Available online at www.sciencedirect.com
SCIENCE DIRECT®

ELSEVIER Journal of Combinatorial Theory, Series A 105 (2004) 15–34

Journal of Combinatorial Theory Series A

http://www.elsevier.com/locate/jcta

Designs and self-dual codes with long shadows

Christine Bachoc[a] and Philippe Gaborit[b,*]

[a] *Laboratoire A2X, Université Bordeaux I, 351, Cours de la Libération, 33405 Talence, France*
[b] *LACO, Université de Limoges, 123, av A. Thomas, 87000 Limoges, France*

Received 5 November 2002

Communicated by Vera Pless

Abstract

In this paper 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 Elkies (Math. Res. Lett. 2(5) (1995) 643) to codes with minimum distance 6, for which we give partial classification.

Keywords: Self-dual codes; Designs; Classification; Shadow

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 [9]. 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 $S := C_0^\perp \backslash C$. 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 [25] extending the well-known bound for the minimum weight of Type II codes to Type I codes.

On the other hand, Elkies has studied in [12] 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

*Corresponding author.
E-mail addresses: bachoc@math.u-bordeaux.fr (C. Bachoc), gaborit@unilim.fr (P. Gaborit).

0097-3165/$ - see front matter
doi:10.1016/j.jcta.2003.09.003

denote the minimum weight of S, then $s \equiv \frac{n}{2} (\mathrm{mod}\, 4)$; Elkies shows that $s \leqslant \frac{n}{2}$ and that $s = \frac{n}{2}$ if and only if C is the direct sum of $\frac{n}{2}$ elementary $[2, 1, 2]$ 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 $2d + s \leqslant \frac{n}{2} + 4$, except in the case $n \equiv 22 (\mathrm{mod}\, 24)$ and $d = 4[n/24] + 6$, where $2d + s = \frac{n}{2} + 8$. We call s-extremal the codes for which $2d + s$ attains the highest possible value, according to these bounds. 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 $22 \leqslant n \leqslant 44$, 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 [21].) 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 $22 \leqslant n \leqslant 44$, and give partial classification results. At last in Sections 6 and 7 we give examples of s-extremal codes and list the codes we used for the classification. Appendices A and B give generator matrices of the codes we found. Throughout the paper, we follow the notations of [26]. All the computations were done with MAGMA [4].

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 [9], there exists $c_0, \ldots, c_{[n/8]} \in \mathbb{R}$ such that

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

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, $2d + s \leqslant \frac{n}{2} + 4$, unless $n \equiv 22 \bmod 24$ and $d = 4[n/24] + 6$, in which case $2d + s = \frac{n}{2} + 8$.*

Definition 2.2. A code which parameters (d, s) satisfy $2d + s = \frac{n}{2} + 4$ or $2d + s = \frac{n}{2} + 8$ is said to be s-extremal. In that case, the polynomials W_C and W_S are uniquely determined.

Remark 2.3. According to Theorem 2.1, the case $2d + s = \frac{n}{2} + 8$ happens if and only if $n \equiv 22 \bmod 24$ and $d = 4[n/24] + 6$. It corresponds to the case of extremal codes (in the sense of [25]) of length $n \equiv 22 \bmod 24$, obtained by shortening of doubly even extremal ones of length congruent to 0 modulo 24.

Examples. The s-extremal codes with $d = 4$ correspond to the codes with long shadows which have been classified in [12]. For $d = 6$, the unique binary self-dual $[26, 13, 6]$ code and the two binary self-dual $[28, 14, 6]$ codes, from the classification of self-dual codes [8] are examples of s-extremal codes. The following lemma provides other examples of s-extremal codes.

Lemma 2.4. *If C is a $[24\mu + 8, 12\mu + 4, 4\mu + 4]$ extremal Type II code then the code obtained by subtraction of the code* (11) *from C is s-extremal.*

Proof. By subtraction of (11) from C one obtains a singly even $[24\mu + 6, 12\mu + 3, d]$ code C' with $d \geqslant 4\mu + 2$ such that using notation of [5]:

$$C = \{0, 0, C'_0\} \cup \{1, 1, C'_2\} \cup \{1, 0, C'_1\} \cup \{0, 1, C'_3\},$$

with $S = C'_1 \cup C'_3$ the shadow of $C' = C'_0 \cup C'_2$. Hence the minimum weight s of S has to be greater than $4\mu + 3$. Therefore C' is s-extremal since $2d + s \geqslant 12\mu + 7 = \frac{n}{2} + 4$. $\square$

More examples of known s-extremal codes will be given in Section 7.

Proof. From (1), the weights in S are congruent to $\frac{n}{2} \bmod 4$, and the weights in C are congruent to $0 \bmod 2$. Let us denote a_i the number of codewords of weight i and b_i the number of words of weight i in S. Let us define s' by $s = \frac{n}{2} - 4s'$. From (1), the conditions

$$\begin{cases} a_0 = 1, \\ a_{2i} = 0 \text{ for } 1 \leqslant i \leqslant \frac{d}{2} - 1, \\ b_{\frac{n}{2} - 4j} = 0 \text{ for } s' + 1 \leqslant j \leqslant [n/8] \end{cases} \tag{2}$$

are linear and independent conditions on the $[n/8] + 1$ coefficients c_i. Their number is $\frac{d}{2} + [n/8] - s'$, which is greater or equal to $[n/8] + 1$ if and only if $2d + s \geqslant 4 + \frac{n}{2}$.

We now assume that the inequality $2d + s \geqslant 4 + \frac{n}{2}$ holds. From the previous discussion, the weight enumerators of C and S are uniquely determined. Bürman–Lagrange formula allows us to calculate the coefficients of these polynomials. Let $t := 4 + \frac{n}{2} - 2d$. We have

$$\begin{cases} W_C(x, y) = 1 + a_d x^{n-d} y^d + a_{d+2} x^{n-d-2} y^{d+2} + \cdots \\ W_S(x, y) = b_t x^{n-t} y^t + b_{t+4} x^{n-t-4} y^{t+4} + \cdots, \end{cases} \tag{3}$$

where b_t is not assumed to be non-zero. The following lemma discusses this possibility and concludes the proof of the theorem.

