On extremal self-dual codes of length 96

Javier de la Cruz and Wolfgang Willems

***Abstract*— Let C be a binary extremal self-dual code of length 96. We prove that an automorphism of C of order 3 has 6 or no fixed points and an automorphism of order 5 has 6 fixed points. Moreover, if all automorphisms of order 3 are fixed point free then $\mathrm{Aut}(C)$ is solvable and its order divides $2^5 3$ or $2^5 5$ or $\mathrm{Aut}(C)$ is the alternating group A_5 which is the only possible group of order 60. Furthermore $|\mathrm{Aut}(C)| = 20$ or 40 cannot occur.**

I. Introduction

Throughout the paper all codes are assumed to be binary and linear if not explicitly stated otherwise. Let $C = C^\perp$ be a binary self-dual code of length n and minimum distance d. By results of Mallows-Sloane [14] and Rains [16], we have

$$d \leq \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4 & \text{if } n \not\equiv 22 \pmod{24} \\ 4\lfloor \frac{n}{24} \rfloor + 6 & \text{if } n \equiv 22 \pmod{24}, \end{cases} \quad (1)$$

and C is called extremal self-dual if the equality holds. Extremal codes are of particular interest if 24 divides n since in that case the supports of codewords of a fixed weight form a 5-design, by a well-known result of Assmus and Mattson [1]. The parameters of C are given by $[24m, 12m, 4m + 4]$ for $m \in \mathbb{N}$.

Javier de la Cruz is with the Universidad del Norte, Departamento de Matemáticas, Km 5 Via Puerto Colombia, Barranquilla, Colombia, and the Institut für Algebra und Geometrie, Fakultät für Mathematik, Otto-von-Guericke Universität, 39016 Magdeburg, Germany (e-mail: jdelacruz@uninorte.edu.co).

Wolfgang Willems is with the Institut für Algebra und Geometrie, Fakultät für Mathematik, Otto-von-Guericke Universität, 39016 Magdeburg, Germany, and with the Universidad del Norte, Departamento de Matemáticas, Km 5 Via Puerto Colombia, Barranquilla, Colombia (e-mail: willems@ovgu.de).

For $m = 1$ there is up to equivalence exactly one such code, namely the binary extended $[24, 12, 8]$ Golay code ([15], Theorem 5). Its automorphism group is the Mathieu group M_{24} ([13], Ch. 20, Corollary 5). For $m = 2$ there is again up to equivalence exactly one code, the so-called binary extended $[48, 24, 12]$ quadratic residue code [8]. Its automorphism group is $\mathrm{PSL}(2, 23)$ ([11], Theorem 6). Note that in both cases the automorphism group is a simple non-abelian group.

Actually for $m \geq 3$ no examples are known so far and the existence of such a code is a long standing question in coding theory [17]. In order to attack the existence problem knowledge of a possible automorphism group may be helpful.

For $m = 3$, i.e. a self-dual $[72, 36, 16]$ code, it has been proved in [3] and [4] that the automorphism group has order bounded by 36. In particular, the automorphism group is solvable. If $m = 4$, i.e. C is a self-dual $[96, 48, 20]$ code, then only the primes $2, 3$ and 5 may divide $|\mathrm{Aut}(C)|$ (see [5]). Moreover, elements of order 5 have 16 or 6 fixed points, elements of order 3 have $24, 18, 6$ or no fixed points. By [2], involutions are acting fixed point freely.

In this paper we show that particular types of automorphisms do not occur. Under the assumption that all elements of order 3 do not have fixed points we can restrict the order of the automorphism group. More precisely, we shall prove

Theorem Let C be an extremal self-dual code of length 96.

a) If σ is an automorphism of C of prime order p then its cycle structure is given by

p	number of p-cycles	number of fixed points
2	48	0
3	$30, 32$	$6, 0$
5	18	6

b) If all elements of order 3 have no fixed points then Aut(C) is solvable of order dividing $2^5 3$ or $2^5 5$, or Aut(C) is the simple alternating group A_5 which is the only possible automorphism group of order 60. Furthermore $|\text{Aut}(C)| \neq 20, 40$.

