MATHEMATICAL COMMUNICATIONS
Math. Commun. **21**(2016), 97–107

Self-dual codes with an automorphism of order 17

Müberra Gürel[1,*] and Nikolay Yankov[2]

[1] *Safir Company Haznedar Mah. Menderes Cad. No:5/B, Gungoren, Istanbul, Turkey*
[2] *Faculty of Mathematics and Informatics, Shumen University, Bulgaria, Shumen, 9 700, 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, and 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:

$$d \leq 4\lfloor n/24 \rfloor + 4, \quad \text{if } n \not\equiv 22 \pmod{24},$$
$$d \leq 4\lfloor n/24 \rfloor + 6, \quad \text{if } n \equiv 22 \pmod{24}.$$

Codes achieving this bound are called *extremal*.

We say that a code C of length n has an automorphism σ of *type* $p - (c, f)$ for a prime p if σ 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), jankov_niki@yahoo.com (N. Yankov)

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 $|\mathrm{Aut}(C)| = 68$ 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 $f = 0, 2$, and 4.

2. Construction method

Let C be a binary self-dual code of length n with an automorphism σ 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

$$\sigma = (1, 2, \cdots, p)(p+1, p+2, \cdots, 2p) \cdots (p(c-1)+1, p(c-1)+2, \cdots, pc) \quad (1)$$

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

Denote the cycles of σ by $\Omega_1, \Omega_2, \ldots, \Omega_c$, and the fixed points by $\Omega_{c+1}, \ldots, \Omega_{c+f}$. Let $F_\sigma(C) = \{v \in C \mid v\sigma = v\}$ and $E_\sigma(C) = \{v \in C \mid \mathrm{wt}(v|\Omega_i) \equiv 0 \pmod 2, i = 1, \cdots, c+f\}$, where $v|\Omega_i$ is the restriction of v on Ω_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 σ 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 $v \in F_\sigma(C)$, $(v\pi)_i = v_j$ 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 $E_\sigma(C)^*$. So $E_\sigma(C)^*$ is a self-orthogonal binary code of length pc. For v in $E_\sigma(C)^*$, we let $v|\Omega_i = (v_0, v_1, \cdots, v_{p-1})$ 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 $\varphi : E_\sigma(C)^* \to \mathcal{P}^c$. The code $\mathcal{P}$ is a cyclic code of length p with a generator polynomial $x - 1$. It is known that $\varphi(E_\sigma(C)^*)$ 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 σ 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 $c + f$;

(ii) for every two vectors u, v from $C_\varphi = \varphi(E_\sigma(C)^*)$ we have

$$u_1(x)v_1(x^{-1}) + \cdots + u_c(x)v_c(x^{-1}) = 0. \tag{2}$$

Let $x^p - 1 = (x-1)h_1(x)\cdots h_s(x)$, where $h_1(x), \ldots, h_s(x)$ are irreducible binary polynomials. If $g_j(x) = (x^p-1)/h_j(x)$, and $I_j = \langle g_j(x)\rangle$ is the ideal in $\mathbb{F}_2[x]/\langle x^p-1\rangle$, generated by $g_j(x)$, then I_j is a field with $2^{deg(h_j(x))}$ elements, $j = 1, 2, \ldots, s$, and $\mathcal{P} = I_1 \oplus I_2 \oplus \cdots \oplus I_s$ ([14]).

Lemma 1 (see [21]). *Let $M_j = \{u \in \varphi(E_\sigma(C)^*) | u_i \in I_j, i = 1, 2, \ldots, c\}$, $j = 1, 2, \ldots, s$. Then:*

1) M_j is a linear space over I_j, $j = 1, 2, \ldots, s$;

2) $C_\varphi = \varphi(E_\sigma(C)^*) = M_1 \oplus M_2 \oplus \cdots \oplus M_s$ (direct sum of $\mathcal{P}$-submodules);

3) If C is a self-dual code, then $\sum_{j=1}^{s} \dim_{I_j} M_j = cs/2$.

To classify the codes, we need additional conditions for equivalence and we use the following theorem.

Theorem 3 (see [22]). *The following transformations preserve the decomposition and send code C to an equivalent one:*

(i) a permutation of the fixed coordinates;

(ii) a permutation of the p-cycles coordinates;

(iii) a substitution $x \to x^2$ in C_φ;

(iv) a cyclic shift to each p-cycle independently.

