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

I. Introduction

The existence of a binary self-dual doubly-even $[72, 36, 16]$ code remains a long-standing question, first posed by Sloane [17] in 1973. Determining the automorphism group of such a code may be a useful first step to construct it. In a series of papers [4], [5], [7], [10], [14], [15], [20], both its order and structure were investigated. The strongest result 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 paper, we exclude all groups of order $72, 56$ and all but one group of order 36, obtaining the following.

Theorem *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* $A_4 \times C_3$*.*

Critical to our proof is the observation that if a code C has a specific automorphism group G, then C is a submodule of the group algebra KG where K is the binary field. We use a variety of results, some new, from modular representation theory to deduce significant consequences for the structure of KG when C is a self-dual doubly-even $[72, 36, 16]$ code. We apply these results to devise a practical algorithm to decide if G is the automorphism group of C. Finally we use this algorithm to study KG computationally. If KG does not satisfy the requisite properties, then we conclude that G cannot be the automorphism group of the code; otherwise our algorithm constructs C. For groups of order 36 (with the noted exception), 56, and 72, this program was successful.

All computations 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].

II. Background and notation

Let K be the binary field $\mathbb{F}_2$ and let $KG = \{\sum_{g \in G} k_g g \mid k_g \in K\}$ denote the group algebra of a finite (multiplicative written) group G over K. The multiplication in the algebra KG is given by the multiplication in the group G extended linearly.

If H is a subgroup of G, then we may write $G = \cup_{i=1}^{s} Hg_i$ where $\{g_1, \ldots, g_s\}$ is a set of transversals from H in G. Let K_H^G denote the K-vector space generated by $\{Hg_1, \ldots, Hg_s\}$, hence $K_H^G = \oplus_{i=1}^{s} KHg_i$. For an arbitrary $g \in G$ we have $Hg_i g = Hg_j$ where $1 \leq j \leq s$ depending on i. Thus K_H^G is a KG-module

via this action and is the permutation module corresponding to the permutation action of G on the cosets Hg_i. In particular, $KG = K_H^G$ for $H = \langle 1 \rangle$.

If we consider K_H^G as the ambient space of a code then $Hg_1, \ldots, Hg_s$ are used as the fixed basis. The natural non-degenerate bilinear form on K_H^G which defines the concept of duality for codes is given by

$$(Hg_i, Hg_j) = \delta_{ij}. \tag{1}$$

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

$$(Hg_ix, Hg_jx) = (Hg_i, Hg_j)$$

for all $x \in G$ and $i, j = 1, \ldots, s$. In particular, for the group algebra $KG = K_1^G$ the bilinear form is given by

$$(g, h) = \delta_{gh}. \tag{2}$$

Let C be 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 $i_1, \ldots, i_s$ are representatives of the orbits of G on $\Omega = \{1, \ldots, n\}$ and if G_i denotes the stabilizer of $i \in \Omega$ in G, then

$$V = K^n = K_{G_{i_1}}^G \perp \ldots \perp K_{G_{i_s}}^G. \tag{3}$$

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

III. Preliminaries

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

Lemma 1: If $V = K^n = KG$ and $C = C^\perp$ is doubly-even then the Sylow 2-subgroup of G is not cyclic.

Proof: See the main result of [18], or [12, Theorem 4.4]. ■

Lemma 2 requires some facts from representation theory which we now recall. If V is a KG-module then $V^* = \mathrm{Hom}_K(V, K)$ becomes a KG-module via

$$v(fg) = (vg^{-1})f$$

where $v \in V, f \in V^*$ and $g \in G$. The module V^* is the *dual module* of V. If V^* is isomorphic to V as a KG-module then V is *self-dual* (as a module). Recall that the trivial KG-module is K on which all elements of G act as the identity; it is self-dual. The regular KG-module $V = KG$ is also self-dual since $\alpha : KG \to KG^*$ defined by

$$x(y\alpha) = (x, y)$$

for $x, y \in KG$ and $(\cdot\,,\cdot)$ as in (2) is an isomorphism. It is well know that

$$KG = P_1 \oplus \ldots \oplus P_m$$

with indecomposable modules P_i. By the Krull-Schmidt Theorem [9, Chap. I, Theorem 11.4], this decomposition is unique up to isomorphism. Each summand P_i is a *projective indecomposable module* for KG. Since the P_i are direct summands of KG, a free module, they have a particular structure which we now describe.

