On the Automorphisms of Order 15 for a Binary Self-Dual $[96, 48, 20]$ Code

Stefka Bouyuklieva
Faculty of Mathematics and Informatics,
Veliko Tarnovo University, 5000 Veliko Tarnovo, Bulgaria
stefka@uni-vt.bg

Wolfgang Willems
Otto-von-Guericke Universität, Magdeburg, Germany
willems@ovgu.de

Nikolay Yankov
Faculty of Mathematics and Informatics,
Shumen University, Bulgaria
jankov_niki@yahoo.com

Abstract

The structure of binary self-dual codes invariant under the action of a cyclic group of order pq for odd primes $p \neq q$ is considered. As an application we prove the nonexistence of an extremal self-dual $[96, 48, 20]$ code with an automorphism of order 15 which closes a gap in [2].

Index Terms: *Self-dual codes, doubly-even codes, automorphisms*

1 Introduction

Let $C = C^{\perp}$ be a binary self-dual code of length n and minimum distance d. A binary code is doubly-even if the weight of every codeword is divisible by four. Self-dual doubly-even codes exist only if n is a multiple of eight. Rains [9] proved that the minimum distance d of a binary self-dual $[n, k, d]$ code satisfies the following bound:

$$d \leq 4\lfloor n/24 \rfloor + 4, \quad \text{if } n \not\equiv 22 \pmod{24},$$

$$d \leq 4\lfloor n/24 \rfloor + 6, \quad \text{if } n \equiv 22 \pmod{24}.$$

Codes achieving this bound are called extremal. If n is a multiple of 24, then a self-dual code meeting the bound must be doubly-even [9]. Moreover, for any nonzero weight w in such a code, the codewords of weight w form a 5-design [1]. This is one reason why extremal codes of length $24m$ are of particular interest. Unfortunately, only for $m = 1$

and $m = 2$ such codes are known, namely the $[24, 12, 8]$ extended Golay code and the $[48, 24, 12]$ extended quadratic residue code (see [10]). To date the existence of no other extremal code of length $24m$ is known. For $n = 96$, only the primes $2, 3$ and 5 may divide the order of the automorphism group of the extremal code and the cycle structure of prime order automorphisms are as follows

p	number of p-cycles	number of fixed points
2	48	0
3	$30, 32$	$6, 0$
5	18	6

(1)

(see Theorem, part a) in [2]). We would like to mention here that in part b) of the Theorem (the case where elements of order 3 are acting fixed point freely) four orders of possible automorphism groups are missing, namely $15, 30, 240$ and 480. The gap is due to the fact that the existence of elements of order 15 with six cycles of length 15 and two cycles of length 3 are not excluded in the given proof. We close this gap by proving

Theorem 1 *A binary doubly-even* $[96, 48, 20]$ *self-dual code with an automorphism of order 15 does not exist.*

This note consists of three sections. Section 2 is devoted to some theoretical results on binary self-dual codes invariant under the action of a cyclic group. In Section 3 we study the structure of a putative extremal self-dual $[96, 48, 20]$ code having an automorphism of order 15. Using this structure and combining the possible subcodes we prove Theorem 1. In an additional section, namely Section 4, we prove that an extremal self-dual code of length 96 does not have automorphisms of type 3-(28,12). This assertion is used by other authors but no proof has been published so far.

2 Theoretical results

Let C be a binary linear code of length n and let σ be an automorphism of C of order r where r is odd (not necessarily a prime). Let

$$\sigma = \Omega_1 \Omega_2 \dots \Omega_m \tag{2}$$

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 $\mathrm{lcm}(l_1, \dots, l_m) = r$ and l_i divides r. Therefore l_i is odd for $i = 1, \dots, m$ and $1 \le l_i \le r$.

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

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

where $v|\Omega_i$ is the restriction of v on Ω_i. With this notation we have the following.

Theorem 2 *The code C is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$.*

Proof: We follow the proof of Lemma 2 in [4]. Obviously, $F_\sigma(C)\cap E_\sigma(C)=\{0\}$. Let $v\in C$ and $w=v+\sigma(v)+\cdots+\sigma^{r-1}(v)$. Since $w\in C$ and $\sigma(w)=w$ we get $w\in F_\sigma(C)$.

On the other hand, $\mathrm{wt}(\sigma^j(v)|_{\Omega_i})=\mathrm{wt}(v|_{\Omega_i})$ for all $i=1,2,\ldots,m$ and $j\geq 1$. Hence $\sigma(v)+\cdots+\sigma^{r-1}(v)|_{\Omega_i}$ is a sum of an even number of vectors of the same weight. Thus $\mathrm{wt}(\sigma(v)+\cdots+\sigma^{r-1}(v)|_{\Omega_i})$ is even for $i=1,2,\ldots,m$. It follows that $u=\sigma(v)+\cdots+\sigma^{r-1}(v)\in E_\sigma(C)$. So $v=w+u\in F_\sigma(C)+E_\sigma(C)$ which proves that $C=F_\sigma(C)\oplus E_\sigma(C)$. □

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the binary field $\mathbb{F}_2$, and $\pi: F_\sigma(\mathbb{F}_2^n)\to\mathbb{F}_2^m$ be the projection map, i.e., $(\pi(v))_i=v_j$ for some $j\in\Omega_i$ and $i=1,2,\ldots,m$. Clearly, $v\in F_\sigma(C)$ iff $v\in C$ and v is constant on each cycle.

