МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 1999
MATHEMATICS AND EDUCATION IN MATHEMATICS, 1999
Proceedings of Twenty Eighth Spring Conference of
the Union of Bulgarian Mathematicians
Montana, April 5–8, 1999

# SELF-DUAL [24,12,8] QUATERNARY CODES WITH A PERMUTATION AUTOMORPHISM OF ORDER 3*

**Radka Russeva**

In this paper we apply a general decomposition theorem to find all Hermitian self-dual quaternary [24, 12, 8] codes which have a permutation automorphism of order 3. There exist at most 8 such codes up to equivalence.

**1. Introduction.** In [1] and [8] a complete enumeration of all self-dual quaternary codes of a length up to 16 is presented. It is reasonable for higher lengths $n$ to investigate only those of the largest minimum weight $d = 2\ [n/6] + 2$ . Such codes are called extremal. The extremal self-dual codes of lengths 18 and 20 are classified in [6]. All inequivalent extremal self-dual codes of lengths 22, 26 and 28 which have a nontrivial odd order automorphism are known [3,5]. In [7] the nonexistence of an [24, 12, 10] self-dual quaternary code was verified. All self-dual [24, 12, 8] quaternary codes possessing a monoial automorphism of prime order $r > 3$ are obtained up to equivalence in [9]. We proceed with the prime $r = 3$ now. We construct all [24, 12, 8] self-dual codes which have a permutation automorphism of order 3. We use a general decomposition theory of self-dual quaternary codes which possess a monomial automorphism of order a power of 3 developed in [4,5].

Let $C$ be an [n, k] code over $F_4 = GF(4)$ where $F_4 = \{0, 1, \omega, \omega^2\}$, with $\omega^2 = \omega + 1$. The Hermitian inner product $< .,. >$ in $F_4^n$ is given by

$$< u, v >= \sum_{i=1}^{n} u_i v_i^2 \text{ ,where } u, v \in F_4^n,\ u = (u_1, \cdots, u_n), v = (v_1, \cdots, v_n).$$

The dual of $C$ is the [n, n-k] code $C^\perp = \{v \in F_4^n :< u, v >= 0 \text{ for all } u \in C\}$. If $C \subseteq C^\perp$ it is called self-ortogonal and if $C = C^\perp$, $C$ is self-dual.

Define $M_n$ as the group of all $n \times n$ monomial matrices over $F_4$. Let $Gal(F_4) = \{1, \tau\}$ be the Galois group of $F_4$ and $M_n^\star$ be the semidirect product of $M_n$ extended by $Gal(F_4)$. If $T \in M_n^\star$, we write $T = PD\nu$, where $P$ is a permutation (matrix), $D$ is a diagonal matrix and $\nu \in Gal(F_4)$. Codes $C$ and $C'$ of length $n$ over $F_4$ are called equivalent whenever $C' = CT$ for some $T \in M_n^\star$. The automorphism group of the code $C$ is the group $Aut(C) = \{T \in M_n^\star : CT = C\}$. In [4] were examined the automorphisms $M$ of a code $C$ where $M$ was of Type I or Type II.

*This work was partially supported by the Bulgarian national Science Fund under Contract No.MM-503/1995.

**2. Construction Method.** For the remainder of the paper we assume $C$ is an [24, 12, 8] self-dual quaternary code possessing a permutation automorphism $P$ of order 3 with $c$ 3-cycles and $f$ fixed points, where $24 = 3c + f$. We can assume that $P$ acts as follows

(1) $$P = (1, 2, 3)(4, 5, 6) \dots (3c - 2, \dots, 3c)$$

Denote the r-cycles of $P$ by $\Omega_1, \Omega_2, \dots, \Omega_c$ and the fixed points by $\mathcal{F}$ .To decompose the code $C$ we applay the decomposition theory for a quaternary code possessing a Type I automorphism [5]. Denote by $R$ the semisimple ring $F_4[X]/\left\langle X^3 + 1\right\rangle$, where $X$ is an indeterminate. Then $R = I_0 \oplus I_1 \oplus I_2$, where the $I_k$ for $k = 0, 1, 2$ are the minimal ideals in $R$. Each $I_k$ is a field isomorphic to $F_4$, with identity $i_k(X) = 1 + \omega^{2k}X + \omega^k X^2$. Identify the element $a_0 + a_1\omega^{2k}X + a_2\omega^k X^2 \in R$ with the quaternary triple $a_0a_1a_2$. In (2) are presented the isomorphisms between the fields $F_4$ and $I_k$ for $k = 0, 1, 2$.