Lemma 2.5. *With the previous notations and assumptions, we have*

$$a_d = \frac{n}{d} \sum_{\substack{j,k \in \mathbb{N} \\ j+k=\frac{d}{2}-1}} (-1)^j \binom{\frac{n}{2}-2d+j}{j} \binom{d+k-1}{k}, \tag{4}$$

$$b_t = (-1)^{\frac{d}{2}} \frac{n 2^{\frac{n}{2}-3d+6}}{d-2} \sum_{\substack{j,k \in \mathbb{N} \\ j+k=\frac{d}{2}-2}} (-1)^j \binom{\frac{n}{2}-2d+4+j}{j} \binom{d+k-3}{k}. \tag{5}$$

Moreover, the coefficient b_t is positive, unless $n \equiv 22 \bmod 24$ and $d = 4[n/24]+6$, in which case b_t equals 0 and the coefficient b_{t+4} is positive.

Proof. We have in (1) $c_i = 0$ for all $i > \frac{d}{2}-1$. Setting $x = 1$ and dividing by $(1+y^2)^{\frac{n}{2}}$ the first equation of (1) leads to

$$\sum_{i=0}^{\frac{d}{2}-1} c_i \left\{ \frac{y(1-y^2)}{(1+y^2)^2} \right\}^{2i} = \frac{1}{(1+y^2)^{\frac{n}{2}}} + \frac{1}{(1+y^2)^{\frac{n}{2}}} \{a_d y^d + \cdots\}.$$

Let $g(y) := \frac{y(1-y^2)}{(1+y^2)^2}$. From this last expression, we see that $c_0, c_1, \ldots, c_{\frac{d}{2}-1}, -a_d$ are the first coefficients of the development of $\frac{1}{(1+y^2)^{\frac{n}{2}}}$ as a series in $g(y)$. From the Bürman–Lagrange formula, we obtain

$$-a_d = \frac{1}{d!} \frac{\partial^{d-1}}{\partial y^{d-1}} \left(\frac{\partial}{\partial y} \left(\frac{1}{(1+y^2)^{\frac{n}{2}}} \right) \left(\frac{(1+y^2)^2}{1-y^2} \right)^d \right)_{y=0}$$

which, after simplification, becomes

$$a_d = \frac{n}{d} \left\{ \text{coeff. of } y^{d-2} \text{ in} : \frac{1}{(1+y^2)^{\frac{n}{2}-2d+1}(1-y^2)^d} \right\}$$

and, finally, leads to the announced formula.

From (3), we have $b_t = (-1)^{\frac{d}{2}-1} 2^{\frac{n}{2}-3d+6} c_{\frac{d}{2}-1}$, and a similar calculation leads to

$$c_{\frac{d}{2}-1} = \frac{-n}{d-2} \left\{ \text{coeff. of } y^{d-4} \text{ in} : \frac{1}{(1+y^2)^{\frac{n}{2}-2d+5}(1-y^2)^{d-2}} \right\}.$$

We have obviously

$$c_{\frac{d}{2}-1} = \frac{-n}{d-2} \left\{ \text{coeff. of } y^{d-4} \text{ in} : \frac{1}{(1+y^2)^{\frac{n}{2}-3d+7}(1-y^4)^{d-2}} \right\}.$$

It is worth noticing that, because of the known bounds for d (see [25]), $\frac{n}{2}-2d+5$ is always positive, while $\frac{n}{2}-3d+7$ may be negative. Taking account of the bounds in

[25], one easily sees that $\frac{n}{2} - 3d + 7 = 0$ can only happen when $n = 24m + 22$ and $d = 4m + 6$. If $\frac{n}{2} - 3d + 7 < 0$, the coefficients in the development of $\frac{1}{(1+y^2)^{\frac{n}{2}-3d+7}(1-y^4)^{d-2}}$ are all positive numbers. If $\frac{n}{2} - 3d + 7 > 0$, we have

$$\begin{aligned} c_{\frac{d}{2}-1} &= \frac{-n}{d-2} \sum_{\substack{j,k \in \mathbb{N} \\ j+2k=\frac{d}{2}-2}} (-1)^j \binom{\frac{n}{2} - 3d + 6 + j}{j} \binom{d+k-1}{k} \\ &= \frac{-n}{d-2} (-1)^{\frac{d}{2}} \sum_{\substack{j,k \in \mathbb{N} \\ j+2k=\frac{d}{2}-2}} \binom{\frac{n}{2} - 3d + 6 + j}{j} \binom{d+k-1}{k} \end{aligned}$$

which shows that $c_{\frac{d}{2}-1}$ and hence b_t cannot be zero.

In the case $n = 24m + 22$ and $d = 4m + 6$, we have $b_t = 0$, and a similar calculation shows that $b_{t+4} > 0$. More precisely, we calculate $b_{t+4} = -2^5 c_{2m+1}$, and

$$c_{2m+1} = -\frac{12m + 11}{2m + 1} \sum_{i+2k=2m} \binom{5+i}{i} \binom{4m+k+1}{k}. \qquad \square$$

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 $k \equiv 0 \bmod 2$, $Z_{C,f} \in \mathbb{C}[x^2 + y^2, x^2y^2(x^2 - y^2)^2]$ (respectively if $k \equiv 1 \bmod 2$, $Z_{C,f} \in Q_8\mathbb{C}[x^2 + y^2, x^2y^2(x^2 - y^2)^2]$, 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 W_i, respectively S_i denote the set of words of weight i in C, respectively S.*

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

Proof. We recall that, from the very definition of the harmonic functions, W_i is a t-design if and only if the coefficient of $x^{n-i}y^i$ equal 0 in $W_{C,f}$, for all harmonic function f of degree k with $1 \leqslant k \leqslant t$. One can define analogously the polynomials $W_{S,f}$. The following transformation formula, where again $Z_{S,f} := (xy)^{-k} W_{S,f}$, is proved in [20]

$$Z_{S,f}(x,y) = (-i)^k Z_{C,f}\left(\frac{x+y}{\sqrt{2}}, i\frac{x-y}{\sqrt{2}}\right). \tag{6}$$

One calculates $Q_8\left(\frac{x+y}{\sqrt{2}}, i\frac{x-y}{\sqrt{2}}\right) = i(x^8 - y^8)$. Altogether, we obtain an expression similar to (1) for $Z_{C,f}$ and $Z_{S,f}$.