II. Preliminaries

Let C be a binary code with an automorphism σ of odd prime order p. If σ has c cycles of length p and f fixed points we say that σ is of type p-$(c; f)$. Without loss of generality we may assume that

$$\begin{aligned} \sigma &= (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \ldots \\ &\quad ((c-1)p+1, (c-1)p+2, \ldots, cp). \end{aligned}$$

Let $\Omega_1, \Omega_2, \ldots, \Omega_c$ be the cycle sets, i.e. $\Omega_i = \{(i-1)p+1, (i-1)p+2, \ldots, ip\}$, and let $\Omega_{c+1}, \Omega_{c+2}, \ldots, \Omega_{c+f}$ be the fixed points of σ. We put $F_\sigma(C) = \{v \in C \mid v\sigma = v\}$. If $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$ denotes the map defined by $\pi(v|_{\Omega_i}) = v_j$ for some $j \in \Omega_i$ and $i = 1, 2, \ldots, c+f$ then $\pi(F_\sigma(C))$ is a binary self-dual $[c+f, \frac{c+f}{2}]$ code (see [9], Lemma 1). Moreover, in case $p \equiv 1 \pmod 4$ the code $\pi(F_\sigma(C))$ is doubly-even.

Clearly, a generator matrix of $\pi(F_\sigma(C))$ can be written in the form

$$\text{gen}(\pi(F_\sigma(C))) = \begin{pmatrix} A & O \\ O & B \\ D & E \end{pmatrix}, \qquad (2)$$

where the matrices A and D have c columns and B resp. E have f columns, O being the appropriate size zero matrix. Let $\mathcal{A}$ resp. $\mathcal{A}_D$ be the codes of length c generated by A resp. A and D. Let $\mathcal{B}$ resp. $\mathcal{B}_E$ be the codes of length f generated by B resp. B and E.

With this notation we have

Lemma 1: ([10], Theorem 9.4.1) If $k_1 = \dim \mathcal{A}$ and $k_2 = \dim \mathcal{B}$ then

a) (Balance Principle) $k_1 - \frac{c}{2} = k_2 - \frac{f}{2}$.
b) $\text{rank}\, D = \text{rank}\, E = \frac{c+f}{2} - k_1 - k_2$.
c) $\mathcal{A}^\perp = \mathcal{A}_D$ and $\mathcal{B}^\perp = \mathcal{B}_E$.

Lemma 2: Let C be a binary self-dual code with minimum distance d and let $\sigma \in Aut(C)$ of type p-$(c; f)$ where p is an odd prime and $c = f < d$. Then $\pi(F_\sigma(C))$ has a generator matrix of the form $(I_c \mid E')$ where I_c is the identity matrix of size c.

Proof: We write $\text{gen}(\pi(F_\sigma(C)))$ as in (2) and apply Lemma 1. The condition $f < d$ forces $k_2 = 0$. Since $c = f$, the Balance Principle yields $k_1 = 0$ and part b) of Lemma 1 implies that D is regular. Thus

$$D^{-1}\text{gen}(\pi(F_\sigma(C))) = (I_c \mid E')$$

is a generator matrix of $\pi(F_\sigma(C))$. ∎

For the rest of this paper we define $S_{u,v} = |\text{supp}(u) \cap \text{supp}(v)|$ for $u, v \in \mathbb{F}_2^n$.

Lemma 3: Let C be a binary code of length n and minimum distance d. If $u \neq v \in C$ with $\text{wt}(u) = \text{wt}(v) = d$ then $S_{u,v} \leq \frac{d}{2}$.

Proof: We have $d \leq \text{wt}(u+v) = \text{wt}(u) + \text{wt}(v) - 2S_{u,v} = 2d - 2S_{u,v}$ from which the assertion follows. ∎

III. Cycle-types of the automorphisms

Lemma 4: Let C be a self-dual $[96, 48, 20]$ code. Then C has no automorphism of type 3-$(24; 24)$.

