МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2018
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2018
Proceedings of the Forty-seventh Spring Conference
of the Union of Bulgarian Mathematicians
Borovets, April 2–6, 2018

OPTIMAL SELF-DUAL CODES OF LENGTH 74 WITH AN AUTOMORPHISM OF ORDER 9 AND NEW SELF-DUAL $[74, 37, 12]$ CODES*

Nikolay Yankov, Radka Russeva, Emine Karatash

We prove that a self-dual $[74, 37, 14]$ code possessing an automorphism of order 9 does not exists. In the process of constructing optimal self-dual codes of length 74 with an automorphism of order 9 and by shortening all known self-dual $[76, 38, 14]$ codes we obtain new self-dual $[74, 37, 12]$ codes.

1. Introduction. The highest attainable minimum weight for binary self-dual codes of length 74 is 14 [7]. However the existence of a binary self-dual $[74, 37, 14]$ code is still unknown. One of the first examples of binary self-dual $[74, 37, 12]$ codes were constructed in [9].

Let C be a putative self-dual $[74, 37, 14]$ code. The structure of its automorphism group Aut (C) is examined in [3, 9]. It is proved that the order of Aut (C) is either $2^k.3^l$, or $2^k.3^l.7$ where $k \geq 0$ and $l \in \{0, 1, 2\}$.

In this paper we investigate the existence of a binary self-dual $[74, 37, 14]$ code under the assumption that such a code possesses an automorphism of order 9. We prove that such codes do not exist. In the process of constructing optimal self-dual codes of length 74 via an automorphism of order 9 and by shortening all known self-dual $[76, 38, 14]$ codes we obtain many new self-dual $[74, 37, 12]$ codes.

2. Codes of length 74 with automorphism of order 9. Let C be a self-dual $[74, 37, 14]$ code having an automorphism σ of order 9. It is known that σ may be only of type 9-$(8, 0, 2)$ [9]. That means that σ has 8 cycles of order 9, no cycles of order 3 and 2 fixed points in its decomposition.

In [4] a method for constructing binary self-dual codes having an automorphism of order p^2, where p is an odd prime, was presented. We consider the case $p = 3$.

Thus we have

$$\sigma = (1, 2, \ldots, 9)(10, 11, \ldots, 18) \ldots (64, 65, \ldots, 72)(73)74). \tag{1}$$

Denote by Ω_i, $i = 1, \ldots, 10$ the cycles in σ. Define $F_\sigma(C) = \{v \in C \mid v\sigma = v\}$, $E_\sigma(C) = \{v \in C \mid \mathrm{wt}(v|\Omega_i) \equiv 0 \pmod 2\}$, where $v|\Omega_i$ denotes the restriction of v to Ω_i. Clearly $v \in F_\sigma(C)$ iff $v \in C$ is constant on each cycle. Denote $\pi : F_\sigma(C) \to F_2^{10}$ the projection map where if $v \in F_\sigma(C)$, $(\pi(v))_i = v_j$ for some $j \in \Omega_i$, $i = 1, \ldots, 10$. Then the following lemma holds.

*2010 Mathematics Subject Classification: 94B05.
Key words: self-dual codes, automorphisms, optimal codes.
This research is partially supported by Shumen University under Project No RD-08-111/05.02.2018.

Lemma 1 ([4]). *$C = F_\sigma(C) \oplus E_\sigma(C)$. $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual code of length* 10.

Thus each choice of the codes $F_\sigma(C)$ and $E_\sigma(C)$ determines a self-dual code C. Denote by $E_\sigma(C)^*$ the subcode $E_\sigma(C)$ with the last 2 zero coordinates deleted. $E_\sigma(C)^*$ is a self-orthogonal binary code of length $8.3^2 = 72$ and dimension $\frac{8}{2}(3^2-1) = 32$. For $v \in E_\sigma(C)^*$ we let $v|\Omega_i = (v_0, v_1, \cdots, v_8)$ correspond to the polynomial $v_0 + v_1 x + \cdots + v_8 x^8$ from $\mathcal{T}$, where $\mathcal{T}$ is the ring of even-weight polynomials in $F_2[x]/(x^9 - 1)$. Thus we obtain the map $\varphi : E_\sigma(C)^* \to \mathcal{T}^8$. Denote $C_\varphi = \varphi(E_\sigma(C)^*)$.

