THE AUTOMORPHISM GROUP OF A SELF-DUAL [72,36,16] CODE DOES NOT CONTAIN $S_3$, $A_4$ OR $D_8$

Martino Borello and Francesca Dalla Volta
Dipartimento di Matematica e Applicazioni
Università degli Studi di Milano Bicocca
20125 Milan, Italy

Gabriele Nebe
Lehrstuhl D für Mathematik
RWTH Aachen University
52056 Aachen, Germany

(Communicated by Wolfgang Willems)

Abstract. A computer calculation with Magma shows that there is no extremal self-dual binary code $C$ of length 72 whose automorphism group contains the symmetric group of degree 3, the alternating group of degree 4 or the dihedral group of order 8. Combining this with the known results in the literature one obtains that $\text{Aut}(C)$ has order at most 5 or is isomorphic to the elementary abelian group of order 8.

1. Introduction

Let $C = C^\perp \leq F_2^n$ be a binary self-dual code of length $n$. Then the weight $wt(c) := |\{i \mid c_i = 1\}|$ of every $c \in C$ is even. When in particular $wt(C) := \{wt(c) \mid c \in C\} \subseteq 4\mathbb{Z}$, the code is called doubly-even. Using invariant theory, one may show [10] that the minimum weight $d(C) := \min\{wt(C \setminus \{0\})\}$ of a doubly-even self-dual code is at most $4 + 4\left\lfloor \frac{n}{24} \right\rfloor$. Self-dual codes achieving this bound are called extremal. Extremal self-dual codes of length a multiple of 24 are particularly interesting for various reasons: for example they are always doubly-even [12] and all their codewords of a given nontrivial weight support 5-designs [2]. There are unique extremal self-dual codes of length 24 (the extended binary Golay code $G_{24}$) and 48 (the extended quadratic residue code $QR_{48}$) and both have a fairly big automorphism group (namely $\text{Aut}(G_{24}) \cong M_{24}$ and $\text{Aut}(QR_{48}) \cong \text{PSL}_2(47)$). The existence of an extremal code of length 72 is a long-standing open problem [13]. A series of papers investigates the automorphism group of a putative extremal self-dual code of length 72 excluding most of the subgroups of $S_{72}$. The most recent result is contained in [3] where the first author excluded the existence of automorphisms of order 6.

In this paper we prove that neither $S_3$ nor $A_4$ nor $D_8$ is contained in the automorphism group of such a code.

2010 Mathematics Subject Classification: Primary: 94B05, 20B25.
Key words and phrases: Extremal self-dual code, Automorphism group.

M. Borello and F. Dalla Volta are members of INdAM-GNSAGA, Italy. F. Dalla Volta and G. Nebe were partially supported by MIUR-Italy via PRIN “Group theory and applications”.

503 ©2013 AIMS
The method to exclude $S_3$ (which is isomorphic to the dihedral group of order 6) is similar to that used for the dihedral group of order 10 in [8] and based on the classification of additive trace-Hermitian self-dual codes in $\mathbb{F}_2^{12}$ obtained in [7].

For the alternating group $A_4$ of degree 4 and the dihedral group $D_8$ of order 8, we use their structure as a semidirect product of an elementary abelian group of order 4 and a group of order 3 and 2 respectively. By [11] we know that the fixed code of any element of order 2 is isomorphic to a self-dual binary code $D$ of length 36 with minimum distance 8. These codes have been classified in [1]; up to equivalence there are 41 such codes $D$. For all possible lifts $\tilde{D} \leq \mathbb{F}_2^{12}$ that respect the given actions we compute the codes $\mathcal{E} := \tilde{D}^{A_4}$ and $\mathcal{E} := \tilde{D}^{D_8}$ respectively. We have respectively only three and four such codes $\mathcal{E}$ with minimum distance $\geq 16$. Running through all doubly-even $A_4$-invariant self-dual overcodes of $\mathcal{E}$ we see that no such code is extremal. Since the group $D_8$ contains a cyclic group of order 4, say $C_4$, we use the fact [11] that $\mathcal{C}$ is a free $\mathbb{F}_2 C_4$-module. Checking all doubly-even self-dual overcodes of $\mathcal{E}$ which are free $\mathbb{F}_2 C_4$-modules we see that, also in this case, none is extremal.