3. Codes with an automorphism of order 17

Let C 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 $I_i = \langle g_i(x)\rangle$ are fields with $2^{\deg h_j(x)} = 2^8$ 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, $C_\varphi = M_1 \oplus M_2$, where $M_j = \{u \in C_\varphi \mid u_i \in I_j, i = 1, \ldots, c\}$ is a linear code over the field I_j, $j = 1, 2$, and $\dim_{I_1} M_1 + \dim_{I_2} M_2 = 4$. The idempotents $e_1 = x + x^2 + x^4 + x^8 + x^9 + x^{13} + x^{15} + x^{16}$ and $e_2 = x^3 + x^5 + x^6 + x^7 + x^{10} + x^{11} + x^{12} + x^{14}$ generate the ideals I_1 and I_2 defined above. Without loss of generality, we can assume that $\dim_{I_1} M_1 \geq \dim_{I_2} M_2$. 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 $I_1 = \{0, x^i\delta^j \mid 0 \le i \le 16, 0 \le j \le 14\}$. For a fixed $0 \le j \le 14$, the elements $x^i\delta^j$ are right cyclic shifts of δ^j and have the same weight. We list the elements δ^j in Table 3. It is obvious that every element $\delta^k \in I_1$, $k = 0, \ldots, 14$ is invariant under the transformation $\mu : x \to x^{-1}$. Let $\tau = g_2^{17} = x + x^3 + x^8 + x^9 + x^{14} + x^{16}$ be an element of multiplicative order 15. Then $I_2 = \{0, x^i\tau^j \mid 0 \le i \le 16, 0 \le j \le 14\}$.

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		
2		1		1			1					1			1		1
3		1			1	1	1		1	1		1	1	1			1
4			1			1	1					1	1			1	
5			1	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	
8					1	1		1			1		1	1			
9			1	1	1		1		1	1		1		1	1	1	
10		1		1	1	1	1	1			1	1	1	1	1		1
11		1	1	1		1							1		1	1	1
12		1	1	1	1			1			1			1	1	1	1
13		1					1	1	1	1	1	1					1
14				1	1	1			1	1			1	1	1		

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

The next lemma is obvious.

Lemma 2. *The minimum distance of C_φ is at least* 2.

Lemma 3. *The generator matrix of C_φ has one of the three forms:*

$$\begin{pmatrix} e_1 & 0 & e_1 & 0 \\ 0 & e_1 & 0 & e_1 \\ e_2 & 0 & x^{i_1}\tau^l & x^{i_2}\tau^m \\ 0 & e_2 & x^{i_3}\tau^m & x^{i_4}\tau^l \end{pmatrix}, \begin{pmatrix} e_1 & 0 & \delta & \delta^{12} \\ 0 & e_1 & \delta^{12} & \delta \\ e_2 & 0 & x^{i_1}\tau^l & x^{i_2}\tau^m \\ 0 & e_2 & x^{i_3}\tau^m & x^{i_4}\tau^l \end{pmatrix}, \begin{pmatrix} e_1 & 0 & \delta^5 & \delta^{10} \\ 0 & e_1 & \delta^{10} & \delta^5 \\ e_2 & 0 & x^{i_1}\tau^l & x^{i_2}\tau^m \\ 0 & e_2 & x^{i_3}\tau^m & x^{i_4}\tau^l \end{pmatrix},$$

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

Proof. Denote $\dim_{I_j} M_j = k_j$, $j = 1, 2$. We have $k_1 \ge k_2$ and $k_1 + k_2 = 4$.

If $k_1 = 4, k_2 = 0$, the generator matrix G of C_φ 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 $\begin{pmatrix} e_1 & 0 & 0 & \delta^i \\ 0 & e_1 & 0 & \delta^j \\ 0 & 0 & e_1 & \delta^k \end{pmatrix}$. 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 $\begin{pmatrix} e_1 & 0 & \delta^i & 0 \\ 0 & e_1 & \delta^j & x^k\delta^l \end{pmatrix}$, 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 $\begin{pmatrix} e_1 & 0 & \delta^i & \delta^j \\ 0 & e_1 & \delta^k & x^l\delta^m \end{pmatrix}$. Here the $(2,3)$ element is a power of δ 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 $i \le j$. 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 $\begin{pmatrix} e_1 & 0 & \delta^i & \delta^j \\ 0 & e_1 & \delta^j & \delta^i \end{pmatrix}$, where $(i,j) \in Q$.

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

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

We consider the matrix for the M_2 part in the form $W = \begin{pmatrix} e_2 & 0 & x^{i_1}\tau^{l_1} & x^{i_2}\tau^{l_2} \\ 0 & e_2 & x^{i_3}\tau^{l_3} & x^{i_4}\tau^{l_4} \end{pmatrix}$, 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 $i_1 + i_4 \equiv i_2 + i_3 \pmod{17}$. □

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

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

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} are summarized in Table 2.*

In the next sections, using the above codes C_φ, 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_φ to be fixed as one of the above 2891 codes and consider all possible generator matrices for the subcode F_σ. Assume that Q is a generator matrix for the subcode C_π. Let A be a subgroup of the automorphism group of the binary

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

Table 2: *The number of codes obtained with* A_{12}

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}^{τ} the $[2k, k]$ binary self-dual code generated by $E_\sigma(C)^* = \varphi^{-1}(H_i)$ and $F_\sigma(C)$ generated by the preimage of Q_1 with columns permuted by $\tau \in S_4$. If τ_1 and τ_2 belong to the same right coset of G' in S_4, then the codes $C_{2k}^{\tau_1}$ and $C_{2k}^{\tau_2}$ 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 β, γ 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_π is the unique $[4, 2]$ binary self-dual code $2i_2$ 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 3×2891 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

groups of all codes obtained. Among the constructed codes there are 23 codes with an automorphism group of order 68 from [7].