Proof: Assume that $\sigma \in \text{Aut}(C)$ is of type 3-$(24; 24)$. We consider a generator matrix for the self-dual code $\pi(F_\sigma(C))$ in the form of (2). Since $c = f$ we get $k_1 = k_2$, by the Balance Principle (see Lemma 1). Furthermore, $\mathcal{B}$ is a doubly-even $[24, k_2, d']$ code with $d' = 20$ or $d' = 24$.

If $k_2 \geq 2$ then obviously $\pi(F_\sigma(C))$ and therefore C contains a codeword of weight less or equal to 8, a contradiction. Thus $k_1 = k_2 \leq 1$.

If $k_2 = 0$ then $k_1 = 0$ and by Lemma 1 b), the matrix D is regular. Thus we have $\mathrm{gen}(\pi(F_\sigma(C))) = (I_{24} \,|\, E)$. Let $(e_i \,|\, v_i)$ be the i-th row of E for $i = 1, \ldots, 24$. Since $\mathrm{wt}(\pi^{-1}(e_i \,|\, v_i)) = 3 + \mathrm{wt}(v_i) \geq 20$ we get $\mathrm{wt}(v_i) = 17$ or 21. If $\mathrm{wt}(v_i) = 17$ and $\mathrm{wt}(v_j) = 21$ for some i and j then

$$S_{v_i,v_j} = |\,\mathrm{supp}(v_i) \cap \mathrm{supp}(v_j)\,| \geq 14,$$

and therefore $\mathrm{wt}(\pi^{-1}(e_i + e_j \,|\, v_i + v_j)) = 6 + \mathrm{wt}(v_i + v_j) \leq 16$, a contradiction. If both $\mathrm{wt}(v_i) = 21$ and $\mathrm{wt}(v_j) = 21$ then

$$S_{v_i,v_j} = |\,\mathrm{supp}(v_i) \cap \mathrm{supp}(v_j)\,| \geq 18,$$

and therefore $\mathrm{wt}(\pi^{-1}(e_i + e_j \,|\, v_i + v_j)) = 6 + \mathrm{wt}(v_i + v_j) \leq 12$, a contradiction again. Thus we have $\mathrm{wt}(v_i) = 17$ for all $i = 1, \ldots, 24$. Clearly, $S_{v_i,v_j} \geq 10$ and $v_i \neq v_j$ for $i \neq j$. On the other hand, for $x = (e_i \,|\, v_i)$ and $y = (e_j \,|\, v_j)$ we have $S_{x,y} = S_{v_i,v_j}$, and Lemma 3 yields $S_{x,y} \leq 10$.

Consequently $S_{v_i,v_j} = 10$ for all $i \neq j$ with $i, j \in \{1, \ldots, 24\}$. In particular, the vectors $v_i \neq v_j$ do not have a coordinate 0 simultaneously. This implies that the dimension of $\mathrm{gen}(\pi(F_\sigma(C)))$ is at most 3, a contradiction.

If $k_2 = 1$ then $\pi(F_\sigma(C))$ has a generator matrix of the form

$$\begin{pmatrix} a & 0\ldots0 \\ 0\ldots0 & b \\ D & E \end{pmatrix},$$

where $\mathrm{wt}(b) = 20$ or 24. Since C is doubly-even, $\mathrm{wt}(a) \in \{8, 12, 16, 20, 24\}$. Suppose that $\mathrm{wt}(a) = 24$, i.e. a is the all one vector of length 24. Thus there exists $z \in \mathcal{A}^\perp$ with $\mathrm{wt}(z) = 2$ and $(z \,|\, u) \in \pi(F_\sigma(C))$ with $\mathrm{wt}(u) \geq 14$. If $\mathrm{wt}(b) = 24$ it follows that