Theorem 3 *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.*

Proof: Let $v,w\in F_\sigma(C)$. If $\langle\cdot,\cdot\rangle$ denotes the Euclidean inner product on $\mathbb{F}_2^n$ then $\langle v,w\rangle=\langle\pi(v),\pi(w)\rangle=0$ since l_i is odd for all i. Hence C_π is a self-orthogonal code. If $u\in C_\pi^\perp$ and $u'=\pi^{-1}(u)$ then $\langle u',v\rangle=\langle u,\pi(v)\rangle=0$ for all $v\in F_\sigma(C)$. Furthermore, $\langle u',v\rangle=\sum_{i=1}^m\langle u'|_{\Omega_i},v|_{\Omega_i}\rangle=0$ for all $v\in E_\sigma(C)$ since u' is constant on Ω_i and $\mathrm{wt}(v|_{\Omega_i})$ is even. Thus $u'\in C^\perp=C$. Hence $u'\in F_\sigma(C)$ and therefore $u=\pi(u')\in C_\pi$ which proves that C_π is a self-dual code. □

Corollary 4 *Let C be a binary self-dual code of length $n=cr+f$ and let σ be an automorphism of C of odd order r such that*

$$\sigma=\Omega_1\ldots\Omega_c\Omega_{c+1}\ldots\Omega_{c+f} \tag{3}$$

where $\Omega_i=((i-1)r+1,\ldots,ir)$ are cycles of length r for $i=1,\ldots,c$, and $\Omega_{c+i}=(cr+i)$ are the fixed points for $i=1,\ldots,f$. Then $F_\sigma(C)$ and $E_\sigma(C)$ have dimension $(c+f)/2$ and $c(r-1)/2$, respectively.

Proof: Clearly, $m=c+f$ is the number of orbits of σ. Therefore $\dim F_\sigma(C)=\dim C_\pi=(c+f)/2$. Hence $\dim E_\sigma(C)=n/2-(c+f)/2=(cr+f)/2-(c+f)/2=c(r-1)/2$. □

If σ is of prime order p with c cycles of length p and f fixed points we say that σ is of type p-(c,f).

2.1 Connections with quasi-cyclic codes

For further investigations, we need two theorems concerning the theory of finite fields and cyclic codes. Let r be a positive integer coprime to the characteristic of the field $\mathbb{F}_l$ of cardinality l, where l is the power of a prime. Consider the factor ring $\mathcal{R}=\mathbb{F}_l[x]/(x^r-1)$, where (x^r-1) is the principal ideal in $\mathbb{F}_l[x]$ generated by x^r-1. Let

$$x^r-1=f_0(x)f_1(x)\ldots f_s(x)$$

be the factorization of x^r-1 into irreducible factors $f_i(x)$ over $\mathbb{F}_l$ where $f_0(x)=x-1$. Let $I_j=\langle\frac{x^r-1}{f_j(x)}\rangle$ be the ideal of $\mathcal{R}$ generated by $\frac{x^r-1}{f_j(x)}$ for $j=0,1,\dots,s$. Finally, by $e_j(x)$ we denote the generator idempotent of I_j; i.e., $e_j(x)$ is the identity of the two-sided ideal I_j. With these notations we have the following well-known result.

Theorem 5 (see [5])
(i) $\mathcal{R}=I_0\oplus I_1\oplus\cdots\oplus I_s$.
(ii) I_j *is a field which is isomorphic to the field* $\mathbb{F}_{l^{deg(f_j(x))}}$ *for* $j=0,1,\dots,s$.
(iii) $e_i(x)e_j(x)=0$ *for* $i\neq j$.
(iv) $\sum_{j=0}^{s}e_j(x)=1$.

According to [7] there is a decomposition

$$x^r-1=g_0(x)g_1(x)\cdots g_m(x)h_1(x)h_1^*(x)\cdots h_t(x)h_t^*(x),$$

where $s=m+2t$ and $\{g_0,g_1,\dots g_m,h_1,h_1^*,\dots,h_t,h_t^*\}=\{f_0,f_1,\dots,f_s\}$. Furthermore, $h_i^*(x)$ is the reciprocal polynomial of $h_i(x)$, $h_i^*\neq h_i$ for $i=1,\dots,t$ and $g_i(x)$ coincides with its reciprocal polynomial where $g_0(x)=f_0(x)=x-1$. Finally, we denote the field $\langle\frac{x^r-1}{g_j(x)}\rangle$ by G_j for $j=0,1,\dots,m$, $\langle\frac{x^r-1}{h_j(x)}\rangle$ by H_j for $j=1,\dots,t$, and $\langle\frac{x^r-1}{h_j^*(x)}\rangle$ by H_j^* for $j=1,\dots,t$.

