ON THE AUTOMORPHISMS OF THE OPTIMAL SELF-DUAL CODE OF LENGTH 74*

Radka P. Russeva, Nikolay I. Yankov, Emine A. Karatash

ABSTRACT: *We investigate binary self-dual* $[74, 37, 14]$ *codes with an automorphism of type* $7-(10, 4)$ *and we obtain some results for the structure of its automorphism group G. Eventually we prove that 49 do not divide the order of G. We calculate the possible weight enumerators for self-dual* $[74, 37, 12]$ *codes and we construct examples of such codes for 292 different values of the parameters in these functions. All of these codes are not previously known to exist.*

KEYWORDS: *Automorphisms, Self-dual codes.*

1 Introduction

All possible weight enumerators for binary extremal or optimal self-dual codes are given in [8] for lengths up to 72 and for lengths up to 100 in [4]. The highest possible minimum weight for singly-even self-dual codes of lengths $70 \leq n \leq 78$ is 14. Dougherty, Gulliver and Harada in [4] proved that singly-even self-dual codes with $d = 14$ exist for even lengths $n \geq 78$. There is no known self-dual codes of length 74 with minimum distance neither 14 or 12 in the literature.

Let C be a putative self-dual $[74, 37, 14]$ code. It has been proved that if σ is an automorphism of C of an odd prime order then σ is of type $7-(10, 4), 3-(20, 14), 3-(22, 8)$ or $3-(24, 2)$ [2].

First we investigate binary self-dual $[74, 37, 14]$ codes having an automorphism of type $7-(10, 4)$. We didn't obtain such codes, but we construct 292 examples of self-dual $[74, 37, 12]$ codes. All of them are new codes not previously known to exist. We make use of the method for constructing self-dual codes via an automorphism of an odd prime order p developed by Huffman and Yorgov in ([6], [9], [10]). We start with a description of this method in Section 2. In Section 3, we apply the method for a self-dual $[74, 37, 14]$ code in the case $p = 7$. In Table 3, we give the automorphism groups and the weight enumerators of the $[74, 37, 12]$ codes we constructed that have either biggest or smallest values of the numbers of weight 12 vectors.

In Section 4, we consider the possibilities of the order of the automorphism group of a self-dual $[74, 37, 14]$ code and as a main result we prove that 49 does not divide it.

2 Construction method

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

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

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

Denote the cycles of σ by $\Omega_1, \dots, \Omega_c$, and the fixed points by $\Omega_{c+1}, \dots, \Omega_{c+f}$. Let

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

*This work is partially supported by a project No RD-08-103/05.02.2016 of Shumen University

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

Theorem 2.1 ([6]). *Assume C is a self-dual code. The code C is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$. $F_\sigma(C)$ and $E_\sigma(C)$ are subspaces of dimensions $\frac{c+f}{2}$ and $\frac{c(p-1)}{2}$, 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 $v_0+v_1x+\cdots+v_{p-1}x^{p-1}$ from $\mathcal{P}$, where $\mathcal{P}$ is the set of even-weight polynomials in the factor ring $\mathbb{F}_2[x]/\langle x^p-1\rangle$. Thus we obtain the map $\varphi : E_\sigma(C)^* \to \mathcal{P}^c$. $\mathcal{P}$ is a cyclic code of length p with generator polynomial $x-1$. It is known that $\varphi(E_\sigma(C)^*)$ is a submodule of the $\mathcal{P}$-module $\mathcal{P}^c$ [6], [9].

Theorem 2.2 ([9]). *A binary $[n, n/2]$ code C with an automorphism σ is self-dual if and only if the following two conditions hold:*

(i) $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual code of length $c+f$,

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

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

Let $x^p-1 = (x-1)h_1(x)h_2(x)\ldots h_s(x)$, where $h_1(x), h_2(x), \ldots, h_s(x)$ are irreducible binary polynomials. If $g_j(x) = (x^p-1)/h_j(x)$, and $I_j = \langle g_j(x)\rangle$ is the ideal in $\mathbb{F}_2[x]/\langle x^p-1\rangle$, generated by $g_j(x)$, then I_j is a field with $2^{deg(h_j(x))}$ elements, $j = 1, 2, \ldots, s$, and $\mathcal{P} = I_1 \oplus I_2 \oplus \cdots \oplus I_s$.