We assume $k = 1$. There exists coefficients d_i, such that

$$\begin{cases} Z_{C,f}(x,y) = Q_8 \sum_{i=0}^{[\frac{n-10}{8}]} d_i(x^2+y^2)^{\frac{n}{2}-5-4i}\{x^2y^2(x^2-y^2)^2\}^i, \\ Z_{S,f}(x,y) = (x^8-y^8)\sum_{i=0}^{[\frac{n-10}{8}]} d_i(-1)^i 2^{\frac{n}{2}-5-6i}(xy)^{\frac{n}{2}-5-4i}(x^4-y^4)^{2i}. \end{cases} \tag{7}$$

Clearly, since the minimum weight of C is d, $d_i = 0$ for $0 \leqslant i \leqslant \frac{d}{2} - 2$, and since the minimum weight of S is $s = \frac{n}{2} - 4s'$, $d_i = 0$ for $i \geqslant s'$. Now the hypothesis on the s-extremality of the code C implies that all the d_i are equal to 0 and hence that $Z_{C,f} = Z_{S,f} = 0$.

In the case $k = 2$, a similar argument shows that all the coefficients but one are equal to zero. More precisely, and for later use, we have

If $k = 2$:

$$\begin{cases} Z_{C,f}(x,y) = d_{\frac{d}{2}-1}(x^2+y^2)^{\frac{n}{2}+2-2d}\{x^2y^2(x^2-y^2)^2\}^{\frac{d}{2}-1}, \\ Z_{S,f}(x,y) = d_{\frac{d}{2}-1}(-1)^{\frac{d}{2}}2^{\frac{n}{2}+4-3d}(xy)^{\frac{n}{2}+2-2d}(x^4-y^4)^{d-2}. \end{cases} \tag{8}$$

In the case $d = \frac{n+8}{6}$, the powers of (x^2+y^2) and (x^2-y^2) are identical in $Z_{C,f}$. Hence, the polynomial $Z_{C,f}$ equals up to a multiplicative constant $(xy)^{d-2}(x^4 - y^4)^{d-2}$, and the codewords of weight $\equiv d + 2 \bmod 4$ hold a 2-design. Moreover, we have $Z_{S,f} = (-1)^{\frac{d}{2}} Z_{C,f}$. Hence, if $d \equiv 2 \bmod 4$, $Z_{S,f} + Z_{C,f} = 0$ and the sets $W_i \cup S_i$ hold 2-designs. $\square$

Remark 3.2. A similar argument shows that, in the exceptional case of the extremal codes of length $n \equiv 22 \bmod 24$ and distance $d = 4[n/24] + 6$, the sets W_i and S_i hold 3-designs (see [20]).

Let C be a singly even self-dual code, with doubly even subcode C_0, then $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$, where C_i for $i = 0, 1, 2, 3$ are the cosets of C_0 in $C_0^\perp$. We fix for instance $C = C_0 \cup C_2$; then the shadow S of C is $S = C_1 \cup C_3$. In the case where C is s-extremal, the preceding theorem states that C and S hold 1-designs; in the following proposition we point out some stronger properties of these designs for particular s-extremal codes.

Proposition 3.3. *With the preceding notations, let C be a s-extremal $[24\mu + 8m, 12\mu + 4m, 4\mu + 2]$ code for $m = 1$ or 2, then the set of words of given weight in the cosets C_0, C_1, C_2 and C_3, independently, hold 1-designs.*

Proof. From Theorem 3.1, the codewords of given weight of $C = C_0 \cup C_2$ hold 1-designs, and therefore since the weight of the codewords of C_0 are congruent to 0 modulo 4 and those of C_2 are congruent to 2 mod 4, the codewords of given weight of C_0 and C_2 independently hold 1-designs. Now since the length n is congruent to 0 modulo 8 and C is s-extremal, the words of S have weights congruent to 0 modulo 4 and the two doubly even neighbors of C, namely $C_0 \cup C_1$ and $C_0 \cup C_3$, are extremal of minimum weight $4\mu + 4$. By the Assmus–Mattson theorem, these two codes hold at least 1-designs, and since C_0 holds 1-designs, C_1 and C_3 themselves also hold 1-designs. $\square$

Remark 3.4. In the case of lengths $24\mu + 16$, the preceding proposition is partly related to Theorem 2 of [17].

4. Codes with long shadows

In [12], 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 minimum weight $n/2 - 8$. Such codes are s-extremal if their minimum weight equals 6. The corresponding problem for lattices is handled in [21]. We prove here the following theorem:

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

In the following, we freely identify a word x of $\mathbb{F}_2^n$ and its support, and we denote by $\bar{x}$ the complement of x over $\mathbb{F}_2^n$. 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 of the coefficients in (3) leads to: $c_1 = -n/2$, $c_2 = n(n-22)/8$,

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

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 $n \leqslant 86$. On the other hand, the bound announced in the theorem $n \leqslant 44$ is optimal since the code of length 44 which is the direct sum of two copies of the $[22, 11, 6]$ code 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 [20])

$$\sum_j jn_{i,j}(y) = \frac{ia_i wt(y)}{n}. \tag{9}$$

Let y be a word of W_6. Then, for all $x \in W_6$, $|x \cap y| = 0, 2, 6$, and Eq. (9) leads to

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

Now we assume that $wt(y) = 8$. Again, for $x \in W_6$, we have $|x \cap y| = 0, 2, 4$; but (9) 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

$$\{(x, y) : x \in W_6, y \in W_8 \mid |x \cap y| = 4\}$$

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

$$mv = \frac{1}{a_8} \sum_{y \in W_8} n_4(y) = \frac{a_6}{a_8} m_2 = \frac{(n^2 - 66n + 1136)(n^2 - 66n + 1128)}{n^3 - 92n^2 + 2684n - 23248}. \tag{10}$$

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

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

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 $\bar{y}$.*

Proof. First x_i and x_j cannot intersect in their two positions on $\bar{y}$ else $x_i + y$ and x_j or x_i and x_j would intersect in at least four positions. Now if x_i and x_j intersect in one position on $\bar{y}$ then x_i and x_j but also $x_i + y$ and x_j must intersect only in one position on y which is not possible. $\square$

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

$$\begin{array}{lcccccccccccccccccccccc}
y & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0, \\
t_1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0, \\
t_2 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0, \\
t_3 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0, \\
t_4 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0, \\
t_5 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0, \\
t_6 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0, \\
t_7 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1.
\end{array}$$

In particular, $n_4(y) \leqslant 14$. 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.

