Finite Fields and Their Applications 18 (2012) 1104–1113

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Classification of binary self-dual $[48, 24, 10]$ codes with an automorphism of odd prime order

Stefka Bouyuklieva [a], Nikolay Yankov [b], Jon-Lark Kim [c,*]

[a] *Faculty of Mathematics and Informatics, Veliko Tarnovo University, 5000 Veliko Tarnovo, Bulgaria*
[b] *Faculty of Mathematics and Informatics, Shumen University, 9700 Shumen, Bulgaria*
[c] *Department of Mathematics, Sogang University, Seoul 121-742, South Korea*

ARTICLE INFO

Article history:
Received 19 January 2012
Revised 1 August 2012
Accepted 14 August 2012
Available online 24 August 2012
Communicated by W. Cary Huffman

MSC:
94B05

Keywords:
Automorphism groups
Cubic self-dual codes
Self-dual codes

ABSTRACT

The purpose of this paper is to complete the classification of binary self-dual $[48, 24, 10]$ codes with an automorphism of odd prime order. We prove that if there is a self-dual $[48, 24, 10]$ code with an automorphism of type p-(c, f) with p being an odd prime, then $p = 3$, $c = 16$, $f = 0$. By considering only an automorphism of type 3-$(16, 0)$, we prove that there are exactly 264 inequivalent self-dual $[48, 24, 10]$ codes with an automorphism of odd prime order, equivalently, there are exactly 264 inequivalent cubic self-dual $[48, 24, 10]$ codes.

1. Introduction

A linear $[n, k]$ code over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. A linear code C is called *self-dual* if it is equal to its dual $C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ for any } c \in C\}$. The classification of binary self-dual codes was initiated and done up to length 20 by V. Pless [15]. Since then the classification of self-dual codes has been one of the most active research topics (see [16,14]). The classification of binary self-dual $[38, 19, 8]$ codes has been recently done by Aguilar-Melchor, Gaborit, Kim, Sok, and Solé [1] and independently by Betsumiya, Harada and Munemasa [2]. Very recently, Bouyuklieva and Bouyukliev [7] have classified all binary self-dual $[38, 19]$ codes.

In this paper, we are interested in the classification of binary self-dual $[48, 24, 10]$ codes with an automorphism of odd prime order. It was motivated by the following reasons. Bonnecaze, et al. [3]

* Corresponding author.
E-mail addresses: stefka@uni-vt.bg (S. Bouyuklieva), jankov_niki@yahoo.com (N. Yankov), ctryggoggo1@gmail.com (J.-L. Kim).

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2012.08.002

constructed binary self-dual codes with a fixed-point free automorphism of order 3, called *cubic self-dual codes* due to the correspondence with self-dual codes over a ring $\mathbb{F}_2[Y]/(Y^3-1)$. They gave a partial list of binary cubic self-dual codes of lengths $\leqslant 72$ by combining binary self-dual codes and Hermitian self-dual codes. Later, Han, et al. [11] have given the classification of binary cubic optimal self-dual codes of length $6k$ where $k=1,2,\ldots,7$. Hence it is natural to ask exactly how many binary cubic self-dual optimal $[48,24,10]$ codes exist and we answer it in this paper. On the other hand, we have noticed that Huffman [14, Table 2] listed all possible values of the type p-(c,f) with p odd for an automorphism of a self-dual $[48,24,10]$ code. They are 11-(4, 4), 7-(6, 6), 5-(8, 8), 3-(14, 6), and 3-(16, 0). We will show that the first four types are not possible. Therefore, the classification of binary $[48,24,10]$ self-dual codes with a nontrivial odd order automorphism coincides with the classification of binary $[48,24,10]$ self-dual cubic codes.

There are two possible weight enumerators for self-dual $[48,24,10]$ codes [10]:

$$W_{48,1}(y)=1+704y^{10}+8976y^{12}+56\,896y^{14}+267\,575y^{16}+\cdots, \tag{1}$$

$$W_{48,2}(y)=1+768y^{10}+8592y^{12}+57\,600y^{14}+267\,831y^{16}+\cdots. \tag{2}$$

Brualdi and Pless [8] found a self-dual $[48,24,10]$ code with weight enumerator $W_{48,1}$. The order of its group of automorphisms is 4. A classification of binary self-dual $[48,24,10]$ codes with $W_{48,1}$ is known [12]. A code with weight enumerator $W_{48,2}$ is given in [10].

The first author [6] showed that any code with $W_{48,1}(y)$ has no automorphism of odd prime order and that any code with $W_{48,2}(y)$ has a group of automorphisms of order 2^l3^s for some integers $l\geqslant 0$ and $s\geqslant 0$. However, this result has received less attention and hence we will include it briefly. In this paper, we prove that if there is a self-dual $[48,24,10]$ code with an automorphism of type p-(c,f) with p being an odd prime, then $p=3$, $c=16$, $f=0$. Therefore by considering only an automorphism of type 3-(16, 0), we prove that there are exactly 264 inequivalent self-dual $[48,24,10]$ codes with an automorphism of odd prime order. To do that we apply the method for constructing binary self-dual codes possessing an automorphism of odd prime order (see [13,17,18]).

2. Construction method

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

$$\sigma=(1,2,\ldots,p)(p+1,p+2,\ldots,2p)\cdots\big((c-1)p+1,(c-1)p+2,\ldots,cp\big), \tag{3}$$

and say that σ is of *type* p-(c,f).

We begin with a theorem which gives a useful restriction for the type of the automorphism.

