

On binary self-dual codes of lengths 60, 62, 64 and 66 having an automorphism of order 9

Radka Russeva · Nikolay Yankov

Received: 4 March 2006 / Revised: 9 August 2007 / Accepted: 23 August 2007 /
Published online: 26 September 2007
© Springer Science+Business Media, LLC 2007

Abstract A method for constructing binary self-dual codes having an automorphism of order p^2 for an odd prime p is presented in (S. Bouyuklieva et al. IEEE. Trans. Inform. Theory, 51, 3678–3686, 2005). Using this method, we investigate the optimal self-dual codes of lengths $60 \leq n \leq 66$ having an automorphism of order 9 with six 9-cycles, t cycles of length 3 and f fixed points. We classify all self-dual $[60, 30, 12]$ and $[62, 31, 12]$ codes possessing such an automorphism, and we construct many doubly-even $[64, 32, 12]$ and singly-even $[66, 33, 12]$ codes. Some of the constructed codes of lengths 62 and 66 are with weight enumerators for which the existence of codes was not known until now.

Keywords Self-dual Codes · Automorphisms · Optimal codes

AMS Classification 94B05

1 Introduction

A linear $[n, k]$ code C is a k -dimensional subspace of the vector space \mathbb{F}_q^n , where \mathbb{F}_q is the finite field of q elements. The elements of C are called codewords, and the (Hamming) weight of a codeword is the number of its non-zero coordinates. The minimum weight d of C is the smallest weight among all non-zero codewords of C , and C is called an $[n, k, d]$ code. A matrix whose rows form a basis of C is called a generator matrix of this code. The weight enumerator $W(y)$ of a code C is given by $W(y) = \sum_{i=0}^n A_i y^i$ where A_i is the number of codewords of weight i in C . Unless otherwise stated, the inner product we use will be the

Communicated by Q. Xiang.

R. Russeva (✉) · N. Yankov
Faculty of Mathematics and Informatics, Shumen University, Shumen 9712, Bulgaria
e-mail: russeva@fmi.shu-bg.net

N. Yankov
e-mail: jankov_niki@yahoo.com

ordinary inner product given by $(u, v) = \sum_{i=1}^n u_i v_i$ computed in \mathbb{F}_q , where $u, v \in \mathbb{F}_q^n$. The dual code of C is $C^\perp = \{u \in \mathbb{F}_q^n : (u, v) = 0 \text{ for all } v \in C\}$. C^\perp is a linear $[n, n - k]$ code. If $C \subseteq C^\perp$, C is termed self-orthogonal, and if $C = C^\perp$, C is self-dual. If C is self-dual, then $k = \frac{1}{2}n$.

A doubly-even code is a binary code for which all weights are divisible by four. A self-dual code with some codeword of weight not divisible by four is called singly-even. Self-dual doubly-even codes exist if and only if n is a multiple of eight. The codes with the largest minimum weight among all self-dual codes of given length are named optimal self-dual codes.

Two binary codes are equivalent if one can be obtained from the other by a permutation of coordinates. The permutation $\sigma \in S_n$ is an automorphism of the binary code C if $C = \sigma(C)$. The set of all automorphisms of C forms the automorphism group $Aut(C)$ of C .

Two codes over \mathbb{F}_q are (monomially) equivalent if one can be obtained from the other by a coordinate permutation followed by multiplying some (or no) coordinates by a nonzero element of \mathbb{F}_q .

Huffman and Yorgov (cf. [13, 19, 20]) developed a method for constructing binary self-dual codes with an automorphism of odd prime order. Dontcheva, van Zanten and Dodunekov extended the method for automorphisms of odd composite order [6]. A method for constructing binary self-dual codes having an automorphism of order p^2 for an odd prime p is presented in [3], and all self-dual optimal codes possessing an automorphism of order 9 with six 9-cycles without cycles of length 3 are obtained there. In this work we continue the investigations for binary optimal self-dual codes with an automorphism of order 9 with six 9-cycles and cycles of length 3. We classify all self-dual $[60, 30, 12]$ and $[62, 32, 12]$ codes possessing such an automorphism. We construct many doubly-even $[64, 32, 12]$ and singly-even $[66, 33, 12]$ codes. Some of the constructed codes of lengths 62 and 66 have weight enumerators for which the existence of codes was not known before. We give the description of the method used in Sect. 2. The authors suggest the reader consult [3] for more details.

2 Construction method

We will use the notations from [3]. Let C be a binary self-dual code of length n , and σ be an automorphism of C of type $9 - (c, t, f)$, i.e. σ has c independent 9-cycles, t independent cycles of length 3 and f fixed points. Obviously, $n = 9c + 3t + f$. Then σ^3 is an automorphism of type $3 - (3c, 3t + f)$, and the parameter c must be even. Without loss of generality we can assume that

$$\sigma = \Omega_1 \dots \Omega_c \Omega_{c+1} \dots \Omega_{c+t} \Omega_{c+t+1} \dots \Omega_{c+t+f} \tag{1}$$

where $\Omega_i = (9i - 8, \dots, 9i)$, $i = 1, \dots, c$ are the cycles of length 9, $\Omega_{c+i} = (9c + 3(i - 1) + 1, \dots, 9c + 3i)$, $i = 1, \dots, t$ are the cycles of length 3, and $\Omega_{c+t+i} = (9c + 3t + i)$, $i = 1, \dots, f$ are the fixed points.

Let $F_\sigma(C) = \{v \in C : v\sigma = v\}$ and $E_\sigma(C) = \{v \in C : wt(v|\Omega_i) \equiv 0 \pmod{2}, i = 1, \dots, c + t + f\}$, where $v|\Omega_i$ is the restriction of v on Ω_i . Then $C = F_\sigma(C) \oplus E_\sigma(C)$.

Each vector $v \in F_\sigma(C)$ is constant on any cycle of σ . Let $\pi : F_\sigma(C) \rightarrow \mathbb{F}_2^{c+t+f}$ be the projection map where if $v \in F_\sigma(C)$, $(v\pi)_i = v_j$ for some $j \in \Omega_i$, $i = 1, 2, \dots, c + t + f$. It is known that the ‘‘contracted’’ code $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual code of length $c + t + f$. The code $F_\sigma(C)$ is uniquely determined by the code C_π .

