

# On involutions in extremal self-dual codes and the dual distance of semi self-dual codes.

Martino Borello

*Member INdAM-GNSAGA (Italy)*  
*Dipartimento di Matematica e Applicazioni*  
*Università degli Studi di Milano Bicocca*  
*20125 Milan, Italy*  
*e-mail: martino.borello@unimib.it*

Gabriele Nebe

*Lehrstuhl D für Mathematik,*  
*RWTH Aachen University,*  
*52056 Aachen, Germany,*  
*e-mail: nebe@math.rwth-aachen.de.*

---

## Abstract

A classical result of Conway and Pless is that a natural projection of the fixed code of an automorphism of odd prime order of a self-dual binary linear code is self-dual [13]. In this paper we prove that the same holds for involutions under some (quite strong) conditions on the codes.

In order to prove it, we introduce a new family of binary codes: the semi self-dual codes. A binary self-orthogonal code is called semi self-dual if it contains the all-ones vector and is of codimension 2 in its dual code. We prove upper bounds on the dual distance of semi self-dual codes.

As an application we get the following: let  $\mathcal{C}$  be an extremal self-dual binary linear code of length  $24m$  and  $\sigma \in \text{Aut}(\mathcal{C})$  be a fixed point free automorphism of order 2. If  $m$  is odd or if  $m = 2k$  with  $\binom{5k-1}{k-1}$  odd then  $\mathcal{C}$  is a free  $\mathbb{F}_2\langle\sigma\rangle$ -module. This result has quite strong consequences on the structure of the automorphism group of such codes.

*Keywords:* semi self-dual codes, bounds on minimum distance, automorphism group, free modules, extremal codes

---

## 1. Introduction

The research in this paper is motivated by the study of involutions of extremal self-dual codes, which plays a fundamental role in [17, 6, 5, 8, 7, 21].

Let  $m \in \mathbb{N}$  and  $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^{24m}$  be an extremal binary self-dual code, so  $d(\mathcal{C}) = 4m + 4$  [15]. Then  $\mathcal{C}$  is doubly even [19]. There are unique extremal self-dual codes of length 24 and 48 and these are the only known extremal codes of length  $24m$ . It is an intensively studied open question raised in [20], whether an extremal code of length 72 exists. A series of many papers has shown that if such a code exists, then its automorphism group  $\text{Aut}(\mathcal{C}) = \{\sigma \in S_{24m} \mid \sigma(\mathcal{C}) = \mathcal{C}\}$  has order  $\leq 5$  (see [4] for an exposition of this result). Stefka Bouyuklieva [9] studies automorphisms of order 2 of such codes. She shows that if  $\mathcal{C}$  is an extremal code of length  $24m$ ,  $m \geq 2$  and  $\sigma \in \text{Aut}(\mathcal{C})$  has order 2, then the permutation  $\sigma$  has no fixed points, with one exception,  $m = 5$ , where there might be 24 fixed points. If  $\sigma = (1, 2) \dots, (24m - 1, 24m)$  is a fixed point free automorphism of a doubly even self dual code  $\mathcal{C}$ , then its *fixed code*

$$\mathcal{C}(\sigma) := \{c \in \mathcal{C} \mid \sigma(c) = c\}$$

is isomorphic to

$$\pi(\mathcal{C}(\sigma)) = \{(c_1, \dots, c_{12m}) \in \mathbb{F}_2^{12m} \mid (c_1, c_1, c_2, c_2, \dots, c_{12m}, c_{12m}) \in \mathcal{C}\}$$

such that

$$\pi(\{c + \sigma(c) \mid c \in \mathcal{C}\}) = \pi(\mathcal{C}(\sigma))^\perp \subseteq \pi(\mathcal{C}(\sigma)).$$

