# New 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 an important step toward the complete classification of all optimal binary self-dual codes of length 52 that possess an automorphism of odd prime order. Using a method for constructing and classifying binary self-dual codes with an automorphism of odd prime order p we give full classification of all [52, 26, 10] binary self-dual codes with an authomorphism of type 3-(16,4) and a certain generator matrix for the fixed subcode. Also, we construct 178727 optimal codes with weight enumerator* $W_{52,1}(y)$*. All but one of the constructed codes are new. For all constructed codes we give the order of its automorphism group.*

***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 a $[n,k,d]$ 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.

A self-dual code *C* is doubly-even if all codewords of *C* have a weight divisible by four, and singly-even if there is at least one codeword of weight congruent 2 modulo 4. Self-dual doubly-even codes exist only when *n* is divisible by eight. The codes with the largest possible minimum weight among all self-dual codes of a given length are named optimal self-dual codes. For singly-even self-dual codes, Conway and Sloane [1] provided new upper bounds for the minimum weight, and gave a list of the possible weight enumerators of singly-even self-dual codes meeting the bounds for lengths up to 64 and for length 72.

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*.

## CONSTRUCTION METHOD

Huffman and Yorgov (cf. [2]-[4]) developed a method for constructing binary self-dual codes with an automorphism of odd prime order.

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

$$\sigma=\Omega_1\cdots\Omega_c\Omega_{c+1}\cdots\Omega_{c+t}, \quad \textbf{(1)}$$

[1] This paper is supported by Shumen University under Grant RD-08-241/12.03.2013

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 $\sigma$ is of type $p-(c,f)$. Then we have $cp+f=n$.

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

**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** [2] 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 $v\,|\,\Omega_i=(a_0,a_1,\ldots,a_{p-1})$ as a polynomial $\phi(v\,|\,\Omega_i)$ in the following way

$$\phi(v\,|\,\Omega_i)=a_0+a_1x+\cdots+a_{p-1}x^{p-1},\ \text{for}\ 1\le i\le c. \qquad \textbf{(2)}$$

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

**Theorem 1** [4] 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** [5] Let the permutation $\sigma$, 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 $C_\phi$;

b) any multiplication of the *j*-th coordinate of $C_\phi$ 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*.

**NEW OPTIMALBINARY SELF-DUAL CODES OF LENGTH 52**

In this section we apply method described in Section 2 and we classify all optimal binary [52, 26, 10] self-dual codes with an automorphism of type 3-(16, 4) and a particular generator matrix for the subcode $C_\pi$.

The weight enumerators of the extremal self-dual codes of length 52 are known [6]:

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

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 $\beta = 1, \ldots, 12$ [6].

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

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

Then $C_\varphi$ is a hermitian $[16, 8, \ge 5]$ code over the field $F_4$ of four elements. There are exactly four inequivalent such codes $2f_8$, $1_6 + 2f_5$, $1_{16}$, $4f_4$ [7] with generator matrices

$$H_1 = \left( E_8 \;\middle|\; \begin{array}{c} 0\,1111111 \\ 101\omega\bar{\omega}\bar{\omega}\omega 1 \\ 1101\omega\bar{\omega}\bar{\omega}\omega \\ 1\omega 101\omega\bar{\omega}\bar{\omega} \\ 1\bar{\omega}\omega 101\omega\bar{\omega} \\ 1\bar{\omega}\bar{\omega}\omega 101\omega \\ 1\omega\bar{\omega}\bar{\omega}\omega 101 \\ 11\omega\bar{\omega}\bar{\omega}\omega 10 \end{array} \right), \quad H_2 = \left( \begin{array}{c} 1100000\omega 00\omega 00\bar{\omega}\bar{\omega}0 \\ 101000\omega 0\omega 00000\bar{\omega}\bar{\omega} \\ 1001000\omega 0\omega 0\bar{\omega}000\bar{\omega} \\ 10001000\omega 0\omega\bar{\omega}\bar{\omega}000 \\ 100001\omega 00\omega 00\bar{\omega}\bar{\omega}00 \\ 00\bar{\omega}00\bar{\omega}0\omega 0\bar{\omega}000\bar{\omega}0\omega \\ 0\bar{\omega}0\bar{\omega}0000\omega 0\bar{\omega}\omega 00\bar{\omega}0 \\ 0000001\omega 00\omega 1\omega 00\omega \end{array} \right),$$

$$H_3 = \left( \begin{array}{c} 1100000\omega\bar{\omega}\omega 00000\bar{\omega} \\ 10100000\omega\bar{\omega}\omega\bar{\omega}0000 \\ 100100\omega 00\omega\bar{\omega}0\bar{\omega}000 \\ 100010\bar{\omega}\omega 00\omega 00\bar{\omega}00 \\ 100001\omega\bar{\omega}\omega 00000\bar{\omega}0 \\ 010\bar{\omega}0\omega 1\bar{\omega}0000000\omega \\ 0\omega 10\bar{\omega}001\bar{\omega}00\omega 0000 \\ 00\omega 10\bar{\omega}001\bar{\omega}00\omega 000 \end{array} \right) \text{ and } H_4 = \left( E_8 \;\middle|\; \begin{array}{c} 0\,1111111 \\ 1000\omega\omega\bar{\omega}\bar{\omega} \\ 111\bar{\omega}000\bar{\omega} \\ 11\bar{\omega}1\bar{\omega}\bar{\omega}0\bar{\omega} \\ 1\bar{\omega}011\bar{\omega}00 \\ 1\bar{\omega}0\omega 1\omega 1\bar{\omega} \\ 1\bar{\omega}1\bar{\omega}\bar{\omega}0\bar{\omega}1 \\ 1\bar{\omega}\bar{\omega}\omega\omega 011 \end{array} \right), \text{ respectively.}$$