Denote by $E_\sigma(C)^*$ the code $E_\sigma(C)$ with the last f coordinates deleted. So $E_\sigma(C)^*$ is a binary self-orthogonal $[9c + 3t, 4c + t]$ code. For $v \in E_\sigma(C)^*$ we identify $v|\Omega_i = (v_0, v_1, \dots, v_8)$ with the polynomial $v_0 + v_1x + \dots + v_8x^8$ from \mathcal{T} for $i = 1, \dots, c$, and $v|\Omega_i = (v_0, v_1, v_2)$ with the polynomial $v_0 + v_1x + v_2x^2$ from \mathcal{P} for $i = c + 1, \dots, c + t$, where \mathcal{T} and \mathcal{P} are the sets of even-weight polynomials in $\mathbb{F}_2[x]/(x^9 - 1)$ and $\mathbb{F}_2[x]/(x^3 - 1)$, respectively. Thus we obtain the map $\phi : E_\sigma(C)^* \rightarrow \mathcal{T}^c \times \mathcal{P}^t$.

Definition 1 [3] A linear code $\mathcal{C} \subset \mathcal{T}^c \times \mathcal{P}^t$ is a subset of $\mathcal{T}^c \times \mathcal{P}^t$ such that $v + w \in \mathcal{C}, \forall v, w \in \mathcal{C}$ and $xv \in \mathcal{C}, \forall v \in \mathcal{C}$.

Then $C_\phi = \phi(E_\sigma(C)^*)$ is a linear code in $\mathcal{T}^c \times \mathcal{P}^t$. Following [15] we define Hermitian inner products over \mathcal{T} and \mathcal{P} as $\langle v, w \rangle = \sum_{i=1}^c v_i(x)w_i(x^{-1}) = \sum_{i=1}^c v_i(x)w_i(x^8), v, w \in \mathcal{T}^c$ and $\langle v', w' \rangle = \sum_{i=1}^t v'_i(x)w'_i(x^{-1}) = \sum_{i=1}^t v'_i(x)w'_i(x^8), v', w' \in \mathcal{P}^t$. Using these two inner products we can define the inner product in $\mathcal{T}^c \times \mathcal{P}^t$ in the following way:

$$\langle (v_1, v_2), (w_1, w_2) \rangle = \langle v_1, w_1 \rangle + (x^6 + x^3 + 1)\langle v_2, w_2 \rangle \tag{2}$$

for all vectors $v_1, w_1 \in \mathcal{T}^c$ and $v_2, w_2 \in \mathcal{P}^t$. If \mathcal{C} is a linear code in $\mathcal{T}^c \times \mathcal{P}^t$ we define its dual code as the set \mathcal{C}^\perp of all vectors $w \in \mathcal{T}^c \times \mathcal{P}^t$ such that $\langle v, w \rangle = 0$ for all vectors $v \in \mathcal{C}$. It is easy to prove that the dual of a linear code in $\mathcal{T}^c \times \mathcal{P}^t$ is linear, too. If \mathcal{C} coincides with its dual code, it is called self-dual. The next theorem is the main tool in our investigation, and it is a direct consequence of Theorem 1 in [3].

Theorem 1 *The binary code \mathcal{C} having an automorphism σ defined in (1) is self-dual iff C_π is a binary self-dual code and $C_\phi = \phi(E_\sigma(C)^*)$ is a self-dual code in $\mathcal{T}^c \times \mathcal{P}^t$ with respect to the inner product (2).*

As 2 is a primitive root modulo 9, the factorization of the polynomial $x^9 - 1$ into irreducible factors over \mathbb{F}_2 is given by $x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$. Then \mathcal{P} is a field with four elements, and $\mathcal{T} = I_1 \oplus I_2$, where I_1 and I_2 are the cyclic codes with parity check polynomials $x^2 + x + 1$ and $x^6 + x^3 + 1$, respectively. Hence $I_1 \cong GF(4)$ and $I_2 \cong GF(2^6)$, and for every element $a(x) \in \mathcal{T}$, we have $a = a_1(x) + a_2(x)$ where $a_1 \in I_1, a_2 \in I_2$.

Let A be the largest subcode of $E_\sigma(C)^*$ which is zero on the last $3t$ coordinates corresponding to the cycles of length 3, and let B be the largest subcode of $E_\sigma(C)^*$ which is zero on the first $9c$ coordinates corresponding to the 9-cycles. Denote by A^* the code A with the last $3t$ coordinates deleted, and by B^* the code B with the first $9c$ coordinates deleted. Then A^* is a binary linear code of length $9c$ having an automorphism of order 9 with c independent 9-cycles. Then $M = \phi(A^*) = M_1 \oplus M_2$, where $M_j = \{u \in \phi(A^*) | u_i \in I_j, i = 1, \dots, c\}, j = 1, 2$ is a linear code over I_j . The code $B_\phi = \phi(B^*)$ is a linear code over \mathcal{P} of length t and dimension k_t . So we can consider a generator matrix for C_ϕ in the form

$$G_\phi = \begin{pmatrix} \text{gen}_{I_1} M_1 & 0 \\ \text{gen}_{I_2} M_2 & 0 \\ 0 & \text{gen}_{\mathcal{P}} B_\phi \\ D_c & D_t \end{pmatrix} \text{ and by [3] the following theorem holds:}$$

Theorem 2 *If \mathcal{C} is a binary self-dual $[n, \frac{n}{2}, d]$ code with automorphism of type $9 - (c, t, f)$. Then:*

- (1) M_2 is a self-dual $[c, \frac{c}{2}]$ code over I_2 .
- (2) $\dim_{I_1} M_1 = \frac{c-t}{2} + k_t$ and $\text{rank}(D_c) = \text{rank}(D_t) = t - 2k_t$.
- (3) The rows of $\text{gen}_{I_1} M_1$ and D_c generate the code M_1^\perp and the rows of $\text{gen}_{\mathcal{P}} B_\phi$ and D_t generate the code B_ϕ^\perp .