Let $e_1 = x^8 + x^7 + x^5 + x^4 + x^2 + x$ and $e_2 = x^6 + x^3$. In [4] we proved that $\mathcal{T} = I_1 \oplus I_2$, where $I_1 = \{0, e_1, \omega = xe_1, \overline{\omega} = x^2 e_1\}$ is a field with identity e_1 and I_2 is a field with 2^6 elements with identity e_2. The element $\alpha = (x+1)e_2$ is a primitive element in I_2 so $I_2 = \{0, \alpha^k, 0 \le k \le 62\}$.

The following theorem is from [2].

Theorem 1 ([2]). *$C_\varphi = M_1 \oplus M_2$, where $M_j = \{u \in E_\sigma(C)^* | u_i \in I_j, i = 1, \ldots, 8\}$, $j = 1, 2$. Moreover M_1 and M_2 are Hermitian self-dual codes over the fields I_1 and I_2, respectively. If C is a binary self-dual code having an automorphism σ of type* (1) *then $E_\sigma(C)^* = E_1 \oplus E_2$ where $M_i = \varphi(E_i)$, $i = 1, 2$.*

This proves that C has a generator matrix of the form

$$\mathcal{G} = \begin{pmatrix} \varphi^{-1}(M_2)\ 0\ 0 \\ \varphi^{-1}(M_1)\ 0\ 0 \\ F_\sigma \end{pmatrix}. \tag{2}$$

Let A_s, B_s and E_s denote the number of words of weight s in C, $F_\sigma(C)$ and $E_\sigma(C)^*$, respectively. Every word of weight s in $E_\sigma(C)^*$ is in an orbit of length 3, therefore, $E_s \equiv 0 \pmod 3$ and $A_s \equiv B_s \pmod 3$ for $1 \le s \le n$.

Since the minimum distance of C is 14 the code M_2 is a $[8, 4]$ Hermitian self-dual code over F_{64}, having minimal distance $d \ge 4$. Using Singleton bound $d \le n - k + 1$ we have $d = 5$ or $d = 4$. The case $d = 5$ is studied in [2] and there are exactly 96 MDS Hermitian $[8, 4, 5]_{64}$ self-dual codes such that the minimum distance of $\varphi^{-1}(M_2)$ is 16. The case for the near MDS codes is completed in [10] and the number of the codes is 26. We state the following theorem.

Theorem 2 ([2], [10]). *Up to equivalence, there are exactly* 122 *Hermitian $[8, 4]_{64}$ self-dual codes such that the minimum distance of $\varphi^{-1}(M_2)$ is* 16.

We denote these codes by $\mathcal{M}_{2,i}$ for $1 \le i \le 122$. Their generator parameters can be obtained from [10].

We fix the upper part of $\mathcal{G}$ in (2) to be generated by one of the 122 already constructed Hermitian MDS or NMDS $[8, 4]_{64}$ codes. Now we continue with construction of the middle part, i.e. the code M_1. Theorem 1 states that M_1 is a quaternary Hermitian self-dual $[8, 4, 4]$ code. There exists a unique such code e_8 [5] with a generator matrix $Q_1 = \begin{pmatrix} 10000111 \\ 01001011 \\ 00101101 \\ 00011110 \end{pmatrix}$. We have to put together the two codes from M_2 and M_1 in (2), but we have to examine carefully all transformations on Q_1 that can lead to a different joined code. The full automorphism group of e_8 is of order $2.3^8(8!)$ and we have to consider the

following transformations that preserve the decomposition of the code C :

(i) a permutation $\tau \in S_8$ acting on the set of columns.

(ii) a multiplication of each column by a nonzero element e_1, ω or $\overline{\omega}$ in I_1.

(iii) a Galois automorphism γ which interchanges ω and $\overline{\omega}$.

