Self-dual codes with an automorphism of order 17

Müberra Gürel\textsuperscript{1,*} and Nikolay Yankov\textsuperscript{2}

\textsuperscript{1}Safir Company Haznedar Mah. Menderes Cad. No:5/B, Gungoren, Istanbul, Turkey
\textsuperscript{2}Faculty of Mathematics and Informatics, Shumen University, Bulgaria, Shumen, 9700, Bulgaria

Received October 19, 2015; accepted November 17, 2015

Abstract. In this paper, we study optimal binary self-dual codes with minimum distance 12 having an automorphism of order 17. We prove that all such codes have parameters $[68 + f, 34 + f/2, 12], \ f = 0, 2, 4$ and an automorphism of type $17 - (4, f), \ f = 0, 2, 4$ and provide a full classification of these codes. This classification gives new values $\beta = 17, 153, 170, 187, 221, 255$ for $\gamma = 0$ in the weight enumerator $W_{68,2}$ of $[68, 34, 12]$ codes; new values $\beta = 102, 136, 170, 204, 238, 272, 306, 340, 374, 408, 442, 476, 510, 544, 578, 612$ for $\gamma = 0$ in $W_{70,1}$ of $[70, 35, 12]$ codes; and numerous singly-even and doubly-even $[72, 36, 12]$ codes with new parameters in their weight enumerators.

AMS subject classifications: 94B05
Key words: automorphism, classification, self-dual code

1. Introduction

The largest possible minimum weights of singly even self-dual codes of lengths up to 72 are determined in [3]. Rains [16] proved that the minimum distance $d$ of a binary self-dual $[n, k, d]$ code satisfies the following bound:

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

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

Codes achieving this bound are called extremal.

We say that a code $C$ of length $n$ has an automorphism $\sigma$ of type $p - (c, f)$ for a prime $p$ if $\sigma$ has exactly $c$ independent $p$-cycles and $f = n - cp$ fixed points in its decomposition.

Neil Sloane (see [18]) asked a question which is still unanswered: is there a self-dual doubly-even $[72, 36, 16]$ code? The non-existence of such a code with an automorphism of order 17 was proven by V. Pless and J. Thompson in [15], but it is still unknown how many doubly-even $[72, 36, 12]$ codes exist.

The self-dual codes of length 68 are of special interest to researchers for the fact that such a code with $d = 12$ and a specific weight enumerator is related to a putative self-dual $[70, 35, 14]$ code linked to the doubly-even $[72, 36, 16]$ self-dual code. This connection is explained in details by Dougherty et al. in [6].

*Corresponding author. Email addresses: muberragurel@hotmail.com (M. Gürel), jankovniki@yahoo.com (N. Yankov)

http://www.mathos.hr/mcc ©2016 Department of Mathematics, University of Osijek
All extremal and optimal self-dual codes are classified up to length 50 [19]. In [17], Russeva proved that a unique self-dual [36, 18, 8] code with an automorphism of order 17 exists. In [11], Huffman presented a survey of the status of the classification of binary self-dual codes. Also in [11, Table 2], the cases of binary self-dual codes of lengths 68 and 70 with an automorphism of order 17 with 4 cycles are listed as open. The extremal pure double circulant singly even codes of length 68, studied in [7], have an automorphism group of order 68. Therefore [68, 34, 12] self-dual codes with an automorphism of order 17 do exist. In [7], the total of 23 codes with $|\text{Aut}(C)| = 68$ were constructed.

This paper is organized as follows. In Section 2, we will introduce the construction method used in this paper. In Section 3, we classify all Hermitian [6, 3, $\geq 3$] codes over a finite field with $2^{10}$ elements. Finally, in Section 4 using the codes from Section 3, we classify all binary self-dual [68 + f, 34 + f/2, 12] codes with an automorphism of type 17 – (4, f) for $f = 0, 2, 4$.

2. Construction method

Let C be a binary self-dual code of length $n$ with an automorphism $\sigma$ of prime order $p \geq 3$ with exactly $c$ independent $p$-cycles and $f = n - cp$ fixed points in its decomposition. We may assume that

$$\sigma = (1, 2, \ldots, p)(p + 1, p + 2, \ldots, 2p) \cdots (p(c - 1) + 1, p(c - 1) + 2, \ldots, pc)$$ \hspace{1cm} (1)

and concisely that $\sigma$ is of type $p - (c, f)$.

