The automorphism group of a self-dual $[72, 36, 16]$ code is not an elementary abelian group of order 8

Martino Borello

Member INdAM-GNSAGA (Italy), IEEE
Dipartimento di Matematica e Applicazioni
Università degli Studi di Milano Bicocca
20125 Milan, Italy
e-mail: m.borello1@campus.unimib.it

Abstract

The existence of an extremal self-dual binary linear code $\mathcal{C}$ of length 72 is a long-standing open problem. We continue the investigation of its automorphism group: looking at the combination of the subcodes fixed by different involutions and doing a computer calculation with Magma, we prove that $\mathrm{Aut}(\mathcal{C})$ is not isomorphic to the elementary abelian group of order 8. Combining this with the known results in the literature one obtains that $\mathrm{Aut}(\mathcal{C})$ has order at most 5.

Keywords: automorphism group, self-dual extremal codes

1. Introduction

A binary linear code of length n is a subspace of $\mathbb{F}_2^n$, where $\mathbb{F}_2$ is the field with 2 elements. A binary linear code $\mathcal{C}$ is called *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$ with respect to the Euclidean inner product. It follows immediately that the dimension of such a code has to be the half of the length. The *minimum distance* of $\mathcal{C}$ is defined as $\mathrm{d}(\mathcal{C}) := \min_{c \in \mathcal{C}\setminus\{0\}}\{\#\{i \mid c_i = 1\}\}$. In [7] an upper bound for the minimum distance of self-dual binary linear codes is given. Codes achieving this bound are called *extremal*. The most interesting codes, for various reasons, are those whose length is a multiple of 24: in this case $\mathrm{d}(\mathcal{C}) = 4m + 4$, where $24m$ is the length of the code, and they give rise to beautiful combinatorial structures [2]. There are unique extremal self-dual codes of length 24 (the extended binary Golay code $\mathcal{G}_{24}$) and 48 (the extended quadratic residue code $\mathcal{QR}_{48}$). For nearly forty years many people have tried unsuccessfully to find an extremal self-dual code of length 72 [9]. The usual approach to this problem is to study the possible automorphism groups (see next section for the detailed definition of it). Most of the subgroups of S_{72} are now excluded: the last result is contained in [4], in which the authors finished to exclude all the non-abelian groups with order greater than 5.

In this paper we prove that the elementary abelian group of order 8 cannot occur as automorphism group of such a code, obtaining the following.

Theorem 1.1. *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.

The techniques which we use are similar to those of [3]. We know [8], up to equivalence, the possible subcodes fixed by all the non-trivial involutions. So we combine them pairwise, checking the minimum distance to be 16, and we classify their sum, up to equivalence. We get only a few extremal codes and all of them satisfy certain intersection properties that, with easy dimension arguments, make it impossible to sum a third fixed subcode without loosing the extremality.

All results are obtained using extensive computations in MAGMA [5].

2. Basic definitions and notations

Throughout the paper we will use the following notations for groups:

- C_m is the cyclic group of order m;
- S_m is the symmetric group of degree m;
- if A and B are two groups, $A \times B$ indicates their direct product;
- if A and B are two groups, $A \wr B$ indicates their wreath product.

Given a group G and a subgroup H of G ($H \leq G$) we denote $\mathrm{C}_G(H)$ the centralizer of H in G. Let $\kappa \in G$. Then $\mathrm{C}_G(\kappa) := \mathrm{C}_G(\langle\kappa\rangle)$, where $\langle\kappa\rangle$ is the (cyclic) group generated by κ.

Let us consider the ambient space $\mathbb{F}_2^n$. We will indicate with calligraphic capital letters the subspaces of $\mathbb{F}_2^n$, in order to distinguish them from groups. We have a natural (right) action of S_n on $\mathbb{F}_2^n$ defined as follows: let $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ and $\sigma \in S_n$; then

$$v^\sigma := (v_{1^{\sigma^{-1}}}, \ldots, v_{n^{\sigma^{-1}}}).$$

We have an action induced naturally on the subspaces of $\mathbb{F}_2^n$:

$$\mathcal{C}^\sigma := \{c^\sigma \mid c \in \mathcal{C}\},$$

where $\mathcal{C} \leq \mathbb{F}_2^n$ and $\sigma \in S_n$.

