg. and Combin. Coding Theory, 18-24 June, Bulgaria*, (2000), 51-54.

[2] C. Bachoc, On Harmonic weight enumerators of binary codes, *Designs, Codes and Cryptography*, **18** (1999), 11-28.

[3] C. Bachoc and P. Gaborit, "Designs and self-dual codes with long shadows", submitted to JCT(A).

[4] R. A. Brualdi and V. S. Pless, Weight Enumerators of Self-Dual Codes, *IEEE Trans. Inf. Th.*, **37** (1991), 1222-1225.

[5] R. T. Bilous and G. H. J. van Rees, An enumeration of self-dual codes of length 32, preprint.

[6] W. Bosma and J. Cannon, "Handbook of Magma Functions", Sydney, 1995.

[7] S. Buyuklieva and V. Yorgov, Singly-Even self-dual codes of length 40, *Des. Codes Cryptog.*, **9**, (1996) , vol 9, 131-141.

[8] S. Buyuklieva, New extremal self-dual codes of length 42 and 44, *IEEE Trans. Inf. Th.*, **43** (1997), 1607-1612.

[9] J.H. Conway and V. S. Pless, On the enumeration of self-dual codes, *J. Combin. Theory Ser. A* **28** (1980), 26-53.

[10] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inf. Th.*, **36** (1990), 1319-1333.

[11] S.T. Dougherty, T. A. Gulliver and M. Harada, Extremal binary self-dual codes, *IEEE Trans. Inform. Theory*, **43**, (1997), 2036-2047.

[12] R. Dontcheva and M. Harada, New Extremal Self-Dual Codes of Length 62 and related Extremal Self-Dual Codes, preprint.

[13] N. Elkies, Lattices and codes with long shadows, *Math. Res. Lett.*, **2** (1995) no. 5, 643-651.

[14] T. A. Gulliver, M. Harada and J-L. Kim, Construction of new extremal self-dual codes, *preprint*.

[15] P. Gaborit and A. Otmani, Experimental constructions of self-dual codes, preprint.

[16] M. Harada, New extremal self-dual codes of lengths 36 and 38, *IEEE Trans. Inform. Theory*, **45**, (1999), 2541-2543.

[17] M. Harada, Classification of extremal double circulant codes of lengths 64 to 72, *Des. Codes Cryptog.*, **13**, (1998) , n.3, 257-269.

[18] M. Harada, A. Munemasa and K. Tanabe, Extremal self-dual [40,20,8] codes with covering radius 7, preprint

[19] W.C. Huffman and V.D. Tonchev, The [52,26,10] binary self-dual codes with an automorphism of order 7, *Finite Fields Appl.*, **7**, (2001), 341-349.

[20] J.-L. Kim, New extremal self-dual codes of lengths 36,38 and 58, *IEEE Trans. Inform. Theory*, **47**, (2001), n.4, 1575-1580.

[21] M. Lalaude-Labayle, On binary linear codes supporting t-designs, *IEEE Trans. Inf. Th.*, **47**, (2001),n. 6, 2249-2255.

[22] G. Nebe and B. Venkov, Unimodular lattices with long shadow, to appear.

[23] V. Pless, "Introduction to the Theory of Error Correcting Codes", Wiley, New York, 3$^{\rm rd}$ edition, 1998.

[24] V. Pless, A classification of self-orthogonal codes over $GF(2)$, *Discrete Math.* **3** (1972), 209-246.

[25] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, *J. Combin. Theory Ser. A* **A18** (1975), 313-335.

[26] E. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Inf. Th.* ,**44**(1) (1998), 134-139.

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

[28] H.-P. Tsai and Y.J. Yiang, Some new extremal self-dual [58,29,10] codes, *IEEE Trans. Inf. Th.*, **44**, (1998), 813-814.