As  $\mathcal{C}$  is doubly-even, all words in  $\pi(\mathcal{C}(\sigma))$  have even weight. It is shown in [17] and [5] that the code  $\mathcal{C}$  is a free  $\mathbb{F}_2\langle\sigma\rangle$ -module, if and only if  $\pi(\mathcal{C}(\sigma))$  is self-dual. If  $\pi(\mathcal{C}(\sigma))$  is not self-dual then it contains the dual  $\mathcal{D}^\perp$  of some code  $\mathcal{D}$  of length  $12m$  with

$$\mathbf{1} := (1, \dots, 1) \in \pi(\mathcal{C}(\sigma))^\perp \subseteq \mathcal{D} \subseteq \mathcal{D}^\perp \subseteq \pi(\mathcal{C}(\sigma)).$$

In particular  $d(\mathcal{D}^\perp) \geq d(\pi(\mathcal{C}(\sigma))) = \frac{1}{2}d(\mathcal{C}(\sigma)) \geq \frac{1}{2}d(\mathcal{C})$ .

**Definition 1.1.** A binary self-orthogonal code  $\mathcal{D} \subseteq \mathcal{D}^\perp \leq \mathbb{F}_2^n$  of length  $n$  is called *semi self-dual*, if  $\mathbf{1} := (1, \dots, 1) \in \mathcal{D}$  and  $\dim(\mathcal{D}^\perp/\mathcal{D}) = 2$ .

Self-orthogonal codes always consist of words of even weight, so  $\text{wt}(c) := |\{i \mid c_i = 1\}| \in 2\mathbb{Z}$  for all  $c \in \mathcal{D}$ . Hence already the condition that  $\mathbf{1} \in \mathcal{D}$

implies that the length  $n = 12m$  of  $\mathcal{D}$  is even. Note that  $\mathcal{D}^\perp \subseteq \mathbf{1}^\perp = \{c \in \mathbb{F}_2^n \mid \text{wt}(c) \in 2\mathbb{Z}\}$  implies that also  $\mathcal{D}^\perp$  consists of even weight vectors. The *dual distance* of  $\mathcal{D}$  is the minimum weight of the dual code  $\text{dd}(\mathcal{D}) := d(\mathcal{D}^\perp) := \min(\text{wt}(\mathcal{D}^\perp \setminus \{0\}))$ .

In this paper we will bound the dual distance  $\text{dd}(\mathcal{D}) = d(\mathcal{D}^\perp)$  of semi self-dual codes. In particular if the length of  $\mathcal{D}$  is  $12m$  with either  $m$  odd or  $m = 2\mu$  such that  $\binom{5\mu-1}{\mu-1}$  is odd, then  $\text{dd}(\mathcal{D}) \leq 2m$  (see Theorem 2.1 below for the general statement).

Then we may conclude the following Theorem.

**Theorem 1.2.** *Let  $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^{24m}$  be an extremal code of length  $24m$  and  $\sigma \in \text{Aut}(\mathcal{C})$  be a fixed point free automorphism of order 2. Then  $\mathcal{C}$  is a free  $\mathbb{F}_2\langle\sigma\rangle$ -module if  $m$  is odd or if  $m = 2\mu$  with  $\binom{5\mu-1}{\mu-1}$  odd.*

In particular, for  $m = 3$ , we obtain [17, Theorem 3.1] without appealing to the classification of all extremal codes of length 36 in [1] and without any serious computer calculation.

**Remark 1.3.** *In [22], Zhang proved that extremal self-dual binary linear codes of length a multiple of 24 may exist only up to length  $3672 = 153 \cdot 24$ . About 72% of these lengths are covered by Theorem 1.2. In particular the projections of fixed codes by fixed point free involutions in self-dual [96, 48, 20] and [120, 60, 24] codes (see [11, 10] for an exposition of the state of the art for the codes with these parameters) are self-dual.*

The same arguments as in [17] can now be applied to obtain the following quite strong consequence on the structure of the automorphism group of such extremal codes.

**Corollary 1.4.** *Let  $m \geq 3$  be odd and assume that  $m \neq 5$ . Let  $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^{24m}$  be an extremal code. If 8 divides  $|\text{Aut}(\mathcal{C})|$  then a Sylow 2-subgroup of  $\text{Aut}(\mathcal{C})$  is isomorphic to  $C_2 \times C_2 \times C_2$ ,  $C_2 \times C_4$  or  $D_8$ .*

*Proof.* Let  $S$  be a Sylow-2-subgroup of  $\text{Aut}(\mathcal{C})$ .