The present state of research is summarized in the following theorem.

**Theorem 1.** The automorphism group of a self-dual $[72, 36, 16]$ code is either cyclic of order 1, 2, 3, 4, 5 or elementary abelian of order 4 or 8.

All results are obtained using extensive computations in Magma [4].

2. The symmetric group of degree 3

2.1. Preliminaries. Let $\mathcal{C}$ be a binary self-dual code and let $g$ be an automorphism of $\mathcal{C}$ of odd prime order $p$. Define $\mathcal{C}(g) := \{c \in \mathcal{C} \mid c^g = c\}$ and $\mathcal{E}(g)$ the set of all the codewords that have even weight on the cycles of $g$. From a module theoretical point of view, $\mathcal{C}$ is a $\mathbb{F}_2(g)$-module and $\mathcal{C}(g) = \mathcal{C} \cdot (1 + g + \ldots + g^{p-1})$ and $\mathcal{E}(g) = \mathcal{C} \cdot (g + \ldots + g^{p-1})$.

In [9] Huffman notes (it is a special case of Maschke’s theorem) that

$$\mathcal{C} = \mathcal{C}(g) \oplus \mathcal{E}(g).$$

In particular it is easy to prove that the dimension of $\mathcal{E}(g)$ is $\frac{(p-1)e}{2}$ where $e$ is the number of cycles of $g$. In the usual manner we can identify vectors of length $p$ with polynomials in $Q := \mathbb{F}_2[x]/(x^p - 1)$; that is $(v_1, v_2, \ldots, v_p)$ corresponds to $v_1 + v_2 x + \ldots + v_p x^{p-1}$. The weight of a polynomial is the number of nonzero coefficients. Let $\mathcal{P} \subset Q$ be the set of all even weight polynomials. If $1 + x + \ldots + x^{p-1}$ is irreducible in $\mathbb{F}_2(x)$ then $\mathcal{P}$ is a field with identity $x + x^2 + \ldots + x^{p-1}$ [9]. There is a natural map that we will describe only in our particular case in the next section, from $\mathcal{E}(g)$ to $\mathcal{P}^e$. Let us observe here only the fact that, if $p = 3$, then $1 + x + x^2$ is irreducible in $\mathbb{F}_2[x]$ and $\mathcal{P}$ is isomorphic to $\mathbb{F}_4$, the field with four elements. The identification is the following:

<table>
<thead>
<tr>
<th>0</th>
<th>000</th>
<th>$\omega$</th>
<th>110</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>011</td>
<td>$\overline{\omega}$</td>
<td>101</td>
</tr>
</tbody>
</table>

2.2. The computations for $S_3$. Let $\mathcal{C}$ be an extremal self-dual code of length 72 and suppose that $G \leq \text{Aut}(\mathcal{C})$ with $G \cong S_3$. Let $\sigma$ denote an element of order 2 and $g$ an element of order 3 in $G$. By [5] and [6], $\sigma$ and $g$ have no fixed points. So, in particular, $\sigma$ has 36 2-cycles and $g$ has 24 3-cycles. Let us suppose, w.l.o.g. that $\sigma = (1, 4)(2, 6)(3, 5) \ldots (67, 70)(68, 72)(69, 71)$

Advances in Mathematics of Communications

Volume 7, No. 4 (2013), 503–510
and
\[ g = (1, 2, 3)(4, 5, 6) \ldots (67, 68, 69)(70, 71, 72). \]

As we have seen in Section 2.1,
\[ C = \mathcal{C}(g) \oplus \mathcal{E}(g) \]
where \( \mathcal{E}(g) \) is the subcode of \( C \) of all the codewords with an even weight on the cycles of \( g \), of dimension 24. We can consider a map
\[ f : \mathcal{E}(g) \rightarrow \mathbb{F}_4^{24} \]
extending the identification \( \mathcal{P} \cong \mathbb{F}_4 \), stated in Section 2.1, to each cycle of \( g \).