Theorem 2.1. *(See [18].) Let C be a binary self-dual $[n,n/2,d]$ code with an automorphism of type p-(c,f) where p is an odd prime. Denote $g(k)=d+\lceil\frac{d}{2}\rceil+\cdots+\lceil\frac{d}{2^{k-1}}\rceil$. Then:*

(i) *$pc\geqslant g(\frac{(p-1)c}{2})$ and if $d\leqslant 2^{(p-1)c/2-2}$ the equality does not occur;*
(ii) *if $f>c$ then $f\geqslant g(\frac{f-c}{2})$ and if $d\leqslant 2^{(f-c)/2-2}$ the equality does not occur;*
(iii) *if 2 is a primitive root modulo p then c is even.*

Applying the theorem for the parameters $n=48$ and $d=10$, we obtain

Corollary 2.2. *Any putative automorphism of an odd prime order for a singly-even self-dual $[48,24,10]$ code is of type* 47-(1, 1), 23-(2, 2), 11-(4, 4), 7-(6, 6), 5-(8, 8), 3-(12, 12), 3-(14, 6), *or* 3-(16, 0).

Denote the cycles of σ by $\Omega_1=\{1,2,\ldots,p\}$, $\Omega_2,\ldots,\Omega_c$, and the fixed points by $\Omega_{c+1}=\{cp+1\},\ldots,\Omega_{c+f}=\{cp+f=n\}$. Define

$$F_\sigma(C) = \{ v \in C \mid \sigma(v) = v \},$$
$$E_\sigma(C) = \{ v \in C \mid \mathrm{wt}(v|\Omega_i) \equiv 0 \pmod 2,\ i = 1, \ldots, c+f \},$$

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

Theorem 2.3. *(See [13].)* $C = F_\sigma(C) \oplus E_\sigma(C)$, $\dim(F_\sigma(C)) = \frac{c+f}{2}$, $\dim(E_\sigma(C)) = \frac{c(p-1)}{2}$.

We have that $v \in F_\sigma(C)$ if and only if $v \in C$ and v is constant on each cycle. The cyclic group generated by σ splits the set of codewords into disjoint orbits which consists of p or 1 codewords. Moreover, a codeword v is the only element in an orbit if and only if $v \in F_\sigma(C)$. Using that all codewords in one orbit have the same weight, we obtain the following proposition.

Proposition 2.4. *Let $(A_0, A_1, \ldots, A_n)$ and $(B_0, B_1, \ldots, B_n)$ be the weight distributions of the codes C and $F_\sigma(C)$, respectively. Then $A_i \equiv B_i \pmod p$.*

Proposition 2.4 eliminates the first two types from Corollary 2.2. In fact, these cases were eliminated by Huffman [14, Appendix] in a different way.

Corollary 2.5. *If C is a self-dual $[48, 24, 10]$ code, then C does not have automorphisms of orders 47 and 23.*

Proof. Let σ be an automorphism of C. If σ is of type 47-(1, 1) then $F_\sigma(C)$ is the repetition $[48, 1, 48]$ code and therefore $B_{10} = 0$. Since neither 704 nor 768 is congruent 0 modulo 47, this case is not possible.

If the type is 23-(2, 2) then $B_i = 0$ for $0 < i < 24$. Therefore $B_{10} = 0$ and $A_{10} \not\equiv B_{10} \pmod{23}$ – a contradiction. □

To understand the structure of a self-dual code C invariant under the permutation (3), we define two maps. The first one is the projection map $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$ where $(\pi(v))_i = v_j$ for some $j \in \Omega_i$, $i = 1, 2, \ldots, c+f$, $v \in F_\sigma(C)$.

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 $\mathbb{F}_2[x]/(x^p - 1)$. $\mathcal{P}$ is a cyclic code of length p with generator polynomial $x - 1$. Moreover, if 2 is a primitive root modulo p, $\mathcal{P}$ is a finite field with 2^{p-1} elements [13]. In this way we obtain the map $\varphi : E_\sigma(C)^* \to \mathcal{P}^c$. Let $C_\pi = \pi(F_\sigma(C))$ and $C_\varphi = \varphi(E_\sigma(C)^*)$. The following theorems give necessary and sufficient conditions for a binary code with an automorphism of type (3) to be self-dual.

Theorem 2.6. *(See [18].) 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_π is a binary self-dual code of length $c+f$,*
(ii) *for every two vectors $u, v \in C_\varphi$ we have $\sum_{i=1}^{c} u_i(x) v_i(x^{-1}) = 0$.*

Theorem 2.7. *(See [13].) Let 2 be a primitive root modulo p. Then the binary code C with an automorphism σ is self-dual if and only if the following two conditions hold*:

(i) *C_π is a self-dual binary code of length $c+f$;*
(ii) *C_φ is a self-dual code of length c over the field $\mathcal{P}$ under the inner product $(u, v) = \sum_{i=1}^{c} u_i v_i^{2^{(p-1)/2}}$.*

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

Theorem 2.8. *(See [17].) 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, $1 \leqslant t \leqslant p-1$;*
(b) *multiplication of the jth coordinate of C_φ by x^{t_j} where t_j is an integer, $0 \leqslant t_j \leqslant p-1$, $j = 1, 2, \dots, c$;*
(c) *permutation of the first c cycles of C;*
(d) *permutation of the last f coordinates of C.*

3. Codes with an automorphism of odd prime order

3.1. Codes with an automorphism of order 3

In this section we first classify self-dual codes with an automorphism of order 3.

Let C be a self-dual $[48, 24, 10]$ code with an automorphism of order 3. According to Corollary 2.2 this automorphism is of type 3-(12,12), 3-(14,6) or 3-(16,0). In this section we prove that only the type 3-(16,0) is possible. Moreover, we classify all binary self-dual codes with the given parameters which are invariant under a fixed point free permutation of order 3.