Let $\mathcal{C} \leq \mathbb{F}_2^n$. Then the *automorphism group* of the code $\mathcal{C}$ is the subgroup of S_n defined as

$$\mathrm{Aut}(\mathcal{C}) := \{\sigma \in S_n \mid \mathcal{C}^\sigma = \mathcal{C}\}.$$

Given a code $\mathcal{C}$ and an automorphism $\sigma \in \mathrm{Aut}(\mathcal{C})$ we define

$$\mathcal{C}(\sigma) := \{c \in \mathcal{C} \mid c^\sigma = c\}.$$

This is a subcode of $\mathcal{C}$ and we call it the *subcode fixed by* σ.

3. Preliminary observations

Let $\mathcal{C}$ be a self-dual $[72, 36, 16]$ code such that

$$\mathrm{Aut}(\mathcal{C}) \cong C_2 \times C_2 \times C_2 = \langle \alpha, \beta, \gamma \rangle.$$

By [6] all non-trivial elements of $\mathrm{Aut}(\mathcal{C})$ are fixed point free (that is of degree n) and we may relabel the coordinates so that

$$\begin{aligned}
\alpha &= (1,2)(3,4)(5,6)(7,8)\ldots(71,72) \\
\beta &= (1,3)(2,4)(5,7)(6,8)\ldots(70,72) \\
\gamma &= (1,5)(2,6)(3,7)(4,8)\ldots(68,72).
\end{aligned}$$

Definition 3.1. *Let $\mathcal{V} := \mathbb{F}_2^n$. Then*

$$\begin{aligned}
&\pi_\alpha : \mathcal{V}(\alpha) \to \mathbb{F}_2^{36} \\
&(v_1, v_1, v_2, v_2, v_3, v_3, v_4, v_4, \ldots, v_{36}, v_{36}) \mapsto (v_1, v_2, \ldots, v_{36})
\end{aligned}$$

denote the bijection between the subspace of fixed by α and $\mathbb{F}_2^{36}$,

$$\begin{aligned}
&\pi_\beta : \mathcal{V}(\beta) \to \mathbb{F}_2^{36} \\
&(v_1, v_2, v_1, v_2, v_3, v_4, v_3, v_4 \ldots, v_{35}, v_{36}) \mapsto (v_1, v_2, \ldots, v_{36})
\end{aligned}$$

denote the bijection between the subspace fixed by β and $\mathbb{F}_2^{36}$ and

$$\begin{aligned}
&\pi_\gamma : \mathcal{V}(\gamma) \to \mathbb{F}_2^{36} \\
&(v_1, v_2, v_3, v_4, v_1, v_2, v_3, v_4 \ldots, v_{35}, v_{36}) \mapsto (v_1, v_2, \ldots, v_{36})
\end{aligned}$$

denote the bijection between the subspace fixed by γ and $\mathbb{F}_2^{36}$.

Remark 3.2. *The centralizer* $\mathrm{C}_{S_{72}}(\alpha) \cong C_2 \wr S_{36}$ *of* α *acts on the set of fixed points of* α. *Using the isomorphism* π_α *we hence obtain a group epimorphism which we denote by* η_α

$$\eta_\alpha : \mathrm{C}_{S_{72}}(\alpha) \to S_{36}$$

with kernel C_2^{36}. *Similarly we obtain the epimorphisms*

$$\eta_\beta : \mathrm{C}_{S_{72}}(\beta) \to S_{36}$$

and

$$\eta_\gamma : \mathrm{C}_{S_{72}}(\gamma) \to S_{36}.$$

By [8] we have that all the projections of the fixed codes $\pi_\alpha(\mathcal{C}(\alpha))$,$\pi_\beta(\mathcal{C}(\beta))$ and $\pi_\gamma(\mathcal{C}(\gamma))$ are self-dual $[36, 18, 8]$ codes. Such codes have been classified in [1], up to equivalence (under the action of the full symmetric group S_{36}) there are 41 such codes. Notice that

$$\langle \eta_\alpha(\beta), \eta_\alpha(\gamma)\rangle = \langle \eta_\beta(\alpha), \eta_\beta(\gamma)\rangle = \langle \pi_\gamma(\alpha), \eta_\gamma(\beta)\rangle = \langle \chi, \mu\rangle \leq S_{36},$$

with

$$\chi = (1, 2)(3, 4) \dots (35, 36)$$

and

$$\mu = (1, 3)(2, 4) \dots (34, 36),$$

are contained in $\mathrm{Aut}(\pi_\alpha(\mathcal{C}(\alpha)))$, $\mathrm{Aut}(\pi_\beta(\mathcal{C}(\beta)))$ and $\mathrm{Aut}(\pi_\gamma(\mathcal{C}(\gamma)))$ respectively. Only 14 of the 41 codes, say $\mathbb{Y} := \{\mathcal{Y}_1, \dots, \mathcal{Y}_{14}\}$, have an automorphism group which contains at least one subgroup conjugate to $\langle \chi, \mu\rangle$.

