Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 193-198*

On the binary self-dual $[96, 48, 20]$ codes with an automorphism of order 9 [1]

NIKOLAY YANKOV n.yankov@shu-bg.net
Faculty of Mathematics and Informatics, Shumen University, Shumen, BULGARIA

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. In this paper we study the existence of binary self-dual [96, 48, 20] codes possessing an automorphism of order 9. Using a method for classification of binary self-dual codes having an automorphism of order p^2 for an odd prime p we prove the nonexistence of an optimal self-dual code of length 96 with an automorphism of order 9 with 10 cycles and 6 fixed points.

1 Introduction

A linear $[n, k]$ *code* C is a k-dimensional subspace of the vector space $\mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field of q elements. 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 $\mathrm{wt}(v)$ to denote the weight of a codeword. The *minimum weight* d of C is the smallest weight among all its non-zero codewords, and C 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. Every code satisfies the Singleton bound $d \le n - k + 1$. A code is *maximum distance separable* or *MDS* if $d = n - k + 1$, and *near MDS* or *NMDS* if $d = n - k$.

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*.

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 $\equiv 2 (\mathrm{mod}\ 4)$. Self-dual doubly-even codes exist only if n is a multiple of eight.

The *Hermitian inner product* on $\mathbb{F}_4^n$ is given by $u.v = \sum_{i=1}^{n} u_i v_i^2$ and we denote by $C^{\perp H}$ the dual of C under Hermitian inner product. C is *Hermitian self-dual* if $C = C^{\perp H}$.

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. Following [5] we say that

[1] This research is partially supported by Shumen University under Grant RD-08-245/13.03.2013.

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 PAut(C). Two codes C and C' of the same length over $\mathbb{F}_q$ are *equivalent* provided there is a monomial matrix M and an automorphism γ of the field such that $C = C'M\gamma$.

An automorphism $\sigma \in \mathcal{S}_n$, $|\sigma| = p^2$ is of *type* $p^2-(c,t,f)$ if when decomposed to independent cycles it has c cycles of length p^2, t cycles of length p, and f fixed points. Obviously, $n = cp^2 + tp + f$.

The study of the existence of a doubly-even self-dual $[24k, 12k, 4k+4]$ for $k \geq 3$ is a growing trend. Recent results include but are not limited to $k = 4$ [4] and $k = 5$ [2].

In [3] it was shown that only the primes 2, 3 and 5 divide the order of the automorphism group of a $[96, 48, 20]$ code. Also in [3, Lemma2.1.8] the possible cycle structure for an automorphism of order p^2 in $[96, 48, 20]$ code was narrowed to an automorphism of order 9 with $c = 10$ and $t = 0$, 1 or 2. Since 2 is a primitive root modulo 3 the number of 3-cycles must be even [1]. Thus only two cases of a $[96, 48, 20]$ code with an automorphism of order 9 remain:

- $9-(10,0,6)$;
- $9-(10,2,0)$.

In this paper, we investigate the case $9-(10,0,6)$. The main result is the following.

Theorem 1. *There does not exists a binary self-dual doubly-even* $[96, 48, 20]$ *code with an automorphism of type* $9-(10,0,6)$.

2 Construction method

Assume that C is a doubly-even self-dual $[96, 48, 20]$ code with an automorphism of type $9-(10,0,6)$. We apply the method for constructing binary self-dual codes possessing an automorphism of order p^2 for a prime p from [1].

Thus we can assume that

$$\sigma = (1,2,\ldots,9)(10,11,\ldots,18)\ldots(82,83,\ldots,90). \tag{1}$$

Denote by Ω_i, $i = 1,\ldots,10$ the cycles of length 9 in σ; for $i = 11,\ldots,16$ – the fixed points in σ. Define $F_\sigma(C) = \{v \in C \mid v\sigma = v\}$, $E_\sigma(C) = \{v \in C \mid \mathrm{wt}(v|\Omega_i) \equiv 0(\bmod 2)\}$, 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 $\pi : \mathbb{F}_\sigma(C) \to \mathbb{F}_2^{16}$ the projection map where if $v \in F_\sigma(C)$, $(\pi(v))_i = v_j$ for some $j \in \Omega_i$, $i = 1,\ldots,16$. Then the following lemma holds.

