AAECC (2021) 32:97–111
https://doi.org/10.1007/s00200-019-00403-0

ORIGINAL PAPER

On the self-dual codes with an automorphism of order 5

Nikolay Yankov[1] · Damyan Anev[1]

Received: 4 May 2018 / Revised: 8 September 2018 / Accepted: 1 November 2019 /
Published online: 7 November 2019

Abstract

For lengths 60, 62, and 64, by applying the method for constructing self-dual codes having an automorphism of odd prime order, we classify all optimal singly even self-dual codes with an automorphism of order 5 with 12 cycles. For the binary self-dual [62, 31, 12] codes we have found five new values of the parameter in the weight enumerator thus doubling the number of know values. For length 64 we have found codes with 14 new parameter values for both known weight enumerators. By shortening all binary self-dual [60, 30, 12] codes having an automorphism of order 5 we construct many new [58, 29, 10] self-dual codes. We have found a new value of the parameter in the weight enumerator of these codes.

Keywords Automorphism · Classification · Self-dual codes · Shortening

Mathematics Subject Classification 94B05 · 11T71

1 Introduction

Let $\mathbb{F}_q$ be the finite field of q elements, for a prime power q. A linear $[n, k]_q$ *code* C is a k-dimensional subspace of $\mathbb{F}_q^n$. The elements of C are called *codewords*, and the *(Hamming) weight* of a codeword $v \in C$ is the number of the non-zero coordinates of v. We use $\mathrm{wt}(v)$ to denote the weight of a codeword. The *minimum weight* d of C is the minimum nonzero weight of any codeword in C and the code is called an $[n, k, d]_q$ code. A matrix whose rows form a basis of C is called a *generator matrix* of this code.

✉ Nikolay Yankov
jankov_niki@yahoo.com

Damyan Anev
damian_anev@mail.bg

1 Faculty of Mathematics and Informatics, Konstantin Preslavski University of Shumen, 9712 Shumen, Bulgaria

Table 1 Self-dual codes with an automorphism of order 5 with 10 cycles

$[50, 25, 10]_{SE}$,#270	$[52, 26, 10]_{SE}$,#18777	$[54, 27, 10]_{SE}$,#119162
$[56, 28, 12]_{DE}$,#3763	$[58, 29, 10]_{SE}$,#1823426	$[60, 30, 12]_{SE}$,#79

Let $(u, v) \in \mathbb{F}_q$ for $u, v \in \mathbb{F}_q^n$ be an inner product in $\mathbb{F}_q^n$. The *dual code* of an $[n, k]_q$ code C is $C^\perp = \{u \in \mathbb{F}_q^n \mid (u, v) = 0 \text{ for all } v \in C\}$ and $C^\perp$ is a linear $[n, n-k]_q$ code. In the binary case the inner product is the standard one, namely, $(u, v) = \sum_{i=1}^{n} u_i v_i$. If $C \subseteq C^\perp$, C is termed *self-orthogonal*, and if $C = C^\perp$, C is *self-dual*. A binary self-dual code is *doubly-even* if all codewords have weight divisible by four, and *singly-even* if there is at least one nonzero codeword of weight $\equiv 2 \pmod 4$. Self-dual doubly-even codes exist only if n is a multiple of eight.

The weight enumerator $W(y)$ of a code C is defined as $W(y) = \sum_{i=0}^{n} A_i y^i$, where A_i is the number of codewords of weight i in C. We say that two binary linear codes C and C' are *equivalent* if there is a permutation of coordinates which sends C to C'. The set of coordinate permutations that maps a code C to itself forms a group called the *automorphism group* of C (denoted by $\mathrm{Aut}(C)$). Let S_n be the symmetric group of degree n. We say that a permutation $\sigma \in S_n$ is of *type* $p-(c, f)$ if it has exactly c cycles of length p and f fixed point in its decomposition.

All optimal binary self-dual codes of lengths 52–60 having an automorphism of order 7 or 13 were classified in [1].

Recently, all codes of lengths $50 \le n \le 60$ having an automorphism of type 5-$(10, f)$ for $f = 0, 2, 4, 6, 8$ and 10 were classified up to equivalence in [2]. For comparison reasons, we give the information for the number of inequivalent such codes, in Table 1.

From [3, Table 3] we have the following cases for the length n and the type of automorphism: $n = 60 + 2t$, type 5-$(12, 2t)$, $t = 0, 1, \ldots, 5$. So we have been intrigued to investigate and classify optimal self-dual codes of lengths $60 \le n \le 64$ with an automorphism of order 5 with 12 cycles. To do so we continue with some properties of the binary self-dual codes having an automorphism of prime odd order.

2 Construction method

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

$$\begin{aligned}\sigma = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \cdots (p(c-1)+1,\\ p(c-1)+2, \ldots, pc),\end{aligned} \tag{1}$$

of type $p-(c, f)$, where $f = n - pc$. 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 $F_\sigma(C) = \{v \in C \mid v\sigma = v\}$, $E_\sigma(C) = \{v \in C \mid wt(v|\Omega_i) \equiv 0 \pmod 2, i = 1, \ldots, c+f\}$, where $v|\Omega_i$ is the restriction of v on Ω_i.

Theorem 1 [4] *Assume C is a self-dual code having an automorphism of type $p-(c, f)$. The code C is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$. Then $F_\sigma(C)$ and $E_\sigma(C)$ are subspaces of dimensions $\frac{c+f}{2}$ and $\frac{(p-1)c}{2}$, respectively.*

From the definition of $F_\sigma(C)$ it follows 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 $v|\Omega_i = (v_0, v_1, \ldots, v_{p-1})$ correspond to the polynomial $v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$ from $\mathcal{P}$, where $\mathcal{P}$ is the set of even-weight polynomials in $\mathbb{F}_2[x]/\langle x^p - 1\rangle$. Thus we obtain the map $\varphi : E_\sigma(C)^* \to \mathcal{P}^c$.