Lemma 2: Let P be an indecomposable direct summand of KG.

a) P has a largest completely reducible submodule, namely its socle $S := \mathrm{soc}\,(P)$, and S is irreducible.
b) P has a unique maximal submodule $\mathrm{J}(P)$ and $P/\mathrm{J}(P) \cong S$.
c) The isomorphism type of P is uniquely determined by the isomorphism type of S. (We call P the *projective cover* of S and write $P = P(S)$.)
d) Let Q be a direct sum of projective indecomposable modules; i.e. an arbitrary

projective module. If Q is a submodule or a factor module of some module W then Q is (up to isomorphism) a direct summand of W.

Its proof can be found in [11, Chap. VII, §10–11].

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

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

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. Obviously,

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

and $\text{soc}\,(P_i) = S_i$ for pairwise non-isomorphic irreducible modules S_i, by Lemma 2 c). Suppose that, for some i, $\text{soc}\,(P_i) \not\subseteq \text{soc}\,(C)$. Since the socle of P is irreducible, $C \cap P_i = 0$. If we define $\alpha : V \to C^*$ by $c(v\alpha) = b(v, c)$ for $v \in V$ and $c \in C$ then we easily see that

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

since Ker $\alpha = C^\perp = C$ (see [19, Proposition 2.3]). Thus P_i is (up to isomorphism) a submodule of C^*. It follows that P_i^* is a factor module of $(C^*)^* \cong C$. Hence P_i is (up to isomorphism) a factor module of C since $P_i^* \cong P_i$. Thus there is a chain

$$0 \leq X \leq Y \leq C \leq Z \leq U \leq V$$

of KG-modules with

$$Y/X \cong U/Z \cong P_i.$$

Applying Lemma 2 d), the projective indecomposable module P_i has multiplicity at least two in $V = KG$, contradicting the assumption of the lemma. ∎

In order to carry out computations successfully, we need a finer splitting of the ambient space V as given in (3). Note that KG is both a left and a right KG-module. Thus we may write

$$KG = B_1 \oplus \ldots \oplus B_s \tag{4}$$

with two-sided ideals B_i. If we write

$$1 = f_1 + \ldots + f_s \tag{5}$$

with $f_i \in B_i$, then the f_i are in the center of the algebra KG and $f_i f_j = \delta_{i,j} f_i$. Moreover $B_i = f_i KG = KGf_i$. We say that (5) is a decomposition of 1 into *central orthogonal idempotents*. If B_i cannot be split into a non-trivial direct sum of two-sided ideals then we call B_i a *block* and f_i a *block idempotent*. The block idempotent f_i is uniquely determined by the block B_i.

To obtain an orthogonal decomposition in (4) with respect to the bilinear form on KG defined in (2), we need a particular property of the idempotents f_i. Let $\hat{}: KG \to KG$ denote the antialgebra automorphism of KG defined by $g \to g^{-1}$ for $g \in G$. Suppose that all f_i in (5) satisfy $\hat{f}_i = f_i$. Then

$$KG = B_1 \perp \ldots \perp B_s. \tag{6}$$

For, if $x, y \in KG$ and $i \neq j$, then

$$\begin{aligned}(B_i, B_j) = (xf_i, yf_j) = (f_i x \hat{f}_j, y) = \\ (f_i x f_j, y) = (f_i f_j x, y) = (0, y) = 0.\end{aligned} \tag{7}$$

Moreover, the restriction of $(\cdot\,,\cdot)$ on B_i is non-degenerate, or in other words $B_i \cong B_i^*$ as a right KG-module. Finally, we put $V_i = Vf_i$ and $C_i = Cf_i \subseteq V_i$ for $i = 1, \ldots, t$. Note that V_i and C_i are KG-modules since the f_i are in the center of KG.

Lemma 4: Consider an arbitrary V as in (3).

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]). The proof that the decompositions are orthogonal is as in (7). For, 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,

$$(V_i, V_j) = (Vf_i, Vf_j) = (V, Vf_j\hat{f}_i) = (V, Vf_jf_i) = 0$$

for $i \neq j$. This proves that the decompositions of V and C are orthogonal.
b) Since $C = C^{\perp}$ in V and $C_i \subseteq V_i$, it follows that $C_i = C_i^{\perp}$ in the space V_i. ■

The basic algorithm
Let C be 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

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

Finding such decompositions is easy since the groups we consider are solvable and small. For instance, if H is a normal subgroup of G of odd order then we may take $f_1 = \sum_{h \in H} h$ and $f_2 = 1 - f_1$.

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 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.