(2)

| $F_4$ | $I_0$ | $I_1$ | $I_2$ |
|---|---|---|---|
| $\mathbf{0}$ | 000 | 000 | 000 |
| $\mathbf{1}$ | 111 | $1\ \bar\omega\ \omega$ | $1\ \omega\ \bar\omega$ |
| $\omega$ | $\omega\ \omega\ \omega$ | $\omega\ 1\ \bar\omega$ | $\omega\ \bar\omega\ 1$ |
| $\bar\omega = \omega^{\mathbf{2}}$ | $\bar\omega\ \bar\omega\ \bar\omega$ | $\bar\omega\ \omega\ 1$ | $\bar\omega\ 1\ \omega$ |

If $v \in F_4^n$ let $x|\Omega_i$ be the restriction of v to $\Omega_i$. Define $E_0(M) = \{v \in C : v|\Omega_i \in I_0$ for $1 \le i \le c\} = \{v \in C : vM = v\}$, and for $k = 1, 2$ $E_k(M) = \{v \in C : v|\Omega_i \in I_k$ for $1 \le i \le c$ and $v_i = 0$ if $i \in \mathcal{F}\}$. Notice that if $v \in E_k(M), vM = \omega^k v$. By Theorem 1 of [4] $C = E_0(P) \oplus E_1(P) \oplus E_2(P)$. Associate to $u \in E_0(P)$ an element $u^\star = (u_1^\star, \cdots, u_{c+f}^\star) \in F_4^{c+f}$, where for $1 \le i \le c, u_i^\star = u_j$ for some $j$ in $\Omega_i$ and for $1 \le i \le c + f$ $u_i^\star = u_i$. For $k = 1, 2$ associate to $u \in E_k(P)$ an element $u^\star = (u_1^\star, \cdots, u_c^\star) \in F_4^c$, where $u_i^\star = u|\Omega_i$ viewed as an element of $I_k$. Define $E_k(P)^\star = \{u^\star : u \in E_k(P)\}$ for $k = 0, 1, 2$. Because $C$ is self-dual, by Theorem 1 of [4], so are $E_k(P)^\star$ presented as codes over the fields $I_k$ for $k = 0, 1, 2$.

We use the following transformations which preserve the decomposition and lead the code $C$ to an equivalent code $C'$:

a) permutations of the first c 3-cycles of $C$.

b) permutations of the last f coordinates of $C$.

c) multiplication of each 3-cycle $\Omega_i$, $1 \le i \le c$ and each fixed point by constants from $F_4$.

d) cycle shifts to the entries of the 3-cycles independently which is equivalent to scaling the columns of $E_k(P)^\star$ by power of $w^k$.

e) transformation $s\tau$ where $s = (2, 3)(5, 6) \cdots (3c - 1, 3c)$ which acts as conjugation on $E_k(P)^\star$.

f) permutations to the fields $I_k$ when the codes $E_k(P)^\star$ are of the same dimension which permute these codes .

Let the subgroups of $M_n^\star$ generated by these transformations be $\Sigma_c, \Sigma_f, D, W,$ $< s\tau >$, and $S$ respectively.

The equivalence of two codes with the same Type I automorphism was discussed in [5]. In particular for [24, 12, 8] self-dual codes with a permutation automorphism $P$ defined in (1) we obtain the following theorem:

**Theorem 1.** *Let $C$ and $C'$ have the same permutation automorphism $P$.*

*1) Assume $< P, \omega I >$ is a Syllow 3-subgroup of $Aut(C)$. Then $C$ and $C'$ are equivalent iff $C' = CN$ for some $N \in \Sigma_c \Sigma_f D < s\tau > SW$.*

*2) Suppose $C' = CN$ with $N \in \Sigma_c \Sigma_f D < s\tau > SW$ then $N = TQ$ where $T \in \Sigma_c \Sigma_f D < s\tau >$ and $Q \in SW$. Let $\hat{T}$ be the action of $T$ induced on $E_0(P)^\star$. Then $E_0(P)^\star \hat{T} = E_0'(P)^\star$ and if $E_0(P) = E_0'(P)$ then $\hat{T} \in Aut(E_0(P)^\star)$.*

