Eighth International Workshop on Optimal Codes and Related Topics
July 10-14, 2017, Sofia, Bulgaria *pp. 128-133*

New self-dual $[78, 39, 14]$ codes with an automorphism of order 13[1]

Nikolay Yankov jankov_niki@yahoo.com
Faculty of Mathematics and Informatics,
Shumen University, 9700 Shumen, Bulgaria
Damyan Anev damian_anev@mail.bg
Faculty of Mathematics and Informatics,
Shumen University, 9700 Shumen, Bulgaria

Abstract. We apply a method by Huffman and Yorgov for constructing binary self-dual codes C having an automorphism of odd prime order $p = 13$. According the method all such codes are a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$. For the code $E_\sigma(C)$ we obtain exactly 322103 inequivalent codes with minimum distance $d \geq 14$. Using these codes we present a full classification of binary self-dual $[78, 39, 14]$ codes having a fixed points free automorphism of order 13. The total number of such codes is 1592 and among them are codes with 6 new values of the integer parameters in their respective weight enumerator.

1 Introduction

Let $\mathbb{F}_q$ be the finite field of q elements, for a prime power q. A linear $[n, k]_q$ *code* C is a k-dimensional subspace of $\mathbb{F}_q^n$. The elements of C are called *codewords*, and the *(Hamming) weight* of a codeword $v \in C$ is the number of the nonzero coordinates of v. We use $\mathrm{wt}(v)$ to denote the weight of a codeword. The *minimum weight* d of C is the minimum nonzero weight of any codeword in C and the code is called an $[n, k, d]_q$ code. A matrix whose rows form a basis of C is called a *generator matrix* of this code (denoted by $\mathrm{gen}(C)$).

By O, I, J we denote the zero, identity and all-ones matrices, respectively.

For every $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ from $\mathbb{F}_2^n$, $u.v = \sum_{i=1}^{n} u_i v_i$ defines the *inner product* in $\mathbb{F}_2^n$. The *dual code* of C is $C^\perp = \{v \in \mathbb{F}_2^n \mid u.v = 0, \forall\ u \in C\}$. If $C \subseteq C^\perp$, C is called *self-orthogonal*, and if $C = C^\perp$, we say that C is *self-dual*. We call a binary code *self-complementary* if it contains the all-ones vector. Every binary self-dual code is self-complementary.

A self-dual code is *doubly-even* if all codewords have weight divisible by four, and *singly-even* if there is at least one nonzero codeword of weight $\equiv 2 \pmod 4$. Self-dual doubly-even codes exist if and only if n is a multiple of eight.

[1]This research was supported by Shumen University by Project No RD-08-107/06.02.2017

The weight enumerator $W(y)$ of a code C is defined as $W(y) = \sum_{i=0}^{n} A_i y^i$, where A_i is the number of codewords of weight i in C. We say that two linear codes C and C' are *permutation equivalent* if there is a permutation of coordinates which sends C to C'. The set of coordinate permutations that maps a code C to itself forms a group denoted by $\mathrm{Aut}(C)$.

Rains [10] proved that the minimum distance d of a binary self-dual $[n, k, d]$ code satisfies the following bound:

$$\begin{aligned} d &\leq 4\lfloor n/24 \rfloor + 4, \quad \text{if } n \not\equiv 22 \pmod{24}, \\ d &\leq 4\lfloor n/24 \rfloor + 6, \quad \text{if } n \equiv 22 \pmod{24}. \end{aligned} \tag{1}$$

Codes achieving this bound are called *extremal*. A self-dual code is called *optimal* if it has the highest minimum weight among all self-dual codes.

The possible weight enumerators for extremal and optimal binary self-dual codes of lengths $72 \leq n \leq 100$ are known from Steven Dougherty, T. Aaron Gulliver and Masaaki Harada [3]. Later in [7] some additional restrictions for the parameters are proved.

For $[78, 39, 14]$ self-dual codes there are two possible weight enumerators:

$$\begin{aligned} W_{78,1} = 1 &+ (3705 + 8\beta)y^{14} + (62244 + 512\alpha - 24\beta)y^{16} \\ &+ (774592 - 4608\alpha - 64\beta)y^{18} + \cdots \end{aligned}$$

where $0 \leq \alpha \leq -\frac{\beta}{16} \leq 2$, and

$$W_{78,2} = 1 + (3705 + 8\alpha)y^{14} + (71460 - 24\alpha)y^{16} + (658880 - 64\alpha)y^{18} + \cdots$$

where $-468 \leq \alpha \leq -135$. Codes exist for $W_{78,1}$ when $\alpha = \beta = 0$ (see [3] and [5]), $\alpha = 0$, $\beta = -19$ (see [2]), $\alpha = 0$, $\beta = -26$ (see [6]), $\alpha = 0$, $\beta = -78$ (see [5]), and for $W_{78,2}$ for $\alpha = -135$ (see [5]). Very recently in [15] 16 inequivalent self-dual $[78, 39, 14]$ codes were found. The authors obtained codes with dihedral automorphism group D_{38} and a weight enumerator $W_{78,1}$: 4 codes with $\alpha = 0$, $\beta = -38$; 12 codes have $\alpha = \beta = 0$.