As c is even, so are the parameters t and $f = n - 9c - 3t$. All optimal self-dual codes with an automorphism of type $9 - (c, t, f)$ for $c = 2, 4$ and for $c = 6, t = 0$ are constructed in [2] and [3]. In this work we continue the investigations for $c = 6$ and $t \neq 0$.

The following theorem is a particular case of the results in [[3], Theorem 5]; here $n(k, d)$ is the minimum length n for which a binary linear $[n, k, d]$ code exists.

Theorem 3 *If C is a binary self-dual $[n, \frac{n}{2}, d]$ code with automorphism of type $9 - (6, t, f)$ then we have the following inequalities:*

- (1) $54 \geq n(18, d)$.
- (2) *If $3t + f > 18$, the following inequality holds: $3t + f \geq n(\frac{3t+f}{2} - 9, d)$.*
- (3) *If $f > 6 + t$, the following inequality holds: $f \geq n(\frac{f-t}{2} - 3, d)$.*

3 Self-dual codes with an automorphism of order 9 with $c = 6$

As described in Sect. 2, $\mathcal{T} = I_1 \oplus I_2$. $I_1 = \{0, x^s e_1 | s = 0, 1, 2\}$ is a field of four elements with identity $e_1 = x^8 + x^7 + x^5 + x^4 + x^2 + x$, and I_2 is a field of 2^6 elements with identity $e_2 = x^6 + x^3$. The element $\alpha = (x + 1)e_2$ is a primitive element of I_2 . The element $\delta = \alpha^9 = x^2 + x^4 + x^5 + x^7$ has multiplicative order 7 in I_2 and $I_2 = \{0, x^s \delta^k | 0 \leq s \leq 8$ and $0 \leq k \leq 6\}$.

Let C be a binary optimal self-dual $[n, k, d]$ code having an automorphism σ of order 9 defined in (1) with six independent 9-cycles, $t \neq 0$ independent 3-cycles and f fixed points. Hence $n \geq 60$ and so $d \geq 12$. Then $C_\phi = M_1 \oplus M_2$ where M_2 is a Hermitian self-dual $[6, 3]$ code over the field I_2 .

To actually construct a generator matrix of the code C we use four matrices: $gen C_\pi$, $gen_{I_2} M_2$, $S = (gen_{I_1} M_1 / D_6)$ and D_t . To narrow our calculations we use the following transformations which preserve the decomposition and send the code C to an equivalent one:

- (i) a permutation of the last f fixed coordinates.
- (ii) a permutation of the t 3-cycles coordinates.
- (iii) a permutation of the six 9-cycles coordinates.
- (iv) a substitution $x \rightarrow x^2$ in C_ϕ .
- (v) a cyclic shift to each 9-cycle independently. This action preserves $gen C_\pi$, and it is equivalent to multiplication of the coordinates of $gen_{I_2} M_2$ and S by x^k for $k = 0, 1, \dots, 8$ and by x^k for $k = 0, 1, 2$, respectively.
- (vi) a cyclic shift to each 3-cycle independently. This action also preserves $gen C_\pi$.

There exist four monomially nonequivalent possibilities for M_2 with generator matrices

$$L_1 = \begin{pmatrix} e_2 & 0 & 0 & \delta & \delta^3 & 0 \\ 0 & e_2 & 0 & \delta^2 & e_2 & \delta^2 \\ 0 & 0 & e_2 & \delta^5 & \delta^3 & \delta^6 \end{pmatrix}, L_2 = \begin{pmatrix} e_2 & 0 & 0 & e_2 & \delta & \delta \\ 0 & e_2 & 0 & \delta^2 & \alpha^2 & \alpha^{10} \\ 0 & 0 & e_2 & \delta^2 & \alpha^{14} & \alpha^{39} \end{pmatrix},$$

$$L_3 = \begin{pmatrix} e_2 & 0 & 0 & e_2 & \delta & \delta \\ 0 & e_2 & 0 & \delta^3 & \alpha^{12} & \alpha^{38} \\ 0 & 0 & e_2 & \delta^3 & \alpha^{50} & \alpha^{46} \end{pmatrix} \text{ and } L_4 = \begin{pmatrix} e_2 & 0 & 0 & e_2 & \delta & \delta \\ 0 & e_2 & 0 & \delta^5 & e_2 & \delta^5 \\ 0 & 0 & e_2 & \delta^5 & \delta & \delta^2 \end{pmatrix}.$$

The code $\phi^{-1}(M_2)$ is a linear $[54, 18, 12]$ code at each one of these possibilities. Hence the minimum weight of the code is 12 and $60 \leq n \leq 68$. So the following lemma holds:

Lemma 1 *The minimum weight of a binary self-dual optimal $[n, \frac{n}{2}]$ code having an automorphism of type $9 - (6, t, f)$ is 12 and $60 \leq n \leq 68$. The possibilities for the parameters*

t and f are either: (1) $t = 2, f = 0$ or (2) $t = 2, f = 2$ or (3) $t = 2, f = 4$ or (4) $t = 4, f = 0$ or (5) $t = 4, f = 2$.

In this work we investigate optimal self-dual codes of lengths $60 \leq n \leq 66$ i.e. all cases in Lemma 1 except case 5). As the parameter t is at most 4, $k_t = \dim B_\phi = 0$, and we can take D_t to be the identity matrix over the field \mathcal{P} .

We can fix $gen_{I_2} M_2 = L_i$, for $i = 1, \dots, 4$ and D_t . First we determine all possibilities for the matrix $H = \begin{pmatrix} gen C_\pi \\ gen_{I_2} M_2 0 \end{pmatrix}$. After that we add the matrices S and D_t and check the constructed codes for equivalence, using the program **Q-extension** [1].

