On the dual distance of semi self-dual codes.

Martino Borello and Gabriele Nebe

January 24, 2014

Abstract

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 $C$ be an extremal self-dual binary linear code of length $24m$ and $\sigma \in \text{Aut}(C)$ 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 $C$ is a free $F_2(\sigma)$-module.

1 Introduction

A binary self-orthogonal code $D \subseteq D^\perp \leq F_2^n$ of length $n$ is called semi self-dual, if $1 := (1, \ldots, 1) \in D$ and $\dim(D^\perp/D) = 2$. 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 $c \in D$. Hence already the condition that $1 \in D$ implies that the length $n$ of $D$ is even. Note that $D^\perp \subseteq 1^\perp = \{c \in F_2^n \mid \text{wt}(c) \in 2\mathbb{Z}\}$ implies that also the dual code of $D$ consists of even weight vectors. The dual distance of $D$ is the minimum weight of the dual code $\text{dd}(D) := d(D^\perp) := \min(\text{wt}(D^\perp \setminus \{0\}))$.

Applying the methods from [10], we show the following main theorem.

Theorem 1.1. Let $D \leq F_2^n$ be a semi self-dual code. Then the dual distance of $D$ is bounded by

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

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

$$\text{dd}(D) = d(D^\perp) \leq 4\mu.$$
Theorem 1.1 follows by combining Remark 2.1 Proposition 3.1 Proposition 4.2 and Proposition 4.3.

Remark 1.2. The well-known Kummer’s theorem on binomial coefficients implies that \((\frac{5\mu-1}{\mu-1})\) 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 of all self-dual binary linear codes of length up to 40, we get the following.

Remark 1.3. There exist 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 \([22, 12, 6]\). So the bound is reached for \(n \equiv 4, 6, 8, 10, 12, 14, 16, 18, 20, 22 \pmod{24}\). There exists a doubly-even semi self-dual code with dual code of parameters \([24, 13, 4]\). So the bound is reached for \(n \equiv 0 \pmod{24}\) in the doubly-even case.

The research in this paper is part of the PhD thesis of the first author. It is motivated by the study of automorphisms of order 2 of extremal self-dual codes of length a multiple of 24.

Let \(m \in \mathbb{N}\) and \(C = C^\perp \leq \mathbb{F}_2^{24m}\) be an extremal binary self-dual code, so \(d(C) = 4m + 4\). Then \(C\) is doubly even \((\text{10})\). 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 \([11]\), 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 \(\text{Aut}(C) = \{\sigma \in S_{24m} | \sigma(C) = C\}\) has order \(\leq 5\) (see \([4]\) for an exposition of this result). Stefka Bouyuklieva \([6]\) studies automorphisms of order 2 of such codes. She shows that if \(C\) is an extremal code of length 24m, \(m \geq 2\) and \(\sigma \in \text{Aut}(C)\) has order 2, then the permutation \(\sigma\) has no fixed points, with one exception, \(m = 5\), where there might be 24 fixed points. If \(\sigma = (1, 2) \ldots , (24m - 1, 24m)\) is a fixed point free automorphism of a doubly even self-dual code \(C\), then its fixed code \(C(\sigma) := \{c \in C | \sigma(c) = c\}\) is isomorphic to

\[\pi(C(\sigma)) = \{(c_1, \ldots, c_{12m}) \in \mathbb{F}_2^{12m} | (c_1, c_1, c_2, c_2, \ldots, c_{12m}, c_{12m}) \in C\}\]

and such that

\[\pi(\{c + \sigma(c) | c \in C\}) = \pi(C(\sigma))^\perp \subseteq \pi(C(\sigma)).\]

As \(C\) is doubly-even, all words in \(\pi(C(\sigma))\) have even weight. It is shown in \([9]\) and \([5]\) that the code \(C\) is a free \(\mathbb{F}_2(\sigma)\)-module, if and only if \(\pi(C(\sigma))\) is self-dual. If \(\pi(C(\sigma))\) is not self-dual then it contains the dual \(D^\perp\) of a semi self-dual code, so \(2m + 2 \leq d(\pi(C(\sigma))) \leq d(D^\perp)\).

So Theorem 1.1 implies the following

Corollary 1.4. Let \(C = C^\perp \leq \mathbb{F}_2^{24m}\) be an extremal code of length 24m and \(\sigma \in \text{Aut}(C)\) be a fixed point free automorphism of order 2. Then \(C\) is a free \(\mathbb{F}_2(\sigma)\)-module if \(m\) is odd or if \(m = 2\mu\) with \((\frac{5\mu-1}{\mu-1})\) odd.

In particular we obtain \([9]\) Theorem 3.1] without appealing to the classification of all extremal codes of length 36 in \([11]\).
2 Self-dual subcodes

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

**Remark 2.1.** There are exactly three self-dual codes \( C_i = C_i^\perp \) \((i \in \{1, 2, 3\})\) with \( D \subset C_1, C_2, C_3 \subset D^\perp \).

From the bound on \( d(C_i) \) given in \([10, \text{Theorem 5}]\) we obtain

\[
dd(D) = d(D^\perp) \leq d(C_1) \leq \begin{cases} 
4\mu + 6 & \text{if } n \equiv 22 \pmod{24} \\
4\mu + 4 & \text{otherwise}
\end{cases}
\]

We aim to find a better bound.