To continue the investigations, we need to prove some properties of binary linear codes of length cr with an automorphism τ of order r which has c independent r-cycles. If C is such a code then C is a quasi-cyclic code of length cr and index c. Next we define a map $\phi:\mathbb{F}_2^{cr}\to\mathcal{R}^c$ by

$$\phi(v)=(v_0(x),v_1(x),\dots,v_{c-1}(x))\in\mathcal{R}^c,$$

where $v_i(x)=\sum_{j=0}^{r-1}v_{ij}x^j$ and $(v_{i0},\dots,v_{i,c-1})=v|_{\Omega_i}$. Clearly, $\phi(C)$ is a linear code over the ring $\mathcal{R}$ of length c. Moreover, according to [7], we have $\phi(C)^\perp=\phi(C^\perp)$ where the dual code $C^\perp$ over $\mathbb{F}_2$ is taken under the Euclidean inner product, and the dual code $\phi(C)^\perp$ in $\mathcal{R}^c$ is taken with respect to the following Hermitian inner product:

$$\langle u,v\rangle=\sum_{i=0}^{c-1}u_i\overline{v}_i\in\mathcal{R}^c,\quad \overline{v}_i=v_i(x^{-1})=v_i(x^{r-1}).$$

In particular, the quasi-cyclic code C is self-dual if and only if $\phi(C)$ is self-dual over $\mathcal{R}$ with respect to the Hermitian inner product.

Every linear code C over the ring $\mathcal{R}$ of length c can be decomposed as a direct sum

$$C=(\bigoplus_{i=0}^{m}C_i)\oplus(\bigoplus_{j=1}^{t}(C_j'\oplus C_j'')),$$

where C_i is a linear code over the field G_i $(i=0,1,\dots,m)$, C_j' is a linear code over H_j and C_j'' is a linear code over H_j^* $(j=1,\dots,t)$.

Theorem 6 (see [7]) *A linear code C over $\mathcal{R}$ of length c is self-dual with respect to the Hermitian inner product, or equivalently a c-quasi-cyclic code of length cr over $\mathbb{F}_q$ is self-dual with respect to the Euclidean inner product, if and only if*

$$C = (\bigoplus_{i=0}^{m} C_i) \oplus (\bigoplus_{j=1}^{t} (C'_j \oplus (C'_j)^{\perp})),$$

where C_i is a self-dual code over G_i for $i = 0, 1, \ldots, m$ of length c (with respect to the Hermitian inner product) and C'_j is a linear code of length c over H_j and $(C'_j)^{\perp}$ is its dual with respect to the Euclidean inner product for $1 \leq j \leq t$,.

2.2 The case $r = pq$

We consider now the case $r = pq$ for different odd primes p and q such that 2 is a primitive root modulo p and modulo q. The ground field is $\mathbb{F}_2$. Then

$$x^r - 1 = (x-1)Q_p(x)Q_q(x)Q_r(x) = (1+x)(1+x+\cdots+x^{p-1})(1+x+\cdots+x^{q-1})Q_r(x)$$

where $Q_i(x)$ is the i-th cyclotomic polynomial. Moreover, both $Q_p(x)$ and $Q_q(x)$ are irreducible over $\mathbb{F}_2$ since 2 is primitive modulo p and modulo q as well. Finally, if

$$Q_r(x) = g_3(x) \ldots g_s(x) h_1(x) h_1^*(x) \cdots h_t(x) h_t^*(x)$$

is the factorization of the r-th cyclotomic polynomial into irreducible factors over $\mathbb{F}_2$, then these factors have the same degree, namely $\frac{\phi(r)}{s-2+2t} = \frac{(p-1)(q-1)}{s-2+2t}$, where ϕ is Euler's phi function.

Let

$$\sigma = \Omega_1 \ldots \Omega_c \Omega_{c+1} \ldots \Omega_{c+t_q} \Omega_{c+t_q+1} \ldots \Omega_{c+t_q+t_p} \Omega_{c+t_q+t_p+1} \ldots \Omega_{c+t_q+t_p+f} \quad (4)$$

where
$\Omega_i = ((i-1)r+1, \ldots, ir)$ are cycles of length pq for $i = 1, \ldots, c$,
$\Omega_{c+i} = (cr + (i-1)q + 1, \ldots, cr + iq)$ are cycles of length q for $i = 1, \ldots, t_q$,
$\Omega_{c+t_q+i} = (cr + t_q q + (i-1)p + 1, \ldots, cr + t_q q + ip)$ are cycles of length p for $i = 1, \ldots, t_p$,
and $\Omega_{c+t_q+t_p+i} = (c + t_q + t_p + i)$ are the fixed points for $i = 1, \ldots, f$.

Let $E_\sigma(C)^*$ be the shortened code of $E_\sigma(C)$ obtained by removing the last $t_q q + t_p p + f$ coordinates from the codewords having 0's there. Let $C_\phi = \phi(E_\sigma(C)^*)$. Since $E_\sigma(C)^*$ is a binary quasi-cyclic code of length cr and index c, C_ϕ is a linear code over the ring $\mathcal{R}$ of length c. Moreover

$$C_\phi = (\bigoplus_{i=0}^{m} M_i) \oplus (\bigoplus_{j=1}^{t} (M'_j \oplus M''_j)),$$

where M_i is a linear code over the field G_i, $i = 1, \dots, m$, M'_j is a linear code over H_j and M''_j is a linear code over H_j^*, $j = 1, \dots, t$. For the dimensions we have

$$\dim E_\sigma(C)^* = \dim C_\phi =$$
$$(p-1)\dim M_1 + (q-1)\dim M_2 + \tfrac{(p-1)(q-1)}{s-2+2t}\left(\textstyle\sum_{i=3}^{s} \dim M_i + \sum_{j=1}^{t}(\dim M'_j + \dim M''_j)\right).$$