By our assumption and [9] all elements of order 2 in  $\text{Aut}(\mathcal{C})$  act without fixed points on the places  $\{1, \dots, 24m\}$ . This immediately implies that all  $S$ -orbits have length  $|S|$ , so  $|S|$  divides  $24m$  and hence  $|S| = 8$ .

So we only need to exclude  $S = C_8$  and  $S = Q_8$ . This is done by considering the module structure of  $\mathcal{C}$  as an  $\mathbb{F}_2 S$ -module. Note that both groups have a unique elementary abelian subgroup, say  $Z$ , and  $Z \cong C_2$ . By Theorem 1.2

the module  $\mathcal{C}$  is a free  $\mathbb{F}_2 Z$ -module. Chouinard's Theorem [12] states that a module is projective if and only if its restriction to every elementary abelian subgroup is projective. Then  $\mathcal{C}$  is also a free  $\mathbb{F}_2 S$ -module of rank

$$\text{rk}_{\mathbb{F}_2 S}(\mathcal{C}) = \frac{\dim_{\mathbb{F}_2}(\mathcal{C})}{|S|} = \frac{12m}{8} = 3 \cdot \frac{m}{2} \notin \mathbb{N}$$

a contradiction. □

**Remark 1.5.** *Note that the cyclic group  $C_8$  is already excluded by the Sloane-Thompson Theorem (see also [14]) because  $S \cong C_8$  acting fixed point freely on  $24m$  points implies that  $S$  is not in the alternating group, so  $S$  does not fix any doubly-even self-dual code.*

## 2. Bounds on the dual distance of semi self-dual codes

In the previous section we introduced the definition of semi self-dual codes. Now we will prove upper bounds on their dual distance. Even if this family of codes was introduced as a tool for the proof of Theorem 1.2, it seems to be interesting also by itself. Applying the methods from [19], we show the following theorem.

**Theorem 2.1.** *Let  $\mathcal{D} \leq \mathbb{F}_2^n$  be a semi self-dual code. Then the dual distance of  $\mathcal{D}$  is bounded by*

$$\text{dd}(\mathcal{D}) = d(\mathcal{D}^\perp) \leq \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 2 & \text{if } n \equiv 0, 2, 4, 6, 8, 10, 12, 14 \pmod{24} \\ 4\lfloor \frac{n}{24} \rfloor + 4 & \text{if } n \equiv 16, 18, 20 \pmod{24} \\ 4\lfloor \frac{n}{24} \rfloor + 6 & \text{if } n \equiv 22 \pmod{24}. \end{cases}$$

*If  $n = 24\mu$  for some integer  $\mu$  and  $\mathcal{D}$  is doubly-even or  $\binom{5\mu-1}{\mu-1}$  is odd then*

$$\text{dd}(\mathcal{D}) = d(\mathcal{D}^\perp) \leq 4\mu.$$

Theorem 2.1 follows by combining Remark 3.1, Proposition 4.1, Proposition 5.2 and Proposition 5.3.

**Remark 2.2.** *The well-known Kummer's theorem on binomial coefficients implies that  $\binom{5\mu-1}{\mu-1}$  is odd if and only if there are no carries when  $4\mu$  is added to  $\mu - 1$  in base 2.*

By direct calculations with MAGMA, using a database [16] of all self-dual binary linear codes of length up to 40, most of the bounds of Theorem 2.1 can be shown to be sharp. In particular, we have semi self-dual codes such that their dual codes have parameters  $[4, 3, 2]$ ,  $[6, 4, 2]$ ,  $[8, 5, 2]$ ,  $[10, 6, 2]$ ,  $[12, 7, 2]$ ,  $[14, 8, 2]$ ,  $[16, 9, 4]$ ,  $[18, 10, 4]$ ,  $[20, 11, 4]$  and  $[22, 12, 6]$  and a doubly-even semi self-dual code with dual code of parameters  $[24, 13, 4]$ .

### 3. Self-dual subcodes

From now on let  $\mathcal{D}$  be a semi self-dual code of even length  $n \geq 4$ . Furthermore, let  $\mu = \lfloor \frac{n}{24} \rfloor$ .