Proof. The set $A := \{x \cap y \mid x \in N_4(y)\}$ is a set of elements of $\mathbb{F}_2^8$ satisfying the conditions:

- For all $a \in A$, $wt(a) = 4$.
- For all $a \in A$, $\bar{a} \in A$.
- For all $a, b \in A$, $|a \cap b| = 0, 2$,

where the last condition is a consequence of Lemma 4.3.

It is well-known (and easy to check) that, under these conditions, A is a subset of the set of codewords of weight 4 of the extended Hamming code (which has 14 elements). More precisely, a direct computation shows that, if the cardinality of A equals 2, 4, 10, 12 and of course 14, the set A is unique up to permutation, while there are two possibilities for the cardinality 6 and 8. □

We now prove the theorem

Proof of Theorem 4.1. First, by the classification of self-dual codes, we have $n \geqslant 22$ because $d \geqslant 6$. Suppose $n \geqslant 46$. Then, $a_8 > 0$, so let $y \in W_8$. Then, from Lemma 4.4, $n_4(y) \leqslant 14$, which gives $mv \leqslant 14$. But, from (10),

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

is positive for $n \geqslant 46$, a contradiction. □

5. Classification results

We now prove some results on the classification of the s-extremal codes of minimum 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 $N_4^{\max} := \{y : y \in W_8 \mid n_4(y) = n_4^{\max}\}$.

Let $y \in W_8$. We denote $D(y)$ the code generated by y and $N_4(y)$, after deletion of the zero coordinates (hence the length of $D(y)$ is at most equal to 22). We denote $E(y)$ the code generated by y, $N_4(y)$, and $N_2(y)$, again after deletion of the zero coordinates. We denote $E_D(y)$ the code obtained from $E(y)$ by restriction to the support of $D(y)$. Obviously we have $D(y) \subset E_D(y) \subset D(y)^{\perp}$.

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

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.

Generating matrices are explicitly given for all these codes in Appendix B.

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.

Proof. We give in Table 1 the value of mv computed from (10) for $d = 6$ and $22 \leqslant n \leqslant 44$.

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

Proof of Theorem 5.2. *Case* $n_4^{\max} = 14$: The following lemma is easily proved by a direct computation.

Lemma 5.4. *Let* D_8 *denote the* $[22, 8, 6]$ *code generated by the words* $\{y, t_1, t_2, t_3, t_4, t_5, t_6, t_7\}$ *given in Lemma* 4.4. *Up to the action of the permutation group of* D_8, *for each dimension* $k = 9, 10, 11$, *there is a unique code* D_k *such that* $D_8 \subset D_k \subset D_k^{\perp} \subset D_8^{\perp}$ *and* $d(D_k) = 6$. *Moreover, the cardinality of the set* $\{x : x \in D_k \mid wt(x) = 6 \text{ and } |x \cap y| = 2\}$ *equals respectively* $0, 8, 24, 56$ *for* $k = 8, 9, 10, 11$. *The code* D_{11} *is equivalent to the shorter Golay code.*

Now let C be an *s*-extremal code of distance 6 and length n, with $n_4^{\max} = 14$. Let $y \in N_4^{\max}$. Then, $D(y)$ is equivalent to D_8. Let $x \in N_2(y)$, and let $I := x \cap y$. We have

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

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

$I \cap t = (10)$ or (01) for exactly 4 of the 14 elements of $N_4(y)$. Thus, x must intersect these t outside of y; since the $t \cap \bar{y}$ are pairwise disjoint weight 2 words, we can conclude that x is contained in the support of $D(y)$. So, $E(y) = E_D(y)$ is a code satisfying the conditions of Lemma 5.4.

But Eq. (9) calculates $n_2(y) = (n^2 - 66n + 1136)/2 - 2n_4(y)$; we find $n_2(y) = -4, 0, 8, 20, 36, 56$ respectively for $n = 34, 36, 38, 40, 42, 44$. Hence, from Lemma 5.4 we can conclude that the only possible values for n are $n = 36$, in which case $E(y) \simeq D_8$, $n = 38$ and $E(y) \simeq D_9$, and $n = 44$ and $E(y) \simeq D_{11}$. Since D_{11} is the only self-dual code of length 22 and minimum weight 6, clearly in the case $n = 44$ the code C can only be the orthogonal sum of two copies of this code.

We recall a lemma on the structure of self-dual codes, which we shall apply several times. We refer to [23] for a proof.

Lemma 5.5. *Let C be a binary self-dual code of length $n = a + b$. Let A (respectively B) be the code generated by the words of C which supports lie under the a first coordinates (respectively the b last coordinates). Then, $2(\dim(A) - \dim(B)) = a - b$, and C has a generating matrix of the form*

$$\begin{pmatrix} A & 0 \\ 0 & B \\ D & E \end{pmatrix},$$

where $A^\perp = A + D$ and $B^\perp = B + E$.

In Section 6 and Table 2 we give the classification of maximal self-orthogonal codes of minimum distance 6 and lengths $10 \leqslant n \leqslant 21$. We will refer to this classification in the rest of the section.

If $n = 36$, we have $A = D_8$ and B has length 14, dimension 4, and distance at least 6. Moreover, since C and D_8 both contain the all-one word, so does B. One shows that these conditions leave only one possibility for B (cf. Table 2). This code B has the following property: under the action of $\mathrm{Aut}(B)$, the quotient $B^\perp/B$ has two non-trivial orbits, one consists of the classes of weight 2 and the other consists of the classes of weight 4. The code $D_8^\perp$ contains 7 words of weight 2, which are transitively permuted by its permutation group. We can choose such a word for the first line of D; then it must be extended by a word of weight 4 of $B^\perp$ in order to ensure that the minimum weight of C is 6. Hence C contains a subcode F of length 36 and dimension 13, obtained from D_8, B and one of the equivalent words of weight 6 built up as described before. The final step consists in the exhaustive consideration of the maximal totally isotropic subspaces of the 10-dimensional symplectic space $F^\perp/F$. The number of such subspaces is exactly 75 735, so we could actually list them (in fact up to the action of the group of F). It is worth noticing that the next dimension 12 gives 4 922 775 maximal isotropic subspaces which is too big to be exhausted.

