On the Automorphisms of Order 15 for a Binary Self-Dual \([96, 48, 20]\) Code

Stefka Bouyuklieva  
Faculty of Mathematics and Informatics,  
Veliko Tarnovo University, 5000 Veliko Tarnovo, Bulgaria  
stefka@uni-vt.bg

Wolfgang Willems  
Otto-von-Guericke Universität, Magdeburg, Germany  
willems@ovgu.de

Nikolay Yankov  
Faculty of Mathematics and Informatics,  
Shumen University, Bulgaria  
jankov_niki@yahoo.com

Abstract

The structure of binary self-dual codes invariant under the action of a cyclic group of order \(pq\) for odd primes \(p \neq q\) is considered. As an application we prove the nonexistence of an extremal self-dual \([96, 48, 20]\) code with an automorphism of order 15 which closes a gap in [2].

Index Terms: Self-dual codes, doubly-even codes, automorphisms

1 Introduction

Let \(C = C^\perp\) be a binary self-dual code of length \(n\) and minimum distance \(d\). A binary code is doubly-even if the weight of every codeword is divisible by four. Self-dual doubly-even codes exist only if \(n\) is a multiple of eight. Rains [9] proved that the minimum distance \(d\) of a binary self-dual \([n, k, d]\) code satisfies the following bound:

\[
d \leq 4\lfloor n/24 \rfloor + 4, \quad \text{if } n \not\equiv 22 \pmod{24},
\]

\[
d \leq 4\lfloor n/24 \rfloor + 6, \quad \text{if } n \equiv 22 \pmod{24}.
\]

Codes achieving this bound are called extremal. If \(n\) is a multiple of 24, then a self-dual code meeting the bound must be doubly-even [9]. Moreover, for any nonzero weight \(w\) in such a code, the codewords of weight \(w\) form a 5-design [1]. This is one reason why extremal codes of length \(24m\) are of particular interest. Unfortunately, only for \(m = 1\)

1
and \( m = 2 \) such codes are known, namely the \([24,12,8]\) extended Golay code and the \([48,24,12]\) extended quadratic residue code (see [10]). To date the existence of no other extremal code of length \( 24m \) is known. For \( n = 96 \), only the primes 2, 3 and 5 may divide the order of the automorphism group of the extremal code and the cycle structure of prime order automorphisms are as follows

\[
\begin{array}{c|c|c}
 p & \text{number of } p\text{-cycles} & \text{number of fixed points} \\
2 & 48 & 0 \\
3 & 30, 32 & 6, 0 \\
5 & 18 & 6 \\
\end{array}
\]  

(see Theorem, part a) in [2]). We would like to mention here that in part b) of the Theorem (the case where elements of order 3 are acting fixed point freely) four orders of possible automorphism groups are missing, namely 15, 30, 240 and 480. The gap is due to the fact that the existence of elements of order 15 with six cycles of length 15 and two cycles of length 3 are not excluded in the given proof. We close this gap by proving

**Theorem 1** A binary doubly-even \([96,48,20]\) self-dual code with an automorphism of order 15 does not exist.

This note consists of three sections. Section 2 is devoted to some theoretical results on binary self-dual codes invariant under the action of a cyclic group. In Section 3 we study the structure of a putative extremal self-dual \([96,48,20]\) code having an automorphism of order 15. Using this structure and combining the possible subcodes we prove Theorem [1].

In an additional section, namely Section 4, we prove that an extremal self-dual code of length 96 does not have automorphisms of type 3-(28,12). This assertion is used by other authors but no proof has been published so far.

## 2 Theoretical results

Let \( C \) be a binary linear code of length \( n \) and let \( \sigma \) be an automorphism of \( C \) of order \( r \) where \( r \) is odd (not necessarily a prime). Let

\[
\sigma = \Omega_1 \Omega_2 \ldots \Omega_m
\]

be the factorization of \( \sigma \) into disjoint cycles (including the cycles of length 1). If \( l_i \) is the length of the cycle \( \Omega_i \) then \( \text{lcm}(l_1, \ldots, l_m) = r \) and \( l_i \) divides \( r \). Therefore \( l_i \) is odd for \( i = 1, \ldots, m \) and \( 1 \leq l_i \leq r \).

Let \( F_\sigma(C) = \{ v \in C : v \sigma = v \} \) and

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

where \( v|\Omega_i \) is the restriction of \( v \) on \( \Omega_i \). With this notation we have the following.