**2. Results.** The only two possibilities for $(c, f)$ are (8, 0) and (6, 6) [9].

**The case c=8, f=0**. Let $C$ be a self-dual [24, 12, 8] code with a permutation automorphism $P$ with 8 3-cycles without fixed points. The codes $E_k(P)^\star$ for k=0,1,2 are self-dual [8, 4, d] quaternary codes with $d \geq \frac{8}{3}$ because of minimal distance of $C$. By [8] $E_k(P)^\star = E_8$. We can fix a binary generator matrix for $E_0(P)^\star$ in the form

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \tag{3}$$

Generator matricies for $E_i(P)^\star, i = 1, 2$ may be obtained from $gen(E_0(P)^\star)$ by transposition of the columns.

To construct a generator matrix of the code $E_k(P)$ we replace the entries of $gen(E_k(P)^\star)$ by the corresponding 3-tuples in (1).

**Lemma 1.** *There is not a binary 4-weight vector contained in each $E_k(P)^\star$ at the same time.*

**Proof**. Since $i_o(X) + i_1(X) + i_2(X) = 1$ then if the codes $E_k(P)^\star$ contain one and the same 4-weight binary vector, the sum of the corresponding vectors in $E_k(P)$ is a 4-weight vector in C - a contradiction.

To determine generator matricies of $E_1(P)^\star$ and $E_2(P)^\star$ we use a terminology given in [2]. Call a duo any pair of coordinates. A cluster for a code is a set of disjoint duos such that the union of any two duos is a support of a 4-weight vector of the code. A d-set for a cluster is a subset of coordinates containing precisely one element of each duo in the cluster. A defining set of a code consist of a cluster and a d-set provided that the 4-weight vectors arrising from the cluster and the vector with support the d-set generate the code.

$E_8$ has a defining set. We try to find defining sets of $E_1(P)^\star$ and $E_2(P)^\star$ satisfying Lemma 1. The 3-transitivity of $Aut(A_8)$ implies that a cluster for $E_8$ can be chosen so that any pair of coordinates forms a duo. So we can assume that {1, 2} is a duo for $E_1(P)^\star$ and $E_2(P)^\star$. Applying permutation from $Aut(E_0(P)^\star)$ we obtain all possible defining sets for $E_1(P)^\star$. In a similar manner by the permutations that do not affect $gen(E_0(P)^\star)$ and $gen(E_1(P)^\star)$ we obtain all possibilities for $gen(E_2(P)^\star)$. We find 43 cases for $gen(C)$. Applying elements from $\Sigma_c S$ we by hand reduce the number of cases to check. We obtain 3 classes [24, 12, 8] self-dual codes. Denote by $C_1, C_2$ and $C_3$ their representatives. The codes $C_2$ and $C_3$ have the same weight enumerators. In the next table we give a defining set of $E_k(P)^\star, k = 1, 2$ for these codes and the number $A_8$ of

8-weight vectors in them.

| | defining set of $E_1(P)^\star$ | defining set of $E_2(P)^\star$ | $A_8$ |
|---|---|---|---|
| $C_1$ | {1,2}, {3,4}, {5,6}, {7,8}; 1,3,5,7 | {1,2}, {3,5}, {4,7}, {6,8}; 1,3,4,8 | 2277 |
| $C_2$ | {1,2}, {3,4}, {5,6}, {7,8}; 1,3,5,8 | {1,2}, {3,5}, {4,7}, {6,8}; 1,3,4,6 | 1089 |
| $C_3$ | {1,2}, {3,5}, {4,7}, {6,8}; 1,3,4,6 | {1,2}, {3,8}, {4,6}, {5,7}; 1,3,4,5 | 1089 |

In these notation for the code $C_1$ $gen(E_1(P)^\star = gen(E_0(P)^\star$ presented in (3) and $gen(E_2(P)^\star = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$. We can formulate the following theorem.