Optimal self-dual codes with an automorphism of odd prime order are a well studied subject. In fact all such codes are classified up to length 50 [11]. In [6] P. Gaborit and A. Otmani have constructed a $[78, 39, 14]$ self-dual code with an automorphism of order 13 with $W_{78,1}$ for $\alpha = 0$, $\beta = -26$. The extremal or optimal binary self-dual codes with an automorphism of order 13 with 4 cycles are classified in [14]. We continue the investigation of binary self-dual codes with an automorphism of order 13 with the next possible case, i.e. with 6 independent 13-cycles.

By the Rains bound (1) we have $d \leq 16$ for binary self-dual codes of lengths 78 to 92. Let C be an optimal binary self-dual $[78, 39, \geq 14]$ code possessing an automorphism σ of order 13 with $c = 6$ cycles and no fixed points.

For the computations, in this work, we use **GAP 4.8** [4] for the generation of the codes and **Q-extension** [1] for the code equivalence.

2 Construction method

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

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

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

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

Theorem 1 ([9]). *Assume that C is a self-dual code. Then the code C is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$. The subcodes $F_\sigma(C)$ 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 $v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$ 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 from [9] and [12] that $\varphi(E_\sigma(C)^*)$ is a submodule of the $\mathcal{P}$-module $\mathcal{P}^c$.

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

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

In order to classify the codes that we have obtained we need additional conditions for equivalence given by the following.

Theorem 3 ([13]). *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; (iv) a cyclic shift to each p-cycle independently.*

3 Constructing the $E_\sigma(C)^*$ subcode

By [14], 2 is a primitive root modulo 13, and hence $\mathcal{P}$ is a field with 2^{12} elements and identity $e(x) = x+\cdots+x^{12}$. We use the element $\alpha = 1+x+x^3+x^5$ which is a primitive element in $\mathcal{P}$ [13]. Using $\beta = \alpha^{13}$ which is an element of multiplicative order 315 in $\mathcal{P}$ we can write $\mathcal{P}^* = \{x^i\beta^j | 0 \le i \le 12, 0 \le j \le 314\}$.

After Gaussian elimination we can take the generator matrix for C_φ to be in the form $G = (e(x)I|Z)$, where Z is a 3×3 matrix over $\mathcal{P}$. Since every row of G has weight divisible by 4 and $E_\sigma(C)^*$ is a self-orthogonal code we claim that the code $E_\sigma(C)^*$ is double-even so its minimum weight should be $d \ge 16$. Using Theorem 3 we can transform the matrix Z to the following

$$Z = \begin{pmatrix} \beta^{i_1} & \beta^{i_2} & \beta^{i_3} \\ \beta^{i_4} & x^{l_5}\beta^{i_5} & x^{l_6}\beta^{i_6} \\ \beta^{i_7} & x^{l_8}\beta^{i_8} & x^{l_9}\beta^{i_9} \end{pmatrix},$$

where $i_1 \le i_2 \le i_3$, $0 \le i_t \le 314$, $0 \le l_t \le 12$, or some of the elements in Z are zeroes. Using the orthogonal condition (2) and checking that $d \ge 16$ we calculated all possible inequivalent choices of the first row of Z and found 1676 triples (i_1, i_2, i_3). Next, we added the second row of Z and we obtained 4086196 different 2×3 submatrices. Finally, after adding the last row we obtained exactly 322103 inequivalent codes with minimum distance $d = 16$.

Theorem 4. *There are exactly* 322103 *inequivalent codes C_φ of length* 6 *over the set $\mathcal{P}$ of all even-weight polynomials in $\mathbb{F}_2[x]/\langle x^{13}-1\rangle$ such that $d(E_\sigma(C)^*) =$* 16.

The order of the automorphism groups of the codes that we have obtained are listed in Table 1.