Denote the cycles of $\sigma$ by $\Omega_1, \Omega_2, \ldots, \Omega_c$, and the fixed points by $\Omega_{c+1}, \ldots, \Omega_{c+f}$. Let $F_\sigma(C) = \{v \in C \mid \forall \omega \in v\}$ and $E_\sigma(C) = \{v \in C \mid \text{wt}(v|\Omega_i) \equiv 0 \pmod{2}, i = 1, \ldots, c+f\}$, where $v|\Omega_i$ is the restriction of $v$ on $\Omega_i$.

**Theorem 1** (see [10]). The self-dual code $C$ is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$, and these subcodes have dimensions $\frac{c+f}{2}$ and $\frac{c(p-1)}{2}$, respectively.

Thus each choice of the codes $F_\sigma(C)$ and $E_\sigma(C)$ determines a self-dual code $C$. So for a given length $n$, all self-dual codes with an automorphism $\sigma$ can be obtained.

We have that $v \in F_\sigma(C)$ iff $v \in C$ and $v$ is constant on each cycle. Let $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$ be the projection map where if $v \in F_\sigma(C)$, $(\pi v)_i = v_j$ for some $j \in \Omega_i$, $i = 1, 2, \ldots, c+f$.

Denote the code $E_\sigma(C)$ with the last $f$ coordinates deleted by $E_\sigma(C)^\ast$. So $E_\sigma(C)^\ast$ is a self-orthogonal binary code of length $pc$. For $v$ in $E_\sigma(C)^\ast$, we let $v|\Omega_i = (v_0, v_1, \ldots, v_{p-1})$ correspond to the polynomial $v_0 + v_1 x + \cdots + v_{p-1} x^{p-1}$ from $\mathcal{P}$, where $\mathcal{P}$ is a set of even-weight polynomials in the factor ring $\mathbb{F}_2[x]/(x^p - 1)$. Thus we obtain the map $\varphi : E_\sigma(C)^\ast \to \mathcal{P}^c$. The code $\mathcal{P}$ is a cyclic code of length $p$ with a generator polynomial $x - 1$. It is known that $\varphi(E_\sigma(C)^\ast)$ is a submodule of the $\mathcal{P}$-module $\mathcal{P}^c$ [10, 21].

**Theorem 2** (see [21]). A binary $[n, n/2]$ code $C$ with an automorphism $\sigma$ is self-dual if and only if the following two conditions hold:

(i) $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual code of length $c + f$;
Let \( C_{17} \) be a binary self-dual \([68 + f, 34 + \frac{f}{2}, 12]\) code, where \( f = 0, 2, 4 \). Assume that \( C \) has an automorphism of type \( 17 \) \( - (4, f) \), \( f = 0, 2, 4 \). Using the decomposition

\[ x^{17} - 1 = (x - 1)(1 + x + x^2 + x^4 + x^6 + x^7 + x^8)(1 + x^3 + x^4 + x^5 + x^8) = (x - 1)h_1(x)h_2(x), \]

we have \( \mathcal{P} = I_1 \oplus I_2 \), where \( I_j \) is the irreducible cyclic code of length 17 with a parity-check polynomial \( h_j(x) \), \( j = 1, 2 \). Therefore \( I_j = (g_j(x)) \) are fields with \( 2^{\deg h_j(x)} \cdot 2^8 \) elements, with generator polynomials \( g_1(x) = 1 + x + x^3 + x^6 + x^8 + x^9 \) and \( g_2(x) = 1 + x^3 + x^4 + x^5 + x^6 + x^9 \), respectively.

According to Lemma 1, \( C_{17} = M_1 \oplus M_2 \), where \( M_j = \{ u \in C_{17} \mid u_i \in I_j, i = 1, \ldots, c \} \) is a linear code over the field \( I_j, j = 1, 2 \), and \( \dim I_1 + \dim I_2 = 4 \). The idempotents \( e_1 = x + x^2 + x^4 + x^5 + x^6 + x^{13} + x^{15} + x^{16} \) and \( e_2 = x^3 + x^5 + x^7 + x^{10} + x^{11} + x^{12} + x^{14} \) generate the ideals \( I_1 \) and \( I_2 \) defined above. Without loss of generality, we can assume that \( \dim I_1 \geq \dim I_2 \). The subcode \( \varphi(E_\sigma(C)) = M_1 \oplus M_2 \) is a code over \( \mathcal{P} = I_1 \oplus I_2 \) satisfying the orthogonal condition (2).
Consider $\delta = g_1(x)^{17}$. Since the order of $g_1(x)$ is $2^8 - 1 = 15 \cdot 17$, the order of $\delta = x^3 + x^7 + x^8 + x^9 + x^{10} + x^{14}$ is 15. Then $I_1 = \{0, x^i \delta^j \mid 0 \leq i \leq 16, 0 \leq j \leq 14\}$. For a fixed $0 \leq j \leq 14$, the elements $x^i \delta^j$ are right cyclic shifts of $\delta^j$ and have the same weight. We list the elements $\delta^j$ in Table 3. It is obvious that every element $\delta^k \in I_1$, $k = 0, \ldots, 14$ is invariant under the transformation $\mu : x \rightarrow x^{-1}$. Let $\tau = g_2 \delta^j = x + x^3 + x^8 + x^9 + x^{14} + x^{16}$ be an element of multiplicative order 15. Then $I_2 = \{0, x^i \tau^j \mid 0 \leq i \leq 16, 0 \leq j \leq 14\}$.

