SELF-DUAL CODES WITH AN AUTOMORPHISM OF ORDER 13

Nikolay Yankov and Damyan Anev
Faculty of Mathematics and Informatics
Shumen University, 9700 Shumen, Bulgaria

Müberra Gürel
Istanbul Aydin University
Istanbul, Turkey

(Communicated by Simon Litsyn)

Abstract. Using a method for constructing binary self-dual codes having an automorphism of odd prime order \( p \) we classify, up to equivalence, all singly-even self-dual \([78, 39, 14]\), \([80, 40, 14]\), \([82, 41, 14]\), and \([84, 42, 14]\) codes as well as all doubly-even \([80, 40, 16]\) codes for \( p = 13 \). The results show that there are exactly 1592 inequivalent binary self-dual \([78, 39, 14]\) codes with an automorphism of type \( 13 - (6, 0) \) and we found 6 new values of the parameter in the weight function thus increasing more than twice the number of known values.

As for binary \([80, 40]\) self-dual codes with an automorphism of type \( 13 - (6, 2) \) there are 162696 singly-even self-dual codes with minimum distance 14 and 195 doubly-even such codes with minimum distance 16. We also construct many new codes of lengths 82 and 84 with minimum distance 14. Most of the constructed codes for all lengths have weight enumerators for which the existence was not known before.

1. Introduction

Let \( \mathbb{F}_q \) be the finite field of \( q \) elements, for a prime power \( q \). A linear \([n, k]_q\) code \( C \) is a \( k \)-dimensional subspace of \( \mathbb{F}_q^n \). The elements of \( C \) are called codewords, and the (Hamming) weight of a codeword \( v \in C \) is the number of the non-zero coordinates of \( v \). We use \( \text{wt}(v) \) to denote the weight of a codeword. The minimum weight \( d \) of \( C \) is the minimum nonzero weight of any codeword in \( C \) and the code is called an \([n, k, d]_q\) code. A matrix whose rows form a basis of \( C \) is called a generator matrix of this code (denoted by \( \text{gen}(C) \)).

By \( O, I, J \) we denote the zero, identity and all-ones matrices, respectively.

For every \( u = (u_1, \ldots, u_n) \) and \( v = (v_1, \ldots, v_n) \) from \( \mathbb{F}_2^n \), \( u.v = \sum_{i=1}^{n} u_i v_i \) defines the inner product in \( \mathbb{F}_2^n \). The dual code of \( C \) is \( C^\perp = \{ v \in \mathbb{F}_2^n \mid u.v = 0, \forall u \in C \} \). If \( C \subset C^\perp \), \( C \) is called self-orthogonal, and if \( C = C^\perp \), we say that \( C \) is self-dual. We call a binary code self-complementary if it contains the all-ones vector. Every binary self-dual code is self-complementary.

A self-dual code is doubly-even if all codewords have weight divisible by four, and singly-even if there is at least one nonzero codeword of weight \( \equiv 2 \pmod{4} \). Self-dual doubly-even codes exist if and only if \( n \) is a multiple of eight.
The weight enumerator $W(y)$ of a code $C$ is defined as $W(y) = \sum_{i=0}^{n} A_i y^i$, where $A_i$ is the number of codewords of weight $i$ in $C$. We say that two linear codes $C$ and $C'$ are permutation equivalent if there is a permutation of coordinates which sends $C$ to $C'$. The set of coordinate permutations that maps a code $C$ to itself forms a group denoted by $\text{Aut}(C)$.

Rains [15] proved that the minimum distance $d$ of a binary self-dual $[n, k, d]$ code satisfies the following bound:

\begin{align}
    d &\leq 4\lfloor n/24 \rfloor + 4, \quad \text{if } n \not\equiv 22 \pmod{24}, \\
    d &\leq 4\lfloor n/24 \rfloor + 6, \quad \text{if } n \equiv 22 \pmod{24}.
\end{align}

Codes achieving this bound are called extremal. A self-dual code is called optimal if it has the highest minimum weight among all self-dual codes.

Optimal self-dual codes with an automorphism of odd prime order are a well studied subject. In fact all such codes are classified up to length 50 [18]. By Gilliver and Harada [8] there exist 5 extremal double circulant doubly-even self-dual codes of length 80 with an automorphism of order 13. The orders of automorphism groups of those codes are: 246680 for one code ($P_{80,1} = B_{80,5}$) which is both pure and bordered double circulant; 4 codes ($B_{80,1} - B_{80,4}$) have $|\text{Aut}(C)| = 78$. In [5] P. Gaborit and A. Otmani have constructed a $[78, 39, 14]$ self-dual code with an automorphism of order 13 with $W_{78,1}$ for $\alpha = 0, \beta = -26$.

R. Dontcheva and M. Harada in [3] have classified all doubly-even $[80, 40, 16]$ codes with an automorphism of order 19.

The extremal or optimal binary self-dual codes with an automorphism of order 13 with 4 cycles are classified in [19]. We continue the investigation of binary self-dual codes with an automorphism of order 13 with the next possible case, i.e. with 6 independent 13-cycles. We should note that St. Kapralov et al. in [14] have constructed 35 doubly-even $[80, 40, 14]$ codes with an automorphism of type 13-(6, 2) but give no classification.