By direct calculation on these 14 codes we get the following conditions on the intersection of the codes.

Lemma 3.3. *Let*

$$(\chi', \mu', \zeta') \in \{(\alpha, \beta, \gamma), (\alpha, \gamma, \beta), (\beta, \alpha, \gamma), (\beta, \gamma, \alpha), (\gamma, \alpha, \beta), (\gamma, \beta, \alpha)\}.$$

Then we have only the following possibilities:

$\dim(\mathcal{C}(\chi') \cap \mathcal{C}(\mu') \cap \mathcal{C}(\zeta'))$	$\dim(\mathcal{C}(\chi') \cap \mathcal{C}(\mu'))$	$\dim(\mathcal{C}(\chi') \cap \mathcal{C}(\zeta'))$
5	9	9
5	9	10
6	9	9
6	9	10
6	9	11
6	10	10
6	10	11

Let $G := \mathrm{C}_{S_{72}}(\mathrm{Aut}(\mathcal{C}))$. Then G acts on the set of extremal self-dual codes with automorphism group $\langle \alpha, \beta, \gamma \rangle$ and we aim to find a system of orbit representatives for this action. Here we have some differences with the non-abelian cases, since the full group $\langle \alpha, \beta, \gamma \rangle$ is a subgroup of the automorphism group of all the fixed subcodes $\mathcal{C}(\alpha), \mathcal{C}(\beta)$ and $\mathcal{C}(\gamma)$. The main property that we use is the following, which is straightforward to prove:

$$\pi_\alpha(\mathcal{C}(\alpha))(\chi) = \pi_\beta(\mathcal{C}(\beta))(\chi) \tag{1}$$

and similar relations for the other fixed subcodes. This allows us to combine properly $\mathcal{C}(\alpha)$ and $\mathcal{C}(\beta)$ classifying their sum.

4. Description of the calculations

Let

$$\mathbb{D} := \{\mathcal{D} = \mathcal{D}^\perp \leq \mathbb{F}_2^{36} \mid \mathrm{d}(\mathcal{D}) = 8,\ \langle \chi, \mu \rangle \leq \mathrm{Aut}(\mathcal{D})\}.$$

The group

$$G_{36} := \mathrm{C}_{S_{36}}(\langle \chi, \mu \rangle) = \eta_\alpha(G) = \eta_\beta(G) = \eta_\gamma(G)$$

acts, naturally, on this set.

Lemma 4.1. *A set of representatives of the G_{36}-orbits on $\mathbb{D}$ can be computed by performing the following computations on each $\mathcal{Y} \in \mathbb{Y}$:*

- *Let $\chi_1, \ldots, \chi_s$ represent the conjugacy classes of fixed point free elements of order 2 in $\mathrm{Aut}(\mathcal{Y})$.*
- *Compute elements $\tau_1, \ldots, \tau_s \in S_{36}$ such that $\tau_k^{-1}\chi_k\tau_k = \chi$ and put $\mathcal{Y}_k := \mathcal{Y}^{\tau_k}$ so that $\chi \in \mathrm{Aut}(\mathcal{Y}_k)$.*
- *For every $\mathcal{Y}_k$, consider the set of fixed point free elements $\tilde{\mu}$ of order 2 in $\mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_k)}(\chi)$ such that $\langle \chi, \tilde{\mu} \rangle$ is conjugate to $\langle \chi, \mu \rangle$ in S_{36}. Let $\mu_1, \ldots, \mu_{t_k}$ represent the $\mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_k)}(\chi)$-conjugacy classes in this set.*
- *Compute elements $\sigma_1, \ldots, \sigma_{t_k} \in \mathrm{C}_{S_{36}}(\chi)$ such that $\sigma_l^{-1}\mu_l\sigma_l = \mu$ and put $\mathcal{Y}_{k,l} := \mathcal{Y}_k^{\sigma_l}$ so that $\langle \chi, \mu \rangle \leq \mathrm{Aut}(\mathcal{Y}_{k,l})$.*

Then $\mathbb{D}' := \{\mathcal{Y}_{k,l} \mid \mathcal{Y} \in \mathbb{Y}, 1 \leq k \leq s, 1 \leq l \leq t_k\}$ represents the G_{36}-orbits on $\mathbb{D}$.