Proposition 3.1. *Self-dual* $[48, 24, 10]$ *codes with an automorphism of type* 3-$(12, 12)$ *do not exist.*

Proof. In this case the code C_φ is a self-dual $[12, 6]$ code over the field $\mathcal{P} = \{0, e(x) = x + x^2, xe(x), x^2e(x)\}$ under the inner product $(u, v) = u_1v_1^2 + u_2v_2^2 + \cdots + u_{12}v_{12}^2$. The highest possible minimum distance of a quaternary Hermitian self-dual $[12, 6]$ code is 4 (see [9]), hence the minimum distance of $E_\sigma(C)$ can be at most 8 – a conflict with the minimum distance of C. □

Proposition 3.2. *Self-dual* $[48, 24, 10]$ *codes with an automorphism of type* 3-$(14, 6)$ *do not exist.*

Proof. Assume that $\sigma = (1, 2, 3)(4, 5, 6) \cdots (40, 41, 42)$ is an automorphism of the self-dual $[48, 24, 10]$ code C. Then C_π is a binary self-dual $[20, 10, 4]$ code. There are exactly 7 inequivalent self-dual $[20, 10, 4]$ codes, namely J_{20}, $A_8 \oplus B_{12}$, K_{20}, L_{20}, S_{20}, R_{20} and M_{20} (see [15]). If C_π is equivalent to any of these codes there is a vector $v = (v_1, v_2)$ in C_π with $v_1 \in \mathbb{F}_2^{14}$, $v_2 \in \mathbb{F}_2^6$ and $wt(v_1) = wt(v_2) = 2$. Thus the vector $\pi^{-1}(v) \in F_\sigma(C)$ has weight 8 which contradicts the minimum distance. □

Let now C be a singly-even $[48, 24, 10]$ code, possessing an automorphism with 16 cycles of length 3 and no fixed point in its decomposition into independent cycles.

According to Theorem 2.6, the subcode C_π is a binary self-dual $[16, 8, \geqslant 4]$ code. We further show that C_π is singly-even as follows. By Theorem 2.7(ii), C_φ is Hermitian self-dual over $\mathcal{P}$, which is the field of 4 elements given in the proof of Proposition 3.1. So C_φ has only even weight vectors, implying that $E_\sigma(C)$ has all vectors of weights a multiple of 4. If C_π is doubly-even, all vectors in $F_\sigma(C)$ also have weights a multiple of 4, making C doubly-even, a contradiction. So C_π is singly-even.

There is one such code, denoted by F_{16} in [15], with a generator matrix

$$G_B = \begin{pmatrix} 1000001110010010 \\ 0100001110011101 \\ 0010001110001111 \\ 0001001100011010 \\ 0000101010011010 \\ 0000010110011010 \\ 0000000001010110 \\ 0000000000110011 \end{pmatrix}.$$

It is more convenient for us to denote this code by B. The automorphism group of B is generated by the permutations $(1,12,4,2,13,15,9,3)(5,16,8,11)(6,14)(7,10)$ and $(1,8,7)(5,6,13)(10,12)(14,15)$. Its order is 76 728.

According to Theorem 2.6 the subcode C_φ is a quaternary Hermitian self-dual $[16,8,\geqslant 5]$ code. There are exactly 4 inequivalent such codes 1_{16}, 1_6+2f_5, $4f_4$, and $2f_8$ [9]. Their generator matrices in standard form are $G_i=(I|X_i)$, $i=1,\dots,4$, where

$$X_1=\begin{pmatrix} 0 & 0 & \omega & 1 & 1 & 1 & 0 & \omega^2\\ \omega^2 & \omega^2 & 0 & \omega^2 & \omega & \omega^2 & 1 & 1\\ \omega & 0 & 1 & \omega & 0 & 1 & \omega & 0\\ 1 & \omega^2 & \omega^2 & \omega & \omega^2 & \omega^2 & \omega^2 & 0\\ 0 & 1 & 1 & 1 & \omega^2 & \omega^2 & \omega & 1\\ \omega^2 & 1 & \omega^2 & 0 & \omega & 0 & \omega & 0\\ \omega & 0 & \omega & \omega^2 & 1 & \omega & 1 & \omega^2\\ 0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 \end{pmatrix},$$

$$X_2=\begin{pmatrix} \omega^2 & 1 & \omega^2 & 0 & \omega^2 & 0 & \omega & 0\\ 1 & \omega^2 & \omega & \omega^2 & 1 & 1 & 0 & 1\\ \omega & 1 & 1 & \omega^2 & 1 & \omega^2 & \omega^2 & 0\\ 0 & \omega & 0 & \omega^2 & 0 & 1 & \omega^2 & \omega^2\\ 1 & \omega & 0 & \omega & 1 & 1 & \omega^2 & 1\\ 0 & \omega^2 & \omega & 1 & \omega^2 & \omega & \omega & \omega^2\\ \omega & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & 0\\ 0 & \omega & \omega^2 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 \end{pmatrix},$$

$$X_3=\begin{pmatrix} \omega & 0 & \omega^2 & 0 & 0 & \omega^2 & 1 & \omega^2\\ 1 & \omega^2 & \omega & \omega^2 & 1 & 1 & 0 & 1\\ \omega^2 & \omega^2 & \omega^2 & \omega & 0 & \omega & \omega & 1\\ 1 & \omega^2 & 0 & \omega^2 & \omega^2 & \omega & 0 & 0\\ 1 & \omega & 0 & \omega & 1 & 1 & \omega^2 & 1\\ 0 & 1 & \omega^2 & \omega & \omega & \omega^2 & \omega^2 & \omega\\ 1 & 1 & 1 & \omega & 0 & 0 & 0 & \omega^2\\ 1 & \omega & 0 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 \end{pmatrix},$$

