Self-Dual Codes With an Automorphism of Order 11

Nikolay Yankov, Moon Ho Lee, Müberra Gürel, and Milena Ivanova

***Abstract*— Using a method for constructing self-dual codes having an automorphism of odd prime order, we classify up to equivalence all binary self-dual codes with an automorphism of order 11 with 6 cycles and minimum distance 12. This classification gives new [72, 36, 12] codes with weight enumerator that was previously not obtained as well as many [66, 33, 12], [68, 34, 12], and [70, 35, 12] codes with new values of the parameters in their respective weight enumerators.**

***Index Terms*— Self-dual codes, automorphisms.**

I. Introduction

The largest possible minimum weights of singly even self-dual codes of lengths up to 72 are determined in [3]. Rains [20] proved that the minimum distance d of a binary self-dual $[n, k, d]$ code satisfies the following bound:

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

Codes achieving this bound are called *extremal*.

More than forty years ago Neil Sloane (see [17]) 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 11 was proven in [13] but it is still unknown how many doubly-even $[72, 36, 12]$ codes exist.

Extremal and optimal self-dual codes with an automorphism of odd prime order are an extensively studied subject. All such codes are classified up to length 50 [21]. In recent works [14]–[16] some self-dual codes with automorphisms of order $2^r p$ for primes $p = 5, 7,$ and 11 were constructed using codes over rings $\mathbb{F}_2 + u\mathbb{F}_2$, $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, $\mathbb{F}_4 + u\mathbb{F}_4$, and R_k.

We say that a code C of length n has an automorphism σ of *type* p-(c, f) for prime p if σ has exactly c independent p-cycles and $f = n - cp$ fixed points in its decomposition. Without loss of generality we may assume that

$$\sigma = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p)\ldots (p(c-1)+1, p(c-1)+2, \ldots, pc). \qquad (1)$$

In [25] and [26] the self-dual codes with an automorphism of order 11 with four cycles are studied. There is a unique $[44, 22, 8]$ code with an automorphism of type 11-(2, 22), and 11 codes with an automorphism of type 11-(4, 0). Huffman in [12] presented a survey of the status of the classification of self-dual codes over $\mathbb{F}_2$. Also there [12, Table 2], the case of binary self-dual codes of lengths 66, 68 and 70 with an automorphism of order 11 with 6 cycles is listed as open.

This work is organized as follows. In Section II we introduce the construction method used in this paper. In Section III we classify all Hermitian $[6, 3, \ge 3]$ codes over finite field with 2^{10} elements. Finally in Section IV using some of the codes from Section III we classify all binary self-dual $[66 + 2s, 33 + s, 12]$ codes with an automorphism of type 11-$(6, 2s)$ for $s = 0, 1, 2, 3$.

II. Preliminaries

We apply a method for constructing binary self-dual codes possessing an automorphism of odd prime order from [11] and [23].

Let C be a binary self-dual code of length n with an automorphism σ of type p-(c, f). Let $\Omega_1, \ldots, \Omega_c$ be the p-cycles of σ and $\Omega_{c+1}, \ldots, \Omega_{c+f}$ be the fixed points. Define

$$F_\sigma(C) = \{v \in C \mid v\sigma = v\},$$

and

$$E_\sigma(C) = \{v \in C \mid \text{wt}(v|\Omega_i) \equiv 0 (\text{mod } 2), i = 1, \cdots, c+f\},$$

where $v|\Omega_i$ is the restriction of v on Ω_i.

Theorem 2.1 [11]: $C = F_\sigma(C) \oplus E_\sigma(C), \dim(F_\sigma) = \frac{c+f}{2}, \dim(E_\sigma) = \frac{c(p-1)}{2}$.

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 by $E_\sigma(C)^*$ the code $E_\sigma(C)$ with the last f coordinates deleted. 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 the set of even-weight polynomials in $\mathbb{F}_2[x]/\langle x^p - 1\rangle$. Thus we obtain the map $\varphi : E_\sigma(C)^* \to \mathcal{P}^c$. $\mathcal{P}$ is a cyclic code of length p with generator polynomial $x - 1$.

