Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 32-37*

On the classification of binary self-dual [44,22,8] codes with an automorphism of order 3[1]

Stefka Bouyuklieva stefka@uni-vt.bg
Veliko Tarnovo University, 5000 Veliko Tarnovo, BULGARIA
Radka Russeva, Nikolay Yankov, Nikola Ziapkov, Milena Nikolova
Faculty of Mathematics and Informatics, Shumen University,
Shumen 9712, BULGARIA

Abstract. All binary self-dual $[44, 22, 8]$ codes with an automorphism of order 3 with 8, 10, and 12 independent cycles are classified up to equivalence. There exist exactly 4570 inequivalent codes with automorphism of order 3 with 8 independent cycles, 8738 inequivalent such codes with 10 cycles, and 123147 inequivalent codes with 12 cycles.

1 Introduction

In this paper, we consider optimal binary self-dual [44,22,8] codes. The codes having automorphisms of prime orders $p \geq 5$ are classified in [13], [14], [10], [3], and [2]. That's why we focus on the automorphisms of order 3, and we complete the classification of [44,22,8] SD codes having an automorphism of prime odd order. The codes with automorphisms of order 3 with 6 independent 3-cycles are considered in [3]. We continue with the next possibilities for the number of cycles – 8, 10, and 12. The case of 14 cycles is solved in [11]. To do that we apply the method developed by Huffman and Yorgov (see [7], [12]).

2 Construction Method

Let C be a binary self-dual code of length $n = 44$ with an automorphism σ of order 3 with exactly c independent 3-cycles and $f = 44 - 3c$ fixed points in its decomposition. We may assume that

$$\sigma = (1, 2, 3)(4, 5, 6) \cdots (3c - 2, 3c - 1, 3c), \tag{1}$$

and shortly say that σ is of type $3 - (c, f)$.

Denote the cycles of σ by $\Omega_1, \dots, \Omega_c$, and the fixed points by $\Omega_{c+1}, \dots, \Omega_{c+f}$. Let $F_\sigma(C)=\{v \in C \mid v\sigma = v\}$ and $E_\sigma(C)=\{v \in C \mid \mathrm{wt}(v|\Omega_i) \equiv 0(mod\ 2), i = 1, \cdots, c+f\}$, where $v|\Omega_i$ is the restriction of v on Ω_i. Then $C = F_\sigma(C) \oplus E_\sigma(C)$.

We have that $v \in F_\sigma(C)$ iff $v \in C$ and v is constant on each cycle. Let $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$ be the projection map where if $v \in F_\sigma(C)$, $(v\pi)_i = v_j$ for some $j \in \Omega_i, i = 1, 2, \dots, c+f$. It is known that $\pi(F_\sigma(C))$ is a binary self-dual code of length $c+f$ [7].

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 $3c$. For v in $E_\sigma(C)^*$ we let $v|\Omega_i = (v_0, v_1, v_2)$ correspond to the polynomial $v_0 + v_1x + v_2x^2$ from P, where P is the set of even-weight polynomials in $\mathbb{F}_2[x]/(x^3+1)$. In our case $P = \{0, e = x+x^2, w = 1+x^2, w^2 = 1+x\} \cong \mathbb{F}_4$ where e is the identity of P and $\mathbb{F}_4$ is the Galois field of 4 elements. Thus we obtain the map $\varphi : E_\sigma(C)^* \to P^c$.

Theorem 1 *[7] The binary code C with an automorphism σ defined in (1) is self-dual iff the following two conditions hold:*

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

(ii) $\varphi(E_\sigma(C)^*)$ is a self-dual code of length c over the field P under the inner product $(u, v) = \sum_{i=1}^n u_i v_i^2$.

So we have that $\varphi(E_\sigma(C)^*)$ is a Hermitian quaternary self-dual code of length c. Since the minimum distance of $E_\sigma(C)$ is at least 8, this Hermitian code should have minimum distance at least 4.