**Theorem 2.** *There exist at most 3 inequivalent [24, 12, 8] self-dual codes possessing a permutation automorphism of order 3 with 8 cycles without fixed points..*

**The case c=6, f=6.** Let $P$ be a permutation automorphism defined in (1) with 6 3-cycles and 6 fixed points. We obtain the following theorem:

**Theorem 3.** *There exist at most 6 inequivalent [24, 12, 8] self-dual codes possessing a permutation automorphism of order 3 with 6 cycles and 6 fixed points.*

**Proof:** In this case $E_0(P)^\star$ is an [12, 6] self-dual quaternary code. Its minimal distance is at least $\frac{8}{3}$. Hence by [8] $E_0(P)^\star = E_6 \oplus E_6, E_{12}, C_{12}, D_{12}$ or $F_{12}$. The codes $E_k(P)^\star$ are [6, 3, 4] self-dual quaternary codes for $k = 0, 1, 2$.

Let $E_0(P)^\star$ be $E_6 \oplus E_6$. Since $E_6$ is an MDS [6, 3, 4] code there is a 4-weight vector in $E_6$ nonzero on three fixed points, which leads to a low weight vector in $C$.

Let $E_0(P)^\star$ be $E_{12}$. This code has a defining set. If any of the duos consists of fixed points or cycle coordinates we would obtain a low weight vector in $E_0(P)$. Therefore we can fix the $gen(E_0(P)^\star)$ in the form

$$gen(E_0(P)^\star = \left(\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

with the fixed points on the right.

Let $E_0(P)^\star = C_{12}, D_{12}, F_{12}$. We examin the generator matricies of these codes given in [8] and the vectors of weight 4 in them. We consider all alternatives for fixed points.

When $E_0(P)^\star = C_{12}$ there always exists a 4-weight vector in it nonzero on 3 or 4 fixed points. This contradicts $E_0(P)^\star = C_{12}$.

When $E_0(P)^\star = D_{12}$ or $F_{12}$ we obtain a unique possibility for $gen(E_0(P)^\star)$ up to equivalence in the form $\left( \begin{array}{c|c} I_6 & A \end{array} \right)$, where $A$ is the matrix

$$\begin{pmatrix} 0 & 1 & 1 & \omega & \omega & \omega \\ 1 & 0 & 1 & \omega & \omega & \omega \\ 1 & 1 & 0 & \omega & \omega & \omega \\ \omega & \omega & \omega & 0 & 1 & 1 \\ \omega & \omega & \omega & 1 & 0 & 1 \\ \omega & \omega & \omega & 1 & 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & \bar\omega & \bar\omega & 1 & 1 \\ 0 & 1 & \bar\omega & \bar\omega & 1 & 1 \\ \omega & \omega & 0 & 1 & 1 & 1 \\ \omega & \omega & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \text{ respectively.}$$

We obtain $gen(E_1(P)^\star)$ by row reducing, scaling columns and applying elements from $Aut(E_0(P)^\star)$. In any choice of $gen(E_0(P)^\star)$ the generator matrix for $E_1(P)^\star$ can be fixed in the form $gen(E_1(P)^\star) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \bar{\omega} \\ 0 & 0 & 1 & 1 & \bar{\omega} & \omega \end{pmatrix}$. Then by row reducing we obtain

$$gen(E_2(P)^\star) = \begin{pmatrix} 1 & 0 & 0 & b & c & d \\ 0 & 1 & 0 & e & x & y \\ 0 & 0 & 1 & f & z & t \end{pmatrix} \tag{4}$$

where $b, c, d, e, f \in \{1, \omega, \bar{\omega}\}$, $x = \bar{b}ce\gamma, y = \bar{b}de\bar{\gamma}, z = \bar{b}cf\bar{\gamma}, t = \bar{b}df\gamma$ and $\gamma \in \{\omega, \bar{\omega}\}$. All coordinates in $gen(E_1(P)^\star)$ and $gen(E_2(P)^\star)$ are cyclic. To obtain the generator matricies of subcodes $E_k(P), k = 0, 1, 2$ we replace the cycle coordinates of $E_k(P)^\star$ by the corresponding triples in (2). We save the fixed points in $gen(E_0(P)^\star)$ and adjoin 000000 at the end of each row in $gen(E_j(P)^\star), j = 1, 2$. To reduce the number of cases to check we applay to code $C$ by computer elements from groups $\hat{G} = \{\hat{T} : T \in \Sigma_c\Sigma_f D < s\tau >\} \cap Aut(E_0(P)^\star)$ followed by elements from $SW$. In any case of $E_0(P)^\star$ we receive two classes codes with representatives for $gen(E_2(P)^\star)$ in the form (4) with $b = c = d = e = f$ and $\gamma = \omega$ or $\bar{\omega}$. The notation of the obtained codes is given in the table bellow. The codes are with 4 different spectrums.