| $j$ | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|-----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0   | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |
| 1   |    | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |
| 2   |    |    | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |
| 3   |    |    |    | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |
| 4   |    |    |    |    | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |
| 5   |    |    |    |    |    | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |
| 6   |    |    |    |    |    |    | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |
| 7   |    |    |    |    |    |    |    | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |
| 8   |    |    |    |    |    |    |    |    | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  |
| 9   |    |    |    |    |    |    |    |    |    | 1  | 1  | 1  | 1  | 1  | 1  | 1  |
| 10  |    |    |    |    |    |    |    |    |    |    | 1  | 1  | 1  | 1  | 1  | 1  |
| 11  |    |    |    |    |    |    |    |    |    |    |    | 1  | 1  | 1  | 1  | 1  |
| 12  |    |    |    |    |    |    |    |    |    |    |    |    | 1  | 1  | 1  | 1  |
| 13  |    |    |    |    |    |    |    |    |    |    |    |    |    | 1  | 1  | 1  |
| 14  |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 1  | 1  |
| 15  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | 1  |
| 16  |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

Table 1: The elements $\delta^j$, $j = 0, \ldots, 14$ from $I_1$

The next lemma is obvious.

**Lemma 2.** The minimum distance of $C_\varphi$ is at least 2.

**Lemma 3.** The generator matrix of $C_\varphi$ has one of the three forms:

\[
\begin{pmatrix}
e_1 & 0 & e_1 & 0 \\
0 & e_1 & 0 & e_1 \\
e_2 & x^{i_1} x^{l} & x^{i_2} & x^{m} \\
0 & x^{i_3} & x^{m} & x^{l+1}
\end{pmatrix}
\begin{pmatrix}
e_1 & 0 & \delta & \delta^{12} \\
0 & e_1 & \delta^{12} & \delta \\
e_2 & x^{i_3} x^{l} & x^{i_2} x^{m} \\
0 & e_2 & x^{i_3} x^{m} & x^{l+1}
\end{pmatrix}
\begin{pmatrix}
e_1 & 0 & \delta^5 & \delta^{10} \\
0 & e_1 & \delta^{10} & \delta^5 \\
e_2 & x^{i_3} x^{l} & x^{i_2} x^{m} \\
0 & e_2 & x^{i_3} x^{m} & x^{l+1}
\end{pmatrix}
\]

where $0 \leq l, m \leq 14$, $0 \leq i_1, i_2, i_3, i_4 \leq 16$, $i_1 + i_4 \equiv i_2 + i_3 \pmod{17}$ or some of the entries with coordinates $(3, 3), (3, 4), (4, 3), (4, 4)$ in these three matrices are zeroes.

**Proof.** Denote $\dim J, M_j = k_j, j = 1, 2$. We have $k_1 \geq k_2$ and $k_1 + k_2 = 4$.

If $k_1 = 4, k_2 = 0$, the generator matrix $G$ of $C_\varphi$ is the identity matrix. Then $v = (0, 0, 0, e_1) \in C_\varphi$, which contradicts Lemma 2.