Lemma 1. *[1]* $C = F_\sigma(C) \oplus E_\sigma(C)$. $C_\pi = \pi(F_\sigma(C))$ *is a binary self-dual code of length 16.*

Denote by E^* the code E_σ with the last f coordinates deleted. For $v \in E^*$ we let $v|\Omega_i = (v_0, v_1, \cdots, v_{10})$ correspond to the polynomial $v_0 + v_1 x + \cdots + v_8 x^{10}$ from $\mathcal{T}$, where $\mathcal{T}$ is the ring of even-weight polynomials in $\mathbb{F}_2[x]\langle x^9 - 1\rangle$. Thus we obtain the map $\varphi : E^* \to \mathcal{T}^{10}$. In our work [1] we have proved that in the case $p = 3$, $\mathcal{T} = I_1 \oplus I_2$. Denote $C_\varphi = \varphi(E^*)$.

Theorem 2. *[8] $C_\varphi = \varphi(M_1) \oplus \varphi(M_2)$, where $M_j = \{u \in E_\sigma(C) | u_i \in I_j, i = 1, \ldots, 10\}$, $j = 1, 2$. 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 $9-(c, t, f)$ then $C = E_1 \oplus E_2 \oplus F_\sigma$ where $E_1 \oplus E_2 = E_\sigma$, $M_i = \varphi(E_i)$, $i = 1, 2$.*

This proves that C has a generator matrix of the form

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

Since the minimum distance of C is 20 the code M_2 is a $[10, 5]$ Hermitian self-dual code over $\mathbb{F}_{64}$, having minimal distance $d \geq 5$. Using the Singleton bound $d \leq n - k + 1$ we have $d = 6$ or $d = 5$.

We look for Hermitian MDS or NMDS codes M_2 over $I_2 \cong \mathbb{F}_{64}$ under the inner product $(u, v) = \sum_{i=1}^{10} u_i v_i^8$. Consider the element $\delta = \alpha^9 = x^2 + x^4 + x^5 + x^7$ of multiplicative order 7 in I_2. We have that $I_2 = \{0, x^s \delta^l | 0 \leq s \leq 8, 0 \leq l \leq 6\}$.

2.1 MDS codes over $\mathbb{F}_{64}$

Theorem 3. *There are exactly 3144 inequivalent MDS codes M_2 over $\mathbb{F}_{64}$ such that $\varphi^{-1}(M_2)$ have minimum weight 20.*

Proof. Let $G = (E_5|A)$ be a generator matrix for the code M_2 for

$$A = \begin{pmatrix} \delta^{a_{11}} & \delta^{a_{12}} & \delta^{a_{13}} & \delta^{a_{14}} & \delta^{a_{15}} \\ \delta^{a_{21}} & \gamma_{22} & \gamma_{23} & \gamma_{24} & \gamma_{25} \\ \delta^{a_{31}} & \gamma_{32} & \gamma_{33} & \gamma_{34} & \gamma_{35} \\ \delta^{a_{41}} & \gamma_{42} & \gamma_{43} & \gamma_{44} & \gamma_{45} \\ \delta^{a_{51}} & \gamma_{52} & \gamma_{53} & \gamma_{54} & \gamma_{55} \end{pmatrix}, \tag{3}$$

where $0 \leq a_{11} \leq a_{12} \leq a_{13} \leq a_{14} \leq a_{15} \leq 6$, $0 \leq a_{21} \leq a_{31} \leq a_{41} \leq a_{51} \leq 6$, $\gamma_{ij} \in I_2^*$, $i = 2, \ldots, 5$, $j = 2, \ldots, 5$. Using the orthogonality condition, it turns out that there are exactly 7 permutational inequivalent possibilities for the vector $v = (a_{11}, a_{12}, a_{13}, a_{14}, a_{15})$: $(0, 0, 0, 3, 3)$, $(0, 0, 1, 2, 5)$, $(0, 0, 3, 5, 6)$, $(0, 1, 1, 2, 2)$, $(0, 1, 1, 3, 3)$, $(0, 1, 1, 5, 5)$, $(0, 1, 2, 3, 6)$. Using a computer program that constructs all 5 rows of A in each of these 7 cases we have found exactly 3144 inequivalent codes.