Since $E_\sigma(C)^*$ is a self-orthogonal code, C_ϕ is also self-orthogonal over the ring $\mathcal{R}$ with respect to the Hermitian inner product. This means that M_i are self-orthogonal codes of length c over G_i for $i = 1, \dots, m$ (with respect to the Hermitian inner product) and, for $1 \le j \le t$, we have $M''_j \subseteq (M'_j)^\perp$ with respect to the Euclidean inner product. This forces $\dim M_i \le c/2$ for $i = 1, 2, \dots, s$ and $\dim M'_j + \dim M''_j \le c$. It follows that

$$\dim E_\sigma(C)^* \le (p-1)\frac{c}{2} + (q-1)\frac{c}{2} + \frac{(p-1)(q-1)}{s-2+2t}((s-2)\frac{c}{2} + tc) = \frac{c(pq-1)}{2}. \qquad (5)$$

3 Self-dual $[96, 48, 20]$ codes and permutations of order 15

Let C be a binary extremal self-dual $[96, 48, 20]$ code with an automorphism σ of order 15. We decompose σ in a product of c independent cycles of length 15, t_5 cycles of length 5, t_3 cycles of length 3 and f cycles of length 1. Then σ^5 and σ^3 are automorphisms of C of type 3-$(5c + t_3, 5t_5 + f)$ and 5-$(3c + t_5, 3t_3 + f)$, respectively. According to (1),

$$3c + t_5 = 18, \quad 3t_3 + f = 6, \quad 5c + t_3 = 30 \text{ or } 32, \quad 5t_5 + f = 6 \text{ or } 0.$$

This leads to

$$t_5 = 0, \quad c = 6, \quad (t_3, f) = (2, 0) \text{ or } (0, 6).$$

Lemma 7 *If $(t_3, f) = (2, 0)$ then C_π is the extended $[8, 4, 4]$ Hamming code. If $(t_3, f) = (0, 6)$ then C_π is the self-dual $[12, 6, 4]$ code.*

Proof: Let C be a binary extremal self-dual $[96, 48, 20]$ code and

$$\sigma = \Omega_1\Omega_2\Omega_3\Omega_4\Omega_5\Omega_6\Omega_7\Omega_8,$$

be its automorphism of order 15, where $\Omega_i = (15(i-1)+1, \dots, 15i)$ for $i = 1, \dots, 6$, $\Omega_7 = (91, 92, 93)$, $\Omega_8 = (94, 95, 96)$. Hence C_π is a binary self-dual code of length 8. If $x = (x_1, \dots, x_8) \in C_\pi$ then $\mathrm{wt}(\pi^{-1}(x)) = 15(x_1 + \cdots + x_6) + 3x_7 + 3x_8 \equiv 3\mathrm{wt}(x) \pmod 4$. Since C is a doubly-even code, $\mathrm{wt}(x) \equiv 0 \pmod 4$ and C_π must be a doubly-even code, too. The only doubly-even self-dual code of length 8 is the extended $[8, 4, 4]$ Hamming code. Its automorphism group acts 2-transitively on the code, so we can take any pair of coordinates for the two 3-cycles.

In the case $f = 6$ C_π is a self-dual code of length 12 and so its minimum weight is at most 4. If $x = (x_1, \dots, x_{12}) \in C_\pi$ then

$$\mathrm{wt}(\pi^{-1}(x)) = 15(\underbrace{x_1 + \cdots + x_6}_{a}) + \underbrace{x_7 + \cdots + x_{12}}_{b} = 15a + b \ge 20.$$

Hence $a \geq 1$ and if $a = 1$ then $b = 5$. It follows that C_π is a self-dual $[12, 6, 4]$ code with a generator matrix in the form $(I_6\ D)$. The only such code is d_{12}^+ (see [10]). For the structure of d_{12}^+ we use the terms from [4]. This code have a defining set which means that its coordinates can be partitioned into duo's $\{l_1, l_2\}$, $\{l_3, l_4\}$, $\{l_5, l_6\}$, $\{l_7, l_8\}$, $\{l_9, l_{10}\}$, $\{l_{11}, l_{12}\}$, such that its 15 codewords of weight 4 are the vectors with supports $\{l_{2i-1}, l_{2i}, l_{2j-1}, l_{2j}\}$ where $1 \leq i < j \leq 6$ (clusters). Since C_π does not contain a codeword x of weight 4 with $(a, b) = (1, 3)$ or $(0, 4)$ it turns out that $\{l_1, l_3, l_5, l_7, l_9, l_{11}\} = \{1, 2, 3, 4, 5, 6\}$ and $\{l_2, l_4, l_6, l_8, l_{10}, l_{12}\} = \{7, 8, 9, 10, 11, 12\}$. As a basis for the code we can take the clusters $\{l_i, l_{i+1}, l_{i+6}, l_{i+7}\}$ for $i = 1, 2, \ldots, 5$, with the d-set $\{1, 7, 8, 9, 10, 11, 12\}$. Hence C_π has a generator matrix of shape $(I_6|I_6 + J_6)$ where I_6 is the identity matrix and J_6 is the all-ones matrix of size 6. $\square$

