On the Automorphism Group of a Binary Self-Dual $[120, 60, 24]$ Code

Stefka Bouyuklieva[1], Javier de la Cruz[2] and Wolfgang Willems[3]

[1] University of Veliko Tarnovo, Veliko Tarnovo, Bulgaria

[2] Universidad del Norte, Barranquilla, Colombia

[3] Otto-von-Guericke Universität, Magdeburg, Germany

Abstract

We prove that an automorphism of order 3 of a putative binary self-dual $[120, 60, 24]$ code C has no fixed points. Moreover, the order of the automorphism group of C divides $2^a \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 23 \cdot 29$ with $a \in \mathbb{N}_0$. Automorphisms of odd composite order r may occur only for $r = 15$, 57 or $r = 115$ with corresponding cycle structures $3 \cdot 5$-$(0, 0, 8; 0)$, $3 \cdot 19$-$(2, 0, 2; 0)$ or $5 \cdot 23$-$(1, 0, 1; 0)$ respectively. In case that all involutions act fixed point freely we have $|\mathrm{Aut}(C)| \leq 920$, and $\mathrm{Aut}(C)$ is solvable if it contains an element of prime order $p \geq 7$. Moreover, the alternating group A_5 is the only non-abelian composition factor which may occur in $\mathrm{Aut}(C)$.

1 Introduction

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

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

and C is called extremal if equality holds. Due to interesting connections with designs, extremal codes of length $24m$ are of particular interest. Unfortunately, only for $m = 1$ and $m = 2$ such codes are known, namely the $[24, 12, 8]$ extended Golay code and the $[48, 24, 12]$ extended quadratic residue code (see [15],[11]). To date the existence of no other extremal code of length $24m$ is known. In numerous papers the automorphism group of a $[72, 36, 16]$, respectively a $[96, 48, 20]$ code has been studied. In case $n = 72$ only 10 nontrivial automorphism groups may occur. The largest has order 24 (see Theorem 1 of [1]). For $n = 96$, only the primes $2, 3$ and 5 may divide $|\mathrm{Aut}(C)|$ and the cycle structure of prime order automorphisms are 2-$(48; 0), 3$-$(30; 6), 3$-$(32; 0), 5$-$(18; 0)$ (see Theorem, part a) in [5]). We would like to mention here that in part b) of the Theorem (the case where elements of order 3 act fixed point freely) four group orders are missing, namely $15, 30, 240$ and 480. The gap is due to the fact that the existence of elements of order 15 with six cycles of length 15 and two cycles of length 2 are not excluded in the given proof.

In his thesis [7] the second author considered the case $n = 120$. This case is of particular interest since for $n = 24m$ with $m \geq 2$ the involutions of the automorphism group act fixed point freely except possibly the case $n = 120$ (see [3]). It turned out that the only primes which may divide the order of the automorphism group are 2, 3, 5, 7, 19, 23 and 29. More precisely, in Theorem 2 of [6] which is part of the thesis the second author proves the following. 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	$48, 60$	$24, 0$
3	$32, 34, 36, 38, 40$	$24, 18, 12, 6, 0$
5	24	0
7	17	1
19	6	6
23	5	5
29	4	4

(2)

In the first part of this note we prove Theorem A which is also contained in the thesis [7] of the second author. The crucial part is the first statement, i.e., that elements of order 3 act fixed point freely. Its proof is joint work of the three authors.

Theorem A Let C be an extremal self-dual code of length 120 with automorphism group G.

a) If σ is an automorphism of C of prime order 3, then σ has no fixed points.

b) If $p \neq 2$, then $p^2 \nmid |G|$. Therefore $|G|$ divides $2^a \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 23 \cdot 29$ where $a \in \mathbb{N}_0$.

c) If σ is an automorphism of C of odd composite order r, then $r = 15, 57$ or $r = 115$ and the cycle structure of σ is given by 15-$(0, 0, 8; 0)$, 57-$(2, 0, 2; 0)$ and 115-$(1, 0, 1; 0)$.