3 Shadows: the doubly-even case

**Proposition 3.1.** If \( D \) is doubly-even, then

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

**Proof.** Since every doubly-even binary linear code is self-orthogonal, \( D^\perp \) cannot be doubly-even and so in \( D^\perp \) there exists a codeword of weight \( w \equiv 2 \pmod{4} \). Thus we can take \( D < F = F^\perp < D^\perp \) with \( F \) not doubly-even, so that \( D = F_0 := \{ f \in F \mid \text{wt}(f) \equiv 0 (\pmod{4}) \} \) is the maximal doubly-even subcode of \( F \).

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

\[
2d(F) + d(S(F)) \leq 4 + \frac{n}{2} \tag{1}
\]

Note that \( d(D^\perp) = \min\{d(F), d(S(F))\} \), since \( D^\perp = S(F) \cup F \). Since we have the bound \([3]\), the maximum for \( \min\{d(F), d(S(F))\} \) is reached if

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

so that

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

which yields the proposition since \( d(D^\perp) \) is even. \(\square\)
4 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:

- $N := \frac{n}{2}, 2d := d(\mathcal{D}^\perp)$;
- $A(x, y) := W_D(x, y) = \sum_{c \in \mathcal{D}} x^{n - wt(c)} y^{wt(c)} = x^{2N} + \sum_{i=d}^{N-d} a_i x^{2N-2i} y^{2i} + y^{2N}$ 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 $\mathcal{D}^\perp$;
- $B(x, y) := A(x, y) - D(x, y) = \frac{1}{2} x^{2N} + \sum_{i=d}^{N-d} b_i x^{2N-2i} y^{2i} + \frac{1}{2} y^{2N}$;
- $F(x, y) := B \left( \frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}} \right) = \frac{1}{2} \left( W_{S(\mathcal{D})}(x, y) - W_{S(\mathcal{D})} \left( \frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}} y \right) \right)$, where $S(\mathcal{D}) = \mathcal{D}_0^\perp - \mathcal{D}_1^\perp$ 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

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

(2)

and, consequently,

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

(3)

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

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

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

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

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

Then we get the following.
Corollary 4.1. Let $e_i$ be as in (2) and (3) and put $\epsilon_i := (-1)^i2^{N-1-6i}e_i$. 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 $\epsilon_i := (-1)^i2^{N-1-6i}e_i$. 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.

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

Then $f_j = 0$ if $j \not\equiv r \mod 4$. 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 Bürmann-Lagrange theorem (see [10, Lemma 8]) to obtain

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

In particular

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

is a non-negative integer for all $h$. □
Proposition 4.2. If $D$ is not doubly-even and $n \equiv 0, 2, 4, 6, 8, 10, 12, 14 \mod 24$ then $d(D^\perp) \leq 4\mu + 2$

Proof. We have that

$$B(1,Y) = 1/2 + \sum_{j=d}^{N-d} b_j Y^j + 1/2 Y^N =$$

$$(1 - 6Y + Y^2)(1 + Y)^{N-2} \sum_{i=0}^{[N/2]} e_i (Y(1-Y)^2(1+Y)^{-4})^i$$

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

$$f(Y) = \sum_{i=0}^{[N/2]} \alpha_i(N) g(Y)^i.$$ 

Then, for $i < d$,

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

Since $g(0) = 0$ and $g'(0) \neq 0$, we can apply Bürmann-Lagrange theorem, in the version of [10, Lemma 8], to compute

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

We compute

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

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 $\rho = 0, 1, 2, 3, 5, 6, 7$. \hfill \Box

We aim to find an analogous result to Proposition 3.1 for semi-self-dual codes of length $24\mu$. So we need to find the bound $d(d(D)) \leq 4\mu$ also for not doubly even semi-self dual codes $D$ of length $24\mu$. For certain values of $\mu$, we may show that some coefficient of $F(x, y)$ is not integral.
Proposition 4.3. If $D$ is not doubly-even and $n = 24\mu$ with $\binom{5\mu-1}{\mu-1}$ odd then $d(D^\perp) \leq 4\mu$.

Proof. With the notations used above, we get

\[ \alpha_{2\mu}(12\mu) = \text{coeff. of } Y^{2\mu} \text{ in } (1 - Y^2)^{-4\mu-1}(1 + 2Y + Y^2) = \]
\[ = \text{coeff. of } Z^\mu \text{ in } (1 - Z)^{-4\mu-1} + \text{coeff. of } Z^{\mu-1} \text{ in } (1 - Z)^{-4\mu-1} = \]
\[ = \binom{5\mu}{\mu} + \binom{5\mu-1}{\mu-1} = 6\binom{5\mu-1}{\mu-1} \]

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

\[ \alpha_{2\mu}(12\mu) = 2e_{2\mu} = 2^2\epsilon_{2\mu}. \]

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

It seems to be impossible to obtain the same bound for the other values of $\mu$ 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 $W_D(1, y) = 1 + O(y^{22})$, $W_{D^\perp}(1, y) = 1 + O(y^{27})$ and $W_{S(D)}(1, y) = O(y^{18})$, 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.

References

[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] 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.

[7] P. Gaborit, *A bound for certain s-extremal lattices and codes*, Archiv der Mathematik **89** (2007) 143-151.

[8] A. Munemasa, *Database of binary self-dual codes*, Online available.

[9] G. Nebe, *An extremal [72, 36, 16] binary code has no automorphism group containing $\mathbb{Z}_2 \times \mathbb{Z}_4$, $Q_8$, or $\mathbb{Z}_{10}$*, Finite Fields and their applications **18** (2012) 563–566.

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

[11] N.J.A. Sloane, *Is there a (72; 36) d = 16 self-dual code?*, IEEE Trans. Inform. Theory **2** (1973) 251.