Again by [9], \( \mathcal{E}(g)' := f(\mathcal{E}(g)) \) is an Hermitian self-dual code over \( \mathbb{F}_4 \) (that is \( \mathcal{E}(g)' = \{ \epsilon \in \mathbb{F}_4^{24} \mid \sum_{i=0}^{24} \epsilon_i \overline{\gamma_i} = 0 \text{ for all } \gamma \in \mathcal{E}(g)' \} \), where \( \overline{\alpha} = \alpha^2 \) is the conjugate of \( \alpha \) in \( \mathbb{F}_4 \). Clearly the minimum distance of \( \mathcal{E}(g)' \) is \( \geq 8 \). So \( \mathcal{E}(g)' \) is a \([24, 12, \geq 8]_4\) Hermitian self-dual code.

The action of \( \sigma \) on \( \mathcal{C} \subset \mathbb{F}_2^{24} \) induces an action on \( \mathcal{E}(g)' \subset \mathbb{F}_4^{24} \), namely
\[ (\epsilon_1, \epsilon_2, \ldots, \epsilon_{24})' = (\epsilon_2, \epsilon_1, \ldots, \epsilon_{23}, \epsilon_{24}). \]
Note that this action is only \( \mathbb{F}_2 \)-linear. In particular, the subcode fixed by \( \sigma \), say \( \mathcal{E}(g)'(\sigma) \), is
\[ \mathcal{E}(g)'(\sigma) = \{(\epsilon_1, \epsilon_1, \ldots, \epsilon_{12}, \overline{\epsilon_{12}}) \in \mathcal{E}(g)' \}. \]

**Proposition 1.** (cf. [8, Cor. 5.6]) The code
\[ \mathcal{X} := \pi(\mathcal{E}(g)'(\sigma)) := \{(\epsilon_1, \ldots, \epsilon_{12}) \in \mathbb{F}_4^{12} \mid (\epsilon_1, \overline{\epsilon_1}, \ldots, \epsilon_{12}, \overline{\epsilon_{12}}) \in \mathcal{E}(g)' \} \]
is an additive trace-Hermitian self-dual \([12, 2^{12}, \geq 4]_4\) code such that
\[ \mathcal{E}(g)' := \phi(\mathcal{X}) := \{(\epsilon_1, \overline{\epsilon_1}, \ldots, \epsilon_{12}, \overline{\epsilon_{12}}) \mid (\epsilon_1, \ldots, \epsilon_{12}) \in \mathcal{X} \} \mathbb{F}_4. \]

**Proof.** For \( \gamma, \epsilon \in \mathcal{X} \) the inner product of their preimages in \( \mathcal{E}(g)'(\sigma) \) is
\[ \sum_{i=1}^{12} (\epsilon_i \overline{\gamma_i} + \overline{\epsilon_i} \gamma_i) \]
which is 0 since \( \mathcal{E}(g)'(\sigma) \) is self-orthogonal. Therefore \( \mathcal{X} \) is trace-Hermitian self-orthogonal. Thus
\[ \dim_{\mathbb{F}_2}(\mathcal{X}) = \dim_{\mathbb{F}_2}(\mathcal{E}(g)'(\sigma)) = \frac{1}{2} \dim_{\mathbb{F}_2}(\mathcal{E}(g)') \]
since \( \mathcal{E}(g)' \) is a projective \( \mathbb{F}_2(\sigma) \)-module, and so \( \mathcal{X} \) is self-dual. Since \( \dim_{\mathbb{F}_2}(\mathcal{X}) = 12 = \dim_{\mathbb{F}_2}(\mathcal{E}(g)') \), the \( \mathbb{F}_4 \)-linear code \( \mathcal{E}(g)' \subset \mathbb{F}_4^{24} \) is obtained from \( \mathcal{X} \) as stated. \( \square \)

All additive trace-Hermitian self-dual codes in \( \mathbb{F}_4^{12} \) are classified in [7]. There are 195,520 such codes that have minimum distance \( \geq 4 \) up to monomial equivalence.

