МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2008
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2008
Proceedings of the Thirty Seventh Spring Conference of
the Union of Bulgarian Mathematicians
Borovetz, April 2–6, 2008

CLASSIFICATION OF THE BINARY SELF-DUAL [44,22,8] CODES WITH AUTOMORPHISMS OF ORDER 7*

Nikolay Ivanov Yankov, Radka Peneva Russeva

All binary self-dual [44,22,8] codes with an automorphism of order 7 are classified up to equivalence. There are exactly three nonequivalent codes with automorphism of order 7 with 3 independent cycles, and 154 nonequivalent codes with automorphism of order 7 with 6 independent cycles.

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. 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 C, if $C = \sigma(C)$. The set of all automorphisms of C forms the *automorphism group* $Aut(C)$ of C. The *dual code* of C is $C^\perp = \{u \in \mathbb{F}_q^n \mid (u, v) = 0 \text{ for all } v \in C\}$ and $C^\perp$ is a linear $[n, n-k]$ code. If $C \subseteq C^\perp$, then C is termed *self-orthogonal*, and if $C = C^\perp$, then C is self-dual. If C *is self-dual*, then $k = \frac{1}{2}n$. We call a binary code *self-complementary* if it contains all the ones vector. Every binary self-dual code is self-complementary.

In this paper, we consider optimal binary self-dual $[44, 22, 8]$ codes. The self-dual codes with these parameters have been constructed as double circulant and bordered double circulant codes and via automorphisms [3]. All odd primes p dividing the order of the automorphism group of a self-dual $[44, 22, 8]$ code are 11, 7, 5, and 3. The codes with automorphism of order 11 and 5 are classified in [9], [10], [5], [4]. The codes with automorphisms of order 3 with 6 independent 3-cycles are classified in [5]. In this paper, we give a classification of the self-dual $[44, 22, 8]$ codes with an automorphism of order 7. To do that we apply the method developed by Huffman and Yorgov [2], [7].

2. Construction Method. Let C be a binary self-dual code of length $n = 44$ with an automorphism σ of order 7 with exactly c independent 7-cycles and $f = 44 - 7c$ fixed

*2000 Mathematics Subject Classification: 94B05.
Key words: Self-dual codes, automorphisms, optimal codes.
The research is partially supported by Shumen Univesity under Project No 8/2007.

points in its decomposition. We may assume that: $\sigma = (1, 2, \ldots, 7)(8, 9, \ldots, 14)\ldots(7(c-1)+1, 7(c-1)+2, \ldots, 7c)$, and say shortly that σ is of type $7-(c, f)$.

Theorem 1. *(see [8]) Let the self-dual code C have an automorphism of type $7-(c, f)$. If $\lceil x \rceil$ denotes the smallest integer not less than x, then one has:*

1) $7c \geq \sum_{i=0}^{3c-1} \left\lceil \frac{d}{2^i} \right\rceil$, *where the sign of equality does not occur if $d \leq 2^{3c-2} - 2$;*

2) *if $f > c$, then $c \geq \sum_{i=0}^{\frac{f-c}{2}-1} \left\lceil \frac{d}{2^i} \right\rceil$, where the sign of equality does not occur if $d \leq 2^{\frac{f-c}{2}-2} - 2$.*

Denote the cycles of σ by $\Omega_1, \Omega_2, \ldots, \Omega_c$, and the fixed points by $\Omega_{c+1}, \ldots, \Omega_{c+f}$. Let $F_\sigma(C)=\{v \in C \mid v\sigma = v\}$ and $E_\sigma(C)=\{v \in C \mid wt(v|\Omega_i) \equiv 0(mod\ 2), i = 1, \ldots, c+f\}$, where $v|\Omega_i$ is the restriction of v on Ω_i. Then, we have $C = F_\sigma(C) \oplus E_\sigma(C)$ (see [2]).

Clearly, $v \in F_\sigma(C)$ 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 $v \in F_\sigma(C)$, then $(v\pi)_i = v_j$ for some $j \in \Omega_i, i = 1, 2, \ldots, c+f$. It is well-known that $\pi(F_\sigma(C))$ is a binary $[c+f, \frac{c+f}{2}]$ self-dual code [2].