**Theorem 2** The code \( C \) is a direct sum of the subcodes \( F_\sigma(C) \) and \( E_\sigma(C) \).
Corollary 5

If $\sigma$ of type 3

Proof: Let $C$ be a product of cycles of length 3, 5, $t_3$ cycles of length 3 and $f$ cycles of length 1. Then $\sigma^5$ and $\sigma^3$ are automorphisms of $C$ of type 3\(-5c + t_3, 5t_5 + f\) and 5\(-3c + t_3, 3t_3 + f\), respectively. According to \([1]\),

$$3c + t_5 = 18,$$
$$3t_3 + f = 6,$$
$$5c + t_3 = 30 \text{ or } 32,$$
$$5t_5 + f = 6 \text{ or } 0.$$
This leads to
\[ t_5 = 0, \ c = 6, \ (t_3, f) = (2, 0) \text{ or } (0, 6). \]

Suppose that \( f = 6 \). In this case \( C_\pi \) is a self-dual code of length 12. According to [8] there are three codes up to equivalence, namely \( B_{12}, C_2^6 \) and \( C_2 \oplus A_8 \). The code \( C_\pi \cong B_{12} \) has a generator matrix of shape

\[
G_\pi = \begin{pmatrix}
100000 & 100011 \\
010000 & 010111 \\
001000 & 001111 \\
000100 & 000111 \\
000010 & 000111 \\
000001 & 111110 \\
000001 & 111101
\end{pmatrix}.
\]

But then \( C \) contains vectors of weight \( 15 + 3 = 18 \) which contradicts its minimum distance. The other two types can obviously not occur since its minimum distance is 2. Hence \( f = 6 \) is not possible. Thus if \( C \) has an automorphism \( \sigma \) of order 15, then \( \sigma \) has six cycles of length 15 and two cycles of length 3. \( \square \)

**Corollary 6** If \( C \) is a binary extremal self-dual \([96, 48, 20]\) code with an automorphism \( \sigma \) of order 15, then \( C_\pi \) is the extended \([8, 4, 4]\) Hamming code.

**Proof**: Let \( C \) be a binary extremal self-dual \([96, 48, 20]\) code with an automorphism \( \sigma \) of order 15. According to the previous corollary, we may assume that

\[ \sigma = \Omega_1 \Omega_2 \Omega_3 \Omega_4 \Omega_5 \Omega_6 \Omega_7 \Omega_8, \]

where \( \Omega_i = (15(i - 1) + 1, \ldots, 15i) \) for \( i = 1, \ldots, 6 \), \( \Omega_7 = (91, 92, 93) \), \( \Omega_8 = (94, 95, 96) \). Hence \( C_\pi \) is a binary self-dual code of length 8. If \( x = (x_1, \ldots, x_8) \in C_\pi \) then \( \text{wt}(\pi^{-1}(x)) = 15(x_1 + \cdots + x_6) + 3x_7 + 3x_8 \equiv 3\text{wt}(x) \pmod{4} \). Since \( C \) is a doubly-even code, \( \text{wt}(x) \equiv 0 \pmod{4} \) and \( C_\pi \) must be a doubly-even code, too. The only doubly-even self-dual code of length 8 is the extended \([8, 4, 4]\) Hamming code. \( \square \)

### 2.1 Connections with quasi-cyclic codes

For further investigations, we need two theorems concerning the theory of finite fields and cyclic codes. Let \( r \) be a positive integer coprime to the characteristic of the field \( \mathbb{F}_l \), where \( l \) is the power of a prime. Consider the factor ring \( R = \mathbb{F}_l[x]/(x^r - 1) \), where \( (x^r - 1) \) is the principal ideal in \( \mathbb{F}_l[x] \) generated by \( x^r - 1 \). Let

\[ x^r - 1 = f_0(x)f_1(x) \ldots f_s(x) \]

be the factorization of \( x^r - 1 \) into irreducible factors \( f_i(x) \) over \( \mathbb{F}_l \) where \( f_0(x) = x - 1 \). Let \( I_j = (x^r - 1)_{f_j(x)} \) be the ideal of \( R \) generated by \( \frac{x^r - 1}{f_j(x)} \) for \( j = 0, 1, \ldots, s \). Finally, by \( e_j(x) \) we denote the generator idempotent of \( I_j \); i.e., \( e_j(x) \) is the identity of the two-sided ideal \( I_j \). With these notations we have the following well-known result.
Theorem 7 (see [5])

(i) \( \mathcal{R} = I_0 \oplus I_1 \oplus \cdots \oplus I_s \).

(ii) \( I_j \) is a field which is isomorphic to the field \( \mathbb{F}_{r^{deg(f_j(x))}} \) for \( j = 0, 1, \ldots, s \).

(iii) \( e_i(x)e_j(x) = 0 \) for \( i \neq j \).

(iv) \( \sum_{j=0}^t e_j(x) = 1. \)

According to [7] there is a decomposition

\[
x^r - 1 = g_0(x)g_1(x) \cdots g_m(x)h_1(x)h_1^*(x) \cdots h_t(x)h_t^*(x),
\]

where \( s = m + 2t \) and \( \{g_0, g_1, \ldots, g_m, h_1, h_1^*, \ldots, h_t, h_t^*\} = \{f_0, f_1, \ldots, f_s\} \). Furthermore, \( h_i^*(x)\) is the reciprocal polynomial of \( h_i(x) \), \( h_i^* \neq h_i \) for \( i = 1, \ldots, t \) and \( g_i(x) \) coincides with its reciprocal polynomial where \( g_0(x) = f_0(x) = x - 1 \). Finally, we denote the field \( (\frac{x^r-1}{g_j(x)}) \) by \( G_j \) for \( j = 0, 1, \ldots, m \), \( (\frac{x^r-1}{h_j(x)}) \) by \( H_j \) for \( j = 1, \ldots, t \), and \( (\frac{x^r-1}{h_j^*(x)}) \) by \( H_j^* \) for \( j = 1, \ldots, t \).