By the Rains bound [1] we have $d \leq 16$ for binary self-dual codes of lengths 78 to 92. Let $C$ be an optimal binary self-dual $[2k, k, d]$ code for $39 \leq k \leq 46$ and $d = 16$ or 14. We assume that the code $C$ has an automorphism $\sigma$ of order 13 with $c = 6$ cycles and $f$ fixed points for $0 \leq f = 78 - 2k \leq 14$. By [21] if $f > c = 6$ we have $f \geq \sum_{i=0}^{(f-c)/2-1} \left\lceil \frac{d}{i^2} \right\rceil$, which for $d = 16$ and $k \geq 1$ gives $f \geq 16$. Therefore we have $f = 0, 2, 4$ or 6 and $39 \leq k \leq 42$.

The possible weight enumerators for extremal and optimal binary self-dual codes of lengths 72 $\leq n \leq 100$ are known from Steven Dougherty, T. Aaron Gulliver and Masaaki Harada [5]. Later in [11] some additional restrictions for the parameters are proved. Since as of now no singly-even $[2k, k, 16]$, $k = 39, 40, 41, 42$ codes are known we have calculated the possible weight enumerators for self-dual singly-even $[2k, k, 14]$, $k = 39, 40, 41, 42$ codes. For $[78, 39, 14]$ self-dual codes there are two possible weight enumerators:

\[
W_{78,1} = 1 + (3705 + 8\beta)y^{14} + (62244 + 512\alpha - 24\beta)y^{16} + (774592 - 4608\alpha - 64\beta)y^{18} + \cdots
\]

where $0 \leq \alpha \leq -\frac{d}{16} \leq 2$, and

\[
W_{78,2} = 1 + (3705 + 8\alpha)y^{14} + (71460 - 24\alpha)y^{16} + (658880 - 64\alpha)y^{18} + \cdots
\]
where $-468 \leq \alpha \leq -135$. Codes exist for $W_{78,1}$ when $\alpha = \beta = 0$ ([5] and [9]), $\alpha = 0, \beta = -19$ ([1]), $\alpha = 0, \beta = -26$ ([6]), $\alpha = 0, \beta = -78$ ([9]), and for $W_{78,2}$ for $\alpha = -135$ ([9]). Very recently in [22] 16 inequivalent self-dual $[78,39,14]$ codes were found. The authors obtained codes with dihedral automorphism group $D_{38}$ and weight enumerator $W_{78,1}$: 4 codes with $\alpha = 0, \beta = -38$; 12 codes have $\alpha = \beta = 0$.

For doubly-even $[80,40,16]$ codes there is a unique weight distribution:

$$W_{80,1} = 1 + 97565y^{16} + 12882688y^{20} + 590073120y^{24} + \cdots$$

The extended quadratic residue code of length 80 is a known extremal code of this length, there are also 11 inequivalent such codes with an automorphism of order 19 [3], more codes are constructed in [14]. By the Assmus-Mattson theorem, the codewords of a fixed weight in an extremal doubly-even $[80,40,16]$ code form a 3-design (see [3]).

For the weight distribution of a singly-even $[80,40,14]$ self-dual code we have found the formula:

$$W_{80,2} = 1 + (3200 + 4\alpha)y^{14} + (47645 - 8\alpha + 256\beta)y^{16} + \cdots$$

where $\alpha, \beta$ are integer parameters. One singly-even self-dual $[80,40,14]$ code is constructed in [4] but its weight enumerator is not given. A pure double circulant such code is constructed in [8] with $\alpha = -280, \beta = 10$.

Considering self-dual $[82,42,14]$ codes, we have found codes with the following two weight enumerators:

$$W_{82,1} = 1 + (3280 + 4\alpha)y^{14} + (36244 - 4\alpha + 128\beta)y^{16} + (514345 - 52\alpha - 896\beta)y^{18} + \cdots,$$

$$W_{82,2} = 1 + (3280 + 4\alpha)y^{14} + (36244 - 4\alpha + 128\beta)y^{16} + (350505 - 52\alpha - 896\beta)y^{18} + \cdots,$$

where $\alpha$ and $\beta$ are integer parameters. Pure double circulant codes with $W_{82,1}$ for $\alpha = -328, \beta = 0$ are constructed in [5] and [8].

The $[84,42,14]$ self-dual codes possess two weight enumerators:

$$W_{84,1} = 1 + (4080 - \alpha)y^{14} + (28644 + 64\beta)y^{16} + (390368 + 14\alpha - 384\beta)y^{18} + (4935033 + 320\beta)y^{20} + \cdots,$$

$$W_{84,2} = 1 + (4080 - \alpha)y^{14} + 39524y^{16} + (247264 + 14\alpha)y^{18} + 6185465y^{20} + \cdots,$$

where $\alpha, \beta$ are integer parameters. There is one bordered double circulant code from [8] which have $W_{84,2}$ for $\alpha = 3342$. Also a self-dual $[84,42,14]$ code is constructed in [6].

This work is organized as follows. In Section 2 we will give the construction method used. In Sections 3 we classify hermitian self-dual codes of length 6 over the set of all even-weight polynomials in $\mathbb{F}_2[x]/(x^{13} - 1)$. Using these codes, in Sections 4–7 we classify all optimal self-dual codes of lengths $78 \leq n \leq 84$ with an automorphism of order 13 with 6 cycles.