Lemma 2.3 ([9]). *Let $M_j = \{u \in \varphi(E_\sigma(C)^*) | u_i \in I_j, i = 1, 2, \ldots, c\}$, $j = 1, 2, \ldots, s$. Then*

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

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

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

To classify the codes that we have obtained we need additional conditions for equivalence. The following theorem is useful in that regard.

Theorem 2.4 ([10]). *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 cyclic shift to each p-cycle independently.*

3 Self-dual $[74, 37, 14]$ codes with an automorphism of type 7-$(10, 4)$

Binary doubly-even self-dual $[72, 36, 16]$ code with an automorphism of order 7 does not exist [5]. Let C be an optimal binary self-dual $[74, 37, 14]$ code. We assume that the code C has an automorphism σ of type $7-(10, 4)$.

By Theorem 2.2, the subcode C_π is a binary self-dual $[14, 7, \geq 2]$ code. There are four such codes ([7]): $7i_2$, $i_2 + d_{12}$, $3i_2 + h_8$ and $2e_7$, the latter is the only code with $d = 4$. Only for the codes $i_2 + d_{12}$ and $2e_7$ the coordinate positions can be split into two disjoined sets: the set of cyclic positions X_c, and X_f – the fixed positions, in such a way that $d(F_\sigma(C))$ is at least 14. We have found three arrangements: one from i_2+d_{12} and two from $2e_7$. The generator matrices for C_π are (the vertical line is dividing each matrix into: X_c – left hand side and the rest: X_f):

$$G_1 = \left(\begin{array}{c|c} 1000000100 & 0011 \\ 0100000100 & 1001 \\ 0010010100 & 0001 \\ 0001010000 & 1111 \\ 0000110100 & 1110 \\ 0000001100 & 0101 \\ 0000000011 & 0000 \end{array}\right), G_2 = \left(\begin{array}{c|c} 1000101000 & 1110 \\ 0100101000 & 0001 \\ 0010001000 & 1111 \\ 0001100000 & 1111 \\ 0000010001 & 0110 \\ 0000000101 & 1010 \\ 0000000011 & 1100 \end{array}\right), G_3 = \left(\begin{array}{c|c} 1000100001 & 1110 \\ 0100100000 & 1001 \\ 0010000001 & 1111 \\ 0001100001 & 0111 \\ 0000010010 & 0110 \\ 0000001011 & 0010 \\ 0000000111 & 0100 \end{array}\right).$$

Denote $h_1(x) = x^3+x+1$ and $h_2(x) = x^3+x^2+1$. As $x^7-1 = (x-1)h_1(x)h_2(x)$, we have $\mathcal{P} = I_1 \oplus I_2$, where I_j is the irreducible cyclic code of length 7 with parity-check polynomial $h_j(x)$, $j = 1, 2$. According to Lemma 2.3, $C_\varphi = M_1 \oplus M_2$, where $M_j = \{u \in C_\varphi \mid u_i \in I_j, i = 1, \ldots, c\}$ is a linear code over the field I_j, $j = 1, 2$, and $\dim_{I_1} M_1 + \dim_{I_2} M_2 = c$. The idempotents $e_1 = x^4 + x^2 + x + 1$ and $e_2 = x^6 + x^5 + x^3 + 1$ generate the ideals I_1 and I_2 defined above. The transformation $x \to x^{-1}$ interchanges e_1 and e_2. The orthogonal condition (1) implies that once chosen, M_1 determines M_2 and the whole C_φ.

Using Lemma 2.3, we have that $C_\varphi = M_1 \oplus M_2$ and $M_i = \{u \in C_\varphi \mid u_j \in I_i, j = 1, \ldots 10\}$, $i = 1, 2$ is a linear code.

