МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2015
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2015
Proceedings of the Forty Fourth Spring Conference
of the Union of Bulgarian Mathematicians
SOK "Kamchia", April 2–6, 2015

CLASSIFICATION OF BINARY SELF-DUAL [68, 34, 12] CODES WITH AN AUTOMORPHISM OF ORDER 11*

Nikolay Yankov, Milena Ivanova

We classify up to equivalence all optimal binary self-dual [68, 34, 12] codes having an automorphism of order 11 with 6 independent cycles and two fixed points. Using a method for constructing self-dual codes via an automorphism of odd prime order we prove that there are exactly 243789 inequivalent such codes. Our results show that there exist 8821 such codes with 21 different new values of the parameter in both possible weight enumerator.

1. Introduction. Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements. A linear $[n, k]_q$ *code* C is a k-dimensional subspace of $\mathbb{F}_q^n$. We call the codes *binary* if $q = 2$. The number of the nonzero coordinates of a vector in $\mathbb{F}_q^n$ is called its *weight*. An $[n, k, d]_q$ code is an $[n, k]_q$ linear code with minimum nonzero weight d.

Let $(u, v) = \sum_{i=1}^{n} u_i v_i \in \mathbb{F}_2$ for $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ be the inner product in $\mathbb{F}_2^n$. Then if C is a binary $[n, k]$ code, its *dual* $C^\perp = \{u \in \mathbb{F}_2^n \mid (u, v) = 0 \text{ for all } v \in C\}$ is a $[n, n-k]$ binary code. If $C \subseteq C^\perp$, the code C is termed *self-orthogonal*, in case of $C = C^\perp$, C is called *self-dual*.

Two binary codes are *equivalent* if one can be obtained from the other by a permutation of the coordinate positions. The permutation $\sigma \in S_n$ is an *automorphism* of C, if $C = \sigma(C)$. The set of all automorphisms of a code forms a group called *the automorphism group* Aut (C). If a code C have an automorphism σ of odd prime order p, where σ has c independent p-cycles and f fixed points, then σ is said to be of *type* p-(c, f).

Self-dual codes with an automorphism of odd prime order are an extensively studied subject. All such codes are classified up to length 50 [9]. In recent works [7], [5], [6] some self-dual codes with automorphisms of order $2^r p$ for primes $p = 5, 7$, and 11 were constructed using codes over rings $F_2 + uF_2$, $F_2 + uF_2 + u^2F_2$, $F_4 + uF_4$, and R_k.

We say that a code C of length n have an automorphism σ of *type* $p - (c, f)$ for a prime p if σ have exactly c independent p-cycles and $f = n - cp$ fixed points in its decomposition. Without loss of generality we may assume that

$$(1) \qquad \sigma = (1, 2, \cdots, p)(p+1, p+2, \cdots, 2p) \cdots (p(c-1)+1, p(c-1)+2, \cdots, pc).$$

In [13], [14] the self-dual codes with an automorphism of order 11 with four cycles are studied. There is a unique [44, 22, 8] code with an automorphism of type $11-(2, 22)$, and

*2010 Mathematics Subject Classification: 94B05.
Key words: self-dual codes, automorphisms, optimal codes.
This research is partially supported by Shumen University under Project No RD-08-234/12.03.2014.

11 codes with an automorphism of type $11-(4,0)$. Huffman in [4] presented a survey of the status of the classification of self-dual codes over $\mathbb{F}_2$. Also there [4, Table 2] the case of binary self-dual codes of lengths 68 with an automorphism of order 11 with 6 cycles is listed as open.

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 fixed points in its decomposition (1).

Denote the cycles of σ by $\Omega_1, \Omega_2, \dots, \Omega_c$, and the fixed points by $\Omega_{c+1}, \dots, \Omega_{c+f}$. Let $F_\sigma(C)=\{v \in C \mid v\sigma = v\}$ and $E_\sigma(C)=\{v \in C \mid wt(v|\Omega_i) \equiv 0 \pmod 2, i = 1, \cdots, c+f\}$, where $v|\Omega_i$ is the restriction of v on Ω_i.