Proof. Clearly these codes lie in $\mathbb{D}$.
Since $G_{36} \leq S_{36}$, if we consider different elements in $\mathbb{Y}$, say $\mathcal{Y}$ and $\mathcal{Y}'$, then $\mathcal{Y}'_{k',l'}$ is not in the same orbit of $\mathcal{Y}_{k,l}$ for any k', l', k, l.
Now assume that there is some $\lambda \in G_{36}$ such that

$$\mathcal{Y}^{\tau_{k'}\sigma_{l'}} = \mathcal{Y}^{\lambda}_{k',l'} = \mathcal{Y}_{k,l} = \mathcal{Y}^{\tau_k \sigma_l}.$$

Then

$$\epsilon := \tau_{k'}\sigma_{l'}\lambda\sigma_l^{-1}\tau_k^{-1} \in \mathrm{Aut}(\mathcal{Y})$$

satisfies $\epsilon\chi_k\epsilon^{-1} = \chi_{k'}$, so χ_k and $\chi_{k'}$ are conjugate in $\mathrm{Aut}(\mathcal{Y})$, which implies $k = k'$ (and so $\tau_k = \tau_{k'}$). Now,

$$\mathcal{Y}^{\tau_k\sigma_{l'}\lambda} = \mathcal{Y}_k^{\sigma_{l'}\lambda} = \mathcal{Y}_k^{\sigma_l} = \mathcal{Y}^{\tau_k\sigma_l}.$$

Then

$$\epsilon' := \sigma_{l'}\lambda\sigma_l^{-1} \in \mathrm{Aut}(\mathcal{Y}_k)$$

commutes with χ. Furthermore $\epsilon'\sigma_l\epsilon'^{-1} = \sigma_{l'}$ and hence $l = l'$.

Now let $\mathcal{Z} \in \mathbb{D}$ and choose some $\xi \in S_{36}$ such that $\mathcal{Z}^{\xi} = \mathcal{Y} \in \mathbb{Y}$. Then $\xi^{-1}\chi\xi$ is conjugate to some of the chosen representatives $\chi_k \in \mathrm{Aut}(\mathcal{Y})$ $(i = 1, \ldots, s)$ and we may multiply ξ by some automorphism of $\mathcal{Y}$ so that

$$\xi^{-1}\chi\xi = \chi_k = \tau_k\chi\tau_k^{-1}.$$

So $\xi\tau_k \in \mathrm{C}_{S_{36}}(\chi)$ and $\mathcal{Z}^{\xi\tau_k} = \mathcal{Y}^{\tau_k} = \mathcal{Y}_k$.
It is straightforward to prove that the element $(\xi\tau_k)^{-1}\mu(\xi\tau_k) \in \mathrm{Aut}(\mathcal{Y}_k)$ is a fixed point free element of order 2 in $\mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_k)}(\chi)$ such that $\langle \chi, (\xi\tau_k)^{-1}\mu(\xi\tau_k)\rangle$ is conjugate to $\langle \chi, \mu \rangle$ in S_{36}. So there is some automorphism $\omega \in \mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_k)}(\chi)$ and some $l \in \{1, \ldots, t_k\}$ such that $(\xi\tau_k\omega)^{-1}\mu(\xi\tau_k\omega) = \mu_l$. Then

$$\mathcal{Y}^{\xi\tau_k\omega\sigma_l} = \mathcal{Y}_{k,l}$$

where $\xi\tau_k\omega\sigma_l \in G_{36}$. □

There are 242 such representatives. For our purposes we need to modify this set a little: consider the set $\{\mathcal{Y}(\chi) \mid \mathcal{Y} \in \mathbb{D}\}$ and take a set of representatives for the action of G_{36} on this set, say $\mathbb{E} := \{\mathcal{E}_1, \ldots, \mathcal{E}_m\}$. By calculations $m = 40$. For every $1 \leq i \leq m$ define the set

$$\tilde{\mathbb{D}}_i := \{\mathcal{Y}^{\epsilon} \mid \mathcal{Y} \in \mathbb{D}' \text{ such that there exists } \epsilon \in G_{36} \text{ so that } \mathcal{Y}(\chi)^{\epsilon} = \mathcal{E}_i\}.$$

