On the automorphism group of a binary self-dual doubly-even [72,36,16] code

E.A. O'Brien and Wolfgang Willems

Abstract

We prove that the automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code has order $5, 7, 10, 14$ or d where d divides 18 or 24, or it is $A_4 \times C_3$.

Keywords Automorphism group, extremal code of length 72

1 Introduction

The existence of a binary self-dual doubly-even $[72, 36, 16]$ code remains a long-standing question, first posed by Sloane [16] in 1973. Determining the automorphism group of such a code may be a useful first step to construct it. In a series of papers [7], [13], [14], [10], [4], [5], [19], both its order and structure have been investigated. The best result in this direction is the following established in [6].

The automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ *code has order* $5, 7, 10, 14, 56$*, or a divisor of* 72.

In this note we exclude all groups of order $72, 56$ and all but one group of order 36, obtaining the following.

Theorem 1 *The automorphism group of a binary self-dual doubly-even* $[72, 36, 16]$ *code has order* $5, 7, 10, 14$ *or* d*, where* d *divides* 18 *or* 24*, or it is* $A_4 \times C_3$*.*

Our proof combines methods from modular representation theory and extensive computations; the latter were carried out using Magma [1]. The minimum distance of a code was determined using the algorithm of Brouwer & Zimmermann [3]. We use the descriptions and identifiers of the groups of certain orders provided by the SmallGroups library [2].

Let K be the binary field $\mathbb{F}_2$ and let KG denote the group algebra of a finite group G over K. For a subgroup H of G, let K_H^G be the trivial H-module induced to G (see [11, Chap. VII, Section 4]). Note that $KG = K_H^G$ for $H = \langle 1 \rangle$. If we consider

K_H^G as the ambient space of a code then $Hg_1, \dots, Hg_s$ are used as the fixed basis, where $\{g_1, \dots, g_s\}$ is a set of transversal representatives of H in G. In particular, $a \in K_H^G$ can be written uniquely as $a = \sum_{i=1}^s a_i H g_i$ with $a_i \in K$. The natural non-degenerate bilinear form on K_H^G which defines the concept of duality for codes is given by

$$(Hg_i, Hg_j) = \delta_{ij}.$$

Observe that the form $(\cdot\,,\cdot)$ is G-invariant:

$$(Hg_i x, Hg_j x) = (Hg_i, Hg_j)$$

for all $x \in G$ and $i, j = 1, \dots, s$. For a KG-module V we denote by $\mathrm{soc}\,(V)$ the largest completely reducible submodule of V. Inductively, the k-th socle $\mathrm{soc}_{\,k}(V)$ of V is defined by

$$\mathrm{soc}_{\,k}(V)/\mathrm{soc}_{\,k-1}(V) = \mathrm{soc}\,(V/\mathrm{soc}_{\,k-1}(V)).$$

For other notation and basic facts about modular representation theory, we refer the reader to [11, Chap. VII].

Now suppose that C is a binary linear code of length n with automorphism group G. Thus C is a subspace of the vector space $V = K^n$. Via the action of G as a group of permutations on the coordinate positions, the space V carries the structure of a (right) KG-module. Since C is invariant under G, we deduce that C is a submodule of V. The module structure of the ambient space V can be described as follows. If $i_1, \dots, i_s$ are representatives of the orbits $\Omega_1, \dots, \Omega_s$ of G on $\Omega = \{1, \dots, n\}$ and if G_i denotes the stabilizer of $i \in \Omega$ in G, then

$$V = K^n = K_{G_{i_1}}^G \perp \dots \perp K_{G_{i_s}}^G. \tag{1}$$

Furthermore, if $|\Omega_{i_j}| = |G : G_{i_j}| = n_j$ then the elements in the first component $K_{G_{i_1}}^G$ have non-zero entries in the first n_1 positions, the elements in the second component $K_{G_{i_2}}^G$ have non-zero entries in positions $n_1 + 1, \dots, n_1 + n_2$, and so on. The bilinear form on V is the orthogonal sum of the bilinear forms on the components $K_{G_{i_j}}^G$.

2 Preliminaries

As above let V denote the ambient space of a binary code C with automorphism group G.