Theorem 1 ([3])**.** *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.*

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 $v \in F_\sigma(C)$, $(v\pi)_i = v_j$ for some $j \in \Omega_i, i = 1, 2, \dots, c+f$.

Theorem 2 ([12])**.** *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 $u, v \in C_\varphi = \varphi(E_\sigma(C)^*)$ we have $\sum_{i=1}^{c} u_i(x)v_i(x^{-1}) = 0$.

Furthermore, if 2 is a primitive root modulo p then C_φ is a self-dual code of length c over the field $\mathcal{P} \cong \mathbb{F}_{2^{p-1}}$ under the inner product $(u, v) = \sum_{i=1}^{c} u_i v_i^{2^{(p-1)/2}}$.

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 pc. For v in $E_\sigma(C)^*$ we let $v|\Omega_i = (v_0, v_1, \cdots, v_{p-1})$ correspond to the polynomial $v_0 + v_1x + \cdots + v_{p-1}x^{p-1}$ from P, where P is the set of even-weight polynomials in $\mathbb{F}_2[x]/(x^p - 1)$. Thus we obtain the map $\varphi : E_\sigma(C)^* \to P^c$. P is a cyclic code of length p with generator polynomial $x + 1$ and check polynomial $1 + x + \cdots + x^{p-1}$.

It is known [3], [12] that $\varphi(E_\sigma(C)^*)$ is a P-module and for each $u, v \in \varphi(E_\sigma(C)^*)$ it holds that

$$u_1(x)v_1(x^{-1}) + u_2(x)v_2(x^{-1}) + \cdots + u_c(x)v_c(x^{-1}) = 0. \tag{2}$$

To classify the codes, we need additional conditions for equivalence. For that purpose we use the following theorem:

Theorem 3 ([11])**.** *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, $1 \le t \le p-1$;

b) multiplication of the jth coordinate of C_φ by x^{t_j} where t_j is an integer, $0 \le t_j \le p-1$, $j = 1, 2, \dots, c$;

c) permutation of the first c cycles of C;

d) permutation of the last f coordinates of C.

3. Hermitian [6, 3] codes over a $\mathbb{F}_{2^{10}}$. By Theorem 2 using that 2 is a primitive root modulo $p = 11$ we can conclude that the $\varphi(E_\sigma(C))$ is a Hermitian $[6, 3, \ge 3]$ self-dual code over $\mathcal{P} \cong \mathbb{F}_{2^{10}}$ under the inner product

$$(u,v) = \sum_{i=1}^{6} u_i v_i^{32}. \tag{3}$$

$\mathcal{P}$ has identity $e(x) = x + x^2 + \cdots + x^{10}$ and a primitive element $\alpha = x + x^3 + x^5 + x^8 + x^9 + x^{10}$. Let $\delta = \alpha^{11}$ be an element of $\mathcal{P}$ with multiplicative order 93. Then we can represent $\mathcal{P} \cong \mathbb{F}_{2^{10}} = \{0, x^i\delta^j | 0 \le i \le 10, 0 \le j \le 92\}$. We omit the proofs of the next two statements. For more information we refer the reader to [10].

Proposition 1. *Let C be a binary self-dual code with minimum distance $d = 12$, having an automorphism σ of order 11 with 6 cycles. Then (up to a transformation form Theorem 3) the generator matrix of the code $\varphi(E_\sigma(C))$ is in the form*

$$A = \begin{pmatrix} e & 0 & 0 & t_1 & t_2 & t_3 \\ 0 & e & 0 & t_4 & t_5 & t_6 \\ 0 & 0 & e & t_7 & t_8 & t_9 \end{pmatrix}, \tag{4}$$

where $t_i \in \{0, \delta^j, 0 \le j \le 92\}$, $i = 1, \ldots, 4, 7$, $t_j \in \mathcal{P}$, $j = 5, 6, 8, 9$.

Using the orthogonality condition (3) we computed all different cases for A. We summarize the final results in the following.