$$\mathrm{wt}(\pi^{-1}((z \,|\, u) + (0 \,|\, b))) \leq 6 + 10 = 16,$$

a contradiction. Hence $\mathrm{wt}(b) = 20$. If $\overline{1}$ denotes the all one vector of length 96 we get

$$\mathrm{wt}(\pi^{-1}(a \,|\, b) + \overline{1}) \leq 4,$$

a contradiction again. Thus $\mathrm{wt}(a) \leq 20$. Therefore the vector a must contain at least four zeros. Consequently, there are at least 4 vectors of the form $z_i = (0, 0, \ldots, 1, \ldots, 0, 0) \in \mathbb{F}_2^{24}$ which are orthogonal to a. By Lemma 1 c), we obtain again $z_i \in \mathcal{A}^\perp = \mathcal{A}_D$. The contradiction now follows as in case $k_2 = 0$. ∎

Lemma 5: Let C be a self-dual $[96, 48, 20]$ code. Then C has no automorphism of type 3-$(26; 18)$.

Proof: Let $\sigma \in \mathrm{Aut}(C)$ be of type 3-$(26; 18)$. We consider again a generator matrix for $\pi(F_\sigma(C))$ in the form of (2). Since $f = 18 < 20$ we obtain $k_2 = 0$ and the Balance Principle (see Lemma 1) implies $k_1 = 4$. Thus $\pi(F_\sigma(C))$ has a generator matrix of the form

$$\begin{pmatrix} A & 0 \\ D & E \end{pmatrix}.$$

Note that $\mathcal{A}$ is a doubly-even $[26, 4, d^*]$ code with $d^* \geq 8$. Furthermore, the table [6] shows that the dual distance $(d^*)^\perp$ of $\mathcal{A}$ is 1 or 2.

Next we observe that there are no two codewords $a_1, a_2 \in \mathcal{A}^\perp$ both of weight 1. If so then $(a_i \,|\, b_i) \in \pi(F_\sigma(C))$ with $\mathrm{wt}(b_i) = 17$. It follows

$$0 \neq c = \pi^{-1}(a_1 + a_2 \,|\, b_1 + b_2) \in C$$

with $\mathrm{wt}(c) \leq 8$, a contradiction. Thus if the dual distance $(d^*)^\perp = 1$ then A contains a zero column. Removing this column we get a doubly-even $[25, 4, \geq 8]$ code $\mathcal{A}'$ with dual distance at least 2 since there are no two codewords of weight 1 in $\mathcal{A}^\perp$. Clearly, $\mathcal{A}'^\perp$ has length 25 and dimension 21. The table in [6] shows that its minimum distance is at most 2. Therefore $\mathcal{A}^\perp$ contains codewords of weight 2. Now we choose $a_i \in \mathcal{A}^\perp$ of weight i for $i = 1, 2$. Thus there exist vectors $(a_i \,|\, b_i) \in \pi(F_\sigma(C))$ with $\mathrm{wt}(b_1) = 17$ and $\mathrm{wt}(b_2) = 14$ or 18. Consequently $\mathrm{wt}(\pi^{-1}(a_1 + a_2 \,|\, b_1 + b_2)) \leq 9 + 5 < 20$, a contradiction.

Now let $(d^*)^\perp = 2$ and suppose that $a_1, a_2 \in \mathcal{A}^\perp$ with $a_1 \neq a_2$ and $\mathrm{wt}(a_1) = \mathrm{wt}(a_2) = 2$. Thus there are vectors $(a_i \,|\, b_i) \in \pi(F_\sigma(C))$ with $\mathrm{wt}(b_i) = 14$ or 18 for $i = 1, 2$.