The action of (i) and (ii) can be represented by a monomial matrix $M = PD$ for a diagonal matrix D and permutational matrix P. Since every column of Q_1 consists only of 0 and 1 the action of $PD\gamma$ on Q_1 can be obtained via $P\overline{D}$. Thus we apply only transformations (i) and (ii).

Denote by M_1^τ the code determined by the matrix Q_1 with columns permuted by τ. To narrow down the computations we can use $PAut(M_1) = \langle\, (47)(56), (45)(67), (12)(3586), (24)(68), (34)(78)\,\rangle$, $|PAut(M_1)| = 1344$ and the right transversal T of S_8 with respect to $PAut(M_1)$

T=$\{(), (78), (67), (678), (687), (68), (56), (56)(78), (567), (5678), (5687), (568), (576),$
$(5786), (57), (578), (57)(68), (5768), (5876), (586), (587), (58), (5867), (58)(67),$
$(45678), (4568), (4578), (45768), (458), (458)(67)\}$.

For every one of the 122 codes $\mathcal{M}_{2,i}$ and $\tau \in T$ we considered 3^8 possibilities for $gen(M_1^\tau)$ and checked the minimum distance in the corresponding binary code $E_\sigma(C)^*$. We state the following result.

Theorem 3. *There are exactly* 36659 *inequivalent self-orthogonal* $[72, 32, 16]$ *codes having an automorphism with* 8 *cycles of order* 9.

Denote the codes obtained by $C_{72,i}$, $i = 1, \ldots, 36659$.

The code C_π is a $[10, 5]$ binary self-dual code. There are two such codes $5i_2$ and i_2+h_8 [8]. Only the code $i_2 + h_8$ can be arranged so that the minimum distance of the code $F_\sigma(C)$ is ≥ 14. The unique possible generator matrix in this case, up to a permutation of the cycle coordinates is

$$G_1 = \left(\begin{array}{cccccccc|cc} 1&1&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&1&1&1\\ 0&0&0&1&0&0&1&0&1&1\\ 0&0&0&0&1&0&1&1&0&1\\ 0&0&0&0&0&1&1&1&1&0 \end{array}\right),$$

For a permutation $\mu \in S_8$ we denote by G_1^μ the matrix derived from G_1 after permuting its columns by μ. Denote by $C_{74,i}^\mu$, $i = 1, \ldots, 36659$, the $[74, 37]$ binary self-dual code with a generator matrix in the form (2):

$$G_i^\mu = \left(\begin{array}{cc} gen(C_i) & O \\ \pi^{-1}(G_1^\mu) & \end{array}\right),$$

and O is a 32×2 all-zeros matrix.

Let A be the subgroup of the automorphism group of the $[10, 5]$ binary code generated by the matrix G_1 consisting of the automorphisms of this code that permute the first 8 coordinates (corresponding to the 9-cycle coordinates) among themselves and permute the last 2 coordinates (corresponding to the fixed point coordinates) among themselves. Let G' be the subgroup of the symmetric group S_8 consisting of the permutations in

A restricted to the first 8 coordinates, ignoring the action on the fixed points. Using Bouyukliev's application Q-extensions [1] we computed that $G' = \langle (1,2)(3,5,7)(4,8,6), (3,4)(7,8), (3,8)(4,7)(5,6) \rangle$ is a group of cardinality 420.

The following lemma gives sufficient conditions for the equivalence of two codes $C_{74,i}^{\mu_1}$ and $C_{74,i}^{\mu_2}$, $i = 1, \ldots, 36659$.

Lemma 2. *If μ_1 and μ_2 belong to one and the same right coset of G' in S_8, then the codes $C_{74,i}^{\mu_1}$ and $C_{74,i}^{\mu_2}$ are equivalent.*

Thus we only need the permutations from the set T – a right transversal of S_8 with respect to G'. Our exhaustive search is summarized in the following.

Theorem 4. *There does not exists a binary self-dual* $[74, 37, 14]$ *code with an automorphism of type* 9-$(8, 0, 2)$.

Nevertheless we have constructed all $[74, 37, 12]$ self-dual codes and computed their weight enumerators. Due to the fact that in Theorem 3 we have calculated only codes with $E_\sigma(C)$ having $d = 16$ we are unable to give full classification of all codes codes of length 74 with minimum weight $d = 12$.

