Further results on the classification of binary self-dual [52, 26, 10] codes with an automorphism of odd prime order[1]

Nikolay Yankov, Radka Russeva

Abstract: *The paper presents the next step on the complete classification of all optimal binary self-dual codes of length* 52 *that possess an automorphism of odd prime order. Applying the method for constructing binary self-dual codes with an automorphism of odd prime order p=3 we give full classification of all* [52, 26, 10] *binary self-dual codes with an automorphism of type* 3-(16,4) *for the next unsolved case for the generator matrix of the fixed subcode. Thus we construct* 6494315 *optimal codes with weight enumerator* $W_{52,2}(y)$ *for* $\beta = 1,4,$ *and* 7*. Only a small portion of the codes we have obtained were previously known. Tables for the weight enumerators and order of the automorphism groups of all constructed codes are given.*

Key words: *automorphism; classification; code; self-dual code*

INTRODUCTION

A *linear* $[n,k]$ *code C* is a *k*-dimensional subspace of the vector space F_q^n, where 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 nonzero coordinate positions. The *minimum weight d* of *C* is the smallest weight among all nonzero code words of *C*, and *C* is called an $[n,k,d]$ code.

A matrix which 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*. Let $(u,v): F_q^n \times F_q^n \to F_q$ be an inner product in the linear space F_q^n. The *dual code* of *C* is $C^{\perp} = \{u \in F_q^n : (u,v) = 0 \text{ for all } v \in C\}$. The dual code $C^{\perp}$ is a linear $[n, n-k]$ code. We call the code *C self-orthogonal* if $C \subseteq C^{\perp}$. If $C = C^{\perp}$ then the code *C* is termed *self-dual*.

The codes with the largest possible minimum weight among all self-dual codes of a given length are named *optimal* self-dual codes. For self-dual codes, Rains [1] provided new upper bounds for the minimum weight

$$d \le \begin{cases} 4\left\lfloor n/24 \right\rfloor + 4, \text{ when } n \not\equiv 22 (\mathrm{mod}\, 24); \\ 4\left\lfloor n/24 \right\rfloor + 4, \text{ when } n \equiv 22 (\mathrm{mod}\, 24). \end{cases}$$

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 a group, called the *automorphism group* $Aut(C)$ of *C*. Some researchers on self-dual codes work towards full classification of all inequivalent codes for a given length. The last results in this regards are for length 38 by Bouyuklieva and Bouyukliev [2] and for length 40 by Bouyukliev et all [3]. In both of these cases a complete classification is given. Alas, since the number of all inequivalent codes grow exponentially with the length, for bigger lengths even the classification of optimal codes is infeasible at this time. This leads to imposing some restrictions on the codes that we are trying to construct, in our case we look for codes having a specific type of automorphism.

In this paper we consider optimal self-dual [52, 26, 10] codes with an automorphism of order 3. The codes having automorphisms of prime order $p \ge 5$ are classified in [4]. The codes with automorphisms of order 3 with 14 independent 3-cycles are classified in [5].

[1] This paper is supported by Shumen University under Grants RD-08-277/11.03.2015 and RD-08-287/12.03.2015.

The case of 16 cycles is partially solved in [6]. We continue with the next step on the classification of all optimal binary self-dual codes of length 52 that possess an automorphism of order 3 of type 3–(16,4). To do that we apply the method developed by Huffman and Yorgov (cf. [7] – [9]).

CONSTRUCTION METHOD

Let C be a binary self-dual code of length n and σ be an automorphism of C of order p for an odd prime p. Without loss of generality we can assume that

$$\sigma = \Omega_1 \cdots \Omega_c \Omega_{c+1} \cdots \Omega_{c+t}, \tag{7}$$

where $\Omega_1,\ldots,\Omega_c$ are the cycles of length p and $\Omega_{c+1},\ldots,\Omega_{c+t}$ are the fixed points. We shortly say that σ is of type $p-(c,f)$. Then we have $cp+f=n$.

Let $F_\sigma(C)=\{v\in C : v\sigma = v\}$ and $E_\sigma(C)=\{v\in C : wt(v\mid\Omega_i)\equiv 0(\mathrm{mod}2)\}$, $i=1,2,\ldots,c$, where $v\mid\Omega_i$ is the restriction of the vector v on Ω_i. We have the following lemma [7].