3.1 $t = 2$

In our construction, $D_2 = \begin{pmatrix} e_3 & 0 \\ 0 & e_3 \end{pmatrix}$ where $e_3 = x + x^2$ is the identity element of \mathcal{P} . Since the minimum weight of C is 12, M_1 is a $[4, 2, 4]$ self-orthogonal code over the field I_1 . Applying the orthogonal condition (2) and row reducing, we obtain a unique possibility for the matrix S up to a permutation of the coordinates followed by multiplying the coordinates by x^k for $k = 0, 1, 2$, and it is

$$S = \begin{pmatrix} e_1 & 0 & e_1 & e_1 & e_1 & 0 \\ 0 & e_1 & 0 & xe_1 & xe_1 & e_1 \\ \hline 0 & 0 & e_1 & e_1 & 0 & x^2e_1 \\ 0 & 0 & e_1 & 0 & e_1 & x^2e_1 \end{pmatrix}. \tag{3}$$

3.1.1 $f = 0, [60, 30, 12]$ codes

The possible weight enumerators were derived in [4] and [8]:

$$W_{60,1} = 1 + (2555 + 64\beta)y^{12} + (33600 - 384\beta)y^{14} + \dots$$

and

$$W_{60,2} = 1 + 3451y^{12} + 24128y^{14} + 336081y^{16} + \dots,$$

where β is an integer with $0 \leq \beta \leq 10$. An optimal self-dual code with weight enumerator $W_{60,2}$ was constructed in [4]. For weight enumerators of type $W_{60,1}$, self-dual codes were constructed with $\beta = 0, 1, 7$ and 10 (see [3, 5, 11, 16]).

In this case C_π is a binary $[8, 4]$ self-dual code, equivalent either to C_2^4 or to the extended Hamming code H_8 . When $C_\pi \approx C_2^4$, we obtain exactly five nonequivalent self-dual $[60, 30, 12]$ codes with weight enumerators $W_{60,1}$ for $\beta = 0$. All of them have automorphism group of order 18. When $C_\pi \approx H_8$, we construct exactly three nonequivalent self-dual $[60, 30, 12]$ codes with weight enumerators $W_{60,1}$ for $\beta = 1$ and 8 codes for $\beta = 10$. These codes have automorphism groups of orders either 9, 18 or 54. The following theorem summarizes these results:

Theorem 4 *There exist exactly 16 nonequivalent binary self-dual $[60, 30, 12]$ codes having an automorphism of order 9 with 6 9-cycles and 2 3-cycles. All of them have weight enumerator $W_{60,1}$ for $\beta = 0, 1$, and 10.*

The first known self-dual $[60, 30, 12]$ code with weight enumerator $W_{60,1}$ for $\beta = 1$ has been constructed in [3] via an automorphism of type 9-(6,0,6), and it is equivalent to one of

Table 1 New self-dual [60, 30, 12] codes with weight enumerators $W_{60,1}$ for $\beta = 1$

$genM_2$	S	C_π	$ Aut $
L_2	$\begin{pmatrix} e_1 & 0 & 0 & x^2e_1 & xe_1 & xe_1 \\ 0 & e_1 & xe_1 & e_1 & x^2e_1 & 0 \\ 0 & 0 & e_1 & x^2e_1 & 0 & xe_1 \\ 0 & 0 & e_1 & 0 & xe_1 & xe_1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & & 0 & 1 \end{pmatrix}$	18
L_4	$\begin{pmatrix} e_1 & 0 & e_1 & xe_1 & x^2e_1 & 0 \\ 0 & xe_1 & xe_1 & x^2e_1 & 0 & e_1 \\ 0 & 0 & e_1 & 0 & x^2e_1 & x^2e_1 \\ 0 & 0 & 0 & xe_1 & x^2e_1 & x^2e_1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & & 0 & 1 \end{pmatrix}$	9

our codes. Thus we conclude that there exist at least three self-dual [60, 30, 12] codes with weight enumerators $W_{60,1}$ for $\beta = 1$.

The new self-dual [60, 30, 12] codes with $\beta = 1$ are presented in Table 1 with the order of their automorphism groups $|Aut|$.

3.1.2 $f = 2$, [62, 31, 12] codes

There are two possible forms for the weight enumerator of an optimal self-dual code of length 62 [5]:

$$W_{62,1} = 1 + 2308y^{12} + 23767y^{14} + 279405y^{16} + \dots$$

and

$$W_{62,2} = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + (255533 + 96\beta)y^{16} + \dots,$$

where β is an integer with $0 \leq \beta \leq 93$. Only codes with weight enumerator $W_{62,2}$ where $\beta = 0, 10, 15$ are known until now (see [5, 10]). In this work we construct self-dual [62, 32, 12] codes with weight enumerator $W_{62,1}$ and codes with weight enumerator $W_{62,2}$ for $\beta = 0, 9$. All obtained optimal codes of length 62 have automorphism groups of order 9.

The code C_π in this case is a binary [10,5,2] self-dual code. Up to equivalence there are two such codes – C_2^5 and $C_2 \oplus H_8$. We obtain self-dual [62, 32, 12] codes only when $C_\pi \approx C_2 \oplus H_8$. There are two possibilities for its generator matrix

$$G_{\pi,1} = \begin{pmatrix} 110000|00|00 \\ 001000|01|11 \\ 000100|10|11 \\ 000010|11|01 \\ 000001|11|10 \end{pmatrix} \text{ and } G_{\pi,2} = \begin{pmatrix} 111100|00|00 \\ 000001|10|00 \\ 110010|01|00 \\ 011010|00|10 \\ 101010|00|01 \end{pmatrix}$$

up to a permutation of the 9-cycles coordinates and a permutation of the last four coordinates corresponding to the 3-cycles and the fixed points.