**Remark 3.1.** *There are exactly three self-dual codes  $\mathcal{C}_i = \mathcal{C}_i^\perp$  ( $i \in \{1, 2, 3\}$ ) with*

$$\mathcal{D} \subset \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \subset \mathcal{D}^\perp.$$

*From the bound on  $d(\mathcal{C}_i)$  given in [19, Theorem 5] we obtain*

$$dd(\mathcal{D}) = d(\mathcal{D}^\perp) \leq d(\mathcal{C}_1) \leq \begin{cases} 4\mu + 6 & \text{if } n \equiv 22 \pmod{24} \\ 4\mu + 4 & \text{otherwise.} \end{cases}$$

We aim to find a better bound.

### 4. Shadows: the doubly-even case

**Proposition 4.1.** *If  $\mathcal{D}$  is doubly-even, then*

$$d(\mathcal{D}^\perp) \leq \begin{cases} 4\mu & \text{if } n \equiv 0 \pmod{24} \\ 4\mu + 2 & \text{if } n \equiv 4, 8, 12 \pmod{24} \\ 4\mu + 4 & \text{if } n \equiv 16, 20 \pmod{24}. \end{cases}$$

*Proof.* Since every doubly-even binary linear code is self-orthogonal,  $\mathcal{D}^\perp$  cannot be doubly-even and so in  $\mathcal{D}^\perp$  there exists a codeword of weight  $w \equiv 2 \pmod{4}$ . Thus we can take  $\mathcal{D} < \mathcal{F} = \mathcal{F}^\perp < \mathcal{D}^\perp$  with  $\mathcal{F}$  not doubly-even, so that  $\mathcal{D} = \mathcal{F}_0 := \{f \in \mathcal{F} \mid \text{wt}(f) \equiv 0 \pmod{4}\}$  is the maximal doubly-even subcode of  $\mathcal{F}$ .

Let  $S(\mathcal{F}) := \mathcal{D}^\perp - \mathcal{F}$  denote the shadow of  $\mathcal{F}$ . By [3],

$$2d(\mathcal{F}) + d(S(\mathcal{F})) \leq 4 + \frac{n}{2}. \tag{1}$$

Note that  $d(\mathcal{D}^\perp) = \min\{d(\mathcal{F}), d(S(\mathcal{F}))\}$ , since  $\mathcal{D}^\perp = S(\mathcal{F}) \cup \mathcal{F}$ . Since we have the bound (1), the maximum for  $\min\{d(\mathcal{F}), d(S(\mathcal{F}))\}$  is reached if

$$d(\mathcal{D}^\perp) = d(\mathcal{F}) = d(S(\mathcal{F})) = \left\lfloor \frac{4 + \frac{n}{2}}{3} \right\rfloor$$

so that

$$d(\mathcal{D}^\perp) \leq \left\lfloor \frac{8 + n}{6} \right\rfloor,$$

which yields the proposition since  $d(\mathcal{D}^\perp)$  is even.  $\square$

In [18] Rains proved more general bounds on the dual distance of doubly-even binary linear codes, without assuming that they contain the all-ones vector.

Length	Rains' bound	Our bound
$24\mu$	$4\mu + 4$	$4\mu$
$24\mu + 4$	$4\mu + 2$	$4\mu + 2$
$24\mu + 8$	$4\mu + 4$	$4\mu + 2$
$24\mu + 12$	$4\mu + 2$	$4\mu + 2$
$24\mu + 16$	$4\mu + 4$	$4\mu + 4$
$24\mu + 20$	$4\mu + 4$	$4\mu + 4$

With our additional assumption there is a substantial improvement in particular for lengths divisible by 24.