In the case of $k_1 = 3, k_2 = 1$, without loss of generality, we can assume that the generator matrix of $M_1$ is

\[
\begin{pmatrix}
e_1 & 0 & 0 & \delta^i \\
0 & e_1 & 0 & \delta^i \\
0 & 0 & e_1 & \delta^i \\
0 & 0 & e_1 & \delta^i
\end{pmatrix}
\]

The orthogonal condition (2) forces $i = j = k = 0$, so row 1 cannot be orthogonal to row 2, which is absurd.
In the last case, $k_1 = k_2 = 2$, we can assume that there is a 2-weight vector in $M_1$ and consider the generator matrix of $M_1$ in the form $\begin{pmatrix} e_1 & 0 & \delta^3 & 0 \\
0 & e_1 & \delta^3 & x^3 \delta^3 \end{pmatrix}$, or the element $(2,3)$ of this matrix is 0. Since row 1 must obey (2) we have $i = 0$. Then the orthogonality of rows 1 and 2 forces the element $(2,3)$ of $G$ to be 0, thus $G_1 = \begin{pmatrix} e_1 & 0 & e_1 & 0 \\
0 & e_1 & 0 & e_1 \end{pmatrix}$. If the minimum distance of $M_1$ is 3, after Gaussian elimination and applying (iv) from Theorem 3 to columns 3 and 4, the generator matrix is $\begin{pmatrix} e_1 & 0 & \delta^3 & \delta^j \\
0 & e_1 & \delta^k & x^3 \delta^m \end{pmatrix}$. Here the $(2,3)$ element is a power of $\delta$ since otherwise we can use multiplication of row 2 by $x^{-k}$ and (iv) from Theorem 3 to column 2. Also without loss of generality, we can take $i \leq j$. The orthogonality of row 1 gives $(i,j) \in Q = \{(1,12), (2,9), (3,4), (5,10), (6,8), (7,13), (11,14)\}$. For the second row to be orthogonal to itself, we have $l = 0$. Lastly, the orthogonality of rows 1 and 2 gives us $i = m$ and $j = k$, forcing the generator matrix in the form $\begin{pmatrix} e_1 & 0 & \delta^3 & \delta^j \\
0 & e_1 & \delta^k & \delta^m \end{pmatrix}$, where $(i,j) \in Q$.

Using $x \rightarrow x^2$ (Theorem 3 (iii)) we have three orbits for $Q : \{(1,12), (2,9), (3,4), (6,8)\}, \{(5,10)\}, \{(7,13), (11,14)\}$. But $(3,4)$ and $(11,14)$ generate the same code since if we use the permutation $(2,3)$ and then Gaussian elimination, we have

$$\begin{pmatrix} e_1 & 0 & \delta^3 & \delta^4 \\
0 & e_1 & \delta^3 & \delta^4 \end{pmatrix} \rightarrow \begin{pmatrix} e_1 & \delta^3 & 0 & \delta^4 \\
0 & \delta^3 & e_1 & \delta^4 \end{pmatrix} \rightarrow \begin{pmatrix} e_1 & \delta^3 & 0 & \delta^4 \\
0 & e_1 & \delta^3 & \delta^4 \end{pmatrix} \rightarrow \begin{pmatrix} e_1 & 0 & \delta^{14} & \delta^{11} \\
0 & e_1 & \delta^{11} & \delta^{14} \end{pmatrix}.$$ 

We consider the matrix for the $M_2$ part in the form $W = \begin{pmatrix} e_2 & 0 & x^{i_1} x^{i_2} & x^{i_3} x^{i_4} \\
0 & e_2 & x^{i_1} x^{i_2} & x^{i_3} x^{i_4} \end{pmatrix}$, or some of the elements in columns 3 or 4 of $W$ is 0. This matrix must obey (2), which leads to $l_1 = l_4, l_2 = l_3$, and $i_1 + i_4 \equiv i_2 + i_3$ (mod 17).

Using a computer, we have calculated all inequivalent codes $C_\varphi$ with minimum distance $d \geq 12$. We give the following result.

**Theorem 4.** *Up to equivalence, there are exactly 2891 codes $C_\varphi$ of length 4 over the set $\mathcal{P}$ of all even-weight polynomials in $F_2[x]/(x^{17} - 1)$ such that $d(E_\varphi(C^*)) \geq 12$.*

**Remark 1.** *We use the program Q-extensions [1] for computing the minimum distance and for equivalence testing of all codes in this paper. The codes in Theorem 4 have the following cardinality of the automorphism group: 2056 codes with $|Aut(C)| = 17$; 705 codes with $|Aut(C)| = 34$; 2 codes with $|Aut(C)| = 51$; 128 code with $|Aut(C)| = 68$. The number of codes with different values of $A_{12}$ is summarized in Table 2.*