If we assume that all involutions act fixed point freely then according to Theorem A and the list in (2) all elements of $\mathrm{Aut}(C)$ have a unique cycle structure. Using the Cauchy-Frobenius lemma ([13], 1A.6) and methods from elementary group theory we can further restrict the structure of $\mathrm{Aut}(C)$. More precisely, we have

Theorem B Let C be an extremal self-dual code of length 120 with automorphism group G. If all involutions of G act fixed point freely then the following holds true.

a) $|G| \leq 920$.

b) If a prime $p \geq 7$ divides the order of G then G is solvable.

c) The only nonabelian composition factor which might occur in G is the alternating group A_5.

2 Preliminaries

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

$$\sigma = (1, 2, \ldots, p)(p + 1, p + 2, \ldots, 2p) \ldots ((c - 1)p + 1, (c - 1)p + 2, \ldots, cp). \tag{3}$$

By $\Omega_1, \Omega_2, \ldots, \Omega_c$ we denote the cycle sets and by $\Omega_{c+1}, \Omega_{c+2}, \ldots, \Omega_{c+f}$ the fixed points of σ. Furthermore let $F_\sigma(C) = \{v \in C \mid v\sigma = v\}$. If $\pi : F_\sigma(C) \to F_2^{c+f}$ 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 $[c + f, \frac{c+f}{2}]$ self-dual code. Let C_{π_1} be the subcode of $\pi(F_\sigma(C))$ which consists of all codewords which have support in the first c coordinates, and let C_{π_2} be the subcode of all codewords in $\pi(F_\sigma(C))$ which have support in the last f coordinates. Thus a generator matrix of $\pi(F_\sigma(C))$ may be written in the form

$$\mathrm{gen}(\pi(F_\sigma(C))) = \begin{pmatrix} A & O \\ O & B \\ D & E \end{pmatrix}, \tag{4}$$

where $(A\, O)$ is a generator matrix of C_{π_1} and $(O\, B)$ is a generator matrix of C_{π_2}, O being the appropriate size zero matrix. With this notation we have

Lemma 1 ([12], section 9.4) *If $k_1 = dim\, C_{\pi_1}$ and $k_2 = dim\, C_{\pi_2}$, then the following holds true.*

a) (*Balance Principle*) $k_1 - \frac{c}{2} = k_2 - \frac{f}{2}$.

b) $rank(D) = rank(E) = \frac{c+f}{2} - k_1 - k_2$.

c) Let $\mathcal{A}$ be the code of length c generated by A, $\mathcal{A}_D$ the code of length c generated by A and D, $\mathcal{B}$ the code of length f generated by B, and $\mathcal{B}_E$ the code of length f generated by B and E. Then $\mathcal{A}^\perp = \mathcal{A}_D$ and $\mathcal{B}^\perp = \mathcal{B}_E$.

The following Lemma, whose proof is trivial, plays a central role when dealing with the code $\mathcal{A}$. For an n-tupel we use sometimes the notion $(*|*)$ where the length of the first and the second part is clear from the given context.

Lemma 2 *If $\mathcal{A}$ is a binary linear code $[n, k]$ code with dual distance* 1*, then (after a suitable permutation of the coordinates) $\mathcal{A} = (0|\mathcal{A}_1)$, where $\mathcal{A}_1$ is a linear $[n - 1, k]$ code. Furthermore $\mathcal{A}^\perp = (0|\mathcal{A}_1^\perp) \cup (1|\mathcal{A}_1^\perp)$.*

3 Cyclic structure of automorphisms of order 3

Throughout this section let C be a binary self-dual $[120, 60, 24]$ code. As stated in (2) an automorphism of C of order 3 with c cycles and f fixed points satisfies $(c; f) = (32; 24)$, $(34; 18)$, $(36; 12)$, $(38; 6)$ or $(40; 0)$. In this section we prove that only the last case can occur; i.e., an element of order 3 must act fixed point freely.

Lemma 3 *C does not have an automorphism of type* 3-(32; 24).

Proof: Let $\sigma \in \mathrm{Aut}(C)$ be of type 3-(32; 24). For $\pi(F_\sigma(C))$ we take a generator matrix in the form (4). By the Balance Principle (see Lemma 1), we get $k_1 = k_2 + 4$. Since $f = d = 24$ we have $k_2 = 0$ or 1.