To continue the investigations, we need to prove some properties of binary linear codes of length \( cr \) with an automorphism \( \tau \) of order \( r \) which has \( c \) independent \( r \)-cycles. If \( C \) is such a code then \( C \) is a quasi-cyclic code of length \( cr \) and index \( c \). Next we define a map \( \phi : \mathbb{F}_2^c \rightarrow \mathcal{R}^c \) by

\[
\phi(v) = (v_0(x), v_1(x), \ldots, v_{c-1}(x)) \in \mathcal{R}^c,
\]

where \( v_i(x) = \sum_{j=0}^{c-1} v_j \cdot j \) and \( v_{0}, v_{1}, \ldots, v_{c-1} = v_i |_{\Omega} \). Clearly, \( \phi(C) \) is a linear code over the ring \( \mathcal{R} \) of length \( c \). Moreover, according to [7], we have \( \phi(C) = \phi(C^\perp) \) where the dual code \( C^\perp \) over \( \mathbb{F}_2 \) is taken under the Euclidean inner product, and the dual code \( \phi(C)^\perp \) in \( \mathcal{R}^c \) is taken with respect to the following Hermitian inner product:

\[
\langle u, v \rangle = \sum_{i=0}^{c-1} u_i \overline{v}_i \in \mathcal{R}^c, \quad \overline{v}_i = v_i(x^{-1}) = v_i(x^{r-1}).
\]

In particular, the quasi-cyclic code \( C \) is self-dual if and only if \( \phi(C) \) is self-dual over \( \mathcal{R} \) with respect to the Hermitian inner product.

Every linear code \( C \) over the ring \( \mathcal{R} \) of length \( c \) can be decomposed as a direct sum

\[
C = \bigoplus_{i=0}^{m} C_i \oplus \bigoplus_{j=1}^{t} (C_j' \oplus C_j'^\perp),
\]

where \( C_i \) is a linear code over the field \( G_i \) \( i = 0, 1, \ldots, m \), \( C_j' \) is a linear code over \( H_j \) and \( C_j'^\perp \) is a linear code over \( H_j^* \) \( j = 1, \ldots, t \).

**Theorem 8 (see [7])** A linear code \( C \) over \( \mathcal{R} \) of length \( c \) is self-dual with respect to the Hermitian inner product, or equivalently a \( c \)-quasi-cyclic code of length \( cr \) over \( \mathbb{F}_q \) is self-dual with respect to the Euclidean inner product, if and only if

\[
C = \bigoplus_{i=0}^{m} C_i \oplus \bigoplus_{j=1}^{t} (C_j' \oplus (C_j'^\perp)),
\]

where \( C_i \) is a self-dual code over \( G_i \) for \( i = 0, 1, \ldots, m \) of length \( c \) (with respect to the Hermitian inner product) and \( C_j' \) is a linear code of length \( c \) over \( H_j \) and \( (C_j')^\perp \) is its dual with respect to the Euclidean inner product for \( 1 \leq j \leq t \).
2.2 The case \( r = pq \)

We consider now the case \( r = pq \) for different odd primes \( p \) and \( q \) such that 2 is a primitive root modulo \( p \) and modulo \( q \). The ground field is \( \mathbb{F}_2 \). Then

\[
x^r - 1 = (x - 1)Q_p(x)Q_q(x)Q_r(x) = (1 + x)(1 + x + \cdots + x^{p-1})(1 + x + \cdots + x^{q-1})Q_r(x)
\]

where \( Q_i(x) \) is the \( i \)-th cyclotomic polynomial. Moreover, both \( Q_p(x) \) and \( Q_q(x) \) are irreducible over \( \mathbb{F}_2 \) since 2 is primitive modulo \( p \) and \( q \) as well. Finally, if

\[
Q_r(x) = g_3(x) \cdots g_s(x)h_1(x)h_1^c(x) \cdots h_t(x)h_t^c(x)
\]

is the factorization of the \( r \)-th cyclotomic polynomial into irreducible factors over \( \mathbb{F}_2 \), then these factors have the same degree, namely \( \frac{\phi(r)}{s-2+2t} = \frac{(p-1)(q-1)}{s-2+2t} \), where \( \phi \) is Euler’s phi function.