In the next sections, using the above codes $C_\varphi$, we will construct all binary self-dual codes $C$ for lengths 68, 70, and 72 having an automorphism of type $17 - (4, f), f = 0, 2, 4$ and minimum distance 12. To do that we consider the generator matrix of $C_\varphi$ to be fixed as one of the above 2891 codes and consider all possible generator matrices for the subcode $F_\varphi$. Assume that $Q$ is a generator matrix for the subcode $C_\varphi$. Let $A$ be a subgroup of the automorphism group of the binary
code generated by \( Q \) consisting of the automorphisms of this code that permute the first 4 coordinates (corresponding to the 17-cycle coordinates) among themselves and permute the last \( f \) coordinates (corresponding to the fixed coordinates) among themselves. Let \( G' \) be a subgroup of the symmetric group \( S_4 \) consisting of the permutations in \( A \) restricted to the first 4 coordinates, ignoring the action on the fixed points. Denote by \( C'_{2k} \) the \([2k,k]\) binary self-dual code generated by \( E_\tau(C)^* = \varphi^{-1}(H_\tau) \) and \( E_\tau(C) \) generated by the preimage of \( Q_1 \) with columns permuted by \( \tau \in S_4 \). If \( \tau_1 \) and \( \tau_2 \) belong to the same right coset of \( G' \) in \( S_4 \), then the codes \( C_{\tau_1}^{2k} \) and \( C_{\tau_2}^{2k} \) are equivalent. Therefore, we only need to consider permutations from the right transversal of \( S_4 \) with respect to the subgroup \( G' \).

4. Classification of the \([68,34,12]\) self-dual codes

There are two possible weight enumerators for a \([68,34,12]\) binary self-dual code:

\[
W_{68,1} = 1 + (442 + 4\beta)y^{12} + (10864 - 8\beta)y^{14} + \ldots,
\]

where \( \beta, \gamma \) are integer parameters. Codes are known with both weight enumerators. For most recent information on the known values of the parameters we refer the reader to [13].

Using Theorem 2 (i), the code \( C_\pi \) is the unique \([4,2]\) binary self-dual code \( 2\|_2 \) with a generator matrix \[
\begin{pmatrix}
1100 \\
0011
\end{pmatrix}
\]

having an automorphism group \( \langle (1,2), (1,4)(2,3) \rangle \). Then the representatives of the different right coset are \( (1,1,3) \) and \( (2,3) \). After constructing all \( 3 \times 2891 \) codes we have the following result.

**Theorem 5.** Up to equivalence, there exist 1588 inequivalent \([68,34,12]\) self-dual codes with an automorphism of order 17, all having weight enumerator \( W_{68,2} \) for \( \gamma = 0 \).

Self-dual \([68,34,12]\) codes with weight enumerators corresponding to the values \( \beta = 17, 153, 187, 221 \), and 255 were not known in previously published research. These values also appear in extended codes from a modified four circulant construction in [12]. In Table 4, we present the weight enumerators and automorphism

<table>
<thead>
<tr>
<th>( A_{12} )</th>
<th>170</th>
<th>187</th>
<th>204</th>
<th>221</th>
<th>238</th>
<th>255</th>
<th>272</th>
<th>289</th>
<th>306</th>
<th>323</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>14</td>
<td>27</td>
<td>56</td>
<td>70</td>
<td>83</td>
<td>120</td>
</tr>
<tr>
<td>( A_{12} )</td>
<td>340</td>
<td>357</td>
<td>374</td>
<td>391</td>
<td>408</td>
<td>425</td>
<td>442</td>
<td>459</td>
<td>476</td>
<td>493</td>
</tr>
<tr>
<td>number</td>
<td>128</td>
<td>159</td>
<td>176</td>
<td>188</td>
<td>211</td>
<td>197</td>
<td>198</td>
<td>171</td>
<td>175</td>
<td>122</td>
</tr>
<tr>
<td>( A_{12} )</td>
<td>510</td>
<td>527</td>
<td>544</td>
<td>561</td>
<td>578</td>
<td>595</td>
<td>612</td>
<td>629</td>
<td>646</td>
<td>663</td>
</tr>
<tr>
<td>number</td>
<td>147</td>
<td>91</td>
<td>97</td>
<td>66</td>
<td>62</td>
<td>49</td>
<td>45</td>
<td>39</td>
<td>33</td>
<td>20</td>
</tr>
<tr>
<td>( A_{12} )</td>
<td>680</td>
<td>697</td>
<td>714</td>
<td>731</td>
<td>748</td>
<td>765</td>
<td>782</td>
<td>799</td>
<td>816</td>
<td>833</td>
</tr>
<tr>
<td>number</td>
<td>27</td>
<td>13</td>
<td>17</td>
<td>17</td>
<td>18</td>
<td>6</td>
<td>12</td>
<td>2</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>( A_{12} )</td>
<td>867</td>
<td>884</td>
<td>918</td>
<td>935</td>
<td>952</td>
<td>969</td>
<td>986</td>
<td>1020</td>
<td>1088</td>
<td>1190</td>
</tr>
<tr>
<td>number</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 2: The number of codes obtained with \( A_{12} \)
groups of all codes obtained. Among the constructed codes there are 23 codes with an automorphism group of order 68 from [7].