Clearly $\bigcup_{i=1}^m \tilde{\mathbb{D}}_i$ is still a set of representatives of the G_{36}-orbits on $\mathbb{D}$, but now $\mathcal{Y}_j(\chi)$ and $\mathcal{Y}_k(\chi)$ are equal if $\mathcal{Y}_j$ and $\mathcal{Y}_k$ belong to the same $\tilde{\mathbb{D}}_i$ and they are not equivalent via the action of G_{36} if $\mathcal{Y}_j$ and $\mathcal{Y}_k$ do not belong to the same $\tilde{\mathbb{D}}_i$.

Let

$$\mathbb{D}_{(\alpha,\beta)_i} = \{\pi_\alpha^{-1}(\mathcal{Y}_\alpha)+(\pi_\beta^{-1}(\mathcal{Y}_\beta))^\omega \leq \mathbb{F}_2^{72} \mid \mathcal{Y}_\alpha, \mathcal{Y}_\beta \in \tilde{\mathbb{D}}_i, \omega \in \mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_\beta(\chi))}(\langle \chi, \mu \rangle)\}.$$

Remark 4.2. *Considering $(\pi_\beta^{-1}(\mathcal{Y}_\beta))^\omega$ with ω varying in $\mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_\beta(\chi))}(\langle \chi, \mu \rangle)$ is exactly the same as considering $(\pi_\beta^{-1}(\mathcal{Y}_\beta))^\tau$ with τ varying in a right transversal of*

$$\mathrm{Aut}(\mathcal{Y}_\beta(\chi)) \cap \mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_\beta(\chi))}(\langle \chi, \mu \rangle)$$

in

$$\mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_\beta(\chi))}(\langle \chi, \mu \rangle).$$

Obviously this makes the calculations faster.

Lemma 4.3. *The code $\mathcal{C}(\alpha) + \mathcal{C}(\beta) := \{v + w \mid v \in \mathcal{C}(\alpha) \text{ and } w \in \mathcal{C}(\beta)\}$ is equivalent, via the action of G, to an element of $\bigcup_{i=1}^m \mathbb{D}_{(a,b)_i}$.*

Proof. By Lemma 4.1 and by construction of $\bigcup_{i=1}^m \tilde{\mathbb{D}}_i$, there exist $i \in \{1, \dots, m\}$, $\mathcal{Y}_a \in \tilde{\mathbb{D}}_i$ and $\bar{\rho} \in G_{36}$ such that $\pi_\alpha(\mathcal{C}(\alpha))^{\bar{\rho}} = \mathcal{Y}_\alpha$. Choose $\rho \in \eta_\alpha^{-1}(\bar{\rho})$. Then it is easy to observe that

- $\pi_\beta(\mathcal{C}^\rho(\beta))$ is a self-dual $[36, 18, 8]$ code;
- $\langle \chi, \mu \rangle \leq \mathrm{Aut}(\pi_\beta(\mathcal{C}^\rho(\beta)))$ (since $\rho \in G$);
- $(\pi_\beta(\mathcal{C}^\rho(\beta)))(\chi) = (\pi_\alpha(\mathcal{C}^\rho(\alpha)))(\chi) = \mathcal{E}_i$ (as in (1)).

Now, $\{(\mathcal{Y}_\beta)^\tau \mid \mathcal{Y}_\beta \in \tilde{\mathbb{D}}_i,\ \tau \in \mathrm{C}_{\mathrm{Aut}(\mathcal{Y}_\beta(\chi))}(\langle \chi, \mu \rangle)\}$ is the set of all possible such codes, so $(\pi_\beta(\mathcal{C}^\rho(\beta)))(\chi)$ is one of these codes. □