We consider both possibilities for the structure of σ simultaneously. Since

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

we obtain

$$\dim E_\sigma(C)^* = 2\underbrace{\dim M_1}_{\leq 3} + 4\underbrace{\dim M_2}_{\leq 3} + 4(\underbrace{\dim M' + \dim M''}_{\leq 6}).$$

According to the balance principle (see [2], [5] or [10]), the dimension of the subcode of C consisting of the codewords with 0's in the last six coordinates, is equal to $42 = 48 - 6$. Hence if $f = 6$ then $\dim E_\sigma(C)^* = 42$. In the other case, the dimension of the subcode of $C_\pi \cong e_8$, consisting of the codewords with 0's in the last two coordinates, is 2 and therefore $\dim E_\sigma(C)^* = 40$. It follows that

$$\dim M_1 = 2 \text{ or } 3, \quad \dim M_2 = 3 \text{ and } \dim M' + \dim M'' = 6.$$

This means that

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

where M_1 is a Hermitian self-orthogonal $[6, 2, \geq 2]$ code in the case $f = 0$ and a self-dual $[6, 3, \geq 2]$ code in the case $f = 6$ 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. If v is a codeword of weight t in M_2, M' or M'' then the vectors $\phi^{-1}(v)$, $\phi^{-1}(xv)$, $\phi^{-1}(x^2v)$ and $\phi^{-1}(x^3v)$ generate a binary code of dimension 4 and effective length $15t$. It is a subcode of C and therefore its minimum distance should be at least 20. Since binary codes of length 30, dimension 4 and minimum distance ≥ 20 do not exist [3], $d_2 = 3$ or 4, $d' \geq 3$ and the minimum distance of M'' is at least 3. In the following we list the three possible cases for M' and M'' where

$$e = e(x) = x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x$$

is the identity of the field $H = \{0, e, xe, x^2e, \ldots, x^{14}e\}$.

1. M' is an MDS $[6,2,5]$ code and M'' is its dual MDS $[6,4,3]$ code. It is well known that any MDS $[n,k,n-k+1]$ code over $\mathbb{F}_q$ is an n-arc in the projective geometry $PG(k-1,q)$. There are exactly four inequivalent $[6,2,5]$ MDS codes over $\mathbb{F}_{16}$ [6] (their dual codes correspond to the 6-arcs in $PG(3,16)$). We list here generator matrices of these codes:

$$\begin{pmatrix} e & 0 & e & e & e & e \\ 0 & e & e & xe & x^2e & x^3e \end{pmatrix} \quad \begin{pmatrix} e & 0 & e & e & e & e \\ 0 & e & e & xe & x^2e & x^4e \end{pmatrix}$$

$$\begin{pmatrix} e & 0 & e & e & e & e \\ 0 & e & e & xe & x^3e & x^7e \end{pmatrix} \quad \begin{pmatrix} e & 0 & e & e & e & e \\ 0 & e & e & xe & x^3e & x^{11}e \end{pmatrix}$$

2. M' and M'' are both MDS $[6,3,4]$ codes. According to [6], there are 22 MDS codes with the needed parameters over $\mathbb{F}_{16}$ (they correspond to the 6-arcs in $PG(2,16)$). We consider generator matrices of these codes in the form

$$\begin{pmatrix} e & 0 & 0 & e & e & e \\ 0 & e & 0 & e & x^{a_1}e & x^{a_2}e \\ 0 & 0 & e & e & x^{a_3}e & x^{a_4}e \end{pmatrix}, \quad a_i \in \{1,2,\ldots,14\},\ i=1,2,3,4.$$

Note that $a_i \geq 1$ for $i=1,2,3,4$ since the minimum distance of M' is 4. We calculated the weight distributions and the automorphism groups of $\phi^{-1}(M' \oplus M'')$ for all 22 codes M'. The results are listed in Table 1. Five of the binary codes have minimum distance 24, and six of them have minimum distance 20.

Table 1: The $[90,24]$ codes in case 2

(a_1,a_2,a_3,a_4)	A_{16}	A_{20}	A_{24}	A_{28}	A_{32}	A_{36}	$\lvert\mathrm{Aut}\rvert$
$(1,2,2,1)$	270	0	5400	15840	195345	941400	1440
$(1,2,2,4)$	60	120	2730	18480	189885	950280	240
$(1,2,2,5)$	15	30	2070	17535	187815	963480	30
$(1,2,2,6)$	45	180	1935	17505	183015	975420	90
$(1,2,2,8)$	45	0	2580	15660	188715	965040	240
$(1,2,2,9)$	15	30	2130	17355	187575	965160	30
$(1,2,3,1)$	30	120	2430	19650	192105	937200	120
$(1,2,3,6)$	-	-	2325	16320	192585	953040	60
$(1,2,3,7)$	-	60	1875	17955	189465	956220	30
$(1,2,3,8)$	-	-	2145	17340	190185	956400	30
$(1,2,3,12)$	-	60	1965	18060	187545	960120	60
$(1,2,4,6)$	-	60	2040	17910	187485	959400	60
$(1,2,5,7)$	-	90	1830	18390	186405	963900	30
$(1,2,6,1)$	60	0	3090	17400	194205	941400	240
$(1,2,9,1)$	30	120	2910	17250	196425	933840	120
$(1,2,12,1)$	90	360	3240	23940	192825	909720	720
$(1,3,2,6)$	-	-	2325	16320	192585	953040	60
$(1,3,3,2)$	-	180	1665	18720	185625	960840	90
$(1,3,7,2)$	-	-	2295	16830	191745	950040	180
$(1,3,7,10)$	-	180	1755	18450	185265	963360	360
$(1,3,11,8)$	-	-	2730	14100	197925	944760	600
$(5,10,10,5)$	450	0	14580	16200	329625	507960	259200