<table>
<thead>
<tr>
<th>$\beta$</th>
<th>$\gamma$</th>
<th>$\delta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>2</td>
<td>153</td>
</tr>
<tr>
<td>34</td>
<td>6</td>
<td>170</td>
</tr>
<tr>
<td>51</td>
<td>19</td>
<td>187</td>
</tr>
<tr>
<td>68</td>
<td>40</td>
<td>204</td>
</tr>
<tr>
<td>85</td>
<td>60</td>
<td>221</td>
</tr>
<tr>
<td>102</td>
<td>89</td>
<td>238</td>
</tr>
<tr>
<td>119</td>
<td>56</td>
<td>255</td>
</tr>
<tr>
<td>136</td>
<td>110</td>
<td>272</td>
</tr>
</tbody>
</table>

Table 3: The parameters of $[68,34,12]$ codes, all with $W_{68,2}, \gamma = 0$

5. Classification of $[70, 35, 12]$ self-dual codes

The first binary self-dual $[70, 35, 12]$ codes are constructed in [9]. All such codes with an automorphism of order 23 are classified in [4]. The possible weight enumerator of binary self-dual $[70, 35, 12]$ code is [9]:

$$W_{70,1} = 1 + 2\beta y^{12} + (11730 - 2\beta - 128\gamma)y^{14} + (150535 - 22\beta + 896\gamma)y^{16} + \ldots$$

or

$$W_{70,2} = 1 + 2\beta y^{12} + (9682 - 2\beta)y^{14} + (173063 - 22\beta)y^{16} + \ldots,$$

where $\beta$ and $\gamma$ are integer parameters. Only codes with $W_{70,1}$ for $\gamma = 1$, $\beta = 416$ (see [9]) and $\gamma = 0$ for $\beta = 138, 184, 230, 276, 322, 368, 414, 460, and 1012$ (see [4]) are known.

Lemma 4. There is a unique generator matrix (up to a permutation on the cyclic or fixed positions) for $F_{\sigma}$

$$\text{gen}(F_{\sigma}(C)) = \begin{pmatrix} 1001 & 00 \\ 0100 & 10 \\ 0010 & 01 \end{pmatrix},$$

in a $[70, 35, 12]$ self-dual code with an automorphism of order 17, where 0 and 1 denote zero and all-one vectors of length 17, respectively.

Proof. By Theorem 2, $C_{\pi}$ is the unique self-dual $[6, 3]$ code $3i_2$ with a generator matrix $\begin{pmatrix} 110000 \\ 001100 \\ 000011 \end{pmatrix}$. We have to arrange two of the six coordinates to be the fixed points. At least one of the two coordinates in the support of a 2-weight vector in $3i_2$ should be a cycle point, otherwise the code $F_{\sigma}$ will have minimum distance 2.
This gives only one possible generator matrix (up to a permutation of the cycle or a permutation of the fixed points) for the code \( F_\sigma(C) \), namely the matrix given in (3).

We give our results for this code length in the next statement.

**Theorem 6.** The are exactly 4227 inequivalent \([70, 35, 12]\) self-dual codes with an automorphism of order 17, all having a weight enumerator \( W_{70,1} \) for \( \gamma = 0 \).

The values of the parameters of the weight enumerators and the order of the automorphism groups of the constructed codes are summarized in Table 5. All obtained codes have new values of \((\beta, \gamma)\) in \( W_{70,1} \).

<table>
<thead>
<tr>
<th></th>
<th>([\text{Aut}(C)])</th>
<th>([\text{Aut}(C)])</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\beta)</td>
<td>17</td>
<td>37</td>
</tr>
<tr>
<td>102</td>
<td>1</td>
<td>374</td>
</tr>
<tr>
<td>136</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>170</td>
<td>60</td>
<td>4</td>
</tr>
<tr>
<td>204</td>
<td>400</td>
<td>9</td>
</tr>
<tr>
<td>238</td>
<td>775</td>
<td>18</td>
</tr>
<tr>
<td>272</td>
<td>965</td>
<td>34</td>
</tr>
<tr>
<td>306</td>
<td>961</td>
<td>29</td>
</tr>
<tr>
<td>340</td>
<td>513</td>
<td>19</td>
</tr>
</tbody>
</table>