Lemma 2 *If $V = K^n = KG$ and $C = C^\perp$ is doubly-even then the Sylow 2-subgroup of G is not cyclic.*

Proof. See [17], or [12, Theorem 4.4]. □

Lemma 3 *Let $V = K^n = KG$ and suppose that all projective indecomposable modules are self-dual and occur with multiplicity 1 in a direct decomposition of V. If $C = C^\perp$ then*

$$\mathrm{soc}\,(C) = \mathrm{soc}\,(V) = \mathrm{soc}\,(KG).$$

Proof. Write $V = KG = P_1 \oplus \ldots \oplus P_m$ with projective indecomposable modules P_i. By assumption, the P_i are pairwise non-isomorphic. Furthermore,

$$\mathrm{soc}\,(V) = \mathrm{soc}\,(P_1) \oplus \ldots \oplus \mathrm{soc}\,(P_m),$$

and $\mathrm{soc}\,(P_i) = S_i$ for pairwise non-isomorphic simple modules S_i. Suppose that, for some i, $\mathrm{soc}\,(P_i) \not\subseteq \mathrm{soc}\,(C)$. Thus $C \cap P_i = 0$. According to [18]

$$V/C = V/C^\perp \cong C^*.$$

Thus P_i is (up to isomorphism) a submodule of C^*. Since P_i is projective, and so injective (see [11, Chap. VII, Theorem 7.8]), the submodule P_i is a direct summand of C^*. It follows that $P_i \cong P_i^*$ is a direct summand in $(C^*)^* \cong C$. Thus P_i occurs with multiplicity at least twice in V as a direct summand, a contradiction to the Krull-Schmidt Theorem (see [9, Chap. I, Theorem 11.4]). □

In order to carry out computations successfully, we need a finer splitting for the ambient space V as given in (1). Let $\hat{}: KG \to KG$ denote the antialgebra automorphism of KG defined by $g \to g^{-1}$ for $g \in G$. Let

$$1 = f_1 + \ldots + f_t$$

be a decomposition of $1 \in KG$ into central idempotents $f_i \in KG$ with $\hat{f_i} = f_i$. The latter condition means that $f_i KG \cong (f_i KG)^*$ as KG-modules. Finally, we put $V_i = V f_i$ and $C_i = C f_i \subseteq V_i$ for $i = 1, \ldots, t$.

Lemma 4 *With this notation we have*

a) $V = V_1 \perp \ldots \perp V_t$ and $C = C_1 \perp \ldots \perp C_t$ as KG-modules.

b) If $C = C^\perp$ then C_i is a self-dual code in V_i for $i = 1, \ldots, t$.

Proof. a) Clearly, $V = Vf_1 \oplus \ldots \oplus Vf_t$ and $C = Cf_1 \oplus \ldots \oplus Cf_t$ by standard arguments (see [11, Chap. VII, Theorem 12.1]). Since the idempotents f_i are central, the spaces Vf_i and Cf_i are KG-modules. It remains to prove that the decompositions are orthogonal. Let v and w be elements in $V = K^n$. Since G is a group of isometries on V, we have $(vg, w) = (v, wg^{-1})$ for all $g \in G$. In particular,

$$(V_i, V_j) = (Vf_i, Vf_j) = (V, Vf_j\hat{f_i}) = (V, Vf_jf_i)$$

since $\hat{f_i} = f_i$. But $f_jf_i = 0$ for $i \neq j$ which yields $(V_i, V_j) = 0$ for $i \neq j$. This proves that the decomposition for each of V and C is orthogonal.
b) Since $C = C^\perp$ in V and $C_i \subseteq V_i$, it follows that C_i is a self-dual code in V_i. □

2.1 The basic algorithm

Let C denote a binary self-dual doubly-even $[72, 36, 16]$ code. We use the following algorithm to demonstrate that a specified group G is not the automorphism group of C.

First, we search for pairwise orthogonal central idempotents in KG, say $f_1, \ldots, f_t$, such that $\hat{f_i} = f_i$ for $i = 1, \ldots, t$ and

$$1 = f_1 + \ldots + f_t.$$

Lemma 4 implies that $C = Cf_1 \perp \ldots \perp Cf_t$ where Cf_i is a self-dual doubly-even code in Vf_i.

Next we carry out the following steps:

Step 1. In each Vf_i we compute all self-dual doubly-even and G-invariant codes, say U_i, of minimum distance at least 16. We call such codes *good*. Let $\mathcal{L}_i$ be a listing of all good codes in Vf_i.