IV. Excluding $|G| = 72$

Throughout this section we assume that $|G| = 72$. Since elements of order 2 and 3 in G act fixed-point-freely on the 72 coordinate positions (see [4, Theorem 5.3] and [5, Theorem 1.1]), the action of G on the positions is regular: namely, G has just one orbit on the 72 positions. 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 1, we may assume that the Sylow 2-subgroup of G is not cyclic. Among the remaining 43 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 the quaternion group of order 8, D_8 the 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 conjugation action of D_8 on H has three orbits: namely 1, the orbit x, x^2, y, y^2, and the orbit xy, x^2y, xy^2, x^2y^2. We put $f_1 = \sum_{h \in H} h$, $f_2 = x + x^2 + y + y^2$ and $f_3 = xy + x^2y + xy^2 + x^2y^2$. One easily checks that the f_i are central orthogonal idempotents in KG and $1 = f_1 + f_2 + f_3$. Furthermore, $f_i = \hat{f}_i$ for $i = 1, 2, 3$. Finally, $\dim KGf_1 = 8$ 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 all $4 \times 90 \times 90$ 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. 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 the involution t inverts all elements of order 3 and the Sylow 2-subgroup of G 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) let $T = \{1, t_2, t_2^{-1}, \ldots, t_5, t_5^{-1}\}$ be a Sylow 3-subgroup of G. If we put $f_1 = \sum_{t \in T} t$ and $f_i = t_i + t_i^{-1}$ for $i = 2, \ldots, 5$ then

$$1 = f_1 + \ldots + f_5$$

is a decomposition of 1 into central pairwise orthogonal idempotents. Since the f_i are also block idempotents and $f_i = \hat{f}_i$, we may apply the algorithm.

In Step 1 we get 6 good codes in the block 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).

Next let $G = C_3 \times C_2 \times \mathrm{A}_4$ and let x be a generator of the normal subgroup of order 3. We put $f_1 = 1 + x + x^2$ and $f_2 = 1 - f_1$. Clearly, f_1 and f_2 are central orthogonal idempotents with $1 = f_1 + f_2$. Since the f_i are again block idempotents and $f_i = \hat{f}_i$, we proceed as above. One computes that $\dim KGf_1 = 24$, so $\dim KGf_2 = 48$. The block KGf_2 contains exactly three irreducible modules, all of dimension 2. Lemma 3 implies that $\mathrm{soc}\,(Cf_2) = \mathrm{soc}\,(KGf_2)$. We now compute 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 the KG-submodule Cf_2 of 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 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 $|G| = 72$.

V. Excluding $|G| = 56$

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

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

Proof: Observe that [6, Lemma 2] implies $|N_G(T)| = 7$ or 14. Since $|G : N_G(T)| \equiv 1 \bmod 7$ 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, Theorem 5.3], an involution has no fixed points, and by [8, proof of Proposition 4.1], an element of order 7 has exactly two fixed points. Thus the Cauchy-Frobenius Lemma [16, Theorem 3.22] 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 the group $56\#11$.

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

b) $P_1 \cong P_2$ is the projective cover $P(K)$ of the trivial module K.

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

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

Proof: a) This follows immediately by Lemma 5.

b) It is easy to see that P_i is isomorphic to the KG-module eKG where $e = \frac{1}{|T|}\sum_{t \in T} t$. Since $e^2 = e$ we get $KG = eKG \oplus (1-e)KG$. Thus P_i is a direct summand of KG. Since $\dim P_i = 8$, and a result of Dickson (see [11, Corollary 7.16]) implies that $8 \mid \dim P_i$, we deduce that P_i must be indecomposable. Since P_i is a permutation module, it contains the trivial module as a submodule. Thus, by Lemma 2, the socle of P_i must be the trivial module.

c) Note that $P_1 \oplus P_2$ has non-zero entries in at most 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

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

Since $P_i^* \cong P_i$ it follows that

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

is a submodule of $C^{**} \cong C$. Since a projective submodule or factor module is always a direct summand (see Lemma 2 d)), the module $P_1 \cong P_2$ occurs (up to isomorphism) in a direct decomposition of $V = K^{72}$ into indecomposable modules with multiplicity at least 4. This contradicts the fact that V contains the projective cover of the trivial module exactly three times since KG contains it only once.

d) 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 $\dim C = 36$. ■

Recall that for a KG-module V the socle $\mathrm{soc}(V) := \mathrm{soc}_1(V)$ is defined as the largest completely reducible submodule of V. Inductively, we define the k-th socle $\mathrm{soc}_k(V)$ of V by

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

We call $\mathrm{soc}_1(V) \subseteq \mathrm{soc}_2(V) \subseteq \ldots$ the *socle series* of V.