$$X_4=\begin{pmatrix} 1 & 0 & \omega^2 & \omega^2 & \omega & 1 & \omega^2 & 1\\ 1 & \omega^2 & \omega & \omega^2 & 1 & 1 & 0 & 1\\ \omega & 1 & 1 & \omega^2 & 1 & \omega^2 & \omega^2 & 0\\ \omega & \omega^2 & 0 & 0 & 1 & 0 & \omega & \omega\\ 1 & \omega & 0 & \omega & 1 & 1 & \omega^2 & 1\\ 1 & 0 & \omega & \omega^2 & 0 & 1 & 1 & 0\\ \omega & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & 0\\ 0 & \omega^2 & 1 & \omega & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Denote by C_i^τ the self-dual $[48,24,10]$ code with a generator matrix

$$\operatorname{gen} C_i^\tau=\begin{pmatrix}\pi^{-1}(\tau B)\\ \varphi^{-1}(X_i)\end{pmatrix},$$

where τ is a permutation from the symmetric group S_{16}, and $1\leqslant i\leqslant 4$. We use the following.

Lemma 3.3. *(See [18].) If τ_1 and τ_2 are in one and the same right coset of* $\mathrm{Aut}(B)$ *in S_{16}, then $C_i^{\tau_1}$ and $C_i^{\tau_2}$ are equivalent.*

Table 1
Generating permutations and $|\mathrm{Aut}(C)|$ for codes with $C_\varphi = 1_{16}$.

Permutation	|Aut|	Permutation	|Aut|	Permutation	|Aut|
(5,6)(12,14)	3	(2,3,14,8,12,6)(5,9,11)	6	(2,14,8,12,6)(5,9,11)	6
(3,6,5,12,10,9,11)	6	(3,6,7,5,12,14,15,9,11)	6		

Table 2
Generating permutations and $|\mathrm{Aut}(C)|$ for codes with $C_\varphi = 1_6 + 2f_5$.

Permutation	|Aut|	Permutation	|Aut|	Permutation	|Aut|
(1,2,16,14,15,10,13)	3	(1,7,12,13,5,2,10,11,9)	3	(1,12,16,9)(2,10,13,6,5)	3
(2,10,13,4,8,7,12,16,11,9)	3	(2,11,16,5,10,8,12,13)	3	(2,12)(4,6,8,7)(14,16)	3
(2,12,9,11,14,6,7,8)	3	(2,13)(3,7,12,6,11,10)	3	(2,14,12,13,4,6,11,9,8,3)	3
(2,15,3,11,10,13)	3	(2,8,11,14,16,13,4)(6,12)	3	(2,8,11,5,12,13)	3
(2,8,7,15,11,16)(6,14)	3	(2,9,7,12,10,16,13)(6,15)	3	(2,16,8,13)(6,11,7,12,10,9)	3
(3,10)(4,7,11,13)(6,12,8)	3	(2,3,11,10,6,5,8,4,12)	6	(2,8,14,6,5,9,15)	6
(2,8,15,9,11,10,6,5)	6	(2,12,3)(7,10,9,8)	6		

In order to classify all codes we have considered all representatives of the right transversal of S_{16} with respect to $\mathrm{Aut}(B)$. We have checked the equivalence of codes using Q-Extension [4]. The obtained inequivalent codes and the orders of their automorphism groups are listed in Tables 1–4, where the column labeled "permutation" is the value of τ used to construct $\mathrm{gen}\, C_i^\tau$.

Proposition 3.4. *There are exactly* 264 *inequivalent binary* $[48, 24, 10]$ *self-dual codes with an automorphism of type* 3-$(16, 0)$.

Corollary 3.5. *There are exactly* 264 *inequivalent binary cubic self-dual* $[48, 24, 10]$ *codes.*

3.2. Codes with automorphisms of orders 5, 7, and 11

The first author [6] showed that there are no self-dual $[48, 24, 10]$ codes with automorphisms of orders 5, 7, and 11. However, these results have received less attention since even Huffman in his survey paper [14] could not eliminate these types of automorphisms. Hence it is worth sketching the nonexistence of self-dual $[48, 24, 10]$ codes with automorphisms of orders 5, 7, and 11.

Let C be a binary singly-even self-dual $[48, 24, 10]$ code with an automorphism of order 11 and

$$\sigma = (1, 2, \dots, 11)(12, \dots, 22)(23, \dots, 33)(34, \dots, 44)$$

be an automorphism of C. Then $\pi(F_\sigma(C))$ is a binary self-dual code of length 8.

Lemma 3.6. *The code $\pi(F_\sigma(C))$ is generated by the matrix $(I_4|I_4 + J_4)$ up to a permutation of the last four coordinates. Here I_4 is the identity matrix and J_4 is the all-one matrix.*

Since 10 is the multiplicative order of 2 modulo 11, $C_\varphi = \varphi(E_\sigma(C)^*)$ is a self-dual $[4, 2]$ code over the field $\mathcal{P}$ of even-weight polynomials in $F_2[x]/(x^{11} - 1)$ with 2^{10} elements under the inner product

$$(u, v) = u_1 v_1^{32} + u_2 v_2^{32} + u_3 v_3^{32} + u_4 v_4^{32}. \tag{4}$$

Lemma 3.7. *C_φ is a* $[4, 2, 3]$ *self-dual code over the field $\mathcal{P}$.*

By considering all possibilities of C_φ, one can get the following.

Theorem 3.8. *(See [6].) There does not exist a self-dual* $[48, 24, 10]$ *code with an automorphism of order* 11.

Table 3
Generating permutations and $|\mathrm{Aut}(C)|$ for codes with $C_\varphi = 4f_4$.