Step 2. We construct all modules U in $\mathcal{L} := \{U = U_1 + \ldots + U_t \mid U_i \in \mathcal{L}_i\}$.

Step 3. We compute the minimum distance of every $U \in \mathcal{L}$.

Suppose that the minimum distance for all $U \in \mathcal{L}$ computed in Step 3 is always strictly smaller than 16. Since C is one particular module in $\mathcal{L}$, the group G cannot be the automorphism group of C.

In the remainder, let C always be a binary self-dual doubly-even $[72, 36, 16]$ code with automorphism group G.

3 Excluding $|G| = 72$

Throughout this section we assume that $|G| = 72$. Since elements of order 2 and 3 act fixed-point-freely on the 72 coordinate positions (see [4] and [5]), the action of G on the positions is regular. Thus C is a self-dual doubly-even G-invariant code in the group algebra KG.

To show that none of the 50 groups of order 72 occurs as an automorphism group of C, we proceed as follows. By Lemma 2, we may assume that the Sylow 2-subgroup of G is not cyclic. Among the remaining groups, precisely three do not have a normal subgroup of order 3. They are:

(i) $G = (C_3 \times C_3).Q_8$

(ii) $G = (C_3 \times C_3).D_8$

(iii) $G = (C_3 \times C_3).(C_4 \times C_2)$

where Q_8 is a quaternion group of order 8, D_8 a dihedral group of order 8 and C_n is cyclic of order n.

For G of type (i), the ambient space KG has exactly 602361 submodules of dimension 36. All have minimum distance strictly smaller than 16. Thus G cannot be the automorphism group of C.

Next we consider the group G of type (ii). Let $H = \langle x, y\rangle$ denote the normal Sylow 3-subgroup of G. The action of D_8 on H has three orbits: 1; the orbit x, x^2, y, y^2; and the orbit xy, x^2y, xy^2, x^2y^2. The group algebra KG consists of three blocks generated by the principal block idempotent $f_1 = \sum_{h\in H} h$ and two other block idempotents $f_2 = x + x^2 + y + y^2$ resp. $f_3 = xy + x^2y + xy^2 + x^2y^2$. Note that $f_i = \hat{f}_i$ for $i = 1, 2, 3$. Furthermore, $\dim KGf_1 = 8$ and $\dim KGf_2 = KGf_3 = 32$. We now follow the three steps of the algorithm described above.

Step 1. The component KGf_1 contains exactly 6 modules $U_1 \in \mathcal{L}_1$. In each of KGf_2 and KGf_3 there are 90 modules $U_2 \in \mathcal{L}_2$ resp. $U_3 \in \mathcal{L}_3$.

Step 2. We compute all $6 \times 90 \times 90$ modules $U \in \mathcal{L}$.

Step 3. All modules $U \in \mathcal{L}$ have minimum distance strictly smaller than 16.

Thus G is not the automorphism group of C.

Finally, the group in (iii) can be ruled out similarly: we check $4\times 90\times 90$ modules $U \in \mathcal{L}$.

There remain 40 groups of order 72 which have a normal subgroup H of order 3. Let $f = \sum_{h\in H} h$. Clearly, f is a central idempotent in KG which satisfies $\hat{f} = f$. We put $f_1 = f$ and $f_2 = 1-f$ and apply the algorithm again. For 37 of these groups, all relevant $U \in \mathcal{L}$ have minimum distance strictly smaller than 16. Consequently these groups do not occur as automorphism groups.

In three cases it was not possible to compute directly $\mathcal{L}_2$. These are:

(α) $G = [(C_3 \times C_3) \times (C_2 \times C_2)]\langle t\rangle$ where t inverts all elements of order 3 and the Sylow 2-subgroup is a dihedral group of order 8.

(β) $G = C_3 \times C_2 \times \mathrm{A}_4$ where A_4 is the alternating group on 4 letters.

(γ) $G = (C_3 \times \mathrm{A}_4)\langle t\rangle$ where the involution t acts nontrivially on C_3 and $\mathrm{A}_4\langle t\rangle \cong \mathrm{S}_4$.