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

a) There are (up to isomorphism) exactly three irreducible modules: the trivial module K and two modules V resp. V^* with $V \ncong V^*$, both of dimension 3.
b) The projective cover $P(K)$ of the trivial module K has exactly 4 submodules different from 0, namely $K \subset V_1 \subset V_2 \subset P(K)$ with $V_1/K \cong V$, $V_2/V_1 \cong V^*$ and $P(K)/V_2 \cong K$.
c) Let $P(V)$ and $P(V^*)$ denote the projective covers of V resp. V^*. Then $\operatorname{soc}_3(P(V)) \neq P(V)$, but $\operatorname{soc}_4(V) = P(V)$. The same holds for V^*.
d) $C_0 \leq \operatorname{soc}_3(KG)$.

Proof: a) Over the field $\mathbb{F}_8$, the group G has exactly 7 irreducible modules since the normal Sylow 2-subgroup H is in the kernel of every irreducible module. Over the binary field K we have only three irreducible modules, the trivial one K and two modules V and $V^* \ncong V$ of dimension 3. The latter are direct sums of 3 Galois conjugate modules over $\mathbb{F}_8$ of dimension 1.

b) By the proof of Lemma 6 we know that $P(K) \cong eKG = eKH$ where $e = \frac{1}{|T|}\sum_{t\in T} t$. Thus, $P(K)$ is the regular module KH on which T acts by conjugation. This proves already that the module $P(K)$ has exactly 4 submodules different from 0, namely

$$eJ^3 \subset eJ^2 \subset eJ \subset eKH$$

where $J = \{a \mid a \in KH,\ a \text{ has even weight}\}$ is the unique maximal ideal in KH. Observe that the factor modules J^i/J^{i+1} are irreducible and J/J^3 is not completely irreducible. Since $P(K) \cong P(K)^*$ the assertion now follows.

c) This is a consequence of the fact that $P(V) \cong P(K) \otimes V$ resp. $P(V^*) \cong P(K) \otimes V^*$.

d) Note that $KG = P(K) \oplus P(V) \oplus P(V^*)$. Since the weights of the code words in C_0 are divisible by 2, the subcode C_0 is contained in the unique maximal ideal M of KG with $KG/M \cong K$. Thus, if $C_0 \not\subseteq \operatorname{soc}_3(KG)$ 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.

VI. Excluding $|G| = 36$

Throughout this section we assume that $|G| = 36$. Since neither involutions nor elements of order 3 have fixed points by [4, Theorem 5.3] and [5, Theorem 1.1], the action of G on the 72 coordinate positions is fixed-point-free. Thus the ambient space K^{72} is an orthogonal sum of two copies of the regular module KG:

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

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. For each group G, we deduce, using Schur's algorithm [13] as implemented in MAGMA, that all of its irreducible representations, and hence all of its projective indecomposable 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 $f_i = \hat{f}_i \in KG$. Recall that G is 2-*nilpotent* if it has a normal subgroup N where $2 \nmid |N|$ and G/N is a 2-group. If G is 2-nilpotent, then each block contains (up to isomorphism) exactly one irreducible 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 $U_i \in \mathcal{L}_i$.

#	Group	Dimensions of irreducible modules	$\dim Vf_i$	$\dim \operatorname{soc}_k(Vf_t)$
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 I
DATA FOR CERTAIN GROUPS OF ORDER 36

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 $s < t$ 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 I, for each group 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.

To prove Lemma 9 we need Lemma 8 which easily follows from the fact that projective KG-modules are injective (see [11, Chap. VII, Theorem 7.8]).

Lemma 8: Let W be a KG-module and let P be a projective KG-module with $\operatorname{soc}(P) \cong \operatorname{soc}(W)$. Then W is (up to isomorphism) a submodule of P.

Lemma 9: Let $f = \hat{f}$ be a central idempotent of KG and suppose that KGf contains only one irreducible module (up to isomorphism) as composition factor. Then

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

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

$$\begin{aligned} &Cf \leq P_1 \oplus \ldots \oplus P_{m'} \leq \\ &P_1 \oplus \ldots \oplus P_{m'} \oplus \ldots \oplus P_{2m} = Vf \end{aligned} \tag{8}$$

where all P_i are isomorphic to a projective indecomposable module P with socle isomorphic to S. To see this, note that

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

follows directly from Lemma 8. Furthermore Vf is projective and contains only S as a composition factor. Thus Vf is a direct sum of projective indecomposable modules isomorphic to P and W is (up to isomorphism) a submodule and hence a direct summand of Vf, which proves (8). Finally 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. ■

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 irreducible module in V_t has dimension 6 and the socle series of V_t has dimensions $24, 48$. Applying Lemma 9, 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 irreducible submodules S in V_t/M and take the *pullback* of S in V_t: namely, $\{v \mid v \in V_t,\ v+M \in S\}$. 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 irreducible submodules of V_t/U and take their pullbacks 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 irreducible modules which have 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 irreducible module of dimension 2. Thus both groups have a block which contains the irreducible 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

$$\begin{array}{ccc} & W & \\ W & & W \\ & W & \end{array}.$$

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 an irreducible socle.