- (1) Let $C_\pi \approx \langle G_{\pi,1} \rangle$. We did not obtain optimal codes when M_2 is generated by L_1 . In the other cases for M_2 we found exactly 3 nonequivalent [62, 32, 12] codes with weight enumerators $W_{62,2}$. We have one code for $\beta = 0$ and two codes for $\beta = 9$. The constructed codes with $W_{62,2}$ for $\beta = 9$ are the first known codes with this weight enumerator. They are generated by the matrices $G_{62,1}$ and $G_{62,2}$.

$$G_{62,2} = \begin{pmatrix} 111111111000000000000000000000000111111111000000000 & 000000 & 00 \\ 000000000111111111000000000000000000000000000000 & 111111 & 01 \\ 000000000000000000011111111100000000000000000000000 & 000111 & 11 \\ 00000000000000000000000000000001111111110000000000000000 & 111000 & 11 \\ 000 & 111111 & 10 \\ \hline 0001001000000000000000000000000100100001011010001011010 & 000000 & 00 \\ 000010010000000000000000000000010010000101101000101101 & 000000 & 00 \\ 00000100100000000000000000000001001100010110100010110 & 000000 & 00 \\ 1000001000000000000000000000010000100010001011010001011 & 000000 & 00 \\ 0100000100000000000000000000010000010101000101101000101 & 000000 & 00 \\ 001000001000000000000000000001000001110100010110100010 & 000000 & 00 \\ 0000000000001001000000000000010011001000101101001110111 & 000000 & 00 \\ 0000000000000100100000000001010011001000101110011101 & 000000 & 00 \\ 000000000100000100000000000001010011101000101111001110 & 000000 & 00 \\ 000000000010000010000000000100101001110100010011100111 & 000000 & 00 \\ 00000000001000001000000000110010100011010001101110011 & 000000 & 00 \\ 0000000000000000000000000100100010011001010010000011001010 & 000000 & 00 \\ 000000000000000000000000010010101001100001001000001100101 & 000000 & 00 \\ 00000000000000000000000001001010100110000100100100110010 & 000000 & 00 \\ 000000000000000000000000010000100001010011000010010010011001 & 000000 & 00 \\ 000000000000000000000000010000010100101001000001001101001100 & 000000 & 00 \\ 00000000000000000000000001000001110010100100000100010100110 & 000000 & 00 \\ 01101101100000000001101101111011011011011011000000000 & 000000 & 00 \\ 10110110100000000010110110101101101101101101100000000 & 000000 & 00 \\ 000000000101101101000000000011011011011011011110110110 & 000000 & 00 \\ 0000000001101101100000000001011011011011011011011011 & 000000 & 00 \\ \hline 00000000000000000001101101111011011000000000101101101 & 011000 & 00 \\ 0000000000000000000101101101011011011000000000110110110 & 101000 & 00 \\ 000000000000000000011011011000000000110110110101101101 & 000011 & 00 \\ 000000000000000000010110110100000000011011011110110110 & 000101 & 00 \end{pmatrix}$$

3.1.3 $f = 4$, [64, 32, 12] codes

There exist singly-even [64, 32, 12] codes and more than 3,250 doubly-even self-dual codes with these parameters constructed from 2-designs and double circulant matrices (see [14] and the references given therein). C_π is a binary self-dual [12, 6, $d \geq 2$] code equivalent either to $C_2^2 \oplus H_8$ or B_{12} . In the first case we proved that the code $F_\sigma(C)$ is a doubly-even subcode. As the subcode $E_\sigma(C)^*$ is also doubly-even, so are the obtained codes C . We constructed 10,637 nonequivalent doubly-even [64, 32, 12] codes, and we stopped our calculations. All obtained codes have automorphism groups of order either 9 or 18. When $C_\pi \approx B_{12}$, there does not exist optimal codes of length 64. Hence all the [64,32,12] self-dual codes with an automorphism of order 9 with 6 9-cycles and 2 3-cycles are doubly-even.