In case (α) the group algebra consists of 5 blocks. Thus we have the decomposition $1 = f_1 + \ldots + f_5$ with block idempotents f_i. Since each $f_i \in KT$ where T is a Sylow 3-subgroup of G and t inverts all 3-elements, all simple KG-modules are self-dual. In particular $\hat{f}_i = f_i$ for all i. We apply the algorithm again. In Step 1 we get 4 spaces U_1 in KGf_1 and 18 in each block KGf_i for $i = 2, \ldots, 5$. Step 2 produces 629856 modules U. Step 3 shows that all have minimum distance strictly smaller than 16. This eliminates (α).

Let $G = C_3 \times C_2 \times \mathrm{A}_4$. Since $O_2(G)$ is in the kernel of every simple module (see [11, Chap. VII, Theorem 13.4]), the group algebra KG has exactly 5 simple modules which are all self-dual. Furthermore, KG is a direct sum of non-isomorphic projective indecomposable modules. Thus the assumptions of Lemma 3 are satisfied. Moreover, KG has exactly two block idempotents, namely $f_1 = 1 + x + x^2$ where x generates the normal subgroup of order 3 and $f_2 = 1 - f_1$. It yields $\dim KGf_1 = 24$, hence $\dim KGf_2 = 48$. The block KGf_2 contains exactly three simple modules, all of dimension 2. Lemma 3 implies that $\mathrm{soc}\,(Cf_2) = \mathrm{soc}\,(KGf_2)$. We compute now the spaces $U = U_1 + \mathrm{soc}\,(KGf_2)$ for all $U_1 \in \mathcal{L}_1$. (Here we take only a particular subspace of KGf_2 in Step 1 which is contained in $Cf_2 \leq C$.) All such modules have minimum distance strictly smaller than 16. Thus a group of type (β) cannot be the automorphism group of C.

In the last case $G = (C_3 \times \mathrm{A}_4)\langle t\rangle$ where the involution t acts non-trivially on C_3 and $\mathrm{A}_4\langle t\rangle \cong \mathrm{S}_4$. We again put $f_1 = 1+x+x^2$ where x generates the normal subgroup of order 3 and $f_2 = 1 - f_1$. As in case (β), $\dim KGf_1 = 24$ and $\dim KGf_2 = 48$. The block KGf_1 contains 7607 submodules. Exactly 48 of them are good. The component KGf_2 has 9576333 submodules. Exactly 5184 are good. All modules in $\mathcal{L}$ have minimum distance strictly smaller than 16. Thus we have eliminated G and this completes the proof for $|G| = 72$.

4 Excluding $|G| = 56$

Throughout this section we assume that $|G| = 56$. Let T denote a Sylow 7-subgroup of G.

Lemma 5 *G contains a normal subgroup H of order 8 isomorphic to $C_2 \times C_2 \times C_2$ on which an element of order 7 acts faithfully. Moreover, the action of G on the 72 coordinate positions has three orbits of lengths 56, 8, 8.*

Proof. Observe that [6, Lemma 2 b)] implies $|N_G(T)| = 7$ or 14. Since the index $|G : N_G(T)| \equiv 1 \bmod 7$ we get $|N_G(T)| = 7$. Thus G has exactly 8 Sylow 7-subgroups and contains $6 \cdot 8 = 48$ elements of order 7. Hence the Sylow 2-subgroup of G is normal. Since a 7-element does not centralize an involution, G has exactly 7 involutions. This implies that the Sylow 2-subgroup is elementary abelian. By [4], an involution has no fixed points, and by [8], an element of order 7 has exactly two fixed points. Thus the Cauchy-Frobenius Lemma [15] implies that the action of G on the coordinate positions has

$$\frac{1}{56}(56 + 8 \cdot 6 \cdot 2) = 3$$

orbits, say of lengths m_1, m_2, m_3. Since $m_i \mid 56$ and $m_1+m_2+m_3 = 72$, we find the unique solution $m_1 = 56, m_2 = m_3 = 8$ (up to renumbering). □

Just one of the 13 groups of order 56, namely 56#11 in the notation of the SmallGroups library, satisfies Lemma 5.

Lemma 6 *Let G be 56#11 having group algebra KG.*

a) $V = K^{72} = KG \oplus P_1 \oplus P_2$ *where* $P_1 \cong P_2 \cong K_T^G$ *is the projective cover of the trivial KG-module. The elements of KG have non-zero entries only in the first 56 positions, the elements of P_1 in position 57 up to 64 and P_2 in the last 8 positions.*

b) $C \cap (P_1 \oplus P_2) = \{0, v\}$ *where v has entry 1 exactly in the last 16 coordinates.*

c) If $C_0 = KG \cap C \leq KG$ *then C_0 contains the all one-vector of KG and* $\dim C_0 = 21$.