Theorem 4. *Up to equivalence there are 31611 subcodes E_σ over $\mathcal{P}$ such that $\varphi^{-1}(C_\varphi)$ generates a code with minimum distance 12.*

4. Binary self-dual [68, 34, 12] codes with an automorphism of type 11 − (6, 2). There are two possible weight enumerators for a $[68, 34, 12]$ binary self-dual code:

$$W_{68,1} = 1 + (442 + 4\beta)y^{12} + (10864 - 8\beta)y^{14} + \ldots,$$

and

$$W_{68,2} = 1 + (442 + 4\beta)y^{12} + (14960 - 8\beta - 256\gamma)y^{14} + \ldots,$$

where β and γ are integer parameters. Codes are know with both weight enumerators. For most recent information on the known values of β and γ we refer the reader to [7].

There are exactly two $[8, 4]$ binary self-dual codes $4i_2$ and e_8 [8]. Denote by $X_c \subset \{1, \ldots, 8\}$ – the coordinate positions in the two above codes that correspond to the 11-cycles of σ, and by $X_f \subset \{1, \ldots, 8\}$ – the fixed points. We have that $X_c \cap X_f = \emptyset$ and $X_c \cup X_f = \{1, \ldots, 8\}$.

In the case of $4i_2$ we cannot have the full support of any weight 2 vector in X_f therefore assuming the first 6 coordinates are cyclic we get only one matrix for C_π that is

$$G_1 = \left(\begin{array}{c|c} 101000 & 00 \\ 000110 & 00 \\ 000001 & 10 \\ 010000 & 01 \end{array}\right),$$

where the vertical line splits the cyclic coordinates in the left hand side and the fixed points in the right hand side. The automorphism group of the extended Hamming code e_8 is 3-transitive so we can choose any two coordinates for X_f thus we have a unique matrix

$$G_2 = \left(\begin{array}{c|c} 100001 & 11 \\ 010010 & 11 \\ 001011 & 01 \\ 000111 & 10 \end{array} \right).$$

Proposition 2. *There are exactly* 243789 *inequivalent binary* $[68, 34, 12]$ *self-dual codes having an automorphism of type* $11 - (6, 2)$.

4.1. $\boldsymbol{C_\pi = G_1}$***.*** All of the codes we have found are with $W_{68,2}, \gamma = 0$ for different values of β listed in Table 1. Note that the values $\beta = 11$, 22, 33, 143, 154, 165, 176, 187, 198, 209, 220, 231, 308, and 330 are new and are listed in bold font. Thus we constructed 5279 inequivalent codes with new values of (β, γ) in their weight enumerator.

Table 1. The parameters of $[68, 34, 12]$ codes when $C_\pi = G_1$ all with $W_{68,2}$

		|Aut (C)|							|Aut (C)|		
β	#	11	22	44	110	220	β	#	11	22	44
11	**22**	**20**	**2**				**143**	**1949**	**1687**	**262**	
22	**213**	**184**	**25**	**4**			**154**	**922**	**760**	**159**	**3**
33	**964**	**923**	**41**				**165**	**560**	**454**	**106**	
44	3100	2980	110	9	1		**176**	**347**	**249**	**91**	**7**
55	7276	7068	208				**187**	**154**	**125**	**29**	
66	12648	12223	415	10			**198**	**86**	**62**	**20**	**4**
77	16787	16329	458				**209**	**35**	**28**	**7**	
88	17598	16979	607	11		1	**220**	**17**	**6**	**9**	**2**
99	14870	14357	513				**231**	**8**	**6**	**2**	
110	11232	10606	614	12			**308**	**1**			**1**
121	7032	6591	441				**330**	**1**		**1**	
132	3899	3506	388	5							

4.2. $\boldsymbol{C_\pi = G_2}$***.*** We found codes all with $W_{68,1}$ for different values of β listed in Table 2. The values $\beta = 115$, 247, 280, 291, 313, 324 and 379 are new and are listed