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

Lemma 10: Let Cf be a good code in Vf with $\mathrm{soc}\,(Vf) \subseteq Cf$. Then $Cf \subseteq \mathrm{soc}_2(Vf)$.

Proof: If $\mathrm{soc}\,(Vf) \subseteq Cf$ then $(w,0) \in Cf \subseteq Vf = P_1 \perp P_2$ 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 10, for all submodules, say X, in $\mathrm{soc}_2(Vf)$ of dimension 12 and take their pullbacks in Vf, i.e.

$$\{v \mid v \in Vf_t,\, v + \mathrm{soc}_2(V_t) \in X\}.$$

The resulting list $\mathcal{L}_\alpha$ contains only those modules 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 11: A good code in (β) is a projective indecomposable module.

Proof: Let Cf be a code in (β). Since the socle of Cf is irreducible, Cf is a submodule of the projective cover P of $\mathrm{soc}\,(Cf)$, by Lemma 8. Since $\dim Cf = 24 = \dim P$, we deduce that $Cf = P$. ■

To construct 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 11, 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 irre-

ducible modules K, W_1, W_2, W_3, W_4 of dimension $1, 2, 2, 2, 2$ and two blocks. The principal block contains K and say W_1. Furthermore, if $P_0 = P(K)$ and $P_i = P(W_i)$

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

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 socle series of the blocks are as follows:

$$KGf_1 = \begin{matrix} & 1 & \\ W_1 & & W_1 \\ & 1 & \end{matrix} \oplus \begin{matrix} & W_1 & \\ 1 & & 1 \\ & W_1 & \end{matrix}$$

$$KGf_2 = \begin{matrix} & W_2 & \\ W_3 & & W_4 \\ & W_2 & \end{matrix} \oplus \begin{matrix} & W_3 & \\ W_2 & & W_4 \\ & W_3 & \end{matrix} \oplus \begin{matrix} & W_4 & \\ W_2 & & W_3 \\ & W_4 & \end{matrix}$$

It is easy to determine that $\mathcal{L}_1$ contains exactly 192 good codes in Vf_1. However we were unable, using existing resources, 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. Finally, we thank the referees and editor for many suggestions which improved the paper substantially.

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] W. PLESKEN. Presentations and representations of groups. Algorithmic algebra and number theory (Heidelberg, 1997), 423–434, Springer, Berlin, 1999.

[14] 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.

[15] 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.

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

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

[18] N.J.A. SLOANE AND J.G. THOMPSON. Cyclic self-dual codes. *IEEE Trans. Inform. Theory* **29**, 364–366, 1983.

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

[20] V. YORGOV. On the automorphism group of a putative code. *IEEE Trans. Inform. Theory* **52**, 1724–1726, 2006.

E.A. O'Brien E.A. O'Brien received a BSc in 1983 from the National University of Ireland (Galway) and a PhD from the Australian National University in 1988. He was an Assistant Professor at Marquette University, Milwaukee, from 1988-1990, a Research Fellow in Canberra from 1990-1995, a Humboldt Research Fellow at RWTH Aachen from 1995-1997, and since 1997 is a member of the Department of Mathematics at the University of Auckland. His primary research interests are algorithmic and computational aspects of group theory.

Wolfgang Willems Wolfgang Willems (M'00) received the Diploma in 1974 and the PhD degree in 1977, both in mathematics, and from the Johannes-Gutenberg University, Mainz, Germany. From 1974 to 1998, he was mainly with the Department of Mathematics, the University of Mainz. He spent 1986-1987 and 1989-1991 as Visiting Professor at the University of Essen, Germany and the Institute of Experimental Mathematics, Essen. In 1996 he was Acting Professor at the Otto-von-Guericke University, Magdeburg, Germany. Since 1998, he has been Professor for Pure Mathematics at the University of Magdeburg. His primary research interests are algebraic coding theory and representation theory of finite groups.