**Remark 1.** The computations were made by two of the authors independently. Both computations match exactly. One of the computations use GAP 4.8 [7] for the generation of the codes and Q-extension [2] for the code equivalence. The
second computation was made with own Delphi code for code generation and Q-extension for the code equivalence. The generating parameters for the matrices of the codes from Sections 3-7 are available in [17].

2. Construction method

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

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

and say that $\sigma$ is of type $p - (c, f)$.

Denote the cycles of $\sigma$ by $\Omega_1, \ldots, \Omega_c$, and the fixed points by $\Omega_{c+1}, \ldots, \Omega_{c+f}$. Let

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

and

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

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

**Theorem 2.1** ([12]). Assume that $C$ is a self-dual code. Then the code $C$ is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$. The subcodes $F_\sigma(C)$ and $E_\sigma(C)$ are subspaces of dimensions $\frac{c+f}{2}$ and $\frac{c(p-1)}{2}$, respectively.

From the definition of $F_\sigma(C)$ it follows 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 $j \in \Omega_i$, $i = 1, \ldots, c + f$.

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 $pc$. For $v$ in $E_\sigma(C)^*$ we let $v|\Omega_i = (v_0, v_1, \ldots, v_{p-1})$ 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 the factor ring $\mathbb{F}_2[x]/(x^p - 1)$. 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 $x - 1$. It is known that $\varphi(E_\sigma(C)^*)$ is a submodule of the $\mathcal{P}$-module $\mathcal{P}^c$ [12, 20].

**Theorem 2.2** ([20]). A binary $[n, n/2]$ code $C$ with an automorphism $\sigma$ is self-dual if and only if the following two conditions hold:

(i) $C_\sigma = \pi(F_\sigma(C))$ is a binary self-dual code of length $c + f$,

(ii) for every two vectors $u, v$ from $C_\sigma$, $\varphi(E_\sigma(C)^*)$ we have

$$u_1(x)v_1(x^{-1}) + \cdots + u_c(x)v_c(x^{-1}) = 0.$$

In order to classify the codes that we have obtained we need additional conditions for equivalence given by the following.

**Theorem 2.3** ([21]). The following transformations preserve the decomposition and send the code $C$ to an equivalent one: (i) a permutation of the fixed coordinates; (ii) a permutation of the $p$-cycles coordinates; (iii) a substitution $x \to x^2$ in $C_\sigma$; (iv) a cyclic shift to each $p$-cycle independently.
3. Constructing the $E_0(C)^*$ subcode

By [19], 2 is a primitive root modulo 13, and hence $\mathcal{P}$ is a field with $2^{12}$ elements and identity $e(x) = x + \cdots + x^{12}$. We use the element $\alpha = 1 + x + x^3 + x^5$ which is a primitive element in $\mathcal{P}$ [21]. Denote $\beta = \alpha^{13}$ an element of multiplicative order 315 in $\mathcal{P}$. We can write $\mathcal{P}^* = \{x^i \beta^j | 0 \leq i \leq 12, 0 \leq j \leq 314\}$.

After Gaussian elimination we can take the generator matrix to be in the form $G = (I \vert Z)$, where $Z$ is a $3 \times 3$ matrix over $\mathcal{P}$. Using Theorem 2.3 we can transform the matrix $Z$ to the following

$$Z = \begin{pmatrix}
\beta^{i_1} & \beta^{i_2} & \beta^{i_3} \\
\beta^{i_4} & x^{i_5} \beta^{i_5} & x^{i_6} \beta^{i_6} \\
\beta^{i_7} & x^{i_8} \beta^{i_8} & x^{i_9} \beta^{i_9}
\end{pmatrix},$$

where $i_1 \leq i_2 \leq i_3$, $0 \leq i_4 \leq 314$, $0 \leq i_5 \leq 12$, or some of the elements in $Z$ are zeroes. Using the orthogonal condition (2) and checking that $d = 16$ we calculated all possible inequivalent choices of the first row of $Z$ and found 1676 triples $(i_1, i_2, i_3)$. Next, we added the second row of $Z$ and we obtained 4086196 different $2 \times 3$ submatrices. Finally, after adding the last row we obtained exactly 322103 inequivalent codes with minimum distance $d = 16$.

**Theorem 3.1.** There are exactly 322103 inequivalent codes $C_\beta$ of length 6 over the set $\mathcal{P}$ of all even-weight polynomials in $\mathbb{F}_2[x]/\langle x^{13} - 1 \rangle$ such that $d(E_0(C)^*) = 16$.

The number of inequivalent codes $E_0(C)^*$ sorted by $A_{16}$ (the number of different codewords of weight 16) are given in Table 1. The order of the automorphism groups of the codes that we have obtained are listed in Table 2.

4. Classification of $[78, 39, 14]$ self-dual codes with an automorphism of type 13 – (6, 0)

Assume that $C$ is a $[78, 39, 14]$ self-dual code with an automorphism of type 13 – (6, 0). By Theorem 2.2 $C_\tau$ is a binary self-dual [6, 3, 2] code. There is a unique such code: $3i_2$ ([13]) with generator matrix $G_1 = (I_3 \vert I_3)$. By Theorem 2.1 $C$ is a direct sum of $F_2(C)$ and $E_0(C)$. We fix the generator matrix of $E_0(C)$ to be the generator matrix of one of the codes from Theorem 3.1. For all permutations $\tau \in S_6$ we consider the generator matrix of $C_\tau$ to be $\tau(G_1)$. We summarize the results in the following.