The code $C_\pi$ is a [16, 8] binary self-dual code with minimum distance at least 4. The following Lemma was proved in [6]:

**Lemma 2** Let $C$ be a binary self-dual code of length 52 with an automorphism $\sigma$ from (3)**.** Up to a permutation, there are exactly three up to equivalence possible generator matrices $B_1, B_2$ and $B_3$ for the subcode $C_\pi$ as follows:

$$B_1 = \begin{pmatrix} 11110000000000000000 \\ 00001110000000001000 \\ 00000001110000000100 \\ 00000000001110000010 \\ 00000000000001110001 \\ 00000001100101100010 \\ 11000000001100100001 \\ 01011100000001100000 \\ 11000101100000001000 \\ 00001100101100000100 \end{pmatrix}, B_2 = \begin{pmatrix} 11110000000000000000 \\ 00111100000000000000 \\ 00000011110000000000 \\ 00000000111000001000 \\ 00000000000111100000 \\ 00000000000001110100 \\ 10101010101101010010 \\ 10100110100101001101 \\ 10101000001101001100 \\ 00001110100101011000 \end{pmatrix}, B_3 = \begin{pmatrix} 11110000000000000000 \\ 00111000000000001000 \\ 00000111100000000000 \\ 00000001110000000100 \\ 00000000001111000000 \\ 00000000000011100010 \\ 10101101011010110000 \\ 10100101001010001111 \\ 10101000011010000110 \\ 00001101001010101100 \end{pmatrix}.$$

*In this paper we consider the case* gen $C_\pi = B_3$. *For a permutation* $\tau \in S_{16}$ *we denote by* $B_3^\tau$ *the matrix derived from* $B_3$ *after permuting its columns by* $\tau$. *Denote by* $C_i^\tau$, $i = 1, \dots, 4$ *, the [52, 26] binary self-dual code with a generator matrix in the form:*

$$G_i^\tau = \begin{pmatrix} \pi^{-1}(B_3^\tau) & \\ \varphi^{-1}(H_i) & O \end{pmatrix}, \tag{4}$$

*where* O *is a* $16 \times 4$ *all-zeros matrix.*

Let *A* be the subgroup of the automorphism group of the [16, 8] binary code generated by the matrix $B_3$ 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 $G'$ be the subgroup of the symmetric group $S_{16}$ consisting of the permutations in *A* restricted to the first 16 coordinates, ignoring the action on the fixed points.

Using Iliya Bouyukliev's application *Q-extensions* [8] we computed that $G' = \langle (3,4)(5,6), (3,5)(4,6), (13,16)(14,15), (1,15,14,7,16,13)(2,8)(3,9)(4,10)(5,12)(6,11) \rangle$ is a group of cardinality 768.

The following lemma gives sufficient conditions for the equivalence of two codes $C_i^{\tau_1}$ and $C_i^{\tau_2}$, $i = 1, \dots, 4$.

**Lemma 3** If $\tau_1$ and $\tau_2$ belong to one and the same right coset of $G'$ in $S_{16}$, then the codes $C_3^{\tau_1}$ and $C_3^{\tau_2}$ are equivalent.

Thus we only need the permutations from the set *T* − a right transversal of $S_{16}$ with respect to $G'$. The downside is that the size of *T* is huge 27243216000 thus the computations are time consuming. Since we only compute codes constructed from the same subcode $C_\pi$ with generator matrix $B_3$ all optimal self-dual [52, 26, 10] codes will have the same weight distribution $W_{52,1}(y)$ (see [6]). We conclude a summary of the orders of the automorphism group for each of the four cases displayed in Table 1.

**Table 1. Orders of the automorphism groups of the constructed codes**

| case | $\|\mathrm{Aut}(C)\|=3$ | $\|\mathrm{Aut}(C)\|=6$ | $\|\mathrm{Aut}(C)\|=150$ | Total codes |
|---|---|---|---|---|
| $C_\varphi = H_1$ | 16675 | 586 | | 17261 |
| $C_\varphi = H_2$ | 33321 | 138 | | 33459 |
| $C_\varphi = H_3$ | 4241 | 177 | 1 | 4419 |
| $C_\varphi = H_4$ | 122654 | 934 | | 123588 |

**Theorem 3** Let $C$ be a binary self-dual code of length 52 with an automorphism $\sigma$ from (3) and $C_\pi = B_3$. Up to equivalence there are exactly 178727 such codes all with weight enumerator $W_{52,1}(y)$.

*Remark:* One of the constructed [52, 26, 10] codes has an automorphism group of order $150 = 2.3.5$ and is equivalent to a code from [9]. Thus all the rest 178726 codes are new.

**REFERENCES**

[1] Conway J.H., Sloane N.J.A. A new upper bound on the minimal distance of self-dual codes. IEEE Trans. Inform. Theory, vol. 36, pp. 1319–1333, 1990.

[2] 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.

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

[4] 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.

[5] Yorgov V.Y. The extremal codes of length 42 with automorphism of order 7. Discr. Math., vol 19, pp. 201-213, 1998.

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

[7] Conway, J. H., V. Pless, Sloane, N. J. A. Self-dual codes over GF(3) and GF(4) of length not exceeding 16. IEEE Transactions on Information Theory, 25(3), 312–322, 1979.

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

[9] Yankov, N., M.H. Lee, New binary self-dual codes of lengths 50-60. to appear in Designs, Codes and Cryptography, 2013.

**About the authors:**

Assoc.Prof. Nikolay Yankov, PhD, 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

**The paper is reviewed.**