The automorphism group of a binary self-dual doubly-even [72,36,16] code is solvable

Stefka Bouyuklieva, E.A. O'Brien and Wolfgang Willems

Abstract

We prove that the automorphism group of a putative binary self-dual doubly-even [72,36,16] code is solvable. Moreover, its order is 5, 7, 10, 14, 56, or a divisor of 72.

1 Introduction

An $[n, k]$ linear code C over the binary field $\mathbb{F}_2$ is a k-dimensional subspace of $\mathbb{F}_2^n$. The Hamming weight of a vector in $\mathbb{F}_2^n$ is defined by the number of its nonzero coordinates. We call C an $[n, k, d]$ code if d is the minimum among the weights of nonzero codewords in C. The inner product of vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ in $\mathbb{F}_2^n$ is given by

$$\langle u, v\rangle = u_1v_1 + u_2v_2 + \cdots + u_nv_n.$$

As usual we denote by

$$C^{\perp} = \{v \in \mathbb{F}_2^n \mid \langle u, v\rangle = 0 \text{ for all } u \in C\}$$

the dual code of C. If $C \subseteq C^{\perp}$ then C is called self-orthogonal; if $C = C^{\perp}$ then C is called self-dual. A binary code is doubly-even if the weight of every codeword is divisible by four. Self-dual doubly-even codes exist only if n is a multiple of eight (see for instance [16]). Rains [21] proved that the minimum distance d of a binary self-dual $[n, k, d]$ code satisfies the following bound:

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

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

Codes achieving this bound are called extremal. If n is a multiple of 24, then a self-dual code meeting the bound must be doubly-even [21]. Moreover, for any nonzero weight w in such a code, the codewords of weight w form a 5-design [2].

Thus extremal self-dual codes of length a multiple of 24 are of particular interest. The extended Golay code g_{24} is the only [24,12,8] code (see for instance [18]) and the extended quadratic residue code q_{48} is the only [48,24,12] self-dual doubly-even code [12]. In 1973 Sloane [23] posed a question which remains unresolved: is there a self-dual doubly-even $[72, 36, 16]$ code? In a one-page paper he lists its complete and unique weight distribution.

Recall that $\sigma \in S_n$ is an automorphism of a binary linear code C if $C = \sigma(C)$. The set of all automorphisms of C form its automorphism group $Aut(C)$. Of course, knowledge of the existence of a non-trivial automorphism group is very useful in constructing a code.

The automorphism group of the extended Golay code is the 5-transitive Mathieu group M_{24} of order $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ (see [3]). The automorphism group of q_{48} is only 2-transitive. It is isomorphic to the projective special linear group $\mathrm{PSL}(2, 47)$ and has order $2^4 \cdot 3 \cdot 23 \cdot 47$ (see [5], [15]). Both M_{24} and $\mathrm{PSL}(2, 47)$ are nonabelian simple groups, and so in particular are not solvable.

What can we say about the automorphism group of a putative self-dual doubly-even [72,36,16] code C? Primes larger than 7 cannot divide its order (see [10], [13], [19], [20]). Permutations of odd composite orders except 9 cannot be automorphisms of such a code (see [11] and [25]). If $\sigma \in Aut(C)$ has order 5 or 7, then σ fixes two coordinates [11]; if σ has order 2 or 3, then it is a fixed-point-free permutation (see [7] and [8]).

Recently Yorgov [25, Theorem 3] stated that there are at most 22 possibilities for the order of the automorphism group of such a code, namely

$$(*) \qquad 504, 360, 252, 180, 60, 56, 14, 10, 7, 5, \text{ or a divisor of } 72.$$

A careful reading of his proof shows that even more is true: *every subgroup* of the automorphism group has an order listed in $(*)$. We will prove that an automorphism group of order 60, 180, 252, 360 or 504 must be simple. However, simple groups of order 180 and 252 do not exist. Hence a simple automorphism group is isomorphic to $\mathrm{SL}(2, 8)$ of order 504, or to the alternating groups, A_6 and A_5, of order 360 and 60, respectively. We employ techniques from representation theory to exclude these three groups.

In summary, our main result is the following.