Table 2 New self-dual [62, 32, 12] codes with weight enumerators $W_{62,1}$

τ	$\mu(i_1, i_2, i_3, i_4, i_5, i_6)$	$genM_2$	τ	$\mu(i_1, i_2, i_3, i_4, i_5, i_6)$	$genM_2$
(1,6)(8,9)	(2,3)(5,6)(0,0,1,1,2,1)	L_1	(1,6)(8,9)	(2,3)(5,6)(0,1,1,2,2,1)	L_1
(1,6)(7,8,9)	(3,6)(0,0,2,0,1,2)	L_1	(1,6)(8,10)	(3,4)(5,6)(0,0,1,1,0,2)	L_1
(1,6)(7,8,10)	(3,6,4)(0,1,1,0,1,2)	L_1	(1,6,4)	(4,5,6)(0,0,1,2,2,2)	L_1
(1,6,4)(7,8,9)	(3,6,4)(0,0,2,2,1,1)	L_1	(1,6,4)(7,8,10)	(3,4)(5,6)(0,0,0,0,1,1)	L_1
(1,6,3,4)	(3,4,5,6)(0,0,2,0,0,1)	L_1	(1,6,3,4)(7,8)	(3,4)(5,6)(0,0,2,0,0,0)	L_1
(1,6,3,4)(8,9)	(3,5,6,4)(0,1,0,0,0,0)	L_1	(1,6,2)(3,4)(8,9)	(3,5,6,4)(0,1,0,0,0,0)	L_1
(1,6,2)(3,4)(7,8,9)	(2,3)(0,0,1,0,0,0)	L_1	(1,6,2)(3,4)(7,8,9)	(2,3)(0,1,1,2,2,1)	L_1
(7,8,10)	id(0,2,2,0,0,1)	L_2	(1,6)(8,10)	(4,5,6)(0,0,0,2,1,1)	L_2
(1,6,4)(8,10)	(3,5,6,4)(0,1,2,1,2,0)	L_2	(1,6,4)(8,10)	(23)(56)(0,1,1,1,0,2)	L_2
(1,6,4)(8,10)	(2,3)(4,5,6)(0,2,1,0,0,2)	L_2	(1,6,4)(8,10)	(2,3)(4,5,6)(0,2,2,0,0,2)	L_2
(1,6,3,4)(8,9)	(3,6)(0,1,2,2,1,0)	L_2	(1,6,3,4)(7,8,9)	(4,5,6)(0,1,2,0,2,1)	L_2
id	(3,5,4)(0,0,1,2,0,1)	L_3	id	(3,6,5,4)(0,2,2,1,0,1)	L_3
id	(23)(56)(0,1,0,0,0,0)	L_3	(7,8)	(2,3)(5,6)(0,2,1,0,2,0)	L_3
(8,9)	(3,4)(5,6)(0,0,0,2,2,1)	L_3	(8,10)	(3,6,4)(0,0,1,2,2,2)	L_3
(8,10)	(3,6,4)(0,1,1,0,1,0)	L_3	(7,8,10)	(3,4)(5,6)(0,1,1,2,2,1)	L_3
(7,8,10)	(3,5,6,4)(0,0,2,0,0,0)	L_3	(1,6)	id(0,1,2,2,1,1)	L_3
(1,6)(8,9)	(23)(56)(0,1,0,1,1,1)	L_3	(1,6)(7,8,9)	(3,4,5,6)(0,2,2,0,1,2)	L_3
(1,6)(8,10)	(4,5,6)(0,0,2,1,1,2)	L_3	(1,6)(8,10)	(4,5,6)(0,0,2,2,1,0)	L_3
(1,6)(8,10)	(2,3)(0,1,2,2,2,1)	L_3	(1,6)(7,8,10)	(4,5,6)(0,0,2,2,2,2)	L_3
(1,6)(7,8,10)	(3,4)(5,6)(0,0,0,1,2,0)	L_3	(1,6,4)	(5,6)(0,0,2,1,2,0)	L_3
(1,6,4)	(4,5,6)(0,0,2,1,1,2)	L_3	(1,6,4)	(3,4)(0,1,0,2,2,1)	L_3
(1,6,4)	(3,4)(0,1,1,1,1,1)	L_3	(1,6,4)(7,8)	(4,5,6)(0,1,0,0,1,0)	L_3
(1,6,4)(8,9)	(3,5,6)(0,1,1,2,1,2)	L_3	(1,6,4)(7,8,9)	(3,5,6)(0,2,2,2,2,2)	L_3
(1,6,4)(7,8,9)	(3,6,4)(0,1,0,1,1,0)	L_3	(1,6,4)(8,10)	(3,5,6,4)(0,1,0,2,1,2)	L_3
(1,6,4)(8,10)	(3,5,6,4)(0,2,1,0,2,0)	L_3	(1,6,4)(7,8,10)	(2,3)(5,6)(0,2,1,1,2,2)	L_3
(1,6,4)(7,8,10)	(2,3)(4,5,6)(0,0,1,2,0,1)	L_3	(1,6,4)(7,8,10)	(2,3)(4,5,6)(0,2,2,0,1,2)	L_3
(1,6,3,4)(7,8,9)	(3,5,6,4)(0,0,2,0,1,1)	L_3	(1,6,3,4)(7,8,9)	(3,5,6,4)(0,0,2,2,0,0)	L_3
(1,6,3,4)(7,8,9)	(3,6)(0,1,0,2,1,1)	L_3	(1,6,3,4)(8,10)	(5,6)(0,0,0,2,2,0)	L_3
(1,6,3,4)(8,10)	(2,3)(0,1,2,0,1,0)	L_3	(1,6,3,4)(8,10)	(2,3)(4,5,6)(0,2,1,2,2,1)	L_3
(1,6,3,4)(7,8,10)	(2,3)(0,0,1,1,2,2)	L_3	(1,6,2)(3,4)	(3,6)(0,0,1,2,1,2)	L_3
(1,6,2)(3,4)(7,8)	(3,6,4)(0,0,1,2,2,1)	L_3	(1,6,2)(3,4)(7,8)	(3,6,4)(0,1,1,1,1,0)	L_3
(1,6,2)(3,4)(7,8)	(3,6,4)(0,1,2,0,2,0)	L_3	(1,6,2)(3,4)(7,8)	(3,6)(0,2,0,2,1,1)	L_3
(1,6,2)(3,4)(7,8,9)	(3,5,6,4)(0,2,2,2,2,2)	L_3	(1,6,2)(3,4)(8,10)	(23)(56)(0,0,0,2,1,2)	L_3
(1,6,2)(3,4)(7,8,10)	(4,5,6)(0,0,2,1,0,2)	L_3			

3.2 $t = 4, f = 0$

There exist three possible forms for the weight enumerator of an optimal self-dual code of length 66 [7]:

$$W_{66,1} = 1 + 1690y^{12} + 7990y^{14} + \dots ,$$

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

where $0 \leq \beta \leq 778$ and

$$W_{66,3} = 1 + (858 + 8\beta)y^{12} + (18166 - 24\beta)y^{14} + (255533 + 96\beta)y^{16} + \dots,$$

where $14 \leq \beta \leq 756$.