Lemma 3.1. *The minimum distance of the code $C_\varphi = \varphi(E_\sigma(C)^*)$ is at least 4.*

Proof: Any nonzero element of $I_j = \{0, e_j, xe_, \ldots, x^6 e_j\}$, $j = 1, 2$ generates a binary cyclic $[7, 3, 4]$ code. Using [7, Theorem 1.4.8] we can also conclude that when $p = 7$ the subcode $E_\sigma(C)^*$ is doubly-even. Applying $d(C) = 14$, the implication is that $d(E_\sigma(C)^*) \geq 16$ which leads to $d(C_\varphi) \geq 4$. □

Denoting $\dim_{I_j}(M_j) = k_j$, $j = 1, 2$ we have that $k_1 \leq k_2$ and $k_1 + k_2 = c = 10$. Using Lemma 3.1 and the Singleton's bound $d \leq n - k_i + 1$ we have $4 \leq 10 - k_i + 1$ leading to $k_i \leq 7$ therefore the possible values of the couple (k_1, k_2) are $(3, 7)$, $(4, 6)$, and $(5, 5)$. Since all nonzero elements in I_1 are cyclic shifts of e_1 when constructing the generator matrix G of M_1 we can assume that the first nonzero element in every column of G is e_1 (because we can use (iv) from Theorem 2.4).

When $k_1 = 3$, $k_2 = 7$ there is a unique MDS code with generator matrix

$$\text{gen } M_1 = \left(\begin{array}{c|ccccccc} & e_1 & e_1 & e_1 & e_1 & e_1 & e_1 & e_1 \\ I_3 & e_1 & xe_1 & x^2e_1 & x^3e_1 & x^4e_1 & x^5e_1 & x^6e_1 \\ & e_1 & x^2e_1 & x^4e_1 & x^6e_1 & xe_1 & x^3e_1 & x^5e_1 \end{array}\right).$$

When $k_1 = 4$, $k_2 = 6$ we have considered the case of

$$\text{gen } M_1 = \left(\begin{array}{c|cccccc} & e_1 & e_1 & e_1 & e_1 & e_1 & e_1 \\ I_4 & e_1 & x^{i_1}e_1 & x^{i_2}e_1 & x^{i_3}e_1 & x^{i_4}e_1 & x^{i_5}e_1 \\ & e_1 & x^{i_6}e_1 & * & * & * & * \\ & e_1 & x^{i_7}e_1 & * & * & * & * \end{array}\right),$$

Table. 1: Number of codes with $|\mathrm{Aut}(E_\sigma^*)|$ obtained for $E_\sigma^* = \varphi^{-1}(G_2)$

$\lvert\mathrm{Aut}(E_\sigma^*)\rvert$	7	14	21	28	42	63	126	147	441	1176
Frequency	6621	105	26	4	7	1	2	1	1	1

Table. 2: Number of codes with $|\mathrm{Aut}(E_\sigma^*)|$ obtained for $E_\sigma^* = \varphi^{-1}(G_3)$

$\lvert\mathrm{Aut}(E_\sigma^*)\rvert$	7	14	21	28	42	56	70	84	126	168	2352
Frequency	56893	964	28	4	3	2	2	1	1	1	1

where $1 \le i_1 < i_j$, $j = 2, \dots, 6$, $i_6 < i_7$ and $*$ denotes an arbitrary element in I_1. We have found 6769 inequivalent codes $E_\sigma^*(C)$ with $A_{16} = 9177 + 7l$, where

$$l \in \{1, 5, 6, \dots, 101, 102, 104, 106, 107, 108, 109, 111, 112, 113, 117, 118, 119, 125, 155, 686\}.$$

Denote the generator matrices of these codes with $H_{3,i}, i = 1, \dots, 6769$. The order of the automorphism groups of these codes are listed in Table 1.

