On the Doubly-Even Self-Dual Codes of Length 96

Radinka Dontcheva

Abstract—We prove that 23, 11, and 7 do not divide the order of the automorphism group of a binary [96, 48, 16] doubly-even self-dual code. We construct 25 new inequivalent binary [96, 48, 16] doubly-even self-dual codes via an automorphism of order 23.

Index Terms—Automorphisms, doubly-even self-dual codes, weight enumerators.

I. INTRODUCTION

An \([n, k]\) linear code \(C\) over the binary field \(F_2\) is a \(k\)-dimensional subspace of \(F_2^n\), where \(F_2^n\) is the \(n\)-dimensional vector space. The weight of a vector in \(F_2^n\) is the number of its nonzero coordinates. The \emph{minimum distance} \(d\) of \(C\) is the minimum weight of its nonzero codewords and \(\overline{C}\) is called an \([n, k, d]\) code.

For every \(u \equiv (u_1, u_2, \ldots, u_n)\), \(v = (v_1, v_2, \ldots, v_n) \in F_2^n\),

\(u \cdot v = u_1v_1 + u_2v_2 + \cdots + u_nv_n \in F_2\)

defines the inner product in \(F_2^n\).

The dual code of code \(C\) is \(C^\perp = \{v \in F_2^n : u \cdot v = 0 \text{ for all } u \in C\}\).

If \(C \subseteq C^\perp, C\) is called self-orthogonal and if \(C = C^\perp, C\) is self-dual.

A doubly-even code is a binary code in which the weight of every vector is divisible by four. Self-dual doubly-even code exists only when the length \(n\) is a multiple of eight and its minimum distance \(d\) satisfies \(d \leq 4\lfloor \frac{n}{8} \rfloor + 4\) (see [5]). If \(d = 4\lfloor \frac{n}{8} \rfloor + 4, C\) is called extremal.

For a permutation \(\sigma\) of \(n\) elements and \(v = (v_1, v_2, \ldots, v_n) \in F_2^n\), we define

\(v\sigma = (v_{\sigma^{-1}(1)}, v_{\sigma^{-1}(2)}, \ldots, v_{\sigma^{-1}(n)})\).

The binary code \(C\) and its image \(C\sigma\) are called equivalent. If \(C = C\sigma\) then the permutation \(\sigma\) is an \emph{automorphism} of \(C\). The set of all automorphisms of the code \(C\) forms the automorphism group of the code \(C\).

A list of the possible weight enumerators for extremal self-dual codes of length from 72 to 100 was given by Dougherty, Gulliver, and Harada in [2]. The existence of a binary [96, 48, 20] self-dual doubly-even code is still unknown.

In [11], Shiterev, Yorgov, and Ziapkov proved that a binary [96, 48, 20] self-dual doubly-even code cannot have automorphisms of order 17 and 31. Bouyuklieva shows that the same code cannot have an automorphism of order 2 with \(f\)-fixed points for \(f > 0\) (see [11]).

The largest minimum distance for a known [96, 48] self-dual doubly-even code is 16. The first example of a [96, 48, 16] code was found by Feit in [3].

We use the method for constructing binary self-dual codes with an automorphism of an odd prime order developed by Huffman and Yorgov in [4], [9] and [10]. In Section II, for completeness, we
describe the method and prove that a binary [96, 48, 20] self-dual doubly-even code cannot have an automorphism of order 23, 11, or 7. In Section III, we present 25 new binary [96, 48, 16] self-dual doubly-even codes.

II. DESCRIPTION OF THE METHOD AND GENERAL RESULTS

Let C be a binary \([n, n/2, d]\) self-dual doubly-even code with an automorphism \(\sigma\) of an odd prime order \(p\) with \(c\) cycles and \(f\) fixed points in its decomposition. In short, we say that \(\sigma\) is of type \(p^{c} \cdot f\).