## 5. Weight enumerators: the non doubly-even case.

In this section we assume that  $\mathcal{D}$  is not doubly-even. We will use the following notation:

- $N := \frac{n}{2}$ ,  $2d := d(\mathcal{D}^\perp)$ ;
- $A(x, y) := W_{\mathcal{D}}(x, y) = \sum_{c \in \mathcal{D}} x^{n-\text{wt}(c)} y^{\text{wt}(c)} = x^{2N} + \sum_{i=d}^{N-d} a_i x^{2N-2i} y^{2i} + y^{2N}$  the weight enumerator of  $\mathcal{D}$ ;
- $D(x, y) := A\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) = \frac{1}{2}x^{2N} + \sum_{i=d}^{N-d} d_i x^{2N-2i} y^{2i} + \frac{1}{2}y^{2N}$ , so that  $2D$  is the weight enumerator of  $\mathcal{D}^\perp$ ;
- $B(x, y) := A(x, y) - D(x, y) = \frac{1}{2}x^{2N} + \sum_{i=d}^{N-d} b_i x^{2N-2i} y^{2i} + \frac{1}{2}y^{2N}$ ;

- $F(x, y) := B\left(\frac{x+y}{\sqrt{2}}, i\frac{x-y}{\sqrt{2}}\right) = \frac{1}{2} \left( W_{S(\mathcal{D})}(x, y) - W_{S(\mathcal{D})}\left(\frac{1+i}{\sqrt{2}}x, \frac{1-i}{\sqrt{2}}y\right) \right)$ , where  $S(\mathcal{D}) = \mathcal{D}_0^\perp - \mathcal{D}^\perp$  is the shadow of  $\mathcal{D}$ .

The polynomial  $B(x, y)$  is anti-invariant under the MacWilliams transformation  $H : (x, y) \mapsto 1/\sqrt{2}(x+y, x-y)$  and invariant under the transformation  $I : (x, y) \mapsto (x, -y)$ , so by [2, Lemma 3.2]

$$B(x, y) \in (x^4 - 6x^2y^2 + y^4) \cdot \mathbb{C}[x^2 + y^2, x^2y^2(x^2 - y^2)^2].$$

and we can write

$$B(x, y) = (x^4 - 6x^2y^2 + y^4) \cdot \sum_{i=0}^{\lfloor \frac{N-2}{4} \rfloor} e_i (x^2 + y^2)^{N-2-4i} (x^2y^2(x^2 - y^2)^2)^i \quad (2)$$

and, consequently,

$$F(x, y) = 2(x^4 + y^4) \cdot \sum_{i=0}^{\lfloor \frac{N-2}{4} \rfloor} e_i (2xy)^{N-2-4i} \left( -\frac{1}{4}x^8 + \frac{1}{2}x^4y^4 - \frac{1}{4}y^8 \right)^i. \quad (3)$$

Notice that (3) implies that the degrees of the monomials of  $F(x, y)$  are congruent to  $N - 2 \pmod{4}$ . Since

$$\begin{aligned} F(x, y) &= \frac{1}{2} \left( W_{S(\mathcal{D})}(x, y) - W_{S(\mathcal{D})}\left(\frac{1+i}{\sqrt{2}}x, \frac{1-i}{\sqrt{2}}y\right) \right) = \\ &= \frac{1}{2} \left( W_{S(\mathcal{D})}(x, y) - i^N W_{S(\mathcal{D})}(x, -iy) \right), \end{aligned}$$

it is easy to see that  $F(x, y)$  is the weight enumerator of the following set

$$\mathcal{S} := \{s \in S(\mathcal{D}) \mid \text{wt}(s) \equiv N - 2 \pmod{4}\}.$$

So the coefficients of  $F(x, y)$  are non-negative integers.

Then we get the following.

**Corollary 5.1.** *Let  $e_i$  be as in (2) and (3) and put  $\epsilon_i := (-1)^i 2^{N-1-6i} e_i$ . Then all  $\epsilon_i$  are non-negative integers.*

*Proof.* We have

$$F(1, y) = (1 + y^4)y^{N-2} \cdot \sum_{i=0}^{\lfloor \frac{N-2}{4} \rfloor} \epsilon_i y^{-4i} (1 - y^4)^{2i}.$$

with  $\epsilon_i := (-1)^i 2^{N-1-6i} e_i$ . Substitute  $\lfloor \frac{N-2}{4} \rfloor - i = h$ .

