On the Classification of [66, 33, 12] Binary Self-dual Codes with an Automorphism of Order 11 with 6 Cycles [1]

Nikolay Yankov

Abstract: *We complete the classification of all optimal binary self-dual codes of length 66 that have an automorphism of order 11 with 6 cycles. Using a method for constructing and classifying binary self-dual codes with an automorphism of odd prime order p we give all [66, 33, 12] binary self-dual codes with such an automorphism for p = 11. Many of the codes we obtain have new values of the parameters in their respective weight enumerators.*

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.

The codes with the largest possible minimum weight among all self-dual codes of a given length are named optimal self-dual codes. 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. [1], [2]) 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 σ be an automorphism of C of order p for an odd prime p. Without loss of generality we can assume that

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

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.

Lemma 1 [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.

[1] This paper is supported by Shumen University under Grant RD-08-234/12.03.2014.

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

Lemma 2 [1] 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

$$\phi(v \mid \Omega_i) = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1}, \text{ for } 1 \le i \le c. \qquad \textbf{(2)}$$

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

Theorem 1 [3] 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 $(u,v) = \sum_{i=0}^{c} u_i v_i^{2(p-1)/2}$, where $u = (u_1, \ldots, u_c)$, $v = (v_1, \ldots, v_c) \in P^c$.

Theorem 2 [4] 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 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.

HERMITIAN [6,3] CODES OVER F_{1024}

By Theorem 1 since 2 is a primitive root modulo $p = 11$ we can conclude that the $\phi(E_\sigma(C))$ is a Hermitian $[6, 3, \ge 3]$ self-dual code over the set of all even-weight polynomials in $F_2[x]/\langle x^{11} - 1\rangle$ under the inner product

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

Furthermore $P \cong F_{1024} = \{0, x^i \delta^j \mid 0 \le i \le 10, 0 \le j \le 92\}$, for $\delta = (x + x^3 + x^5 + x^8 + x^9 + x^{10})^{11}$.

The next theorem is proved in [5].

Theorem 3 [5] Up to equivalence there are 31611 codes over P such that $\phi^{-1}(C_\phi)$ generates a binary self-orthogonal [66, 30] code with minimum distance 12.

All codes have generator matrix of the following type: $A=\begin{pmatrix} e & 0 & 0 & t_1 & t_2 & t_3 \\ 0 & e & 0 & t_4 & t_5 & t_6 \\ 0 & 0 & e & t_7 & t_8 & t_9 \end{pmatrix}$, where $t_i \in \{0, \delta^j, 0 \le j \le 92\}$, $i = 1,\ldots,4, 7$; $t_j \in P$, $j = 5,6,8,9$.

We list the cardinality of the automorphism groups of all constructed codes in table 1.

Table 1. The order of the automorphism groups for $\phi^{-1}(C_\phi)$

$\lvert \mathrm{Aut}(C) \rvert$	11	22	44	55	66	110	132	264	550	660	6600
number of codes	28672	2738	141	6	39	3	6	3	1	1	1

We have computed the first subcode $E_\sigma(C)$ in Theorem 3. Let us fix the E_σ part of

$$\mathrm{gen}\, C = \begin{pmatrix} \mathrm{gen}\, E_\sigma \\ \mathrm{gen}\, F_\sigma \end{pmatrix} \qquad \textbf{(4)}$$

and consider all permutation of the 11-cycles in $F_\sigma(C)$ that can generate different binary code C. Assume that we have a generator matrix B of a [12,6] binary code that we can use in (4) substituting $\mathrm{gen}\, F_\sigma = \pi^{-1}(B)$. For a permutation $\tau \in S_6$ denote by C_τ the self-dual code determined by the matrix (4) where as the generator matrix for F_σ we use $\tau(B)$. We fix the Hermitian part E_σ and consider the generator matrix of C is (4) for all $\tau \in S_6$.

For a [66, 33, 12] binary self-dual code there are three possible form of the weight enumerator:

$$W_{66,1} = 1 + 1690y^{12} + 7990y^{14} + 302705y^{16} + 867035y^{18} + \ldots,$$

$$W_{66,2} = 1 + (858 + 8\beta)y^{12} + (18678 - 24\beta)y^{14} + (201201 - 48\beta)y^{16} + \ldots,$$

where $0 \le \beta \le 778$ and

$$W_{66,3} = 1 + (858 + 8\beta)y^{12} + (18166 - 24\beta)y^{14} + (205809 - 48\beta)y^{16} + \ldots,$$

where $14 \le \beta \le 756$.