In particular $\mathrm{wt}(b_1+b_2) \le 8$. If $\mathrm{wt}(a_1+a_2) = 2$ then

$$\mathrm{wt}(\pi^{-1}(a_1+a_2 \,|\, b_1+b_2)) =$$
$$6+\mathrm{wt}(b_1+b_2) \le 6+8 < 20,$$

a contradiction. Therefore $\mathrm{wt}(a_1+a_2) = 4$. Since

$$\mathrm{wt}(\pi^{-1}(a_1+a_2 \,|\, b_1+b_2)) =$$
$$12+\mathrm{wt}(b_1+b_2) \ge 20$$

we obtain $\mathrm{wt}(b_1+b_2) = 8$ and $\mathrm{wt}(b_i) = 14$. There are at most four vectors b_i which satisfy these conditions. Thus there are at most four vectors $a_i \in \mathcal{A}^\perp$ with $\mathrm{wt}(a_i) = 2$. Denote the exact number by $s \le 4$. Next we puncture the code $\mathcal{A}$ on the support of the vector $a_1+\ldots+a_s$. We get either a $[26-2s, 4, \ge 2]$ code or an $[18, 3, \ge 2]$ code in case $s = 4$ and $a_1+\ldots+a_s \in \mathcal{A}$. Call this code $\mathcal{A}'$. Let $0 \ne v \in \mathcal{A}'^\perp$. If $\mathrm{wt}(v) = 1$ then we may add zeros at the positions of $\mathrm{supp}(a_1+\ldots+a_s)$ to get a vector of weight 1 in $\mathcal{A}^\perp$, a contradiction. If $\mathrm{wt}(v) = 2$ then the same construction leads to a vector of weight 2 in $\mathcal{A}^\perp$ different from a_i for $i = 1,\ldots,s$, a contradiction again. This shows that the minimum distance of $\mathcal{A}'^\perp$ is at least 3. On the other hand, the table [6] shows that the minimum distance of any $[26-2s, 22-2s]$ code for $s = 1,\ldots,4$ and any $[18,15]$ code is at most 2, which completes the proof. ∎

Lemma 6: Let C be a self-dual $[96,48,20]$ code. Then C has no automorphism of type 5-$(16;16)$.

Proof: Since $p = 5 \equiv 1 \pmod 4$ the space $\pi(F_\sigma(C))$ is a doubly-even self-dual $[32,16,d_\pi]$ code, by ([9], Lemma 1). Furthermore $c = f = 16 < d = 20$. According to Lemma 2 we can take a generator matrix of $\pi(F_\sigma(C))$ of the form $\mathrm{gen}\,(\pi(F_\sigma(C))) = (I_{16} \mid E')$. If $x = (1\,0\,0\ldots0 \mid x')$ and $y = (0\,1\,0\ldots0 \mid y')$ denotes the first resp. the second row of $(I_{16} \mid E')$ then

$$\begin{aligned}\mathrm{wt}(\pi^{-1}(x)) &= \mathrm{wt}(\pi^{-1}((1\,0\,0\ldots0 \mid x'))) \\ &= 5+\mathrm{wt}(x') \ge 20.\end{aligned}$$

Therefore $15 \le \mathrm{wt}(x') \le 16$. Since C is doubly-even we have $\mathrm{wt}(x') = 15$. Similarly $\mathrm{wt}(y') = 15$. This implies that $\mathrm{wt}(x'+y') \le 2$. Hence

$$\begin{aligned}\mathrm{wt}(\pi^{-1}(x+y)) &= \mathrm{wt}(\pi^{-1}(1\,1\,0\ldots0 \mid x'+y')) \\ &= 10+\mathrm{wt}(x'+y') \le 12,\end{aligned}$$

a contradiction. ∎

In conclusion we have shown in this section that an automorphism of odd prime order of an extremal self-dual code of length 96 can only have the following cycle structures: 5-$(18;6)$, 3-$(32;0)$ or 3-$(30;6)$. Since involutions are acting fixed point freely by [2], the proof of part a) of the theorem is complete.

IV. The Automorphism Group

Let $G = \mathrm{Aut}(C)$ where C is a binary self-dual $[96,48,20]$ code. By [5], we know that $|G| = 2^a 3^b 5^c$ with $a,b,c \in \mathbb{N}_0$. According to the assumption in theorem b) we assume from now on that elements of order 3 do act fixed point freely on the 96 coordinates. For some elementary facts from group theory like Sylow's theorem we refer the reader to the textbook [12].