Table 1: The order of the automorphism groups of all $E_\sigma(C)^*$

$\lvert\mathrm{Aut}(C)\rvert$	13	26	39	52	78	156	234	468
#	317529	4314	42	167	41	8	1	1

4 Classification of $[78, 39, 14]$ self-dual codes with an automorphism of type $13-(6,0)$

Assume that C is a $[78, 39, 14]$ self-dual code with an automorphism of type $13-(6,0)$. By Theorem 2, C_π is a binary self-dual $[6, 3, 2]$ code. There is a unique such code: $3i_2$ (see [8]) with generator matrix $G_1 = (I_3|I_3)$. By Theorem 1, C is a direct sum of $F_\sigma(C)$ and $E_\sigma(C)$. We fix the generator matrix of

$E_\sigma(C)$ to be the generator matrix of one of the codes from Theorem 4. For all permutations $\tau \in S_6$ we consider the generator matrix of C_π to be $\tau(G_1)$. We summarize the results in the following.

Proposition 1. *There are exactly* 1592 *inequivalent binary* $[78, 39, 14]$ *self-dual codes having an automorphism of type* $13 - (6, 0)$.

All codes that we have obtained possess weight enumerator $W_{78,1}$ for $\beta = -117, -104, -78, -65, -52, -39, -26, -13$, and 0. All values except $\beta = -78, -13$, and 0 are new. We list the number of inequivalent codes with the different pairs $(\beta, |\mathrm{Aut}(C)|)$ in Table 2 where the new values are marked in bold. One of the three codes with the pair $(\beta, |\mathrm{Aut}(C)|) = (-78, 78)$ is the code $C_{78,1}$ from [5].

Table 2: β in $W_{78,1}$ and $|\mathrm{Aut}(C)|$ for $[78, 34, 14]$ self-dual codes with an automorphism of type $13 - (6, 0)$

	$\lvert\mathrm{Aut}(C)\rvert$					$\lvert\mathrm{Aut}(C)\rvert$			
β	13	26	39	78	β	13	26	39	78
−117			**1**		**−39**	**302**			
−104		**1**			−26	437	30		
−78	5	7	1	3	**−13**	**421**			
−65	**37**				0	171	18		5
−52	**137**	**14**	**2**						

5 Conclusion and future work

As we have seen in this work there are no $[78, 39, 16]$ binary self-dual codes with an automorphism of order 13. The remaining cases for the prime order of the automorphisms of this codes are $p = 19, 7, 5$ and 3.

For future work we can use the codes obtained in Section 3 to classify all binary self-dual $[2k, k, d]$ codes for $k = 40, 41$ and 42 and $d \geq 14$.

References

[1] I. Bouyukliev, *About the code equivalence in Advances in Coding Theory and Cryptography vol. 3*, World Scientific Publishing Company, 2007, 126–151.

[2] A. Baartmans and V. Yorgov, Some new extremal codes of lengths 76 and 78, *IEEE Trans. Infor. Theory*, **49(5)**, 1353–1354, 2003.

[3] S. T. Dougherty, T. A. Gulliver, and M. Harada, Extremal binary self-dual codes, *IEEE Trans. Infor. Theory*, vol. 43, no. 6, 2036–2047, 1997.

[4] *GAP – Groups, Algorithms, and Programming, Version 4.8.6*, The GAP Group, 2016. [Online]. Available: http://www.gap-system.org

[5] T. A. Gulliver, M. Harada, and J.-L. Kim, Construction of new extremal self-dual codes, *Discrete Math.*, **263(1-3)**, 81–91, 2003.

[6] P. Gaborit and A. Otmani, Experimental constructions of self-dual codes, *Finite Fields Appl.*, **9(3)**, 372–394, 2003.

[7] M. Harada and A. Munemasa, Some restrictions on weight enumerators of singly even self-dual codes, *IEEE Trans. Infor. Theory*, **52(3)**, 1266–1269, 2006.

[8] W. C. Huffman and V. S. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

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

[10] E. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Infor. Theory*, **44(1)**, 134–139, 1998.

[11] N. Yankov and M. H. Lee, Classification of self-dual codes of length 50 with an automorphism of odd prime order, *Des. Codes Cryptogr.*, **74(3)**, 571–579, 2015.

[12] V. Yorgov, Binary Self-Dual Codes with Automorphisms of Odd Order, *Probl. Inform. Transm.*, **19(4)**, 260–270, 1983.

[13] V. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, *IEEE Trans. Infor. Theory*, **33(1)**, 77–82, 1987.

[14] N. Yankov and R. Russeva, Binary Self-Dual Codes of Lengths 52 to 60 With an Automorphism of Order 7 or 13, *IEEE Trans. Infor. Theory*, **57(11)**, 7498–7506, 2011.

[15] T. Zhang, J. Michel, T. Feng, and G. Ge, On the Existence of Certain Optimal Self-Dual Codes with Lengths Between 74 and 116, *Electron. J. Combin.*, **22(4)**, P4.33, 2015.