Theorem 1 *The automorphism group of a binary self-dual doubly-even* $[72, 36, 16]$ *code is a solvable group of order* $5, 7, 10, 14, 56$*, or a divisor of* 72*.*

2 The structure of the automorphism group

Let G denote the automorphism group of a self-dual doubly-even $[72, 36, 16]$ code C. Recall that the normalizer of $H \leq G$ is defined by

$$N_G(H) = \{\sigma \in G \mid \sigma H \sigma^{-1} = H\}.$$

Let $\tau \in G$; we denote its order by $|\tau|$ and write $N_G(\tau)$ for $N_G(\langle\tau\rangle)$. In [25] Yorgov proved the following lemma about the normalizers of particular elements.

Lemma 2 *Let $\tau \in G$.*

a) If $|\tau| = 5$ then 3, 4 and 7 do not divide $|N_G(\tau)|$.

b) If $|\tau| = 7$ then 3, 4 and 5 do not divide $|N_G(\tau)|$.

c) If $|\tau| = 3$ then 5 and 7 do not divide $|N_G(\tau)|$.

We use this result and Sylow's Theorem [22] to deduce additional properties of G. Recall that if $|G| = p^s m$ where p is a prime and p does not divide m, then the Sylow p-subgroups of G have order p^s. For a fixed p, let n_p denote the number of these subgroups. Then n_p divides m, $n_p \equiv 1 \pmod{p}$, and all Sylow p-subgroups of G are conjugate in G.

Lemma 3 *If $H \leq G$ and $|H| = 9$, then 5 and 7 do not divide $|N_G(H)|$.*

Proof. Let $\tau \in N_G(H)$ be of order 5.

If $H = \langle\sigma\rangle$ is cyclic of order 9, then $\langle\sigma^3\rangle$ is the unique subgroup of H of order 3. Hence $\tau \in N_G(\sigma^3)$ and 5 divides $|N_G(\sigma^3)|$ which contradicts Lemma 2c).

If H is elementary abelian of order 9, then H has four subgroups of order 3 which we denote by $A_i, 1 \leq i \leq 4$. Now τ acts to permute these. Since the length of each orbit divides 5, $\tau \in N_G(A_i)$ for all i, a contradiction to Lemma 2c).

Hence $|N_G(H)|$ is not divisible by 5. The proof that 7 does not divide $|N_G(H)|$ is similar. □

Corollary 4 *Let $p = 5$ or $p = 7$.*

a) If $|G| = p \cdot 3^\alpha \cdot 2^\beta$, then $n_p = 3^\alpha \cdot 2^\beta$ or $3^\alpha \cdot 2^{\beta-1}$.

b) If $|G| = p \cdot 3^\alpha \cdot 2^\beta$ where $\alpha = 1$ or $\alpha = 2$, then $n_3 = p \cdot 2^x$ for some integer $x \leq \beta$. Moreover x must be even if $p = 7$ and odd if $p = 5$.

Proof. a) Let $\tau \in G$ have order p. Since the Sylow p-subgroups are conjugate,

$$\frac{|G|}{n_p} = |N_G(\tau)| = p \cdot 3^{\alpha-x} \cdot 2^{\beta-y}$$

with $0 \leq x \leq \alpha$ and $0 \leq y \leq \beta$. Lemma 2 implies that $x = \alpha$ and $y = \beta$ or $y = \beta - 1$ which proves the assertion.
b) Let H be a Sylow 3-subgroup of G. Since all Sylow 3-subgroups are conjugate,

$$|N_G(H)| = \frac{|G|}{n_3} = p^{1-y} \cdot 2^{\beta-x} \cdot 3^{\alpha}$$

with $0 \leq y \leq 1$ and $0 \leq x \leq \beta$. Applying Lemma 2c) or Lemma 3 for $\alpha = 1$ or 2 respectively, we obtain $y = 1$, hence $n_3 = p \cdot 2^x$. Moreover $n_3 \equiv 1 \pmod 3$ by Sylow's Theorem. On the other hand, $7 \cdot 2^x \equiv (-1)^x \pmod 3$ and $5 \cdot 2^x \equiv -(-1)^x \pmod 3$. Thus x must be even if $p = 7$, and x is odd if $p = 5$. □

Proposition 5 *There is no binary self-dual doubly-even* $[72, 36, 16]$ *code with automorphism group of order* 252 *or* 180.