Lemma 1 $C=F_\sigma(C)\oplus E_\sigma(C)$, where the symbol $\oplus$ means a direct sum of codes, $\dim F_\sigma(C)=(p-1)c/2$. When C is a self-dual code and 2 is a primitive root modulo p, then c is even.

Obviously $v\in F_\sigma(C)$ iff $v\in C$ and v is constant on each cycle. Let $\pi : F_\sigma(C)\to F_2^{c+f}$ be the projection map where if $v\in F_\sigma(C)$, $(v\pi)_i = v_j$ for some $j\in\Omega_i$, $i=1,2,\ldots,c+f$.

Every vector of length p can be represented with a polynomial in the factor ring $F_2[x]/(x^p-1)$, namely $(a_0,a_1,\ldots,a_{p-1})\mapsto a_0+a_1x+\cdots+a_{p-1}x^{p-1}$. We call the weight of a polynomial the number of its nonzero coefficients. Let P be the set of all even-weight polynomials in $F_2[x]/(x^p-1)$. Then P is a cyclic code of length p with generator polynomial $x-1$.

Lemma 2 [7] Let p be an odd prime such that $1+x+x^2+\cdots+x^{p-1}$ is irreducible over F_2. Then P is a field with identity $x+x^2+\cdots+x^{p-1}$.

Denote by $E_\sigma(C)^*$ the code $E_\sigma(C)$ with the last f coordinates deleted. Consider for $v\in E_\sigma(C)$ each $v\mid\Omega_i=(a_0,a_1,\ldots,a_{p-1})$ as a polynomial $\phi(v\mid\Omega_i)$ in the following way

$$\phi(v\mid\Omega_i)=a_0+a_1x+\cdots+a_{p-1}x^{p-1},\ \text{for}\ 1\le i\le c. \tag{8}$$

This way we define the map $\phi : E_\sigma(C)^*\to P^c$.

Theorem 1 [7] Assume that the polynomial $1+x+x^2+\cdots+x^{p-1}$ is irreducible over F_2. A code C, possessing an automorphism (1), is self-dual if and only if the following conditions hold:

i) $C_\pi=\pi(F_\sigma(C))$ is a $[c+f,\frac{c+f}{2}]$ binary self-dual code;

ii) $C_\phi=\phi(E_\sigma(C)^*)$ is a self-dual $[c,c/2]$ code over the field P under the inner product $(u,v)=\sum_{i=0}^{c}u_iv_i^{2^{(p-1)/2}}$, where $u=(u_1,\ldots,u_c)$, $v=(v_1,\ldots,v_c)\in P^c$.

Theorem 2 [9] Let the permutation σ, defined in (1), 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) a substitution $x\to x^t$ for $t=1,\ldots,p-1$ in C_ϕ; b) any multiplication of the j-th coordinate of C_ϕ by x^{t_j}, where t_j is an integer, $1\le t_j\le p-1$, $j=1,\ldots,c$; c) any permutation of the first c cycles of C; d) any permutation of the last f coordinates of C.

OPTIMAL BINARY SELF-DUAL CODES OF LENGTH 52

In this section we apply the method described in the previous and we classify a new part of optimal binary [52, 26, 10] self-dual codes with an automorphism of type 3–(16, 4).

The weight enumerators of the extremal self-dual codes of length 52 are known [5]:

$$W_{52,1}(y) = 1 + 250y^{10} + 7980y^{12} + 423800y^{14} + \cdots \quad \text{and}$$

$$W_{52,2}(y) = 1 + (442 - 16\beta)y^{10} + (6188 + 64\beta)y^{12} + 53040y^{14} + \cdots,$$

for $0 \le \beta \le 12$. Codes exist with weight enumerators for $W_{52,1}$ and $W_{52,2}$ for $\beta = 1,\ldots, 12$ [5].

Let C be a binary self-dual code of length $n = 52$ with an automorphism σ of order $p = 3$ with exactly 16 independent 3-cycles and 4 fixed points in its factorization. We may assume that

$$\sigma = (1,2,3)(4,5,6)\ldots(46,47,48). \tag{9}$$

Then C_φ is a Hermitian $[16,8,\ge 5]$ code over the field F_4 of four elements. There are exactly four inequivalent such codes $2f_8$, $1_6 + 2f_5$, 1_{16}, $4f_4$ [10] with generator matrices denoted by $H_1,\ldots,H_4$, respectively. The exact matrices can be found in [5].