**Proposition 1.** There are exactly 1592 inequivalent binary $[78, 39, 14]$ self-dual codes having an automorphism of type 13 – (6, 0).

All codes that we have obtained possess weight enumerator $W_{78,1}$ for $\beta = -117, -104, -78, -65, -52, -39, -26, -13, 0$. All values except $\beta = -78, -13$, and 0 are new. We list the number of inequivalent codes with the different pairs $(\beta, |\text{Aut}(C)|)$ in Table 3 where the new values are marked in bold. One of the three codes with the pair $(\beta, |\text{Aut}(C)|) = (-78, 78)$ is the code $C_{78,1}$ from [9].

5. Classification of doubly-even [80, 40, 16] and singly-even [80, 40, 14] self-dual codes with an automorphism of type 13 – (6, 2)

Let $C$ be a $[80, 40, d]$ self-dual code with an automorphism of type 13 – (6, 3). By Theorem 2.2 $C_\tau$ is a binary self-dual $[8, 4, \geq 2]$ code. There are two such codes ([13]): the singly-even $4i_2$ and the doubly-even $8i_8$. Since we need to choose 2 out of 8 coordinate positions for the set $X_I$ of fixed points, in the case $4i_2$, in order to
Table 1. The number of codes with different $A_{16}$

| $A_{16}$ # | $A_{16}$ | $A_{16}$ # | $A_{16}$ | $A_{16}$ # | $A_{16}$ | $A_{16}$ # | $A_{16}$ | $A_{16}$ # |
|------------|---------|------------|---------|------------|---------|------------|---------|---------|
| 14586      | 1       | 15002      | 359     | 15379      | 4290    | 15756      | 4993    | 16133     | 1458    |
| 14612      | 1       | 15015      | 417     | 15392      | 4292    | 15769      | 4803    | 16146     | 1381    |
| 14625      | 2       | 15028      | 528     | 15405      | 4380    | 15782      | 4902    | 16150     | 1198    |
| 14651      | 1       | 15041      | 539     | 15418      | 4551    | 15795      | 4609    | 16172     | 1089    |
| 14677      | 4       | 15054      | 608     | 15431      | 4766    | 15808      | 4414    | 16185     | 1111    |
| 14690      | 1       | 15067      | 707     | 15444      | 4805    | 15821      | 4425    | 16198     | 1077    |
| 14703      | 2       | 15080      | 735     | 15457      | 4842    | 15834      | 4215    | 16211     | 1007    |
| 14716      | 3       | 15093      | 870     | 15470      | 5185    | 15847      | 4008    | 16224     | 856     |
| 14729      | 9       | 15106      | 957     | 15483      | 5164    | 15869      | 3988    | 16237     | 876     |
| 14742      | 4       | 15119      | 1033    | 15496      | 5366    | 15873      | 3865    | 16250     | 767     |
| 14755      | 6       | 15132      | 1176    | 15509      | 5939    | 15886      | 3854    | 16263     | 762     |
| 14768      | 8       | 15145      | 1277    | 15522      | 5480    | 15899      | 3641    | 16276     | 706     |
| 14781      | 11      | 15158      | 1328    | 15555      | 5401    | 15912      | 3428    | 16289     | 662     |
| 14794      | 18      | 15171      | 1557    | 15548      | 5568    | 15925      | 3369    | 16302     | 579     |
| 14807      | 20      | 15184      | 1724    | 15561      | 5671    | 15938      | 3255    | 16315     | 541     |
| 14820      | 37      | 15197      | 1899    | 15574      | 5617    | 15961      | 3027    | 16328     | 572     |
| 14833      | 42      | 15210      | 1934    | 15587      | 5752    | 15964      | 2914    | 16341     | 508     |
| 14846      | 30      | 15223      | 2092    | 15600      | 5577    | 15977      | 2751    | 16354     | 394     |
| 14859      | 50      | 15236      | 2299    | 15613      | 5632    | 15990      | 2533    | 16367     | 438     |
| 14872      | 53      | 15249      | 2439    | 15626      | 5669    | 16003      | 2531    | 16380     | 384     |
| 14885      | 86      | 15262      | 2597    | 15639      | 5764    | 16016      | 2320    | 16393     | 312     |
| 14898      | 99      | 15275      | 2848    | 15652      | 5552    | 16029      | 2328    | 16406     | 334     |
| 14911      | 141     | 15288      | 2972    | 15665      | 5459    | 16042      | 2136    | 16419     | 279     |
| 14924      | 152     | 15301      | 3066    | 15678      | 5353    | 16065      | 2075    | 16432     | 285     |
| 14937      | 182     | 15314      | 3219    | 15687      | 5259    | 16086      | 1969    | 16453     | 243     |
| 14950      | 199     | 15327      | 3487    | 15704      | 5482    | 16081      | 1812    | 16458     | 257     |
| 14963      | 200     | 15340      | 3668    | 15717      | 5213    | 16094      | 1711    | 16471     | 241     |
| 14976      | 271     | 15353      | 3875    | 15730      | 5359    | 16107      | 1597    | 16484     | 203     |
| 14989      | 304     | 15366      | 4068    | 15743      | 5498    | 16120      | 1502    | 16497     | 208     |