Let \(\Omega_1, \Omega_2, \ldots, \Omega_c\) be the cycles and \(\Omega_{c+1}, \Omega_{c+2}, \ldots, \Omega_{c+f}\) be the fixed points of \(\sigma\). Denote \(F_\sigma(C) = \{ v \in C | \sigma(v) = v \}\) and

\[E_\sigma(C) = \{ v \in C | \text{wt}(v/\Omega_i) \equiv 0 \pmod{2}, i = 1, \ldots, c + f \}\]

where \(v/\Omega_i\) is the restriction of \(v\) on \(\Omega_i\).

**Lemma 1 [4]:** If the code \(C\) is self-dual then \(C = F_\sigma(C) \oplus E_\sigma(C)\) (\(\oplus\) denotes the internal direct sum) and \(\dim_{F_\sigma} E_\sigma(C) = \frac{p^{c} \cdot f}{\phi}\). If \(F\) is a primitive root (mod \(p\)) then \(c\) is even.

By Lemma 1, a generator matrix of the code \(C\) can be represented in the form

\[
\begin{bmatrix}
A & 0 \\
X & Y
\end{bmatrix}
\]

\[
\begin{bmatrix}
\text{cycles} \\
\text{fixed points}
\end{bmatrix}
\]

\[
\begin{bmatrix}
\text{gen}(E_\sigma(C)) \\
\text{gen}(F_\sigma(C))
\end{bmatrix}
\]

Denote the map \(\pi: F_\sigma(C) \rightarrow F_2^{c+f}\), defined by \(\pi(v/\Omega_i) = v_j\) for some \(j \in \Omega_i, i = 1, 2, \ldots, c + f\). It is known that \(\pi(F_\sigma(C))\) is a binary \([c + f, \frac{p^{c} \cdot f}{\phi}, \frac{p^{c} \cdot f}{2\phi}]\) self-dual code [4]. Every vector of length \(p\) is identified by a polynomial in the factor-ring \(F_2[x]/(x^{p} - 1)\), namely, \((v_0, v_1, \ldots, v_{p-1})\) corresponds to \(v_0 + v_1x + \cdots + v_{p-1}x^{p-1}\). Let \(P\) be the set of even-weight polynomials in \(F_2[x]/(x^{p} - 1)\). It is known that \(P\) is a cyclic code of length \(p\) generated by \(x - 1\).

By \(E_\sigma(C)^+\) the code \(E_\sigma(C)\) with the last \(f\) coordinates deleted. For \(v \in E_\sigma(C)^+\) we can consider each \(v/\Omega_i = (v_0, v_1, \ldots, v_{p-1})\) as a polynomial

\[
\varphi(v/\Omega_i)(x) = v_0 + v_1x + \cdots + v_{p-1}x^{p-1}
\]

in \(P, i = 1, 2, \ldots, c\). In this way we define the map \(\varphi: E_\sigma(C)^+ \rightarrow P^c\). It is known [4] that \(\varphi(E_\sigma(C)^+)\) is a submodule of the \(P\)-module \(P^c\) and for each \(u, v \in \varphi(E_\sigma(C)^+)\) it holds (see [9])

\[
u(u(x)v(x)^{-1}) + u_2(x)v_2(x^{-1}) + \cdots + u_c(x)v_c(x^{-1}) = 0.
\]

Let

\[
x^p - 1 = (x - 1)h_1(x)h_2(x)\cdots h_s(x)
\]

where \(h_j(x)\) is an irreducible polynomial in \(P\) for \(j = 1, 2, \ldots, s\). Thus, \(P = I_1 \oplus I_2 \oplus \cdots \oplus I_s\), where \(I_j = \langle \frac{p^{c} \cdot f}{\phi} \rangle\) for \(j = 1, 2, \ldots, s\) is an irreducible cyclic code and

\[
M_j = \{ u \in \varphi(E_\sigma(C)^+) | u_i \in I_j, i = 1, 2, \ldots, s \}
\]

is a code over the field \(I_j\) for \(j = 1, 2, \ldots, s\). It is proved in [9] that \(\varphi(E_\sigma(C)^+) = M_1 \oplus M_2 \oplus \cdots \oplus M_s\) and \(\dim \varphi(E_\sigma(C)^+) = \frac{p^{c} \cdot f}{2}\).