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 $7c$. For v in $E_\sigma(C)^*$, we let $v|\Omega_i = (v_0, v_1, \ldots, v_6)$ correspond to the polynomial $v_0 + v_1 x + v_6 x^6$ from P, where P is the set of even-weight polynomials in $\mathbb{F}_2[x]/(x^7 - 1)$. Thus, we obtain the map $\varphi : E_\sigma(C)^* \to P^c$. P is a cyclic code of length 7 with generating polynomial $x+1$ and check polynomial $1+x+\cdots+x^6$.

It is well-known [2], [8] that $\varphi(E_\sigma(C)^*)$ is a P-module and for each $u, v \in \varphi(E_\sigma(C)^*)$ it holds.

$$u_1(x)v_1(x^{-1}) + u_2(x)v_2(x^{-1}) + \cdots + u_c(x)v_c(x^{-1}) = 0. \tag{1}$$

Denote $h_1(x) = (x^3 + x + 1)$ and $h_2(x) = (x^3 + x^2 + 1)$. As $x^6 + x^5 + \cdots + x + 1 = h_1(x)h_2(x)$, we have $P = I_1 \oplus I_2$, where I_j is an irreducible cyclic code of length 7 with parity-check polynomial $h_j(x), j = 1, 2$. Thus, $M_j = \{u_i \in \varphi(E_\sigma(C)^*) \mid u_i \in I_j, i = 1, 2\}$ is code over the field $I_j, j = 1, 2$. It is well-known [8] that $\varphi(E_\sigma(C)^*) = M_1 \oplus M_2$ and $\dim_{I_1} M_1 + \dim_{I_2} M_2 = c$. The polynomials $e_1(x) = x^4 + x^2 + x + 1$ and $e_2(x) = x^6 + x^5 + x^3 + 1$ generate the ideals I_1 and I_2 defined above. Any nonzero element of $I_j = \{0, e_j, xe_j \ldots, x^6 e_j\}, j = 1, 2$ generates a binary cyclic $[7, 4, 3]$ code. Since the minimum weight of the code C is 8, every vector of $\varphi(E_\sigma(C)^*)$ must contain at least 2 nonzero coordinates.

The following result is a particular case of Theorem 3 from [7]:

Theorem 2. *Let the permutation σ be an automorphism of the self-dual codes C and C'. A sufficient condition for equivalence of C and C' is that C' can be obtained from C by application of a product of some of the following transformations:*

a) ubstitution $x \to x^t$ for $t = 1, 2, \ldots, 6$ in $\varphi(E_\sigma(C)^*)$;

b) multiplication of the j-th coordinate of $\varphi(E_\sigma(C)^*)$ by x^{t_j} where t_j is an integer, $0 \leq t_j \leq 6$, for $j = 1, 2, \ldots, c$;

c) permutation of the first c cycles of C;

d) permutation of the last f coordinates of C.

Since the transformation $x \to x^3$ from Theorem 2 a) interchange $e_1(x)$ into $e_2(x)$ and

vice versa then, without loss of generality, we can assume that $\dim M_1 \leq \dim M_2$. Once chosen, M_1 determines M_2 and the whole $\varphi(E_\sigma(C)^*)$. Thus, we can examine only M_1.

Let $\mathcal{B}$, respectively $\mathcal{D}$, be the largest subcode of $\pi(F_\sigma(C))$ 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 $\pi(F_\sigma(C))$ of the form

$$G_\pi = \begin{pmatrix} B & 0 \\ 0 & D \\ E & F \end{pmatrix}, \tag{2}$$

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, we have the following lemma:

Lemma 1. *With the notation of the previous paragraph:*
(i) $k_3 = \operatorname{rank}(E) = \operatorname{rank}(F)$,
(ii) $k_2 = k + k_1 - c = \dfrac{c+f}{2} + k_1$, *and*
(iii) $\mathcal{B}_E^\perp = \mathcal{B}^*$ *and* $\mathcal{D}_F^\perp = \mathcal{D}^*$.

3. Optimal Self-Dual Codes of Length 44 with automorphisms of order 7. The weight enumerators of self-dual codes of length 44 are known [1]:
$W_{44,1}(y) = 1 + (44 + 4\beta)y^8 + (976 - 8\beta)y^{10} + (12289 - 20\beta)y^{12} + \cdots$
for $10 \leq \beta \leq 122$ and
$W_{44,2}(y) = 1 + (44 + 4\beta)y^8 + (1232 - 8\beta)y^{10} + (10241 - 20\beta)y^{12} + \cdots$
for $10 \leq \beta \leq 154$.