The code C_π is a [16, 8] binary self-dual code with minimum distance at least 4. In [5] it was proved that, there are exactly three possible generator matrices B_1, B_2 and B_3 for the subcode C_π up to equivalence as follows:

$$B_1 = \begin{pmatrix} 1111000000000000000 \\ 0000111000000001000 \\ 0000000111000000100 \\ 0000000000111000010 \\ 0000000000000111001 \\ 0000000110010110001 0 \\ 1100000000110010000 1 \\ 0101110000000110000 0 \\ 1100010110000000100 0 \\ 0000110010110000010 0 \end{pmatrix}, B_2 = \begin{pmatrix} 1111000000000000000 \\ 0011110000000000000 \\ 0000001111000000000 \\ 0000000011100000100 0 \\ 0000000000011110000 0 \\ 0000000000000111010 0 \\ 1010101010110101001 0 \\ 1010011010010100110 1 \\ 1010100000011010011 00 \\ 0000111010010101100 0 \end{pmatrix}, B_3 = \begin{pmatrix} 1111000000000000000 \\ 0011100000000001000 \\ 0000011110000000000 \\ 0000000111000000100 \\ 0000000001111000000 \\ 0000000000001110001 0 \\ 1010110101101011000 0 \\ 1010010100101000111 1 \\ 1010100001101000011 0 \\ 0000110100101010110 0 \end{pmatrix}.$$

Here we will consider the case gen $C_\pi = B_2$. The codes in the case gen $C_\pi = B_3$ are classified in [6]. For a permutation $\tau \in S_{16}$ we denote by B_2^τ the matrix derived from B_2 after permuting its columns by τ. Denote by C_i^τ, $i = 1,\ldots,4$, the [52, 26] binary self-dual code with a generator matrix in the form:

$$G_i^\tau = \begin{pmatrix} \pi^{-1}(B_2^\tau) \\ \varphi^{-1}(H_i) \quad O \end{pmatrix}, \tag{10}$$

where O is a 16×4 all-zeros matrix.

Let R_i be the subgroup of the automorphism group of the [16, 8] binary code generated by the matrix $B_i, i = 1,2,3$ consisting of the automorphisms of this code that permute the first 16 coordinates (corresponding to the 3-cycle coordinates) among themselves and permute the last 4 coordinates (corresponding to the fixed point coordinates) among themselves. Let U_i be the subgroup of the symmetric group S_{16} consisting of the permutations in R_i restricted to the first 16 coordinates, ignoring the action on the fixed points. Using Iliya Bouyukliev's program *Q-extensions* [11] we have

computed all groups R_i for i = 1,2,3. We have found that $|R_1| = 96, |R_3| = 768,$ and the group $R_2 = \langle (1,15,14,7,16,13)(2,8)(3,9)(4,10)(5,12)(6,11),(13,16)(14,15),\ (3,4)(5,6),\ (3,5)(4,6) \rangle$ has order 192. Also using *Q-extensions* [11] we computed the automorphism groups of the codes generated by $H_1,\ldots,H_4,$ which we denote by $L_1,\ldots,L_4$ summarized in Table 1.

Table 1. Automorphism groups of the Hermitian subcodes of the [52, 26, 10] codes having an automorphism of type 3–(16,4)

group	generating permutations for the automorphism group	order of the group
L_1	(1,7,4,5,3,8,2,6)(9,15,12,13,11,16,10,14), (1,12,5,15,3,14,8,10)(2,9,4,13,7,11,6,16)	672
L_2	(1,2,3,4)(7,15,11,14)(8,13)(9,12,10,16), (1,6,4,5,3)(7,14,8,16,10,12,9,13,11,15)	240
L_3	(1,6,9,10,16)(3,12,15,7,13)(4,14,11,5,8), (1,8,11,13,6,9)(2,4,5,16,14,12)(3,15)(7,10)	960
L_4	(1,3,11,9,13,5,15,6)(2,14,8,16,7,10,4,12), (1,16,2,10,11,9,13,12,7,14,15,6)(3,4,5,8)	96

Let H and K be subgroups of a group G. A H and K-*double coset* for some $x \in G$ is a set of the form $HxK = \{hxk \mid h \in H, k \in K\}$. We denote the set of double cosets as $H\backslash G/L$. A known fact is that for a fixed i if $\tau_1, \tau_2 \in S_{16}$ if the double cosets $U_2\tau_1 L_i$ and $U_2\tau_2 L_i$ coincide then the codes $C_i^{\tau_1}$ and $C_i^{\tau_2}$ are equivalent [8]. Thus we only need to compute codes that arise from the double transversals $T_i = U_2 \backslash S_{16} / L_i, i = 1,\ldots,4.$ We use the computer algebra system GAP [12] for computing the double transversals. Unfortunately this is a very time and resource consuming process, for example the computation for the transversal with the smallest group (H_4) takes about two weeks and up to 180 Gb of RAM on a specially dedicated Ubuntu server with 8 core Opteron processor, 32 Gb RAM and 200 Gb swap partition on a solid state drive. The numbers of elements in the transversals T_i are listed in Table 2.

