Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 341–346*

Determination of the weight enumerator for optimal binary self-dual codes of length 52[1]

Nikolay Yankov jankov_niki@yahoo.com
Faculty of Mathematics and Informatics, Shumen University, Shumen, BULGARIA

Abstract. In this paper we give full classification of all binary $[52, 26, 10]$ self-dual codes with an automorphism of order 5. This completes the classification of all such codes with an automorphism of odd prim order $p > 3$. There are exactly 18777 such codes having an automorphism of type $5 - (10, 2)$. One of the constructed codes have weight enumerator $W_{52,2}$ for $\beta = 10$ thus completely determines the weight enumerators for which there exists a binary self-dual $[52, 26, 10]$ code.

1 Introduction

We apply a method for constructing binary self-dual codes possessing an automorphism of odd prime order from [3] and [6].

Let C be a binary self-dual code of length n with an automorphism σ of prime order $p \geq 3$ with exactly c independent p-cycles and $f = n - cp$ fixed points in its decomposition. We may assume that

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

and shortly say that σ is of *type* $p - (c, f)$. Let $\Omega_1, \ldots, \Omega_c$ are the p-cycles of σ and $\Omega_{c+1}, \ldots, \Omega_{c+f}$ – the fixed points. Define

$$F_\sigma(C) = \{v \in C \mid v\sigma = v\},$$

$$E_\sigma(C) = \{v \in C \mid \ \mathrm{wt}(v|\Omega_i) \equiv 0 (\mathrm{mod}\ 2), i = 1, \cdots, c+f\},$$

where $v|\Omega_i$ is the restriction of v on Ω_i.

Theorem 1. *[3]* $C = F_\sigma(C) \oplus E_\sigma(C)$, $\dim(F_\sigma) = \frac{c+f}{2}$, $\dim(E_\sigma) = \frac{c(p-1)}{2}$.

We have 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 $j \in \Omega_i$, $i = 1, 2, \ldots, c+f$.

[1]This research is by Shumen University under Project RD-05-274/15.03.12

Theorem 2. *[7] 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 $u, v \in C_\varphi = \varphi(E_\sigma(C)^*)$ we have $\sum_{i=1}^{c} u_i(x)v_i(x^{-1}) = 0$.
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 $v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$ from $\mathcal{P}$, where $\mathcal{P}$ is the set of even-weight polynomials in $\mathbb{F}_2[x]/\langle x^p - 1\rangle$. 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 $x - 1$.

For $[52, 26, 10]$ self-dual codes there are two possible weight enumerators:

$$W_{52,1}(y) = 1 + 250y^{10} + 7980y^{12} + 42,800y^{14} + \cdots, \tag{1}$$

$$W_{52,2}(y) = 1 + (442 - 16\beta)y^{10} + (6188 + 64\beta)y^{12} + 53,040y^{14} + \cdots, \tag{2}$$

where $0 \le \beta \le 12$, $\beta \ne 11$ [1]. Codes exist for $W_{52,1}$ and for $W_{52,2}$ when $\beta = 1, \ldots 9, 12$ [8].

2 The subcode $E_\sigma(C)^*$

Let C be a binary self-dual code with minimum distance $d \ge 10$, possessing an automorphism of order 5 with 10 cycles. Using Theorem 2 we have that the subcode C_φ is a self-dual code of length 10 over the field $\mathcal{P}$ under the inner product

$$(u, v) = \sum_{i=1}^{10} u_i v_i^4. \tag{3}$$

Since 2 is a primite root modulo 5, $\mathcal{P}$ is a finite field with 16 elements, $\mathcal{P} \cong \mathbb{F}_{16} = \{0, \alpha^k | k = 0, 14\}$, where $e = x + x^2 + x^3 + x^4$, $\alpha = x + 1$ is a primitive element of multiplicative order 15. Denoting by $\delta = \alpha^5$ an element of multiplicative order 3 we list the elements of $\mathcal{P}$ in Table 1.

The proof of the following statements is omitted.