Table 3 New self-dual [66, 33, 12] codes with weight enumerators $W_{66,2}$

β	τ	$G_{\pi,i}$	$\mu(i_1, i_2, i_3, i_4, i_5, i_6)$	S_j	$genM_2$
2	(2, 3)(8, 9, 10)	$G_{\pi,3}$	(2, 5) (0, 2, 0, 1, 2, 2)	S_3	L2
5	(9, 10)	$G_{\pi,5}$	(1, 2, 3) (0, 2, 1, 0, 2, 2)	S_3	L2
6	<i>id</i>	$G_{\pi,4}$	(2, 4, 6, 5) (0, 0, 1, 2, 1, 0)	S_3	L1
9	<i>id</i>	$G_{\pi,4}$	(2, 5)(4, 6) (0, 0, 1, 0, 0, 2)	S_3	L1
11	(9, 10)	$G_{\pi,6}$	(2, 6, 5, 4, 3) (0, 0, 0, 0, 1, 1)	S_1	L4
18	<i>id</i>	$G_{\pi,4}$	(2, 5, 3)(4, 6) (0, 2, 2, 0, 0, 0)	S_3	L1
20	<i>id</i>	$G_{\pi,3}$	(2, 5)(4, 6) (0, 2, 1, 2, 2, 0)	S_3	L1
23	<i>id</i>	$G_{\pi,5}$	<i>id</i> (0, 1, 2, 0, 0, 1)	S_3	L1
27	<i>id</i>	$G_{\pi,4}$	(2, 5)(4, 6) (0, 1, 1, 0, 0, 0)	S_3	L1
29	<i>id</i>	$G_{\pi,5}$	(2, 5, 4, 3) (0, 0, 2, 0, 1, 1)	S_1	L3
32	<i>id</i>	$G_{\pi,5}$	<i>id</i> (0, 1, 2, 0, 0, 2)	S_3	L1
33	<i>id</i>	$G_{\pi,4}$	(2, 3)(4, 6, 5) (0, 1, 0, 0, 0, 0)	S_3	L1
35	<i>id</i>	$G_{\pi,6}$	(2, 3, 4, 5) (0, 0, 0, 0, 1, 2)	S_2	L1
42	<i>id</i>	$G_{\pi,4}$	(2, 3)(4, 5) (0, 2, 2, 1, 1, 2)	S_3	L1
44	<i>id</i>	$G_{\pi,6}$	(2, 3, 4, 5) (0, 1, 2, 0, 1, 0)	S_2	L1
47	<i>id</i>	$G_{\pi,3}$	(2, 5)(3, 4, 6) (0, 0, 0, 1, 0, 0)	S_2	L1
50	<i>id</i>	$G_{\pi,5}$	(3, 5, 4) (0, 1, 0, 1, 1, 2)	S_3	L1
51	<i>id</i>	$G_{\pi,4}$	(2, 4, 5, 3) (0, 0, 1, 0, 0, 1)	S_3	L1
53	<i>id</i>	$G_{\pi,6}$	(2, 4, 6, 5) (0, 0, 1, 1, 1, 1)	S_2	L1
54	<i>id</i>	$G_{\pi,4}$	(1, 2, 6, 4, 5, 3) (0, 1, 2, 0, 1, 1)	S_3	L1
56	<i>id</i>	$G_{\pi,3}$	(2, 6, 3, 4, 5) (0, 1, 0, 0, 2, 1)	S_2	L1
59	(8, 9)	$G_{\pi,5}$	(3, 5, 4) (0, 2, 1, 0, 2, 0)	S_3	L1
60	<i>id</i>	$G_{\pi,4}$	(2, 4, 5, 3) (0, 1, 1, 0, 2, 1)	S_3	L1
62	<i>id</i>	$G_{\pi,6}$	(2, 4, 6, 5) (0, 2, 0, 0, 1, 1)	S_2	L1
63	(8, 9, 10)	$G_{\pi,4}$	(2, 4, 5 <i>t</i>) (0, 2, 1, 2, 0, 2)	S_3	L1
65	<i>id</i>	$G_{\pi,3}$	(2, 5)(3, 4, 6) (0, 0, 0, 0, 0, 0)	S_2	L1
68	(8, 9)	$G_{\pi,5}$	(3, 4) (0, 1, 0, 0, 1, 2)	S_3	L1
69	<i>id</i>	$G_{\pi,4}$	(2, 3, 5, 4) (0, 2, 0, 0, 0, 0)	S_3	L1
71	<i>id</i>	$G_{\pi,6}$	(1, 2, 3, 4, 5) (0, 1, 2, 2, 2, 1)	S_2	L1
72	(8, 9, 10)	$G_{\pi,4}$	(2, 4, 5, 3) (0, 0, 1, 2, 0, 0)	S_3	L1
77	(1, 6)	$G_{\pi,5}$	(1, 2, 6, 5, 4, 3) (0, 2, 2, 2, 2, 2)	S_3	L1
83	(8, 9, 10)	$G_{\pi,3}$	(2, 4, 6, 3, 5) (0, 1, 0, 1, 2, 2)	S_2	L1
86	(1, 6)	$G_{\pi,5}$	(1, 2, 3)(4, 6, 5) (0, 1, 1, 2, 2, 1)	S_3	L1
87	(8, 9)	$G_{\pi,4}$	(1, 2, 6, 5, 4, 3) (0, 2, 2, 1, 1, 2)	S_3	L1
92	(7, 8, 10, 9)	$G_{\pi,3}$	(2, 4, 6, 5) (0, 0, 1, 1, 1, 1)	S_2	L1

Codes exist with weight enumerator $W_{66,1}$ [17] and $W_{66,2}$ when $\beta = 0, 3, 8, 10, 14, \dots, 17, 22, 24, 26, 31, 36, 38, 41, 43, 45, 46, 52, 59, 66, 73, 74, 76, 78$ and 80 ([4, 9, 12, 14]). In this work we construct a number of optimal self-dual $[66,33,12]$ codes with weight enumerators $W_{66,2}$ for 35 new values of the parameter as follows: $\beta = 2, 5, 6, 9, 11, 18, 20, 23, 27, 29, 32, 33, 35, 42, 44, 47, 50, 51, 53, 54, 56, 59, 60, 62, 63, 65, 68, 69, 71, 72, 77, 83, 86, 87, 92$.

Remark In the second review the authors have been informed that Tsai, Shih, Su, and Chen in [18] find the first examples of codes for $W_{66,3}$ with $\beta = 28, 33,$ and 34 . They also find codes for $W_{66,2}$ with $\beta = 40$ and 44 .

Let C be a binary self-dual $[66, 33, 12]$ code having an automorphism σ of type $9-(6,4,0)$ defined in (1). We can fix D_4 to be the identity matrix over the field \mathcal{P} . In this case the code M_1 is a $[6, 1, d_1]$ self-orthogonal code over the field I_1 . There are many possibilities for the matrix S . We consider three forms up to a permutation of the coordinates followed by multiplying the coordinates by x^k for $k = 0, 1, 2$, denoted by S_1, S_2 and S_3 . In this case C_π is a binary $[10,5,2]$ self-dual code equivalent either to C_2^5 or $C_2 \oplus H_8$. We obtain four forms for $gen C_\pi$, as follows $G_{\pi,3}, G_{\pi,4}$ and $G_{\pi,5}$ up to a permutation of the first six coordinates and a permutation of the last four coordinates corresponding to the 3-cycles.