3. M' and M'' are both $[6,3,3]$ codes. We consider generator matrices of M' in the form

$$\begin{pmatrix} e & 0 & 0 & 0 & e & e \\ 0 & e & 0 & e & \beta_1 & \beta_2 \\ 0 & 0 & e & e & \beta_3 & \beta_4 \end{pmatrix}, \quad \beta_i \in H,\ i = 1,2,3,4,$$

where $\beta_i = x^{b_i}e$, $b_i \in \{0,1,\ldots,14\}$, or $\beta_i = 0$, $i = 1,2,3,4$.

We calculated that there are 18 inequivalent $[6,3,3]$ codes M' over $\mathbb{F}_{16}$ such that $d(\phi^{-1}(M' \oplus M'')) \geq 20$. The weight distributions and the automorphism groups of $\phi^{-1}(M' \oplus M'')$ for all 18 codes are listed in Table 2. Ten of the binary codes have minimum distance 24, and eight of them have minimum distance 20.

Table 2: The $[90,24]$ codes in case 3

(b_1,b_2,b_3,b_4)	A_{20}	A_{24}	A_{28}	A_{32}	A_{36}	$\lvert\mathrm{Aut}\rvert$
$(0,0,0,7)$	-	2250	17640	187605	960120	180
$(0,0,2,3)$	-	2070	18060	187125	963960	60
$(0,0,2,6)$	-	1950	18420	187605	960600	30
$(0,2,2,9)$	-	2175	17670	188625	957480	60
$(0,2,3,4)$	-	2070	17730	189285	958080	15
$(0,2,3,7)$	-	2025	17865	189465	956820	15
$(0,2,3,11)$	-	2070	18030	187485	962280	30
$(0,2,3,12)$	-	2010	18210	187725	960600	15
$(0,2,4,7)$	-	2190	16890	191925	953040	30
$(0,2,4,13)$	-	2100	17640	189165	958920	60
$(0,0,0,2)$	90	1755	18900	184545	968940	90
$(0,0,2,5)$	30	1905	18630	186585	961260	30
$(0,0,2,9)$	30	2025	18270	186105	964620	30
$(0,0,3,5)$	30	1935	18540	186465	962100	30
$(0,2,2,3)$	60	2055	18030	186225	963600	30
$(0,2,2,5)$	60	1935	18015	188265	958860	30
$(0,2,2,8)$	180	1800	18630	184365	962760	180
$(0,2,4,0)$	90	1830	18630	185445	964860	30

In the following G_1 is the field with four elements and identity

$$e_1 = x + x^2 + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{14},$$

and G_2 the field with 16 elements and identity

$$e_2 = x + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{12} + x^{13} + x^{14},$$

defined in the beginning of this section. Furthermore $\mu_2 = x^{11} + x^{10} + x^6 + x^5 + x + 1$ is a generator of G_2.

According to [12], there are two Hermitian self-dual $[6,3,d \geq 3]$ codes over $\mathbb{F}_{16}$ up to the equivalence defined in the following way: Two codes are equivalent if the second one is obtained from the first one via a sequence of the following transformations:

- a substitution $x \to x^t$, $t = 2,4,8$;

- a multiplication of any coordinate by x;
- a permutation of the coordinates.

Their generator matrices are

$$H_1 = \begin{pmatrix} e_2 & 0 & 0 & 0 & \mu_2^5 & \mu_2^{10} \\ 0 & e_2 & 0 & \mu_2^5 & \mu_2^5 & e \\ 0 & 0 & e_2 & \mu_2^{10} & e_2 & \mu_2^{10} \end{pmatrix}, \qquad H_2 = \begin{pmatrix} e_2 & 0 & 0 & e_2 & \mu_2^5 & \mu_2^5 \\ 0 & e_2 & 0 & e_2 & \mu_2^2 & \mu_2^8 \\ 0 & 0 & e_2 & e_2 & \mu_2^6 & \mu_2^9 \end{pmatrix}.$$

We fix the $M' \oplus M''$ part of the generator matrix and 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. We consider the two possible matrices for the M_2 part under the products of the following maps: 1) a permutation $\tau \in S_6$ of the 15-cycle coordinates; 2) multiplication of each of the 6 columns by nonzero element of F_{16}; 3) automorphism of the field ($x \to x^t$, $t = 2, 4, 8$). After computing all possible generator matrices we obtain exactly 675 inequivalent $[90, 36, 20]$ binary codes: 232 from the first matrix H_1, and 443 from the second H_2. These codes have automorphism groups of orders 15 (557 codes), 30 (111 codes), 45 (2 codes) and 90 (5 codes).