**Remark 1.** If \( X \) and \( Y \) are monomial equivalent, via a \( 12 \times 12 \) monomial matrix \( M := (m_{i,j}) \), then \( \phi(X) \) and \( \phi(Y) \) are monomial equivalent too, via the \( 24 \times 24 \) monomial matrix \( M' := (m'_{i,j}) \), where \( m'_{2i-1,2j-1} = m_{i,j} \) and \( m'_{2i,2j} = \overline{m_{i,j}} \), for all \( i, j \in \{1, \ldots, 12\} \).

An exhaustive search with Magma (of about 7 minutes CPU on an Intel(R) Xeon(R) CPU X5460 @ 3.16GHz) shows that the minimum distance of \( \phi(X) \) is \( \leq 6 \), for each of the 195,520 additive trace-Hermitian self-dual \([12, 2^{12}, \geq 4]_4\) codes. But \( \mathcal{E}(g)' \) should have minimum distance \( \geq 8 \), a contradiction. So we proved the following.
Theorem 2. The automorphism group of a self-dual $[72,36,16]$ code does not contain a subgroup isomorphic to $S_3$.

3. THE ALTERNATING GROUP OF DEGREE 4 AND THE DIHEDRAL GROUP OF ORDER 8

3.1. The action of the Klein four group. For the alternating group $A_4$ of degree 4 and the dihedral group $D_8$ of order 8 we use their structure

$$A_4 \cong \mathcal{V}_4 : C_3 \cong (C_2 \times C_2) : C_3 = \langle g, h : \langle \sigma \rangle \rangle,$$

$$D_8 \cong \mathcal{V}_4 : C_2 \cong (C_2 \times C_2) : C_2 = \langle g, h : \langle \sigma \rangle \rangle$$

as a semidirect product.

Let $H$ be some extremal $[72,36,16]$ code such that $H \leq \text{Aut}(C)$ where $H \cong A_4$ or $H \cong D_8$. Then by [5] and [6] all non trivial elements in $H$ act without fixed points and we may replace $C$ by some equivalent code so that

$$g = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)\ldots(71,72),$$

$$h = (1,3)(2,4)(5,7)(6,8)(9,11)(10,12)\ldots(70,72),$$

$$\sigma = (1,5,9)(2,7,12)(3,8,10)(4,6,11)\ldots(64,66,71) \quad \text{(for $A_4$)},$$

$$\sigma = (1,5)(2,8)(3,7)(4,6)\ldots(68,70) \quad \text{(for $D_8$)}.$$

Let

$\mathcal{G} := C_{S_{72}}(H) := \{ t \in S_{72} \mid tg = gt, th = ht, t\sigma = \sigma t \}$

denote the centralizer of this subgroup $H$ in $S_{72}$. Then $\mathcal{G}$ acts on the set of extremal $H$-invariant self-dual codes and we aim to find a system of orbit representatives for this action.

Definition 1. Let

$$\pi_1 : \{ v \in \mathbb{F}_2^{72} \mid v^9 = v \} \to \mathbb{F}_2^{36},$$

$$(v_1, v_2, v_3, \ldots, v_{36}) \mapsto (v_1, v_2, \ldots, v_{36})$$

denote the bijection between the fixed space of $g$ and $\mathbb{F}_2^{36}$ and

$$\pi_2 : \{ v \in \mathbb{F}_2^{72} \mid v^9 = v \text{ and } v^h = v \} \to \mathbb{F}_2^{18},$$

$$(v_1, v_2, v_3, \ldots, v_{18}) \mapsto (v_1, v_2, \ldots, v_{18})$$

denote the bijection between the fixed space of $\langle g, h \rangle \triangleleft A_4$ and $\mathbb{F}_2^{18}$. Then $h$ acts on the image of $\mathbb{F}_2^{18}$ as

$$(1,2)(3,4)\ldots(35,36).$$

Let

$$\pi_3 : \{ v \in \mathbb{F}_2^{36} \mid v^{\pi_1(h)} = v \} \to \mathbb{F}_2^{18},$$

$$(v_1, v_2, v_3, \ldots, v_{18}) \mapsto (v_1, v_2, \ldots, v_{18}),$$

so that $\pi_2 = \pi_3 \circ \pi_1$.