Table 2. The size of the double transversals

T_1	T_2	T_3	T_4
162168480	454063320	113523120	1135153440

Theorem 3 Let C be a binary self-dual code of length 52 with an automorphism σ from (1) and $C_\pi = B_2$. Up to equivalence there are exactly 6494315 such codes all with weight enumerator $W_{52,2}(y)$ for $\beta = 1,4,$ and 7.

Table 3. $|\mathrm{Aut}(C)|$ **and** β **in** $W_{52,2}(y)$ **for the constructed codes with** $C_\pi = B_2$

	β	$\lvert\mathrm{Aut}(C)\rvert = 3$		β	$\lvert\mathrm{Aut}(C)\rvert = 3$	$\lvert\mathrm{Aut}(C)\rvert = 21$
T_1	1	615716	T_2	1	1399862	0
	4	40040		4	117849	0
	7	138		7	1209	2
	β	$\lvert\mathrm{Aut}(C)\rvert = 3$		β	$\lvert\mathrm{Aut}(C)\rvert = 3$	$\lvert\mathrm{Aut}(C)\rvert = 21$
T_3	1	178432	T_4	1	3823240	0
	4	15305		4	300249	0
	7	136		7	2135	2

Remark: The numbers of obtained codes in each case are listed in Table 3. Only the codes with automorphism of order 21 were previously known from [4].

CONCLUSIONS AND FUTURE WORK

Although with this paper a major advance have been made regarding the classification of all optimal self-dual codes of length 52 with an automorphism of odd prime order still a great deal of work remains to be done. The last case for the binary matrix (B_1) we regard as the most difficult and the reason is that the generator matrix in the case has the smallest automorphism group. Nevertheless we intend to complete this task.

REFERENCES

[1] Rains E.M., Shadow bounds for self-dual codes. IEEE Trans. Inform. Theory, vol. 44(1), pp. 134–139, 1998.

[2] Bouyuklieva S., I. Bouyukliev, An Algorithm for Classification of Binary Self-Dual Codes, IEEE Trans. Inf. Theory, vol. 58(6), pp. 3933–3940, 2012.

[3] Bouyukliev I., M. Dzhumalieva-Stoeva, and V. Monev, Classification of Binary Self-Dual Codes of Length 40, IEEE Trans. Inf. Theory, vol. 61(8), pp. 4253–4258, 2015.

[4] Yankov N., R. Russeva, Binary self-dual codes of lengths 52 to 60 with an automorphism of order 7 or 13. IEEE Trans. Inform. Theory, 57(11), pp. 7498–7506, 2011.

[5] Yankov N., New optimal [52, 26, 10] self-dual codes. Designs, Codes and Cryptography, vol. 69 (2), pp. 151–159, 2013.

[6] Yankov N., R. Russeva. New results on the classification of binary self-dual [52, 26, 10] codes with an automorphism of odd prime order. Proceedings of the University of Ruse, vol. 52, book 6.1, pp. 21–25, 2013.

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

[8] Yorgov V.Y. Binary self-dual codes with an automorphism of odd order. Probl. Inform. Transm. 4, pp. 13–24 (in Russian), 1983.

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

[10] Conway, J. H., V. Pless, N. J. Sloane, Self-dual codes over GF(3) and GF(4) of length not exceeding 16. IEEE Trans. Inform. Theory, vol. 25(3), 312–322, 1979.

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

[12] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.8; 2015. (http://www.gap-system.org)

ABOUT THE AUTHORS

Assoc.Prof. Nikolay Yankov, DSc, Faculty of Mathematics and Informatics, Shumen University, E-mail: n.yankov@shu-bg.net

Assoc.Prof. Radka Russeva, PhD, Faculty of Mathematics and Informatics, Shumen University, E-mail: russeva@fmi.shu-bg.net