SELF-DUAL CODES OF LENGTH 62 WITH AN AUTOMORPHISM OF ORDER 31[1]

NIKOLAY I. YANKOV AND RADKA P. RUSSEVA

In this survey we use a method for constructing binary self-dual codes under the presumption that they posses automorphism of odd prime order. We apply the method to classify, up to equivalence, all optimal [62, 31, 12] binary self-dual codes possessing a fixed points free automorphism with two cycles of length 31. It turns out that no such codes exist.

KEY WORDS: self-dual codes, automorphisms, optimal codes

1. Introduction

A *linear* $[n,k]$ code C is a k-dimensional subspace of the vector space $GF(q)^n$, where $GF(q)$ 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 codewords of C, and C is called a $[n,k,d]$ code.

A matrix which rows form a basis of C is called the *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] proved a 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. We say that an automorphism is of *type* $p-(c, f)$ if it has order p and when decomposed there are c independent p-cycles and f fixed points

In [8] a survey of the current status of the classification and enumeration of self-dual linear codes of small to moderate lengths over the fields $GF(2)$, $GF(3)$, and $GF(4)$ and the rings $\mathbb{Z}_4$, $GF(2) + uGF(2)$, and $GF(2) + vGF(2)$ was performed. In Table 2 of the paper under length $n=62$ the following possible automorphism types are listed open: 31-(2,0), 7-(8,6), 5-(10,12), 5-(12,2), 3-(16, 14), 3-(18, 8), 3-(20,2). We concentrate on the former case and we state.

Main Theorem – There does not exists an optimal singly-even [62, 31, 12] binary self-dual code possessing a fixed points free automorphism with two cycles of length 31.

[1] This work is supported by Shumen University under Project RD-05-274/15.03.2012

2. Self-dual codes with an automorphism of odd prime order

Huffman and Yorgov (cf. [2] – [4]) developed a method for constructing binary self-dual codes with an automorphism of odd prime order. We will give a brief description of the method as well as some important theorems.

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

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

and denote by $\Omega_1, \ldots, \Omega_c$ the cycles of length *p* and by $\Omega_{c+1}, \ldots, \Omega_{c+t}$ the fixed points. Thus σ is of type $p-(c, f)$ and $cp + f = n$.

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

Lemma 1 The self-dual code C is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$, and these subcodes have dimensions $\frac{1}{2}(c+f)$ and $\frac{1}{2}c(p-1)$, respectively.

Obviously $v \in F_\sigma(C)$ iff $v \in C$ and *v* is constant on each cycle. Let $\pi : F_\sigma(C) \to GF(2)^{c+f}$ 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*. Consider for $v \in E_\sigma(C)$ each $v \mid \Omega_i = (a_0, a_1, \ldots, a_{p-1})$ as a polynomial

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

So each $v \mid \Omega_i = (v_0, v_1, \cdots, v_{p-1})$ correspond to a polynomial $v_0 + v_1 x + \ldots + v_{p-1} x^{p-1}$ from P, where P is the set of even-weight polynomials in the factor ring $\mathrm{GF}(2)[x]/\langle x^p - 1\rangle$. Thus we obtain the map

$$\varphi : E_\sigma(C)^* \to P^c .$$

P is a cyclic code of length p with generator polynomial $x-1$. It is known that $\varphi(E_\sigma(C)^*)$ is a submodule of the P-module 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) $C_\varphi = \varphi(E_\sigma(C)^*)$ 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 $u = (u_1, \ldots, u_c)$, $v = (v_1, \ldots, v_c) \in P^c$.

Let

$$x^p - 1 = (x-1)h_1(x)\ldots h_s(x),$$

where $h_1(x),\ldots,h_s(x)$ are irreducible binary polynomials. If $g_j(x) = (x^p-1)/h_j(x)$, and $I_j = \langle g_j(x)\rangle$ is the ideal in GF(2)$[x]/\langle x^p-1\rangle$, generated by $g_j(x)$, then I_j is a field with $2^{deg(h_j(x))}$ elements, $j = 1,2,\ldots,s$, and $P = I_1 \oplus I_2 \oplus \cdots \oplus I_s$ (see [5]).