The possible weight enumerators for a self-dual $[74, 37, 12]$ codes. They depend of two integer parameters α and β and are the following:

$W_{74,12,1}(y) = 1+(\alpha - 1295)y^{12} + (5069 + \alpha + 32\beta)y^{14} + (116143 - 12\alpha - 160\beta)y^{16} + \ldots$

$W_{74,12,2}(y) = 1+(\alpha - 1295)y^{12} + (5069 + \alpha + 32\beta)y^{14} + (153007 - 12\alpha - 160\beta)y^{16} + \ldots$

In [9] at least 294 self-dual $[74, 37, 12]$ codes with both $W_{74,12,1}$ and $W_{74,12,2}$ for different values of the parameters are constructed. After an exhaustive search we have the following result.

Proposition 1. *There exist binary self-dual* $[74, 37, 12]$ *codes with an automorphism of type* 9-$(8, 0, 2)$ *with weight enumerator $W_{74,12,1}$ for $\beta = -2, -11, -20, -29, -38$ for $\alpha \in \{1322, 1826, 1829, 1862\} \cup \{1331 + 3\gamma \mid \gamma \in \{0, \ldots, 162\}, \gamma \not\equiv 2 \pmod 3\}$.*

We constructed more than 8 millions self-dual $[74, 37, 12]$ codes, at this time. Due to the large number of codes obtained we have not check them for equivalence.

3. New $[74, 37, 12]$ codes obtained by subtracting. There exist nine known nonequivalent self-dual $[76, 38, 14]$ codes. Six of them have an automorphism of type $9-(8, 0, 4)$ and are presented in [11] and the other three codes are with an automorphism of type $19 - (4, 0)$ [6].

In this section, using the known binary self-dual $[76, 38, 14]$ codes, we construct new codes by shortening. Let C be one of the codes $C_{76,i}$ $i = 1, 2, \ldots, 9$. By choosing a pair $1 \le i_1 < i_2 \le 76$ of coordinates we can construct a new code

$$C' = \{(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) | (x_1, \ldots, x_{76}) \in C_{76,i}, x_{i_1} = x_{i_2}\}.$$

It is well known that C' is a self-dual code of length 74 and we say that C' is obtained from C by subtracting. Since all codes we are shortening have minimum weight 14, all codes obtained have minimum weight 12 so all C' are self-dual $[74, 37, 12]$ codes. Our search gives the following result.

Proposition 2. *Up to equivalence there are exactly* 1932 *binary self-dual* $[74, 37, 12]$ *codes obtained by subtracting the* $[76, 38, 14]$ *self-dual code with an automorphism of type* 9-$(8, 0, 4)$.

Exactly 36 of the codes obtained have automorphism of type $9 - (8, 0, 2)$ are known from Section 2. All other 1896 codes have a trivial automorphism group and are new.

The following new values for the parameters in the weight enumerator $W_{74,12,1}$ occur:

- $\beta = 0$, $\alpha \in \{1419, \ldots, 1463\} \cup \{1411, 1414, 1416, 1417, 1465, 1471, 1478\}$;
- $\beta = -1$, $\alpha \in \{1416, \ldots, 1471\} \cup \{1413, 1474, 1475\}$;
- $\beta = -2$, $\alpha \in \{1416, 1418, 1419, 1422, 1423, 1425, \ldots, 1432, 1434, \ldots,$ 1438, 1440, 1441, 1443, ..., 1447, 1449, 1450, 1452, ..., 1456, 1458, 1459, 1461, 1462, 1463, 1465, 1468, 1471, 1472$\}$;
- $\beta = -3$, $\alpha \in \{1420, \ldots, 1460\} \cup \{1416, 1417, 1462, 1463, 1465, 1466, 1469, 1470\}$;
- $\beta = -4$, $\alpha \in \{1430, \ldots, 1455\} \cup \{1414, 1424, 1427, 1428, 1457, 1458, 1459, 1460, 1463, 1464, 1471\}$;
- $\beta = -8$, $\alpha \in \{1435, 1439, 1440, 1441, 1444, 1448, 1449, 1452, 1455\}$;
- $\beta = -11$, $\alpha \in \{1445, 1454, 1472, 1478\}$.