**Lemma 2 [9]:** Suppose that \(C\) has an automorphism of type \(p^{c} \cdot f\). The following transformations lead to an equivalent code:

i) a permutation of the first \(c\) cycles of \(C\);

ii) a permutation of the last \(f\) coordinates of \(C\);

iii) a multiplication of the \(j\)th coordinate of \(\varphi(E_\sigma(C)^+)\) by \(x^j_i\), where \(j_i\) is an integer, \(1 \leq j_i \leq p - 1\) for \(j = 1, 2, \ldots, c\);

iv) a substitution \(x \rightarrow x^j\) for \(j = 1, 2, \ldots, p - 1\) in \(\varphi(E_\sigma(C)^+)\).

Let \(C\) be a binary [96, 48, 20] self-dual doubly-even code with an automorphism \(\sigma\) of type \(p^{c} \cdot f\). The only possibilities for \(p^{c} \cdot f\) are as follows: \(23 \cdot (4, 4), 11 \cdot (8, 8), 7 \cdot (12, 12), 7 \cdot (13, 5), 5 \cdot (16, 16), 5 \cdot (18, 6), 3 \cdot (24, 24), 3 \cdot (26, 18), 3 \cdot (30, 6), \) and \(3 \cdot (32, 0)\) [11].

The weight enumerator of the code \(C\) is uniquely determined in [2]

\[
W(y) = 1 + 3217056y^{20} + 369844580y^{24} + 18642839520y^{28} + \cdots + 422069980215y^{2^{16}} + 4552866656416y^{2^{17}} + \cdots
\]

(2)

In what follows, we prove that the maximal possible odd prime order of the automorphism of \(C\) is \(5\).

**Proposition 1:** A self-dual doubly-even [96, 48, 20] code \(C\) cannot have an automorphism of order 23.

**Proof:** Suppose \(C\) has an automorphism \(\sigma\) of order 23. Then, \(\sigma\) is of type \(23 \cdot (4, 4)\) and \(\pi(F_\sigma(C))\) is a binary \([8, 4]\) self-dual code. Such codes are only \(A_8\) or \(C_4^2\) (see [6]) with generator matrices

\[
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 0
\end{bmatrix}
\]

and

\[
\begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

Let \(\pi(F_\sigma(C)) = A_8\). Since the automorphism group of \(A_8\) is 3-transitive, without loss of generality (w.l.o.g.) we may assume that the last three positions in \(\text{gen}(A_8)\) are fixed under \(\sigma\). The forth fixed point can be selected among the first five columns. It is easy to see that in any case the code \(F_\sigma(C)\) will contain a vector of weight 4 or 26. This eliminates \(A_8\).

If \(\pi(F_\sigma(C)) = C_4^2\) then we may choose the generator matrix of \(F_\sigma(C)\) in the form

\[
\begin{bmatrix}
\text{cycles} \\
\text{fixed points}
\end{bmatrix}
\]

\[
\begin{bmatrix}
a & 1 & 0 & 0 & 0 \\
a & 0 & 1 & 0 & 0 \\
a & 0 & 0 & 1 & 0 \\
a & 0 & 0 & 0 & 1
\end{bmatrix}
\]

(3)

where \(a\) is the all-one vector of length 23 and nonindicated entries are equal to zero.

