ON BINARY SELF-DUAL CODES OF LENGTH 62 WITH AN AUTOMORPHISM OF ORDER 7

Nikolay Yankov

We classify up to equivalence all optimal binary self-dual \([62,31,12]\) codes having an automorphism of order 7 with 8 independent cycles. Using a method for constructing self-dual codes via an automorphism of odd prime order, we prove that there are exactly 8 inequivalent such codes. Three of the obtained codes have weight enumerator, previously unknown to exist.

1. Introduction. Let \(F_q\) be a finite field with \(q = p^r\) elements. A linear \([n,k]_q\) code \(C\) is a \(k\)-dimensional subspace of \(F_q^n\). We call the codes binary if \(q = 2\). The number of the nonzero coordinates of a vector in \(F_q^n\) is called its weight. An \([n,k,d]_q\) code is an \([n,k]_q\) linear code with minimal nonzero weight \(d\).

Let \((u,v) = \sum_{i=1}^{n} u_i v_i \in F_2\) for \(u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in F_2^n\) be the inner product in \(F_2^n\). Then, if \(C\) is a binary \([n,k]\) code, its dual \(C^\perp = \{u \in F_2^n \mid (u,v) = 0\text{ for all }v \in C\}\) is a \([n,n-k]\) binary code. If \(C \subseteq C^\perp\), then the code \(C\) is termed self-orthogonal, in case of \(C = C^\perp\), \(C\) is called self-dual. An even code is a binary code for which all codewords have even weight. All self-dual binary codes are even. In addition, some of these codes have all codewords of weight divisible by 4. These codes we call doubly-even; a self-dual code with some codeword of weight not divisible by 4 is named singly-even.

Two binary codes are equivalent if one can be obtained from the other by a permutation of the coordinate positions. The permutation \(\sigma \in S_n\) is an automorphism of \(C\), if \(C = \sigma(C)\). The set of all automorphisms of a code forms a group called the automorphism group \(\text{Aut}(C)\). If a code \(C\) have an automorphism \(\sigma\) of odd prime order \(p\), where \(\sigma\) has \(c\) independent \(p\)-cycles and \(f\) fixed points, then \(\sigma\) is said to be of type \(p-(c,f)\).

A duo is any set of two coordinate positions of a code. A cluster is a set of disjoint duos such that any union of two duos is the support of a vector of weight 4 in the code. A \(d\)-set for a cluster is a subset of coordinates such that there is precisely one element of each duo in the \(d\)-set. A defining set for a code will consist of a cluster and a \(d\)-set provided the code is generated by the weight-4 vectors arising from the cluster and the vector whose support is the \(d\)-set.

In this report we investigate the existence of new extremal self-dual codes. We apply a method for constructing such codes, that posses an automorphism of odd prime order
developed by Huffman and Yorgov [4], [7]. In Section 2 we briefly describe the method and in Section 3 we classify all extremal singly-even [62, 31, 12] codes with an automorphism of order 7 with 8 independent cycles in its decomposition. Three of the obtained codes have new weight enumerator.

2. Construction method Let $C$ be a binary self-dual code of length $n$ with an automorphism $\sigma$ of order 7 with exactly $c$ independent 7-cycles and $f = n - 7c$ fixed points in its decomposition. We may assume that
\[
\sigma = (1, 2, \cdots, 7)(8, 9, \cdots, 17) \cdots (7(c - 1) + 1, 7(c - 1) + 2, \cdots, 7c),
\]
or that $\sigma$ have new weight enumerator.

Denote the cycles of $\sigma$ by $\Omega_1, \Omega_2, \ldots, \Omega_f$, and the fixed points by $\Omega_{c+1}, \ldots, \Omega_{c+f}$. Let
\[
F_\sigma(C) = \{ v \in C \mid \sigma v = v \} \quad \text{and} \quad E_\sigma(C) = \{ v \in C \mid \wt(v|\Omega_i) \equiv 0 (\text{mod } 2), i = 1, \ldots, c + f \},
\]
where $v|\Omega_i$ is the restriction of $v$ on $\Omega_i$.

**Theorem 1** [4]. Assume $C$ is a self-dual code. The code $C$ is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$. $F_\sigma(C)$ and $E_\sigma(C)$ are subspaces of dimensions $\frac{c+f}{2}$ and $\frac{c(p-1)}{2}$, respectively.

Clearly $v \in F_\sigma(C)$ 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 $v \in F_\sigma(C)$, then $(v\pi)_i = v_j$ for some $j \in \Omega_i, i = 1, 2, \ldots, c + f$.