**Table 4:** The parameters of \([70, 35, 12]\) codes, all with \( W_{70,1} \), \( \gamma = 0 \)

6. **Classification for doubly-even and singly-even \([72, 36, 12]\) self-dual codes**

The best known distance for a doubly-even code of length 72 is 12 and there is one possible weight enumerator for such a code (see [3]):

\[
W_{72} = 1 + (4398 + \alpha)y^{12} + (197073 - 12\alpha)y^{16} + (18396972 + 66\alpha)y^{20} + \ldots,
\]

where \( \alpha \) is an integer parameter. Codes are known for 214 different values of \( \alpha \) (see [2], [4], [5], [8], [9], [13], [20]).

There is a unique [8, 4] doubly-even self-dual code – the extended Hamming code \( h_8 \) with a generator matrix \( \text{gen}(h_8) = (I_4|I_4 + J_4) \). We have to take 4 coordinates to be the cycle positions and 4 to be the fixed point. Since the minimum distance is \( d = 12 \), we cannot has a codeword in \( C_\pi \) of weight 4 that have its whole support in the fixed points. Now, if we consider the 4 rows of \( \text{gen}(H_8) \), which are codewords of weight 4, it is obvious that \( \text{gen}(F_\sigma(C)) = \begin{pmatrix} 1000 & 0010 \\ 0100 & 1101 \\ 0110 & 1011 \\ 1110 & 0001 \end{pmatrix} \). The symmetric group \( S_4 \) acting on the cyclic points maps the above code \( F_\sigma(C) \) to itself. Thus in this case we can fix both \( F_\sigma(C) \) and \( E_\sigma(C) \). We give the following result.
Theorem 7. There exist 2891 inequivalent \([72, 36, 12]\) doubly-even self-dual codes with an automorphism of order 17.

The weight enumerators and \(|\text{Aut}(C)|\) of these codes are summarized in Table 5. All codes are new and the values \(\alpha = -4092, -3990, -3888, -2868, -2766, -2664, \) and \(-2562\) in \(W_{72}\) were not known before.

\[
\begin{array}{cccc|cccc}
\alpha & |\text{Aut}(C)| & \alpha & |\text{Aut}(C)| \\
-4092 & 17 & 34 & 51 & 68 & -3276 & 158 & 82 & 19 \\
-3990 & 2 & 1 & 2 & -3174 & 53 & 65 & 6 \\
-3888 & 16 & 11 & 7 & -3072 & 18 & 36 & 10 \\
-3786 & 146 & 34 & 7 & -2970 & 3 & 17 & 14 \\
-3684 & 337 & 76 & 9 & -2868 & 9 \\
-3582 & 476 & 104 & 13 & -2766 & 4 & 3 \\
-3480 & 543 & 137 & 18 & -2664 & 5 & 3 \\
-3378 & 304 & 123 & 1 & 11 & -2562 & 2 & 5 \\
\end{array}
\]

Table 5: The parameters of \([72, 36, 12]\) doubly-even codes

There are two possible weight enumerators for a singly-even \([72, 36, 12]\) code:

\[
W_{72,1} = 1 + 2\beta y^{12} + (8640 - 64\gamma)y^{14} + (124281 - 24\beta + 384\gamma)y^{16} + \ldots
\]

\[
W_{72,2} = 1 + 2\beta y^{12} + (7616 - 64\gamma)y^{14} + (134521 - 24\beta + 384\gamma)y^{16} + \ldots,
\]

where \(\beta\) and \(\gamma\) are integer parameters. Codes with \(W_{72,1}\) are known for more than 300 different values of \(\beta, \gamma\). For \(W_{72,2}\), only the following values of the parameters were known: \(\gamma = 0, \beta = 209, 263, 309, 317, 335; \gamma = 11, \beta = 859\) (see [3], [5], [13]). Recently, in [20], codes with 300 different values of \(\beta\) for \(\gamma = 0, 11, 22, 33,\) and 44 in \(W_{72,2}\) were constructed.

There is a unique \([8, 4]\) singly-even self-dual code: \(4i_2, \text{gen}(4i_2) = \begin{pmatrix} 11000000 \\ 00110000 \\ 00001100 \\ 00000011 \end{pmatrix}\).

We cannot have a codeword in \(C_\pi\) of weight 2 that has its whole support in fixed points. This leads to a unique generator matrix \(\begin{pmatrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{pmatrix}\) of \(F_\sigma(C)\). The stabilizer of the automorphism group of this code on the cycle position is the symmetric group \(S_4\), so we can also fix the generator matrix \(F_\sigma\).