Theorem 2 [5] *A binary $[n, n/2]$ code C with an automorphism σ defined in (1) 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 $u, v \in C_\varphi = \varphi(E_\sigma(C)^*)$ we have $\sum_{i=1}^{c} u_i(x)v_i(x^{-1}) = 0$. 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 $(u, v) = \sum_{i=1}^{c} u_i v_i^{2^{(p-1)/2}}$.

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

Theorem 3 [6] *The following transformations preserve the decomposition and send the 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 and (iv) a multiplication of the j-th coordinate of C_φ by x^{t_j} where t_j is an integer, $0 \le t_j \le p-1$, $j = 1, 2, \ldots, c$.*

3 Self-dual codes with twelve cycles of length five

Let C be an optimal binary self-dual code having an automorphism of order 5 with 12 cycles and $f = 2t$, $t = 0, \ldots, 5$ fixed points. Since 2 is a primitive root modulo 5, according to Theorem 2, the subcode C_φ is a self-dual code of length c over the field $\mathcal{P}$ under the inner product

$$(u, v) = \sum_{i=1}^{c} u_i v_i^4. \tag{2}$$

Furthermore $\mathcal{P}$ is a finite field with 16 elements, $\mathcal{P} \cong \mathbb{F}_{16} = \{0, e = \alpha^0, \alpha^k | k = 1, \ldots, 14\}$, where $e = x + x^2 + x^3 + x^4$, $\alpha = 1 + x$ is a primitive element of multiplicative order 15. We list the elements of $\mathcal{P}^*$—the multiplicative group of $\mathcal{P}$ in Table 2. Denoting $\delta = \alpha^5$ the group $\mathcal{P}^*$ can also be described as $\mathcal{P}^* = \{\alpha^{3t}\delta^l \mid 0 \le t \le 4, 0 \le l \le 2\}$.

Table 2 The multiplicative group of the field $\mathcal{P}^* \cong \mathbb{F}_{16}^*$

e	01111	α	11000	α^2	10100
α^3	11110	α^4	10001	α^5	01001
α^6	11101	α^7	00011	α^8	10010
α^9	11011	α^{10}	00110	α^{11}	00101
α^{12}	10111	α^{13}	01100	α^{14}	01010

Table 3 Cases for the first row of G_φ

$v_1 = (0, 0, 0, 0, 0, e)$	$v_2 = (0, 0, 0, e, e, e)$	$v_3 = (0, 0, 0, e, \delta, \delta)$
$v_4 = (0, 0, 0, e, \delta^2, \delta^2)$	$v_5 = (0, 0, e, e, \delta, \delta^2)$	$v_6 = (0, e, \delta, \delta, \delta, \delta)$
$v_7 = (0, e, \delta^2, \delta^2, \delta^2, \delta^2)$	$v_8 = (0, e, \delta, \delta, \delta^2, \delta^2)$	$v_9 = (0, e, e, e, e, e)$
$v_{10} = (0, e, e, e, \delta, \delta)$	$v_{11} = (0, e, e, e, \delta^2, \delta^2)$	$v_{12} = (e, e, \delta, \delta, \delta, \delta^2)$
$v_{13} = (e, e, \delta, \delta^2, \delta^2, \delta^2)$	$v_{14} = (e, e, e, e, \delta, \delta^2)$	

Proposition 1 *Let C_φ be a self-dual code of length* 12 *over $\mathcal{P}$ under the orthogonality condition* (2)*, such that $E_\sigma(C)$ is a code with minimum weight at least* 12*. Then the code C_φ has a generator matrix*

$$\left(\begin{array}{c|cccccc} & t_{11} & t_{12} & t_{13} & t_{14} & t_{15} & t_{16} \\ & t_{21} & l_{22} & l_{23} & l_{24} & l_{25} & l_{26} \\ & t_{31} & l_{32} & l_{33} & l_{34} & l_{35} & l_{36} \\ eI_6 & t_{41} & l_{42} & l_{43} & l_{44} & l_{45} & l_{46} \\ & t_{51} & l_{52} & l_{53} & l_{54} & l_{55} & l_{56} \\ & t_{61} & l_{62} & l_{63} & l_{64} & l_{65} & l_{66} \end{array}\right), \tag{3}$$

$t_{ij} \in \{0, e, \delta, \delta^2\}$, $j = 1, \ldots, 6$, $l_{ij} \in \mathcal{P}$*. Furthermore* $(t_{11}, \ldots, t_{16})$ *is one of the following seven vectors* $(0, 0, e, e, \delta, \delta^2)$, $(0, e, \delta, \delta, \delta, \delta)$, $(0, e, \delta, \delta, \delta^2, \delta^2)$, $(0, e, e, e, e, e)$, $(0, e, e, e, \delta, \delta)$, $(e, e, \delta, \delta, \delta, \delta^2)$, $(e, e, e, e, \delta, \delta^2)$.