Proof. Let $|G| = 36p$ where $p = 5$ or 7. Corollary 4a) implies that $n_7 = 36$ or 18. Since $n_7 \equiv 1 \pmod 7$ we get $n_7 = 36$. Similarly, if $p = 5$ then $n_5 = 36$. Corollary 4b) implies $n_3 = 7$ or 28 for $p = 7$, and $n_3 = 10$ for $p = 5$.

Now let H be a nontrivial proper normal subgroup of G. Since $|G| = 36p$,

$$|H| \in \{36, 18, 12, 9, 6, 4, 3, 2, 18p, 12p, 9p, 6p, 4p, 3p, 2p, p\}.$$

First suppose that p divides $|H|$. Thus all Sylow p-subgroups of G are subgroups of H and so

$$n_p \mid 18, 12, 9, 6, 4, 3, 2 \text{ or } 1,$$

a contradiction.

If $|H| = 36, 18$ or 9 then H contains all Sylow 3-subgroups of G, and so

$$n_3 \mid 4, 2 \text{ or } 1,$$

again a contradiction.

Thus the remaining possibilities for $|H|$ are $12, 6, 4, 3, 2$. If $|H| = 12$ then H is a maximal normal subgroup of G. Therefore G/H is simple, a contradiction, since there are no simple groups of order $3p$. Since there are no simple groups of orders $6p, 9p$ and $18p$ we obtain $|H| \neq 6, 4$ or 2. Thus we are left with $|H| = 3$. In this case p divides the order of $G = N_G(H)$ contradicting Lemma 2c). Hence G has no nontrivial proper normal subgroup. This completes the argument since there are no simple groups of order 252 or 180. □

Proposition 6 *If* $|G|$ *is* $504, 360$ *or* 60*, then* G *is one of the simple groups* $\mathrm{SL}(2,8), \mathrm{A}_6$ *or* A_5.

Proof. We use Sylow's Theorem and Corollary 4 to count the number of Sylow subgroups in the three cases:

- $|G| = 504 \Rightarrow n_7 = 36$, $n_3 = 7$ or 28.
- $|G| = 360 \Rightarrow n_5 = 36$, $n_3 = 10$ or 40.
- $|G| = 60 \Rightarrow n_5 = 6$, $n_3 = 10$.

Let H be a maximal normal subgroup of G and let τ_p denote an element of prime order p in G. We consider the possible orders of H and prove that H is trivial.

Case 1: 7 divides $|H|$ or 5 divides $|H|$.
If $7 \mid |H|$ then $|G| = 504$ and

$$36 = n_7 = |G : N_G(\tau_7)| = |H : N_H(\tau_7)|.$$

Thus $36 \mid |H|$ and so $|H| = 7 \cdot 36 = 252$. But Proposition 5 implies that a group of order 252 can not occur as an automorphism group of C, a contradiction.

If $5 \mid |H|$ then $|G| = 360$ or 60. In the first case

$$36 = n_5 = |G : N_G(\tau_5)| = |H : N_H(\tau_5)|.$$

Again $36 \mid |H|$ and therefore $|H| = 5 \cdot 36 = 180$ which contradicts Proposition 5 as above. If $|G| = 60$ then

$$6 = n_5 = |G : N_G(\tau_5)| = |H : N_H(\tau_5)|.$$

Thus $|H| = 30$ and H contains τ_3. Moreover,

$$10 = n_3 = |G : N_G(\tau_3)| = |H : N_H(\tau_3)|.$$

Hence H, a subgroup of order 30, contains 24 elements of order 5 and 20 elements of order 3, a contradiction.

Case 2: $9 \mid |H|$.
Now $n_3 = |G : N_G(T_9)| = |H : N_H(T_9)|$ where T_9 is a Sylow subgroup of order 9 contained in H. If $|G| = 504$, then $7 \mid n_3$ and so 7 divides $|H|$. If $|G| = 360$ or 60, then $5 \mid n_3$ and so $5 \mid |H|$. Each possibility is eliminated by Case 1.