Lemma 7: The order of G divides $2^a 3^b 5^c$ where $a \in \{0,1,\ldots,5\}$ and $b,c \in \{0,1\}$.

Proof: Clearly, a Sylow 2-subgroup acts regularly, i.e. without fixed points, on the 96 coordinates since involutions have no fixed points. This implies $a \le 5$.

Since, by assumption, elements of order 3 have no fixed points a Sylow 3-subgroup acts regularly as well which implies $b \le 1$.

In order to prove that $c \le 1$ we may assume that $5 \mid |G| = 2^a 3^b 5^c$. To compute the number t of orbits of the action of G on the 96 coordinates of C we use the Cauchy-Frobenius Lemma (see [12], 1A.6 on p 6) which says that

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

where $\mathrm{Fix}(g)$ denotes the number of coordinates which are fixed under the action of g. Applying part a) of the theorem which we have proved in the previous section and using the assumption that elements of order 3 have no fixed points we see that only automorphisms of order 3, 5 or of even order exist. Thus apart from the identity only elements of order 5 have 6 fixed points. Thus

$$\begin{aligned} t &= \tfrac{1}{2^a3^b5^c}\left(96+\textstyle\sum_{\mathrm{ord}(g)=5} 6\right) \\ &= \tfrac{1}{2^a3^b5^c}\left(6\cdot 16+6y\right) \end{aligned}$$

where $y \in \mathbb{N}_0$. If $G_5 = \{g \in G \mid g^5 = 1\}$ and $|G|_5 = 5^c$ then $5^c = |G|_5$ divides $|G_5| = y+1$, by ([7], Remark 15.10). Therefore $y+1 = 5^c z$ with $z \in \mathbb{N}_0$. It follows

$$t = \frac{1}{2^a3^b5^c}\,6(15+(y+1)) = \frac{1}{2^a3^b5^c}\,6(15+5^c z),$$

hence

$$2^a3^b5^c \cdot t = 6(15+5^c z)$$

from which we deduce $c \leq 1$. ■

Lemma 8: If $15 \mid |G|$ then $|G| \leq 60$. In particular, A_5 is the only non-solvable automorphism group which may occur.

Proof: Let T be a Sylow 5-subgroup of G. Clearly $3 \nmid |\mathrm{N}_G(T)|$ since there are no elements of order 15. Thus

$$|G : \mathrm{N}_G(T)| = \frac{2^a\cdot 3\cdot 5}{2^x \cdot 5} = 2^{a-x}\cdot 3 \equiv 1 (\mathrm{mod}\ 5),$$

by ([12], Corollary 1.17). The only possibilities for (a,x) are

$$(2,1),(3,2),(4,3),(5,4),(5,0).$$

In the last case ($a=5$ and $x=0$) we have $|G| = 32\cdot 15 = 480$ and G has exactly 96 Sylow 5-subgroups. Thus the number of orbits is

$$t = \frac{1}{480}\,(96+96\cdot 4\cdot 6) = 5.$$

This contradicts the fact that the Sylow 2-subgroup has orbits of length $2^a = 32$. In all other cases the number of Sylow 5-subgroups is 6 and therefore the number of orbits is

$$t = \frac{1}{2^a\cdot 3\cdot 5}\,(96+6\cdot 4\cdot 6) = \frac{2^4}{2^a}.$$

Since $t \in \mathbb{N}$ we have $a \leq 4$. If $a=4$ then $t=1$. Thus G acts transitively on the 96 coordinates. In particular, 96 must divides $|G| = 240$ (since $a=4$), a contradiction. In case $a=3$ we have $t=2$. This can also not happen since the orbits of G have length 24. ■

The next two lemmas complete the proof of the theorem.

Lemma 9: If $15 \mid |G|$ then $G = \mathrm{A}_5$.