Manuscript received July 9, 2014; revised January 16, 2015; accepted January 19, 2015. Date of publication January 26, 2015; date of current version February 12, 2015. This work was supported in part by MEST under Grant 20012-002521 through KRF, Korea. N. Yankov was supported by Shumen University, Shumen, Bulgaria, under Project RD-03-243/12.03.2014.

N. Yankov and M. Ivanova are with the Faculty of Mathematics and Informatics, Shumen University, Shumen 9712, Bulgaria (e-mail: jankov_niki@yahoo.com; nicolova_m@abv.bg).

M. H. Lee is with the Institute of Information and Communication, Chonbuk National University, Jeonju 561-756, Korea (e-mail: moonho@jbnu.ac.kr).

M. Gürel is with the Department of Mathematics and Computer Science, İstanbul Aydın University, Istanbul 34295, Turkey (e-mail: muberragurel@hotmail.com).

Communicated by N. Kashyap, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2015.2396915

TABLE I
THE NUMBER OF CODEWORDS OF MINIMUM WEIGHT FOR $\varphi^{-1}(C_\varphi)$

# of codes	A_{12}	# of codes	A_{12}	# of codes	A_{12}	# of codes	A_{12}	# of codes	A_{12}	# of codes	A_{12}
1	55	616	187	1649	319	114	451	27	583	4	726
2	66	903	198	1357	330	116	462	15	594	1	748
1	77	1247	209	1142	341	76	473	10	605	3	759
2	88	1558	220	927	352	78	484	17	616	3	781
5	99	1860	231	756	363	65	495	3	627	1	792
5	110	2182	242	621	374	46	506	6	638	2	814
8	121	2326	253	482	385	43	517	8	649	1	825
22	132	2383	264	397	396	38	528	9	660	1	880
67	143	2417	275	259	407	38	539	3	671	1	913
112	154	2354	286	256	418	29	550	3	682		
220	165	2075	297	184	429	26	561	3	693		
350	176	1937	308	117	440	18	572	3	715		

TABLE II
THE ORDER OF THE AUTOMORPHISM GROUPS FOR $\varphi^{-1}(C_\varphi)$

$\lvert\mathrm{Aut}(C)\rvert$	11	22	44	55	66	110	132	264	550	660	6600
# of codes	28672	2738	141	6	39	3	6	3	1	1	1

Theorem 2.2 [24]: 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 $u, v \in C_\varphi = \varphi(E_\sigma(C)^*)$ we have $\sum_{i=1}^{c} u_i(x)v_i(x^{-1}) = 0$.

Furthermore, if 2 is a primitive root modulo p then C_φ is a self-dual code of length c over the field $\mathcal{P} \cong \mathbb{F}_{2^{p-1}}$ under the inner product $(u, v) = \sum_{i=1}^{c} u_i v_i^{2^{(p-1)/2}}$.

We also need the following.

Lemma 2.1 [24]: If σ is an automorphism of the binary self-dual code C with c cycles and f fixed points, and $g_2(k, d) = \sum_{i=0}^{k-1} \lceil d/2^i \rceil$ then:

1) $pc \geq g_2(\frac{(p-1)c}{2}, d)$;

2) if $f > c$, then $f \geq g_2((f - c)/2, d)$;

To classify the codes, we need additional conditions for equivalence. That's why we use the following theorem:

Theorem 2.3 [23]: The following transformations preserve the decomposition and send the code C to an equivalent one:

a) the substitution $x \to x^t$ in C_φ, where t is an integer, $1 \leq t \leq p - 1$;

b) multiplication of the jth coordinate of C_φ by x^{t_j} where t_j is an integer, $0 \leq t_j \leq p - 1$, $j = 1, 2, \ldots, c$;

c) permutation of the first c cycles of C;

d) permutation of the last f coordinates of C.

III. HERMITIAN $[6, 3]$ CODES OVER $\mathbb{F}_{2^{10}}$

By Theorem 2.2 since 2 is a primitive root modulo $p = 11$ we can conclude that the $\varphi(E_\sigma(C)^*)$ is an Hermitian $[6, 3, \geq 3]$ self-dual code over $\mathcal{P} \cong \mathbb{F}_{2^{10}}$ under the inner product

$$(u, v) = \sum_{i=1}^{6} u_i v_i^{32}. \tag{2}$$

$\mathcal{P}$ has identity $e(x) = x + x^2 + \cdots + x^{10}$ and a primitive element $\alpha = x + x^3 + x^5 + x^8 + x^9 + x^{10}$. Let $\delta = \alpha^{11}$ be an element of $\mathcal{P}$ with multiplicative order 93. Then we can represent $\mathcal{P} = \{0, x^i\delta^j \mid 0 \leq i \leq 10, 0 \leq j \leq 92\} \cong \mathbb{F}_{2^{10}}$.

