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

ON THE NO EXISTENCE OF A [80,40,16] SELF-DUAL CODE WITH AN AUTOMORPHISM OF PRIME ODD ORDER GREATER THAN 7*

Radinka Dontcheva

A [80,40,16] self-dual code of type I cannot have an automorphism of odd prime order greater than 7.

1. Introduction. Let C be a [80,40,16] a self-dual code of type I. It is known [1] that this code has weight enumerators

$$W_1(y) = 1 + (54045 + 256\alpha)y^{16} + (675840 - 2048\alpha)y^{18} + \tag{1}$$
$$(6376192 + 5120\alpha)y^{20} + \cdots$$

and

$$W_2(y) = 1 + 58653y^{16} + 622592y^{18} + 6697728y^{20} + \cdots \tag{2}$$

It is not known whether such a code exists. In this work we try to find such code C applying known method for constructing codes via automorphisms (see [2,4]) and basic theorems in Algebra.

Suppose C has an automorphism σ of odd prime order p with c cycles and f fixed points. We say for short that σ is of type $p-(c,f)$. We denote the cycles of σ by $\Omega_1, \Omega_2, ..., \Omega_c$ and the fixed points by $\Omega_{c+1}, \Omega_{c+2}, ..., \Omega_{c+f}$. Define $F_\sigma(C) = \{v \in C : v\sigma = v\}$ and $E_\sigma(C) = \{v \in C : wt(v|\Omega_i) \equiv 0 \ (mod\ 2),\ i = 1, \ldots, c+f\}$, where $v|\Omega_i$ is the restriction of v on Ω_i. It is known [2] that $C = F_\sigma(C) \oplus E_\sigma(C)$ (a direct sum). Let P be a set of all even weight polynomials in $F_2(x)/\ (x^p - 1)$. It is known that P is a ring with a unit $e(x) = x + x^2 + \ldots + x^{p-2} + x^{p-1}$.

Every vector $v \in F_\sigma(C)$ is constant on each cycle. Let $\pi(F_\sigma(C))$ be a code obtained from $F_\sigma(C)$ by replacing each restriction $v|\Omega_i$, $i = 1, 2, ..., c$, by one of its coordinates. We denote $E_\sigma(C)^*$ the code $E_\sigma(C)$ with the last f coordinates deleted. For $v \in E_\sigma(C)^*$ we can consider each $v|\Omega_i = (a_0, a_1, ..., a_{p-1})$ as a polynomial $a_0 + a_1x + ... + a_{p-1}x^{p-1}$ in the cyclic code P of length p consisting of all even-weight polynomials in $F_2[x]|(x^p - 1)$. The result is denoted by $\varphi(v)$. For each $u, v \in \varphi(E_\sigma(C)^*)$ it holds:

$$u_1(x)v_1(x^{-1}) + u_2(x)v_2(x^{-1}) + ... + u_c(x)v_c(x^{-1}) = 0. \tag{3}$$

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

We will use the following transformations leading to equivalent codes [4]:

(i) a substitution $x \to x^t$ in $\varphi(E_\sigma(C)^*)$, where t is an integer, $1 \le t \le p-1$;

(ii) a multiplication of the j-th coordinate of $\varphi(E_\sigma(C)^*)$ by x^{t_j}, where t_j is an integer, $0 \le t_j \le p-1,\ j = 1, 2, \ldots, c$;

(iii) a permutation of the first c cycles of C;

(iv) a permutation of the last f coordinates of C.

2. Results. The main result of this work is the next theorem.

Theorem 1. *A [80,40,16] self-dual code of type I cannot have an automorphism of odd prime order greater then 7.*

Lemma 1. *Let C be a [80,40,16] self-dual code with an automorphism σ of odd prime order p greater than 7. Then for $p-(c, f)$ exist following cases: $19-(4,4)$ and $13-(6,2)$.*

Proof. The cases $79-(1,1), 73-(1,7), 71-(1,9), 67-(1,13), 61-(1,19), 59-(1,21), 53-(1,27), 47-(1,33), 43-(1,37), 41-(1,39), 37-(1,43), 37-(2,6), 31-(1,49), 31-(2,18), 29-(1,51), 29-(2,22), 23-(1,57), 23-(2,34), 23-(3,11), 19-(1,61), 19-(2,42), 19-(3,23), 17-(1,63), 17-(2,46), 17-(3,29), 17-(4,12), 13-(1,67), 13-(2,54), 13-(3,41), 13-(4,28), 13-(5,15), 11-(1,69), 11-(2,58), 11-(3,47), 11-(4,36), 11-(5,25)$ and $11-(6,14)$ do not satisfy conditions i) and ii) of the Theorem 1 of [4]. The case $11-(7,3)$ contradicts Corollary 2 of [4].

Lemma 2. *Threre does not exist a [80,40,16] self-dual code of type I with an automorphism of order 13.*

Proof. Suppose C is a [80,40,16] self-dual code with an automorphism σ of type 13-(6,2). Hence $\pi(F_\sigma(C))$ is a [8,4] self-dual binary code (see [4]). All such codes are C_2^4 and A_8 [3].