Table 2. The order of the automorphism groups of all $E_8(C)^*$

| $|\text{Aut}(C)|$ | 13 | 26 | 39 | 52 | 78 | 156 | 234 | 468 |
|------------|----|----|----|----|----|-----|-----|-----|
| $#$        | 317529 | 4314 | 42 | 167 | 41 | 8 | 1 | 1 |

Table 3. $\beta$ in $W_{78,1}$ and $|\text{Aut}(C)|$ for $[78,34,14]$ self-dual codes with an automorphism of type $13 - (6,0)$

| $|\text{Aut}(C)|$ | $|\text{Aut}(C)|$ |
|------------|------------|
| $\beta$ | 13 | 26 | 39 | 78 |
| $\beta$ | 13 | 26 | 39 | 78 |
| $-117$ | 1 | -39 | 302 |
| $-104$ | 1 | -26 | 437 | 30 |
| $-78$ | 5 | 7 | 1 | 3 | -13 | 421 |
| $-65$ | 37 | 0 | 171 | 18 | 5 |
| $-52$ | 137 | 14 | 2 |

have $d \geq 14$ we cannot have the support of a whole summand of $i_2$ in $X_f$. The code $h_8$ have a 3-transitive automorphism group thus we can choose any pair of coordinates in $X_f$. Therefore we have the following.
Table 4. The cardinality of the automorphism group for the doubly-even [80, 40, 16] codes

| |Aut(C)| | # |
|---|---|---|---|
|13| 26| 78| 246480 |

Proposition 2. There are two possible generator matrices for the code \( C_\pi \) for a [80, 40, d] self-dual code with an automorphism of type 13 – (6, 3): \( G_2 = (I_4 | I_4) \) and \( G_3 = (I_4 | I_4 + J_4) \), where the rightmost two coordinate positions correspond to the set of fixed points.

Proposition 3. There exist 195 inequivalent doubly-even [80, 40, 16] codes with an automorphism of type 13 – (6, 2). There are 162696 inequivalent self-dual [80, 40, 14] singly-even binary codes having an automorphism of type 13 – (6, 2).

In the case of the doubly-even [80, 40, 16] codes we list the number of codes different values of |Aut(C)| in Table 4. The 4 codes with |Aut(C)| = 78 and the one with |Aut(C)| = 246480 are equivalent to the codes \( B_{80,1} \), \( B_{80,4} \) and \( B_{80,5} \) from [8], respectively. The singly-even [80, 40, 14] self-dual codes have weight enumerator \( W_{80,2} \) for \( \beta = 0 \) and \( \alpha = -17k, k \in \{2, \ldots, 25, 27\} \). In Table 5, we give the number of codes for the different pairs \((\alpha, |Aut(C)|)\). We note that for all these values in \( W_{80,2} \) there were previously no known codes. M. Harada and A. Munemasa in [10] have established the weight enumerators of a putative \( s \)-extremal singly-even self-dual [80, 40, 14] code, none of the codes we have obtained is \( s \)-extremal (\( W_{80,2} \) for \( \alpha = 3 = 0 \)).

| |Aut(C)| | # |
|---|---|---|---|
|13| 26| 78| 246480 |

Table 5. Number of codes with pairs \((\alpha, |Aut(C)|)\) for the singly-even [80, 40, 14] self-dual codes

6. Classification of [82, 41, 14] self-dual codes with an automorphism of type 13 – (6, 4)

Let \( C \) be a [82, 41, 14] self-dual code with an automorphism of type 13 – (6, 4). By Theorem 2.2 \( C_\pi \) is a binary self-dual [10, 5, \geq 2] code. There are two such codes ([13]): \( 5i_2 \) and \( i_2 + h_8 \). Checking the possible arrangements of the 10 coordinate positions of both codes into subsets \( X_c \) and \( X_f \), we found 3 possible generator...
matrices for $C_\pi$:

$$G_4 = \begin{pmatrix} I_5 & I_5 \end{pmatrix}, G_5 = \begin{pmatrix} O & 0 & 1 & 1 \\ 0 & 1 & 0 & I_4 \end{pmatrix}, G_6 = \begin{pmatrix} I_5 \\ 01000 \\ 00111 \\ 10011 \\ 10101 \\ 10110 \end{pmatrix},$$

where $G_4$ is equivalent to $5i_2$ and the other two are equivalent to $i_2 + h_5$. We fix $E_\sigma(C)$ and consider all permutations $\sigma \in S_6$ acting on the cyclic points in $G_i$, $i = 4, 5, 6$.

**Proposition 4.** There does not exists a binary self-dual $[82, 41, 16]$ code with an automorphism of order 13. The inequivalent binary self-dual $[82, 41, 14]$ codes with an automorphism of type $13 - (6, 4)$ are:

- $\text{gen}(C_\pi) = G_4$: 604992 codes with weight enumerator $W_{82,2};$
- $\text{gen}(C_\pi) = G_5$: 164338 codes with weight enumerator $W_{82,2};$
- $\text{gen}(C_\pi) = G_6$: 50989 codes with weight enumerator $W_{82,1}$.