Let C be a binary self-dual code with minimum distance $d = 12$, having an automorphism σ of order 11 with 6 cycles. Then (up to a transformation form Theorem 2.3) the generator matrix of the code $\varphi(E_\sigma(C)^*)$ is in the form

$$A = \begin{pmatrix} e & 0 & 0 & t_1 & t_2 & t_3 \\ 0 & e & 0 & t_4 & t_5 & t_6 \\ 0 & 0 & e & t_7 & t_8 & t_9 \end{pmatrix}, \tag{3}$$

where $t_i \in \{0, \delta^j, 0 \leq j \leq 92\}$, $i = 1, \ldots, 4, 7$, $t_l \in \mathcal{P}$, $l = 5, 6, 8, 9$.

Using the orthogonal condition (2) we computed all different cases for the first row in (3) that generate a code with minimum distance at least 12:

- When $t_1 = 0$ we have 3 inequivalent cases: $(t_1, t_2, t_3) = (0, \delta, \delta^{20})$, $(0, \delta, \delta^{51})$, and $(0, \delta^5, \delta^{39})$.
- When $t_1 \neq 0$ we have exactly 123 inequivalent cases.

Next we add the second and third row of (3). We summarize the final results in the following.

Theorem 3.1: Up to equivalence there are 31611 subcodes E_σ over $\mathcal{P}$ such that $\varphi^{-1}(C_\varphi)$ generates a code with minimum distance 12.

We list the number of codewords of weight 12 and the cardinality of the automorphism groups of all constructed codes in Table I and Table II, respectively.

IV. CONSTRUCTING CODES WITH AN AUTOMORPHISM OF TYPE 11-(6, f)

Denote by gen C a generator matrix of the code C. We have computed all possible generator matrices of $E_\sigma^*(C)$. Let us fix the E_σ^* part of

$$\text{gen } C = \begin{pmatrix} \text{gen } E_\sigma^* & O \\ \text{gen } F_\sigma & \end{pmatrix} \tag{4}$$

and consider all permutations of the 11-cycles in $F_\sigma(C)$ that can generate different binary codes C.

We construct $[n,k]$ self-dual codes with minimum distance $d = 12$ with an automorphism of order 11 with 6 cycles. There exists a $[76,38,14]$ binary self-dual code (see [1]) so $66 \le n \le 74$. In the case of a $[74,37,12]$ binary self-dual code we have automorphism of type 11-(6, 8). Thus $f > c$ and according to 2) from Lemma 2.1 then $8 = f \ge g_2(1,d) = 12$, which is a contradiction so this case is excluded.

Assume that we have a generator matrix B of a $[c+f, \frac{c+f}{2}]$ binary code that we can use in (4) substituting gen $F_\sigma = \pi^{-1}(B)$. For a permutation $\tau \in S_6$ denote by C_τ the self-dual code determined by the matrix (4) where as the generator matrix for F_σ we use $B\tau$. We fix the Hermitian part E_σ and consider the generator matrix of C is (4) for all $\tau \in S_6$.

If the number of fixed points is $f > 0$ then for all binary self-dual $[c+f, \frac{c+f}{2}]$ codes we have to choose a splitting of the set of coordinates $\{1,2,\ldots,c+f\}$ into two disjoint sets X_c – the cycle coordinates and X_f – the fixed coordinates in such a way that $d(F_\sigma(C)) \ge 12$.

A. [66,33,12] Codes With an Automorphism of Type 11−(6,0)

For a $[66,33,12]$ self-dual code there are three possible forms of the weight enumerator [5]:

$$W_{66,1} = 1 + 1690y^{12} + 7990y^{14} + 302705y^{16} + 867035y^{18} + \ldots,$$

$$W_{66,2} = 1 + (858+8\beta)y^{12} + (18678-24\beta)y^{14} + + \ldots,$$

where $0 \le \beta \le 778$ and

$$W_{66,3} = 1 + (858+8\beta)y^{12} + (18166-24\beta)y^{14} + + \ldots,$$

where $14 \le \beta \le 756$.

