Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 103–108*

Some binary self-dual codes having an automorphism of order 15 [1]

Stefka Bouyuklieva stefka@uni-vt.bg
Faculty of Mathematics and Informatics, Veliko Tarnovo University,
and Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
5000 Veliko Tarnovo, Bulgaria
Nikolay Yankov jankov_niki@yahoo.com
Faculty of Mathematics and Informatics, Shumen University, Bulgaria

Abstract. In this paper we study the self-dual codes of lengths 98 and 100 with minimum weight 18 invariant under a cyclic group of order 15. We prove that the putative self-dual $[98, 49, 18]$ codes do not have automorphisms of order 15.

1 Introduction

Let $d(n)$ be the largest minimum weight among singly even self-dual codes of length n. The current state of knowledge about $d(n)$ for $98 \leq n \leq 114$ is given in Table 1 (see [4]). We see that $d(n) \leq 18$ for $n \leq 106$, $n \neq 104$, but self-dual $[n, n/2, 18]$ codes for these values of n are not known instead if $n = 102$.

Table 1: Largest Minimum Weights Of Singly Even Self-Dual Codes

n	98	100	102	104	106	108	110	112	114
$d(n)$	16,18	16,18	18	18,20	16,18	16,18,20	18,20	18,20	18,20

We consider the construction of self-dual codes with minimum weight 18 of length $n = 98$ and 100, using their possible automorphism of order 15. We begin with some important statements. Let σ be an automorphism of the self-dual code C of order r where r is odd (not necessarily a prime), and let

$$\sigma = \Omega_1\Omega_2 \ldots \Omega_m \tag{1}$$

be the factorization of σ into disjoint cycles (including the cycles of length 1). If l_i is the length of the cycle Ω_i then $\mathrm{lcm}(l_1, \ldots, l_m) = r$ and l_i divides r.

[1]This research is partially supported by VTU University Project RD-09-422-13/09.04.2014 and Shumen University Project RD-03-243/12.03.2014.

Let $F_\sigma(C) = \{v \in C : v\sigma = v\}$ and

$$E_\sigma(C) = \{v \in C : \mathrm{wt}(v|\Omega_i) \equiv 0 \pmod 2,\ i = 1, \dots, m\},$$

where $v|\Omega_i$ is the restriction of v on Ω_i. Then the following theorems hold.

Theorem 1. *The code C is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$.*

Let $\pi : F_\sigma(C) \to \mathbb{F}_2^m$ be the projection map, i.e., $(\pi(v))_i = v_j$ for some $j \in \Omega_i$, $i = 1, 2, \dots, m$. Clearly, $v \in F_\sigma(C)$ if and only if $v \in C$ and v is constant on each cycle.

Theorem 2. *If C is a binary self-dual code with an automorphism σ of odd order then $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual code of length m.*

Another important construction which we consider is the following. Let C be a self-dual code of length $n = n_1 + n_2$, and let $\mathcal{B}$, respectively $\mathcal{D}$, be the largest subcode of C whose support is contained entirely in the left n_1, respectively, right n_2, coordinates. Suppose $\mathcal{B}$ and $\mathcal{D}$ have dimensions k_1 and k_2, respectively. Let $k_3 = k - k_1 - k_2$ where $k = n/2$ is the dimension of C. Then there exists a generator matrix for C in the form

$$G = \begin{pmatrix} B & O \\ O & D \\ E & F \end{pmatrix}, \tag{2}$$

where B is a $k_1 \times n_1$ matrix with $gen(\mathcal{B}) = [B\ O]$, D is a $k_2 \times n_2$ matrix with $gen(\mathcal{D}) = [O\ D]$, O is the appropriate size zero matrix, and $[E\ F]$ is a $k_3 \times n$ matrix. Let $\mathcal{B}^*$ and $\mathcal{B}_E$ be the codes of length n_1 generated by B and $\binom{B}{E}$, $\mathcal{D}^*$ and $\mathcal{D}_F$ be the codes of length n_2 generated by D and $\binom{D}{F}$, respectively. The following theorem is a modification of [1, Theorem 9.4.1]:

Theorem 3. *With the notation of the previous paragraph*
(i) $k_3 = rank(E) = rank(F)$,
(ii) $k_2 = k + k_1 - n_1 = k_1 + \frac{n_2 - n_1}{2}$, and
(iii) $\mathcal{B}_E^\perp = \mathcal{B}^*$ and $\mathcal{D}_F^\perp = \mathcal{D}^*$.