| | $C_4$ | $C_5$ | $C_6$ | $C_7$ | $C_8$ | $C_9$ |
|---|---|---|---|---|---|---|
| $E_0(P)^\star$ | $E_{12}$ | $E_{12}$ | $D_{12}$ | $D_{12}$ | $F_{12}$ | $F_{12}$ |
| $\gamma$ in $gen(E_2(P)^\star)$ | $\omega$ | $\bar{\omega}$ | $\omega$ | $\bar{\omega}$ | $\omega$ | $\bar{\omega}$ |
| $A_8$ | 1413 | 2277 | 792 | 792 | 837 | 837 |

**Remark:** The code $C_1$ has a binary generator matrix which generates over $F_2$ the extended [24,12,8] Golay code. It is known that this binary code has an automorphism of order 3 with 6 cycles and 6 fixed points. Therefore the quaternary code $C_1$ has such automorphism too. Between the quaternary codes with such automorphism the code $C_5$ is a unique which has the same weight enumerator as $C_1$. So these codes must be equivalent. It is an open question to distingish the other codes with identical weight distributions. The obtained codes are with 5 different spectrums.

The following theorem summarize the results of Theorem 1, Theorem 2, and the remark.

**Theorem 4.** *All self-dual [24, 12, 8] quaternary codes with a permutation automorphism of order 3 are equivalent to one of the codes* $C_1, C_2, C_3, C_4, C_6, C_7, C_8$ *and* $C_9$ *constructed above.*

## REFERENCES


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

[2] W.C.Huffman, Automorphisms of codes with applications to extremal doubly even codes of length 48,*IEEE Trans. Inform. Theory* **IT-28** (1982), 511-521.

[3] W.C.Huffman, On extremal self-dual quaternary codes of length 18 to 28,I, *IEEE Trans. Info. Theory* **IT-36** (1990), 651-660.

[4] W.C.Huffman, On 3-elements in Monomial Automorphism Groups of Quaternary Codes, and the group of a [24, 12, 10] Code, *IEEE Trans. Info. Theory* **IT-36** (1990), 660-664.

[5] W.C.Huffman, On extremal self-dual quaternary codes of length 18 to 28, II,*IEEE Trans. Info. Theory* **IT-37** (1991), 1206-1216.
[6] W.C.Huffman, Characterisation of Quaternary Extremal Codes of Lengths 18 and 20, *IEEE Trans. Info.Theory* **43** (1997), 1613-1616.
[7] C.W.H.Lam and V.Pless, There is no [24, 12, 10] self-dual quaternary code, *IEEE Trans.Inform.Theory* **36**, (1990), 1153-1156.
[8] F.J.Mac Williams, A.M.Odlyzko, N.J.A.Sloane and H.N.Ward, Self-dual codes over GF(4), *Journ. Combin. Theory* **A25** (1978), 288-318.
[9] V. Yorgov, R. Russeva, On the [24, 12, 8] Self-Dual quaternary codes, *Math. and Education in Math.* **27** (1998), 167-172.

Radka Peneva Russeva
University of Shoumen
Faculty of Mathematics Informatics and Economics
9700 Shoumen
Bulgaria

## САМОДУАЛНИ [24, 12, 8] КОДОВЕ НАД ПОЛЕ С 4 ЕЛЕМЕНТА ПРИТЕЖАВАЩИ ПЕРМУТАЦИОНЕН АВТОМОРФИЗЪМ ОТ РЕД 3

**Радка Пенева Русева**

В тази статия се прилага общата теория за разлагане на кодове. Конструирани са всички самодуални [24, 12, 8] кодове над поле с 4 елемента, притежаващи пермутационен автоморфизъм от ред 3. Получихме, че съществуват най-много 8 такива кодове с точност до еквивалентност.