Codes exist for $W_{44,1}$ when $\beta = 10, \ldots, 68, 70, 72, 74, 82, 86, 90, 122$ and for $W_{44,2}$ when $\beta = 0, \ldots, 56, 58, \ldots, 62, 64, 66, 68, 70, 72, 74, 76, 82, 86, 90, 104, 154$ (see [3]).

Theorem 3. *If C is a binary self-dual $[44, 22, 8]$ code having an automorphism σ of order 7, then σ is of type $7-(3,23)$ or $7-(6,2)$.*

Proof. If C is a binary self-dual $[44, 22, 8]$ code having an automorphism σ of order 7, then σ can be of type $7-(1,37)$, $7-(2,30)$, $7-(3,23)$, $7-(4,16)$, $7-(5,9)$, and $7-(6,2)$. Since $d = 8$, the cases $7-(1,37)$ and $7-(2,30)$ are impossible due to condition 1) of Theorem 1. The cases $7-(4,16)$ and $7-(5,9)$ are contradictions to the assertion 2) of the same Theorem. □

3.1. Codes with automorphism of type 7-(3,23). Let C be a binary self-dual $[44, 22, 8]$ code having an automorphism of type $7-(3,23)$. Then, the subcode $\pi(F_\sigma(C))$ is a binary $[26, 13, \geq 4]$ self-dual code, $\dim \varphi(E_\sigma(C)^*) = 3$, and we have $\dim M_1 + \dim M_2 = 3$. When $\dim M_2 = 3$, we have that $\varphi(E_\sigma(C)^*)$ is a $[3, 3, 1]$ code and this leads to a contradiction with the minimum weight 8 in C. When $\dim M_2 = 2$, we can choose the generator matrix in the form $gen(\varphi(E_\sigma(C)^*)) = \begin{pmatrix} e_2 & 0 & e_2 \\ 0 & e_2 & e_2 \\ e_1 & e_1 & e_1 \end{pmatrix}$. The subcode $\pi(F_\sigma(C))$ is a binary $[26, 13, \geq 4]$ self-dual code. According to Lemma 1, we can take its generator

matrix in the form $\left(\begin{array}{c|c} \overbrace{B}^{3} & \overbrace{0}^{23} \\ \hline 0 & D \\ \hline E & F \end{array}\right)$, where $k_1+k_2+k_3=13$, $k_2=k_1+10$. So we have two cases:

Case I: $k_1=1, k_2=11, k_3=1$. Then, $B=(110)$, *gen* $\pi(F_\sigma(C))=\left(\begin{array}{c|c} 110 & 0 \\ \hline 0 & D \\ \hline E & F \end{array}\right)$, where the matrix D generates a $[23,11,\geq 8]$ binary self-orthogonal code. Since C is self-complimentary, $E=(111)$, $F=(1\ldots1)$. All optimal $[23,11]$ binary self-orthogonal codes are classified in [6]. There is a unique such code – the doubly-even subcode of the Golay code with weight enumerator $W_{23,11}=1+506y^8+1288y^{12}+253y^{16}$. So we obtain one possible generator matrix for the code C and it has minimum weight 6.

Case II: $k_1=0, k_2=10, k_3=3$. *gen* $\pi(F_\sigma(C))=\left(\begin{array}{c|c} 0 & D \\ \hline E & F \end{array}\right)$, where the matrix D generates a $[23,10,\geq 8]$ binary self-orthogonal code. There are three such codes [6] – $A_{23,10,1}, A_{23,10,2}$, and $A_{23,10,3}$ with generator matrices of the form $G_{A_{23,10,i}}=(I_{10}|G^{(i)})$ and all are with minimum distance 8.

$$G^{(1)}=\begin{pmatrix} 1111111000000\\ 1111000111000\\ 1100110110100\\ 1010101101100\\ 1001011011100\\ 0110101110010\\ 1100011101010\\ 0101110011010\\ 0001111100110\\ 0101011110001 \end{pmatrix},\quad G^{(2)}=\begin{pmatrix} 1111111000000\\ 1111000111000\\ 1100110110100\\ 1010101101100\\ 1001011011100\\ 0110101110010\\ 1100011101010\\ 0101110011010\\ 1010011110001\\ 0110110101001 \end{pmatrix},\quad G^{(3)}=\begin{pmatrix} 1101001010110\\ 1100011101100\\ 1100110110010\\ 0110011011010\\ 0011001101110\\ 1011011110000\\ 0101101111000\\ 0010110111100\\ 1011100011010\\ 0101110001110 \end{pmatrix}.$$

Since $k_3=3$, the matrix $E=I_3$, and the matrix F is determined by the condition (iii) of Lemma 1. For each of the three codes there is a unique possibility for the matrix F, up to equivalence. In this way we obtain the codes $C_{44,i}, i=1,2,3$. Their weight distributions and order of automorphism group $|Aut(C)|$ are presented in Table 1. All of these codes have automorphism of order 5 and are well-known [4].