If $n = 38$, we have $A = D_9$ and B has length 16, dimension 6, and distance at least 6, which leaves only one possibility. If $F \coloneqq A \perp B$, since the space $F^\perp/F$ has

Table 2
Maximal self-orthogonal codes with $d = 6$

Code	n	k	$\lvert\mathrm{Aut}(C)\rvert$	Weight enumerator
C_{10}	10	2	2304	$1 + 2y^6 + y^8$
C_{11}	11	2	2304	$1 + 2y^6 + y^8$
C_{12}	12	3	1536	$1 + 4y^6 + 3y^8$
$C_{13,1}$	13	3	1296	$1 + 3y^6 + 3y^8 + y^{10}$
$C_{13,2}$	13	3	1536	$1 + 4y^6 + 3y^8$
$C_{14,1}$	14	4	384	$1 + 6y^6 + 7y^8 + 2y^{10}$
$C_{14,2}$	14	4	21 504	$1 + 7y^6 + 7y^8 + y^{14}$
C_{15}	15	5	720	$1 + 10y^6 + 15y^8 + 6y^{10}$
C_{16}	16	6	11 520	$1 + 16y^6 + 30y^8 + 16y^{10} + y^{16}$
$C_{17,1}$	17	6	96	$1 + 13y^6 + 25y^8 + 18y^{10} + 6y^{12} + y^{14}$
$C_{17,2}$	17	6	120	$1 + 12y^6 + 25y^8 + 20y^{10} + 6y^{12}$
$C_{17,3}$	17	6	11 520	$1 + 16y^6 + 30y^8 + 16y^{10} + y^{16}$
$C_{18,1}$	18	7	1536	$1 + 20y^6 + 46y^8 + 40y^{10} + 16y^{12} + 4y^{14} + y^{16}$
$C_{18,2}$	18	7	144	$1 + 19y^6 + 45y^8 + 42y^{10} + 18y^{12} + 3y^{14}$
$C_{18,3}$	18	7	2160	$1 + 18y^6 + 45y^8 + 45y^{10} + 18y^{12} + y^{18}$
C_{19}	19	8	576	$1 + 28y^6 + 78y^8 + 88y^{10} + 48y^{12} + 12y^{14} + y^{16}$
C_{20}	20	9	3840	$1 + 40y^6 + 130y^8 + 176y^{10} + 120y^{12} + 40y^{14} + 5y^{16}$
C_{21}	21	10	40 320	$1 + 56y^6 + 210y^8 + 336y^{10} + 280y^{12} + 120y^{14} + 21y^{16}$

dimension 8, we can directly look at the 2295 maximal totally isotropic subspaces and find a unique code up to equivalence.

Case $n_4^{\max} = 12$: We select again $y \in N_4^{\max}$. Then, from the proof of Lemma 4.4, $D(y)$ is equivalent to the code with parameters $[20, 7, 6]$ generated by y and t_i for $1 \leqslant i \leqslant 6$, that we shall denote D_7. It has the property that any 2-subset I of y satisfies $I \cap t = (10)$ or (01) for either 3 or 4 of the 12 elements of $N_4(y)$. So a word $x \in N_2(y)$ has at most one coordinate outside of the support of D_7. Let us denote $d + 7 := \dim(E(y)) = \dim(E_D(y))$. Hence, the length of $E(y)$ cannot exceed $20 + d$. Also, from Eq. (9), we have $n_2(y) = 0, 4, 12, 24, 40$ respectively for $n = 34, 36, 38, 40, 42$.

We proceed to the classification with the following steps:

(1) List the possibilities for $E_D(y)$, up to the action of $\mathrm{Aut}(D_7)$, and using the properties $D_7 \subset E_D(y) \subset D_7^{\perp}$ and $wt(E_D(y)) \geqslant 6 - d$. We find 32 possible codes.
(2) For each candidate $E_D(y)$, we fix a set of d codewords which constitute a basis together with a basis of D_7, and we explore the possible extensions of them to words of length $20 + d$, such that the resulting code E is contained in its dual and has minimum weight 6.
(3) Among these codes E, we select those who satisfy:
   - $\mathrm{card}\{x : x \in E_6 \mid |x \cap y| = 2\} \in \{0, 4, 12, 24, 40\}\}$,
   - For all $z \in E_8$, $\mathrm{card}\{x : x \in E_6 \mid |x \cap z| = 4\} \leqslant 12$.

   We find, up to equivalence, nine codes E which are candidates for $E(y)$, with the following parameters, and corresponding n (which is uniquely determined by the value of $n_2(y)$):

(a) $[20,7]$ and $n=34$,
(b) $[21,8]$ and $n=36$,
(c) $[23,10]$ and $n=38$,
(d) $[20,9]$, $[23,10]$, $[22,10]$, $[24,11]$ and $n=40$,
(e) $[21,10]$, $[24,11]$ and $n=42$.

(4) Apply Lemma 5.5 with $A=E(y)$ for each of the nine possibilities found above. We obtain the parameters of the putative complementary codes B. Note that we are not sure that $E(y)$ is not strictly contained in A but this would increase the dimension of B. The putative codes are codes contained in their duals, of minimum weight greater or equal to 6, with parameters: $[14,4]$, $[15,5]$, $[15,6]$, $[20,9]$, $[17,7]$, $[18,8]$, $[16,7]$, $[21,10]$. The classification of Section 6 shows that there are no such codes with parameters $[15,6]$, $[17,7]$, $[18,8]$, $[16,7]$, that a unique code exists with parameters respectively $[21,10,6]$, $[20,9,6]$ and $[15,5,6]$, and that there are two codes with parameters $[14,4,6]$.

(5) In the case $n=34$, $A=D_7$, which does not contain the all-one word. So B must be equivalent to the $[14,4]$ which does not either. The self-dual code C contains as a subcode the 12-dimensional code F generated by the orthogonal sum of A and B, and the all-one word. Since $\dim(F^\perp/F)=10$, we can look at all the possibilities. In the other cases, B is uniquely determined and $F := A\perp B$ satisfies $\dim(F^\perp/F)\leqslant 10$.

Case $n_4^{\max}=10$: Let $y\in N_4^{\max}$. Then, $D(y)$ is equivalent to the code with parameters $[18,6,6]$ generated by y and t_i for $1\leqslant i\leqslant 5$, denoted D_6. Any 2-subset I of y satisfies $I\cap t=(10)$ or (01) for either 2, 3 or 4 of the 5 elements of $\{t_1,t_2,t_3,t_4,t_5\}$. So a word $x\in N_2(y)$ has at most two bits outside of the support of D_6. Therefore, the algorithmic procedure described in the case $n_4^{\max}=12$ cannot be directly applied here because at Step 2, each basis vector added to D_6 may increase the size of the support by 2, so too many cases occur. We have to look at the situation more closely.