Let

\[
\sigma = \Omega_1 \cdots \Omega_c \Omega_{c+1} \cdots \Omega_{c+t_q} \Omega_{c+t_q+1} \cdots \Omega_{c+t_q+t_p} \Omega_{c+t_q+t_p+1} \cdots \Omega_{c+t_q+t_p+f}
\]

where

\[
\Omega_i = ((i-1)r + 1, \ldots, ir) \text{ are cycles of length } pq \text{ for } i = 1, \ldots, c,
\]

\[
\Omega_i = (cr + (i-1)q + 1, \ldots, cr + iq) \text{ are cycles of length } q \text{ for } i = c+1, \ldots, c+t_q,
\]

\[
\Omega_i = (cr + tqq + (i-1)p + 1, \ldots, cr + tqq + ip) \text{ are cycles of length } p
\]
for \( i = c + t_q + 1, \ldots, c + t_q + t_p \), and

\[
\Omega_{c+t_q+t_p+i} = (c + t_q + t_p + i) \text{ are the fixed points for } i = 1, \ldots, f.
\]

Let \( E_\sigma(C)^* \) be the shortened code of \( E_\sigma(C) \) obtained by removing the last \( t_qq + t_pq + f \) coordinates from the codewords having 0’s there. Let \( C_\phi = \phi(E_\sigma(C)^*) \). Since \( E_\sigma(C)^* \) is a binary quasi-cyclic code of length \( cr \) and index \( c \), \( C_\phi \) is a linear code over the ring \( \mathcal{R} \) of length \( c \). Moreover

\[
C_\phi = \bigoplus_{i=0}^m M_i \oplus \bigoplus_{j=1}^t (M_j' \oplus M_j'''),
\]

where \( M_i \) is a linear code over the field \( G_i \), \( i = 1, \ldots, m \), \( M_j' \) is a linear code over \( H_j \) and \( M_j''' \) is a linear code over \( H_j^4 \), \( j = 1, \ldots, t \). For the dimensions we have

\[
\dim E_\sigma(C)^* = \dim C_\phi = (p-1) \dim M_1 + (q-1) \dim M_2 + \frac{(p-1)(q-1)}{s-2+2t} \left( \sum_{i=3}^{s} \dim M_i + \sum_{j=1}^{t} (\dim M_j' + \dim M_j''') \right).
\]

Since \( E_\sigma(C)^* \) is a self-orthogonal code, \( C_\phi \) is also self-orthogonal over the ring \( \mathcal{R} \) with respect to the Hermitian inner product. This means that \( M_i \) are self-orthogonal codes of length \( c \) over \( G_i \) for \( i = 1, \ldots, m \) (with respect to the Hermitian inner product) and, for \( 1 \leq j \leq t \), we have \( M_j''' \subseteq (M_j')^\perp \) with respect to the Euclidean inner product. This forces \( \dim M_i \leq c/2 \) for \( i = 1, 2, \ldots, s \) and \( \dim M_j' + \dim M_j''' \leq c \). It follows that

\[
\dim E_\sigma(C)^* \leq (p-1) \frac{c}{2} + (q-1) \frac{c}{2} + \frac{(p-1)(q-1)}{s-2+2t} \left( (s-2) \frac{c}{2} + tc \right) = \frac{c(pq-1)}{2}. \tag{5}
\]
3 Self-dual [96, 48, 20] codes and permutations of order 15 with six 15-cycles and two 3-cycles

Under the above assumptions the parameters are \( n = 96, \; r = 15, \; c = 6, \; t_3 = 2, \) and \( t_5 = f = 0. \) Since

\[
x^{15} - 1 = (x - 1) (1 + x + x^2) (1 + x + x^2 + x^3 + x^4) (1 + x + x^4) (1 + x^3 + x^4),
\]

we obtain

\[
\dim E_\sigma(C)^* = 2 \dim M_1 + 4 \dim M_2 + 4 (\dim M' + \dim M'').
\]

According to the balance principle (see [2], [5] or [10]), the dimension of the subcode of \( C \) consisting of the codewords with 0's in the last six coordinates, is equal to 42 = 48 - 6. Since three of these codewords together with the zero vector belong to the fixed subcode \( F_\sigma(C) \), we have \( \dim E_\sigma(C)^* = 40 \). It follows that

\[
\dim M_1 = 2, \quad \dim M_2 = 3 \quad \text{and} \quad \dim M' + \dim M'' = 6.
\]