Lemma 2 [6] Let $M_j = \{u \in \varphi(E_\sigma(C)^*) \mid u_i \in I_j, i = 1,2,\ldots,c\}$, $j = 1,2,\ldots,s$. Then

1) M_j is a linear space over I_j, $j = 1,2,\ldots,s$;

2) $C_\varphi = \varphi(E_\sigma(C)^*) = M_1 \oplus M_2 \oplus \cdots \oplus M_s$ (direct sum of P-submodules);

3) If C is a self-dual code, then $\sum_{j=1}^{s} \dim_{I_j} M_j = cs/2$.

3. Codes with an automorphism of order 31

In this section we will use the method described in Section 2 for binary self-dual [62, 31, 12] codes. Using [8] for the weight enumerator of an extremal self-dual code of length 62 we have two forms

$$W_{62,1} = 1 + 2308y^{12} + 23767y^{14} + 279405y^{16} + 1622724y^{18} + \cdots,$$

and

$$W_{62,2} = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + (255533 + 96\beta)y^{16} + \cdots,$$

where $0 \le \beta < 62$.

Only codes with weight enumerator $W_{62,2}$ where $\beta = 0,9,10,$ and 15 are known (see [8], [9]).

Let *C* be a binary singly-even self-dual [62, 31, 12] code possessing an automorphism of type 31-(2, 0). According to Theorem 1, $C_\pi = \pi(F_\sigma(C))$ is a $[2,1,2]$ binary self-dual code. There exists a unique such code denoted by i_2 [5]. So we have the following.

Lemma 3 – The only possible generator matrix for the code C_π is $G = (11)$.

In [6] Yorgov studied doubly-even self-dual [64, 32, 12] codes possessing an automorphism of order 31 and constructs exactly 38 such codes. Unfortunately, some of these codes are equivalent. By out calculation there are exactly 36 inequivalent codes. Since the automorphism in Yorgov's paper is of type 31-(2,2) and the minimum distance $d = 12$ is the same as for *C*, these 36 codes can be used to construct the subcode C_φ. For completeness we give more detailed description of these codes and also we list their generator matrices in the Appendix.

According to Lemma 1, we have $C = \pi^{-1}(C_\pi) \oplus \varphi^{-1}(C_\varphi)$. The numbers of codewords of weight *2k* in *C*, i.e. A_{2k}, $k = 5,6,7,8$ for all resulted 36 codes are listed in Table 1. We have $A_{10} \neq 0$ for all these codes and thus the Main Theorem is proved. The codes have the following order of their automorphism group: 31 for 3 codes, 62 for 25 codes, 155 for 2 codes, 310 for 5 codes and 744000 for 1 code.

Table 1: The values of A_{10}, A_{12}, A_{14} and A_{16} of the constructed [62, 31] codes

# of codes	A_{10}	A_{12}	A_{14}	A_{16}
2	62	1922	27435	254913
3	93	1953	27125	254603
7	124	1984	26815	254293
3	155	2015	26505	253983
8	186	2046	26195	253673
1	186	4030	16275	259625
1	217	2077	25885	253363
9	248	2108	25575	253053
1	279	2139	25265	252743
1	372	2232	24335	251813

Appendix

Let $P, I_1, I_2, \ldots, I_6$ are binary cyclic codes of length 31 generated by the codewords given in Table 2.

Table 2: Generators of the cyclic codes

code	polynomial	codeword
P	$e(x)$	01111111111111111111111111111111
I_1	$e_1(x)$	10000101011101100011111100110100
I_2	$e_2(x)$	10010110011111000110111010100000
I_3	$e_3(x)$	10010011000010110101000011101111
I_4	$e_4(x)$	11111011100010101101000011001000
I_5	$e_5(x)$	11101100111000011010100100010011
I_6	$e_6(x)$	11101000100101011000011100110111

Using Theorem 1 we have that $P = I_1 \oplus I_2 \oplus \cdots \oplus I_6$ (a direct sum of minimal ideals). From Lemma 2 it follows that $C_\varphi = \varphi(E_\sigma(C)^*) = M_1 \oplus M_2 \oplus \cdots \oplus M_6$ (a direct sum of P-modules). Since $\dim \varphi(E_\sigma(C)^*) = 30$ it follows that $\dim_{I_1} M_1 + \dim_{I_2} M_2 + \cdots + \dim_{I_6} M_6 = 6.$

I. When $\dim_{I_j} M_j = 1$ and the weight of every nonzero codeword in M_j, $j = 1, \ldots, 6$ is equal to two.

Thus we have codes with generator matrix $A_{ij} = \begin{pmatrix} e_1 & e_1 \\ e_2 & e_2 \\ e_3 & x^i e_3 \\ e_4 & x^i e_4 \\ e_5 & x^j e_5 \\ e_6 & x^j e_6 \end{pmatrix}$, where $0 \le i, j \le 30.$

Only codes with parameters $i = 1$, $j = 0,1,2,3,4,5,7,8,9,10,15,16,25,26$ and 30; $i = 3$, $j = 0,1,2,10$ and 27; $i = 9$, $j = 2$ and 23, are optimal and inequivalent.