Codes exist with $W_{66,1}$; with $W_{66,2}$ for $\beta = 0$, 2, 3, 5, 6, 8, …, 11, 14, …, 18, 20, …, 29, 31, 32, 33, 35, 36, 37, 38, 40, …, 54, 56, 59, 60, 62, …, 69, 71, …, 74, 76, 77, 78, 80, 83, 86, 87, 92; and with $W_{66,3}$ for $\beta = 28, 33, 34, 54, 56, \ldots, 59, 62$ and 66 (see [10], [14], [18]).

For a binary $[66,33,12]$ self-dual codes with an automorphism of type 11-(6, 0) by Theorem 3.1 the subcode C_π is the unique $[6,3]$ binary self-dual code $3i_2$ [19]. By calculation all codes C_π for $\pi \in S_6$ we have the following result.

Proposition 4.1: There are exactly 5122 inequivalent binary $[66,33,12]$ self-dual codes having an automorphism of type 11-(6, 0).

All constructed codes have weight enumerator $W_{66,2}$ for $\beta = 11k$, $k = 0,\ldots,8$. We list the values of β and the order of the automorphism groups of all constructed codes in Table III. The values $\beta = 55$ and 88 were previously not known so we list the generators for a code with every new value in Table IV. Note that the codes with $|Aut(C)| = 66$, 330 and 660 are the double circulant codes from [8].

TABLE III
THE PARAMETERS OF [66, 33, 12] CODES, ALL WITH $W_{66,2}$

		$\|\mathrm{Aut}(C)\|$					
β	# of codes	11	22	66	220	330	660
0	317	300	15	1		1	
11	1044	1036	8				
22	1660	1633	26		1		
33	1229	1221	8				
44	600	587	13				
55	200	197	3				
66	60	58	1				1
77	11	9	2				
88	1	1					

B. [68,34,12] Codes With an Automorphism of Type 11−(6,2)

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

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

and

$$W_{68,2} = 1 + (442+4\beta)y^{12} + (14960-8\beta-256\gamma)y^{14} + \ldots,$$

where β, γ are integer parameters. Codes are known with both weight enumerators. For the most recent information on the known values of the parameters we refer the reader to [16].

There are exactly two $[8,4]$ binary self-dual codes $4i_2$ and e_8 [19]. In the case of $4i_2$ we cannot have the full support of any weight 2 vector in X_f, therefore assuming the first 6 coordinates correspond to the cycles of σ we get only one matrix for C_π that is $G_1 = \begin{pmatrix} 101000 & 00 \\ 000110 & 00 \\ 000001 & 10 \\ 010000 & 01 \end{pmatrix}$. The automorphism group of the extended Hamming code e_8 is 3-transitive so we can choose any two coordinates for X_f. Thus we have a unique matrix $G_2 = (I_4 | I_4 + A_4)$, where A_4 is the 4×4 all-one matrix.

Proposition 4.2: There are exactly 243789 inequivalent binary $[68,34,12]$ self-dual codes having an automorphism of type 11-(6, 2).

When $C_\pi = G_1$ we found 99721 codes all with $W_{68,2}$, $\gamma = 0$ for different values of β listed in Table V. Note that the values $\beta = 11$, 22, 33, 143, 154, 165, 176, 187, 198, 209, 220, 231, 308, and 330 are new.

When $C_\pi = G_2$ we found 144068 codes all with $W_{68,1}$ for different values of β listed in Table VI. The values $\beta = 115$, 247, 280, 291, 313, 324 and 379 are new. All codes with $|\mathrm{Aut}(C)| = 66, 132$ and 330 are bordered double circulant known from [8, Table 7]. Our results completely match Gulliver and Harada's results [8].