Table 1: All codes with automorphism of type $7-(3,23)$

Code	Weight Distibution	β	$\lvert Aut(C)\rvert$
$C_{44,1}$	$W_{44,1}$	122	$2^{15}\cdot 3^4\cdot 5^2\cdot 7^2=3251404800$
$C_{44,2}$	$W_{44,2}$	104	$2^{13}\cdot 3^4\cdot 5^2\cdot 7$
$C_{44,3}$	$W_{44,2}$	154	$2^{16}\cdot 3^4\cdot 5^2\cdot 7^2\cdot 11^2=786839961600$

Theorem 4. *There are exactly three nonequivalent binary* $[44,22,8]$ *codes having an automorphism of type* $7-(3,23)$.

3.2. Codes with automorphism of type 7-(6,2). Let C be a binary self-dual $[44,22,8]$ code having an automorphism of type $7-(6,2)$. $\pi(F_\sigma(C))$ is a binary $[8,4]$ self-dual code equivalent either to C_2^4 or H_8, generated by the matrices $G_1=(I_4|I_4)$ and $G_2=(I_4|A+I_4)$, where I_4 is the 4×4 identity matrix and A is the all-one 4×4

matrix. Then, $\dim \varphi(E_\sigma(C)^*) = 6$ and so $\dim M_1 + \dim M_2 = 6$. We have four cases: $\dim M_1 = 0, 1, 2$, and 3.

Case I: $\dim M_1 = 0$. Then, $\dim M_2 = 6$ and we can take for its generator matrix the 6×6 diagonal matrix $diag(e_2, e_2 \ldots, e_2)$. This matrix leads to vectors with weight 4 in C, witch is a contradiction to the minimum weight 8 in C.

Case II: $\dim M_1 = 1$. We have $gen(\varphi(M_1) = (e_1, e_1, e_1, e_1, e_1, e_1)$. If $\pi(F_\sigma(C)) \cong C_2^4$, then we have not obtained any optimal $[44, 22]$ codes. When $\pi(F_\sigma(C)) \cong H_8$, we found only one code with $W_{44,1}$ for $\beta = 38$ and $|Aut(C)| = 8064$.

Case III: $\dim M_1 = 2$. We can take $gen(M_1) = \begin{pmatrix} e_1 & 0 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ 0 & e_1 & \alpha_5 & \beta_1 & \beta_2 & \beta_3 \end{pmatrix}$, where $\alpha_i \in \{0, e_1\}, i = 1, \ldots, 5$, and $\beta_i \in I_1, i = 1, 2, 3$. Actually, after considering all such matrices, it turns out that there is only one possibility up to equivalence – $\begin{pmatrix} e_1 & 0 & e_1 & 0 & e_1 & e_1 \\ 0 & e_1 & 0 & e_1 & 0 & 0 \end{pmatrix}$. We fix the generator matrix of $\varphi(E_\sigma(C)^*)$ and consider all possibilities for $\pi(F_\sigma(C))$. For $\pi(F_\sigma(C)) \cong C_2^4$ we found one code with weight distribution $W_{44,2}$ for $\beta = 56$ and $|Aut(C)| = 2688 = 2^7 \cdot 3 \cdot 7$. When $\pi(F_\sigma(C)) \cong H_8$, we found one code with weight distribution $W_{44,1}$ for $\beta = 59$ and $|Aut(C)| = 43008 = 2^{11} \cdot 3 \cdot 7$.

Case IV: $\dim M_1 = \dim M_2 = 3$. We have $gen(M_1) = \begin{pmatrix} e_1 & 0 & 0 & \alpha_1 & \alpha_2 & \alpha_3 \\ 0 & e_1 & 0 & \alpha_4 & \beta_1 & \beta_2 \\ 0 & 0 & e_1 & \alpha_5 & \beta_3 & \beta_4 \end{pmatrix}$, where $\alpha_i \in \{0, e_1\}, i = 1, \ldots, 5$, and $\beta_i \in I_1, i = 1, 2, 3, 4$. There are 18 nonequivalent such codes with minimum weight $d \geq 8$. We can fix the generator matrix for $\varphi(E_\sigma(C)^*)$ and consider all possibilities for $\pi(F_\sigma(C))$:

– If $\pi(F_\sigma(C)) \cong H_8$, then we have 64 nonequivalent codes with $W_{44,1}$ for β =10, 17, 24, 31, 38, 52, 122. The orders of their automorphism groups are given in Table 2. The code with $\beta = 122$ is equivalent to the code $C_{44,1}$.