First we consider the case $k_2 = 0$. In this case we have $k_1 = 4$ and $\pi(F_\sigma(C))$ has a generator matrix of the form

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

Furthermore, $\mathcal{A}$ is a doubly-even $[32, 4, d' \geq 8]$ code and its dual $\mathcal{A}^\perp$ has parameters $[32, 28, d'^\perp]$. Looking at the online table [10] we see that $d(\mathcal{A}^\perp) = d'^\perp \leq 2$.

If $d(\mathcal{A}^\perp) = 1$ we may assume (without loss of generality) that $a_1 = (100\ldots0) \in \mathcal{A}^\perp$. Thus $\pi(F_\sigma(C))$ contains a vector $(a_1|b_1)$ with $b_1 \in \mathbb{F}_2^{24}$. Since

$$\mathrm{wt}(\pi^{-1}(a_1|b_1)) = 3 + \mathrm{wt}(b_1) \geq 24$$

we get $\mathrm{wt}(b_1) = 21$. According to Lemma 2, $\mathcal{A} = (0|\mathcal{A}_1)$ and $\mathcal{A}^\perp = (0|\mathcal{A}_1^\perp) \cup (1|\mathcal{A}_1^\perp)$. The code $\mathcal{A}_1^\perp$ has parameters $[31, 27]$ and by [10], its minimum distance is 1 or 2. If $d(\mathcal{A}_1^\perp) = 1$, then (up to equivalence) there is a codeword $(010\ldots0|b_2) \in \pi(F_\sigma(C))$ with $\mathrm{wt}(b_2) = 21$. But then $\mathrm{wt}(\pi^{-1}((a_1|b_1) + (010\ldots0|b_2))) \leq 6 + 6 < 24$ which contradicts the minimum distance of C. If $d(\mathcal{A}_1^\perp) = 2$, then (up to equivalence) there is a codeword $(0110\ldots0|b_2) \in \pi(F_\sigma(C))$ with $\mathrm{wt}(b_2) = 18$ or 22. Thus we obtain

$$\mathrm{wt}(\pi^{-1}((a_1|b_1) + (0110\ldots0|b_2))) = 9 + \mathrm{wt}(b_1 + b_2) \leq 9 + 9 < 24,$$

again a contradiction.

Now we consider the case $d(\mathcal{A}^\perp) = 2$. Let

$$W_{\mathcal{A}}(y) = 1 + A_8y^8 + A_{12}y^{12} + A_{16}y^{16} + A_{20}y^{20} + A_{24}y^{24} + A_{28}y^{28} + A_{32}y^{32}$$

denote the weight enumerator of $\mathcal{A}$ and let

$$W_{\mathcal{A}^\perp}(y) = 1 + B_2y^2 + B_3y^3 + \ldots$$

be the weight enumerator of its dual code. Since $k_2 = 0$, the code $\mathcal{A}$ does not contain the all one vector. Hence $A_{32} = 0$.

Using the power moments

$$\sum_{j=d}^{n} A_j = 2^k - 1, \quad \sum_{j=d}^{n} jA_j = 2^{k-1}n, \quad \sum_{j=d}^{n} j^2A_j = 2^{k-2}n(n+1) + 2^{k-1}B_2$$

for a linear binary $[n, k, d]$ code with $B_1 = 0$ (see for example [12], section 7.3) we obtain

$$A_{20} = 31 - 10A_8 - 6A_{12} - 3A_{16} + \frac{1}{4}B_2,$$

$$A_{24} = -21 + 15A_8 + 8A_{12} + 3A_{16} - \frac{1}{4}B_2,$$
$$A_{28} = 5 - 6A_8 - 3A_{12} - A_{16} + \frac{1}{4}B_2.$$

Therefore, $A_{24} + 3A_{28} = \frac{1}{2}B_2 - 3A_8 - A_{12} - 6$ and B_2 is a multiple of 4. Since A_j are nonnegative integers, we get $B_2 \geq 12$. Now we consider 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 $\mathrm{wt}(b_i) = 18$ or 22 for $i = 1, 2$. In particular, $\mathrm{wt}(b_1 + b_2) \leq 12$ since $b_1, b_2 \in \mathbb{F}_2^{24}$. It follows that

$$\mathrm{wt}(\pi^{-1}(a_1 + a_2|b_1 + b_2)) \leq 12 + \mathrm{wt}(b_1 + b_2) \leq 24.$$

Since the minimum distance of C is 24, we get $\mathrm{wt}(\pi^{-1}(a_1 + a_2|b_1 + b_2)) = 24$. Moreover $\mathrm{wt}(a_1 + a_2) = 4$, $\mathrm{wt}(b_1 + b_2) = 12$ and $\mathrm{wt}(b_1) = \mathrm{wt}(b_2) = 18$. Using this, we easily see that $B_2 \leq 4$, which contradicts the above inequality $B_2 \geq 12$.