Remark 2. The centraliser $C_{S_{72}}(g) \cong C_2 \wr S_{36}$ of $g$ acts on the set of fixed points of $g$. Using the isomorphism $\pi_1$ we obtain a group epimorphism which we again denote by $\pi_1$

$$\pi_1 : C_{S_{72}}(g) \to S_{36}$$

with kernel $C_{36}^9$. Similarly we obtain the epimorphism

$$\pi_3 : C_{S_{36}}(\pi_1(h)) \to S_{18}.$$

The normalizer $N_{S_{72}}(\langle g, h \rangle)$ acts on the set of $\langle g, h \rangle$-orbits which defines a homomorphism

$$\pi_2 : N_{S_{72}}(\langle g, h \rangle) \to S_{18}.$$
Let us consider the fixed code $C(g)$ which is isomorphic to $\pi_1(C(g)) = \{(c_1, c_2, \ldots, c_{36}) \mid (c_1, c_1, c_2, c_2, \ldots, c_{36}, c_{36}) \in C\}$. By [11], the code $\pi_1(C(g))$ is some self-dual code of length 36 and minimum distance 8. These codes have been classified in [1]; up to equivalence (under the action of the full symmetric group $S_{36}$) there are 41 such codes. Let $Y_1, \ldots, Y_{41}$ be a system of representatives of these extremal self-dual codes of length 36.

**Remark 3.** $C(g) \in \mathcal{D}$ where

$$\mathcal{D} := \left\{ D \leq \mathbb{F}_2^{36} \left| D = D^\perp, d(D) = 8, \pi_1(h) \in \text{Aut}(D) \right. \right. \left. \text{and } \pi_2(\sigma) \in \text{Aut}(\pi_3(D(\pi_1(h)))) \right\}.$$ 

For $1 \leq k \leq 41$ let $\mathcal{D}_k := \{ D \in \mathcal{D} \mid D \cong Y_k \}.$ Let $\mathcal{G}_{36} := \{ \tau \in C_{S_{36}}(\pi_1(h)) \mid \pi_3(\tau)\pi_2(\sigma) = \pi_2(\sigma)\pi_3(\tau) \}.$

**Remark 4.** For $\mathcal{H} \cong A_4$ the group $\mathcal{G}_{36}$ is isomorphic to $C_2 \leq C_3 \leq S_6$. It contains $\pi_1(\mathcal{G}) \cong A_4 \leq S_6$ of index 64. For $\mathcal{H} \cong D_8$ we get $\mathcal{G}_{36} = \pi_1(\mathcal{G}) \cong C_2 \leq C_2 \leq S_6$.

**Lemma 1.** A set of representatives of the $\mathcal{G}_{36}$ orbits on $\mathcal{D}_k$ can be computed by performing the following computations:

- Let $h_1, \ldots, h_s$ represent the conjugacy classes of fixed point free elements of order 2 in $\text{Aut}(Y_k)$.
- Compute elements $\tau_1, \ldots, \tau_s \in S_{36}$ such that $\tau_i^{-1}h_1\tau_i = \pi_1(h)$ and put $D_i := Y_k^{\tau_i}$ so that $\pi_1(h) \in \text{Aut}(D_i)$.
- For all $D_i$ let $\sigma_1, \ldots, \sigma_{t_i}$ a set of representatives of the action by conjugation by the subgroup $\pi_3(C_{\text{Aut}(D_i)}(\pi_1(h)))$ on fixed point free elements of order 3 (for $\mathcal{H} \cong A_4$) respectively 2 (for $\mathcal{H} \cong D_8$) in $\text{Aut}(\pi_3(D_i(\pi_1(h))))$.
- Compute elements $\rho_1, \ldots, \rho_{t_i} \in S_{18}$ such that $\rho_j^{-1}\sigma_j\rho_j = \pi_3(\sigma)$, lift $\rho_j$ naturally to a permutation $\tilde{\rho}_j \in S_{36}$ commuting with $\pi_1(h)$ (defined by $\tilde{\rho}_j(2a - 1) = 2\rho_j(a) - 1$, $\tilde{\rho}_j(2a) = 2\rho_j(a)$) and put $D_{i,j} := (D_i)^{\tilde{\rho}_j} = Y_k^{\tau_i^{\tilde{\rho}_j}}$ so that $\pi_3(\sigma) \in \text{Aut}(\pi_2(D_{i,j}(\pi_1(h))))$.