Proof. a) This follows immediately by Lemma 5.
b) Note that $P_1 \oplus P_2$ has non-zero entries at most in the last 16 coordinates. Thus, if

$$C \cap (P_1 \oplus P_2) \neq 0$$

then the intersection contains v as the only non-zero vector, since the minimum weight of C is 16. Suppose that

$$C \cap (P_1 \oplus P_2) = 0.$$

In this case the projective module $P_1 \oplus P_2$ is (up to isomorphism) a submodule of the factor module

$$K^{72}/C = K^{72}/C^{\perp} \cong C^*,$$

hence a direct summand since $P_1 \oplus P_2$ is injective. It follows that

$$(P_1 \oplus P_2)^* \cong P_1^* \oplus P_2^* \cong P_1 \oplus P_2$$

is a direct summand of $C^{**} \cong C$. Therefore the projective cover of the trivial module has multiplicity at least 4 as a direct summand in K^{72}. This contradicts the fact that V contains the projective cover of the trivial module exactly three times since KG contains it only once.
c) Since C contains both the all one-vector of length 72 and v, it contains their sum which has a 1 as entry exactly in the first 56 coordinates. By repeated shortening of C (16 times), we see that $\dim C_0 = 21$ since $\dim C = 36$. □

Lemma 7 *Let G be 56#11. Its group algebra KG has the following properties.*

a) There are (up to isomorphism) exactly three simple modules: the trivial module 1_G and two modules V resp. V^* with $V \ncong V^*$ both of dimension 3.

b) The projective cover $P(1_G)$ of the trivial module is generated by the (non central) idempotent $e = \sum_{x \in T} x$.

c) $P(1_G)$ is uniserial with composition factors $1_G, V, V^*, 1_G$.

d) The Loewy lengths of the projective covers $P(V)$ and $P(V^*)$ of V resp. V^* are 4 for both.

e) $C_0 \leq \operatorname{soc}_3(KG)$.

Proof. a) Over a large field of characteristic 2, the group G has exactly 7 simple modules since the normal Sylow 2-subgroup H is in the kernel of any simple module. Over the binary field K we have only three simple modules $1_G, V$ and V^*.
b) This is clear since $P(1_G)$ is the trivial module of a 2-complement of G induced to G.
c) $P(1_G)$ considered as an H-module is the regular module KH. Since T acts on KH by conjugation and $P(1_G) \cong P(1_G)^*$ the assertion follows immediately.
d) This is a consequence of the fact that $P(V) \cong P(1_G) \otimes V$ resp. $P(V^*) \cong P(1_G) \otimes V^*$.
e) Note that $KG = P(1_G) \oplus P(V) \oplus P(V^*)$. Since the weights of the code words in C_0 are divisible by 2 the subcode C_0 is contained in the augmentation ideal of KG. Thus, if $C_0 \nleq \operatorname{soc}_3(KG)$ then C_0 contains a direct summand isomorphic to $P(V)$ or $P(V^*)$. This contradicts the fact that dim $C_0 = 21$ and dim $P(V) = \dim P(V^*) = 24$. □

To exclude G as an automorphism group of C we proceed as follows. In $\operatorname{soc}_3(KG)$, we compute all self-orthogonal submodules of dimension 21. The 1394667 such modules all have minimum distance strictly less than 16.

Hence a group of order 56 is not an automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code.

5 Excluding $|G| = 36$

Throughout this section we assume that $|G| = 36$. Since neither involutions nor elements of order 3 have fixed points (see [4] and [5]), the action of G on the 72 coordinate positions is fixed-point-freely. Thus the ambient space K^{72} is an orthogonal sum of two copies of the regular module KG:

$$V = K^{72} = KG \perp KG,$$

#	Group	Dimensions of simple modules	dim Vf_i	$\dim \mathrm{soc}_k(Vf_t)$
1	$D_{18} \times C_2$	1, 2, 6	8, 16, 48	24, 48
2	$C_9 \times C_4$	1, 2, 6	8, 16, 48	12, 24, 36, 48
3		1, 2, 6	24, 48	12, 36, 48
4	$C_9 \cdot C_4$	1, 2, 6	8, 16, 48	24, 48
5	$C_9 \times C_2 \times C_2$	1, 2, 6	8, 16, 48	12, 36, 48
11	$\mathrm{A}_4 \times C_3$	1, 2, 2, 2, 2	24, 48	12, 36, 48

Table 1: Data for certain groups of order 36

where the first KG has non-zero entries in the first 36 positions and the second in the last 36.