Let $\pi(F_\sigma(C))$ be C_2^4. Then $(F_\sigma(C))$ has a vector with weight 14. This eliminate C_2^4.

If $\pi(F_\sigma(C))$ is A_8 then the weight enumerator to $(F_\sigma(C))$ has coefficients: $B_{28} = 3, B_{40} = 8, B_{52} = 3, B_{70} = 1$ and every other is zero. Let C have weight enumerator W_1. Then it is necessarily that $A_{16} \equiv 0\ (mod\ 13)$ and $A_{18} \equiv 0\ (mod\ 13)$. We have $A_{16} \equiv 4 + 9\alpha\ (mod\ 13)$, $A_{18} \equiv 9 - 11\alpha\ (mod\ 13)$. Then $\alpha \equiv 1\ (mod\ 13)$ and $\alpha \equiv 2\ (mod\ 13)$. This contradiction eliminates the case to W_1. As in W_2 $A_{16} \equiv 10\ (mod\ 13)$ we obtain that σ is not an automorphism of order 13.

Lemma 3. *There does not exist a [80,40,16] self-dual code of type I with an automorphism of order 19.*

Proof. Suppose C has an automorphism σ of order 19 with 4 cycles and 4 fixed points. Hence $\varphi(E_\sigma(C)^*)$ is a [4,2] self-dual code. The polynomial $x^{18} + x^{17} + ... + x + 1$ is irreducible over field F_2. Hence P is a direct sum of one irreducible cyclic code (see [4]) of length p, denoted with I. We have $I = \{0, e_j, \mu(x), \mu^2(x), ..., \mu^{2^{18}-2}(x)\}$ where $e = x^{18} + x^{17} + ... + x^2 + x$ and $\mu(x) = x^6 + x^3 + x + 1$ is a primitive element in I. Then $\varphi(E_\sigma(C)^*)$ is a code over the field I. Hence the possible generator matrices for $\varphi(E_\sigma(C)^*)$ are

$$\begin{pmatrix} e_1 & 0 & \alpha_1(x) & \alpha_2(x) \\ 0 & e_1 & \alpha_3(x) & \alpha_4(x) \end{pmatrix},$$

where $\alpha_i(x) \in I$ for $i = 1, 2, 3, 4$.

Applying (3) we obtain the following cases for the first row to the above matrix:

$$(e(x) \quad 0 \quad \mu^{t_1}(x) \quad 0) \tag{4}$$

and

$$(e(x) \quad 0 \quad \mu^{t_1}(x) \quad \mu^{t_2}(x)\ , \tag{5}$$

for $t_i = 0, ..., 2^{18} - 2$ for $i = 1, 2$.

The case (4) is developed in [4] and the inequivalent cases are: $(e(x) \quad 0 \quad e(x) \quad 0)$, $(e(x) \quad 0 \quad \mu^{511\times 19}(x) \quad 0)$, $(e(x) \quad 0 \quad \mu^{511\times 19\times 3}(x) \quad 0)$ and $(e(x) \quad 0 \quad \mu^{511\times 19\times 9}(x) \quad 0)$.

If we add the first and the second row of the corresponding generator matrices for $\varphi(E_\sigma(C)^*)$ in the all four cases we obtain a vector with weight at most 14.

Let us consider the case (5). Applying transformations (i), (ii), (iii) and (iv) to the first row we obtain

$$(e_1 \quad 0 \quad \delta^{t_1}(x) \quad \delta^{t_2}(x))$$

where $\delta(x) \in I$ is of order $7 \times 27 \times 73$, $t_i = 1, ..., 7 \times 27 \times 73$ for $i = 1, 2$. It follows from (3) that $\delta^{t_1(2^9+1)}(x) + \delta^{t_2(2^9+1)}(x) = e(x)$. Let $\gamma(x) = \delta^{513}(x)$. The order of $\gamma(x)$ is 511 and it is a primmitive element of a field of 512 elements. From the addition and multiplication tables of this field and the equality $e(x)+\gamma^{t_1'}(x) = \gamma^{t_2'}(x)$ we can determine all possibilities for (t_1', t_2'). Since $(2t_1', 2t_2')$ and (t_1', t_2') lead to equivalent codes, we obtain only : $t_1 = t_1' + 511 \times k_1$, $t_2 = t_2' + 511 \times k_2$, where $k_i = 0, ..., 26$ for $i = 1, 2$ and (t_1', t_2') and (t_2', t_1') can be $(1, 93)$, $(3, 262)$, $(5, 408)$, $(7, 505)$, $(9, 59)$, $(11, 248)$, $(15, 37)$, $(17, 343)$, $(19, 105)$, $(21, 87)$, $(23, 383)$, $(25, 251)$, $(27, 409)$, $(29, 178)$, $(35, 231)$, $(39, 111)$, $(41, 332)$, $(43, 246)$, $(45, 61)$, $(47, 340)$, $(53, 375)$, $(55, 428)$, $(57, 366)$, $(63, 190)$, $(73, 219)$, $(79, 491)$, $(91, 167)$, $(109, 341)$ and $(125, 187)$.