Permutation	|Aut|	Permutation	|Aut|	Permutation	|Aut|
(1,2,10,5,6,11,13,16)(3,4)	3	(1,14,4,10,11,7,9,3)(8,15)	3	(1,16,7)(2,15,14,6)(4,12,5)	3
(1,16,8,6,14,4,11,12,7,3)	3	(2,3,6,9,8,12,7,16,10)	3	(2,3,9)(4,7,10,5)	3
(2,5,4,9,3,14,6)(12,16)	3	(2,5,6,15)(7,10,11)(9,12)	3	(2,6,10,3,9,15,8,12,4,16)	3
(2,6,16,10)(4,15,5)(7,12)	3	(2,6,16,10)(7,9,8,12)	3	(2,6,3,5,12,13)(7,9,10,16)	3
(2,6,5,12,9,8,14,11)	3	(2,7,9,8,12,13)(5,16,10,14)	3	(2,8,12)(4,16,9,15,6,10)	3
(2,8,12,13)(5,14,9,11,15,6)	3	(2,8,4,3,6,11)(5,15)	3	(2,8,7,15,9,11)(5,10)	3
(2,9,11,10,5,8,12,15,6)	3	(2,9,11,8,14,10,6,5,15)	3	(2,9,15,8,12,6,11,5)	3
(2,9,6,5,12,13)	3	(2,9,8,10,14,5,6)	3	(2,9,8,11,6)(5,16,10)	3
(2,9,8,12,3,6,11)	3	(2,9,8,16,14,6,5,12,3,13)	3	(2,9,8,6)(5,10)	3
(2,9,8,7,14,10,16)(6,12)	3	(2,9,8,7,4,12,15,13)	3	(2,10,5,12,9,8,11,15,6)	3
(2,10,5,16,7,6,4,12,15,13)	3	(2,10,5,4,11,15,9,12,6)	3	(2,11,5,4,3,14,6)(9,15)	3
(2,11,9,12)(5,15)(7,10)	3	(2,13)(3,5,4)(6,16,12,14)	3	(2,13)(5,11,12,9,8,14,6)	3
(2,13)(5,12,16,6,7,9,11,10)	3	(2,14,12,13)(3,5,4)(6,16)	3	(2,14,6)(3,11,5,4,15,9)	3
(2,14,7,5,4,15,8,10,11)	3	(2,14,9,12,6)(4,11,10,5)	3	(3,4)(6,15,11,8,7,14)	3
(3,5)(4,12,16,6)(7,15,14)	3	(3,5)(6,15)(7,12)(14,16)	3	(3,5)(6,15,7,12)	3
(3,5)(6,9,15,10,16,7,12)	3	(3,5,15)(6,10,12)(9,11)	3	(3,5,15,6,10)(9,11)	3
(3,5,15,8,16,6,10)(9,11)	3	(3,6,11,9,5,8,12,10)	3	(3,6,9,15,7,12,5)	3
(3,7,10,16,5,15,11,9,8)	3	(3,7,12,6,16,10,15,5)	3	(3,7,4,12,5)(6,15)(10,11)	3
(3,11)(5,15)(7,8,10,9,12)	3	(3,11,6,4,12,7,15,5)	3	(3,11,8,14,6,10,5,15)	3
(3,11,8,15)(5,14)(6,10)	3	(3,14,11,5,4,12,6,15,7)	3	(3,14,6,15,16,7,4,12,5)	3
(3,16)(5,15,9,12)(7,8,10)	3	(3,16,5,15,9,12,7,8,10)	3	(3,16,6,15,9,10)(5,12)	3
(3,16,7,12,9,5)(6,14)	3	(3,16,7,4,15,6,10,12,5)	3	(3,16,9,5,12)(6,10)(7,14)	3
(5,12,7,10,9,8,14)	3	(5,12,9,11,8,14)(6,10)	3	(5,14,16)(6,11,8,15)	3
(5,15,9,11,8,16,6,10)	3	(7,11,12,9,8)	3	(1,15,7,6,10,11,8,14,4,3)	6
(2,5,3,7)(6,16,14)	6	(2,6,12,5,15)(9,11)	6	(2,6,7,15)(5,12)(9,11)	6
(2,7,10,13)(3,9,8,12,14,5,16)	6	(2,7,10,5,16,9,8,12,13)	6	(2,7,15)(5,6,12,16,9,10)	6
(2,7,8,15,9,10,5,12,11)	6	(2,9,11)(5,8,15,14,6,12)	6	(2,9,11,10,5,16,6,12,13)	6
(2,9,11,6,16,5,8,12,13)	6	(2,9,6,5,11,12,13)(8,14)	6	(2,9,6,5,14,8,11,16,12,13)	6
(2,9,8,14,6,12)(7,15)	6	(2,9,8,14,6,15)(7,12)	6	(2,13)(5,12,9,11)(6,16,14)	6
(2,13)(5,16,7,10)(6,12,9)	6	(2,13)(5,6,12)(7,16)(9,10,11)	6	(2,13)(5,8,12,9,11)(6,16)	6
(2,13)(5,8,16,6,12,9,11)	6	(2,14)(5,12,9,8,15,6,11)	6	(2,14,6,15,9,11)(5,8,12)	6
(2,16,7,10,5,15,9,8,12)	6	(3,5,12,7,10,16)(8,15,9)	6	(3,5,8,15,6,12,9,11)	6
(3,6,11,14,9,8,12)(5,15)	6	(3,7,12,5,4)(6,15,14)	6	(3,7,5,4,12,13)(6,14)	6
(3,9,10,5,6,15,11)(7,12)	6	(3,9,12,7,10,11)(4,15,5)	6	(3,9,8,15,7,10,11)(5,12)	6
(3,10,11,6,12,5)(7,15)	6	(3,11,5,15,9,8,12,7,10)	6	(3,11,7,12,14,6,15,5)	6
(3,11,7,12,6,9,15,10,5,13)	6	(3,11,7,15,5,4)(6,12)	6	(3,11,7,15,6,12,5,4)	6
(3,11,7,9,15,6,12,10,5,13)	6	(4,11,9)(5,15,6,12)	6	(5,6,12)(7,15,9,10,11)	6
(5,8,15,10,6,12,9,11)	6	(5,10)(6,16,7,9,11,8,14)	6	(5,15)(7,8,12,9,10,11)	6
(5,15,7,8,12,9,10,11)	6	(1,16,7)(2,15,5,4,12,14,6)	12	(3,9,12,14,6,11)(4,15,5)	12
(5,15,6,11,9,8,12)	12	(2,6,12,7,16,13)(3,5)	24	(3,6,7,12,9,11,10)(5,15)	24
(2,5,3,6,12,7,16,13)	48				