C. [70,35,12] Codes With an Automorphism of Type 11−(6,4)

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 β and γ are integer parameters. Only codes with $W_{70,1}$ for $\gamma = 1$, $\beta = 416$ (see [9]) and $\gamma = 0$

TABLE IV
THE GENERATORS OF SOME OF THE NEW [66, 33, 12] CODES

β	$t_1, t_2, \dots, t_9$	support of C_π
55	$0, \delta, \delta^{20}, \delta^2, x^9\delta^{60}, x^9\delta^{10}, \delta^{40}, x^9\delta^{53}, x^9\delta^3$	$\{1,4\}, \{2,5\}, \{3,6\}$
88	$e, \delta^3, \delta^{34}, \delta^{21}, x^8\delta^{80}, x^4\delta^{17}, \delta^{52}, x^7\delta^{85}, x^8\delta^{81}$	$\{1,5\}, \{2,6\}, \{3,4\}$

TABLE V
THE PARAMETERS OF [68, 34, 12] CODES WHEN $C_\pi = G_1$ ALL WITH $W_{68,2}$

		|Aut(C)|							|Aut(C)|		
β	# of codes	11	22	44	110	220	β	# of codes	11	22	44
11	22	20	2				143	1949	1687	262	
22	213	184	25	4			154	922	760	159	3
33	964	923	41				165	560	454	106	
44	3100	2980	110	9	1		176	347	249	91	7
55	7276	7068	208				187	154	125	29	
66	12648	12223	415	10			198	86	62	20	4
77	16787	16329	458				209	35	28	7	
88	17598	16979	607	11		1	220	17	6	9	2
99	14870	14357	513				231	8	6	2	
110	11232	10606	614	12			308	1			1
121	7032	6591	441				330	1		1	
132	3899	3506	388	5							

TABLE VI
THE PARAMETERS OF [68, 34, 12] CODES WHEN $C_\pi = G_2$ ALL WITH $W_{68,1}$

		|Aut(C)|								|Aut(C)|				
β	# of codes	11	22	44	66	132	330	β	# of codes	11	22	44	66	132
104	317	300	15		1		1	236	2715	2337	358	5	15	
115	1738	1631	105	2				247	1476	1215	251	10		
126	5412	5110	300	2				258	809	635	174			
137	11208	10657	532	7	12			269	414	284	120	3	7	
148	17023	16276	741	6				280	198	144	54			
159	21494	20570	904	20				291	93	50	42	1		
170	22012	21020	961	7	24			302	36	20	14		2	
181	19809	18678	1110	21				313	19	6	12	1		
192	15717	14797	910	10				324	12	1	11			
203	11487	10646	792	32	16	1		335	10		5	1	2	2
214	7425	6820	599	6				379	6		5	1		
225	4637	4151	467	19				401	1				1	

for $\beta = 138, 184, 230, 276, 322, 368, 414, 460,$ and 1012 (see [4]) are known.

There are two $[10, 5]$ binary self-dual codes $5i_2$ and $i_2 \oplus e_8$ [19]. In the case of $5i_2$ there is one possible generator matrix for C_π that is $G_3 = (I_5|I_5)$. The other code $i_2 \oplus e_8$ has two different configurations for X_c, X_f that generate codes with $d(F_\sigma(C)) \geq 12$. Therefore for $i_2 \oplus e_8$ we have two generator matrices:

$$G_4 = \left(I_5 \left| \begin{matrix} 00111 \\ 01000 \\ 10110 \\ 10101 \\ 10011 \end{matrix} \right. \right), \quad G_5 = \left(I_5 \left| \begin{matrix} 10000 \\ 00111 \\ 01011 \\ 01101 \\ 01110 \end{matrix} \right. \right).$$

Proposition 4.3: There are exactly 456164 inequivalent binary $[70, 35, 12]$ self-dual codes having an automorphism of type 11-$(6, 4)$.

When $C_\pi \cong G_3$ we have 74759 codes with weight enumerator $W_{70,1}$ all with new values of the parameters: $\gamma = 0$, $\beta = 112, 134, 156, 178, 200, 222, 244, 266, 288, 310, 332, 354, 376, 398, 420, 442, 464, 486, 508, 530, 552, 574, 596, 618$; $\gamma = 11$, $\beta = 618, 640, 662, 684$ and 706; $\gamma = 22$, $\beta = 684, 750, 772, 794$.