When we subtract the three $[76, 38, 14]$ codes with an automorphism of type 19-$(4, 0)$ obtained in [6] we have the following:

Proposition 3. *Up to equivalence there are exactly* 450 *binary self-dual* $[74, 37, 12]$ *codes obtained by subtracting the* $[76, 38, 14]$ *self-dual code with an automorphism of type* 19-$(4, 0)$.

All constructed codes are new and have $|\mathrm{Aut}\ (C)| = 1$. The weight enumerator for all codes obtained is $W_{74,12,1}$ for $\beta = 0$, $\alpha \in \{1422, \ldots, 1471, 1474, 1478, 1480\}$.

REFERENCES

[1] I. Bouyukliev. About the code equivalence. *Advances in Coding Theory and Cryptography*, **3** (2007), 126–151. World Scientific Publishing Company.

[2] St. Bouyuklieva. Some MDS codes over $GF(64)$ connected with the binary doubly-even $[72, 36, 16]$ code. Serdica Journal of Computing, **1**, (2007), 185–192.

[3] St. Bouyuklieva, R. Russeva, E. Karatash. Notes on binary optimal self-dual $[74, 37, 14]$ codes. Сборник с доклади от Юбилейна международна научна конференция "25 години факултет Математика и информатика" на ВТУ, стр. 86–90, Издателство "Фабер", ISBN 978–619–00–0419–6, 2015.

[4] St. Bouyuklieva, R. Russeva, N. Yankov. On the Structure of Binary Self-Dual Codes Having an Automorphism of Order a Square of an Odd Prime. *IEEE Trans. Inform. Theory*, **51**, No 10 (2005), 3678–3686.

[5] J. H. Conway, V. S. Pless, N. J. A. Sloan. Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16. *IEEE Trans. Inform. Theory*, **25**, No 3 (1979), 312–322.

[6] R. Dontcheva, V. Yorgov. The extremal codes of length 76 with an automorphism of order 19. *Finite Fields and Their Applications*, **9**, No 4 (2003), 395–399.

[7] S. T. Dougherty, T. A. Gulliver, M. Harada. Extremal binary self-dual codes. *IEEE Trans. Inform. Theory*, **43**, No 6 (1997), 2036–2047.

[8] V. Pless. A classification of self-orthogonal codes over $GF(2)$., *Discrete Mathematics*, **3**, No 1–3 (1972), 209–246.

[9] R. Russeva, N. Yankov, E. Karatash. On the Automorphisms of the Optimal Self-Dual Code of length 74. Proccedings of MATTEX, (2016), 36–42.
[10] N. Yankov. A putative doubly-even [72, 36, 16] code does not have an automorphism of order 9. *IEEE Trans. Inform. Theory*, **58**, No 1 (2012), 159–163.
[11] N. Yankov, R. Russeva, E. Karatash. Classification of binary self-dual [76, 38, 14] codes with an automorphism of order 9. arXiv: 1711.05710v1 [math.CO], 2017.

Nikolay Yankov
e-mail: n.yankov@shu.bg
Radka Russeva
e-mail: russeva@shu.bg
Emine Karatash
e-mail: e.karatash@abv.bg
Faculty of Mathematics and Informatics
University of Shumen
115, Universitetska Str.
970 Shumen, Bulgaria

ОПТИМАЛНИ САМОДУАЛНИ [74, 37, 14] КОДОВЕ С АВТОМОРФИЗЪМ ОТ РЕД 9 И НОВИ САМОДУАЛНИ [74, 37, 12] КОДОВЕ

Николай Янков, Радка Русева, Емине Караташ

Доказано е несъществуването на самодуален [74, 37, 14] код с автоморфизъм от ред 9. Чрез конструиране на оптимални самодуални кодове с дължина 74, притежаващи автоморфизъм от ред 9, и чрез метод за скъсяване на всички известни [76, 38, 14] кодове са получени множество нови самодуални [74, 37, 12] кодове.