Case 3: $3 \mid |H|$, but $9 \nmid |H|$.
Case 1 implies that $|H|$ is not divisible by 5 and 7. Thus $|H| = 3, 6, 12$ or 24. Since $|G| = 504$ and G/H is simple, the only possibility is that $|G/H| = 168$. Thus $|H| = 3$ and $G/H = \mathrm{PSL}(2,7)$. In particular, a 7-element must act trivially on a 3-element,

contradicting Lemma 2c). If $|G| = 360$ the same argument forces $|G/H| = 60$. Thus $|H| = 6$ and $G/H = \mathrm{A}_5$. Since a 5-element centralizes a 3-element, this again contradicts Lemma 2c). Finally, if $|G| = 60$ then $|G/H| = 5$ and $|H| = 12$. Again a 5-element centralizes a 3-element, otherwise H contains at least 10 elements of order 3, a contradiction since $|H| = 12$. Thus $5 \mid |N_G(\tau_3)|$, contradicting Lemma 2c).

Case 4: $|H| = 2, 4$ or 8.
Then G/H has order $252, 180, 30, 126, 90, 15, 63, 45$. But no simple group of any such order exists.

Thus we have proved that G is a simple group of order $504, 360$ or 60. □

In summary, we conclude that the automorphism group of a binary self-dual doubly-even code is solvable of order $5, 7, 10, 14, 56$ or a divisor of 72, or is one of three simple groups $\mathrm{SL}(2,8), \mathrm{A}_6, \mathrm{A}_5$.

3 The module structure of the code

Let C be a binary self-dual doubly-even $[72, 36, 16]$ code with *simple* automorphism group G. We now employ some ideas from modular representation theory, in particular block theory, to eliminate the possible groups. The necessary background information can be found in [14] or [17].

Lemma 7 *G acts transitively on the positions of C if G is $\mathrm{SL}(2,8)$ or A_6, but induces two orbits of lengths 60 and 12 if G is A_5.*

Proof. Clearly, G acts on the 72 positions of C. To compute the number $t(G)$ of orbits, we use the Cauchy-Frobenius Lemma [22] which says that

$$t(G) = \frac{1}{|G|} \sum_{g \in G} Fix(g)$$

where $Fix(g)$ is the number of the fixed points of g. By [7] and [8], permutations of order a power of 2 or 3 do not have fixed points. Elements of order 5 or 7 have exactly 2 fixed points by [11]. Since $\mathrm{SL}(2,8)$ has $n_7 = 36$ Sylow 7-subgroups (as already seen in the proof of Proposition 6), it has exactly $6 \cdot 36$ elements of order 7. Since $\mathrm{SL}(2,8)$ has only 2-, 3- and 7-elements it follows that

$$t(\mathrm{SL}(2,8)) = \frac{1}{504}(72 + 2 \cdot 6 \cdot 36) = 1.$$

Similarly,

$$t(\mathrm{A}_6) = \frac{1}{360}(72 + 2 \cdot 4 \cdot 36) = 1$$

and

$$t(\mathrm{A}_5) = \frac{1}{60}(72 + 2 \cdot 4 \cdot 6) = 2.$$

For the last case let $m_1 \geq m_2$ be the lengths of the two orbits. Then both m_1 and m_2 must divide 60 and $m_1 + m_2 = 72$. The only solution is $m_1 = 60$ and $m_2 = 12$. $\square$

3.1 The A_5 case

We now consider the case where $G = \mathrm{A}_5$ in more detail.

Proposition 8 *If $G = \mathrm{A}_5$ then C contains a self-orthogonal doubly-even* $[60, 24, 16]$ *subcode, say B, which is invariant under the action of G. Moreover, the action of G on the coordinates of B is transitive.*