When $k_1 = k_2 = 5$ we have calculated all codes with a generator matrix

$$\mathrm{gen}\ M_1 = \left(\begin{array}{c|ccccc} & e_1 & e_1 & e_1 & e_1 & e_1 \\ & e_1 & x^{i_1}e_1 & x^{i_2}e_1 & x^{i_3}e_1 & x^{i_4}e_1 \\ I_5 & e_1 & x^{i_5}e_1 & a & a & a \\ & e_1 & x^{i_6}e_1 & a & a & a \\ & e_1 & x^{i_7}e_1 & a & a & a \end{array} \right),$$

where $1 \le i_1 < i_j$, $j = 2, \dots, 5$, $i_5 < i_6 < i_7$ and a denotes an arbitrary element in I_1^*. There are a total of 57900 inequivalent codes with $A_{16} = 9177 + 7l$, where

$$l \in \{0, 4, \dots, 115, 117, 118, 122, \dots, 125, 127, 128, 132, 134, 138, 140, 156, 158, 195, 224, 686\}.$$

Denote the generator matrices of these codes with $H_{4,i}, i = 1, \dots, 57900$. We summarize our results on the automorphism groups in Table 2.

We do not obtain $[74, 37, 14]$ codes, but we have constructed 292 examples of self-dual $[74, 37, 12]$ codes. All of them are new not previously known to exist. First we calculate the possible weight enumerators for a self-dual $[74, 37, 12]$ codes. They depend of two integer parameters α and β and are the following:

$$W_{74,12,1}(y) = 1 + (\alpha - 1295)y^{12} + (5069 + \alpha + 32\beta)y^{14} + (116143 - 12\alpha - 160\beta)y^{16} + \dots$$
$$W_{74,12,2}(y) = 1 + (\alpha - 1295)y^{12} + (5069 + \alpha + 32\beta)y^{14} + (153007 - 12\alpha - 160\beta)y^{16} + \dots$$

We have calculated the weight enumerators for a very small portion of all self-dual $[74, 37, 12]$ codes we can construct and all of them are with different values of the parameters α and β. The following is a summary of the results we have obtained.

I. When $C_\pi = G_1$ we have self-dual $[74, 37, 12]$ codes with weight enumerator $W_{74,12,1}(y)$ for different values of the parameters α, β :

- ♦ $\beta = 0$, $\alpha \in \{1379 + 7l \mid l \in -5, 0, 2, \dots, 44, 47, 48\}$;

Table. 3: The codes with minimum and maximum A_{12}

C_π	$W_{74,12,i}$	A_{12}	α	β	$\lvert\mathrm{Aut}(C)\rvert$
G_1	1	49	1344	0	7
G_1	1	539	1834	-7	7
G_2	2	154	1449	-135	7
G_2	2	868	2163	-135	7
G_3	1	49	1344	-2	7
G_3	1	560	1855	-9	7

- $\beta = -7$, $\alpha \in \{1428 + 7l \mid l \in 0, \dots, 39, 40, 42, 58\}$;
- $\beta = -14$, $\alpha \in \{1477 + 7l \mid l \in 0, 2, 3, 4, 6, \dots, 31\}$.

II. When $C_\pi = G_2$ we have codes with weight enumerator $W_{74,12,2}(y)$, where $\beta = -135$ and α = 1449, 1470, 1491, 1512, 1533, 1554, 1575, 1596, 1617, 1638, 1659, 1680, 1701, 1722, 1743, 1764, 1785, 1806, 1827, 1848, 1869, 1890, 1911, 1932, 1953, 1974, 1995, 2016, 2037, 2058, 2079, 2100, 2121, 2142, and 2163.

III. When $C_\pi = G_3$ we have codes with weight enumerator $W_{74,12,1}(y)$ for α, β :

- $\beta = -2$, $\alpha \in \{1344 + 7l \mid l \in 0, 6, \dots, 53\}$;
- $\beta = -9$, $\alpha \in \{1421 + 7l \mid l \in 0, 2, \dots, 49, 51, 62\}$;
- $\beta = -16$, $\alpha \in \{1477 + 7l \mid l \in 0, 3, \dots, 34, 36, 38, 42\}$;
- $\beta = -23$, α = 1561, 1680, and 1701.