Proof We begin by row reducing the matrix G_φ. Using transformation (iv) from Theorem 3 we can assume that the elements in the first row of G_φ are from the set $\{0, e, \delta, \delta^2\}$. Assume we use the following partial ordering in $\mathcal{P}$ $0 \prec e \prec \delta \prec \delta^2$. Further interchanging the columns of G_φ, it follows that, we can take $0 \preceq t_{11} \preceq t_{12} \preceq t_{13} \preceq t_{14} \preceq t_{15} \preceq t_{16} \preceq \delta^2$. Using (2) we can reduce the vector $v = (t_{11}, \ldots, t_{16})$ to cases listed in Table 3. The transformation $\gamma : x \to x^2$, (iii) from Theorem 3, maps δ to δ^2 and vice versa and we have $v_4 \xrightarrow{\gamma} v_3$, $v_7 \xrightarrow{\gamma} v_6$, $v_{11} \xrightarrow{\gamma} v_{10}$, $v_{13} \xrightarrow{\gamma} v_{12}$.

Obviously, the vectors $(e, 0, \ldots, 0, v_1)$, $\delta(e, 0, \ldots, 0, v_2)$, and $\delta(e, 0, \ldots, 0, v_3)$ have weight 8, which concludes this proof.

Since $\mathcal{P}^* = \{\alpha^{3t}\delta^l\}$, $0 \le t \le 4$, $0 \le l \le 2$ every element $t_{j1} \in \mathcal{P}^*$, $j = 2, \ldots, 6$ can be transformed into e, δ or δ^2 using a multiplication of j-th row of G_φ by α^{-3t}, followed by some cyclic shifts in the j-th column. □

By using a computer for calculating the possible second row of the matrix (3) we have found 242 inequivalent codes. Of these 242 codes: 66 are obtained from v_5, 136

Table 4 The order of the automorphism groups of optimal codes over $\mathbb{F}_{16}$

$\lvert\mathrm{Aut}(C)\rvert$	5	10	15	20	30	40	50	60	80
#	56,190	3815	24	310	32	34	7	28	6
$\lvert\mathrm{Aut}(C)\rvert$	90	100	120	160	200	240	1200	13,200	
#	1	2	8	4	2	2	1	1	

from v_6, 123 from v_8, 17 from v_9, 136 from v_{10}, 193 from v_{11}, and 137 from v_{14} (note that we have some codes that can be obtained from different first row).

Next for each of these 242 inequivalent codes we add a third row and check the result codes for minimum weight and equivalence. Of the 690,626 constructed codes there are exactly 35,191 inequivalent codes after row 3. Then for every one of these codes we add a fourth row and again check the result codes for minimum weight and equivalence. It turns out that there are exactly 681,862 inequivalent such codes (out of a total of 9,084,240 codes).

After that we added the fifth and sixth row of the matrix and check the resulted codes for equivalence and that their minimum weight is at least 12. After checking 7,197,760 codes our exhaustive computer search shows the following result.

Proposition 2 *Up to permutational equivalence there are exactly* 60,467 *codes* C_φ *over* $\mathcal{P}$ *such that the code* $\varphi^{-1}(C_\varphi)$ *has a minimum weight* 12. *Six of these codes have minimum weight 16 and the rest have minimum weight 12.*

The number of the different values of $|\mathrm{Aut}(C)|$ of the constructed codes is given in Table 4.

Denote by H_i, $i = 1, \ldots, 60{,}467$, the generator matrices of the codes obtained. These matrices can be obtained from [7]. For equivalence check and also for finding the weight distribution of the codes obtained we use the program Q-extensions [8] (Table 5).

Remark 1 The calculations involving the construction of the rows of the matrices H_i have been performed by both authors independently. The first author used own Delphi source code for code generation, the total CPU-time for the computation was about a week on a 3 GHz processor. The second author used GAP 4.8 [9] for the generation of the codes. This computation took about two weeks. Both authors constructed the same result with a total of 60,467 codes.

4 [60, 30, 12] binary self-dual codes with an automorphism of type 5-(12, 0)

Let C be a $[60, 30, 12]$ binary self-dual code with an automorphism of type 5-(12, 0). There are two possible forms for the weight enumerator of a binary self-dual $[60, 30, 12]$ code [10]:

Table 5 The number of optimal codes with A_d over $\mathbb{F}_{16}$

$d = 12$										
A_d	15	20	25	30	35	40	45	50	55	60
#	1	5	2	9	16	35	36	93	118	207
A_d	65	70	75	80	85	90	95	100	105	110
#	328	544	690	994	1327	1702	2113	2527	2951	3483
A_d	115	120	125	130	135	140	145	150	155	160
#	3780	3927	4039	4166	3990	3844	3610	3191	2677	2269
A_d	165	170	175	180	185	190	195	200	205	210
#	1775	1602	1145	882	637	496	367	244	162	126
A_d	215	220	225	230	235	240	245	250	255	260
#	77	55	49	51	31	31	20	10	4	6
A_d	265	270	275	280	320	390				
#	1	3	4	5	3	1				
$d = 16$										
A_d	10,395	10,410	10,420	10,450	10,455	10,470				
#	1	1	1	1	1	1				

$$W_{60,1} = 1 + 3451y^{12} + 24{,}128y^{14} + 33{,}6081y^{16} + \cdots,$$
$$W_{60,2} = 1 + (2555 + 64\beta)y^{12} + (33{,}600 - 384\beta)y^{14} + \cdots, \quad 0 \le \beta \le 10.$$

A code exists for $W_{60,1}$ [10] and for $W_{60,2}$ when $\beta = 0, 1, 2, 5, 6, 7,$ and 10 [11].

By Theorem 2 the code C_π is a $[12, 6]$ binary self-dual code. There are exactly three such codes $6i_2$, $2i_2 + h_8$ and d_{12} (see [12]). We have that any 2-weight vector in C_π will lead to a 10-weight vector in $F_\sigma(C)$ therefore we look for a $[12, 6, 4]$ and thus the only possible code is d_{12}.