**Theorem 2** [4], $\pi(F_\sigma(C))$ is a binary $[c + f, (c + f)/2]$ self-dual code.

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 $7c$. For $v$ in $E_\sigma(C)^*$ we let $v|\Omega_i = (v_0, v_1, \ldots, v_6)$ correspond to the polynomial $v_0 + v_1 x + v_6 x^6$ from $P$, where $P$ is the set of even-weight polynomials in $F_2[x]/(x^7 - 1)$. Thus we obtain the map $\varphi : E_\sigma(C)^* \to P^c$. $P$ is a cyclic code of length 7 with generator polynomial $x + 1$ and check polynomial $1 + x + \cdots + x^6$.

It is known [4], [8] that $\varphi(E_\sigma(C)^*)$ is a $P$-module and for each $u, v \in \varphi(E_\sigma(C)^*)$ it holds
\[
(1) \quad u_1(x)v_1(x^{-1}) + u_2(x)v_2(x^{-1}) + \cdots + u_c(x)v_c(x^{-1}) = 0.
\]

Denote $h_1(x) = x^3 + x^2 + 1$ and $h_2(x) = x^3 + x^2 + 1$. As $x^6 + x^5 + \cdots + x + 1 = h_1(x)h_2(x)$, we have $P = I_1 \oplus I_2$, where $I_j$ is an irreducible cyclic code of length 7 with parity-check polynomial $h_j(x), j = 1, 2$. Thus $M_j = \{ u_i \in \varphi(E_\sigma(C)^*) \mid u_i \in I_j, i = 1, 2 \}$ is code over the field $I_j, j = 1, 2$. It is known [8] that $\varphi(E_\sigma(C)^*) = M_1 \oplus M_2$ and $\dim M_1 = \dim M_2 = c$. The polynomials $e_1(x) = e_2(x) = x^6 + x^5 + x^4 + 1$ generate the ideals $I_1$ and $I_2$ defined above. Any nonzero element of $I_j = \{ 0, e_j, xe_j, \ldots, x^6e_j \}, j = 1, 2$ generates a binary cyclic [7, 3, 4] code. Since the minimal weight of the code $C$ is 12, every vector of $\varphi(E_\sigma(C)^*)$ must contain at least 3 nonzero coordinates.

The following result is a particular case of Theorem 3 from [7]:

**Theorem 3.** Let the permutation $\sigma$ 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 $t = 1, 2, \cdots, 6$ in $\varphi(E_\sigma(C)^*)$;

b) a multiplication of the $j$-th coordinate of $\varphi(E_\sigma(C)^*)$ by $x^{t_j}$ where $t_j$ is an integer, $0 \leq t_j \leq 6$, for $j = 1, 2, \cdots, c$.
c) a permutation of the first $c$ cycles of $C$;
d) a permutation of the last $f$ coordinates of $C$.

Since the transformation $x \rightarrow x^3$ from Theorem 3 a) interchanges $e_1(x)$ into $e_2(x)$ and vice versa, then we can assume, without loss of generality, that $\dim M_1 \leq \dim M_2$. Once chosen, the code $M_1$ determines $M_2$ and the whole $\varphi(E_\sigma(C)^*)$. Thus we can examine only $M_1$.

All possible weight enumerators of extremal self-dual codes of lengths 38 to 72 are known [2]. For the singly-even self-dual [62, 31, 12] code there are two possibilities:

$$W_{62.1} = 1 + 2308y^{12} + 23767y^{14} + 279405y^{16} + 1622272y^{18} + \cdots,$$

$$W_{62.2} = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + (255533 + 96\beta)y^{16} + \cdots,$$

where $0 \leq \beta \leq 93$. Thus far only codes with weight enumerator $W_{62.2}$ where $\beta = 0, 9, 10, 15$ are known [2], [5].

3. Codes with an automorphism of type 7-(8,6). Let $C$ be a binary self-dual [62, 31, 12] code having an automorphism of type $7 - (8, 6)$. According to Theorem 1, $\dim \varphi(E_\sigma(C)^*) = \dim M_1 + \dim M_2 = 8$, and $\varphi(E_\sigma(C)^*)$ is a code of length 8. All inequivalent self-orthogonal [8, 8, 3] codes over the set of all even-weight polynomials $P$ in $F_2[x]/(x^2 - 1)$ under the inner product (1) are constructed in [6]. There are exactly 271 codes when $\dim M_1 = 3$, and 1446 codes when $\dim M_1 = 4$. Denote by $H_j, j = 1, \ldots, 1717$ the self-orthogonal codes of length 8 constructed in [6].