II. When $\dim_{I_j} M_j = 1, j = 1,\ldots,6$ and there is a weight one codeword in C_φ.

In this case codes are generated by the matrix $B_j = \begin{pmatrix} e_1 & 0 \\ 0 & e_2 \\ e_3 & e_3 \\ e_4 & e_4 \\ e_5 & x^j e_5 \\ e_6 & x^j e_6 \end{pmatrix}$. Only when $j = 0,3,5,11,$ and 15 the generated codes are inequivalent and optimal. There are also two codes with generator matrices $\begin{pmatrix} e_1 & 0 \\ 0 & e_2 \\ e_3 & 0 \\ 0 & e_4 \\ e_5 & e_5 \\ e_6 & e_6 \end{pmatrix}$ and $\begin{pmatrix} e_1 & 0 \\ 0 & e_2 \\ e_3 & e_3 \\ e_4 & e_4 \\ e_5 & 0 \\ 0 & e_6 \end{pmatrix}$.

III. When for some $1 \le j \le 6$ we have $\dim_{I_j} M_j = 2, j = 1,\ldots,6$ and there is a weight one codeword in C_φ. There are seven inequivalent and optimal codes generated by the matrices

$$\begin{pmatrix} e_1 & 0 \\ 0 & e_1 \\ e_3 & e_3 \\ e_4 & e_4 \\ e_5 & xe_5 \\ e_6 & xe_6 \end{pmatrix}, \begin{pmatrix} e_1 & 0 \\ 0 & e_1 \\ e_3 & e_3 \\ e_4 & e_4 \\ e_5 & x^3 e_5 \\ e_6 & x^3 e_6 \end{pmatrix}, \begin{pmatrix} e_1 & 0 \\ 0 & e_1 \\ e_3 & e_3 \\ e_4 & e_4 \\ e_5 & x^5 e_5 \\ e_6 & x^5 e_6 \end{pmatrix}, \begin{pmatrix} e_1 & 0 \\ 0 & e_1 \\ e_3 & 0 \\ 0 & e_4 \\ e_5 & e_5 \\ e_6 & e_6 \end{pmatrix}, \begin{pmatrix} e_1 & 0 \\ 0 & e_1 \\ e_3 & e_3 \\ e_4 & e_4 \\ e_5 & 0 \\ 0 & e_6 \end{pmatrix}, \begin{pmatrix} e_1 & 0 \\ 0 & e_1 \\ e_3 & 0 \\ 0 & e_3 \\ e_5 & e_5 \\ e_6 & e_6 \end{pmatrix}, \text{and } \begin{pmatrix} e_1 & 0 \\ 0 & e_1 \\ e_4 & 0 \\ 0 & e_4 \\ e_5 & e_5 \\ e_6 & e_6 \end{pmatrix}.$$

REFERENCES**:**

1. **Conway J.H. and Sloane N.J.A.**, A new upper bound on the minimal distance of self-dual codes. // IEEE Transactions on Information 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 Transactions on Information 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 Transactions on Information Theory, vol. 33, pp. 77-82, 1987.
5. **Pless V. and Huffman W.C.**, Handbook of Coding Theory. // Elsevier, Amsterdam, 1998.
6. **Yorgov V.Y.**, Binary self-dual codes with an automorphism of odd order. // Problems Information Transmission, vol. 4, pp. 13--24 (in Russian), 1983 .
7. **Yorgov V.Y.**, The extremal codes of length 42 with automorphism of order 7. // Discrete Mathematics, vol 19, pp. 201-213, 1998.
8. **Huffman W.C.**, On the classification and enumeration of self-dual codes. // Finite Fields and Their Application, vol. 11, pp. 451-490, 2005.
9. **Russeva R. and Yankov N.**, On binary self-dual codes of lengths 60, 62, 64 and 66 having an automorphism of order 9 // Designs, Codes and Cryptography, vol. 45, pp. 335-346, 2007.