For $i=0,1,2$ we denote I_i the set of 2-subsets of y on which $4-i$ elements of $N_4(y)$ equal (10) or (01). We have $\mathrm{card}(I_0)=4$, $\mathrm{card}(I_1)=16$, $\mathrm{card}(I_2)=8$, and $\mathrm{Aut}(D_6)$ permutes transitively the elements of each I_i. We denote $N_2^i := \{x : x\in N_2(y) \mid x\cap y\in I_i\}$. Let $x\in N_2^i$. Then x has i bits outside of the support of D_6. We again denote D_6 the subcode of the same length as $E(y)$, obtained by extending the words of D_6 with enough zeroes. An easy calculation shows that: $\mathrm{card}((D_6+x)\cap N_2(y))$ equals 8 if $x\in N_2^0$, 4 if $x\in N_2^1$, and 2 if $x\in N_2^2$. Also, not more than two elements of $N_2(y)$ can coincide on y (otherwise two of them would have three common bits). Moreover, one checks easily that, if two elements x, x' of N_2^1 coincide on y, then the code generated by D_6, x and x', which is unique up to $\mathrm{Aut}(D_6)$, satisfies $N_4(y)=12$, so this situation can be excluded. We can partition the classes of $E(y)$ modulo D_6 into s_0 (respectively s_1, s_2) classes containing elements of N_2^0 (respectively N_2^1, N_2^2), plus s_{-1} classes containing no elements of $N_2(y)$. From the previous discussion, we have: $8s_0+4s_1+2s_2=n_2(y)$, $0\leqslant s_0\leqslant 1$, $0\leqslant s_1\leqslant 4$, $0\leqslant s_2\leqslant 8$. On the other hand, we have, from Eq. (1), $n_2(y)=4,8,16,28$ respectively for $n=34,36,38,40$.

We are now in the position to calculate all the possibilities for the code $E(y)$. Therefore, we start with D_6, and we add one by one words belonging to $N_2(y)$. At each step, we increase the dimension by one, and calculate $n_2(y)$ until we obtain one of the values $4, 8, 16, 28$.

If $s_0 = 1$, we start with $x \in N_2^0$ and there is only one choice up to equivalence. The resulting code has $n_2(y) = 8$, so it is one possibility for $E(y)$ (it is equivalent to the maximal code $C_{18,1}$). Then, we can either add a word in N_2^1, else the remaining words belong to N_2^2. In the first case, we obtain a single code with parameters $[19, 8]$ and $n_2(y) = 16$, equivalent to the maximal code C_{19}, which is not extendable; the second case does not lead to any code.

In the case $s_0 = 0$, we calculate that at most three independent words in N_2^1 can be added and at most six independent words in N_2^2 can be added.

Finally we find, up to equivalence, 19 codes E which are candidates for $E(y)$, with the following parameters, and corresponding n (which is uniquely determined by the value of $n_2(y)$):

(1) $[19, 7]$, $[21, 8]$, $[22, 8]$ (3 codes) and $n = 34$,
(2) $[18, 7]$, $[20, 8]$, $[22, 9]$, $[23, 9]$ (3 codes), $[26, 10]$, $[25, 10]$, $[24, 10]$ and $n = 36$,
(3) $[19, 8]$, $[21, 9]$, $[25, 11]$, $[26, 12]$ and $n = 38$,
(4) $[25, 12]$ and $n = 40$.

Then, we proceed like in the steps 4 and 5 of the case $n_4^{\max} = 12$. The codes leading to a self-dual code of length 34 have parameters $[19, 7]$, $[22, 8]$ (two codes). The self-dual code of length 36 is obtained from $A = C_{18,1}$ and $B = C_{18,2}$. The self-dual code of length 38 is obtained from $A = B = C_{19}$. $\square$

Remark 5.6. As pointed out by A. Munemasa: the doubly even $[40, 20, 8]$ code with covering radius 7 of [17], is equivalent to the two equivalent doubly even neighbors of the unique s-extremal $[40, 20, 6]$ code. 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 5.7. 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 [21]. The construction is the standard Construction A followed by a neighboring procedure using the all-one vector.

6. The classification of maximal self-orthogonal codes of distance 6 and length up to 21

In this section we classify maximal (in term of dimension) self-orthogonal codes of minimum distance exactly 6 and length up to 21. Unlike self-dual codes, there is no mass formula for these codes and we proceed by induction on the dimension. Let us denote by XC the extension of a code C.

We first give a general algorithm to construct, for not too high parameters, all the self-orthogonal $[n,k,d]$ codes. Let S_i be the set of inequivalent self-orthogonal $[n-k+i,i,d]$ codes. The set S_{i+1} of the $[n-k+i+1,i+1,d]$ codes can be obtained from S_i by the following algorithm : let C be a code of S_i. Then one considers all the inequivalent codes of minimum weight d obtained by addition to XC of a representant x of the different orbits of the quotient $(XC)^{\perp}/XC$. All the codes of S_{i+1} are obtained this way since for any C of S_{i+1}, the shortened code of C in a column for which there exists a word of weight d with a zero coordinate on this column, is in S_i.

Hence all the self-orthogonal $[n,k,d]$ codes are obtained starting from a $[n-k+1,1,d]$ code.

Note that by construction the codes have a codeword of weight d.

To complete the classification one applies the preceding algorithm with different trials on the possible dimensions. We present in Table 2 the results obtained for $d=6$, lengths $10\leqslant n\leqslant 21$ and maximal dimension k. Note that for lengths $6\leqslant n\leqslant 9$ only the trivial code of dimension 1 exists. The codes obtained for lengths 19, 20 and 21 correspond to shortened codes of the self-dual $[22,11,6]$ shorter Golay code. Note that we also used the algorithm to prove that no codes exist with the same length and dimension with a higher minimum distance. The generator matrices are given in the appendix.