Then $\{D_{i,j} \mid 1 \leq i \leq s, 1 \leq j \leq t_i\}$ represent the $\mathcal{G}_{36}$-orbits on $\mathcal{D}_k$.

**Proof.** Clearly these codes lie in $\mathcal{D}_k$.

Now assume that there is some $\tau \in \mathcal{G}_{36}$ such that $Y_k^{\tau \tilde{\rho}_j \tau} = D_i^{\tilde{\rho}_j} = D_{i,j} = Y_k^{\tau_i^{\tilde{\rho}_j}}$. Then

$$\epsilon := \tau_i^{\tilde{\rho}_j} \tau \tilde{\rho}^{-1}_j \tau_i^{-1} \in \text{Aut}(Y_k)$$

satisfies $\epsilon h_i \epsilon^{-1} = h_{i'}$, so $h_i$ and $h_{i'}$ are conjugate in $\text{Aut}(Y_k)$, which implies $i = i'$ (and so $\tau_i = \tau_i$). Now,

$$Y_k^{\tau_i^{\tilde{\rho}_j} \tau} = D_i^{\tilde{\rho}_j} = Y_k^{\tau_i^{\tilde{\rho}_j}}.$$

Then

$$\epsilon' := \tilde{\rho}_j \tau \tilde{\rho}_j^{-1} \in \text{Aut}(D_i)$$

commutes with $\pi_1(h)$. We compute that $\pi_3(\epsilon')\sigma_j \pi_3(\epsilon'^{-1}) = \sigma_j$ and hence $j = j'$. 

---

*Advances in Mathematics of Communications: Volume 7, No. 4 (2013), 503–510*
Now let \( D \in D_k \) and choose some \( \xi \in S_{36} \) such that \( D^\xi = Y_k \). Then \( \pi_1(h)^\xi \) is conjugate to some of the chosen representatives \( h_i \in \text{Aut}(Y_k) \) \( (i = 1, \ldots, s) \) and we may multiply \( \xi \) by some automorphism of \( Y_k \) so that \( \pi_1(h)^\xi = h_i = \pi_1(h)^{\tau_i} \). So \( \xi \tau_i \in C_{S_{36}}(\pi_1(h)) \) and \( D^{\xi \tau_i} = Y_k^{\tau_i} = D_i \). Since \( \varpi \sigma \in \text{Aut}(\pi_3(D(\pi_1(h)))) \) we get
\[
\varpi(3(\pi_3(\pi_1(h)))) \in \text{Aut}(\pi_3(D(\pi_1(h))))
\]
and so there is some automorphism \( \alpha \in \mathcal{P}_3(C_{\text{Aut}}(D_3)(\pi_1(h))) \) and some \( j \in \{1, \ldots, t_i\} \) such that \( (\pi_3(\pi_1(\xi \tau_i)))^\alpha = \sigma_j \). Then
\[
D^{\xi \tau_i \tilde{\alpha} \tilde{\rho}_j} = D_{i,j}
\]
where \( \xi \tau_i \tilde{\alpha} \tilde{\rho}_j \in G_{36} \).

3.2. The computations for \( \mathcal{A}_4 \). We now deal with the case \( \mathcal{H} \cong \mathcal{A}_4 \).

**Remark 5.** With Magma we use the algorithm given in Lemma 1 to compute that there are exactly 25, 299 \( G_{36} \)-orbits on \( D \), represented by, say, \( X_1, \ldots, X_{25,299} \).