Theorem 8. Up to equivalence, there exist 2039 singly-even self-dual \([72, 36, 12]\) codes with an automorphism of order 17, all of which have a weight enumerator \(W_{72,2}\).
Only the codes with parameters $\gamma = 0$ and $\beta = 187, 221, 374, 408$ were previously known (see [20]). The remaining 64 values of $\beta, \gamma$ are new. We list all codes obtained in Table 6.

<table>
<thead>
<tr>
<th>$\gamma = 0$</th>
<th>$\text{Aut}(C)$</th>
<th>$\gamma = 0$</th>
<th>$\text{Aut}(C)$</th>
<th>$\gamma = 0$</th>
<th>$\text{Aut}(C)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\beta$</td>
<td>17</td>
<td>34</td>
<td>51</td>
<td>68</td>
<td>$\beta$</td>
</tr>
<tr>
<td>102</td>
<td>1</td>
<td>255</td>
<td>175</td>
<td>37</td>
<td>6</td>
</tr>
<tr>
<td>119</td>
<td>2</td>
<td>1</td>
<td>272</td>
<td>141</td>
<td>37</td>
</tr>
<tr>
<td>136</td>
<td>8</td>
<td></td>
<td>289</td>
<td>114</td>
<td>34</td>
</tr>
<tr>
<td>153</td>
<td>30</td>
<td>4</td>
<td>3</td>
<td>306</td>
<td>80</td>
</tr>
<tr>
<td>170</td>
<td>57</td>
<td>15</td>
<td></td>
<td>323</td>
<td>55</td>
</tr>
<tr>
<td>187</td>
<td>76</td>
<td>15</td>
<td>5</td>
<td>340</td>
<td>30</td>
</tr>
<tr>
<td>204</td>
<td>111</td>
<td>28</td>
<td>2</td>
<td>357</td>
<td>17</td>
</tr>
<tr>
<td>221</td>
<td>162</td>
<td>15</td>
<td>6</td>
<td>374</td>
<td>12</td>
</tr>
<tr>
<td>238</td>
<td>149</td>
<td>38</td>
<td>8</td>
<td>391</td>
<td>6</td>
</tr>
</tbody>
</table>

Table 6: The parameters of $[72,36,12]$ singly-even codes, all with $W_{72,2}$

References

I. Bouyukliev, V. Fack, J. Winne, 2 – (31, 15, 7), 2 – (35, 17, 8) and 2 – (36, 15, 6)
designs with automorphisms of odd prime order, and their related Hadamard matrices and
codes, Des. Codes Cryptogr. 51(2009), 1–27.

J. Conway, N. J. A. Sloane, A new upper bound on the minimal distance of self-dual


S. T. Dougherty, J.-L. Kim, P. Solé, Double circulant codes from two class associ-

S. T. Dougherty, J.-L. Kim, P. Solé, Open Problems in Coding Theory, Contemp.

T. A. Gulliver, M. Harada, Classification of extremal double circulant self-dual
codes of lengths 64 to 72, Des. Codes Cryptogr. 13(1998), 257–269.

T. A. Gulliver, M. Harada, On doubly circulant doubly even self-dual [72, 36, 12]

Codes, Finite Fields Appl. 3(1997), 131–139.

W. C. Huffman, Automorphisms of codes with applications to extremal doubly even

W. C. Huffman, On the classification and enumeration of self-dual codes, Finite
Fields Appl. 11(2005), 451–490.

A. Kaya, B. Yildiz, A. Pasa, New extremal binary self-dual codes from a modified
four circulant construction, arXiv: 1507.01628 [cs.IT].

A. Kaya, B. Yildiz, I. Siap, New extremal binary self-dual codes of length 68 from
quadratic residue codes over $F_2 + uF_2 + u^2F_2$, Finite Fields Appl. 29, 160–177.


V. Pless, J. Thompson, 17 does not divide the order of the group of a (72, 36, 16)

134–139.

R. P. Russeva, Uniqueness of the [36, 18, 8] double circulant code, in: Proc. Int. Work-

(1973), 251–251.

N. Yankov, M. H. Lee, Classification of self-dual codes of length 50 with an automor-

N. Yankov, M. H. Lee, M. Gürel, M. Ivanova, Self-dual codes with an automor-

V. Yorgov, Binary Self-Dual Codes with Automorphisms of Odd Order, Probl. Inf.

V. Yorgov, A method for constructing inequivalent self-dual codes with applications