This means that

\[
C_\phi = M_1 \oplus M_2 \oplus M' \oplus M'',
\]

where \( M_1 \) is a Hermitian self-orthogonal \([6, 2, 2] \) code over the field \( G_1 \cong \mathbb{F}_4 \), \( M_2 \) is a Hermitian self-dual \([6, 3, d_2] \) code over \( G_2 \cong \mathbb{F}_{16} \), \( M' \) is a linear \([6, k', d'] \) code over \( H \cong \mathbb{F}_{16} \) and \( M'' = (M')^\perp \) is its dual with respect to the Euclidean inner product. If \( v \) is a codeword of weight \( t \) in \( M_2 \), \( M' \) or \( M'' \) then the vectors \( \phi^{-1}(v), \phi^{-1}(xv), \phi^{-1}(x^2v) \) and \( \phi^{-1}(x^3v) \) generate a binary code of dimension 4 and effective length 15t. It is a subcode of \( C \) and therefore its minimum distance should be at least 20. Since binary codes of length 30, dimension 4 and minimum distance \( \geq 20 \) do not exist [3], \( d_2 = 3 \) or 4, \( d' \geq 3 \) and the minimum distance of \( M'' \) is at least 3. In the following we list the three possible cases for \( M' \) and \( M'' \) where

\[
e = e(x) = x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x
\]

is the identity of the field \( H = \{ 0, e, xe, x^2e, \ldots, x^{14}e \} \).

1. \( M' \) is an MDS \([6, 2, 5] \) code and \( M'' \) is its dual MDS \([6, 4, 3] \) code. It is well known that any MDS \([n, k, n-k+1] \) code over \( \mathbb{F}_q \) is an \( n \)-arc in the projective geometry \( PG(k-1, q) \). There are exactly four inequivalent \([6, 2, 5] \) MDS codes over \( \mathbb{F}_{16} \) (their dual codes correspond to the 6-arcs in \( PG(3, 16) \)). We list here generator matrices of these codes:

\[
\begin{pmatrix}
e & 0 & e & e & e & e \\
0 & e & xe & x^2e & x^3e
\end{pmatrix}
\quad
\begin{pmatrix}
e & 0 & e & e & e & e \\
0 & e & xe & x^2e & x^4e
\end{pmatrix}
\quad
\begin{pmatrix}
e & 0 & e & e & e & e \\
0 & e & xe & x^3e & x^7e
\end{pmatrix}
\quad
\begin{pmatrix}
e & 0 & e & e & e & e \\
0 & e & xe & x^3e & x^{11}e
\end{pmatrix}
\]

7
2. $M'$ and $M''$ are both MDS $[6,3,4]$ codes. According to [6], there are 22 MDS codes with the needed parameters over $\mathbb{F}_{16}$ (they correspond to the 6-arcs in $PG(2,16)$). We consider generator matrices of these codes in the form
\[
\begin{pmatrix}
  e & 0 & 0 & e & e & e \\
  0 & e & 0 & e^{a_1} & e^{a_2} & e \\
  0 & 0 & e & e^{a_3} & e^{a_4} & e
\end{pmatrix}, \quad a_i \in \{1,2,\ldots,14\}, \ i = 1,2,3,4.
\]
Note that $a_i \geq 1$ for $i = 1,2,3,4$ since the minimum distance of $M'$ is 4. We calculated the weight distributions and the automorphism groups of $\phi^{-1}(M' \oplus M'')$ for all 22 codes $M'$. The results are listed in Table 1. Five of the binary codes have minimum distance 24, and six of them have minimum distance 20.

| Table 1: The $[90,24]$ codes in case 2 |
|-----------------------------------------|
| $(a_1, a_2, a_3, a_4)$ | $A_{16}$ | $A_{20}$ | $A_{24}$ | $A_{28}$ | $A_{32}$ | $A_{36}$ | $|\text{Aut}|$ |
|--------------------------|---------|---------|---------|---------|---------|---------|---------|
| $(1,2,2,1)$ | 270 | 0 | 5400 | 15840 | 195345 | 9941400 | 1440 |
| $(1,2,2,4)$ | 60 | 120 | 2730 | 18480 | 189885 | 952080 | 240 |
| $(1,2,2,5)$ | 15 | 30 | 2070 | 17535 | 187815 | 963480 | 30 |
| $(1,2,2,6)$ | 45 | 180 | 1935 | 17505 | 183015 | 975420 | 90 |
| $(1,2,2,8)$ | 45 | 0 | 2580 | 15660 | 188715 | 965040 | 240 |
| $(1,2,2,9)$ | 15 | 30 | 2130 | 17355 | 187575 | 965160 | 30 |
| $(1,2,3,1)$ | 30 | 120 | 2430 | 19650 | 192105 | 937200 | 120 |
| $(1,2,3,6)$ | - | - | 2325 | 16320 | 192585 | 953040 | 60 |
| $(1,2,3,7)$ | - | 60 | 1875 | 17955 | 189465 | 956220 | 30 |
| $(1,2,3,8)$ | - | - | 2145 | 17340 | 190185 | 956400 | 30 |
| $(1,2,3,12)$ | - | 60 | 1965 | 18060 | 187545 | 960120 | 60 |
| $(1,2,4,6)$ | - | 60 | 2040 | 17910 | 187485 | 959400 | 60 |
| $(1,2,5,7)$ | - | 90 | 1830 | 18390 | 186405 | 963900 | 30 |
| $(1,2,6,1)$ | 60 | 0 | 3090 | 17400 | 194205 | 941400 | 240 |
| $(1,2,9,1)$ | 30 | 120 | 2910 | 17250 | 196425 | 933840 | 120 |
| $(1,2,12,1)$ | 90 | 360 | 3240 | 23940 | 192825 | 909720 | 720 |
| $(1,3,2,6)$ | - | - | 2325 | 16320 | 192585 | 953040 | 60 |
| $(1,3,3,2)$ | - | 180 | 1665 | 18720 | 185625 | 960840 | 90 |
| $(1,3,7,2)$ | - | - | 2295 | 16830 | 191745 | 950040 | 180 |
| $(1,3,7,10)$ | - | 180 | 1755 | 18450 | 185265 | 963360 | 360 |
| $(1,3,11,8)$ | - | - | 2730 | 14100 | 197925 | 944760 | 600 |
| $(5,10,10,5)$ | 450 | 0 | 14580 | 16200 | 329625 | 507960 | 259200 |