When $C_\pi \cong G_4$ we have 306048 codes with weight enumerator $W_{70,2}$ for $\beta = 204, 226, 226, 248, 270, 270, 292, 314, 314, 336, 358, 358, 380, 402, 402, 424, 446, 446, 468, 490, 490, 512, 534, 534, 556, 578, 600, 622, 644, 666, 798, 842$. This is the first time a code with the weight enumerator $W_{70,2}$ is constructed. For example the code with $\beta = 842$ has C_φ generated by $(t_1, t_2, \dots, t_9) = (\delta^0, \delta, \delta^{63}, \delta^{62}, x^7\delta^{36}, x^4\delta^{25}, \delta^{62}, x^3\delta^{43}, x^8\delta^{51})$ and $C_\pi = G_4$.

In the case $C_\pi \cong G_5$ we found 75357 codes with $W_{70,1}, \gamma = 0$ most having new values $\beta = 88, 110, 132, 154, 176, 198, 220, 242, 264, 286, 308, 330, 352, 374, 396, 418, 440, 462, 484, 506, 528, 1012$. Only the code with $\beta = 1012$ was previously known [4].

D. [72,36,12] Codes With an Automorphism of Type 11−(6,6)

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

$$W_{72} = 1 + (4398 + \alpha)y^{12} + (197073 - 12\alpha)y^{16} + (18396972 + 66\alpha)y^{20} + \dots$$

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 are known: $\gamma = 0$, $\beta = 209, 263, 309, 317, 335$; $\gamma = 11$, $\beta = 859$ (see [3], [6], [16]).

According to Theorem 2.2, we have that C_π is a binary self-dual $[12, 6]$ code. There are three such codes $6i_2$, $2i_2 \oplus e_8$ and b_{12}. After finding all different splittings of the coordinates $\{1, \dots, 12\}$ into X_c and X_f we have 4 generator matrices such that C_π is a $[72, 6, \geq 12]$ binary code: $G_6 = (I_6|I_6)$,

$$G_7 = \left(\begin{array}{c|c} & 101111 \\ & 011111 \\ I_6 & 111000 \\ & 110100 \\ & 110010 \\ & 110001 \end{array}\right), \quad G_8 = \left(\begin{array}{c|c} & 011111 \\ & 101111 \\ I_6 & 110111 \\ & 111011 \\ & 111101 \\ & 111110 \end{array}\right),$$

$$G_9 = \left(\begin{array}{c|c} & 101111 \\ & 011111 \\ I_6 & 111000 \\ & 110100 \\ & 110010 \\ & 110001 \end{array}\right),$$

obtained from $6i_2$, $2i_2 \oplus e_8$, b_{12} and b_{12}, respectively.

Proposition 4.4: There are exactly 63147 inequivalent binary doubly-even $[72, 36, 12]$ self-dual codes having an automorphism of type 11-(6, 6). There are exactly 394368 inequivalent binary singly-even $[72, 36, 12]$ self-dual codes having an automorphism of type 11-(6, 6).

For $C_\pi \cong G_6$ we have found 31536 doubly-even $[72, 36, 12]$ codes with weight enumerator W_{72} for $\alpha = -4062, -3996, -3930, -3864, -3798, -3732, -3666, -3600, -3534, -3468, -3402, -3336, -3270, -3204, -3138, -3072, -3006, -2940, -2874, -2808, -2742, -2676, -2610, -2544, -2412, -2016, -1356$. The values $\alpha = -4062, -3996, -3930, -2940, -2808, -2610, -2544, -2412, -2016$ are new. We have found that a code for $\alpha = -3600$ has $|\mathrm{Aut}(C)| = 7920$ and a code for $\alpha = -1356$ has $|\mathrm{Aut}(C)| = 79200$. These codes are known from [16, Table 4].

When $C_\pi \cong G_7$ there are exactly 196754 singly-even $[72, 36, 12]$ codes with weight enumerator $W_{72,2}$ for 150 different values of β and γ: $\gamma = 0, \beta \in \{1 + 11m \mid 7 \leq m \leq 48, m = 51, 52, 54, 56\}$; $\gamma = 11, \beta \in \{1 + 11m \mid 13 \leq m \leq 48, m = 50, 51, 52, 54, 56, 58, 60, 62, 78\}$; $\gamma = 22, \beta \in \{1 + 11m \mid 23 \leq m \leq 54\}$; $\gamma = 33, \beta \in \{1 + 11m \mid 38 \leq m \leq 57, m = 59, 60, 61, 62\}$; $\gamma = 44, \beta \in \{606, 617, 727\}$. All the above values of the parameters except $\gamma = 0$, $\beta = 309$ and $\gamma = 11$, $\beta = 859$, $|\mathrm{Aut}(C)| = 440$ (see [16] for both) are new.