Since \(x^{23} - 1 = (x - 1)h_1(x)h_2(x)\), where

\[
h_1(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1
\]

\[
h_2(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1
\]
are irreducible polynomials over \( F_2 \), it follows that \( P = I_1 \oplus I_2 \),
\( I_j \equiv \left\{ \frac{2^j - 1}{4} \right\} \) for \( j = 1, 2 \). Hence \( \varphi(E_{\alpha}(C)^\perp) = M_1 \oplus M_2 \) and 
\[ \dim \varphi(E_{\alpha}(C)^\perp) = 4 \]

Denote 
\[ \delta_j(x) = \frac{x^{2^j - 1}}{h_j(x)} \quad \text{for } j = 1, 2. \]

Then \( I_j = \{ 0, \delta_j(x)[k] \mid k = 0, 1, \ldots, 2^{11} - 2 \} \) for \( j = 1, 2 \). The multiplicative order of \( \delta_j(x) \) is \( 2^{11} - 1 = 23 \times 89 \) and we can write \( \delta_j(x) = x \alpha_j(x) \), where the multiplicative order of \( \alpha_j(x) \) is 89 for \( j = 1, 2 \). The idempotents of \( I_1 \) and \( I_2 \) are 
\[ e_1(x) = x^{22} + x^{21} + x^{20} + x^{19} + x^{17} + x^{15} + x^{14} \]
\[ + x^{11} + x^{10} + x^7 + x^3 + 1 \]
and \( e_2(x) = e(x) - e_1(x) \), where \( e(x) = x^{22} + x^{21} + \cdots + x \) is the identity of \( P \).

We have \( \dim M_1 + \dim M_2 = \dim \varphi(E_{\alpha}(C)^\perp) = 4 \). Applying transformations i), iii), and a multiplication with a nonzero element of \( I_1 \) we obtain the generator matrix of \( M_1 \) in the form \( [I|G] \), where \( I \) is the identity matrix, \( G \) is a matrix with elements from \( I_1 \). Thus, \( \dim M_1 = 2 \) or 3 and the generator matrix of \( M_1 \) can be chosen in the form 
\[ L_1 = \begin{pmatrix} e_1 & 0 & 0 & \alpha_1^3(x) \\ 0 & e_1 & 0 & \alpha_2^3(x) \\ 0 & 0 & e_1 & \alpha_3^3(x) \end{pmatrix} \]
where \( t_1 = 0, 1, \ldots, 88 \) for \( l = 1, 2, 3 \).

\[ L_2 = \begin{pmatrix} e_1 & 0 & 0 & \alpha_1^3(x) \\ 0 & e_1 & 0 & \alpha_2^3(x) \\ 0 & 0 & e_1 & \alpha_3^3(x) \end{pmatrix} \]

or 
\[ L_3 = \begin{pmatrix} e_1 & 0 & 0 & \alpha_1^3(x) \\ 0 & e_1 & 0 & \alpha_2^3(x) \\ 0 & 0 & e_1 & \alpha_3^3(x) \end{pmatrix} \]

where \( t_1 = 0, 1, \ldots, 88 \) for \( l = 1, 2, 3, 4 \) and \( k = 0, 1, \ldots, 22 \).

Denote
\[ \alpha_1(x) = x^{20} + x^{17} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^7 + x^3 + x + 1. \]

Applying the substitution \( x \rightarrow x^2 \) to the row vector \( (e_1(x), 0, *, \alpha_1^3(x)) \) for \( t_1 = 0, 1, \ldots, 88 \) we can limit its choice to the set of vectors:
\[ \{ (e_1(x), 0, *, e_1(x)), (e_1(x), 0, *, \alpha_1(x)), (e_1(x), 0, *, \alpha_1^3(x)), (e_1(x), 0, *, \alpha_2^3(x)), (e_1(x), 0, *, \alpha_3^3(x)), (e_1(x), 0, *, \alpha_1^3(x)), (e_1(x), 0, *, \alpha_1^3(x)) \} \]

where * is any element of \( I_1 \). By transformation i) and a multiplication with a nonzero element of \( I_1 \) we can reduce the above set to the following set
\[ \{ (e_1(x), 0, *, e_1(x)), (e_1(x), 0, *, \alpha_1(x)), (e_1(x), 0, *, \alpha_3^3(x)), (e_1(x), 0, *, \alpha_3^3(x)), (e_1(x), 0, *, \alpha_3^3(x)) \}. \]