Let C be a binary singly-even self-dual $[48, 24, 10]$ code with an automorphism of order 7 and let

$$\sigma = (1, 2, \dots, 7)(8, \dots, 14) \cdots (36, \dots, 42).$$

Now $\pi(F_\sigma(C))$ is a $[12, 6]$ self-dual code. Since the minimal distance of $F_\sigma(C)$ is at least 10, $\pi(F_\sigma(C))$ has a generator matrix of the form $(I_6|A)$, where I_6 is the identity matrix. We obtain a unique possibility for A up to a permutation of its columns:

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{5}$$

Table 4
Generating permutations and $|\mathrm{Aut}(C)|$ for codes with $C_\varphi = 2f_8$.

Permutation	|Aut|	Permutation	|Aut|	Permutation	|Aut|
(1,11,12,5,3,13,2,8,15,9)	3	(1,12,3,7,10)(4,5,14,13,16)	3	(2,3,11,12,8,7,5)	3
(2,5,11,12,3,6)(9,10)	3	(2,5,11,6)(8,14,12,15)	3	(2,5,3,10,6,4,11)(7,15)	3
(2,5,3,6)(8,15,16,9,10)	3	(2,5,4,12,3,6)(9,16,10)	3	(2,5,4,3,6)(9,15,16,10)	3
(2,5,7,3,6,15,9,11)	3	(2,5,8,11,12,3,6)(9,10)	3	(2,5,8,15,10,11,6)	3
(2,5,8,15,11,3,6)	3	(2,6)(3,5)(8,15,16,9,10)	3	(2,6)(3,5,4)(9,11,12)	3
(2,6)(3,5,4,15,16,10,9)	3	(2,6)(3,5,4,16,14,9,12)	3	(2,6)(3,5,7)(9,15,10,16)	3
(2,6)(3,5,8,4,10,11,12)	3	(2,6)(3,8,16,9,10,5,12)	3	(2,8,12,3,6)(5,16,9,10)	3
(2,8,4,10,5,11,12,3,6)	3	(2,8,4,12,3,6)(5,11)	3	(2,9,10,11,5)(3,8,7,12)	3
(2,9,11,5,15,8,3,6)	3	(2,9,11,5,3,6)(8,15)	3	(2,9,11,6,8,16,5,12)	3
(2,9,11,8,3,5,15,16,14,6)	3	(2,9,15,5,3,8,11,12,14,6)	3	(2,9,8,14,5,10,6)(15,16)	3
(2,9,8,16,5,12,11,6)	3	(2,9,8,5,6)(12,14,15)	3	(2,9,8,5,6)(12,16,15)	3
(2,9,8,5,6)(15,16)	3	(2,9,8,6)(12,16,15)	3	(2,10,7,9,15)(3,6,11,5)	3
(2,11,12,8,7,5)	3	(2,11,14,15,9,4,5,7)	3	(2,11,3,5,8,4)(6,12)	3
(2,11,6)(5,12,9,8,16)	3	(2,12,16,10,3,9,7,5,4)	3	(2,15)(5,7,10)(6,14)(9,11)	3
(2,15,16,10,9,5,4,6)	3	(2,15,16,11,9,10,5,6)	3	(2,15,16,14,10,8,6,7)	3
(2,15,16,14,6)(4,10,5)	3	(2,15,16,14,6,12,5,4)	3	(2,15,16,14,8,6,7)	3
(2,15,16,9,10,5,14,6)	3	(2,15,16,9,10,5,14,6,7)	3	(2,15,16,9,10,5,6,7)	3
(2,15,5,12,6)(8,16)(9,10)	3	(2,15,5,14,6,7)(9,11,12)	3	(2,15,5,16,8,12,9,11,13,4)	3
(2,15,5,8,10,6)(9,11,12)	3	(2,15,6)(4,11,9)(5,16)	3	(2,15,6)(5,10)(8,14,9,11)	3
(2,15,6)(5,10,9,11,8,14)	3	(2,15,6)(5,11)(8,14)(9,10)	3	(2,15,6)(5,12)(8,16)(9,10)	3
(2,15,8,10,13,4)(5,14,16)	3	(2,15,8,6)(5,12,9,10,11)	3	(3,5)(4,11,7,15,16,6)	3
(3,5,12,6,11,9,8,16)	3	(3,6,4,11,14,5)(7,15,10)	3	(3,7,9,15,6,11,14,12,5)	3
(3,12,5,7)(6,15)(9,11)	3	(3,15,6,8,10,5,14,9,11)	3	(3,16,14,5)(6,11,7,9,15)	3
(3,16,5)(6,8,15,9,11)	3	(3,16,9,11,5,7,15,6)	3	(4,7,11,12,6)(5,15)	3
(5,7,12,9,10)	3	(5,7,14)(6,10)(9,11)	3	(5,15)(6,9,11,12)	3
(1,2,14,15,16,8,11,13,9)	6	(1,2,15,16,13,7,5,10,14,9)	6	(1,2,9)(5,15,11,12,13,7)	6
(1,15,13,12,9)(5,7,10,11)	6	(1,15,9)(5,6,12)(10,13)	6	(2,5,3,6)(8,15)(9,11,10)	6
(2,5,6,10,16)(4,12,13)(9,15)	6	(2,6)(3,14,5,9,15,16)	6	(2,6)(5,10,8,16)(9,11)	6
(2,6,11,5,16,15,8)(9,10)	6	(2,6,7,11)(5,12)(9,10)	6	(2,6,7,8,9,11,12,14)	6
(2,6,8,11,13,4)(3,5)	6	(2,7,11,12)(5,9,10)(6,14)	6	(2,7,11,12)(5,9,10,6,14)	6
(2,8,10,3,13,4)(5,15,16)	6	(2,8,10,5,15,16,3,13,4)	6	(2,9,11,5,3,8,15,14,6)	6
(2,11,12,13,4)(5,10)(8,15)	6	(2,11,12,3,13,4)(5,10,9,7)	6	(2,12,10,16,6,7,8,4)	6
(2,12,16,9,4,10,6)(8,14)	6	(2,15,11,12,10,9,8,5,6)	6	(2,15,11,12,14,6,8,13,4)	6
(2,15,16,10,13,4,11,8,6)	6	(2,15,16,14,6,8,4)	6	(2,15,16,6)(4,10,8,14,9)	6
(2,15,5,11,6)(4,16,8)	6	(2,15,5,9,10,11,6)	6	(2,15,9,4,5,7,10,11,12)	6
(3,5,9,11)(6,10,12)(7,14)	6	(3,9,5,7,10,11,12)	6	(3,16)(5,8,9,15)(6,12)	6
(3,16)(5,9,15)(6,12)	6	(3,16)(5,9,15,6,12)	6	(3,16,15,6,7,9,11)	6
(5,9,10,6,11,12,7,14)	6	(5,9,10,6,14)(7,11,12)	6	(5,9,11,12,7,14)(6,10)	6
(1,16,7,14,6,11,8,2,4,3)	12	(1,15,3,9)(5,7,10,11,13,12)	24	(2,5,7,10,11,13,4,12,9,15)	24
(4,15,5,7,10,16,13)(9,12)	24				