$$F(1, y) = y^{N-2-4\lfloor \frac{N-2}{4} \rfloor} (1+y^4)(1-y^4)^{2\lfloor \frac{N-2}{4} \rfloor} \cdot \sum_{h=0}^{\lfloor \frac{N-2}{4} \rfloor} \epsilon_{\lfloor \frac{N-2}{4} \rfloor - h} (y^4(1-y^4)^{-2})^h.$$

Let  $r := N - 2 - 4\lfloor \frac{N-2}{4} \rfloor$ . Note that  $r$  is the remainder of the division of  $N - 2$  by 4.

$$\begin{aligned} F(1, y) &= \sum_{j=0}^{2N} f_j y^j = f_0 + \dots + f_{r-1} y^{r-1} + y^r \sum_{j=r}^{2N} f_j y^{j-r} \\ &= y^r (1+y^4)(1-y^4)^{2\lfloor \frac{N-2}{4} \rfloor} \cdot \sum_{h=0}^{\lfloor \frac{N-2}{4} \rfloor} \epsilon_{\lfloor \frac{N-2}{4} \rfloor - h} (y^4(1-y^4)^{-2})^h. \end{aligned}$$

Then  $f_j = 0$  if  $j \not\equiv r \pmod{4}$ . Set  $Z = y^4$ . Then

$$\sum_k f_{4k+r} Z^k = (1+Z)(1-Z)^{2\lfloor \frac{N-2}{4} \rfloor} \cdot \sum_{h=0}^{\lfloor \frac{N-2}{4} \rfloor} \epsilon_{\lfloor \frac{N-2}{4} \rfloor - h} (Z(1-Z)^{-2})^h.$$

Put

$$f(Z) := (1+Z)^{-1} (1-Z)^{-2\lfloor \frac{N-2}{4} \rfloor}, \quad g(Z) := Z(1-Z)^{-2}.$$

Then there are coefficients  $\gamma_{h,k}$  such that

$$Z^k f(Z) = \sum_{h=0}^{\lfloor \frac{N-2}{4} \rfloor} \gamma_{h,k} g(Z)^h.$$

Since  $g(0) = 0$  and  $g'(0) \neq 0$ , we can apply the Bürmann-Lagrange theorem (see [19, Lemma 8]) to obtain

$$\gamma_{h,k} = [\text{coeff. of } Z^{h-k} \text{ in } (1-Z)^{-1-2\lfloor \frac{N-2}{4} \rfloor+2h}] = \binom{2\lfloor \frac{N-2}{4} \rfloor - h - k}{h-k} > 0.$$

In particular

$$\epsilon_{\lfloor \frac{N-2}{4} \rfloor - h} = \sum_{k=0}^{\lfloor \frac{h-r}{4} \rfloor} \gamma_{h,k} f_{4k+r}$$

is a non-negative integer for all  $h$ . □



**Proposition 5.2.** *If  $\mathcal{D}$  is not doubly-even and  $n \equiv 0, 2, 4, 6, 8, 10, 12, 14 \pmod{24}$  then  $d(\mathcal{D}^\perp) \leq 4\mu + 2$ .*

*Proof.* We have that

$$\begin{aligned} B(1, Y) &= 1/2 + \sum_{j=d}^{N-d} b_j Y^j + 1/2 Y^N \\ &= (1 - 6Y + Y^2)(1 + Y)^{N-2} \cdot \sum_{i=0}^{\lfloor \frac{N-2}{4} \rfloor} e_i (Y(1 - Y)^2(1 + Y)^{-4})^i. \end{aligned}$$

Let

$$f(Y) := (1 - 6Y + Y^2)^{-1}(1 + Y)^{2-N}, \quad g(Y) := Y(1 - Y)^2(1 + Y)^{-4}.$$

As before we find coefficients  $\alpha_i(N)$  such that

$$f(Y) = \sum_{i=0}^{\lfloor \frac{N-2}{4} \rfloor} \alpha_i(N) g(Y)^i.$$

Then, for  $i < d$ ,

$$e_i = \frac{1}{2} \alpha_i(N).$$

Since  $g(0) = 0$  and  $g'(0) \neq 0$ , we can apply the Bürmann-Lagrange theorem, in the version of [19, Lemma 8], to compute

$$\alpha_i(N) = \text{coeff. of } Y^i \text{ in } \frac{Yg'(Y)}{g(Y)} f(Y) \left( \frac{Y}{g(Y)} \right)^i =: \star$$