Finally we deal with the case $k_2 = 1$. Now $k_1 = 5$ and $\mathcal{A}$ is a doubly-even $[32, 5, d']$ code with $d' \geq 8$. By [10], the dual distance satisfies $d(\mathcal{A}^\perp) \leq 2$. Thus there exist a vector $(a|b) \in \pi(F_\sigma(C))$ with $\mathrm{wt}(a) \leq 2$ and $\mathrm{wt}(b) \geq 18$. Since $k_2 = 1$ we have $v = (0, \ldots, 0|\mathbf{1}) \in \pi(F_\sigma(C))$ where $\mathbf{1}$ is the all one vector of length 24. But then $\mathrm{wt}(\pi^{-1}(a|b + \mathbf{1})) \leq 6 + 6 < 24$, the final contradiction. □

Lemma 4 *C does not have an automorphism of type* 3-(34; 18).

Proof: Let σ be an automorphism of C of type 3-(34; 18). Then $\pi(F_\sigma(C))$ is a self-dual $[52, 26, \geq 8]$ code and we consider again a generator matrix for $\pi(F_\sigma(C))$ of the form (4). Since $f = 18 < 24$ we have $k_2 = 0$, hence

$$\mathrm{gen}(\pi(F_\sigma(C))) = \begin{pmatrix} A & O \\ D & E \end{pmatrix}.$$

The balance principle (see Lemma 1) yields $k_1 = 8$.

If $(a|b)$ is a nonzero codeword in $\pi(F_\sigma(C))$, where a and b are vectors of length 34 and 18 respectively, then $3\mathrm{wt}(a) + \mathrm{wt}(b) \geq 24$. This implies $\mathrm{wt}(a) \geq 2$. Clearly, $\mathcal{A}$ is a doubly-even $[34, 8, d']$ code with $d' \geq 8$ and dual distance $d'^\perp \geq 2$.

We consider first the case $d'^\perp = 2$. If $\mathrm{wt}(a) = 2$ then b is the all one vector of length 18. Suppose that $(a'|b') \in \pi(F_\sigma(C))$ is a codeword where $\mathrm{wt}(a') = x$ and $\mathrm{wt}(b') = y$ are both odd numbers. Since $3x + y \equiv 0 \pmod 4$ we get $y \equiv x \pmod 4$. Thus the weight of the codeword $\pi^{-1}(a + a'|b + b') \in C$ is

$$3x + 6 + 18 - y = 3x - y + 24 \equiv 3x - y \equiv 2x \equiv 2 \pmod 4$$

or

$$3x - 6 + 18 - y = 3x - y + 12 \equiv 3x - y \equiv 2x \equiv 2 \pmod 4.$$

Both cases are not possible for a doubly-even code. This shows that in case $d'^\perp = 2$ the code $\mathcal{A}^\perp$ contains only even weight vectors . Hence $(1, \ldots, 1) \in \mathcal{A}$, a contradiction, since C is doubly-even.

Thus we may assume that $d'^{\perp} \geq 3$. In order to get a final contradiction we calculate the split weight distribution

$$A_{(x,y)} = |\{(u|w) \in \pi(F_\sigma(C)) \mid \mathrm{wt}(u) = x \text{ and } \mathrm{wt}(w) = y\}| \qquad (0 \leq x \leq 34,\ 0 \leq y \leq 18)$$

of $\pi(F_\sigma(C))$. To do so we use the generalized MacWilliams identities

$$A_{(x,y)} = \frac{1}{2^{26}} \sum_{j=0}^{18} \sum_{i=0}^{34} A_{(i,j)} \mathcal{K}_x(i,34) \mathcal{K}_y(j,18),\ 0 \leq y \leq 18,\ 0 \leq x \leq 34$$

(see [17] and [9, Theorem 13]) with the following restrictions:

- $A_{(x,y)} = 0$ if $x + y$ is odd,
- $A_{(x,y)} = 0$ if $3x + y \not\equiv 0 \mod 4$,
- $A_{(x,y)} = 0$ if $0 < x + y < 8$ or $0 < 3x + y < 24$,
- $A_{(1,y)} = 0$ and $A_{(2,y)} = 0$ for $y = 0, 1, \ldots, 18$,
- $A_{(0,0)} = 1$, $A_{(x,y)} = A_{(34-x,18-y)}$.