7. 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 [12]. 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 the lengths $22\leqslant n\leqslant 44$. 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	[22]	34	$\geqslant 2$	[9, Section 5]
24	1	[24]	36	$\geqslant 3$	[9, Section 5]
26	1	[8]	38	$\geqslant 2$	[9, Section 5]
28	2	[8]	40	1	[9, Section 5]
30	9	[8]	42	1	[9, Section 5]
32	19	[3]	44	1	[9, Section 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	[9]
36	$\geqslant 3$	[16,19]
38	$\geqslant 8$	[16,19]
40	$\geqslant 4$	[7,9]
42	$\geqslant 17$	[6,9]
44	$\geqslant 1$	[9]

- $d = 10$:

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

n	Num	Ref
46	$\geqslant 1$	$sub(XQ_{47})$
50	$\geqslant 1$	[9]
52	$\geqslant 460$	[18]
54	$\geqslant 166$	[26, Section 3]
58	$\geqslant 1$	[9]

- $d = 12$:

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	$\geqslant 3$	[10,27]
62	$\geqslant 8$	[10]
66	$\geqslant 2$	[9,15]

- $d \geqslant 14$:

For $d = 14$, two codes are known for length 76 [1,13], which contain 2-designs, and more than 50 codes are known for length 78 from [1,14]. 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 and Lemma 2.4.

Appendix A

Maximal self-orthogonal codes of weight 6 and lengths $10 \leqslant n \leqslant 21$

$$C_{10} = \begin{bmatrix} 1000011111 \\ 0111101111 \end{bmatrix}, \quad C_{11} = \begin{bmatrix} 11000011101 \\ 00111111101 \end{bmatrix}, \quad C_{12} = \begin{bmatrix} 110000111010 \\ 001001100111 \\ 000110011101 \end{bmatrix},$$

$$C_{13,1} = \begin{bmatrix} 1000101111110 \\ 0101110111001 \\ 0010101000111 \end{bmatrix}, \quad C_{13,2} = \begin{bmatrix} 1010001100110 \\ 0101000111010 \\ 0000111011100 \end{bmatrix},$$

$$C_{14,1} = \begin{bmatrix} 10001011111100 \\ 01001001100101 \\ 00101010001110 \\ 00010100010111 \end{bmatrix},$$

$$C_{14,2} = \begin{bmatrix} 10100000110011 \\ 01010001110100 \\ 00001101000111 \\ 00000011111111 \end{bmatrix}, \quad C_{15} = \begin{bmatrix} 100001110100111 \\ 010001010010101 \\ 001001101000011 \\ 000101000101110 \\ 000011001011111 \end{bmatrix},$$

$$C_{16} = \begin{bmatrix} 1000010010110001 \\ 0100010100101010 \\ 0010010101111001 \\ 0001010001011100 \\ 0000110010111110 \\ 0000001111111111 \end{bmatrix},$$

$$C_{17,1} = \begin{bmatrix} 10000101000101010 \\ 01000101001000101 \\ 00110000011110110 \\ 00001100010011001 \\ 00000011011110000 \\ 00000000101011110 \end{bmatrix}, \quad C_{17,2} = \begin{bmatrix} 10000101101110100 \\ 01000100100110001 \\ 00100100111001110 \\ 00010100001100110 \\ 00001101111101101 \\ 00000011011110000 \end{bmatrix},$$

$$C_{17,3} = \begin{bmatrix} 10000101011011010 \\ 01000101010000110 \\ 00100100111100110 \\ 00010100001110010 \\ 00001100111001000 \\ 00000011111111110 \end{bmatrix},$$

$$C_{18,1} = \begin{bmatrix} 100001010001010100 \\ 010001010010001010 \\ 001100000010100011 \\ 000011000001111101 \\ 000000110010101111 \\ 000000001010111100 \\ 000000000101001111 \end{bmatrix}, \quad C_{18,2} = \begin{bmatrix} 100001010001010100 \\ 010001010010001010 \\ 001001000010111011 \\ 000101000101010111 \\ 000011000100110010 \\ 000000110111100000 \\ 000000001010111100 \end{bmatrix},$$

$$C_{18,3} = \begin{bmatrix} 100001010011110111 \\ 010001000001111101 \\ 001001000110000011 \\ 000101000011001100 \\ 000011010111000101 \\ 000000110111100000 \\ 000000001000011111 \end{bmatrix}, \quad C_{19} = \begin{bmatrix} 1000010100010101000 \\ 0100010100100010100 \\ 0010010000101110101 \\ 0001010000000110011 \\ 0000110000011111010 \\ 0000001100101011110 \\ 0000000010101111000 \\ 0000000001010011110 \end{bmatrix},$$

$$C_{20} = \begin{bmatrix} 10000100001101000111 \\ 01000100000000111111 \\ 00100100001011101010 \\ 00010100000001100110 \\ 00001100000111110100 \\ 00000010000010101011 \\ 00000001001000010111 \\ 00000000101011110000 \\ 00000000010100111100 \end{bmatrix}, \quad C_{21} = \begin{bmatrix} 100001000000000011011 \\ 010001000000001111110 \\ 001001000001101000001 \\ 000101000000011001100 \\ 000011000001111101000 \\ 000000100000101010110 \\ 000000010001010111011 \\ 000000001001101110101 \\ 000000000101001111000 \\ 000000000011010010101 \end{bmatrix}.$$

Appendix B

In this appendix we give all the codes mentioned in Theorem 5.2. To save space, we consider the codes in the form $(I\ \ A)$ and we list only the matrices A as sequences of their rows written in hexadecimal: $1 = 0001, 2 = 0010, \ldots, F = 1111$. Note that depending on the length n, the first $4 - (\frac{n}{2} \pmod 4)$ columns of '0' have to be deleted

- $n_4^{\max} = 14$:

$C36\_14$: 3B29E; 38C0F; 36718; 358D4; 2EA9D; 2D774; 23CB4; 1015D; 08378; 04225; 023AF; 0118A; 00AF2; 004D7; 0026F; 0016C; 000E3; 0001F.

$C38\_14$: 77833; 7143C; 6DF14; 6A800; 5D291; 5BF27; 476AD; 21B1B; 101B9; 09AA2; 0431B; 039B9; 006A2; 003BF; 003D5; 00265; 00159; 000D6; 0007F.

$C44\_14$: 293000; 3DA000; 1ED000; 3EB800; 366800; 1B3800; 3C4000; 06C800; 1B8000; 152800; 127000; 000526; 0007B4; 0003DA; 0007D7; 0006CD; 000367; 000788; 0000D9; 000370; 0002A5; 00024E.

- $n_4^{\max} = 12$:

$C34\_12$: 1DA49; 1C653; 1B33B; 1AEB9; 174CF; 16A63; 11F34; 08198; 042B6; 0232E; 01289; 009A7; 00711; 002CF; 00136; 001C5; 001FC.