Therefore, it is sufficient to consider only generator matrices of \( M_1 \) in the form 
\[ L_1' = \begin{pmatrix} e_1 & 0 & 0 & \alpha_1^3(x) \\ 0 & e_1 & 0 & \alpha_2^3(x) \\ 0 & 0 & e_1 & \alpha_3^3(x) \end{pmatrix} \]
Next we recall the notions of a duo and a cluster. A **duo** is any set of two coordinate positions of a code. A **cluster** is a set of disjoint duos such that the union of any two duos is support of a weight-1 vector of the code.

Any weight-1 vector of \( \pi(F_n(C)) \) generates a vector of \( F_n(C) \) with weight in the set \{4, 10, 16, 22, 28\}. Only the last value is possible. Suppose \( \pi(F_n(C)) = H_{18} \). Clearly, the sets

\[
M_1 = \{\{1, 2\}, \{3, 4\}, \{5, 6\}\}
\]

and

\[
M_2 = \{\{7, 8\}, \{9, 10\}, \{11, 12\}\}
\]

are clusters for \( H_{18} \) or every 18 positions cannot be fixed. There are five fixed points by \( \pi \) and this excludes \( H_{18} \).

Consider \( \pi(F_n(C)) = I_{18} \). The sets

\[
M_3 = \{\{13, 14\}, \{15, 16\}, \{17, 18\}\}
\]

are clusters for \( H_{18} \) and hence only two positions (11th and 18th) can be fixed.

Therefore, a binary [96, 48, 20] self-dual doubly-even code cannot have an automorphism of type 7-(13, 5).

Assume now that \( C \) has an automorphism of type 7-(12, 12). Then, \( \pi(F_n(C)) \) is a binary [24, 12] self-dual code.

It is proved in [8] that a generator matrix of a self-dual \([n, n/2]\) code can be chosen in the form

\[
\begin{pmatrix}
A & 0 \\
0 & B \\
D & E
\end{pmatrix}
\]

(7)

where \( A, B, D, \) and \( E \) are matrices of types \( k_1 \times n_1, k_2 \times n_2, k_3 \times n_1 \), and \( k_3 \times n_2 \), respectively. Matrices \( D \) and \( E \) do not have zero rows and also \( k_1 + k_2 + k_3 = n/2 \) and \( k_2 = k + k_1 - n_1 \).

Consider a generator matrix of \( \pi(F_n(C)) \) in the form (7), where \( A, B, D, \) and \( E \) are matrices of types \( k_1 \times 12, k_2 \times 12, k_3 \times 12, \) and \( k_3 \times 12 \). Then \( k_1 + k_2 + k_3 = 12 \) and \( k_2 = 12 + k_1 = 12 \). Hence \( k_1 = k_2 \).

Obviously, the matrix \( B \) must generate a \([12, k_2, d_1]\) code with \( d_1 \geq 20 \). It follows that \( k_2 = 0 \) and also \( k_1 = 0 \).