Next, we separate both cases.

f=0) Let first add the fixed subcode. According to Lemma 7, the code $\pi(F_\sigma(C))$ is equivalent to the extended Hamming $[8, 4, 4]$ code H_8. As we already mentioned in the proof of Lemma 7, we can take any pair of coordinates for the 3-cycles. Then we consider all $6! = 720$ permutation of the 15-cycles that can lead to different subcodes. Only 47 of the constructed codes $\phi^{-1}(M' \oplus M'' \oplus M_2) \oplus F_\sigma(C)$ have minimum distance $d' = 20$ (we list the number of their codewords of weights 20 and 24 and the order of the automorphism groups in Table 3).

Table 3: The $[96, 40, 20]$ codes

	A_{20}	A_{24}	$\|Aut\|$		A_{20}	A_{24}	$\|Aut\|$		A_{20}	A_{24}	$\|Aut\|$
$C_{96,40,1}$	48735	4206590	1620	$C_{96,40,17}$	47925	4216010	540	$C_{96,40,33}$	48045	4213610	540
$C_{96,40,2}$	49545	4197410	1620	$C_{96,40,18}$	48105	4213730	540	$C_{96,40,34}$	48420	4209320	540
$C_{96,40,3}$	47835	4217030	1620	$C_{96,40,19}$	48600	4207760	540	$C_{96,40,35}$	47760	4216160	540
$C_{96,40,4}$	47940	4214600	540	$C_{96,40,20}$	48420	4208120	540	$C_{96,40,36}$	48780	4204760	540
$C_{96,40,5}$	48405	4209530	540	$C_{96,40,21}$	47325	4220810	540	$C_{96,40,37}$	48510	4209500	540
$C_{96,40,6}$	47805	4214810	540	$C_{96,40,22}$	47595	4216070	540	$C_{96,40,38}$	47460	4217720	540
$C_{96,40,7}$	47205	4222490	540	$C_{96,40,23}$	48345	4209650	540	$C_{96,40,39}$	48330	4210100	1080
$C_{96,40,8}$	48690	4204820	540	$C_{96,40,24}$	47925	4213370	540	$C_{96,40,40}$	47415	4221950	1080
$C_{96,40,9}$	47265	4220450	540	$C_{96,40,25}$	47835	4215110	540	$C_{96,40,41}$	48315	4210550	540
$C_{96,40,10}$	47580	4216520	540	$C_{96,40,26}$	47790	4214780	540	$C_{96,40,42}$	47490	4218740	540
$C_{96,40,11}$	47565	4219370	1080	$C_{96,40,27}$	49410	4200020	540	$C_{96,40,43}$	49140	4201880	540
$C_{96,40,12}$	48255	4212110	540	$C_{96,40,28}$	48225	4210610	540	$C_{96,40,44}$	48330	4212500	1080
$C_{96,40,13}$	48555	4207190	540	$C_{96,40,29}$	48360	4209920	540	$C_{96,40,45}$	48870	4212860	1080
$C_{96,40,14}$	48165	4211690	1080	$C_{96,40,30}$	48600	4214000	1080	$C_{96,40,46}$	47970	4213220	540
$C_{96,40,15}$	48555	4206710	1080	$C_{96,40,31}$	47775	4215230	540	$C_{96,40,47}$	47925	4215050	1080
$C_{96,40,16}$	48630	4205900	540	$C_{96,40,32}$	49815	4194350	1620				

Next we add the M_1 part, that is a Hermitian self-orthogonal $[6, 2, \geq 2]$ code over the field $G_1 \cong \mathbb{F}_4$. One can easily compute all such codes up to equivalence. There are exactly 4 inequivalent such codes with generator matrices

$$H_3 = \begin{pmatrix} e_1 & 0 & e_1 & 0 & 0 & 0 \\ 0 & e_1 & 0 & e_1 & 0 & 0 \end{pmatrix}, \quad H_4 = \begin{pmatrix} e_1 & 0 & e_1 & e_1 & e_1 & 0 \\ 0 & e_1 & e_1 & xe_1 & x^2e_1 & 0 \end{pmatrix},$$

$$H_5 = \begin{pmatrix} e_1 & 0 & e_1 & 0 & 0 & 0 \\ 0 & e_1 & 0 & e_1 & e_1 & e_1 \end{pmatrix}, \quad H_6 = \begin{pmatrix} e_1 & 0 & 0 & e_1 & e_1 & e_1 \\ 0 & e_1 & e_1 & 0 & e_1 & e_1 \end{pmatrix}.$$

We fix the generator matrices of the 47 codes and consider the matrices H_3, H_4, H_5, H_6 under compositions of the following transformations: 1) a permutation $\tau \in S_6$ of the 15-cycle coordinates; 2) multiplication of each of the 6 columns by a nonzero element of G_1; 3) automorphism of the field ($x \to x^2$). Thus we construct binary $[96, 44]$ codes. Our computations show that none of these codes has minimum distance $d \geq 20$.

f=6) Now we add the M_1 part, which is a Hermitian quaternary self-dual code of length 6 over the field $G_1 \cong \mathbb{F}_4$. There are two inequivalent codes of this length - i_2^3 with minimum weight 2 and h_6 with minimum weight 4 (see [10]). All 675 inequivalent $[90, 36, 20]$ codes combined with the binary images of the different copies to both quaternary self-dual codes give binary self-orthogonal $[90, 42, \leq 16]$ codes.