Let Q_1 be the automorphism group of the code d_{12} with the generator matrix $G_1 = \begin{pmatrix} I_6 | & \begin{matrix} I_4 & A \\ A^T & I_4 \end{matrix} \end{pmatrix}$, where A in a 2×4 all-ones matrix. We have

$$Q_1 = \langle (1, 3, 8)(2, 7, 9), (1, 11, 6, 4, 2, 9)(3, 7, 12, 5, 10, 8) \rangle, \quad |Q_1| = 23{,}040.$$

For a permutation $\tau \in S_{12}$ denote by $C^\tau_{1,j}$, $j = 1, \ldots, 60{,}467$ the $[62, 31]$ self-dual code determined by the matrix G_1, with columns permuted by τ, as a generator for $F_\sigma(C)$ and H_j as a generator matrix for $E_\sigma(C)^*$. If τ_1 and τ_2 belong to one and the same right coset of Q_1 in S_{12}, then the codes $C^{\tau_1}_{1,j}$ and $C^{\tau_2}_{1,j}$ are equivalent. Thus we can only use the right transversal T_1 of S_{12} with respect to Q_1, we have $|T| = 20{,}790$. After calculating all codes $C^\tau_{1,j}$, $j = 1, \ldots, 60{,}467$ for $\tau \in T_1$ we obtain the following result.

Theorem 4 *Up to equivalence, there are exactly* 236 *optimal binary self-dual* $[60, 30, 12]$ *codes having an automorphism of type* 5-(12, 0).

Table 6 The number of codes obtained for the pair $(\beta, |\mathrm{Aut}(C)|)$

	$\lvert\mathrm{Aut}(C)\rvert$										
	5	10	15	20	30	40	60	100	120	240	4000
$\beta = 0$		8		21	4	6	8		3		
$\beta = 5$		11									
$\beta = 10$	38	75	3	20	19	2	14	2		1	1

Remark 2 All codes that we have obtained have weight enumerator $W_{60,2}$. The number of inequivalent codes for the pairs $(\beta, |\mathrm{Aut}(C)|)$ are summarized in Table 6.

Amongst codes, constructed by us, we have found 13 codes, equivalent to the codes from [13].

5 [62, 31, 12] binary self-dual codes with automorphism of type 5-(12, 2)

For the self-dual [62, 31, 12] code there are two possibilities [10]:

$$W_{62,1} = 1 + 2308y^{12} + 23{,}767y^{14} + 279{,}405y^{16} + \cdots,$$
$$W_{62,2} = 1 + (1860 + 32\beta)y^{12} + (28{,}055 - 160\beta)y^{14} + \cdots,$$

where β is an integer parameter $0 \le \beta \le 93$. Only codes with weight enumerator $W_{62,2}$ where $\beta = 0, 9, 10, 15, 16$ are known (see [3,13,14] and [15]).

According to Theorem 2 C_π is a [14, 7] binary self-dual code. Using [12], there are exactly four such codes, namely $7i_2$, $3i_2 \oplus e_8$, $i_2 \oplus d_{12}$, and $2e_7$. If a 2-weight codeword occur in C_π then the minimum weight of C is $d \le 10$ therefore only a [14, 7, 4] code can generate C_π. Thus we have $C_\pi \cong 2e_7$. Choosing all $\binom{14}{2}$ splittings of $\{1, \ldots, 14\}$ into sets X_c of cyclic and X_f – fixed points we found two different codes C_π generated by $G_2 = (I_7|Z_2)$ and $G_3 = (I_7|Z_3)$, where $Z_2 = \begin{pmatrix} 1&1&1&0&0&0&0\\ 0&1&1&0&1&1&1\\ 1&0&1&0&1&1&1\\ 1&1&0&0&1&1&1\\ 0&0&0&1&0&1&1\\ 0&0&0&1&1&0&1\\ 0&0&0&1&1&1&0 \end{pmatrix}$, $Z_3 = \begin{pmatrix} 1&1&0&0&0&1&0\\ 0&1&0&1&1&1&1\\ 1&0&0&1&1&1&1\\ 1&1&0&1&1&0&1\\ 0&0&1&0&1&0&1\\ 0&0&1&1&0&0&1\\ 0&0&1&1&1&0&0 \end{pmatrix}$, and the generator matrices are given so that $X_f = \{13, 14\}$.

Table 7 Codes obtained with different β using the matrix G_2

β	1	6	11	16	21
#	429	718	523	138	91

Although we have constructed the two direct summands for the code C we have to attach them together. Let the subcode $F_\sigma(C)$ be fixed as generated by the matrix G_2 or G_3. We have to consider all (even equivalent) possibilities for the second subcode $E_\sigma(C)$.

Let $Q_i, i = 2, 3$ be the subgroup of the automorphism group of the [14, 7] binary code generated by G_i consisting of the automorphisms of this code that permute the first 12 coordinates (corresponding to the 5-cycle coordinates) among themselves and permute the last 2 coordinates (corresponding to the fixed point coordinates) among themselves. Let $St_i, i = 2, 3$ be the subgroup of the symmetric group S_{12} consisting of the permutations in Q_i restricted to the first 12 coordinates, ignoring the action on the fixed points. We have:

$$St_2 =\langle(1, 9, 4, 2)(3, 8)(5, 11), (1, 10, 9, 4, 2, 8, 3)(5, 7)(6, 11)\rangle,$$
$$St_3 =\langle(1, 3, 9)(2, 4, 8)(5, 10)(6, 7), (1, 10, 2, 12, 3, 5)(4, 7, 9, 11, 8, 6)\rangle,$$

$|St_2| = 1344$, and $|St_3| = 1152$.