When $C_\pi = G_4$ the codes have weight enumerator $W_{82,2}$ for different values of $\alpha$ for $\beta = 0, 13,$ and 26. All codes that we have obtained with $\beta = 0$ are listed in Table 6 with $\beta = 13$ in Table 7 and there is a unique code with $\beta = 26, \alpha = -364$ and an automorphism group with 78 elements.

When $C_\pi = G_5$ the codes have weight enumerator $W_{82,2}$ for different values of $\alpha$ for $\beta = 0, 13.$ All codes that we have obtained with $\beta = 0$ are listed in Table 7 and with $\beta = 13$ in Table 8.

In the case of $C_\pi = G_6$ there are 50972 codes with an automorphism group of order 13 and 17 codes with $|\text{Aut}(C)| = 39.$ All obtained codes have $\alpha = -680, \beta = 170$ in $W_{82,2}$.

**Table 6.** Number of codes with pairs $(\alpha, |\text{Aut}(C)|)$, $\beta = 0$ in $W_{82,2}$ for the $[82, 41, 14]$ self-dual codes with an automorphism of type $13 - (6, 4), C_\pi = G_4$

| $\alpha$ | $|\text{Aut}(C)|$ | $\alpha$ | $|\text{Aut}(C)|$ | $\alpha$ | $|\text{Aut}(C)|$ | $\alpha$ | $|\text{Aut}(C)|$ |
|---------|------------------|---------|------------------|---------|------------------|---------|------------------|
| -169    | 1                | -208    | 3                | -209    | 1                | -211    | 1                |
| -182    | 2                | -286    | 3                | -309    | 1                | -325    | 2                |
| -195    | 4                | -13     | -312              | -301    | 1                | -289    | 1                |
| -208    | 8                | -299    | 1                | -403    | 1                | -1525   | 1                |
| -221    | 1                | -429    | 3                | -7240   | 1                | -520    | 1                |
| -247    | 2                | -338    | 3                | -429    | 3                |

7. **Classification of $[84, 42, 14]$ self-dual codes with an automorphism of type $13 - (6, 6)$**

Let $C$ be a $[84, 42, 14]$ self-dual code with an automorphism of type $13 - (6, 6)$. By Theorem 2.2 $C_\pi$ is a binary self-dual $[12, 6, \geq 2]$ code. There are three such codes (13): $2i_2 + h_8$, $6i_2$, and $d_{12}$. Checking the possible arrangements of the 12
Self-dual codes with an automorphism of order 13

Table 7. Number of codes with pairs \((\alpha, |\text{Aut}(C)|)\), \(\beta = 13\) in \(W_{82,2}\) for the \([82, 41, 14]\) self-dual codes with an automorphism of type \(13 - (6, 4)\), \(C_\pi = G_4\)

| \(\alpha\) | \(|\text{Aut}(C)|\) | \(\alpha\) | \(|\text{Aut}(C)|\) | \(\alpha\) | \(|\text{Aut}(C)|\) | \(\alpha\) | \(|\text{Aut}(C)|\) |
|---|---|---|---|---|---|---|---|
| -325 | 1 | -377 | 44 | -129 | 148 | -841 | 38 |
| -338 | 3 | -390 | 71 | -442 | 133 | -494 | 21 |
| -351 | 4 | -403 | 123 | -455 | 100 | -507 | 4 |
| -364 | 26 | -416 | 146 | -468 | 59 | 1 | -520 | 3 |

Table 8. Number of codes with pairs \((\alpha, |\text{Aut}(C)|)\), \(\beta = 0\) in \(W_{82,2}\) for the \([82, 41, 14]\) self-dual codes with an automorphism of type \(13 - (6, 4)\), \(C_\pi = G_5\)

| \(\alpha\) | \(|\text{Aut}(C)|\) | \(\alpha\) | \(|\text{Aut}(C)|\) | \(\alpha\) | \(|\text{Aut}(C)|\) | \(\alpha\) | \(|\text{Aut}(C)|\) |
|---|---|---|---|---|---|---|---|
| -209 | 4 | -287 | 32 | -287 | 329 | 41 | -365 | 23481 | 92 |
| -222 | 14 | -300 | 6480 | 67 | -378 | 20367 | 89 | -456 | 447 | 14 |
| -235 | 47 | 3 | -313 | 11032 | 65 | -391 | 15274 | 76 | -469 | 156 | 3 |
| -248 | 196 | 13 | -326 | 16352 | 87 | -404 | 9827 | 44 | -482 | 36 |
| -261 | 557 | 15 | -339 | 20791 | 93 | -417 | 5746 | 89 | -507 | 9 |
| -274 | 1446 | 34 | 1 | -352 | 23588 | 117 | 2 | -430 | 2837 | 19 |
| -287 | 355 | 12 | -372 | 26788 | 137 | 2 | -430 | 2837 | 19 |