$C36\_12$: 3B454; 38AB1; 36061; 35B30; 2EB1B; 2D42B; 23A84; 105B4; 081D5; 04461; 025AA; 011CB; 0081E; 00159; 000C7; 0026C; 0038A; 003F8.

$C40\_12$: E6FE7; F97E7; D47E7; CBF17; ED8F0; EA000; 87800; 5C8F0; 428F0; 59800; 380F0; 004AA; 00495; 004CF; 003AB; 00354; 0020F; 001C9; 001F5; 00133.

$C42\_12$: 1D887F; 1C107F; 1B0800; 1A587F; 17D87F; 16B07F; 11A07F; 08C87F; 04F000; 02387F; 01F87F; 00074E; 00077D; 0006A1; 0006F4; 0005C4; 0005E9; 00044B; 000266; 00011E; 0000F8.

- $n_4^{\max} = 10$:

$C34\_10a$: 1DC61; 1C330; 1B5D5; 1A99F; 1704A; 1687F; 11B2E; 0831B; 04764; 0247F; 012D0; 00EAF; 00159; 000C7; 0026C; 0038A; 003F8.

$C34\_10b$: 1DB90; 1C0E8; 1B376; 1AF5A; 173A1; 16E29; 11ADC; 08754; 046F0; 021A4; 0119B; 0083F; 004D7; 0034C; 0013A; 00067; 0009D.

$C34\_10c$: 1DB65; 1C231; 1B373; 1AEC1; 172F5; 16FAA; 119B9; 084E6; 0440B; 020ED; 0135A; 00BB7; 00586; 00354; 0013A; 00067; 0009D.

$C36\_10$: 3A800; 39B18; 3794E; 350D3; 2FA56; 2D368; 233BB; 11A85; 09A26; 040A3; 038A3; 00654; 0068A; 004BB; 00557; 00532; 003E0; 000BC.

$C38\_10$: 430E2; 4FBE9; 59147; 59800; 4C24C; 2ABE9; 262AE; 1F947; 3E24C; 23947; 3124C; 006A8; 00714; 00575; 00433; 004FA; 0035E; 00178; 0009E.

References

[1] A. Baartmans, V. Yorgov, Some new extremal codes of length 76 and 78, Proceedings of the Seventh International Workshop on Algebra and Combinatorics, Coding Theory, 18–24 June, Bulgaria, 2000, pp. 51–54.

[2] C. Bachoc, On harmonic weight enumerators of binary codes, Des. Codes Cryptogr. 18 (1999) 11–28.
[3] R.T. Bilous, G.H.J. van Rees, An enumeration of self-dual codes of length 32, Des. Codes Cryptogr. 26 (2002) 61–86.
[4] W. Bosma, J. Cannon, Handbook of Magma Functions, University of Sydney, Sydney, 1995.
[5] R.A. Brualdi, V.S. Pless, Weight enumerators of self-dual codes, IEEE Trans. Inform. Theory 37 (1991) 1222–1225.
[6] S. Buyuklieva, New extremal self-dual codes of length 42 and 44, IEEE Trans. Inform. Theory 43 (1997) 1607–1612.
[7] S. Buyuklieva, V. Yorgov, Singly-even self-dual codes of length 40, Des. Codes Cryptogr. 9 (1996) 131–141.
[8] J.H. Conway, V.S. Pless, On the enumeration of self-dual codes, J. Combin. Theory Ser. A 28 (1980) 26–53.
[9] J.H. Conway, N.J.A. Sloane, A new upper bound on the minimum distance of self-dual codes, IEEE Trans. Inform. Theory 36 (1990) 1319–1333.
[10] R. Dontcheva, M. Harada, New extremal self-dual codes of length 62 and related extremal self-dual codes, IEEE Trans. Inform. Theory 48 (2002) 2060–2064.
[11] S.T. Dougherty, T.A. Gulliver, M. Harada, Extremal binary self-dual codes, IEEE Trans. Inform. Theory 43 (1997) 2036–2047.
[12] N. Elkies, Lattices and codes with long shadows, Math. Res. Lett. 2 (5) (1995) 643–651.
[13] P. Gaborit, A. Otmani, Experimental constructions of self-dual codes, Finite Fields Appl. 9 (2003) 372–394.
[14] T.A. Gulliver, M. Harada, J.-L. Kim, Construction of new extremal self-dual codes, Discrete Math. 263 (2003) 81–91.
[15] M. Harada, Classification of extremal double circulant codes of lengths 64 to 72, Des. Codes Cryptogr. 13 (3) (1998) 257–269.
[16] M. Harada, New extremal self-dual codes of lengths 36 and 38, IEEE Trans. Inform. Theory 45 (1999) 2541–2543.
[17] M. Harada, M. Ozeki, Extremal self-dual codes with the smallest covering radius, Discrete Math. 215 (2000) 271–281.
[18] W.C. Huffman, V.D. Tonchev, The [52,26,10] binary self-dual codes with an automorphism of order 7, Finite Fields Appl. 7 (2001) 341–349.
[19] J.-L. Kim, New extremal self-dual codes of lengths 36, 38 and 58, IEEE Trans. Inform. Theory 47 (4) (2001) 1575–1580.
[20] M. Lalaude-Labayle, On binary linear codes supporting t-designs, IEEE Trans. Inform. Theory 47 (6) (2001) 2249–2255.
[21] G. Nebe, B. Venkov, Unimodular lattices with long shadow, J. Number Theory 99 (2003) 307–317.
[22] V. Pless, A classification of self-orthogonal codes over $GF(2)$, Discrete Math. 3 (1972) 209–246.
[23] V. Pless, Introduction to the Theory of Error Correcting Codes, 3rd Edition, Wiley, New York, 1998.
[24] V. Pless, N.J.A. Sloane, On the classification and enumeration of self-dual codes, J. Combin. Theory Ser. A A18 (1975) 313–335.
[25] E. Rains, Shadow bounds for self-dual codes, IEEE Trans. Inform. Theory 44 (1) (1998) 134–139.
[26] E.M. Rains, N.J.A. Sloane, Self-dual codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998, pp. 177–294.
[27] H.-P. Tsai, Y.J. Yiang, Some new extremal self-dual [58,29,10] codes, IEEE Trans. Inform. Theory 44 (1998) 813–814.