For a permutation $\tau \in S_{12}$ denote by $C^\tau_{i,j}, i = 2, 3,\ j = 1, \ldots, 60{,}467$ the [62, 31] self-dual code determined by the matrix G_i, with columns permuted by τ, as a generator for $F_\sigma(C)$ and H_j as a generator matrix for $E_\sigma(C)^*$. If τ_1 and τ_2 belong to one and the same right coset of St_2 (or St_3) in S_{12}, then the codes $C^{\tau_1}_{i,j}$ and $C^{\tau_2}_{i,j}$ are equivalent. Thus we can only use the right transversals T_2 and T_3 of S_{12} with respect to St_2 and St_3. We have calculated $|T_2| = 356{,}400$, $|T_3| = 415{,}800$. After calculating all codes $C^\tau_{i,j}, i = 2, 3,\ j = 1, \ldots, 60{,}467$ for $\tau \in T_i,\ i = 2, 3$ we summarize the results as follows.

Theorem 5 *In total there are exactly* 4636 *inequivalent binary self-dual* [62, 31, 12] *codes with an automorphism of type* 5-(12, 2). *There exist binary self-dual* [62, 31, 12] *codes with weight enumerator* $W_{62,2}$ *for* $\beta = 0, 1, 6, 11$ *and* 21.

Remark 3 We have checked a total of more than 46 billion codes. Computational time for this length was about a week on a 4 core 3Ghz CPU. We have the following result.

The complete information on codes obtained is listed in Table 7 for codes when C_π is generated by G_2 and in Table 8 for the other case. Our results show only codes with weight enumerator $W_{62,2}$. The codes in Table 7 all have $|\mathrm{Aut}(C)| = 5$ that is the reason we only give their weight distribution. We note that the values $\beta = 0, 1, 6, 11$, and 21 for $W_{62,2}$ appear for the first time in the literature. Examples of codes for every new value of β can be obtained from [7]. All self-dual [62, 31, 12] codes with $|\mathrm{Aut}(C)| \equiv 0 \pmod{15}$ from the paper [13] have occurred also in our results.

Table 8 The number of codes for different pairs $(\beta, |\mathrm{Aut}(C)|)$ obtained using the matrix G_3

	$\|\mathrm{Aut}(C)\|$				
	5	10	15	30	60
$\beta = 0$	528	72	9	8	2
$\beta = 5$	1036				
$\beta = 10$	793	74	9	7	
$\beta = 15$	198		1		

6 [64, 32, 12] binary self-dual codes with automorphism of type 5-(12, 4)

For [64, 32, 12] self-dual codes there is one possibility for a doubly-even code:

$$W_{64} = 1 + 2976y^{12} + 454{,}956y^{16} + 18{,}275{,}616y^{20} + \cdots \tag{4}$$

Such codes exist, for example in [16] they are derived from binary image of an extended Reed–Solomon code over $\mathbb{F}_{16}$.

The possible weight enumerators $W_{64,i}$ of extremal singly even self-dual [64, 32, 12] codes are given in [10]:

$$\begin{aligned} W_{64,1} =& 1 + (1312 + 16\beta)y^{12} + (22{,}016 - 64\beta)y^{14} + \cdots, \\ W_{64,2} =& 1 + (1312 + 16\beta)y^{12} + (23{,}040 - 64\beta)y^{14} + \cdots, \end{aligned}$$

where β are integers with $14 \leq \beta \leq 104$ for $W_{64,1}$ and $0 \leq \beta \leq 277$ for $W_{64,2}$. Extremal singly even self-dual codes with weight enumerator $W_{64,1}$ are known for

$$\beta \in \left\{ \begin{array}{l} 14, 16, 18, 20, 22, 24, 25, 26, 28, 29, 30, 32, \\ 34, 35, 36, 38, 39, 44, 46, 53, 59, 60, 64, 74 \end{array} \right\}$$

(see [15,17–19]). Extremal singly even self-dual codes with weight enumerator $W_{64,2}$ are known for

$$\beta \in \left\{ \begin{array}{l} 0, 1, \ldots, 42, 44, 45, 48, 50, 51, 52, 56, 58, 64, 65, 72, \\ 80, 88, 96, 104, 108, 112, 114, 118, 120, 184 \end{array} \right\} \setminus \{31, 39\}$$

(see [15,17–19]).

In this case C_π is a binary self-dual [16, 8] code. There are exactly seven such codes: five singly even $i_2 \oplus 2e_7$, $2i_2 \oplus d_{12}$, $4i_2 \oplus e_8$, $8i_2$, $2d_8$ and two doubly-even d_{16} and $2e_8$. The minimum weight $d = 12$ of the code C limits the minimum weight of C_π to $d' \geq 4$ effectively eliminating all codes with the summand i_2. Using the codes $2d_8$, d_{16}, and $2e_8$ for all possible $\binom{16}{4}$ splittings of $\{1, \ldots, 16\}$ into sets X_c and X_f, we have calculated the minimum weight of the code $F_\sigma(C)$. For a code C_π there occur a total of 8 different generator matrices: one from $2e_8$ generating a doubly-even subcode $F_\sigma(C)$; six from d_{16} with all six codes singly-even; and one doubly-even