Table 9. Number of codes with pairs \((\alpha, |\text{Aut}(C)|)\), \(\beta = 13\) in \(W_{82,2}\) for the \([82, 41, 14]\) self-dual codes with an automorphism of type \(13 - (6, 4)\), \(C_\pi = G_5\)

| \(\alpha\) | \(|\text{Aut}(C)|\) | \(\alpha\) | \(|\text{Aut}(C)|\) | \(\alpha\) | \(|\text{Aut}(C)|\) |
|---|---|---|---|---|---|
| -339 | 1 | -417 | 27 | -482 | 12 | 5 |
| -365 | 5 | 1 | -430 | 20 | -495 | 4 |
| -378 | 6 | | -443 | 12 | 23 | -508 | 1 |
| -391 | 7 | | -456 | 20 | | -521 | 2 |
| -404 | 20 | 2 | | -469 | 17 | | |

Coordinate position of both codes into subsets \(X_c\) and \(X_f\), we found 4 possible generator matrices for \(C_\pi\):

\[
G_7 = \begin{pmatrix} I_6 & I_2 & 0 \\ O & I_4 + J_4 \end{pmatrix}, G_8 = \begin{pmatrix} I_6 & I_6 \end{pmatrix},
\]

\[
G_9 = \begin{pmatrix} 100110 \\ 010110 \\ 001110 \\ 111011 \\ 111011 \\ 000111 \end{pmatrix}, G_{10} = \begin{pmatrix} 100001 & 010010 \\ 010001 & 001010 \\ 001001 & 000110 \\ 000100 & 011111 \\ 000001 & 111101 \\ 000011 & 000011 \end{pmatrix}
\]
where $G_7$ is equivalent to $2i_2 + h_8$, $G_8$ is equivalent to $6i_2$, and the rest to $d_{12}$. We fix $E_0(C)$ and consider all permutations $\tau \in S_6$ acting on the cyclic points in $G_i$, $i = 7, \ldots, 10$.

**Proposition 5.** There does not exist a binary self-dual $[84, 42, 16]$ code with an automorphism of order 13. The inequivalent binary self-dual $[84, 42, 14]$ codes with an automorphism of type 13 – (6, 6) are:

- $\text{gen}(C_{\pi}) = G_7$: 607773 codes with weight enumerator $W_{84,2}$;
- $\text{gen}(C_{\pi}) = G_8$: 113879 codes with weight enumerator $W_{84,1}$;
- $\text{gen}(C_{\pi}) = G_9$: 604064 codes with weight enumerator $W_{84,2}$;
- $\text{gen}(C_{\pi}) = G_{10}$: 113439 codes with weight enumerator $W_{84,1}$.

When $C_\pi = G_7$ the codes have weight enumerator $W_{84,2}$ for different values of $\alpha$. We give the number of codes with different pairs $(\alpha, |\text{Aut}(C)|)$ that we have obtained in Table 10.

For the matrix $G_8$ the codes have weight enumerator $W_{82,1}$ for different values of $\alpha = 2280 + 26l$, $l \in \{0, \ldots, 44, 45\}$ for $\beta = 18, 31, 44, \text{ and } 57$. A total of 112449, 1403, 6, and 21 codes have an automorphism group of order 13, 26, 39, and 78, respectively.

In the case of $C_\pi = G_9$ the codes have weight enumerator $W_{84,2}$ for different values of $\alpha$. We give the number of codes with different pairs $(\alpha, |\text{Aut}(C)|)$ that we have obtained in Table 11.

When $C_\pi = G_{10}$ the codes have weight enumerator $W_{82,1}$ for different values of $\alpha = 2286 + 26l$, $l \in \{0, \ldots, 46, 48\}$ for $\beta = 18, 31, 44, \text{ and } 57$. A total of 112005, 1401, 12, and 21 codes have an automorphism group of order 13, 26, 39, and 78, respectively.

**Table 10.** Number of codes with pairs $(\alpha, |\text{Aut}(C)|)$, $W_{84,2}$ for the $[84, 42, 14]$ self-dual codes with an automorphism of type 13 – (6, 6), $C_\pi = G_7$.

| $\alpha$ | $|\text{Aut}(C)|$ | $|\text{Aut}(C)|$ | $|\text{Aut}(C)|$ |
| --- | --- | --- | --- |
| 3038 | 2 | 3272 | 36692 | 171 | 3506 | 12054 | 126 |
| 3064 | 3 | 3298 | 56508 | 214 | 3532 | 5477 | 84 | 5 |
| 3090 | 32 | 1 | 3324 | 75114 | 280 | 3558 | 2154 | 51 |
| 3116 | 126 | 8 | 3350 | 87114 | 288 | 3584 | 742 | 46 |
| 3142 | 568 | 16 | 2 | 3376 | 87901 | 334 | 3610 | 202 | 12 | 1 |
| 3168 | 1602 | 31 | 1 | 3402 | 77847 | 314 | 3636 | 44 | 6 |
| 3194 | 4452 | 48 | | 3428 | 59855 | 288 | 3662 | 13 | 4 |
| 3220 | 10558 | 70 | 3 | 3454 | 40586 | 214 | 3688 | 1 | 1 |
| 3246 | 21074 | 145 | 1 | 3480 | 24064 | 207 | 1 | | 1 |

**References**

[1] A. Baartmans and V. Yorgov, Some new extremal codes of lengths 76 and 78, *IEEE Trans. Inf. Theory*, 49 (2003), 1353–1354.