Table 2. The parameters of $[68, 34, 12]$ codes when $C_\pi = G_2$ all with $W_{68,1}$

		|Aut (C)|								|Aut (C)|				
β	#	11	22	44	66	132	330	β	#	11	22	44	66	132
104	317	300	15		1		1	236	2715	2337	358	5	15	
115	**1738**	**1631**	**105**	**2**				**247**	**1476**	**1215**	**251**	**10**		
126	5412	5110	300	2				258	809	635	174			
137	11208	10657	532	7	12			269	414	284	120	3	7	
148	17023	16276	741	6				**280**	**198**	**144**	**54**			
159	21494	20570	904	20				**291**	**93**	**50**	**42**	**1**		
170	22012	21020	961	7	24			302	36	20	14		2	
181	19809	18678	1110	21				**313**	**19**	**6**	**12**	**1**		
192	15717	14797	910	10				**324**	**12**	**1**	**11**			
203	11487	10646	792	32	16	1		335	10		5	1	2	2
214	7425	6820	599	6				**379**	**6**		**5**	**1**		
225	4637	4151	467	19				401	1				1	

in bold. The codes with $|\text{Aut }(C)| = 66, 132$ and 330 are the bordered double circulant known from [2, Table 7]. Our results completely match Gulliver and Harada's results [2]. The total number of all inequivalent codes with new values of β in their weight enumerator is 3542.

For equivalence check on the codes in this research we use the software system Q-extensions by Iliya Bouyukliev [1].

REFERENCES

[1] I. Bouyukliev. About the code equivalence. In: Advances in Coding Theory and Cryptography, Series on coding theory and cryptology, vol. **3**, 2007, World Scientific Publishing, 126–151.

[2] T. A. Gulliver, M. Harada. Classification of extremal double circulant self-dual codes of lengths 64 to 72. *Des. Codes Cryptogr.*, **13** (1998), 257–269.

[3] W. C. Huffman. Automorphisms of codes with application to extremal doubly-even codes of length 48. *IEEE Trans. Inform. Theory*, **28** (1982), 511–521.

[4] W. C. Huffman. On the classification and enumeration of self-dual codes. *Finite Fields Appl.*, **11** (2005), 451–490.

[5] S. Karadeniz, B. Yildiz. New extremal binary self-dual codes of length 66 as extensions of self-dual codes over Rk. *Journal of the Franklin Institute*, **350** (2013), 1963–1973.

[6] A. Kaya, B. Yildiz. Extension theorems for self-dual codes over rings and new binary self-dual codes. arXiv:1404.0195, 2014.

[7] A. Kaya, B. Yildiz, I. Siap. New extremal and optimal binary self-dual codes from quadratic residue codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. arXiv:1308.0580, 2013.

[8] W. C. Huffman, V. Pless. Fundamentals of error correcting codes. Cambridge, Cambridge University Press, 2003.

[9] N. Yankov, M. H. Lee. Classification of self-dual codes of length 50 with an automorphism of odd prime order. *Des. Codes Cryptography* (to appear).

[10] N. Yankov, M. H. Lee, M. Gürel, M. Ivanova. Self-dual codes with an automorphism of order 11. Preprint.

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

[12] V. Yorgov. Binary self-dual codes with an automorphism of odd order. *Problems Inform. Transm.*, **4** (1983), 13–24.

[13] V. Yorgov. New extremal singly-even self-dual codes of length 44. In: Proceedings of the Sixth Joint Swedish-Russian International Workshop on Information Theory (Molle, Sweden), 1993, pp. 372–375.

[14] V. Yorgov, R. Ruseva. Two extremal codes of length 42 and 44. *Problems Inform. Trans.*, **29** (1993), 385–388.

Nikolay Ivanov Yankov
e-mail: jankov_niki@yahoo.com
Milena Nikolova Ivanova
e-mail: nicolova_m@abv.bg
Faculty of Mathematics and Informatics
University of Shumen
115, Universitetska Str.
9712 Shumen, Bulgaria

КЛАСИФИКАЦИЯ НА ДВОИЧНИ САМОДУАЛНИ $[68, 34, 12]$ КОДОВЕ С АВТОМОРФИЗЪМ ОТ РЕД 11

Николай Иванов Янков, Милена Николова Иванова

Класифицирани са с точност до еквивалентност всички оптимални двоични самодуални $[68, 34, 12]$ кодове, които притежават автоморфизъм от ред 11 с 6 независими цикъла при разлагане на независими цикли. Използвайки метод за конструиране на самодуални кодове, притежаващи автоморфизъм от нечетен прост ред е доказано, че съществуват точно 8821 нееквивалентни такива кода. Получени са 21 различни нови стойности за параметъра на тегловната функция за тази дължина.