Table 9 The generator matrices $G_4, \ldots, G_{11}$

G_i	Support
G_4	1ade, 29de, 39ae, 49ad, 5cfg, 6bfg, 7bcg, 8bcf
G_5	19fg, 2afg, 3bdefg, 4cdefg, 5bcd, 6bce, 79abcf, 89abcg
G_6	19cg, 2acg, 3bcefg, 4cdefg, 5bde, 6bdf, 79abcd, 89abdg
G_7	19fg, 2afg, 3bcdfg, 4bcefg, 5bde, 6cde, 79adef, 89adeg
G_8	19cg, 2cdg, 3acefg, 4bcefg, 5abe, 6abf, 79abcd, 89abdg
G_9	1ceg, 2cfg, 38abcg, 49abcg, 589a, 689b, 789cef, 89defg
G_{10}	1ceg, 2cfg, 38abcg, 49abcg, 589a, 689b, 789efg, 89cdef
G_{11}	19cg, 2acg, 3bcg, 4cdg, 5ceg, 6cfg, 79abdefg, 89abcdef

Table 10 Number of doubly-even codes for different values of $|\mathrm{Aut}(C)|$, $\mathrm{gen}(C_\pi) = G_4$

	$\|\mathrm{Aut}(C)\|$									
	15	20	30	40	60	80	120	320	480	61,440
#	462	1180	205	32	44	7	3	1	1	1

Table 11 Number of doubly-even codes for different values of $|\mathrm{Aut}(C)|$, $\mathrm{gen}(C_\pi) = G_{11}$

	$\|\mathrm{Aut}(C)\|$								
	15	20	30	40	80	120	320	1280	1920
#	406	1212	8	102	13	1	1	1	1

code from $2d_8$. Denote by $G_4, \ldots, G_{11}$ the generator matrices of these 8 codes, only the matrices G_9 and G_{10} are not in standard form. Assuming that $X_c = \{1, \ldots, 12\}$ we give the support of the rows of the matrices $G_4, \ldots, G_{11}$ in Table 9 (for shortness the coordinates $10, 11, \ldots, 16$ are denoted by the letters $a, b, \ldots g$, respectively). We note $\pi^{-1}(G_4)$ and $\pi^{-1}(G_{11})$ generate doubly-even subcodes $F_\sigma(C)$ and therefore only in both those cases the [64, 32, 12] codes will be doubly-even.

For $4 \le i \le 11$, using the double transversal T_i, of S_{12} with respect to the groups St_i and denoting $C^\tau_{i,j}$ the code determined by the matrix G_i, with columns permuted by τ, as a generator for $F_\sigma(C)$ and H_j, as a generator matrix for $E_\sigma(C)^*$, we have calculated the weight distribution of all codes, except for $C^\tau_{4,j}$ and $C^\tau_{11,j}$ where the resulting [64, 32, 12] codes are doubly-even. For the codes $C^\tau_{4,j}$ and $C^\tau_{11,j}$, due to the huge computer time needed to find all codes, we have calculated only the codes for which the automorphism group of H_j is not of order 5, 10, 20, and 40.

Up to equivalence we summarize our results for code with $|\mathrm{Aut}(C)| \neq 5$ when $\mathrm{gen}(C_\pi) = G_4$ and $\mathrm{gen}(C_\pi) = G_{11}$ in Tables 10 and 11, respectively.

Examining the singly-even [64, 32, 12] codes with an automorphism of type 5-(12, 4) we have calculated their weight distributions and we also did a check for equivalence. The cardinality of the transversals $T_4, \ldots, T_{11}$ and the computational time used to compute these cases are given in Table 12. We have checked a total of more than 530 billion codes. Computational time for this length was about 2 months on a 4 core 3Ghz CPU. We have the following result.

Table 12 Generators of St_i, cardinality of transversals T_i and computational time for $4 \le i \le 11$

i	St_i	$\|T_i\|$	CPU time
4	$\langle(5,7,12,8)(6,11), (1,12)(2,11)(3,7)(4,8)(5,10)(6,9), (5,8,11,12,7,6)\rangle$	103,950	45
5	$\langle(1,8)(7,9), (5,6), (3,4)(11,12), (3,11)(4,12), (1,10,7,9,2,8)\rangle$	1,247,400	169
6	$\langle(1,8)(5,6,11)(7,9), (1,2,7)(6,11)(8,9,10)\rangle$	3,326,400	362
7	$\langle(1,6,7,11,9,12,8,5)(2,3)(4,10), (1,9)(2,10)(7,8), (1,10)(2,9)\rangle$	103,950	95
8	$\langle(3,4)(10,11), (3,10)(4,11), (5,6), (1,4,9,3)(2,5,12,6)(7,11,8,10)\rangle$	3,742,200	436
9	$\langle(2,12,7)(3,4)(5,8,10,9), (1,7,2,12)(3,5,11,4,10,6)(8,9)\rangle$	103,950	73
10	$\langle(2,7,12)(5,9,10,8)(6,11), (1,12,2,7)(3,11,9)(4,6,8)\rangle$	103,950	66
11	$\langle(1,2,7,3)(5,12,6)(8,11,9,10), (1,8,3)(4,5)(7,11,9)\rangle$	103,950	43

Table 13 Values of $(\beta, |\mathrm{Aut}(C)|)$ for $\mathrm{gen}(C_\pi) = G_5$, all codes with $W_{64,2}$

β	$\|\mathrm{Aut}(C)\|$				β	$\|\mathrm{Aut}(C)\|$			
	5	10	20	3840		5	10	20	3840
2	41,405	1276			42	190	55	3	
7	156,993	2653	3		**47**	**13**	**3**		
12	242,328	4093			52	2	3		
17	199,556	3357	6		**57**	**1**			
22	99,742	2672	5		**62**		**1**		
27	32,902	1181	7		112				1
32	7890	599	7						
37	1472	141	7						

Bold values denote the new codes

Theorem 6 *Up to equivalence there exists exactly* 6,834,068 *binary singly-even* [64, 32, 12] *codes with an automorphism of type* 5-(12, 4)*. Of these codes* 1469019 *and* 5365049 *have weight enumerator* $W_{64,1}$ *and* $W_{64,2}$*, respectively. There exist codes with* $W_{64,1}$ *for* $\beta = 19, 49,$ *and,* 54, *and* $W_{64,2}$ *for* $\beta = 31, 39, 46, 47, 49, 54, 55, 57, 60, 62,$ *and* 69.