In particular we obtain the equations

$$\begin{aligned} A_{(9,1)} &= 34 - 22A_{(8,0)} - 4A_{(12,0)}, \\ A_{(31,3)} &= 20A_{(8,0)} + 8A_{(12,0)} + 2A_{(16,0)} - 476, \\ A_{(20,0)} &= 663 - 10A_{(8,0)} - 6A_{(12,0)} - 3A_{(16,0)}. \end{aligned}$$

Thus we obtain $3A_{(31,3)} + 2A_{(20,0)} + 3A_{(9,1)} = -26A_{(8,0)}$ which forces $A_{(8,0)} = 0$ since $A_{(x,y)} \geq 0$. Thus $0 = A_{(9,1)} = 34 - 4A_{(12,0)}$ which is not possible. □

Lemma 5 *C does not have an automorphism of type* 3-(36; 12)*.*

Proof: Let σ be an automorphism of C of type 3-(36; 12). Thus $\pi(F_\sigma(C))$ is a self-dual $[48, 24, \geq 8]$ code.

We take again a generator matrix for $\pi(F_\sigma(C))$ in the form (4). Since $f < 24$, we have $k_2 = 0$. Hence $\pi(F_\sigma(C))$ has a generator matrix of the form

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

The Balance Principle (see Lemma 1) shows that $k_1 = 12$. Note that $\mathcal{A}$ is a doubly-even $[36, 12, d']$ code with $d' \geq 8$. If $a \in \mathcal{A}^{\perp}$, then there exists a vector $(a|b) \in \pi(F_\sigma(C))$ with $3\mathrm{wt}(a) + \mathrm{wt}(b) \geq 24$ and $\mathrm{wt}(b) \leq 12$. Thus $\mathrm{wt}(a) \geq 4$ and the dual distance d' of $\mathcal{A}$ satisfies

$d'^{\perp} \geq 4$. A calculation of the coefficients $A_{(x,y)}$ for $x = 0, 1, \ldots, 36$ and $y = 0, 1, \ldots, 12$ in the split weight enumerator of $\pi(F_\sigma(C))$ yields

$$\begin{aligned} A_{(28,0)} &= 7092 + 39A_{(8,0)} - 4A_{(16,0)} \\ A_{(32,0)} &= A_{(16,0)} - 10A_{(8,0)} - 1773. \end{aligned}$$

Thus $A_{(28,0)} + 4A_{(32,0)} = -A_{(8,0)}$. This implies $A_{(8,0)} = 0$, hence $A_{(28,0)} = A_{(32,0)} = 0$ and $A_{(16,0)} = 1773$. But then

$$A_{(30,2)} = 18A_{(16,0)} - 192A_{(8,0)} - 32076 = 18A_{(16,0)} - 32076 = -162 < 0,$$

a contradiction. □

Lemma 6 *C does not have an automorphism of type* 3-(38; 6).

Proof: Let $\sigma \in \mathrm{Aut}(C)$ be of type 3-(38; 6). Now $\pi(F_\sigma(C))$ is a self-dual $[44, 22, d_\pi]$ code. According to (1) we have $d_\pi \leq 8$. If $d_\pi = x + y$, where x is the number of 1's in the first c coordinates and y is the number of 1's in the last f coordinates of a minimal weight codeword in $\pi(F_\sigma(C))$, then $x + y \leq 8$ and $3x + y \geq 24$. This forces $x \geq 8$, $y = 0$ and $d_\pi = 8$. Thus $\pi(F_\sigma(C))$ is a self-dual $[44, 22, 8]$ code. According to [4] there are two possible weight enumerators for such a code, namely

$$W_1(y) = 1 + (44 + 4\beta)y^8 + (976 - 8\beta)y^{10} + \ldots$$

where $10 \leq \beta \leq 122$ and

$$W_2(y) = 1 + (44 + 4\beta)y^8 + (1232 - 8\beta)y^{10} + (10241 - 20\beta)y^{12} \ldots$$

where $0 \leq \beta \leq 154$.