There are (up to isomorphism) 14 groups of order 36. One easily checks with MAGMA that for all of these groups the simple modules over K are self-dual. Thus the blocks of KG are self-dual and consequently we may write

$$1 = f_1 + \ldots + f_t$$

with block idempotents $f_i = \hat{f}_i \in KG$. If G is 2-nilpotent then each block contains (up to isomorphism) exactly one simple module (see [11, Chap. VII, Theorem 14.9]). This is true for all but two groups: 36#3 and 36#11.

We now proceed as follows. Let $\mathcal{L}_i$ be a listing of good codes in Vf_i for $i = 1, \ldots, t$, and let $\mathcal{L}$ consist of all codes $U = U_1 + \ldots + U_t$ with $U_i \in \mathcal{L}_i$.

Case 1. For each group 36#i with $6 \leq i \leq 10$ and $12 \leq i \leq 14$, we compute

$$U = U_1 + \ldots + U_t$$

where U_j runs over all codes in $\mathcal{L}_j$ for $j = 1, \ldots, t$. None of the codes U is doubly-even and of minimum distance at least 16. Hence none of these groups is an automorphism group. (Of course, we can terminate our investigation for a particular group if the set of modules $U_1 + \ldots + U_s$, where $s < t$ and the U_j are running through all modules in $\mathcal{L}_{i_j}$ with $i_j \neq i_k$ for $j \neq k$, does not contain a doubly-even code of minimum distance at least 16.)

Thus it remains to consider 36#i for $i = 1, 2, 3, 4, 5, 11$. In Table 1, for each we list dim Vf_i for $i = 1, \ldots, t$ and the dimensions of the socle series of Vf_t, the component of dimension 48. Where the group has a name indicating its structure, we use this.

Lemma 8 *Let $f = \hat{f}$ be a central idempotent of KG and suppose that KGf contains only one simple module (up to isomorphism) as composition factor. Then*

$$2 \dim \mathrm{soc}\,(Cf) \geq \dim \mathrm{soc}\,(Vf).$$

Proof. Let S be the unique simple module belonging to KGf and suppose that $\mathrm{soc}\,(KGf)$ contains S with multiplicity m. Since $V = KG \oplus KG$, the socle of Vf has in a direct decomposition $2m$ direct summands (isomorphic to S). Suppose that $\mathrm{soc}\,(Cf)$ has $m' < m$ direct summands. Then

$$Cf \leq P_1 \oplus \ldots \oplus P_{m'} \leq P_1 \oplus \ldots \oplus P_{m'} \oplus \ldots \oplus P_{2m} = Vf$$

where all P_i are isomorphic to the projective cover P of S. Note that $P \cong P^*$ and

$$Vf/Cf = Vf/(Cf)^{\perp} \cong (Cf)^*.$$

As in Lemma 3, $(Cf)^*$ contains more direct summands isomorphic to P than Cf. This contradicts the Krull-Schmidt Theorem (see [9, Chap. I, Theorem 11.4]). □

Case 2. To deal with the groups 36#i for $i = 1, 4$, we modify the computation of all good codes in the component $V_t := Vf_t$ of dimension 48. Note that the simple module in V_t has dimension 6 and the socle series of V_t has dimensions $24, 48$. Applying Lemma 8, we proceed as follows.

(i) We compute all submodules of dimension 12 in $\mathrm{soc}\,(V_t)$.

(ii) For each submodule M in (i) we compute all simple submodules in V_t/M and take the pullback in V_t. This leads to a list, say $\mathcal{M}_1$, of submodules of dimension 18 in V_t.

(iii) We remove from $\mathcal{M}_1$ all submodules which are not good.

(iv) For all U in $\mathcal{M}_1$ we compute all simple submodules of V_t/U and take the pullback in V_t. This leads to a list $\mathcal{M}_2$ of submodules of dimension 24 in V_t.