Let $\mathcal{B}$, respectively $\mathcal{D}$, be the largest subcode of $C_\pi = \pi(F_\sigma(C))$ whose support is contained entirely in the left c, respectively, right f, coordinates. Suppose $\mathcal{B}$ and $\mathcal{D}$ have dimensions k_1 and k_2, respectively. Let $k_3 = k - k_1 - k_2$. Then there exists a generator matrix for C_π in the form

$$G_\pi = \begin{pmatrix} B & O \\ O & D \\ E & F \end{pmatrix} \tag{2}$$

where B is a $k_1 \times c$ matrix with $gen(\mathcal{B}) = [B\ O]$, D is a $k_2 \times f$ matrix with $gen(\mathcal{D}) = [O\ D]$, O is the appropriate size zero matrix, and $[E\ F]$ is a $k_3 \times n$ matrix. Let $\mathcal{B}^*$ be the code of length c generated by B, $\mathcal{B}_E$ the code of length c generated by the rows of B and E, $\mathcal{D}^*$ the code of length f generated by D, and $\mathcal{D}_F$ the code of length f generated by the rows of D and F. Then $k_3 = rank(E) = rank(F)$, $k_2 = k + k_1 - c = \frac{c+f}{2} + k_1$, $\mathcal{B}_E^\perp = \mathcal{B}^*$ and $\mathcal{D}_F^\perp = \mathcal{D}^*$.

3 Optimal Self-Dual Codes of Length 44 with an automorphism of order 3

The weight enumerators of the self-dual codes of length 44 are known [6]:

$$W_{44,1}(y) = 1 + (44 + 4\beta)y^8 + (976 - 8\beta)y^{10} + (12289 - 20\beta)y^{12} + \dots \quad (3)$$

for $10 \le \beta \le 122$ and

$$W_{44,2}(y) = 1 + (44 + 4\beta)y^8 + (1232 - 8\beta)y^{10} + (10241 - 20\beta)y^{12} + \dots \quad (4)$$

for $0 \le \beta \le 154$.

Self-dual codes with a weight enumerator $W_{44,1}$ for $\beta = 10, \dots,$ 68, 70, 72, 74, 82, 86, 90, 122 and $W_{44,2}$ for $\beta = 0, \dots,$ 56, $58, \dots, 62$, 64, 66, 68, 70, 72, 74, 76, 82, 86, 90, 104, 154 are known (see [8]).

3.1 Codes with an automorphism of type $3-(8,20)$

Up to equivalence, a unique Hermitian quaternary [8,4,4] code exists (see [9]). So we have unique up to equivalence subcode $E_\sigma(C)^*$. The code C_π is a binary self-dual $[28, 14, \ge 4]$ code with a generator matrix G_π given in (2) where B generates a $[8, k_1, \ge 4]$, and D generates a $[20, k_1 + 6, \ge 8]$ self-orthogonal code, respectively. Since $0 \le k_1 \le 4$, $\mathcal{D}^*$ is a binary self-orthogonal $[20, 6 \le k_2 \le 10, \ge 8]$ code. All optimal binary self-orthogonal codes of length 20 are classified in [3]. There are exactly 23 inequivalent [20,6,8], four inequivalent [20,7,8], and a unique $[20, 8, 8]$ self-orthogonal codes. Hence $k_1 \le 2$.

In the case $k_1 = 2$ we obtain only two inequivalent optimal codes of length 44, both with weight enumerator $W_{44,2}$, respectively for $\beta = 68$ and $\beta = 76$. For $k_1 = 1$, there exist 31 self-dual [44,22,8] codes - four of them with weight function $W_{44,1}$ for $\beta =$ 42, 44, 46, 50, and the other 27 with $W_{44,2}$ for $\beta = 2s$, $s = 14, 16, \dots, 23, 25, 26$. When $k_1 = 0$, the obtained inequivalent codes are 4537. Their weight enumerators are of both types with $\beta \le 46$.