Remark 4.4. *There are, up to equivalence in the full symmetric group S_{72}, only 22 codes in $\bigcup_{i=1}^m \mathbb{D}_{(\alpha,\beta)_i}$ such that the minimum distance is at least 16, say $\mathcal{D}_1, \dots, \mathcal{D}_{22}$. They are all $[72, 26, 16]$ codes. In particular*

$$\dim(\mathcal{D}_i(\alpha) \cap \mathcal{D}_i(\beta)) = 10.$$

Corollary 4.5. *The code $\mathcal{C}(\alpha) + \mathcal{C}(\beta)$ is equivalent, via the action of the full symmetric group S_{72}, to a code $\mathcal{D}_i$, with $i \in \{1, \dots, 22\}$.*

We can repeat in a completely analogous way all the procedure for the pairs (α, γ) and (β, γ), interchanging the roles of the elements α, β and γ. Then we get the following.

Corollary 4.6. *The codes* $\mathcal{C}(\alpha)+\mathcal{C}(\gamma) := \{v+w \mid v \in \mathcal{C}(\alpha)$ *and* $w \in \mathcal{C}(\gamma)\}$ *and* $\mathcal{C}(\beta)+\mathcal{C}(\gamma) := \{v+w \mid v \in \mathcal{C}(\beta)$ *and* $w \in \mathcal{C}(\gamma)\}$ *are equivalent, via the action of the full symmetric group* S_{72}*, to some codes* $\mathcal{D}_j$ *and* $\mathcal{D}_k$*, with* $j, k \in \{1, \ldots, 22\}$.

This implies that

$$\dim(\mathcal{C}(\alpha) \cap \mathcal{C}(\gamma)) = 10 \quad \text{and} \quad \dim(\mathcal{C}(\beta) \cap \mathcal{C}(\gamma)) = 10. \tag{2}$$

Furthermore, by Magma calculations we get that

$$\dim(\mathcal{C}(\alpha) \cap \mathcal{C}(\beta) \cap \mathcal{C}(\gamma)) = 5. \tag{3}$$

Both statements can be verified by taking all the elements α', β', γ' of order 2 and degree 72 in $\mathrm{Aut}(\mathcal{D}_i)$ such that $\langle \alpha', \beta', \gamma' \rangle$ is conjugate to $\langle \alpha, \beta, \gamma \rangle$ in S_{72}.

To get a contradiction it is now enough to observe that (2) and (3) are not compatible with the table in Lemma 3.3. So we conclude the following.

Theorem 4.7. *The automorphism group of a self-dual* $[72, 36, 16]$ *code does not contain a subgroup isomorphic to* $C_2 \times C_2 \times C_2$.

Acknowledgment

The author expresses his gratitude to F. Dalla Volta and G. Nebe for the fruitful discussions and suggestions. *Laboratorio di Matematica Industriale e Crittografia* of Trento deserves thanks for the help in the computational part.

[1] C. Aguilar Melchor, P. Gaborit, *On the classification of extremal* $[36, 18, 8]$ *binary self-dual codes.* IEEE Trans. Inform. Theory 54 (2008) 4743-4750.

[2] E. F. Assmuss, H.F. Mattson, *New* 5-*designs*, J. Combin. Theory 6 (1969) 122–151.

[3] M. Borello, *The automorphism group of a self-dual* $[72, 36, 16]$ *binary code does not contain elements of order* 6, IEEE Trans. Inform. Theory 58, No. 12 (2012), 7240–7245.

[4] M. Borello, F. Dalla Volta, G. Nebe, *The automorphism group of a self-dual* $[72, 36, 16]$ *code does not contain* $\mathcal{S}_3$, $\mathcal{A}_4$ *or* D_8, Advances in Mathematics of Communications (to appear), arXiv:1303.4899 (2013).

[5] W. Bosma, J. Cannon, C. Playoust, *The* MAGMA *algebra system* I*: The user language*, J. Symbol. Comput. 24 (1997) 235–265.

[6] S. Bouyuklieva, *On the automorphisms of order* 2 *with fixed points for the extremal self-dual codes of length* $24m$, Des. Codes Cryptogr. 25 (2002) 5–13.

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

[8] G. Nebe, *An extremal* $[72, 36, 16]$ *binary code has no automorphism group containing* $Z_2 \times Z_4$, Q_8, *or* Z_{10}, Finite Fields and their applications 18 (2012) 563–566.

[9] N.J.A. Sloane, *Is there a* $(72; 36)$ $d = 16$ *self-dual code?*, IEEE Trans. Inform. Theory 2 (1973) 251.