3. $M'$ and $M''$ are both $[6,3,3]$ codes. We consider generator matrices of $M'$ in the form
\[
\begin{pmatrix}
  e & 0 & 0 & 0 & e & e \\
  0 & e & 0 & e & \beta_1 & \beta_2 \\
  0 & 0 & e & \beta_3 & \beta_4
\end{pmatrix}, \quad \beta_i \in H, \ i = 1,2,3,4,
\]
where $\beta_i = x^{b_i}e$, $b_i \in \{0,1,\ldots,14\}$, or $\beta_i = 0$, $i = 1,2,3,4$.

We calculated that there are 18 inequivalent $[6,3,3]$ codes $M'$ over $\mathbb{F}_{16}$ such that $d(\phi^{-1}(M' \oplus M'')) \geq 20$. The weight distributions and the automorphism groups of $\phi^{-1}(M' \oplus M'')$ for all 18 codes are listed in Table 2. Ten of the binary codes have minimum distance 24, and eight of them have minimum distance 20.
In the following $G_1$ is the field with four elements and identity
\[ e_1 = x + x^2 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14}, \]
and $G_2$ the field with 16 elements and identity
\[ e_2 = x + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{12} + x^{13} + x^{14}, \]
defined in the beginning of this section. Furthermore $\mu_2 = x^{11} + x^{10} + x^6 + x^5 + x + 1$ is a generator of $G_2$.

According to [12], there are two Hermitian self-dual $[6, 3, d \geq 3]$ codes over $\mathbb{F}_{16}$ up to the equivalence defined in the following way: Two codes are equivalent if the second one is obtained from the first one via a sequence of the following transformations:

- a substitution $x \rightarrow x^t$, $t = 2, 4, 8$;
- a multiplication of any coordinate by $x$;
- a permutation of the coordinates.

Their generator matrices are
\[
H_1 = \begin{pmatrix}
    e_2 & 0 & 0 & 0 & \mu_2^5 & \mu_2^{10} \\
    0 & e_2 & 0 & \mu_2^5 & \mu_2 & e \\
    0 & 0 & e_2 & \mu_2^{10} & e_2 & \mu_2^{10}
\end{pmatrix}, \quad H_2 = \begin{pmatrix}
    e_2 & 0 & 0 & e_2 & \mu_2^5 & \mu_2^5 \\
    0 & e_2 & 0 & e_2 & \mu_2 & \mu_2^5 \\
    0 & 0 & e_2 & e_2 & \mu_2^6 & \mu_2^5
\end{pmatrix}.
\]

We fix the $M' \oplus M''$ part of the generator matrix and consider all possible generator matrices for the $M_2$ part. Note that even if the matrices generate equivalent codes $M_2$ the
codes generated by $M' \oplus M'' \oplus M_2$ may not be equivalent. We consider the two possible matrices for the $M_2$ part under the products of the following maps: 1) a permutation $\tau \in S_6$ of the 15-cycle coordinates; 2) multiplication of each of the 6 columns by nonzero element of $F_6$; 3) automorphism of the field $(x \rightarrow x^{t}, t = 2, 4, 8)$. After computing all possible generator matrices we obtain exactly 675 inequivalent $[90, 36, 20]$ binary codes: 232 from the first matrix $H_1$, and 443 from the second $H_2$. These codes have automorphism groups of orders 15 (557 codes), 30 (111 codes), 45 (2 codes) and 90 (5 codes).