Applying (iii) for the above cases we reduce the values for (t_1', t_2') and (t_2', t_1') to the following cases:

$$(1, 93), (3, 262), (5, 408), (9, 59), (11, 248), (17, 343), (19, 105), (29, 178)$$

$$(35, 231), (41, 332)\ \textit{and}\ (73, 219). \tag{6}$$

We can consider a generator matrix for $\varphi(E_\sigma(C)^*)$ of the form

$$\begin{pmatrix} e(x) & 0 & \delta^{t_1}(x) & \delta^{t_2}(x) \\ 0 & e(x) & \delta^{t_3}(x) & x^s.\delta^{t_4}(x) \end{pmatrix}$$

where $t_i = 1, ..., 7 \times 27 \times 73$ for $i = 3, 4$ and $s = 0, ..., 18$.

From the orthogonal condition (3) for the second row we obtain $\delta^{t_3(2^9+1)}(x) + \delta^{t_4(2^9+1)}(x) = e(x)$. Hence $t_3 = t_3' + 511 \times k_3, t_4 = t_4' + 511 \times k_4$, where $k_i = 0, ..., 26$ for $i = 3, 4$ and (t_3', t_4') and (t_4', t_3') can be (6).

The same condition (3) we apply for first and second row. It is follows $\delta^{t_3+2^9 t_1}(x) = x^s.\delta^{t_4+2^9 t_2}(x)$. We denote $t_3 + 2^9 t_1 = l_1$ and $t_4 + 2^9.t_2 = l_2$. Hence

$$\delta^{l_1}(x) = x^s \delta^{l_2}(x). \tag{7}$$

Denote by r_1 the order of δ^{l_2}. We have that δ^{l_2} and x^s are in field I, $\delta^{l_2}.x^s = x^s.\delta^{l_2}$, the order on x^s is 19 for $s = 1, ..., 18$ and $(r_1, 19) = 1$. Then the element $x^s.\delta^{t_2}(x) \in I$ has a order $19 \times r_1$. It follows from (7) that the element δ^{l_1} has order $19 \times r_1$ but 19 does not divide the order of δ^{l_1}. Hence $s = 0$ and the matrix for $\varphi(E_\sigma(C)^*)$ can be the following:

$$\begin{pmatrix} e(x) & 0 & \delta^{t_1{}'+511.k_1}(x) & \delta^{t_2{}'+511.k_2}(x) \\ 0 & e(x) & \delta^{t_3{}'+511.k_3}(x) & \delta^{t_4{}'+511.k_4}(x) \end{pmatrix}.$$

Applying (3) we obtain $\delta^{t_3+t_1 2^9+511(k_3+k_1 2^9)}(x) = \delta^{t_4+t_2 2^9+511(k_4+k_2 2^9)}(x)$

Hence $t_3 + t_1 2^9 + 511(k_3 + k_1 2^9) \equiv t_4 + t_2 2^9 + 511(k_4 + k_2 2^9)(mod\, 511)$ and $t_1{}' - t_2^{'} \equiv t_4{}' - t_3^{'}(mod\, 511)$. It follows that $(t_3{}', t_4{}') = (t_2{}', t_1{}')$.

Using GFQ for every case of $t_1^{'}, t_2^{'}$ we obtain the values for $\delta^{t_1^{'}+511k_1}(x)$ and $\delta^{t_2^{'}+511k_2}(x)$ for $k_i = 0, ..., 26, i = 1, 2$ We include them in computer program and obtain that in all cases the matrix of the code $E_\sigma(C)$ has a vector with a weight at most 14.

Apllying the Lemma 1, Lemma 2 and Lemma 3 completes the proof of the theorem.

Acknowledgment: I would to thank V. Yorgov for the useful discussions.

REFERENCES

[1] Joe Fields,V. Pless. Split weight enumerators of extremal self-dual codes, pre-print.

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

[3] V.Pless. A classification of self-orthogonal codes over GF(2), Discrete Math., vol. 3 (1972) 209-246.

[4] V.Y.Yorgov. Binary self-dual codes with automorphisms of odd order (in Russian), *Probl.Pered.Inform.* **19** (1983) 11-24.

Радинка Александрова Дончева
Катедра Алгебра при ФМИИ на
Шуменски Университет „Еп. Константин Преславски“
Шумен 9712

НЕСЪЩЕСТВУВАНЕ НА [80,40,16] САМОДУАЛЕН КОД С АВТОМОРФИЗЪМ ОТ НЕЧЕТЕН ПРОСТ РЕД ПО-ГОЛЯМ ОТ 7

Радинка Александрова Дончева

Самодуален [80,40,16] код от тип I не притежава автоморфизъм от нечетен прост ред по-голям от 7.