□

2.2 NMDS codes over $\mathbb{F}_{64}$

Theorem 4. *There are exactly 6703 inequivalent NMDS codes M_2 over $\mathbb{F}_{64}$ such that $\varphi^{-1}(M_2)$ have minimum weight 20.*

Proof. We have considered all possibilities for the first row in $G = (E_5|A)$ for

$$A = \begin{pmatrix} 0 & \delta^{a_{12}} & \delta^{a_{13}} & \delta^{a_{14}} & \delta^{a_{15}} \\ \delta^{a_{21}} & \gamma_{22} & \gamma_{23} & \gamma_{24} & \gamma_{25} \\ \delta^{a_{31}} & \gamma_{32} & \gamma_{33} & \gamma_{34} & \gamma_{35} \\ \delta^{a_{41}} & \gamma_{42} & \gamma_{43} & \gamma_{44} & \gamma_{45} \\ \delta^{a_{51}} & \gamma_{52} & \gamma_{53} & \gamma_{54} & \gamma_{55} \end{pmatrix}, \tag{4}$$

where $0 \le a_{12} \le a_{13} \le a_{14} \le a_{15} \le 6$, $0 \le a_{21} \le a_{31} \le a_{41} \le a_{51} \le 6$ (or we have zeros in column 6), $\gamma_{ij} \in I_2$, $i = 2, \dots, 5$, $j = 2, \dots, 5$. It turns out that there is a unique possibility for the vector $w = (a_{12}, a_{13}, a_{14}, a_{15}) = (0, 1, 5, 6)$.

A computer program computing all codes with generator matrix G turn out exactly 6703 inequivalent NMDS codes. □

The orders of the automorphism groups of the constructed MDS and NMDS codes are displayed in Table 1. Denote the generator matrices of $\varphi^{-1}(M_2)$ for the 9847 constructed codes by H_i, $i = 1, \dots, 9847$. All codes have the following weight enumerator

$$W(y) = 1 + 3249y^{20} + 86265y^{24} + 1297215y^{28} + 11648745y^{30} + \dots.$$

2.3 The fixed subcode F_σ

Theorem 5. *Let C be an $[96, 48, 20]$ binary self-dual code with an automorphism (1). Up to equivalence, there is an unique possible generator matrix*

$$B = \left(\begin{array}{c|c} 1000000001 & 000101 \\ 0100000011 & 111110 \\ 0010000010 & 111111 \\ 0001000001 & 010001 \\ 0000100001 & 100001 \\ 0000010011 & 000001 \\ 0000001001 & 001001 \\ 0000000101 & 000011 \end{array}\right)$$

for the the code $C_\pi = \pi(F_\sigma(C))$.

Proof. The code C_π is a binary self-dual $[16, 8, \ge 4]$ code. There exist exactly three such codes: the singly-even d_8^{2+}, and two doubly-even: d_{16}^+, and e_8^2 [7]. We have to choose two disjoint sets $X_c, X_f \subset \{1, \dots, 16\}$, $|X_c| = 10$, $|X_f| = 6$

for cycle and the fixed coordinates, respectively. Since C is doubly-even so is C_π [8].

Let w be a word or weight 6 in C_π. If $|\mathrm{Supp}(w) \cap X_c| = l$, then $|\mathrm{Supp}(w) \cap X_f| = 6 - l$ and $\mathrm{wt}(\pi^{-1}(w)) = 9l + 6 - l = 8l + 6 \equiv 2 \pmod 4$ will always lead to a singly-even code contrary to the above statement. Thus the case d_8^{2+} is rejected.