As \( G \) is the centraliser of \( \mathcal{A}_4 \) in \( S_{72} \) the image \( \pi_1(G) \) commutes with \( \pi_1(h) \) and \( \pi_2(G) \) centralizes \( \pi_2(\sigma) \). In particular the group \( G_{36} \) contains \( \pi_1(G) \) as a subgroup. With Magma we compute that \( |G_{36} : \pi_1(G)| = 64 \). Let \( g_1, \ldots, g_{64} \in G_{36} \) be a left transversal of \( \pi_1(G) \) in \( G_{36} \).

**Remark 6.** The set \( \{X_i^g \mid 1 \leq i \leq 25, 299, 1 \leq j \leq 64 \} \) contains a set of representatives of the \( \pi_1(G) \)-orbits on \( D \).

**Remark 7.** For all \( 1 \leq i \leq 25, 299, 1 \leq j \leq 64 \) we compute the code
\[
\mathcal{E} := \mathcal{E}(X_i^g, \sigma) := \tilde{D} + \tilde{D}^\sigma + \tilde{D}^{\sigma^2}, \text{ where } \tilde{D} = \pi_1^{-1}(X_i^g).
\]
For three \( X_i \) there are two codes \( \tilde{D}_{i,1} = \pi_1^{-1}(X_i^{g_{j1}}) \) and \( \tilde{D}_{i,2} = \pi_1^{-1}(X_i^{g_{j2}}) \) such that \( \mathcal{E}(X_i^{g_{j1}}, \sigma) \) and \( \mathcal{E}(X_i^{g_{j2}}, \sigma) \) are doubly even and of minimum distance 16. In all three cases, the two codes are equivalent. Let us call the inequivalent codes \( \mathcal{E}_1, \mathcal{E}_2 \) and \( \mathcal{E}_3 \), respectively. They have dimension 26, 26, and 25, respectively, minimum distance 16 and their automorphism groups are
\[
\text{Aut}(\mathcal{E}_1) \cong S_4, \text{Aut}(\mathcal{E}_2) \text{ of order 432, Aut}(\mathcal{E}_3) \cong (\mathcal{A}_4 \times \mathcal{A}_5) : 2.
\]
All three groups contain a unique conjugacy class of subgroups conjugate in \( S_{72} \) to \( \mathcal{A}_4 \) (which is normal for \( \mathcal{E}_1 \) and \( \mathcal{E}_3 \)).

These computations took about 26 hours CPU, using an Intel(R) Xeon(R) CPU X5460 @ 3.16GHz.

**Corollary 1.** The code \( \mathcal{C}(g) + \mathcal{C}(h) + \mathcal{C}(gh) \) is equivalent under the action of \( G \) to one of the three codes \( \mathcal{E}_1, \mathcal{E}_2 \) or \( \mathcal{E}_3 \).

Let \( \mathcal{E} \) be one of these three codes. The group \( \mathcal{A}_4 \) acts on \( \mathcal{V} := \mathcal{E}^+ / \mathcal{E} \) with kernel \( \langle g, h \rangle \). The space \( \mathcal{V} \) is hence an \( F_2(\sigma) \)-module supporting a \( \sigma \)-invariant form such that \( \mathcal{C} \) is a self-dual submodule of \( \mathcal{V} \). As in Section 2.1 we obtain a canonical decomposition
\[
\mathcal{V} = \mathcal{V}(\sigma) \perp \mathcal{W}
\]
where \( \mathcal{V}(\sigma) \) is the fixed space of \( \sigma \) and \( \sigma \) acts as a primitive third root of unity on \( \mathcal{W} \).

For \( \mathcal{E} = \mathcal{E}_1 \) or \( \mathcal{E} = \mathcal{E}_2 \) we compute that \( \mathcal{V}(\sigma) \cong F_2^d \) and \( \mathcal{W} \cong F_2^s \). For both codes the full preimage of every self-dual submodule of \( \mathcal{V}(\sigma) \) is a code of minimum distance \( < 16 \).
The automorphism group of a self-dual code does not contain a subgroup isomorphic to $A_4$.