Remark 4 Examples of codes for every new value of β are listed in [7] (Tables 13, 14, 15, 16, 17, 18).

7 New [58, 29, 10] binary self-dual codes

There are two possible weight enumerators for a self-dual [58, 29, 10] code in [10]. Harada in [11] proved that indeed the first weight enumerator only occur for $\gamma = 55$. Thus we have the following enumerators:

Table 14 Values of $(\beta, |\mathrm{Aut}(C)|)$ for $\mathrm{gen}(C_\pi) = G_6$, all codes with $W_{64,2}$

β	$\|\mathrm{Aut}(C)\|$			β	$\|\mathrm{Aut}(C)\|$			β	$\|\mathrm{Aut}(C)\|$		
	5	10	15		5	10	15		5	10	15
1	111,858			21	251,899	32		41	471	3	
6	426,555	6		26	80,756	11		**46**	**69**		
11	649,414	10		**31**	**19,082**	**10**	**3**	51	6		
16	521,540	29	2	36	3377	4					

Bold values denote the new codes

Table 15 Values of $(\beta, |\mathrm{Aut}(C)|)$ for $\mathrm{gen}(C_\pi) = G_7$, all codes with $W_{64,1}$

β	$\|\mathrm{Aut}(C)\|$								
	5	10	15	20	30	40	60	80	120
14	111,063	5763	20	369	40	1	21	1	2
19	208,085	5340		2					
24	204,253	6932		257					
29	123,799	3900	10	7	26				
34	49,982	2639		126		1			
39	13,252	995		3					
44	2515	515	1	40	11		7		
49	267	129		3					
54	25	49		5					
59		2			2				
64	1	3							
74							1		

$$W_{58,1} = 1 + 55y^{10} + 5188y^{12} + 18{,}180y^{14} + 432{,}333y^{16} + \ldots,$$
$$W_{58,2} = 1 + (319 - 24\beta - 2\gamma)y^{10} + (3132 + 152\beta + 2\gamma)y^{12} + \ldots,$$

where $0 \le \beta \le 11$ and $0 \le \gamma \le 159 - 12\beta$. Codes are known with $W_{58,1}$ and with $W_{58,2}$ for [11]:

- $\beta = 0, \gamma \in \{2m | m = 0, \ldots, 65, 68, 71, 79\}$;
- $\beta = 1, \gamma \in \{2m | m = 8, \ldots, 58, 63\}$;
- $\beta = 2, \gamma \in \{2m | 0, 4, 6, \ldots, 55\}$.

Let C be a self-dual [60, 30, 12] code. By choosing a pair $1 \le i_1 < i_2 \le 60$ of coordinates we can construct a new code [20]

$$C' = \{(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) | (x_1, \ldots, x_{60}) \in C_{60,i}, x_{i_1} = x_{i_2}\}.$$

It is well known that C' is a self-dual code of length 58 and we say that C' is obtained from C by subtracting. Since all codes we are shortening have minimum weight 12, all codewords obtained have minimum weight 10 so all C' are self-dual [58, 29, 10] codes.

Table 16 Values of $(\beta, |\mathrm{Aut}(C)|)$ for $\mathrm{gen}(C_\pi) = G_8$, all codes with $W_{64,2}$

β	$\lvert\mathrm{Aut}(C)\rvert$										
	5	10	20	40	60	80	120	160	320	640	1280
0	131,026	4710	215	9		3		2	15	1	1
5	497,611	8391	145		1		1				
10	748,582	14,825	347								
15	590,339	11,627	158								
20	281,964	9395	310			2					
25	90,259	4356	87								
30	22,243	2122	98								
35	4151	603	20								
40	2124	629	95	1		1			12	1	
45	380	73	13				1				
50	56	53	5								
55	1	5	3								
60		5	2								
80									2		

Table 17 Values of $(\beta, |\mathrm{Aut}(C)|)$ for $\mathrm{gen}(C_\pi) = G_9$, all codes with $W_{64,2}$

β	$\lvert\mathrm{Aut}(C)\rvert$								
	5	10	15	20	40	80	120	240	1,290,240
4	3587	345		41					
9	13,807	506		21					
14	20,919	1111		52					
19	17,641	711	1	14					
24	9452	659		61	2				
29	3542	288		1					
34	1068	193		14					
39	192	58		1					
44	43	17		10					
49	5	2		1					
54		3		2					
64						1		1	
69		1					1		
114								1	
184									1

Table 18 Values of $(\beta, |\mathrm{Aut}(C)|)$ for $\mathrm{gen}(C_\pi) = G_{10}$, all codes with $W_{64,1}$

β	$\|\mathrm{Aut}(C)\|$					β	$\|\mathrm{Aut}(C)\|$				
	5	10	20	40	80		5	10	20	40	80
14	112,397	3811	139	2	2	44	2394	367	42		
19	**211,966**	**4147**	**276**	**5**		**49**	**260**	**91**	**11**	**1**	
24	202,640	4712	121			**54**	**23**	**15**	**6**		
29	119,621	2940	117	1		59		3	1		
34	47,117	1844	93	3		64	1	1	1		
39	12,510	816	51	6							

Bold values denote the new codes

We start with the 315 binary self-dual [60, 30, 12] codes with an automorphism of order 5: 236 constructed in Sect. 4, and the 79 codes with an automorphism of type 5-(10, 10) from [21]. Since the minimum weight of all codes we are shortening is 12, all new codewords have minimum weight 10, so all codes C' are in fact optimal self-dual [58, 29, 10] codes. By shortening for all pair (i_1, i_2), $1 \leq i_1 < i_2 \leq 60$ we obtain the following result.