Proposition 1. *Let C_φ be a $[10, 5]$ code over $\mathcal{P}$, self-dual under the orthogonality condition (3), such that $E_\sigma(C)$ is a code with minimum distance at least*

Table 1: The field $\mathcal{P} \cong \mathbb{F}_{16}$

e	01111	α	11000	α^2	10100
α^3	11110	α^4	10001	α^5	01001
α^6	11101	α^7	00011	α^8	10010
α^9	11011	α^{10}	00110	α^{11}	00101
α^{12}	10111	α^{13}	01100	α^{14}	01010

10. Then the generator matrix of C_φ in standard form is

$$G_\varphi = \begin{pmatrix} e & 0 & 0 & 0 & 0 & a_{16} & a_{17} & a_{18} & a_{19} & a_{1,10} \\ 0 & e & 0 & 0 & 0 & a_{26} & a_{27} & a_{28} & a_{29} & a_{2,10} \\ 0 & 0 & e & 0 & 0 & a_{36} & a_{37} & a_{38} & a_{39} & a_{3,10} \\ 0 & 0 & 0 & e & 0 & a_{46} & a_{47} & a_{48} & a_{49} & a_{4,10} \\ 0 & 0 & 0 & 0 & e & a_{56} & a_{57} & a_{58} & a_{59} & a_{5,10} \end{pmatrix}, \tag{4}$$

$a_{1i} \in \{0, e, \delta, \delta^2\}$, $i = 6, \ldots 10$, $a_{j6} \in \{0, e, \delta, \delta^2\}$, $j = 1, \ldots 6$. *Furthermore* $(a_{16}, a_{17}, a_{18}, a_{19}, a_{1,10})$ *is one of the following vectors* $(0, e, e, \delta, \delta^2)$, (e, e, e, e, e), $(e, \delta, \delta, \delta, \delta)$, $(e, \delta, \delta, \delta^2, \delta^2)$, $(e, e, e, \delta, \delta)$.

A computer program for computing all possible generator matrices from Proposition 1, using also the orthogonality condition (3), was constructed. The result is the following.

Theorem 3. *There exist exactly 56 inequivalent* $[10, 5]$ *codes over P such that $E_\sigma(C)^*$ is a code with minimum distance at least 10. All codes can be obtained using* $(e, \delta, \delta, \delta, \delta)$ *as* $(a_{16}, \ldots, a_{1,10})$ *for the first row in G_φ.*

Denote the generator matrices of the codes from Theorem 3 by H_i, $i = 1, \ldots, 56$. The elements $a_{26}, \ldots, a_{5,10}$ for the matrices H_i are listed in Table 4, where the hexadecimal $h = 0, \ldots e$ denote α^h, whereas f denotes the zero of $\mathcal{P}$.

3 Binary self-dual $[52, 26, 10]$ codes with an automorphism of order 5

Let C be a binary self-dual $[52, 26, 10]$ code, possessing an automorphism of order 5. According to [4, Table 2] the possibilities for the cycle structure of the automorphism of order 5 is to be of type $5 - (10, 2)$, i.e.

$$\sigma = (1, 2, \ldots, 5)(6, 7, \ldots, 10) \ldots (46, 47, \ldots, 50).$$

According to Theorem 2 the subcode C_π is a binary self-dual $[12, 6, \geq 2]$ code. There are three such codes, namely $6i_2$, $2i_2 + e_8$, and d_{12} [5] with generator