Codes exist with $W_{66,1}$; with $W_{66,2}$ for $\beta = 0$, 2, 3, 5, 6, 8, …, 11, 14, …, 18, 20, …, 29, 31, 32, 33, 35, 36, 37, 38, 40, …, 54, 56, 59, 60, 62, …, 69, 71, …, 74, 76, 77, 78, 80, 83, 86, 87, 92 and with $W_{66,3}$ for $\beta = 28,33,34,54,56,\ldots,59,62$ and 66 (see [6]-[8]).

In order to find all different matrices B generated by the singly-even code we have to choose a splitting of the set of coordinates $\{1,2,\ldots,6\}$ into two disjoint sets X_c – the cycle coordinates and X_f – the fixed coordinates in such a way that the minimum distance of $F_\sigma(C)$ is at least 12. By Theorem 1 the subcode C_π is the unique [6, 3] binary self-dual code $3i_2$ with generator matrix $G = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$. Since we have 6 cycles and 6 coordinate positions it follows that $X_c = \{1,\ldots,6\}$, $X_f = \varnothing$ and there is a unique generator matrix $B = \pi^{-1}(G)$.

By calculation all codes C_π for $\pi \in S_6$ we have the following result.

Theorem 4 Up to equivalence there exist exactly 5122 binary [66, 33, 12] self-dual codes having an automorphism of type 11-(6, 0).

All constructed codes have weight enumerator $W_{66,2}$ for $\beta = 11k$, $k = 0,\ldots,8$. We list the values of β and the order of the automorphism groups of all constructed codes in Table 2.

Table 2. The parameters of [66, 33, 12] codes all with $W_{66,2}$

β	number of codes	|Aut(C)|					
		11	22	66	220	330	660
0	317	300	15	1		1	
11	1044	1036	8				
22	1660	1633	26		1		
33	1229	1221	8				
44	600	587	13				
55	200	197	3				
66	60	58	1				1
77	11	9	2				
88	1	1					

The values $\beta = 55,77$ and 88 were previously not known so we list the generators for a code with every new value in Table 3.

Table 3. The generators of some of the new [66, 33, 12] codes

β	$t_1,t_2,\ldots,t_9$	support of C_π
55	$0,\ \delta,\ \delta^{20},\ \delta^2,\ x^9,\ x^9\delta^{43},\ \delta^{40},\ x^9\delta^{86},\ x^9\delta^{36}$	{1,4}, {2,5}, {3,6}
77	$0,\ \delta,\ \delta^{20},\ \delta^8,\ x^3\delta^5,\ x^3\delta^{48},\ \delta^{67},\ x^3\delta^{70},\ x^3\delta^{20}$	{1,4}, {2,5}, {3,6}
88	$\delta^0,\ \delta^3,\ \delta^{34},\ \delta^{21},\ x^8\delta^{37},\ x^4\delta^{42},\ \delta^{52},\ x^7\delta^{59},\ x^8\delta^{38}$	{1,5}, {2,6}, {3,4}

Note that the codes with |Aut(C)|=66, 330 and 660 are the double circulant codes from [9].

REFERENCES

[1] 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.

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

[3] 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.

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

[5] Yankov N., M. Nikolova, M.H. Lee, Note on the binary self-dual codes with an automorphism of order 11, Proceedings of the XXI International Workshop on Multimedia Signal Processing and Transmission, pp. 105-109, 2014.

[6] Tsai H.P., P.Y. Shih, R.Y. Wu, W.-K. Su, C.H. Chen, Construction of Self-Dual Codes, IEEE Trans. Inform. Theory, vol. 54(8), pp. 3826-3831, 2008.

[7] Harada M., T. Nishimura, and R. Yorgova, New Extremal Self-Dual Codes of Length 66, Mathematica Balkanica (N. S.), vol. 21, no. 1-2, pp. 113-121, 2007.

[8] Karadeniz S. and B. Yildiz, New extremal binary self-dual codes of length 66 as extensions of self-dual codes over R_k, Journal of the Franklin Institute, vol. 350, pp. 1963-1973, 2013.

[9] Gulliver T.A. and M. Harada, Classification of extremal double circulant self-dual codes of lengths 64 to 72, Des. Codes Cryptogr., vol. 13, pp. 257-269, 1998.

ABOUT THE AUTHORS

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