We compute

$$\star = (1 + Y)^{1-N+4i} (1 - Y)^{-2i-1} = (1 - Y^2)^{-2i-1} (1 + Y)^{2+6i-N}.$$

As  $(1 - Y^2)^{-2i-1}$  is a power series in  $Y^2$  with positive coefficients, we see that  $\alpha_i(N)$  is positive if  $2 + 6i - N > 0$ , so if  $i > \frac{N-2}{6}$ . For  $i < d$  we know that  $\alpha_i(N) = 2e_i = (-1)^i 2^{-N+2+6i} \epsilon_i$  where  $\epsilon_i$  is a non-negative integer, so  $\alpha_i(N)$  is not positive for odd  $i < d$ .

Write  $N = 12\mu + \rho$  with  $0 \leq \rho \leq 7$  and assume that  $d > 2\mu + 1$ . Then  $\alpha_{2\mu+1} > 0$  because  $6(2\mu + 1) + 2 - (12\mu + \rho) = 8 - \rho > 0$  which is a contradiction. We conclude that  $d \leq 2\mu + 1$  for  $\rho = 0, 1, 2, 3, 5, 6, 7$ .  $\square$

We aim to find an analogous result to Proposition 4.1 for semi self-dual codes of length  $24\mu$ . So we need to find the bound  $\text{dd}(\mathcal{D}) \leq 4\mu$  also for not doubly even semi-self dual codes  $\mathcal{D}$  of length  $24\mu$ . For certain values of  $\mu$ , we may show that some coefficient of  $F(x, y)$  is not integral.

**Proposition 5.3.** *If  $\mathcal{D}$  is not doubly-even and  $n = 24\mu$  with  $\binom{5\mu-1}{\mu-1}$  odd then  $\text{d}(\mathcal{D}^\perp) \leq 4\mu$ .*

*Proof.* With the notations used above, we get

$$\begin{aligned} \alpha_{2\mu}(12\mu) &= \text{coeff. of } Y^{2\mu} \text{ in } (1 - Y^2)^{-4\mu-1}(1 + 2Y + Y^2) \\ &= \text{coeff. of } Z^\mu \text{ in } (1 - Z)^{-4\mu-1} + \text{coeff. of } Z^{\mu-1} \text{ in } (1 - Z)^{-4\mu-1} \\ &= \binom{5\mu}{\mu} + \binom{5\mu-1}{\mu-1} = 6 \binom{5\mu-1}{\mu-1}. \end{aligned}$$

On the other hand, assuming that  $\text{d}(\mathcal{D}^\perp) \geq 4\mu + 2$ , we have

$$\alpha_{2\mu}(12\mu) = 2\epsilon_{2\mu} = 2^2\epsilon_{2\mu}.$$

As  $\epsilon_{2\mu}$  is a non-negative integer, we get that  $\binom{5\mu-1}{\mu-1}$  is even.  $\square$

It seems to be impossible to obtain the same bound for the other values of  $\mu$  by just looking at weight enumerators. For  $\mu = 5$  (the first value for which  $\binom{5\mu-1}{\mu-1}$  is even), we get examples of  $\{e_i\}$  for which  $F(x, y)$  has non-negative integer coefficients and  $B(1, y) = 1/2 + O(y^{22})$ . From one of these we computed  $W_{\mathcal{D}}(1, y) = 1 + O(y^{22})$ ,  $W_{\mathcal{D}^\perp}(1, y) = 1 + O(y^{22})$  and  $W_{S(\mathcal{D})}(1, y) = O(y^{18})$ , all with non-negative integer coefficients.

## Acknowledgements

Both authors are indebted to the Dipartimento di Matematica e Applicazioni, Università degli Studi di Milano-Bicocca, and the Lehrstuhl D für Mathematik, RWTH Aachen University, for hospitality and excellent working conditions, while this paper has mainly been written.

This paper is partially in the PhD thesis [4] of the first author who expresses his deep gratitude to his supervisors Francesca Dalla Volta and Massimiliano Sala.