Lastly, we present in Table 3 the automorphism groups and the weight enumerators of the $[74, 37, 12]$ codes we constructed that have either biggest or smallest values of A_{12} in all three cases G_1, G_2, and G_3.

4 Self-dual $[74, 37, 14]$ Codes with an Automorphism of Odd Composite Order

The decomposition of a binary self-dual code having an automorphism of odd order was investigated at first by Dontcheva, van Zanten and Dodunekov in [3].

Let C be a self-dual $[74, 37, 14]$ code possessing an automorphism of odd composite order s. Since 3 and 7 are the only odd prime divisors of the order of the automorphism group of C, $s = 3^\alpha 7^\beta$, where $\alpha = 0, 1, 2, 3$ and $\beta = 0, 1, 2$.

Suppose that the code C has an automorphism σ of order 9 with t_9 cycles of order 9, t_3 cycles of order 3 and f fixed points in its decomposition, where $74 = 9t_9 + 3t_3 + f$. We will say that σ is of type $9-(t_9, t_3, f)$. Then σ^3 is an automorphism of C of order 3 with $3t_9$ cycles and $3t_3 + f$ fixed points. It is proved in [2] that any automorphism of order 3 of C is of type $3-(20, 14), 3-(22, 8)$ or $3-(24, 2)$. So it follows that $3t_9 \in \{20, 22, 24\}$ and therefore the only possible type for an automorphism of order 9 is $9-(8, 0, 2)$.

Now, assume that the code C has an automorphism σ of order 27 with t_{27} cycles of order 27, t_9 cycles of order 9, t_3 cycles of order 3 and f fixed points, where $74 = 27t_{27} + 9t_9 + 3t_3 + f$.

Then the permutations σ^3 of order 9 is an automorphism of C of type $9-(3t_{27}, 3t_9, 3t_3+f)$. Hence $3t_{27}=8$ which is impossible. Therefore, C does not have an automorphism of order 27.

Let σ be an automorphism of C of order 21 with t_{21} cycles of order 21, t_7 cycles of order 7, t_3 cycles of order 3 and f fixed points, where $74 = 21t_{21}+7t_7+3t_3+f$. Denote that σ is of type $21-(t_{21}, t_7, t_3, f)$. Then σ^3 is of order 7 with $3t_{21}+t_7$ cycles and $3t_3+f$ fixed points. Since the automorphisms of order 7 should be of type $7-(10,4)$, it follows that $3t_{21}+t_7=10$ and $3t_3+f=4$. Similarly σ^7 is of order 3 with $7t_{21}+t_3$ cycles and $7t_7+f$ fixed points. Hence $7t_{21}+t_3 \in \{20,22,24\}$ and $7t_7+f \in \{14,8,2\}$. Then it appears that the only possible automorphism of order 21 is of type $21-(3,1,1,1)$.

If σ is an automorphism of order 49 with t_{49} cycles of order 49, t_7 cycles of order 7 and f fixed points, then σ^7 is of order 7 with $7t_{49}$ cycles and $7t_7+f$ fixed points. Hence $7t_{49}=10$ – a contradiction. Therefore, the code C does not have an automorphism of order 49.

Remark. In [1] Bouyuklieva proved that 49 does not divide the order of the automorphism group of a doubly-even $[72,36,16]$ code. In a similar way we can prove the analogous result for a putative self-dual $[74,37,14]$ code.

Theorem 4.1. *Let C be a self-dual $[74,37,14]$ code. 49 does not divide the order of $Aut(C)$.*

Proof: Assume that 49 divides the order of $Aut(C)$. According to Sylow's theorem, there exists a subgroup $H < Aut(C)$ of order 49 and it is Abelian group. As we prowed above there is not an element of order 49 in $Aut(C)$, then H can not be a cyclic group. Hence H is a direct product of two cyclic groups of order 7.