[2] I. Bouyukliev, About the code equivalence, in *Advances in Coding Theory and Cryptography*, World Scient. Publ. Comp., 2007, 126–151.

[3] R. Dontcheva and M. Harada, Extremal doubly-even [80, 40, 16] codes with an automorphism of order 19, *Finite Fields Appl.*, 9 (2003), 157–167.

[4] G. Dorfer and H. Maharaj, Generalized AG codes and generalized duality, *Finite Fields Appl.*, 9 (2003), 194–210.
Table 11. Number of codes with pairs \((\alpha, |\text{Aut}(C)|)\), \(W_{84,2}\) for the \([84, 42, 14]\) self-dual codes with an automorphism of type 13 – (6, 6), \(C_\pi = G_9\).

| \(\alpha\) | \(|\text{Aut}(C)|\) | \(|\text{Aut}(C)|\) | \(|\text{Aut}(C)|\) | \(|\text{Aut}(C)|\) | \(|\text{Aut}(C)|\) |
|---|---|---|---|---|---|
| 3040 | 126 | 1 | 3222 | 7240 | 51 | 3404 | 83416 | 318 | 3 | 3586 | 1227 | 50 |
| 3066 | 62 | 2 | 3248 | 15253 | 88 | 1 | 3430 | 88292 | 330 | 2 | 3612 | 411 | 19 |
| 3092 | 20 | 1 | 3274 | 28921 | 143 | 2 | 3456 | 48818 | 302 | 2 | 3638 | 88 | 13 |
| 3118 | 63 | 51 | 3300 | 46912 | 174 | 2 | 3482 | 30265 | 230 | 1 | 3664 | 17 | 8 |
| 3144 | 304 | 2 | 3326 | 67138 | 223 | 1 | 3508 | 16765 | 168 | 1 | 3690 | 4 | 2 |
| 3170 | 1064 | 15 | 3352 | 82010 | 297 | 5 | 3534 | 7856 | 137 | 5 | 3716 | 2 |
| 3196 | 3002 | 28 | 3378 | 85971 | 312 | 1 | 3660 | 3199 | 79 | 7 | 3742 | 1 |

[5] S. T. Dougherty, T. A. Gulliver and M. Harada, Extremal binary self-dual codes, *IEEE Trans. Inf. Theory*, 43 (1997), 2036–2047.
[6] P. Gaborit and A. Otmani, Experimental constructions of self-dual codes, *Finite Fields Appl.*, 9 (2003), 372–394.
[7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.6, 2016, http://www.gap-system.org
[8] T. A. Gulliver and M. Harada, Classification of extremal double circulant self-dual codes of lengths 74–88, *Discr. Math.*, 306 (2006), 2064–2072.
[9] T. A. Gulliver, M. Harada and J.-L. Kim, Construction of new extremal self-dual codes, *Discr. Math.*, 263 (2003), 81–91.
[10] M. Harada and A. Munemasa, On s-extremal singly even self-dual \([24k + 8, 12k + 4, 4k + 2]\) codes, preprint, arXiv:1511.01297
[11] M. Harada and A. Munemasa, Some restrictions on weight enumerators of singly even self-dual codes *IEEE Trans. Inf. Theory*, 52 (2006), 1266–1269.
[12] W. C. Huffman, Automorphisms of codes with applications to extremal doubly even codes of length 48, *IEEE Trans. Inf. Theory*, 28 (1982), 511–521.
[13] W. C. Huffman and V. S. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge Univ. Press, 2003.
[14] S. Kapralov, R. Russeva and V. Radeva, New extremal doubly even \([80, 40, 16]\) codes with an automorphism of order 13, in Proc. 8th Int. Workshop Algebr. Coding Theory, 2002, 139–142.
[15] E. Rains, Shadow bounds for self-dual codes *IEEE Trans. Inf. Theory*, 44 (1998), 134–139.
[16] N. Yankov, Self-dual \([62, 31, 12]\) and \([64, 32, 12]\) codes with an automorphism of order 7 *Adv. Math. Commun.*, 8 (2014), 73–81.
[17] N. Yankov, D. Anev and M. G" urel, Constructing the self-dual codes with an automorphism of order 13 with 6 cycles, available at http://shu.bg/tadmin/upload/storage/2497.pdf
[18] N. Yankov and M. H. Lee, Classification of self-dual codes of length 50 with an automorphism of odd prime order *Des. Codes Crypt.*, 74 (2015), 571–579.
[19] N. Yankov and R. Russeva, Binary self-dual codes of lengths 52 to 60 with an automorphism of order 7 or 13 *IEEE Trans. Inf. Theory*, 57 (2011), 7498–7506.
[20] V. Yorgov, Binary self-dual codes with automorphisms of odd order, *Probl. Inf. Transm.*, 19 (1983), 260–270.
[21] V. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56 *IEEE Trans. Inf. Theory*, 33 (1987), 77–82.
[22] T. Zhang, J. Michel, T. Feng and G. Ge, On the existence of certain optimal self-dual codes with lengths between 74 and 116, *Electr. J. Combin.*, 22 (2015), P4.33.

Received February 2016; revised January 2017.

E-mail address: jankov.niki@yahoo.com
E-mail address: damian_anev@mail.bg
E-mail address: muberragurel@hotmail.com