Proof. Without loss of generality, we may assume that the two orbits are $\{1, 2, \dots, 60\}$ and $\{61, 62, \dots, 72\}$. Let B be the largest subcode of C whose support is contained entirely in the first 60 coordinates. Obviously, B is doubly-even as a subcode of C. Hence B is a doubly-even $[60, k_B, \geq 16]$ code. If G_B denotes a generator matrix of B, then a generator matrix of C has the form

$$G_C = \begin{bmatrix} G_B & O \\ E & G_D \end{bmatrix}$$

where O is a $k_B \times 12$ zero matrix. Let D be the code generated by the matrix G_D. If $w \in \mathbb{F}_2^{12}$ and $w \perp D$ then $v = (0, 0, \dots, 0, w) \in \mathbb{F}_2^{72}$ is orthogonal to all codewords of C and therefore $v \in C^\perp = C$. But the weight of v is at most 12, hence v must be the zero vector. It follows that $D^\perp = \{0\}$, hence $D = \mathbb{F}_2^{12}$. Thus the matrix G_D has rank 12. Now suppose that G_D has more than 12 rows. Since the rows of G_C are linearly independent, we get a nontrivial linear combination of rows of G_C with zeros in the last 12 coordinates and not contained in B. This contradicts the choice of B. Thus G_D has exactly 12 rows, and G_B has $k_B = 36 - 12 = 24$ rows. Since the minimum distance of a binary $[60, 24]$ code is bounded by 18 (see [9]), B is a doubly-even code with parameters $[60, 24, 16]$. It contains all the coordinates from the first orbit and is therefore invariant under the action of G. $\square$

Hence we may consider B as a self-orthogonal doubly-even G-submodule (equivalently, an ideal) in the group algebra KG where $G = \mathrm{A}_5$ and $K = \mathbb{F}_2$. Now G has exactly three irreducible KG-modules, namely the trivial one, denoted by 1, and two modules of dimension 4, say V and St, where St denotes the Steinberg module which is known to be projective. That there are only 3 irreducible modules instead of 4 (the number of $2'$-conjugacy classes) is a consequence of $\mathbb{F}_2$.

Lemma 9 *The module B contains the Steinberg module with multiplicity two as a composition factor.*

Proof. By Lemma 7, the ambient space K^{72} can be written $K^{72} = KG \oplus K_T^G$, where T denotes a Sylow 5-subgroup of G and K_T^G the trivial KT-module induced to G. The first 60 coordinates of every vector in K^{72} are in KG and the last 12 in K_T^G. Note that K_T^G is a projective KG-module, since the trivial KT-module is projective, by Maschke's Theorem. Further, the trivial KG-module is a quotient of K_T^G and the projective cover of the trivial KG-module, say $\mathrm{P}(1)$, has dimension 12, as one readily computes using the Cartan matrix. Thus $K_T^G \cong \mathrm{P}(1)$ and, in particular, K_T^G does not contain the Steinberg module St as a composition factor.

By [24, Proposition 2.3], we have

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

as KG-modules, where $C^* = \mathrm{Hom}_K(C, K)$ denotes the dual module of C. Since the multiplicity of the Steinberg module St in K^{72} is four (as a composition factor) and $St \cong St^*$, its multiplicity in C is exactly two.

Since St is a projective KG-module, all Steinberg modules in a composition series of C occur as submodules of C. Now let S be a submodule of C isomorphic to the Steinberg module. Since S is irreducible and K_T^G does not contain a copy of the Steinberg module, all vectors in S must have zeros in the last 12 coordinates. This shows that S (ignoring the last 12 trivial coordinates) is a subspace of B.

Therefore B contains the Steinberg module with multiplicity two as composition factor. $\square$

It is well known that KG consists of two 2-blocks, the principal one and a block of defect zero. The latter is the direct sum of four Steinberg modules. Let e respectively $f = 1 - e$ be the corresponding block idempotents. From [17, Chapter 3] and the ordinary character table of A_5, one directly computes that

$$f = 1 - e = \sum_{\substack{x \in G, \\ x^3 = 1 \neq x}} x + \sum_{\substack{y \in G, \\ y^5 = 1 \neq y}} y$$

is the block idempotent of the block of defect zero. Thus

$$e = 1 + \sum_{\substack{x \in G, \\ x^3 = 1 \neq x}} x + \sum_{\substack{y \in G, \\ y^5 = 1 \neq y}} y$$

is a block idempotent generating the principal block.

With this notation we obtain the following.

Proposition 10 $\dim eKG = 44$ *and* $\dim eB = 16$.