In the case $C_\pi \cong G_8$ we found 31611 doubly-even $[72, 36, 12]$ codes with weight enumerator W_{72} for 26 values $\alpha = -4134, -4068, -4002, -3936, -3870, -3804, -3738, -3672, -3606, -3540, -3474, -3408, -3342, -3276, -3210, -3144, -3078, -3012, -2946, -2880, -2814, -2748, -2682, -2616, -2418, -1362$. Seven of the values: $\alpha = -4134, -4068, -4002, -3804, -2748, -2682$, and -2418 are new.

Lastly, when $C_\pi \cong G_9$ there are 197614 singly-even $[72, 36, 12]$ codes with weight enumerator $W_{72,2}$ for 153 different values of β and γ: $\gamma = 0, \beta \in \{11m \mid 6 \leq m \leq 44, m = 47, 59, 68, 74, 76\}$; $\gamma = 11$, $\beta \in \{11m \mid 13 \leq m \leq 54, m = 56, 58\}$; $\gamma = 22$, $\beta \in \{11m \mid 23 \leq m \leq 57\}$; $\gamma = 33, \beta \in \{11m \mid 36 \leq m \leq 38, 40 \leq m \leq 58, 60 \leq m \leq 64\}$; $\gamma = 44$, $\beta \in \{605, 627, 737\}$. All values are new except $\gamma = 0$, $\beta = 209$ known from [16].

Remark 4.1: The computations were made by two of the authors independently. Both computations match exactly. One of the computations use **GAP 4.7** [7] for the generation of the codes and **Q-extension** [2] for the code equivalence. The second computation was made with own Delphi code for code generation and **Q-extension** for the code equivalence. Some examples for the new codes can be accessed online at [22].

Acknowledgment

The authors would like to thank the anonymous referees for the helpful comments and suggestions, which significantly contributed to improving the quality of the publication.

References

[1] A. Baartmans and V. Yorgov, "Some new extremal codes of lengths 76 and 78," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1353–1354, May 2003.

[2] I. G. Bouyukliev, "About the code equivalence," in *Advances in Coding Theory and Cryptography* (Series on Coding Theory and Cryptology), vol. 3. Singapore: World Scientific, 2007, pp. 126–151.

[3] J. Conway and N. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1319–1333, Nov. 1991.

[4] R. Dontcheva, "New binary [70, 35, 12] self-dual and binary [72, 36, 12] self-dual doubly-even codes," *Serdika Math. J.*, vol. 27, no. 4, pp. 287–302, 2001.

[5] S. T. Dougherty, T. A. Gulliver, and M. Harada, "Extremal binary self-dual codes," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 2036–2047, Nov. 1997.

[6] S. Dougherty, J.-L. Kim, and P. Solé, "Double circulant codes from two class association schemes," *Adv. Math. Commun.*, vol. 1, no. 1, pp. 45–64, 2007.

[7] The GAP Group. (2014). *GAP—Groups, Algorithms, and Programming, Version 4.7*. [Online]. Available: http://www.gap-system.org

[8] T. A. Gulliver and M. Harada, "Classification of extremal double circulant self-dual codes of lengths 64 to 72," *Designs, Codes Cryptograph.*, vol. 13, no. 3, pp. 257–269, 1998.

[9] M. Harada, "The existence of a self-dual [70, 35, 12] code and formally self-dual codes," *Finite Fields Appl.*, vol. 3, no. 2, pp. 131–139, Apr. 1997.

[10] M. Harada, T. Nishimura, and R. Yorgova, "New extremal self-dual codes of length 66," *Math. Balkanica (New Ser.)*, vol. 21, nos. 1–2, pp. 113–121, 2007.