2 On the structure of the codes

Let C be a self-dual $[n = 98 \text{ or } 100, n/2, 18]$ code with an automorphism σ of type 15-(c, t_5, t_3, f), which means that σ has c 15-cycles, t_5 5-cycles, t_3 3-cycles and f fixed points in its decomposition into irreducible cycles. Moreover,

- the permutation σ^3 is an automorphism of C of type 5-$(3c + t_5, 3t_3 + f)$;
- the permutation σ^5 is an automorphism of C of type 3-$(5c + t_3, 5t_5 + f)$.

We use the properties of the binary self-dual codes having automorphisms of orders 3 and 5 (see [5], [7]). Let τ_p be an automorphism of C of order p where $p = 3$ or 5, and let τ_p has exactly c_p independent p-cycles and $f_p = n - pc_p$ fixed points in its factorization. For $v \in E_{\tau_p}(C)$ we let $v|\Omega_i = (v_0, v_1, \ldots, v_{p-1})$ correspond to the polynomial $v_0 + v_1x + \cdots + v_{p-1}x^{p-1} \in P_p$, where P_p is the set of even-weight polynomials in $\mathbb{F}_2[x]/(x^p + 1)$, $i = 1, \ldots, c_p$. Thus we obtain the map $\phi_p : E_{\tau_p}(C) \to P_p^{c_p}$. For both primes $p = 3$ and $p = 5$, P_p is a field with 2^{p-1} elements and we can apply the following theorem [5].

Theorem 4. *The binary code C with an automorphism τ_p is self-dual iff the following two conditions hold:*
(i) $\pi(F_{\tau_p}(C))$ is a self-dual binary code of length $c_p + f_p$;
(ii) $\phi_p(E_{\tau_p}(C))$ is a Hermitian self-dual code of length c_p over the field P_p.

It follows that $\phi(E_{\tau_3}(C))$ is a Hermitian self-dual code of length c_3 over the quaternary field $P_3 = \{0, x + x^2, 1 + x, 1 + x^2\}$. Since we consider binary codes with minimum weight $d = 18$, the minimum weight of this quaternary code must be at least 10. Hence $c_3 \geq 28$ (see Table 7 in [6]), and therefore $5c + t_3 \geq 28$. To reduce the possibilities for the parameters c, t_5, t_3 and f, we use the following lemma [7].

Lemma 1. *If τ_p is an automorphism of the binary self-dual code C with c_p cycles and f_p fixed points, and $g_2(k, d) = \sum_{i=0}^{k-1} \lceil d/2^i \rceil$ then:*
1) $pc_p \geq g(\frac{(p-1)c_p}{2}, d)$;
2) if $f_p > c_p$, then $f_p \geq g_2((f_p - c_p)/2, d)$;
3) if 2 is a primitive root modulo p then c_p is even.

Applying this lemma in the considered case, we obtain that $c_5 \geq 16$. If $c_5 = 16$ then $f_5 = 18$, and the fixed code $\pi(F_{\tau_p}(C))$ will be a self-dual binary code of length 34. Consider a generator matrix of this code in the form (2). Since D must generate a $[18, k_2, 18]$ code and $k_2 = k_1 + 1 \geq 1$, we have $k_2 = 1$, $k_1 = 0$. But then $(\underbrace{11\ldots1}_{16}, \underbrace{00\ldots0}_{18}) = (11\ldots1) + (\underbrace{00\ldots0}_{16}, \underbrace{11\ldots1}_{18}) \in \pi(F_{\tau_p}(C))$, which contradicts $k_1 = 0$. Hence $c_5 \geq 18$, and the following possibilities occur: $(c_5, f_5) = (18, 8)$ if $n = 98$, and $(c_5, f_5) = (18, 10)$ or $(20, 0)$ if $n = 100$. For c_3 and f_3 we have: $(c_3, f_3) = (28, 14)$, $(30, 8)$ or $(32, 2)$ if $n = 98$, and $(c_3, f_3) = (28, 16)$, $(30, 10)$ or $(32, 4)$ if $n = 100$. This gives us that

- If $n = 98$ then $(c, t_5, t_3, f) = (6, 0, 0, 8)$ or $(6, 0, 2, 2)$.
- If $n = 100$ then (c, t_5, t_3, f)=$(5, 3, 3, 1)$, $(6, 0, 0, 10)$, $(6, 0, 2, 4)$ or $(6, 2, 0, 0)$.