Proof. The first assertion is clear since the block $fKG = (1-e)KG$ of defect zero has dimension $(\dim St)^2 = 16$. Thus eKG has dimension 44.

We now determine $\dim eB$. Clearly,

$$B = eB \oplus (1-e)B = eB \oplus fB$$

since e is an idempotent. Thus we must compute $\dim fB$. Observe that fB is a direct sum of modules isomorphic to the Steinberg module St and eB does not contain a composition factor (equivalently a submodule) isomorphic to St. Lemma 9 now implies $\dim fB = 8$. Hence $\dim eB = \dim B - \dim fB = 24 - 8 = 16$. □

These results underpin the following approach to decide whether or not A_5 can be the automorphism group of C.

(1) The binary self-orthogonal doubly-even code eB has dimension 16 and minimum distance at least 16 in the fixed space eKG of dimension 44, and is invariant under $G = A_5$. There are 9215 G-invariant subspaces of eKG of dimension 16. Of these, 1270 are self-orthogonal, doubly-even and of minimum distance $d \geq 16$.

(2) Assume that the all one-vector of length 60 is in B. Since $C = C^\perp$, this implies that the all one-vector of length 72 is in C. Thus C contains a vector of weight 12, a contradiction. Therefore we only have to consider the 790 modules from (1) which do not contain the all one-vector.

(3) Now we consider the thirty-five 8-dimensional submodules fB. Clearly, fB is a self-orthogonal, doubly-even code of minimum distance $d \geq 16$ in the 16-dimensional ideal fKG. There are 15 such submodules.

(4) Recall that $B = eB \oplus fB$. Moreover, since $e = \hat{e}$ where $\hat{}: KG \to KG$ is defined by $g \to g^{-1}$ for $g \in G$, we have $KG = eKG \perp (1-e)KG$ and

$$B = eB \perp (1-e)B = eB \perp fB.$$

Thus B is the orthogonal sum of a code listed in (2) and a code listed in (3). We verify that all $11850 = 790 \times 15$ spaces have minimum distance strictly smaller than 16.

Hence we conclude that A_5 cannot be the automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code.

3.2 The other cases

The arguments for the other simple groups, A_6 and $\mathrm{SL}(2,8)$, are easier. In both cases, Lemma 7 implies that $C = C^{\perp}$ is a G-invariant subspace of the group algebra KG. Now A_6 has 4 irreducible KG-modules of dimensions $1, 4, 4$ and 16, and $\mathrm{SL}(2,8)$ also has 4 irreducible KG-modules of dimensions $1, 6, 8$, and 12. The relative size of these dimensions is reflected in the small number of 36-dimensional G-invariant subspaces of KG. We can compute these directly: A_6 has 115 subspaces and $\mathrm{SL}(2,8)$ has 107 subspaces. All have minimum distance strictly smaller than 16. This proves Theorem 1.

The following lemma could also be employed to eliminate $\mathrm{SL}(2,8)$.

Proposition 11 *Let $G = \mathrm{SL}(2,8)$. Then KG contains exactly one submodule, say C_0, of dimension 22. Moreover C_0 is contained in any self-dual G-invariant subspace of KG.*

Proof. Let $V_1 = 1, V_6, V_8, V_{12}$ denote the irreducible KG-modules where $\dim V_i = i$. By [1], the Loewy structure of KG is given by

$$(*) \qquad KG \cong \begin{array}{ccccc} & & 1 & & \\ & & V_6 & & \\ V_{12} & 1 & & 1 & 1 \\ & V_6 & & V_6 & \\ V_{12} & 1 & & 1 & 1 \\ & & V_6 & & \\ & & 1 & & \end{array} \oplus V_8 \oplus V_8 = \mathrm{P}(1) \oplus V_8 \oplus V_8$$

where $\mathrm{P}(1)$ denotes the projective cover of the trivial module. Now suppose that $C = C^{\perp}$ is a G-invariant submodule of KG. Again by [24, Proposition 2.3], we have $KG/C^{\perp} \cong C^*$ as KG-modules. Since all irreducible modules V_i are self-dual as modules and $\dim C = 36$, we conclude that C has Loewy structure

$$\begin{array}{ccccc} & & V_6 & & \\ V_{12} & 1 & & 1 & 1 \\ & & V_6 & & \\ & & 1 & & \end{array} \oplus V_8.$$