	$\lvert\mathrm{Aut}(C)\rvert$				$\lvert\mathrm{Aut}(C)\rvert$		
β	17	34	68	β	17	34	68
17		2		**153**	44	74	
34	19	6	2	170	11	65	23
51	70	19		**187**	8	26	
68	138	40	6	204	1	6	19
85	211	60		**221**	2	11	
102	197	89	21	238		9	15
119	130	56		**255**		2	
136	71	110	19	272		1	5

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]:

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

or

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

where β and γ 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_σ

$$gen(F_\sigma(C)) = \left(\begin{array}{c|c} \mathbf{1001} & 00 \\ \mathbf{0100} & 10 \\ \mathbf{0010} & 01 \end{array}\right), \tag{3}$$

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_π 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_σ 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 (β, γ) in $W_{70,1}$.

	$\lvert\mathrm{Aut}(C)\rvert$			$\lvert\mathrm{Aut}(C)\rvert$	
β	17	37	β	17	37
102		1	**374**	240	17
136	6	4	**408**	82	4
170	60	4	**442**	38	7
204	400	9	**476**	12	5
238	775	18	**510**	10	
272	965	34	**544**		1
306	961	29	**578**	4	2
340	513	19	**612**	5	2

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 α is an integer parameter. Codes are known for 214 different values of α (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 $\mathrm{gen}(h_8) = (I_4|I_4 + J_4)$. 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_π of weight 4 that have its whole support in the fixed points. Now, if we consider the 4 rows of $\mathrm{gen}(H_8)$, which are codewords of weight 4, it is obvious that $\mathrm{gen}(F_\sigma(C)) = \left(\begin{array}{c|c} \mathbf{1000} & 0111 \\ \mathbf{0100} & 1011 \\ \mathbf{0010} & 1101 \\ \mathbf{0001} & 1110 \end{array}\right)$. 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 $|\mathrm{Aut}(C)|$ 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.

	$\lvert\mathrm{Aut}(C)\rvert$					$\lvert\mathrm{Aut}(C)\rvert$		
α	17	34	51	68	α	17	34	68
$\mathbf{-4092}$				1	-3276	158	82	19
$\mathbf{-3990}$	2		1	2	-3174	53	65	6
$\mathbf{-3888}$	16	11		7	-3072	18	36	10
-3786	146	34		7	-2970	3	17	14
-3684	337	76		9	$\mathbf{-2868}$		9	
-3582	476	104		13	$\mathbf{-2766}$		4	3
-3480	543	137		18	$\mathbf{-2664}$		5	3
-3378	304	123	1	11	$\mathbf{-2562}$		2	5

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:

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

and

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

where β and γ are integer parameters. Codes with $W_{72,1}$ are known for more than 300 different values of β, γ. 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 β 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: $4i_2$, $\mathrm{gen}(4i_2) = \begin{pmatrix} 11000000 \\ 00110000 \\ 00001100 \\ 00000011 \end{pmatrix}$.

We cannot have a codeword in C_π of weight 2 that has its whole support in fixed points. This leads to a unique generator matrix $\left(\begin{array}{c|c} \mathbf{1000} & 1000 \\ \mathbf{0100} & 0100 \\ \mathbf{0010} & 0010 \\ \mathbf{0001} & 0001 \end{array}\right)$ 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_σ.

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 $\beta = 187, 221, 374$, and 408 were previously known (see [20]). The remaining 64 values of β, γ are new. We list all codes obtained in Table 6.