Table 2: Generators elements of H_i, $i = 1, \ldots, 56$

H_1 00028007ef08d540953e	H_2 00028007ef5262859fc7	H_3 00028007ef5617558bf1
H_4 00028007efa02e1a5d38	H_5 00028014d751a4f52b9b	H_6 000280157203b080fe46
H_7 0002801572a1c82ae3f6	H_8 0002801572a2438aa1d9	H_9 00028016915191252e4f
H_{10} 00028016915af3c5e4c7	H_{11} 0002801691a137dae2d9	H_{12} 0002801691a20e1aabb0
H_{13} 00028019fb03ebc0fc15	H_{14} 00028019fb51bd352628	H_{15} 00028019fb5a14f5ef5d
H_{16} 00028019fba182caec4b	H_{17} 00028019fba2ed9aa055	H_{18} 0002802715a5d38ab2a3
H_{19} 00028028aaa56f6ab3e1	H_{20} 0002802d8d51ea95a4f1	H_{21} 0002802d8d529005ef5d
H_{22} 0002802d8da572cab867	H_{23} 0002803b08589285c0e6	H_{24} 0002803b08a0a55a84b0
H_{25} 0002803b08acb9fae8ca	H_{26} 0002803ebc507845e4c7	H_{27} 0002803ebca02e1a8eca
H_{28} 0002803ebcac182aea0e	H_{29} 0002803f54a0ccaa812c	H_{30} 00028056bc5290058ee6
H_{31} 00028056bc5648459fc7	H_{32} 00028069aa54b6a5f6d3	H_{33} 00028069aaa084babc9f
H_{34} 00069002ce087fc09470	H_{35} 00069002cea0c6da59e4	H_{36} 00069014eb082aa0d714
H_{37} 000690160da13beae201	H_{38} 000690160da202aaab32	H_{39} 0006901961a2e01aa055
H_{40} 00069028aa51b8f5a8dc	H_{41} 0006902d3f529005ef24	H_{42} 0006903bceacbe4ae86d
H_{43} 0006903e95a022aa8e6d	H_{44} 000690be14a42dfaae8c	H_{45} 0016d00a435671558fb1
H_{46} 0016d00c2e02ba4067a3	H_{47} 0016d01725a1f87aed86	H_{48} 0016d01ae808ea10d610
H_{49} 0016d01c0aa15b6aea0e	H_{50} 0016d0e1b4a1f87aaa5f	H_{51} 001ac01ac05a7235ef42
H_{52} 012570bf915053c51405	H_{53} 015cf0d2d8563385b5f7	H_{54} 5012d530b959d545b2c5
H_{55} 501455305c554105c503	H_{56} 501455305cadd0aaf5dd	

matrices

$$B_1 = \begin{pmatrix} 100000100000 \\ 010000010000 \\ 001000001000 \\ 000100000100 \\ 000010000010 \\ 000001000001 \end{pmatrix}, B_2 = \begin{pmatrix} 100000100000 \\ 010000010000 \\ 001000000111 \\ 000100001011 \\ 000010001101 \\ 000001001110 \end{pmatrix}, B_3 = \begin{pmatrix} 100000100011 \\ 010000010011 \\ 001000001011 \\ 000100000111 \\ 000010111110 \\ 000001111101 \end{pmatrix},$$

respectively.

In these three codes we have to arrange 10 of the coordinate positions $\{1, \ldots, 12\}$ to be the cycle positions X_c and 2 to be the fixed points X_f, in such a way, that the minimum distance of $F_\sigma = \pi^{-1}(C_\pi)$ is at least 10. It is obvious that any choice of two fixed coordinates in B_1 will lead to a word with weight 2 or 6. After calculating all subcodes F_σ for each of the two remaining codes we have three different generators. Denote $G_1 = B_2$, $G_2 = B_3$, and G_3 – the matrix B_3 with columns permuted by $(10, 11)$.

We have constructed the two direct summands for the code C and next we have to attach them together. Let the subcode $E_\sigma(C)^*$ is fixed as generated by H_j, $j = 1, \ldots, 56$. We have to consider different possibilities for the second subcode $F_\sigma(C)$ with generator matrix G_i, $i = 1, 2, 3$. Let St_i, $i = 1, 2, 3$ be the subgroup of symmetric group S_{10} consisting of all permutations on the first ten coordinates, which are induced by an automorphism of the code generated by

Table 3: Order of automorphism groups for $[52, 26, 10]$ codes

$\lvert\mathrm{Aut}(C)\rvert$	5	10	50	150
#	18208	566	2	1

G_i.