We do not know which copies of V_8 and V_6 in the middle of $\mathrm{P}(1)$ in $(*)$ occur. However it is easy to see that C contains a unique submodule, say C_0, of dimension 22, namely

$$C_0 = \begin{array}{ccccc} V_{12} & 1 & & 1 & 1 \\ & & V_6 & & \\ & & 1 & & \end{array}.$$

$\square$

We can easily find the subspace C_0 inside KG. It contains basis vectors of weight $12, 16, 24$ and 36. This proves that $\mathrm{SL}(2,8)$ cannot be the automorphism group of a binary self-dual doubly-even code of length 72.

4 The computational tools

The group algebras and invariant subspaces were constructed and investigated using MAGMA [6]. For $G = \mathrm{SL}(2,8)$ and A_6, we constructed the action of G on its Sylow 7- and 5-subgroup respectively, to obtain a permutation representation of degree 72 and then the resulting group algebra over $\mathbb{F}_2$. For $G = \mathrm{A}_5$, we constructed the 72-dimensional representation over $\mathbb{F}_2$ by taking the direct sum of its action on its Sylow 5-subgroup and its regular representation. We obtained the 44-dimensional and 16-dimensional representations by constructing the action of G on the ideals described in Proposition 10.

The submodule lattice machinery is now used to construct the G-invariant subspaces. A basis for each subspace is written down, and used to define a code whose minimum weight is determined using the algorithm of Brouwer and Zimmermann [4].

Acknowledgement: The first author was supported by a research fellowship from the Alexander von Humboldt Foundation. She is grateful to the University of Magdeburg for the excellent working conditions provided. The second author was supported in part by the Marsden Fund of New Zealand via grant UOA 0412. The third author thanks the Department of Mathematics of the University at Auckland for its hospitality while this work was completed.

References

[1] H.H. Andersen, J. Jørgensen and P. Landrock, The projective indecomposable modules of $\mathrm{SL}(2,2^n)$, *Proc. London Math. Soc.*, **46**, pp. 38-52, 1983.

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

[3] E.R. Berlekamp, Coding theory and the Mathieu groups, *Info. Control*, **18**, pp. 40-64, 1971.

[4] 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.

[5] R.E. Blahut, The Gleason-Prange theorem, *IEEE Trans. Inform. Theory*, **37**, pp. 1269-1273, 1991.

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

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

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

[9] A.E. Brouwer, Bounds on the minimum distance of linear codes, available at `http://www.win.tue.nl/~aeb/voorlincod.html`.

[10] 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**, pp. 143-156, 1982.

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

[12] S.H. Houghton, C.W.H. Lam, L.H. Thiel and J.A. Parker, The extended quadratic residue code is the only $[48, 24, 12]$ self-dual doubly-even code, *IEEE Trans. Inform. Theory*, **49**, pp. 53-59, 2003.

[13] 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**, pp. 749-752, 1987.

[14] B. Huppert and N. Blackburn, *Finite Groups II*, Springer Verlag, Berlin, 1982.

[15] W. Knapp and P. Schmid, Codes with prescribed permutation group, *J. Algebra*, **67**, pp. 415-435, 1980.

[16] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North Holland, Amsterdam 1977.

[17] G. Navarro, *Characters and blocks of finite groups*, Cambridge University Press, Cambridge, 1998.

[18] V. Pless, On the uniqueness of the Golay codes, *J. Combin. Theory*, **5**, pp. 215-228, 1968.

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

[20] 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**, pp. 537-541, 1982.

[21] E.M. Rains, Shadow Bounds for Self-Dual Codes, *IEEE Trans. Info. Theory*, **44**, pp. 134 - 139, 1998.

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

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

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

[25] Vassil Yorgov, On the automorphism group of a putative code, to appear *IEEE Trans. Inform. Theory.*

Addresses:

Stefka Bouyuklieva and Wolfgang Willems
Institut für Algebra und Geometrie
Otto-von-Guericke-Universität
Magdeburg
Germany
e-mail: stefka@uni-vt.bg and wolfgang.willems@mathematik.uni-magdeburg.de

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