We have calculated all possible disjoint sets X_c and X_f for the remaining two codes. It turns out that there is a unique possible doubly-even code F_σ from d_{16}^+ with generator matrix $\pi^{-1}(B)$. □

Table 1: The orders of the automorphism group of the codes M_2

type	total	Aut(M_2)		
		9	18	27
MDS	3144	2965	170	9
NMDS	6703	6590	108	5

2.4 Hermitian self-dual codes M_1 over $\mathbb{F}_4$

We have that M_1 is a hermitian self-dual $[10, 5, \geq 4]$ code over $\mathbb{F}_4 \cong I_1 = \{0, x^s e_1, s = 0, 1, 2\}$, where $e_1 = x^8 + x^7 + x^5 + x^4 + x^2 + x$. There are two $[10, 5, 4]$ hermitian self-dual codes over $\mathbb{F}_4$ (see [6]) with generator matrices in the form $T_k = (E_5|X_i)$, $i = 1, 2$, where

$$X_1 = \begin{pmatrix} 1 & 1 & 1 & w & w^2 \\ 1 & 1 & 1 & w^2 & w \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}, X_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & w^2 & w^2 \\ 1 & w^2 & w & w & w \\ 0 & 0 & w & w^2 & 1 \\ 0 & 0 & w^2 & w & 1 \end{pmatrix}.$$

3 Results

Let C be an $[96, 48, 20]$ binary self-dual code with an automorphism (1). We consider the generator matrix of C in the form (2) and fix the first block as $\varphi^{-1}(H_i)$, $i = 1, \ldots, 9847$.

For a matrix G and permutation τ, denote by G^τ the matrix G with columns permuted by τ. Denote by F_σ^τ the code with generator matrix $\pi^{-1}(B^\tau)$.

Let $I \subseteq \{1, \ldots, 9847\}$ is the set of indices such that a subcode C' of C with minimum distance $d \geq 20$ with generator matrix $G_{1,i,\tau} = \begin{pmatrix} \varphi^{-1}(H_i) \\ F_\sigma^\tau \end{pmatrix}$ exists.

A computer program for calculating the minimum weight of the the code with generator matrix $G_{1,i,\tau}$, $i = 1, \ldots, 9847$, $\tau \in S_{10}$ give that $|I| = 390$.

For $k = 1, 2$ we consider all images $\gamma(T_k)$ of T_k, $k = 1, 2$ using compositions of the following maps: *(i)* a permutation $\tau \in S_{10}$ 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 $\overline{\omega}$. Next, we check the set of indices $J \subseteq I$ such that a subcode C'' of C with minimum distance $d \geq 20$ with generator matrix $G_{2,j,k} = \begin{pmatrix} \varphi^{-1}(H_j) \\ \varphi^{-1}(\gamma(T_k)) \end{pmatrix}$, $k = 1, 2$ exists.

For $k = 1, 2$ and $j \in I$ we have calculate all codes using only compositions of the maps (iii), (ii); and (i) for all permutations $\mu \in S_{10}$ from the right transversal R_k, of S_{10} with respect to $\mathrm{PAut}(T_k)$. The result was that all such codes have minimum distance $d < 20$ which proves Theorem 1.

References

[1] S. 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(10)**, 2005, 3678-3686.

[2] St. Bouyuklieva, J. De la Cruz, W. Willems, On the automorphism group of a binary self-dual [120, 60, 24] code, to appear in Applicable Algebra in Engineering, Communication and Computing, 2013.

[3] J. De la Cruz, Über die Automorphismengruppe extremaler Codes der Langen 96 und 120, Otto-von-Guericke-Universitat Magdeburg, PhD Thesis, 2012.

[4] J. De la Cruz, W. Willems, On extremal self-dual codes of length 96, *IEEE Trans. Inform. Theory*, **57(10)**, 2011, 6820-6823.

[5] W.C. Huffman, V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge University Press, 2003.

[6] J. H. Conway, V. Pless, N. J. A. Sloane, Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16, *IEEE Trans. Inform. Theory* **25**, 1979, 312-322.

[7] V. Pless, N. J. A. Sloane, A classification and enumeration of self-dual codes, *J. Combin. Theory* **18(3)**, 1975, 313-335.

[8] N. Yankov, A putative doubly even [72, 36, 16] code does not have an automorphism of order 9, *IEEE Trans. Inform. Theory* **58(1)**, 2012, 159-163.