Proposition 3 *Up to equivalence there are exactly* 53,968 *binary self-dual* [58, 29, 10] *codes obtained by subtracting the* [60, 30, 12] *self-dual code with an automorphism of type* 5-(12, 0)*. Of these codes* 189 *have* $W_{58,1}$ *and* 53,779 *have* $W_{58,2}$ *for* 80 *different pairs* (γ, β) :

- $\beta = 0, \gamma = 2m, m \in \{0, 26, 29, \ldots, 64, 66\}$;
- $\beta = 1, \gamma = 2m, m \in \{39, \ldots, 55\}$;
- $\beta = 2, \gamma = 2m, m \in \{26, 28, \ldots, 51\}$.

Remark 5 For the first time in the literature we construct [58, 29, 10] codes with $W_{58,2}$ for $\beta = 0$, $\gamma = 132$. Of the three codes constructed 2 have automorphism group of 4 elements and one has $|\mathrm{Aut}(C)| = 8$. All codes with $|\mathrm{Aut}(C)| \equiv 0 \pmod 5$ have an automorphism of type 5-(10, 8) an thus are known from [21]. All other codes are new. An example of a code for the parameters $\beta = 0$, $\gamma = 132$ in $W_{58,2}$ is available in [7].

Acknowledgements This work was supported by European Regional Development Fund and the Operational Program "Science and Education for Smart Growth" under Contract UNITe No. BG05M2OP001-1.001-0004-C01 (2018-2023) and by Shumen University under Project No. RD-08-115/04.02.2019. We thank the reviewers for their very helpful comments and suggestions which helped improve this work.

References

1. Yankov, N., Russeva, R.: Binary self-dual codes of lengths 52 to 60 with an automorphism of order 7 or 13. IEEE Trans. Inf. Theory **57**(11), 7498–7506 (2011)
2. Yankov, N.: New optimal [52, 26, 10] self-dual codes. Des. Codes Crypt. **69**(2), 151–159 (2013)
3. Huffman, W.: On the classification and enumeration of self-dual codes. Finite Fields Appl. **11**(3), 451–490 (2005)
4. Huffman, W.C.: Automorphisms of codes with applications to extremal doubly even codes of length 48. IEEE Trans. Inf. Theory **28**(3), 511–521 (1982)

5. Yorgov, V.: Binary self-dual codes with automorphisms of odd order. Probl. Inf. Transm. **19**(4), 260–270 (1983)
6. Yorgov, V.: A method for constructing inequivalent self-dual codes with applications to length 56. IEEE Trans. Inf. Theory **33**(1), 77–82 (1987)
7. Yankov, N., Anev, D.: Generator matrices of new self-dual codes with an automorphism of order 5. http://shu.bg/tadmin/upload/storage/67274933.pdf
8. Bouyukliev, I.: About the Code Equivalence in Advances in Coding Theory and Cryptography, vol. 3, pp. 126–151. World Scientific Publishing Company, Singapore (2007)
9. The GAP Group: GAP—Groups, Algorithms, and Programming, Version 4.8.1 (2017)
10. Conway, J., Sloane, N.J.A.: A new upper bound on the minimal distance of self-dual codes. IEEE Trans. Inf. Theory **36**(6), 1319–1333 (1990)
11. Harada, M.: Binary extremal self-dual codes of length 60 and related codes. Des. Codes Crypt. **86**(5), 1085–1094 (2018)
12. Huffman, W.C., Pless, V.S.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
13. Dontcheva, R., Harada, M.: New extremal self-dual codes of length 62 and related extremal self-dual codes. IEEE Trans. Inf. Theory **48**(7), 2060–2064 (2002)
14. Russeva, R., Yankov, N.: On binary self-dual codes of lengths 60, 62, 64 and 66 having an automorphism of order 9. Des. Codes Crypt. **45**(3), 335–346 (2007)
15. Yankov, N.: Self-dual [62, 31, 12] and [64, 32, 12] codes with an automorphism of order 7. Adv. Math. Commun. **8**(1), 73–81 (2014)
16. Pasquier, G.: A binary extremal doubly even self-dual code (64, 32, 12) obtained from an extended Reed–Solomon code over $\mathbb{F}_{16}$. IEEE Trans. Inf. Theory **27**(6), 807–808 (1981)
17. Kaya, A.: New extremal binary self-dual codes of lengths 64 and 66 from R_2-lifts. Finite Fields Appl. **46**, 271–279 (2017)
18. Kaya, A., Yildiz, B., Pasa, A.: New extremal binary self-dual codes from a modified four circulant construction. Discrete Math. **339**(3), 1086–1094 (2016)
19. Anev, D., Harada, M., Yankov, N.: New extremal singly even self-dual codes of lengths 64 and 66. J. Algebra Comb. Discrete Struct. Appl. **5**(3), 143–151 (2018)
20. Gulliver, T.A., Harada, M., Kim, J.-L.: Construction of new extremal self-dual codes. Discrete Math. **263**(1–3), 81–91 (2003)
21. Yankov, N., Lee, M.H.: New binary self-dual codes of lengths 50–60. Des. Codes Crypt. **73**(3), 983–996 (2014)