First consider the case $(c, t_5, t_3) = (6, 0, 0)$. Now $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual code of length $c + f$. Let G_π be a generator matrix of this code in the form (2). According to Theorem 3, $k_2 = k_1 + (f - c)/2 \geq k_1 + 1 \geq 1$. Hence D

generates a self-orthogonal $[f \leq 10, k_2 \geq 1, \geq 18]$ code, which is not possible. It turns out that $(c, t_5, t_3, f) \neq (6,0,0,8)$ and $(c, t_5, t_3, f) \neq (6,0,0,10)$.

Let $E_\sigma(C)^*$ be the shortened code of $E_\sigma(C)$ obtained by removing the last $5t_5 + 3t_3 + f$ coordinates from the codewords having 0's there, and let $C_\phi = \phi(E_\sigma(C)^*)$. Since

$$x^{15} - 1 = (x-1)\underbrace{(1+x+x^2)}_{Q_3(x)}\underbrace{(1+x+x^2+x^3+x^4)}_{Q_5(x)}\underbrace{(1+x+x^4)}_{h(x)}\underbrace{(1+x^3+x^4)}_{h^*(x)},$$

then

$$C_\phi = M_1 \oplus M_2 \oplus M' \oplus M'',$$

where M_1 and M_2 are Hermitian self-orthogonal codes over the fields $G_1 \cong \mathbb{F}_4$ and $G_2 \cong \mathbb{F}_{16}$, respectively, M' is a linear $[6, k', d']$ code over $H \cong \mathbb{F}_{16}$ and $M'' \subseteq (M')^\perp$ with respect to the Euclidean inner product. The fields G_1, G_2 and H are generated by the polynomials $(x^{15}-1)/Q_3(x)$, $(x^{15}-1)/Q_5(x)$, $(x^{15}-1)/h(x)$, respectively (more detailed description is given in [2]). Moreover,

$$e_1 = x + x^2 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14},$$
$$e_2 = x + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{12} + x^{13} + x^{14},$$
$$\text{and } e = e(x) = x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12},$$

are the identities of the fields G_1, G_2 and H, respectively.

For the dimensions we have

$$\dim E_\sigma(C)^* = 2\underbrace{\dim M_1}_{\leq c/2} + 4\underbrace{\dim M_2}_{\leq c/2} + 4(\underbrace{\dim M' + \dim M''}_{\leq c}) \leq 7c.$$

Consider now the case $(c, t_5, t_3, f) = (5,3,3,1)$. Taking a generator matrix of C_π in the form (2) we obtain that $k_2 = k_1 + 1 \geq 1$. But $\pi^{-1}(\mathcal{D})$ must be a code of length 25, dimension k_2 and minimum weight at least 18, which gives $k_2 \leq 1$ and therefore $k_2 = 1$, $k_1 = 0$. Hence

$$\dim E_\sigma(C)^* = 26 = 2\underbrace{\dim M_1}_{\leq 2} + 4\underbrace{\dim M_2}_{\leq 2} + 4(\underbrace{\dim M' + \dim M''}_{\leq 5}).$$

Then $\dim M_1 = 1$ and so $M_1 = \langle v \rangle$, $v \in G_1^5$, $v \neq 0$. Since M_1 is a self-orthogonal quaternary code of length 5, $\mathrm{wt}(v) = 2$ or 4. Then the code $\phi(E_\sigma(C))$ contains a subcode generated by the matrix

$$\begin{pmatrix} v & 000 & 000 & 0 \\ B & 000 & I_3 & 0 \end{pmatrix},$$

where $\binom{v}{B}$ generates $M_1^\perp$, and I_3 is the identity matrix over the field $P_3 = \{0, x+x^2, 1+x, 1+x^2\}$. But if the dual distance of M_1 is 1 then the code C will contain a subcode with effective length at most 15+9=24 and dimension 2. Such a subcode can have minimum weight at most 16 [3], which contradicts the minimum weight of C. Hence this case is not possible, either.

3 The case $c = 6$, $t_5 = 0$, $t_3 = 2$

Now $5t_5 + 3t_3 + f = n - 90 < 18$, therefore

$$\dim E_\sigma(C)^* = \frac{90-6-f}{2} - \dim \mathcal{B}_\pi = 42 - \frac{f}{2} - \frac{2-f}{2} = 40$$

$$\Rightarrow 2\underbrace{\dim M_1}_{\leq 3} + 4\underbrace{\dim M_2}_{\leq 3} + 4(\underbrace{\dim M' + \dim M''}_{\leq 6}) = 40,$$