Proof: By Lemma 7 and 8, we have $|G| = 2^a\cdot 3\cdot 5$ with $a \leq 2$. Since G does not have elements of order 15 we have in particular $|G| \neq 15$. If $|G| = 30$ then a Sylow 5-subgroup is normal in G, by ([12], 1E.2 p. 38). Hence a 3-element centralizes a 5-element and we get again an element of order 15 which does not exist. Suppose that $|G| = 60$ and solvable. If G has a normal subgroup N of order 3 or 5 we find again an element of order 15, a contradiction. If $|N| = 4$ then there exists a 2-complement by Hall's Theorem (see [12], Theorem 3.13) which is a group of order 15 and we are done again. Thus $|N| = 2$. Since N is in the center of G we see that G contains a normal subgroup of order 3 or 5 which completes the proof. ■

Lemma 10: $|G| \neq 20, 40$.

Proof: If $|G| = 20$ then a Sylow 5-subgroup is normal since the number of Sylow 5-subgroups is congruent $1 \pmod 5$. Thus, for the number of orbits we get

$$t = \frac{1}{20}(96+6\cdot 4) = 6.$$

Clearly, the orbits have size 20 or 4. But $20m + 4n = 96$ and $m+n = 6$ has no solution in $\mathbb{N}_0$.

In case $|G| = 40$ the Sylow 5-subgroup is again normal, by the same argument as above. Thus the number of orbits is given by

$$t = \frac{1}{40}(96+6\cdot 4) = 3.$$

Now the orbits have size 40 or 8. Since $40m + 8n = 96$ and $m+n = 3$ has no solution in $\mathbb{N}_0$ the group G cannot exist as automorphism group of C. ■

Acknowledgment The authors are deeply indepted to suggestions and comments of the referees which improved an earlier version of this paper. In particular, the proof of Lemma 5 goes back to ideas of one of the referees.

REFERENCES

[1] E.F. Assmus, Jr. and H.F. Mattson Jr., New 5-designs. *J. Combin. Theory* **6** (1969), 122-151.

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

[3] 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** (2006), 4244-4248.

[4] E.A. O'Brien and W. Willems, On the automorphism group of a binary self-dual doubly-even [72,36,16] code. To appear IEEE Trans. Inform. Theory.

[5] R. Dontcheva, On the doubly-even self-dual codes of length 96. *IEEE Trans. Inform. Theory* **48** (2002), 557-560.

[6] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, online available at `http://www.codetables.de`

[7] R. Gow, B. Huppert, R. Knörr, O. Manz and W. Willems. *Representation theory in arbitrary characteristic.* Casa Editrice Dott. Antonio Milani, Padua 1993.

[8] S.K. Houghten, 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* **48** (2002), 53-59.

[9] W.C. Huffman, Automorphisms of codes with application to extremal doubly-even codes of length 48. *IEEE Trans. Inform. Theory* **28** (1982), 511-521.

[10] W.C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes.* Cambridge University Press, Cambridge 2003.

[11] J.S. Leon, V. Pless and N.J.A. Sloane, Duadic codes. *IEEE Trans. Inform. Theory* **30** (1984), 709-714.

[12] I.M. Isaacs, *Finite group theory.* Graduate Studies in Math, Vol. 92, AMS, Providence 2008.

[13] J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam 1977.

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

[15] V. Pless, On the uniqueness of the Golay codes. *J. Comb. Theory* **5** (1968), 215-228.

[16] E.M. Rains, Shadow bounds for self-dual-codes. *IEEE Trans. Inform. Theory* **44** (1998), 134-139.

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

Javier de la Cruz received a M.Sc. in mathematics from the Universidad Nacional, Medellin, Colombia in 2007. From 2006 to 2008, he was with the Department of Mathematics, Universidad del Norte, Barranquilla, Colombia. Since 2009 he is a PhD student in mathematics at the University of Magdeburg, Germany.

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, and since 2010, also Profesor Honorario at the Universidad del Norte, Colombia. His primary research interests are algebraic coding theory and representation theory of finite groups.