Next, we add the fixed subcode. According to Corollary 5, the code $\pi(F_\sigma(C))$ is equivalent to the extended Hamming $[8, 4, 4]$ code $H_8$. We need to choose two out of the eight coordinates in $H_8$ for the cycles of length 3. The automorphism group acts 2-transitively on the code, so we can take any pair of coordinates for these cycles. Then we consider all $6! = 720$ permutation of the 15-cycles that can lead to different subcodes. Only 47 of the constructed codes $\phi^{-1}(M' \oplus M'' \oplus M_2) \oplus F_\sigma(C)$ have minimum distance $d' = 20$ (we list the number of their codewords of weights 20 and 24 and the order of the automorphism groups in Table 3).

| $[96,40,20]$ codes | $A_{20}$ | $A_{24}$ | $|\text{Aut}|$ | $A_{20}$ | $A_{24}$ | $|\text{Aut}|$ | $A_{20}$ | $A_{24}$ | $|\text{Aut}|$ |
|---------------------|---------|---------|---------|---------|---------|---------|---------|---------|---------|
| $C_{96,40,1}$       | 48735   | 4206590 | 1620    | $C_{96,40,17}$ | 47925   | 4216010 | 540     | $C_{96,40,33}$ | 48045   | 4213610 | 540     |
| $C_{96,40,2}$       | 49545   | 4197410 | 1620    | $C_{96,40,18}$ | 48105   | 4213730 | 540     | $C_{96,40,34}$ | 48420   | 4209320 | 540     |
| $C_{96,40,3}$       | 47835   | 4217030 | 1620    | $C_{96,40,19}$ | 48600   | 4207760 | 540     | $C_{96,40,35}$ | 47760   | 4218160 | 540     |
| $C_{96,40,4}$       | 47940   | 4214900 | 540     | $C_{96,40,20}$ | 48420   | 4208120 | 540     | $C_{96,40,36}$ | 48780   | 4204760 | 540     |
| $C_{96,40,5}$       | 48045   | 4209530 | 540     | $C_{96,40,21}$ | 47325   | 4220810 | 540     | $C_{96,40,37}$ | 48510   | 4205050 | 540     |
| $C_{96,40,6}$       | 47805   | 4214480 | 540     | $C_{96,40,22}$ | 47595   | 4216070 | 540     | $C_{96,40,38}$ | 47490   | 4217720 | 540     |
| $C_{96,40,7}$       | 47265   | 4222490 | 540     | $C_{96,40,23}$ | 48345   | 4209650 | 540     | $C_{96,40,39}$ | 48330   | 4210100 | 1080    |
| $C_{96,40,8}$       | 48690   | 4240820 | 540     | $C_{96,40,24}$ | 47925   | 4213370 | 540     | $C_{96,40,40}$ | 47415   | 4221950 | 1080    |
| $C_{96,40,9}$       | 47265   | 4220450 | 540     | $C_{96,40,25}$ | 47835   | 4215110 | 540     | $C_{96,40,41}$ | 48315   | 4210550 | 540     |
| $C_{96,40,10}$      | 47580   | 4216520 | 540     | $C_{96,40,26}$ | 47790   | 4214780 | 540     | $C_{96,40,42}$ | 47490   | 4218740 | 540     |
| $C_{96,40,11}$      | 47565   | 4219370 | 1080    | $C_{96,40,27}$ | 49410   | 4200020 | 540     | $C_{96,40,43}$ | 49140   | 4201880 | 540     |
| $C_{96,40,12}$      | 48255   | 4212110 | 540     | $C_{96,40,28}$ | 48225   | 4210610 | 540     | $C_{96,40,44}$ | 48330   | 4212500 | 1080    |
| $C_{96,40,13}$      | 48555   | 4207190 | 540     | $C_{96,40,29}$ | 48360   | 4209920 | 540     | $C_{96,40,45}$ | 48870   | 4212860 | 1080    |
| $C_{96,40,14}$      | 48165   | 4211690 | 1080    | $C_{96,40,30}$ | 48600   | 4214000 | 1080    | $C_{96,40,46}$ | 47970   | 4213220 | 540     |
| $C_{96,40,15}$      | 48555   | 4206710 | 1080    | $C_{96,40,31}$ | 47775   | 4215230 | 540     | $C_{96,40,47}$ | 47925   | 4215050 | 1080    |
| $C_{96,40,16}$      | 48630   | 4205000 | 540     | $C_{96,40,32}$ | 49815   | 4194350 | 1620    |                   |         |         |         |

Next we add the $M_1$ part, that is a Hermitian self-orthogonal $[6, 2, 2]$ code over the field $G_1 \cong \mathbb{F}_4$. One can easily compute all such codes up to equivalence. There are exactly 4 inequivalent such codes with generator matrices

$$H_3 = \begin{pmatrix} 1 & 0 & e_1 & 0 & 0 & 0 \\ e_1 & 0 & e_1 & 0 & 0 & 0 \end{pmatrix}, \quad H_4 = \begin{pmatrix} 1 & 0 & e_1 & e_1 & e_1 & 0 \\ 0 & e_1 & e_1 & x e_1 & x^2 e_1 & 0 \end{pmatrix},$$

$$H_5 = \begin{pmatrix} 1 & 0 & e_1 & 0 & 0 & 0 \\ e_1 & 0 & e_1 & 0 & e_1 & 0 \end{pmatrix}, \quad H_6 = \begin{pmatrix} 1 & 0 & 0 & e_1 & e_1 & e_1 \\ 0 & e_1 & 0 & e_1 & 0 & e_1 \end{pmatrix}.$$

We fix the generator matrices of the 47 codes and consider the matrices $H_3, H_4, H_5, H_6$ under compositions of the following transformations: 1) a permutation $\tau \in S_6$ of the 15-cycle coordinates; 2) multiplication of each of the 6 columns by a nonzero element of.
G_1; 3) automorphism of the field \((x \rightarrow x^2)\). Thus we construct binary \([96, 44]\) codes. Our computations show that none of these codes has minimum distance \(d \geq 20\). This proves Theorem 1 which states that a binary doubly-even \([96, 48, 20]\) self-dual code with an automorphism of order 15 does not exist.