Since $2^3 \equiv 1 \pmod 7$, 2 is not a primitive root modulo 7 and $\mathcal{P}$ is not a field. Now $\mathcal{P} = I_1 \oplus I_2$, where I_1 and I_2 are cyclic codes generated by the idempotents $e_1(x) = 1 + x + x^2 + x^4$ and $e_2(x) = 1 + x^3 + x^5 + x^6$, respectively, so

$$I_j = \{0, e_j(x), xe_j(x), \ldots, x^6 e_j(x)\}, \quad j = 1, 2.$$

Moreover, I_1 and I_2 are fields of 8 elements [18].

In this case $C_\varphi = \varphi(E_\sigma(C)^*) = M_1 \oplus M_2$, where $M_j = \{u \in C_\varphi \mid u_i \in I_j,\ i = 1, \ldots, 6\}$ is a linear code of length 6 over the field I_j, $j = 1, 2$, and $\dim_{I_1} M_1 + \dim_{I_2} M_2 = 6$ [18]. Since the minimum weight of the code C is 10, every vector of C_φ must contain at least three nonzero coordinates. Hence the minimum weight of M_j is at least 3. Thus by the Singleton Bound, the maximum dimension of M_j is at most 4. Therefore the dimension of M_j is at least 2, $j = 1, 2$.

By Theorem 2.6 for every two vectors $(u_1(x), \ldots, u_6(x))$ from M_1 and $(v_1(x), \ldots, v_6(x))$ from M_2 we have

$$u_1(x)v_1(x^{-1}) + \cdots + u_6(x)v_6(x^{-1}) = 0.$$

Since $e_1(x^{-1}) = e_2(x)$ and $e_1(x)e_2(x) = 0$, M_2 determines the whole code C_φ. The substitution $x \to x^3$ in $\varphi(E_\sigma(C)^*)$ interchanges M_1 and M_2 and therefore we may assume that $\dim_{I_1} M_1 \geqslant \dim_{I_2} M_2$. We have two cases, $\dim_{I_2} M_2 = 2$ and $\dim_{I_2} M_2 = 3$. Each case does not produce a self-dual $[48, 24, 10]$ code with an automorphism of order 7 as follows.

Theorem 3.9. *(See [6].) There does not exist a self-dual* $[48, 24, 10]$ *code with an automorphism of order* 7.

According to Corollary 2.2, if the self-dual $[48, 24, 10]$ code C has an automorphism σ of order 5 then σ is of type 5-$(8, 8)$. Here we prove that this is not possible.

Let C have an automorphism σ of type 5-$(8, 8)$. Then C_φ is a self-dual $[8, 4]$ code over the field $\mathcal{P}$ with 16 elements under the inner product $(u, v) = u_1 v_1^4 + u_2 v_2^4 + \cdots + u_8 v_8^4$, $u, v \in C_\varphi$. There is one-to-one correspondence between the elements of the field $\mathcal{P}$ and the set of 5×5 circulants with rows of even weight defined by

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 \mapsto \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ a_4 & a_0 & a_1 & a_2 & a_3 \\ a_3 & a_4 & a_0 & a_1 & a_2 \\ a_2 & a_3 & a_4 & a_0 & a_1 \\ a_1 & a_2 & a_3 & a_4 & a_0 \end{pmatrix}.$$

Moreover, the rank of a nonzero circulant of this type is 4. Therefore, any nonzero vector $u \in C_\varphi$ corresponds to a subcode of $E_\sigma(C)^*$ of length 40 and dimension 4. Moreover, the effective length of this subcode is $5\mathrm{wt}(u)$. Since self-orthogonal $[15, 4, 10]$ and $[20, 4, 10]$ codes do not exist (see [5]), we have $\mathrm{wt}(u) \geqslant 5$. Hence C_φ must be an MDS $[8, 4, 5]$ Hermitian self-dual code over the field $\mathcal{P} \cong GF(16)$. Huffman proved in [13] that such codes do not exists. So a self-dual $[48, 24, 10]$ code with an automorphism of type 5-(8,8) does not exist.