$\gamma = 0$	$\lvert\mathrm{Aut}(C)\rvert$			
β	17	34	51	68
102				1
119	2		1	
136	8			
153	30	4		3
170	57	15		
187	76	15		5
204	111	28		2
221	162	15		6
238	149	38		8

$\gamma = 0$	$\lvert\mathrm{Aut}(C)\rvert$			
β	17	34	51	68
255	175	37		6
272	141	37	1	6
289	114	34		6
306	80	42		1
323	55	39		9
340	30	37		5
357	17	22		3
374	12	21		10
391	6	20		5

$\gamma = 0$	$\lvert\mathrm{Aut}(C)\rvert$		
β	17	34	68
408	1	10	5
425		7	3
442	1	2	5
459		11	7
476		3	7
493		2	
527		1	2

$\gamma = 17$	$\lvert\mathrm{Aut}(C)\rvert$	
β	17	34
238	2	
255	1	2
272	3	9
289	6	6
306	4	6
323	6	10
340	10	7

$\gamma = 17$	$\lvert\mathrm{Aut}(C)\rvert$	
β	17	34
357	13	14
374	11	9
391	8	8
408	10	11
425	5	11
442	2	10
459		4

$\gamma = 17$	$\lvert\mathrm{Aut}(C)\rvert$	
β	17	34
476	5	8
493	2	9
510	2	6
527	1	2
544	1	
595		1
612	1	

$\gamma = \mathbf{34}$	$\lvert\mathrm{Aut}(C)\rvert$	
β	34	68
306	1	
340	1	
391	1	
408	1	
425		1
442	1	
459		2

$\gamma = \mathbf{34}$	$\lvert\mathrm{Aut}(C)\rvert$		
β	17	34	68
476		1	
493		3	
510		3	
527			1
544		6	
561		3	2
578	1	2	

$\gamma = \mathbf{34}$	$\lvert\mathrm{Aut}(C)\rvert$	
β	34	68
612	1	
646	1	2
663	1	
680	1	
697	1	
714	1	

	$\lvert\mathrm{Aut}(C)\rvert = 34$
$\gamma = \mathbf{71}$, $\beta = \mathbf{765}$	1

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

References

[1] I. BOUYUKLIEV, *About the code equivalence*, in: *Advances in Coding Theory and Cryptography*, (T. Shaska, W. C. Huffman, D. Joyner and V. Ustimenko, Eds.), World Scientific Publishing Co., Singapore, 126–151, 2007.

[2] 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.

[3] J. CONWAY, N. J. A. SLOANE, *A new upper bound on the minimal distance of self-dual codes*, IEEE Trans. Inform. Theory **36**(1990), 1319–1333.

[4] R. DONTCHEVA, *New binary* $[70,35,12]$ *self-dual and binary* $[72,36,12]$ *self-dual doubly-even codes*, Serdica J. Comput. **27**(2001), 287–302.

[5] S. T. DOUGHERTY, J.-L. KIM, P. SOLÉ, *Double circulant codes from two class association schemes*, Adv. Math. Commun. **1**(2007), 45–64.

[6] S. T. DOUGHERTY, J.-L. KIM, P. SOLÉ, *Open Problems in Coding Theory,*, Contemp. Math. **634**(2015), 79–99.

[7] 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.

[8] T. A. GULLIVER, M. HARADA, *On doubly circulant doubly even self-dual* $[72,36,12]$ *codes and their neighbors*, Australas. J. Combin. **40**(2008), 137–144.

[9] M. HARADA, *The Existence of a Self-Dual* $[70,35,12]$ *Code and Formally Self-Dual Codes*, Finite Fields Appl. **3**(1997), 131–139.

[10] W. C. HUFFMAN, *Automorphisms of codes with applications to extremal doubly even codes of length 48*, IEEE Trans. Inform. Theory **28**(1982), 511–521.

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

[12] A. KAYA, B. YILDIZ, A. PASA, *New extremal binary self-dual codes from a modified four circulant construction*, arXiv: 1507.01628 [cs.IT].

[13] 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.

[14] V. PLESS, W. HUFFMAN, *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998.

[15] V. PLESS, J. THOMPSON, *17 does not divide the order of the group of a* $(72,36,16)$ *doubly even code*, IEEE Trans. Inform. Theory **28**(1982), 537–541.

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

[17] R. P. RUSSEVA, *Uniqueness of the* $[36,18,8]$ *double circulant code*, in: *Proc. Int. Workshop Optimal codes and related topics*, May 26?June 1, 1995, Sozopol, Bulgaria, 126?129.

[18] N. SLOANE, *Is there a* $(72,36)d=16$ *self-dual code?*, IEEE Trans. Inform. Theory **19** (1973), 251–251.

[19] N. YANKOV, M. H. LEE, *Classification of self-dual codes of length 50 with an automorphism of odd prime order*, Des. Codes Cryptogr. **74**(2015), 571–579.

[20] N. YANKOV, M. H. LEE, M. GUREL, M. IVANOVA, *Self-dual codes with an automorphism of order 11*, IEEE Trans. Inform. Theory **61**(2015), 1188–1193.

[21] V. YORGOV, *Binary Self-Dual Codes with Automorphisms of Odd Order*, Probl. Inf. Transm. **19**(1983), 260–270.

[22] V. YORGOV, *A method for constructing inequivalent self-dual codes with applications to length 56*, IEEE Trans. Inform. Theory **33**(1987), 77–82.