4 On the automorphism of type 3-(28, 12)

In this section we fill a gap in the literature caused by a missing proof on the nonexistence of an extremal self-dual code of length 96 having an automorphism of type 3-(28, 12). In paper [2], the authors used this assertion in their proof of the main theorem.

**Proposition 9** A binary doubly-even \([96, 48, 20]\) self-dual code with an automorphism of type 3-(28, 12) does not exist.

Proof: Suppose that \(C\) is a self-dual \([96, 48, 20]\) code and \(\sigma\) is an automorphism of \(C\) of type 3-(28,12). Then \(C_\pi\) is a self-dual \([40, 20, 8]\) code. Without loss of generality, we can take the last 12 coordinates for the fixed points. So \(C_\pi\) has a generator matrix of the form

\[
G_\pi = \begin{pmatrix} A & O \\ D & I_{12} \end{pmatrix},
\]

where \(A\) is an \(8 \times 28\) matrix which generates a doubly-even \([28, 8, \geq 8]\) code \(A\) with dual distance \(d_A^\perp \geq 3\). Using the MacWilliams equalities we see that the possible weight distribution for this code is

\[
W_\pi(y) = 1 + \lambda y^8 + (142 - 3\lambda - \mu)y^{12} + (95 + 3\lambda + 3\mu)y^{16} + (18 - \lambda - 3\mu)y^{20} + \mu y^{24},
\]

and the number of codewords of weight 3 in its dual code is \(\nu = 2\lambda - 2\mu - 4\).

Let us consider the partitioned weight enumerator \(A_{ij}\) for the code \(C_\pi\), where \(0 \leq i \leq 28\) and \(0 \leq j \leq 12\). We use the following restrictions:

\[
\begin{align*}
&\text{If } i + j \text{ is odd then } A_{ij} = 0. \\
&\text{If } 3i + j \not\equiv 0 \pmod{4} \text{ then } A_{ij} = 0. \\
&\text{If } 0 < i + j < 8 \text{ or } 32 < i + j < 40 \text{ then } A_{ij} = 0. \\
&\text{If } 0 < 3i + j < 20 \text{ or } 76 < 3i + j < 96 \text{ then } A_{ij} = 0. \\
&\text{If } A_{\bar{i}0} = \alpha_i, \text{ where } \{\alpha_i, i = 0, \ldots, 28\} \text{ is the weight distribution of } A, A_{3,11} = \nu. \\
&\text{If } A_{ij} = A_{28-i,12-j}, \text{ where } i = 0, \ldots, 28, j = 0, \ldots, 12.
\end{align*}
\]

Using the MacWilliams identities for coordinate partitions (see [11]) and the above restrictions, we obtain a system of linear equations which forces \(\lambda = -1\), a contradiction. \(\square\)
References

[1] E.F. Assmus and H.F. Mattson, New 5-designs *J. Combin. Theory* 6 (1969), 122-151.

[2] J. de la Cruz and W. Willems, *On extremal self-dual codes of length 96*, IEEE Trans. Inform. Theory 57 (2011), 6820-6823.

[3] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, [http://www.codetables.de](http://www.codetables.de).

[4] W.C. Huffman, *Automorphisms of codes with application to extremal doubly-even codes of length 48*, IEEE Trans. Inform. Theory 28 (1982), 511-521.

[5] W.C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge 2003.

[6] Gerzson Kéri, Tables for $n$-arcs and lists for complete $n$-arcs in $PG(r,q)$, [http://www.sztaki.hu/~keri/n-arcs/index.htm](http://www.sztaki.hu/~keri/n-arcs/index.htm).

[7] San Ling and Patrick Solé, On the algebraic structure of quasi-cyclic codes I: Finite fields, *IEEE Trans. Inform. Theory* 47 (2001), 2751-2760.

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

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

[10] E. M. Rains and N. J. A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Elsevier, Amsterdam, 1998, pp. 177-294.

[11] J. Simonis, *MacWilliams identities and coordinate partitions*, Linear Algebra Appl. 216 (1995) 81-91.

[12] V. Yorgov and N. Yankov, On the extremal binary codes of lengths 36 and 38 with an automorphism of order 5, Proceedings of the fifth int. workshop ACCT, Sozopol, Bulgaria, 1996, pp. 307-312.