3.2 Codes with an automorphism of type $3-(10,14)$

In this case $\varphi(E_\sigma(C)^*)$ is a Hermitian self-dual $[10, 5, 4]$ code and by [9] is equivalent to either E_{10} or B_{10}. Then we can fix the generator matrix of the subcode $E_\sigma(C)^*$ in two forms.

The code C_π is a binary self-dual $[24, 12, \ge 4]$. There are exactly thirty inequivalent such codes, namely E_8^3, $E_{16} \oplus E_8$, $F_{16} \oplus E_8$, E_{12}^2 and 26 indecomposable codes denoted by $A_{24}, B_{24} \dots Z_{24}$ in [5]. The Golay code G_{24} and Z_{24}

have minimum weights 8 and 6 and all other codes have minimum weight 4. For any 4-weight vector in C_π at most 2 nonzero coordinates may be fixed points. An examination of the vectors of weight 4 in the listed codes eliminates 23 of them. By investigation of all alternatives for a choice of the 3-cycle coordinates in the rest codes G_{24}, R_{24}, U_{24}, W_{24}, X_{24}, Y_{24} and Z_{24} we obtain, up to equivalence, all possibilities for the generator matrix of the code C_π.

Denote by G_π the generator matrix of the code C_π. Let τ be a permutation of the ten cycle coordinates in G_π and let C^τ be the self-dual [44,22] code determined by $\varphi(E_\sigma(C)^*)$ and the matrix $\tau(G_\pi)$. The following transformations preserve the decomposition and send the code C to an equivalent one: (i) a permutation of the last 14 fixed coordinates; (ii) a permutation of the ten 3-cycles coordinates; (iii) a substitution $x \to x^2$ in $\varphi(E_\sigma(C)^*)$ and (iv) a cyclic shift to each 3-cycle independently.

We consider the products of transformations (ii), (iii) and (iv) which preserve the quaternary code $\varphi(E_\sigma(C)^*)$. Their permutational part forms a subgroup of the symmetric group S_{10} which we denote by L. Let $S = Stab(C_\pi)$ be the stabilizer of the automorphism group of the code generated by G_π on the set of the fixed points. It is easy to prove that if τ_1 and τ_2 are the permutations from the group S_{10} the codes C^{τ_1} and C^{τ_2} are equivalent iff the double cosets $S\tau_1 L$ and $S\tau_2 L$ coincide.

In this way from all the cases for C_π we constructed 1815 inequivalent $[44, 22, 8]$ self-dual codes with weight enumerator $W_{44,1}$ for $\beta = 10, \cdots, 52$, 54,55,60,62 and 6923 codes with weight enumerator $W_{44,2}$ for $\beta = 0, 2, \cdots, 16$, 18,21,24. The calculations for these results was done with the GAP Version 4 software system and the program Q-Extension [1].

3.3 Codes with an automorphism of type $3 - (12, 8)$

There exist exactly five inequivalent quaternary self-dual $[12, 6, 4]$ codes, denoted by d_{12}, $2d_6$, $3d_4$, $e_6 \oplus e_6$, and $e_7 + e_5$ [9].

The code C_π is $[20, 10, \geq 4]$ binary self-dual code. There are exactly seven such codes, namely $d_{12} + d_8$, $d_{12} + e_8$, d_{20}, d_4^5, $d_6^3 + f_2$, $d_8^2 + d_4$, and $e_7^2 + d_6$ [5]. The 13th, 14th, ..., and 20th coordinates correspond to the fixed points of C, so each choice for these fixed points can lead to different subcode C_π. We have considered all possibilities for each of these seven codes and we found exactly 7 inequivalent codes for $d_{12} + d_8$, one code for $d_{12} + e_8$, one code for d_{20}, 10 codes for d_4^5, 26 codes for $d_6^3 + f_2$, 18 codes for $d_8^2 + d_4$, and 3 codes for $e_7^2 + d_6$. Denote these codes by $H_{i,j}$, for $i = 1, 2 \ldots, 7$ and $j \geq 1$.