According to Theorem 2 the code $\pi(F_\sigma(C))$ is a binary [14, 7, $\geq 2$] self-dual code. There are four such codes, namely $7i_2, 3i_2 \oplus e_8, i_2 \oplus d_{12}$, and $2e_7$ (see [3]).

Let $X_c$ and $X_f$ be the coordinates of the cycle and fixed positions, respectively. Since $d = 12$, every 2-weight vector in $\pi(F_\sigma(C))$ must have a support contained entirely in $X_c$. Thus the case $7i_2$ is obviously impossible. In the case $3i_2 \oplus e_8$ the three 2-weight vectors from $3i_2$ should take six out of the eight positions in $X_c$. We have to choose 2 cycle positions and 6 fixed points of the $e_8$ component, whereas the automorphism group of $e_8$ is 3-transitive, so taking a 4-weight vector $v$ we can fix 3 out of the 4 elements of its support in $X_c$ and then we have $wt(\pi^{-1}(v)) = 7.1 + 3 = 10 - a contradiction$.

Consider the case $\pi(F_\sigma(C)) \cong 2e_7$. This code have two clusters $Q_1 = \{1, 2\}, \{3, 4\}, \{5, 6\}$, $Q_2 = \{\{8, 9\}, \{10, 11\}, \{12, 13\}\}$, and two $d$-sets, $d_1 = \{1, 3, 5, 7\}, d_2 = \{8, 10, 12, 14\}$, that form a defining set. We have to arrange eight of the coordinate positions $\{1, \ldots, 14\}$ to be cycle positions $X_c$ and six to be fixed positions $X_f$. Since we are looking for a code with minimum distance $d = 12$, every vector with weight 4 in $C_\pi$ must have at least two elements of its support in $X_c$. The cluster $Q_1$ and the $d$-set $d_1$ generates $e_7$, so there are 7 codewords of weight 4 with supports $\{1, 2, 3, 4\}, \{1, 2, 5, 6\}, \{1, 3, 5, 7\}, \{1, 4, 6, 7\}, \{2, 3, 6, 7\}, \{2, 4, 5, 7\}$, and $\{3, 4, 5, 6\}$. The automorphism group of $e_7$ is 2-transitive, so w.l.g. we can assume $1, 2 \in X_c$. But the vector of weight 4 with support $\{3, 4, 5, 6\}$ has at least two cycle coordinates. So we can choose $\{1, 2, 3, 4\} \subset X_c, \{5, 6, 7\} \subset X_f$. After computing all $\binom{12}{7}$ possible choices for the remaining 3 fixed points, it turns out that all codes $F_\sigma(C)$ have minimal weight 10.

Consider the case $\pi(F_\sigma(C)) \cong i_2 \oplus d_{12}$. Every vector of weight two in this code has support in the cycle positions, so the positions corresponding to direct summand $i_2$ must be cycle. Also $d_{12}$ has a cluster $Q = \{1, 2\}, \{3, 4\}, \{5, 6\}, \{7, 8\}, \{9, 10\}, \{11, 12\}$ and $d$-set $\{1, 3, 5, 7, 9, 11\}$ so the six fixed coordinates $X_f$ cannot contain two duos or one duo and two points from disjoint duos. Thus $X_f$ contains six coordinates from all six different
proved the following

Proposition 1. Up to equivalence there is only one possible generator matrix

\[
G = \begin{pmatrix}
11000000 & 000000 \\
00010010 & 110000 \\
00001101 & 011000 \\
00001001 & 001100 \\
00101000 & 000110 \\
00100010 & 000011 \\
00000010 & 111110 \\
\end{pmatrix}
\]

for \(\pi(F_\sigma(C))\) in an optimal binary self-dual \([62, 31, 12]\) code having an automorphism of type \(7 - (8, 6)\).

Although we have constructed the two direct summands for the code \(C\), we have to attach them together. Let the subcode \(F_\sigma(C)\) is fixed as generated by the matrix \(G\) from Proposition 1. We have to consider all even equivalent possibilities for the second subcode \(E_\sigma(C)\).