Table 2: Self-dual $[44, 22, 8]$ codes for $C_\pi \cong H_8$ and $\dim M_1 = 3$.

$\lvert Aut(C)\rvert$	7	14	28	42	56	84	112	126
Number of codes	11	29	4	6	1	1	1	1
$\lvert Aut(C)\rvert$	168	252	336	672	1344	5040	5376	$2^{15} \cdot 3^4 \cdot 5^2 \cdot 7^2$
Number of codes	1	1	2	2	1	1	1	1

– If $\pi(F_\sigma(C)) \cong C_2^4$, then we have 87 nonequivalent codes with $W_{44,2}$ for β =0, 7, 14, 21, 28, 35, 42, 56, 154. The orders of their automorphism groups are presented in Table 3. The code with $\beta = 154$ is equivalent to $C_{44,3}$.

Table 3: Self-dual $[44, 22, 8]$ codes for $C_\pi \cong C_2^4$ and $\dim M_1 = 3$.

$\lvert Aut(C)\rvert$	7	14	28	42	56	112	336
Number of codes	42	28	3	1	2	1	2
$\lvert Aut(C)\rvert$	672	1344	2688	10752	43008	$2^{16} \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11^2$	
Number of codes	1	2	1	1	2	1	

Theorem 5. *There are exactly* 155 *nonequivalent* $[44, 22, 8]$ *codes having an automorphism of order* 7.

REFERENCES

[1] 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.
[2] W. C. Huffman. Automorphisms of codes with application to extremal doubly-even codes of lenght 48, *IEEE Trans. Inform. Theory*, **28** (1982), 511–521.
[3] W. C. Huffman. On the classification and enumeration of self-dual codes, *Finite Fields and Their Applications*, **11** (2005), 451–490.
[4] St. Buyuklieva. New extremal self-dual codes of lengths 42 and 44, *IEEE Trans. Inform. Theory*, **43** (1997), 1607–1612.
[5] St. Buyuklieva. Some optimal self-orthogonal and self-dual codes, *Discrete Mathematics*, **287** (2004), 1–10.
[6] I. Bouyukliev, S. Bouyuklieva, T. A. Gulliver, P. R. J. Ostergard. Classification of optimal binary self-orthogonal codes up to length 24, *Journal of Combinatorial Mathematics and Combinatorial Computing*, **59** (2006), 33–87.
[7] V. Y. Yorgov. A method for constructing inequivalent self-dual codes with applications to length 56, *IEEE Trans. Inform. Theory*, **33** (1987), 77–82.
[8] V. Y. Yorgov. Binary self-dual codes with an automorphism of odd order, *Problems Inform.Transm.*, **4** (1983) 13–24 (in Russian).
[9] V. Y. Yorgov. New extremal singly-even self-dual codes of lenght 44, *Proceedings of the Sixth Joint Swedish-Russian International Workshop on Information Theory* (*Molle, Sweden*) (1993), 372–375.
[10] V. Yorgov, R. Russeva. Two extremal codes of length 42 and 44, *Probl. Pered. Inform.*, **29** (1994), 385–388.

University of Shumen
Faculty of Mathematics and Informatics
9700 Shumen, Bulgaria
e-mail: jankov_niki@yahoo.com; russeva@fmi.shu-bg.net

КЛАСИФИКАЦИЯ НА ДВОИЧНИТЕ САМОДУАЛНИ [44,22,8] КОДОВЕ, ПРИТЕЖАВАЩИ АВТОМОРФИЗЪМ ОТ РЕД 7

Николай Иванов Янков, Радка Пенева Русева

Класифицирани са всички нееквивалентни двоични самодуални [44, 22, 8] кодове, притежаващи автоморфизми от ред 7. Съществуват точно три нееквивалентни кода с автоморфизъм от ред 7 с три независими цикъла и 154 нееквивалентни кода с автоморфизъм от ред 7 с шест независими цикъла.