(v) We remove from $\mathcal{M}_2$ all modules which are not good and obtain $\mathcal{L}_t$.

For 36#1 the list $\mathcal{M}_1$ is already empty which rules out this group. For 36#4 we obtain a non-empty list $\mathcal{L}_t$ and proceed as in Case 1 to rule out this group.

Case 3. Next we consider 36#3 and 36#5. Both groups have exactly three simple modules which are of dimension $1, 2$ and 6 respectively. Since 36#5 is 2-nilpotent, there are three blocks. But 36#3 is not 2-nilpotent and has two blocks. In this case the principal block contains the trivial module and the simple module of dimension 2. Thus both groups have a block which contains the simple module, say W, of dimension 6. If f is the corresponding block idempotent then $Vf = P_1 \perp P_2$ with $P_i \cong P(W)$, which has socle series

$$\begin{matrix} & W & \\ W & & W \\ & W & \end{matrix} .$$

We rule out both groups using the algorithm described in Case 1. To construct the list $\mathcal{L}$ of good codes in Vf, we distinguish two cases:

(α) good codes which contain $\mathrm{soc}\,(Vf)$;

(β) good codes which have a simple socle.

To find the good codes in (α) we apply the following result.

Lemma 9 *Let Cf be a good code in Vf with $\mathrm{soc}\,(Vf) \leq Cf$. Then $Cf \leq \mathrm{soc}_2(Vf)$.*

Proof. If $\mathrm{soc}\,(Vf) \leq Cf$ then $(w,0) \in Cf \leq Vf = P_1 \perp P_2$ for all $w \in \mathrm{soc}\,(P_1)$. Note that $(Cf)^\perp \cap Vf = Cf$ since Cf is good. Let $(x,y) \in Cf$. Thus

$$0 = ((w,0),(x,y)) = (w,x)$$

for all $w \in \mathrm{soc}\,(P_1)$. Since the restriction of $(\cdot\,,\cdot)$ to P_1 is non-degenerate, x must be an element of $\mathrm{soc}_2(P_1)$ since it is the only maximal submodule in P_1. By a symmetry argument, we see that $y \in \mathrm{soc}_2(P_2)$. Thus $(x,y) \in \mathrm{soc}_2(P_1) \perp \mathrm{soc}_2(P_2) = \mathrm{soc}_2(Vf)$. □

To construct the list of good codes in (α) we search, according to Lemma 9, for all submodules in $\mathrm{soc}_2(Vf)$ of dimension 12 and take their pullbacks in Vf. The resulting list $\mathcal{L}_\alpha$ contains only those pullbacks which are good. We combine the modules from $\mathcal{L}_\alpha$ with the good modules from the other blocks, and establish that all resulting codes have minimum distance strictly smaller than 16.

Lemma 10 *A good code in (β) is a projective indecomposable module.*

Proof. Let Cf be a code in the list (β). Since the socle of Cf is simple, Cf is a submodule of the projective cover P of $\mathrm{soc}\,(Cf)$. Since $\dim\, Cf = 24 = \dim\, P$, we deduce that $Cf = P$. □

To obtain the list of good codes in (β) we proceed as follows. First we search for all submodules of $Vf/\mathrm{soc}\,(Vf)$ of dimension 18 by taking maximal submodules of maximal submodules. By Lemma 10, we only consider those which have a 12-dimensional socle. In the next step we take the pullbacks in Vf of the remaining codes, which have dimension 30, and construct all their maximal submodules. Finally we test self-orthogonality and minimum distance at least 16. For both 36#3 and 36#5, the resulting list is empty.

Case 4. The remaining group G is 36#11 and is isomorphic to $\mathrm{A}_4 \times C_3$. There are 5 simple modules $1_G, W_1, W_2, W_3, W_4$ of dimension $1, 2, 2, 2, 2$ and two blocks. The principal block contains 1_G and say W_1. Furthermore,

$$KG = (P_0 \oplus P_1) \perp (P_2 \oplus P_3 \oplus P_4) = KGf_1 \perp KGf_2$$

with block idempotents $f_1 = 1 + y + y^2$ where $C_3 = \langle y \rangle$ and $f_2 = y + y^2$. Note that f_1 defines the principal block. The structures of the blocks are as follows:

$$KGf_1 = \begin{array}{c} 1 \\ W_1 \\ 1 \end{array} \oplus \begin{array}{ccc} & W_1 & \\ W_1 & 1 & 1 \\ & W_1 & \end{array}$$

$$KGf_2 = \begin{array}{ccc} & W_2 & \\ W_3 & & W_4 \\ & W_2 & \end{array} \oplus \begin{array}{ccc} & W_3 & \\ W_2 & & W_4 \\ & W_3 & \end{array} \oplus \begin{array}{ccc} & W_4 & \\ W_2 & & W_3 \\ & W_4 & \end{array}.$$