[11] W. Huffman, "Automorphisms of codes with applications to extremal doubly even codes of length 48," *IEEE Trans. Inf. Theory*, vol. 28, no. 3, pp. 511–521, May 1982.
[12] W. C. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields Appl.*, vol. 11, no. 3, pp. 451–490, Aug. 2005.
[13] W. C. Huffman and V. Yorgov, "A [72, 36, 16] doubly even code does not have an automorphism of order 11 (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 33, no. 5, pp. 749–752, Sep. 1987.
[14] S. Karadeniz and B. Yildiz, "New extremal binary self-dual codes of length 66 as extensions of self-dual codes over R_k," *J. Franklin Inst.*, vol. 350, no. 8, pp. 1963–1973, 2013.
[15] A. Kaya and B. Yildiz. (2014). "Extension theorems for self-dual codes over rings and new binary self-dual codes." [Online]. Available: http://arxiv.org/abs/1404.0195
[16] A. Kaya, B. Yildiz, and I. Siap, "New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$," *Finite Fields Appl.*, vol. 29, pp. 160–177, Sep. 2014.
[17] N. Sloane, "Is there a (72, 36) $d = 16$ self-dual code? (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 19, no. 2, p. 251, Mar. 1973.
[18] H.-P. Tsai, P.-Y. Shih, R.-Y. Wu, W.-K. Su, and C.-H. Chen, "Construction of self-dual codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3826–3831, Aug. 2008.
[19] W. C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[20] E. M. Rains, "Shadow bounds for self-dual codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 134–139, Jan. 1998.
[21] N. Yankov and M. H. Lee, "Classification of self-dual codes of length 50 with an automorphism of odd prime order," *Designs, Codes Cryptograph.*, 2013, doi: 10.1007/s10623-013-9874-8.
[22] N. Yankov, M. H. Lee, M. Gürel, and M. Nikolova. *Supplementary Data for Binary Self-Dual Codes With an Automorphism of Order 11*. [Online]. Available: http://shu.bg/tadmin/upload/storage/1467.pdf, accessed Nov. 25, 2014.
[23] V. Yorgov, "A method for constructing inequivalent self-dual codes with applications to length 56," *IEEE Trans. Inf. Theory*, vol. 33, no. 1, pp. 77–82, Jan. 1987.
[24] V. I. Yorgov, "Binary self-dual codes with automorphisms of odd order," *Problems Inf. Transmiss.*, vol. 19, no. 4, pp. 260–270, 1983.
[25] V. Y. Yorgov, "New extremal singly-even self-dual codes of length 44," in *Proc. 6th Joint Swedish-Russian Int. Workshop Inf. Theory*, Mölle, Sweden, 1993, pp. 372–375.
[26] V. I. Yorgov and R. Ruseva, "Two extremal codes of length 42 and 44," *Problems Inf. Transmiss.*, vol. 29, no. 4, pp. 385–388, 1993.

Nikolay Yankov received the M.S. and Ph.D. degrees both from University of Shumen, Bulgaria in 1997 and 2006, respectively. He is currently an Associate Professor at the Faculty of Mathematics and Informatics, University of Shumen, Bulgaria. His research interests include coding theory, discrete mathematics and linear algebra.

Moon Ho Lee is a professor and former chair of the Department of Electronics Engineering at Chonbuk National University, Korea. He received the Ph.D. degree from Chonnam National University, Korea in 1984, and from the University of Tokyo, Japan in 1990, both Electrical Engineering. He was in University of Minnesota, U.S.A, from 1985 to 1986 as a post-doctor. He has been working in Namyang MBC broadcasting with chief engineer from 1970 to 1980, after then he joined to Chonbuk National University as a Professor. Dr. Lee has made significant original contributions in the areas of mobile communication code design, multi-dimensional source and channel coding. Dr. Lee is a member of the National Academy of Engineering in Korea. He is the inventor of Jacket Matrix.

Müberra Gürel joined the İstanbul Aydın University Mathematics-Computer Programing Department in 2012. She is currently assistant professor. She received both the M.S. degree in 2005 and Ph.D. degree in 2012 in Mathematics from Fatih University, İstanbul, Turkey under the direction of Barış Kendirli. Müberra Gürel's research interests include number theory, algebra, coding theory and cryptography.

Milena Ivanova received the M.S. degree from University of Shumen, Bulgaria in 1997. She is currently an Associate Assistant at the Faculty of Mathematics and Informatics, University of Shumen, Bulgaria. Her research interests include coding theory, and linear algebra.