Let $H=\langle\sigma\rangle\langle\tau\rangle$, $\langle\sigma\rangle\cap\langle\tau\rangle = id$, and $\sigma\tau=\tau\sigma$, where σ and τ are automorphisms of C of order 7. Without loss of generality we may assume that

$$\sigma = (1,2,\ldots,7)(8,9,\ldots,14)\ldots(64,65,\ldots,70)(71)(72)(73)(74).$$

Thus,

$$\sigma = \tau^{-1}\sigma\tau = (1\tau, 2\tau, \ldots, 7\tau)\ldots(64\tau, 65\tau, \ldots, 70\tau)(71\tau)(72\tau)(73\tau)(74\tau)$$

It follows that τ fixes the coordinates 71, 72, 73 and 74, too and the group $\langle\tau\rangle$ acts on the set of the cycles $\{\Omega_1, \Omega_2 \ldots, \Omega_{10}\}$. The length of each orbit is a divisor of 7. Hence, τ fixes at least 3 cycles. Let $\tau(\Omega_1)=\Omega_1$. If $\tau(1)=1$ then τ fixes more then four points, which is not impossible. Hence $\tau(1)=j, 1<j\leq 7$ and $\tau(\Omega_1)=\sigma^{j-1}(\Omega_1)$. Therefore $\tau^{-1}\sigma^{j-1}$ fixes the points $1,2,\ldots,7$ and is an automorphism of order 7 in $Aut(C)$ which is a contradiction. □

The following theorem summarizes the results of this section.

Theorem 4.2. *Let C be a self-dual $[74,37,14]$ code. The order of its automorphism group is $2^k.3^l$, or $2^k.3^l.7$ where $k,l\geq 0$.*

ACKNOWLEDGMENTS. The authors are grateful to Stefka Bouyuklieva for pointing out the problem of examination of self-dual $[74,37,14]$ codes.

References

1. St. Bouyuklieva, *On the Automorphism Group of a Doubly-Even (72,36,16) Code,* IEEE Trans. Inform. Theory, vol. 50, no. 3, pp. 544–547, 2004.

2. St. Bouyuklieva, R. Russeva, E. Karatash, *Notes on binary optimal self-dual* $[74, 37, 14]$ *codes*, Сборник с доклади от Юбилейна международна научна конференция „25 години факултет Математика и информатика" на ВТУ, с. 86–90, Издателство „Фабер", ISBN 978–619–00–0419–6, 2015.
3. R.A. Dontcheva, A.J.van Zanten, St.M. Dodunekov, *Binary Self-Dual Codes With Automorphisms of Composite Order,* IEEE Trans. Inform. Theory, vol. 50, no. 2, pp. 311–318, 2004.
4. S. T. Dougherty, T.A. Gulliver, M. Harada, *Extremal binary self-dual codes,* IEEE Trans. Inform. Theory, vol. 43, no. 6, pp. 2036–2047, 1997.
5. T. Feulner, G. Nebe, *The automorphism group of an extremal* $[72, 36, 16]$ *code does not contain* Z_7, $Z_3 \times Z_3$, *or* D_{10}, IEEE Trans. Inform. Theory, vol. 58(11), pp. 6916–6924, 2012.
6. W.C. Huffman, *Automorphisms of codes with application to extremal doubly-even codes of lenght 48,* IEEE Trans. Inform. Theory vol. 28, pp. 511–521, 1982.
7. W.C. Huffman and V.S. Pless, *Fundamentals of Error-Correcting Codes,* Cambridge University Press, 2003.
8. W.C. Huffman, *On the classification and enumeration of self-dual codes,* Finite Fields and Their Applications, vol. 11, no. 3, pp. 451–490, 2005.
9. V. Yorgov, *Binary Self-Dual Codes with Automorphisms of Odd Order,* Probl. Inf. Transm., vol. 19 (4), pp. 260–270, 1983.
10. V. Yorgov, *A method for constructing inequivalent self-dual codes with applications to length 56,* IEEE Trans. Inf. Theory, vol. 33(1), pp. 77–82, 1987.