It is easy to determine that $\mathcal{L}_1$ contains exactly 192 good codes in Vf_1. However we are unable to determine the good codes in Vf_2 and hence we are not able to eliminate this case.

Acknowledgement: O'Brien was partially supported by the Marsden Fund of New Zealand via grant UOA721. Willems thanks the Department of Mathematics of the University at Auckland for its hospitality and the excellent working conditions while this work was completed. He is also grateful to the Alexander von Humboldt Stiftung for its generous support.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *J. Symbolic Comput.* **24**, 235–265, 1997.

[2] Hans Ulrich Besche, Bettina Eick, and E.A. O'Brien. A millennium project: constructing small groups, *Internat. J. Algebra Comput.*, **12**, 623–644, 2002.

[3] A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, and K.H. Zimmermann. Codierungstheorie – Konstruktion und Anwendung linearer Codes. Springer-Verlag, Berlin–Heidelberg–New York, 1998.

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

[5] S. Bouyuklieva. On the automorphism group of a doubly-even (72,36,16) code. *IEEE Trans. Inform. Theory* **50**, 544-547, 2004.

[6] S. Bouyuklieva, E.A. O'Brien and W. Willems. The automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code is solvable. *IEEE Trans. Inform. Theory* **52**, 4244-4248, 2006.

[7] J.H. Conway and V. Pless. On primes dividing the group order of a doubly-even (72,36,16) code and the group order of a quaternary (24,12,10) code. *Discrete Math.* **38**, 143-156, 1982.

[8] R. Dontcheva, A.J. van Zanten and S. Dodunekov. Binary self-dual-codes with automorphism of composite order. *IEEE Trans. Inform. Theory* **50**, 311-318, 2004.

[9] W. Feit. *The representation theory of finite groups.* North-Holland, Amsterdam/New York/Oxford 1982.

[10] W.C. Huffman and V. Yorgov. A [72,36,16] doubly-even code does not have an automorphism of order 11. *IEEE Trans. Inform. Theory* **33**, 749-752, 1987.

[11] B. Huppert and N. Blackburn. *Finite groups II.* Springer-Verlag, Berlin/Heidelberg/New York 1982.

[12] C. Martínez-Pérez and W. Willems. Self-dual codes and modules of finite groups in characteristic two. *IEEE Trans. Inform. Theory* **50(8)**, 1798-1803, 2004.

[13] V. Pless. 23 does not divide the order of the group of a (72,36,16) doubly-even code. *IEEE Trans. Inform. Theory* **28**, 113-117, 1982.

[14] V. Pless and J.G. Thompson. 17 does not divide the order of the group of a (72,36,16) doubly-even code. *IEEE Trans. Inform. Theory* **28**, 537-541, 1982.

[15] J. Rotman. *An Introduction to the Theory of Groups.* Springer-Verlag, 1994.

[16] N.J.A. Sloane. Is there a (72,36), $d = 16$ self-dual code? *IEEE Trans. Inform. Theory* **19**, 251, 1973.

[17] N.J.A. Sloane and J.G. Thompson. Cyclic self-dual codes. *IEEE Trans. Inform. Theory* **29**, 364-366 (1983).

[18] W. Willems. A note on self-dual group codes. *IEEE Trans. Inform. Theory* **48**, 3107-3109, 2002.

[19] V. Yorgov. On the automorphism group of a putative code. *IEEE Trans. Inform. Theory* **52**, 1724-1726 (2006).

Addresses:

E.A. O'Brien
Department of Mathematics
University of Auckland
Private Bag 92019
New Zealand
e-mail: obrien@math.auckland.ac.nz

Wolfgang Willems
Institut für Algebra und Geometrie
Otto-von-Guericke-Universität
Magdeburg
Germany
e-mail: willems@ovgu.de