Let \(G'\) be the subgroup of symmetric group \(S_8\) consisting of all permutations on the first eight coordinates, which are induced by an automorphism of the code generated by \(G\). Let \(S = \text{Stab}(G')\) be the stabilizer of \(G'\) on the set of the fixed points. We have that \(S = ((12), (34), (45), (56), (68), (38)(67))\). Let \(\tau \in S_8\) be a permutation. Denote by \(C_j^\tau\), \(j = 1, \ldots, 1717\) the \([62, 31]\) self-dual code determined by the matrix \(G\) as a generator for \(F_\sigma(C)\) and \(H_j\) with columns permuted by \(\tau\) as a generator matrix for \(E_\sigma(C)^*\). It is easy to see that if \(\tau_1\) and \(\tau_2\) belong to one and the same left coset of \(S_8\) to \(S\), then the codes \(C_j^{\tau_1}\) and \(C_j^{\tau_2}\) are equivalent. The set \(T = \{(2j)(1i) \mid 1 \leq i < j \leq 8\}\) is a left transversal of \(S_8\) with respect to \(S\). After calculating all codes \(C_j^\tau\), \(j = 1, \ldots, 1717\), \(\tau \in T\) we summarize the results as follows:

Theorem 4. There are exactly 8 inequivalent binary \([62, 31, 12]\) codes having an automorphism of type \(7 - (8, 6)\). The exist at least three codes with weight enumerator \(W_{62,2}\) for \(\beta = 16\).

Remark 1. All constructed codes have weight enumerator \(W_{62,2}\). Note that the value \(\beta = 16\) for \(W_{62,2}\) has not occurred up until now. For every obtained code we list in Table 1 the order of the automorphism group, the weight enumerator and all constructing

| Code | \(\varphi(E_\sigma(C))\) | \(u_1, \ldots, u_{16}\) | \(\tau\) | \(|\text{Aut}(C)|\) | \(A_{12}\) | \(A_{14}\) |
|------|----------------|------------------|---------|----------------|--------|--------|
| 2    | \(H_{11}\)  | \(B_{1,3}\)      | 0111202 | 132            | 42     | 1924   |
| 2    | \(H_{172}\)| \(B_{1,3}\)     | 1222467 | 132            | 42     | 1924   |
| 2    | \(H_{278}\)| \(B_{1,4}\)     | 00100244| 28             | 42     | 1924   |
| 2    | \(H_{1098}\)| \(B_{1,4}\)     | 000224750| 23             | 42     | 1924   |
| 2    | \(H_{1690}\)| \(B_{1,4}\)     | 02313564| (17)(28)       | 42     | 1924   |
| 16   | \(H_{1370}\)| \(B_{1,4}\)     | 01214555| 23             | 14     | 2372   |
| 16   | \(H_{1309}\)| \(B_{1,4}\)     | 01222052| (13)(25)       | 14     | 2372   |
| 16   | \(H_{1412}\)| \(B_{1,4}\)     | 01232226| (15)(26)       | 42     | 2372   |

Table 1. All binary self-dual \([62, 31, 12]\) codes with automorphism of type \(7 - (8, 6)\).
components. The subcode $E_\sigma(C)$ can be obtained using the following two matrices

$$B_{1,3} = \begin{pmatrix} e_1 & e_1 & e_1 & e_1 & e_1 & e_1 & e_1 & e_1 & e_1 \end{pmatrix}, \quad B_{1,4}^T = \begin{pmatrix} e_1 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 \end{pmatrix}.$$ 

In the column denoted by $u_1, \ldots$ the elements $0, e_1, \ldots, x^6e_1$ from $I_1$ are listed with numbers $0, 1, \ldots, 7$, respectively.

**Remark 2.** In the course of this research we have used $Q$-extensions [1] for computing minimal weight and automorphism groups. For computing the transversal we use the system for computational algebra $GAP$ v.4.

**REFERENCES**


Nikolay Ivanov Yankov
University of Shumen
Faculty of Mathematics and Informatics
115, Universitetska Str.
9700 Shumen, Bulgaria
e-mail: jankov_niki@yahoo.com
ДВОИЧНИ САМОДУАЛНИ КОДОВЕ С ДЪЛЖИНА 62
ПРИТЕЖАВАЩИ АВТОМОРФИЗЪМ ОТ РЕД 7

Николай Янков

Класифицирани са с точност до еквивалентност всички оптимални двоични само-
дуални [62, 31, 12] кодове, които притежават автоморфизъм от ред 7 с 8 незави-
сими цикъла при разлагане на независими цикли. Използвайки метода за конс-
труиране на самодуални кодове, притежаващи автоморфизъм от нечетен прост
ред е доказано, че съществуват точно 8 нееквивалентни такива кода. Три от
получените кодове имат тегловна функция, каквато досега не бе известно да
съществува.