3.3. The computations for $D_8$. For this section we assume that $\mathcal{H} \cong D_8$. Then $\pi_1(\mathcal{G}) = \mathcal{G}_{36}$ and we may use Lemma 1 to compute a system of representatives of the $\pi_1(\mathcal{G})$-orbits on the set $\mathcal{D}$.

Remark 8. $\pi_1(\mathcal{G})$ acts on $\mathcal{D}$ with exactly 9,590 orbits represented by, say, $X_1, \ldots, X_{9,590}$. For all $1 \leq i \leq 9,590$ we compute the code

$$\mathcal{E} := E(X_i, \sigma) := \tilde{D} + \tilde{D}\sigma,$$

where $\tilde{D} = \pi_1^{-1}(X_i)$.

For four $X_i$ the code $E(X_i, \sigma)$ is doubly even and of minimum distance 16. Let us call the inequivalent codes $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ and $\mathcal{E}_4$, respectively. All have dimension 26 and minimum distance 16.

Corollary 2. The code $\mathcal{C}(g) + \mathcal{C}(h) + \mathcal{C}(gh)$ is equivalent under the action of $\mathcal{G}$ to one of the four codes $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ or $\mathcal{E}_4$.

This computation is very fast (it is due mainly to the fact that $\mathcal{G}_{36} = \pi(\mathcal{G})$). It took about 5 minutes CPU on an Intel(R) Xeon(R) CPU X5460 @ 3.16GHz.

As it seems to be quite hard to compute all $D_8$-invariant self-dual overcodes of $\mathcal{E}_i$ for these four codes $\mathcal{E}_i$ we apply a different strategy which is based on the fact that $h = (g\sigma)^2$ is the square of an element of order 4. So let

$$k := g\sigma = (1,8,3,6)(2,5,4,7) \ldots (66,69,68,71) \in D_8.$$

By [11], $\mathcal{C}$ is a free $\mathbb{F}_2(k)$-module (of rank 9). Since $\langle k \rangle$ is abelian, the module is both left and right; here we use the right notation. The regular module $\mathbb{F}_2(k)$ has a unique irreducible module, 1-dimensional, called the socle, that is $((1+k+k^2+k^3))$. So $\mathcal{C}$, as
a free $\mathbb{F}_2(k)$-module, has socle $\mathcal{C}(k) = C \cdot (1+k+k^2+k^3)$. This implies that, for every basis $b_1, \ldots, b_9$ of $\mathcal{C}(k)$, there exist $w_1, \ldots, w_9 \in \mathcal{C}$ such that $w_i \cdot (1+k+k^2+k^3) = b_i$ and

$$\mathcal{C} = w_1 \cdot \mathbb{F}_2(k) \oplus \ldots \oplus w_9 \cdot \mathbb{F}_2(k).$$

To get all the possible overcodes of $\mathcal{E}_i$, we choose a basis of the socle $\mathcal{E}_i(k)$, say $b_1, \ldots, b_9$, and look at the sets

$$W_{i,j} = \{ w + \mathcal{E}_i \in \mathcal{E}_i \cap \mathcal{E}_i \mid w \cdot (1+k+k^2+k^3) = b_j \text{ and } d(\mathcal{E}_i + w \cdot \mathbb{F}_2(k)) \geq 16 \}.$$

For every $i$ we have at least one $j$ for which the set $W_{i,j}$ is empty. This computation (of about 4 minutes CPU on the same computer) shows the following.

**Theorem 4.** The automorphism group of a self-dual $[72,36,16]$ code does not contain a subgroup isomorphic to $D_8$.

**ACKNOWLEDGMENTS**

The authors like to express their gratitude to A. Previtali for the fruitful discussions in Milan. They thank Laboratorio di Matematica Industriale e Crittografia of Trento for providing the computational infrastructure including the computer algebra system Magma.

**References**


Received March 2013; revised July 2013.

E-mail address: m.borello1@campus.unimib.it
E-mail address: francesca.dallavolta@unimib.it
E-mail address: nebe@math.rwth-aachen.de