- [1] C. Aguilar Melchor, P. Gaborit, *On the classification of extremal [36, 18, 8] binary self-dual codes*, IEEE Trans. Inform. Theory **54** (2008) 4743–4750.

- [2] C. Bachoc, *On harmonic weight enumerators of binary codes*, Des. Codes Cryptogr. **18** (1999) 11–28.
- [3] C. Bachoc, P. Gaborit, *Designs and self-dual codes with long shadows*, J. Combin. Theory A **105** (2004) 15–34.
- [4] M. Borello, *Automorphism groups of self-dual binary linear codes with a particular regard to the extremal case of length 72*, PhD Thesis, Università degli studi di Milano-Bicocca 2014.
- [5] M. Borello, W. Willems, *Automorphisms of order  $2p$  in binary self-dual extremal codes of length a multiple of 24*, IEEE Trans. Inform. Theory **59** (2013) 3378–3383.
- [6] M. Borello, *The automorphism group of a self-dual  $[72, 36, 16]$  binary code does not contain elements of order 6*, IEEE Transactions on Information Theory **58** (2012) 7240–7245.
- [7] M. Borello, *The automorphism group of a self-dual  $[72, 36, 16]$  code is not an elementary abelian group of order 8*, Finite Fields and Their Applications **25** (2014) 1–7.
- [8] M. Borello, F. Dalla Volta and G. Nebe, *The automorphism group of a self-dual  $[72, 36, 16]$  code does not contain  $\mathcal{S}_3$ ,  $\mathcal{A}_4$  or  $D_8$* , Advances in Mathematics of Communications **7** (2013) 503–510.
- [9] S. Bouyuklieva, *On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length  $24m$* , Des. Codes Cryptogr. **25** (2002) 5–13.
- [10] S. Bouyuklieva, J. de la Cruz and W. Willems, *On the automorphism group of a binary self-dual  $[120, 60, 24]$  code*, Appl. Algebra Engrg. Comm. Comput. **24** (2013), 201–214.
- [11] S. Bouyuklieva, W. Willems, and N. Yankov, *On the Automorphisms of Order 15 for a Binary Self-Dual  $[96, 48, 20]$  Code*, arXiv:1403.4735 (2014).
- [12] L. Chouinard, *Projectivity and relative projectivity over group rings*, J. Pure and Applied Algebra **7** (1976) 278–302.

- [13] J.H. Conway and V. Pless, *On primes dividing the group order of a doubly-even (72; 36; 16) code and the group order of a quaternary (24; 12; 10) code*, Discrete Mathematics **38** (1982) 143–156.
- [14] A. Günther and G. Nebe, *Automorphisms of doubly even self-dual binary codes*, Bulletin of the London Mathematical Society **41** (2009) 769–778.
- [15] C.L. Mallows and N.J.A. Sloane, *An upper bound for self-dual codes*, Inf. Control **22** (1973) 188–200.
- [16] A. Munemasa, *Database of binary self-dual codes*, Online available.
- [17] G. Nebe, *An extremal [72, 36, 16] binary code has no automorphism group containing  $Z_2 \times Z_4$ ,  $Q_8$ , or  $Z_{10}$* , Finite Fields and their applications **18** (2012) 563–566.
- [18] E.M. Rains, *Bounds for Self-Dual Codes Over  $Z_4$* , Finite Fields and Their Applications **6** (2000) 146–163.
- [19] E.M. Rains, *Shadow bounds for self-dual codes*, IEEE Trans. Inform. Theory **44** (1998) 134–139.
- [20] N.J.A. Sloane, *Is there a (72; 36)  $d = 16$  self-dual code?*, IEEE Trans. Inform. Theory **2** (1973) 251.
- [21] V. Yorgov and D. Yorgov, *The Automorphism Group of a Self-Dual [72, 36, 16] Code Does Not Contain  $Z_4$* , IEEE Trans. Inform. Theory **60** (2014) 3302–3307.
- [22] S. Zhang, *On the nonexistence of extremal self-dual codes*, Discrete Appl. Math. **91** (1999) 277–286.