hence $\dim M_1 = 2$, $\dim M_2 = 3$, $\dim M' + \dim M'' = 6$. It follows that M_1 is a Hermitian self-orthogonal $[6, 2, \geq 2]$ code over the field $G_1 \cong \mathbb{F}_4$, M_2 is a Hermitian self-dual $[6, 3, d_2]$ code over $G_2 \cong \mathbb{F}_{16}$, M' is a linear $[6, k', d']$ code over $H \cong \mathbb{F}_{16}$ and $M'' = (M')^\perp$ is its dual with respect to the Euclidean inner product. Moreover, the code $\phi(E_\sigma(C))$ has a generator matrix the form

$$G_\phi = \begin{pmatrix} genM' & 0 \\ genM'' & 0 \\ genM_2 & 0 \\ genM_1 & 0 \\ D & I_2 \end{pmatrix}, \tag{3}$$

where the matrix $\binom{genM_1}{D}$ generates the dual code of M_1 over G_1, and I_2 is the identity matrix over the quaternary field P_3.

We begin with the construction of M' and M''. There are 33 codes M' of length 6, dimensions 2 and 3, and minimum weight $d' \geq 3$ such that $d(\phi^{-1}(M' \oplus M'') \geq 20$. Generator matrices of these codes are presented in [2].

After fixing the $M' \oplus M''$ part of the generator matrix, we consider all possible generator matrices for the M_2 part. Note that even if the matrices generate equivalent codes M_2 the codes generated by $M' \oplus M'' \oplus M_2$ may not be equivalent. After computing all possible generator matrices we obtain exactly 675 inequivalent $[90, 36, 20]$ binary codes. These codes have automorphism groups of orders 15 (557 codes), 30 (111 codes), 45 (2 codes) and 90 (5 codes) [2].

Next we add the M_1 part, that is a Hermitian self-orthogonal $[6, 2, \geq 2]$ code over the field G_1. One can easily compute all such codes up to equivalence (four codes). We fix the generator matrices of the 675 codes and consider all possibilities for M_1 under compositions of the following transformations: 1) a permutation $\tau \in S_6$ of the coordinates; 2) multiplication of each of the six columns by a nonzero element of G_1; 3) automorphism of the field. Thus we construct binary $[96, 44]$ codes $E_\sigma(C)$ (96 is the effective length). These codes are doubly-even (see [1, Theorem 1.4.8]). Our computations show that none of these codes has minimum distance $d \geq 20$ thus $d \leq 16$. This proves

Theorem 5. *A binary self-dual* $[98, 49, 18]$ *code does not have automorphisms of order 15. A binary self-dual* $[100, 50, 18]$ *code does not have an automorphism of type* $15 - (6, 0, 2, 4)$.

As a corollary we obtain that if a binary self-dual $[100, 50, 18]$ code has an automorphism σ of order 15, then σ is of type 15-$(6, 2, 0, 0)$. This case seems to be more complicated, with a few subcases depending on the dimensions of the quaternary codes involved in the construction.

Nevertheless the negative result in Theorem 5, we constructed self-dual [98,49,16] codes having an automorphism σ of type $15-(6, 0, 2, 2)$. The weight distribution of a binary self-dual $[98, 49, 16]$ code is known from [4] and it depends on five parameters $\alpha, \beta, \gamma, \delta$ and ϵ. Only one $[98, 49, 16]$ code with $(\alpha, \beta, \gamma, \delta, \epsilon) = (0, 0, 0, -96, 18063)$ is known (see [4]). We calculated only a small portion (less than a percent) of all codes with $d = 16$. We have over 14000 new $[98, 49, 16]$ codes. In their weight enumerators $\gamma = 0$, $\delta = -(15i+6)$ and $-(15i + 11)$, $i = 0, 1, \dots, 8$, $\epsilon = 16308 + 5j$, where $j = 0$, 7, 13, 15, 19, 20, 22, 23 and many more.

References

[1] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge 2003.

[2] S. Bouyuklieva, W. Willems, N. Yankov, On the Automorphisms of Order 15 for a Binary Self-Dual $[96, 48, 20]$ Code, arXiv:1403.4735 [cs.IT].

[3] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, `http://www.codetables.de`.

[4] M. Harada, M. Kiermaier, A. Wassermann, and R. Yorgova, New Binary Singly Even Self-Dual Codes, *IEEE Trans. Inform. Theory,* **56**, 1612–1617, 2010.

[5] W. C. Huffman, Automorphisms of codes with application to extremal doubly-even codes of lenght 48, *IEEE Trans. Inform. Theory,* **28**, 511–521, 1982.

[6] W. C. Huffman, On the classification and enumeration of self-dual codes, *Finite Fields Appl.,* **11**, 451–490, 2005.

[7] V.Y.Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, *IEEE Trans. Inform. Theory,* **33**, 77–82, 1987.