$$\begin{aligned}
 S_1 &= \begin{pmatrix} e_1 & e_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & e_1 & e_1 & e_1 & 0 \\ 0 & 0 & e_1 & e_1 & 0 & e_1 \\ 0 & 0 & e_1 & 0 & e_1 & e_1 \\ 0 & 0 & 0 & e_1 & e_1 & e_1 \end{pmatrix} & G_{\pi,3} &= \begin{pmatrix} 110000|0000 \\ 001000|1000 \\ 000100|0100 \\ 000010|0010 \\ 000001|0001 \end{pmatrix} & G_{\pi,4} &= \begin{pmatrix} 110000|0000 \\ 001000|0111 \\ 000100|1011 \\ 000010|1101 \\ 000001|1110 \end{pmatrix} \\
 S_2 &= \begin{pmatrix} e_1 & e_1 & e_1 & e_1 & 0 & 0 \\ 0 & 0 & e_1 & e_1 & 0 & e_1 \\ e_1 & e_1 & 0 & 0 & e_1 & 0 \\ 0 & e_1 & x^2e_1 & xe_1 & e_1 & e_1 \\ 0 & e_1 & xe_1 & x^2e_1 & e_1 & e_1 \end{pmatrix} & G_{\pi,5} &= \begin{pmatrix} 111100|0000 \\ 000001|1000 \\ 110010|0100 \\ 011010|0010 \\ 101010|0001 \end{pmatrix} & G_{\pi,6} &= \begin{pmatrix} 110000|0000 \\ 000000|1111 \\ 001111|0000 \\ 001100|1100 \\ 000110|0110 \end{pmatrix} \\
 S_3 &= \begin{pmatrix} e_1 & e_1 & e_1 & e_1 & e_1 & e_1 \\ 0 & e_1 & xe_1 & x^2e_1 & xe_1 & xe_1 \\ 0 & e_1 & x^2e_1 & xe_1 & x^2e_1 & x^2e_1 \\ 0 & 0 & e_1 & 0 & xe_1 & x^2e_1 \\ 0 & 0 & e_1 & 0 & x^2e_1 & xe_1 \end{pmatrix}
 \end{aligned}$$

Optimal self-dual $[66,33,12]$ codes do not exist for the matrices $G_{\pi,3}$ and $S_1, G_{\pi,4}$ and $S_1, G_{\pi,4}$ and $S_2,$ and $G_{\pi,6}$ and S_3 . In the other cases we constructed many self-dual $[66,32,12]$ codes with weight enumerators $W_{66,2}$ for 49 different values of the parameter $\beta \in \{0, 2, 5, 6, 8, 9, 11, 14, 15, 17, 18, 20, 23, 24, 26, 27, 29, 32, 33, 35, 36, 38, 41, 42, 44, 45, 47, 50, 51, 53, 54, 56, 59, 60, 62, 63, 65, 68, 69, 71, 72, 74, 77, 78, 80, 83, 86, 87, 92\}$. As was mentioned above, for 35 of them the obtained codes are the first known codes with this weight enumerators.

In Table 3 we present one code for each new value of β we have obtained.

Acknowledgments The authors are grateful to the anonymous referees for their comments. Due to their criticism the manuscript has been considerably improved. Partially supported by the Bulgarian National Science Fund under Contract MM1304/2003 and by Shumen University under Project No 31/2005.

References

1. Bouyukliev I.: An algorithm for finding isomorphisms of codes. In: Proceedings of Third Workshop OCRT'2001, pp. 35–40. Sunny Beach, Bulgaria (2001).
2. Bouyuklieva S., Russeva R., Yankov N.: Binary self-dual codes having an automorphism of order p^2 . *Mathematica Balkanica, New Series* **19**, 25–31 (2005).
3. Bouyuklieva S., Russeva R., Yankov N.: On the structure of binary self-dual codes having an automorphism of order a square of an odd prime. *IEEE Trans. Inform. Theory* **51**, 3678–3686 (2005).
4. Conway J.H., Sloane N.J.A.: A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inform. Theory* **36**, 1319–1333 (1990).
5. Dontcheva R.A., Harada M.: New extremal self-dual codes of length 62 and related extremal self-dual codes. *IEEE Trans. Inform. Theory* **48**, 2060–2064 (2002).
6. Dontcheva R.A., van Zanten A.J., Dodunekov S.M.: Binary self-dual codes with automorphisms of composite order. *IEEE Trans. Inform. Theory* **50**, 311–318 (2004).
7. Dougherty S.T., Gulliver T.A., Harada M.: Extremal binary self-dual codes. *IEEE Trans. Inform. Theory* **43**, 2036–2047 (1997).
8. Gulliver T.A., Harada M.: Weight enumerators of extremal singly-even $[60,30,12]$ codes. *IEEE Trans. Inform. Theory* **42**, 658–659 (1996).
9. Gulliver T.A., Harada M.: Classification of extremal double circulant self-dual codes of lengths 64 to 72. *Des. Codes Cryptogr.* **13**, 257–269 (1998).
10. Harada M.: Construction of an extremal self-dual codes of length 62. *IEEE Trans. Inform. Theory* **45**, 1232–1233 (1999).
11. Harada M., Gulliver T.A., Kaneta H.: Classification of extremal double circulant self-dual codes of length up to 62. *Discrete Math.* **188**, 127–136 (1998).
12. Harada M., Nishimura T., Yorgova R.: New extremal self-dual codes of length 66. *Mathematika Balkanica* **21**, 113–121 (2007).
13. Huffman W.C.: Automorphisms of codes with application to extremal doubly-even codes of length 48. *IEEE Trans. Inform. Theory* **28**, 511–521 (1982).
14. Huffman W.C.: On the classification and enumeration of self-dual codes. *Finite Fields and Their Applications* **11**, 451–490 (2005).
15. Ling S., Sole P.: On the algebraic structure of quasi-cyclic codes I: Finite fields. *IEEE Trans. Inform. Theory* **47**, 2751–2760 (2001).
16. Tsai H.P.: Existence of certain extremal self-dual codes. *IEEE Trans. Inform. Theory* **38**, 501–504 (1992).
17. Tsai H.P.: Extremal self-dual codes of length 66 and 68. *IEEE Trans. Inform. Theory* **45**, 2129–2133 (1999).
18. Tsai H.P., Shih P.Y., Su W.K., Chen C.H.: Cosets of Self-Dual Codes. *Des. Codes Cryptogr.* (Submitted).
19. Yorgov V.Y.: A method for constructing inequivalent self-dual codes with applications to length 56. *IEEE Trans. Inform. Theory* **33**, 77–82 (1987).
20. Yorgov V.Y.: Binary self-dual codes with an automorphism of odd order. *Problems Inform.Transm.* **4**, 13–24 (1983) (in Russian).