For a permutation $\tau \in S_{10}$, denote by $C^{\tau}_{i,j}$, $i = 1, 2, 3$, $j = 1, \ldots, 56$ the $[52, 26]$ self-dual code determined by the matrix G_i, as a generator for $F_\sigma(C)$ and H_j with columns permuted by τ as a generator matrix for $E_\sigma(C)$. It is easy to see that if τ_1 and τ_2 belong to one and the same right coset of S_{10} to G_i, then the codes $C^{\tau_1}_{i,j}$ and $C^{\tau_2}_{i,j}$ are equivalent. We need only to consider $\tau \in S_{10}$ from the right transversal T_i, $i = 1, 2$ of S_{10} with respect to St_i, $i = 1, 2, 3$.

Case 1. F_σ **generated by** G_1**.** St_1 is a group of cardinality 384, generated by the permutations $(2, 8)(3, 6, 10, 5)$, $(2, 8)(3, 4, 5)(6, 10, 9)$, $(3, 10)(4, 9)(5, 6)$, $(1, 2)(3, 10)(4, 9)(5, 6)(7, 8)$. The transversal T_1 have 9450 elements. There are exactly 10486 inequivalent codes with weight enumerator $W_{52,2}$: 9881 with $\beta = 0$; 604 with $\beta = 5$; and one code with $\beta = 10$.

Remark: The code with $\beta = 10$ is generated by H_{42} and G_1 permuted by $(1, 2, 6, 8, 10, 3)(5, 7)$. This code have automorphism group of order 5.

Case 2. F_σ **generated by** G_2**.** Then $St_2 = \langle$(5,6),(4,5)(6,10),(3,4)(9,10), (2,3)(8,9), (1,2)(7,8)$\rangle$ have 3840 elements. So the transversal T_2 have 945 elements. There exist exactly 147 inequivalent codes all with weight enumerator $W_{52,1}$.

Case 3. F_σ **generated by** G_3**.** $St_3 = \langle$(2,8)(3,6,9,5),(1,2,3,7,8,9)(4,10)(5,6)$\rangle$ is a group with 384 elements, $|T_3| = 9450$. We constructed exactly 8144 inequivalent codes. Their weight enumerator is $W_{52,2}$: 7624 codes for $\beta = 2$, and 520 codes for $\beta = 7$.

Proposition 2. *There are exactly 18777 inequivalent binary* $[52, 26, 10]$ *self-dual codes having an automorphism of type* $5 - (10, 2)$*. One of these codes have weight enumerator* $W_{52,2}$ *for* $\beta = 10$*.*

Theorem 4. *There exists an optimal binary self-dual* $[52, 26, 10]$ *code with weight enumerator* W *if and only if* $W = W_{52,2}$ *in* (2) *with* $\beta \in [0..12]$, $\beta \neq 11$ *or* W *is given by* (1)*.*

We list the order of the automorphism groups of all constructed codes in Table 3 and their weight enumerators in Table 4. The two codes with an automorphism group of size 50 constructed here are known. They are the pure double-circulant self-dual codes $P_{50,1}$ and $P_{50,2}$ from [2, Table 2]. All other 268 codes are new.

Table 4: Weight enumerators of all $[52, 26, 10]$ codes

#	A_{10}	A_{12}	$W_{52,i}$	β
147	250	7980	$W_{52,1}$	-
9881	442	6188	$W_{52,2}$	0
7624	410	6316	$W_{52,2}$	2
604	362	6508	$W_{52,2}$	5
520	330	6636	$W_{52,2}$	7
1	282	6828	$W_{52,2}$	10

References

[1] St. Bouyuklieva, M. Harada, A. Munemasa, Restrictions on the weight enumerators of binary self-dual codes of length $4m$, *Proc. Int. Workshop OCRT*, White Lagoon, Bulgaria, 40–44, 2007.

[2] M. Harada, T.A. Gulliver, H. Kaneta, Classification of extremal double circulant self- dual codes of length up to 62, *Discrete Math.*, **188**, pp. 127–136, 1998.

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

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

[5] W.C. Huffman, V. Pless, Fundamentals of error correcting codes, *Cambridge University Press* (2003).

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

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

[8] N. Yankov, New optimal $[52, 26, 10]$ self-dual codes, *to appear in Designs, Codes and Cryptography*, DOI: 10.1007/s10623-012-9639-9