Using the method from Section 3.2, considering the transformations (ii), (iii) and (iv) (see Section 3.2) and the stabilizer of the automorphism group of the codes $H_{i,j}$ on the fixed points, we classified all codes up to equivalence. There are exactly 123147 inequivalent codes. Their weight enumerators are of type $W_{44,1}$ for $\beta = 10, \ldots, 68, 70, 72, 74, 82, 86, 90, 122$ and of type $W_{44,2}$ for $\beta = 0, \ldots, 56, 58, \ldots, 62, 64, 66, 68, 70, 72, 74, 76, 82, 86, 90, 104, 154$. The results are displayed in the Table below. The number of inequivalent codes in each case are written in the following manner: number of codes with weight enumerator $W_{44,1}$ (number of codes with weight enumerator $W_{44,2}$).

Table: $c = 12$

	$d_{12}+d_8$	$d_{12}+e_8$	d_{20}	d_4^5	$d_6^3+f_2$	$d_8^2+d_4$	$e_7^2+d_6$
d_{12}	11 (29)	3 (0)	0 (0)	431 (1894)	379 (1531)	103 (383)	34 (0)
$2d_6$	74 (416)	15 (0)	0 (6)	5760 (30678)	5099 (26962)	977 (5859)	357 (0)
$3d_4$	37 (203)	9 (0)	0 (4)	2375 (12627)	2042 (11759)	422 (2566)	148 (0)
$e_6 \oplus e_6$	3 (17)	1 (0)	0 (2)	30 (88)	45 (123)	18 (70)	6 (0)
e_7+e_5	16 (95)	3 (0)	0 (2)	710 (3304)	817 (3437)	201 (894)	72 (0)

References

[1] I. Bouyukliev, About the code equivalence, in *Adv. Coding Theory Cryptol.*, World Scientific Publishing, Hackensack, NJ, 2007.

[2] S. Buyuklieva, New extremal self-dual codes of lengths 42 and 44, *IEEE Trans. Inform. Theory* 43, 1997, 1607-1612.

[3] S. Bouyuklieva, Some optimal self-orthogonal and self-dual codes, *Discr. Math.* 287, 2004, 1-10.

[4] S. Bouyuklieva, N. Yankov, R. Russeva, Classification of the binary self-dual $[42, 21, 8]$ codes having an automorphism of order 3, *Fin. Fields Their Appl.* 13, 2007, 605-615.

[5] J. H. Conway, V. Pless, N. J. A. Sloane, The binary self-dual codes of length up to 32: a revised enumeration, *J. Combin. Theory* A-60, 1992, 183-195.

[6] 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.

[7] W. C. Huffman, Automorphisms of codes with application to extremal doubly-even codes of lenght 48, *IEEE Trans. Inform. Theory* 28, 1982, 511-521.

[8] W. C. Huffman, On the classification and enumeration of self-dual codes, *Fin. Fields Their Appl.* 11, 2005, 451-490.

[9] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, H. N. Ward, Self-dual codes over $GF(4)$, *J. Combin. Theory* A-25, 1978, 288-318.

[10] N. Yankov, R. Russeva, Classification of the binary self-dual [44,22,8] codes with automorphisms of order 7, *Proc.* 37^{th} *Spring Conf. Union Bulg. Math.*, 2008, 239-244.

[11] N. Yankov, Extremal self-dual [44,22,8] codes with automorphism of order 3 with 14 cycles, *Proc. Fifth Intern. Workshop OCRT*, Bulgaria, June 2007, 249-254.

[12] V. Y. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, *IEEE Trans. Inform. Theory* 33, 1987, 77-82.

[13] V. Y. Yorgov, New extremal singly-even self-dual codes of lenght 44, *Proc. Sixth Swedish-Russian Intern. Workshop Inform. Theory*, Molle, Sweden, 1993, 372-375.

[14] V. Yorgov, R. Russeva, Two extremal codes of length 42 and 44, *Probl. Pered. Inform.* 29, 1994, 385-388.