Theorem 3.10. *(See [6].) A self-dual* $[48, 24, 10]$ *code* C *does not have automorphisms of order* 5.

Lemma 3.11. *(See [6].) A self-dual* $[48, 24, 10]$ *code with an automorphism of order* 3 *has weight enumerator* $W_{48,2}(y)$.

Putting together the above results, we have the following theorems.

Theorem 3.12. *(See [6].) If* C *is a singly-even self-dual* $[48, 24, 10]$ *code with weight enumerator* $W_{48,1}(y)$, *the automorphism group of* C *is of order* 2^s *with* $s \geqslant 0$.

Theorem 3.13. *(See [6].) If* C *is a self-dual singly-even* $[48, 24, 10]$ *code with weight enumerator* $W_{48,2}(y)$, *then the automorphism group of* C *is of order* $2^s 3^t$ *with* $s \geqslant 0$, $t \geqslant 0$.

Therefore, using Proposition 3.4, we summarize our result below.

Theorem 3.14. *If there is a self-dual* $[48, 24, 10]$ *code with an automorphism of type* p-(c, f) *with* p *being an odd prime, then* $p = 3$, $c = 16$, $f = 0$. *Moreover, there are exactly* 264 *inequivalent binary* $[48, 24, 10]$ *self-dual codes with an automorphism of odd prime order, which is in fact of type* 3-$(16, 0)$. *Hence there are exactly* 264 *inequivalent binary cubic self-dual* $[48, 24, 10]$ *codes.*

Acknowledgments

S. Bouyuklieva was partially supported by VTU Science Fund under Contract RD-642-01/26.07.2010. N. Yankov was partially supported by Shumen University under Project RD-05-274/15.03.2012.

J.-L. Kim was partially supported by the Project Completion Grant (year 2011–2012) at the University of Louisville, and also by Korea Institute for Advanced Study. We also thank the referees for their valuable comments.

References

[1] C. Aguilar-Melchor, P. Gaborit, J.-L. Kim, L. Sok, P. Solé, Classification of extremal and *s*-extremal binary self-dual codes of length 38, IEEE Trans. Inform. Theory 58 (2012) 2253–2262.
[2] K. Betsumiya, M. Harada, A. Munemasa, A complete classification of doubly even self-dual codes of length 40, arXiv:1104.3727v2, May 31, 2011, arXiv:1104.3727v1, April 19, 2011.
[3] A. Bonnecaze, A.D. Bracco, S.T. Dougherty, L.R. Nochefranca, P. Solé, Cubic self-dual binary codes, IEEE Trans. Inform. Theory 49 (9) (2003) 2253–2259.
[4] I. Bouyukliev, About the code equivalence, in: Advances in Coding Theory and Cryptology, Series on Coding Theory and Cryptology, vol. 3, World Scientific Publishing, Hackensack, NJ, 2007.
[5] I. Bouyukliev, S. Bouyuklieva, T. Aaron Gulliver, Patric Östergård, Classification of optimal binary self-orthogonal codes, J. Combin. Math. Combin. Comput. 59 (2006) 33–87.
[6] S. Bouyuklieva, On the automorphism group of the extremal singly-even self-dual codes of length 48, in: Proceedings of Twenty Sixth Spring Conference of the Union of Bulgarian Mathematicians, Bulgaria, 1997, pp. 99–103.
[7] S. Bouyuklieva, I. Bouyukliev, An algorithm for classification of binary self-dual codes, IEEE Trans. Inform. Theory 58 (2012) 3933–3940.
[8] R.A. Brualdi, V. Pless, Weight enumerators of self-dual codes, IEEE Trans. Inform. Theory 37 (1991) 1222–1225.
[9] J.H. Conway, V. Pless, N.J.A. Sloane, Self-dual codes over GF(3) and GF(4) of length not exceeding 16, IEEE Trans. Inform. Theory 25 (1979) 312–322.
[10] J.H. Conway, N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory 36 (1991) 1319–1333.
[11] S. Han, J.-L. Kim, H. Lee, Y. Lee, Construction of quasi-cyclic self-dual codes, Finite Fields Appl. 18 (2012) 613–633.
[12] M. Harada, M. Kitazume, A. Munemasa, B. Venkov, On some self-dualcodes and unimodular lattices in dimension 48, European J. Combin. 26 (2005) 543–557.
[13] W.C. Huffman, Automorphisms of codes with application to extremal doubly-even codes of length 48, IEEE Trans. Inform. Theory 28 (1982) 511–521.
[14] W.C. Huffman, On the classification and enumeration of self-dual codes, Finite Fields Appl. 11 (2005) 451–490.
[15] V. Pless, A classification of self-orthogonal codes over GF(2), Discrete Math. 3 (1972) 209–246.
[16] E.M. Rains, N.J.A. Sloane, Self-dual codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998, pp. 177–294.
[17] V.Y. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, IEEE Trans. Inform. Theory 33 (1987) 77–82.
[18] V. Yorgov, Binary self-dual codes with an automorphism of odd order, Probl. Inf. Transm. 4 (1983) 13–24.