A weight-1 vector of \( \pi(F_n(C)) \) generates only weight-28 vector of \( F_n(C) \) and then \( k_1 = 0 \). Therefore, \( \pi(F_n(C)) \) cannot have a weight-1 vector. Hence, \( \pi(F_n(C)) \) is either \([24, 12, 6]\) or \([24, 12, 8]\) self-dual code. Up to equivalence, the extended Golay \([24, 12, 8]\) code \( G_{24} \) and the \([24, 12, 6]\) code \( Z_{24} \) are unique (see [7]). A computer check shows that if \( \pi(F_n(C)) \) is either \( G_{24} \) or \( Z_{24} \) then the code \( F_n(C) \) contains a vector of weight less than 20 or a vector of a weight not divisible by 4. Hence, the code \( C \) cannot have an automorphism of type 7-(12, 12) either.
III. New [96, 48, 16] Self-Dual Doubly-Even Codes

Let $D$ be a [96, 48, 16] self-dual doubly-even code. The weight enumerator for the code $D$ is given in [2] and it is

$$W(y) = 1 + (−2808+α)y^{10} + (3666+423−16α)y^{20} + (3664+7456+120α)y^{21} + \cdots.$$  (8)

The first such code was found by Feit [3] and it has a weight enumerator (8) for $α = 37722$. Recently, Dougherty, Gulliver, and Harada [2] found four new inequivalent [96, 48, 16] self-dual doubly-even codes for $α = \{37584; 37500; 37524; 37598\}$.

Here we consider 25 new codes via an automorphism of order 23. Consider a [96, 48, 16] code $D$ possessing an automorphism of order 23 with four cycles and four fixed points. We choose the generator matrix of $F_α(D)$ in the form

$$\text{gen}(F_α(D)) = \begin{pmatrix}
  a & 1 & 0 & 0 & 0 \\
  a & 0 & 1 & 0 & 0 \\
  a & 0 & 0 & 1 & 0 \\
  a & 0 & 0 & 0 & 1 
\end{pmatrix}$$

where $a$ is the all-one vector of length 23 and where nonindicated entries are equal to zero (as $\text{gen}(F_α(C))$ from (3)).

We have $F_α(D)^\ast$ = $M_1 \oplus M_2$ and $\dim M_1 = 3$ or 2. Hence, the generator matrix of $M_1$ can have the forms (4)–(6).

Applying the orthogonality condition (1), we obtain the corresponding generator matrices for $M_2$. In this way, we obtain a generator matrix of the code $D$ in the form

$$\begin{pmatrix}
a & 1 & 0 & 0 & 0 \\
a & 0 & 1 & 0 & 0 \\
a & 0 & 0 & 1 & 0 \\
a & 0 & 0 & 0 & 1 \\
u & w_1 & 0 & 0 & 0 \\
u & w_2 & 0 & 0 & 0 \\
u & w_3 & 0 & 0 & 0 \\
w_4 & w_5 & w_6 & v & 0 & 0 & 0 
\end{pmatrix}$$

and

$$\begin{pmatrix}
a & 1 & 0 & 0 & 0 \\
a & 0 & 1 & 0 & 0 \\
a & 0 & 0 & 1 & 0 \\
a & 0 & 0 & 0 & 1 \\
u & r_1 & r_2 & 0 & 0 & 0 \\
u & r_3 & r_4 & 0 & 0 & 0 \\
r_5 & r_6 & v & 0 & 0 & 0 \\
r_7 & r_8 & v & 0 & 0 & 0 
\end{pmatrix}$$

where $a$ is the all-one vector of length 23, nonindicated entries are equal to zero, and the cells $u, v, w_i$ for $i = 1, \ldots, 6$, and $r_j$ for $j = 1, \ldots, 8$ are $11 \times 23$ circulant matrices.

<table>
<thead>
<tr>
<th>Code</th>
<th>$r_5$</th>
<th>$r_6$</th>
<th>$r_7$</th>
<th>$r_8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_{96,23}$</td>
<td>92FC8A</td>
<td>92FC8A</td>
<td>92FC8A</td>
<td>92FC8A</td>
</tr>
<tr>
<td>$D_{96,24}$</td>
<td>5E1FA0</td>
<td>77EC02</td>
<td>FACCA0</td>
<td></td>
</tr>
</tbody>
</table>

The author wishes to thank the referees for their detailed remarks and Prof. S. Dodunekov for helpful discussions.

REFERENCES