This proves Theorem 1 which states that a binary doubly-even $[96, 48, 20]$ self-dual code with an automorphism of order 15 does not exist.

4 On the automorphism of type 3-$(28, 12)$

In this section we fill a gap in the literature caused by a missing proof on the nonexistence of an extremal self-dual code of length 96 having an automorphism of type 3-$(28, 12)$. In paper [2], the authors used this assertion in their proof of the main theorem.

Proposition 8 *A binary doubly-even* $[96, 48, 20]$ *self-dual code with an automorphism of type* 3-$(28, 12)$ *does not exist.*

Proof: Suppose that C is a self-dual $[96, 48, 20]$ code and σ is an automorphism of C of type 3-(28,12). Then C_π is a self-dual $[40, 20, 8]$ code. Without loss of generality, we can take the last 12 coordinates for the fixed points. So C_π has a generator matrix of the form

$$G_\pi = \begin{pmatrix} A & O \\ D & I_{12} \end{pmatrix}, \tag{6}$$

where A is an 8×28 matrix which generates a doubly-even $[28, 8, \geq 8]$ code $\mathcal{A}$ with dual distance $d_{\mathcal{A}}^{\perp} \geq 3$. Using the MacWilliams equalities we see that the possible weight distribution for this code is

$$W_{\mathcal{A}}(y) = 1 + \lambda y^8 + (142 - 3\lambda - \mu)y^{12} + (95 + 3\lambda + 3\mu)y^{16} + (18 - \lambda - 3\mu)y^{20} + \mu y^{24},$$

and the number of codewords of weight 3 in its dual code is $\nu = 2\lambda - 2\mu - 4$.

Let us consider the partitioned weight enumerator A_{ij} for the code C_π, where $0 \leq i \leq 28$ and $0 \leq j \leq 12$. We use the following restrictions:

- If $3i + j \not\equiv 0 \pmod 4$ then $A_{ij} = 0$.
- If $0 < i + j < 8$ or $32 < i + j < 40$ then $A_{ij} = 0$.
- If $0 < 3i + j < 20$ or $76 < 3i + j < 96$ then $A_{ij} = 0$.
- $A_{i0} = \alpha_i$, where $\{\alpha_i, i = 0, \dots, 28\}$ is the weight distrubution of $\mathcal{A}$.
- $A_{ij} = A_{28-i,12-j}$, $i = 0, \dots, 28$, $j = 0, \dots, 12$.

According to the MacWilliams identities for coordinate partitions (see [11]) and the above restrictions, we obtain the following system of linear equations

$$2^{20} A_{s,0} = \sum_{i=0}^{28} \sum_{j=0}^{12} \mathcal{K}_s(i;28)\mathcal{K}_0(j;12)A_{i,j}; \qquad 2^{20} A_{s,1} = \sum_{i=0}^{28} \sum_{j=0}^{12} \mathcal{K}_s(i;28)\mathcal{K}_1(j;12)A_{i,j}$$

$$\Longleftrightarrow \; 2^{20} A_{s,0} = \sum_{i=0}^{28} \sum_{j=0}^{12} \mathcal{K}_s(i;28)A_{i,j}; \qquad 2^{20} A_{s,1} = \sum_{i=0}^{28} \sum_{j=0}^{12} \mathcal{K}_s(i;28)(12-2j)A_{i,j}$$

$$\Longleftrightarrow \; 2^{20} A_{s,0} = \sum_{i=0}^{28} \sum_{j=0}^{12} \mathcal{K}_s(i;28)A_{i,j}; \qquad 2^{20}(12A_{s,0} - A_{s,1}) = 2\sum_{i=0}^{28} \sum_{j=0}^{12} j\mathcal{K}_s(i;28)A_{i,j}$$

Solving this system with respect to 25 of the unknowns, using Computer Algebra System Maple, we obtain $\lambda = -1$, a contradiction. $\square$

References

[1] E.F. Assmus and H.F. Mattson, New 5-designs *J. Combin. Theory* 6 (1969), 122-151.

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

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

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

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

[6] Gerzson Kéri, Tables for n-arcs and lists for complete n-arcs in $PG(r, q)$, `http://www.sztaki.hu/ keri/n-arcs/index.htm.`

[7] San Ling and Patrick Solé, On the algebraic structure of quasi-cyclic codes I: Finite fields, *IEEE Trans. Inform. Theory* 47 (2001), 2751-2760.

[8] C.L. Mallows and N.J.A. Sloane, *An upper bound for self-dual codes*, Inform. and Control 22 (1973), 188-200.

[9] E.M. Rains, Shadow bounds for self-dual-codes, *IEEE Trans. Inform. Theory* 44 (1998), 134-139.

[10] E. M. Rains and N. J. A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Elsevier, Amsterdam, 1998, pp. 177-294.

[11] J. Simonis, *MacWilliams identities and coordinate partitions*, Linear Algebra Appl. 216 (1995) 81-91.

[12] V. Yorgov and N. Yankov, On the extremal binary codes of lengths 36 and 38 with an automorphism of order 5, Proceedings of the fifth int. workshop ACCT, Sozopol, Bulgaria, 1996, pp. 307-312.