Now we take a generator matrix for $\pi(F_\sigma(C))$ in the form of (4). Since $f < 24$, we have $k_2 = 0$. Hence a generator matrix of $\pi(F_\sigma(C))$ is of the form

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

By the Balance Principle (see Lemma 1), we get $k_1 = 16$. Observe that $\mathcal{A}$ is a doubly-even $[38, 16, d']$ code with $d' \geq 8$. Since $d_\pi = 8$ there is a vector $(u|w) \in \pi(F_\sigma(C))$ with $\mathrm{wt}(u|w) = 8$ and $3\mathrm{wt}(u) + \mathrm{wt}(w) \geq 24$. This implies $\mathrm{wt}(u) = 8$ and $\mathrm{wt}(w) = 0$, hence $d' = 8$.

On the other hand, if $a \in \mathcal{A}^{\perp}$, then there exists a vector $(a|b) \in \pi(F_\sigma(C))$ with $3\mathrm{wt}(a) + \mathrm{wt}(b) \geq 24$ and $\mathrm{wt}(b) \leq 6$. Hence $\mathrm{wt}(a) \geq 6$. Consequently, $\mathcal{A}$ is a doubly-even $[38, 16, 8]$ code with dual distance $d'^{\perp} \geq 6$. Furthermore, $\mathcal{A}$ does not contain a codeword of weight 36 since for $(u|0) \in \pi(F_\sigma(C))$ with $\mathrm{wt}(u) = 36$ we get

$$\mathrm{wt}(\pi^{-1}(u + \mathbf{1}|\mathbf{1})) \leq 6 + 6 < 24.$$

Now let

$$W_{\mathcal{A}}(y) = 1 + A_8 y^8 + A_{12} y^{12} + \ldots + A_{32} y^{32}$$

and

$$W_{\mathcal{A}^\perp}(y) = 1 + A_6^\perp y^6 + A_7^\perp y^7 + \ldots$$

denote the weight enumerators of $\mathcal{A}$ and $\mathcal{A}^\perp$. Using the MacWilliams identity equations and Maple calculations we get

$$A_{12} = 2808 - 6A_8, \ldots, A_{28} = 632 - 6A_8,\ A_{32} = -27 + A_8$$

and

$$A_6^\perp = 4A_8 - 87,\ A_7^\perp = 480 - 8A_8,\ A_8^\perp = 660 + 4A_8,\ A_9^\perp = 1920,\ A_{10}^\perp = 7952 - 24A_8,\ \ldots$$

To finish the proof we also need the weight enumerator

$$W_{\pi(F_\sigma(C))}(y) = \sum A_i^\pi y^i$$

of $\pi(F_\sigma(C))$. Note that $A_8 = A_8^\pi$.

Since $A_7^\perp = 480 - 8A_8 \geq 0$, we obtain $A_8 = A_8^\pi = 44 + 4\beta \leq 60$. Hence $0 \leq \beta \leq 4$ which shows that W_2 is the weight enumerator of $\pi(F_\sigma(C))$.

On the other hand,

$$A_{12}^\pi = A_{(12,0)} + A_{(10,2)} + A_{(8,4)} + A_{(6,6)},$$

where

$$\begin{aligned}
A_{(12,0)} &= A_{12} = 2808 - 6A_8 = 2544 - 26\beta, \\
A_{(10,2)} &= (A_{(10,2)} + A_{(10,6)}) - A_{(10,6)} = A_{10}^\perp - A_{(28,0)} = A_{10}^\perp - A_{28} = 7320 - 18A_8 \\
&= 6528 - 72\beta, \\
A_{(8,4)} &= (A_{(8,4)} + A_{(8,0)}) - A_{(8,0)} = A_8^\perp - A_8 = 660 + 3A_8 = 792 + 12\beta \quad \text{and} \\
A_{(6,6)} &= A_{(32,0)} = A_{32} = -27 + A_8 = 17 + 4\beta.
\end{aligned}$$

It follows $A_{12}^\pi = 9881 - 82\beta$. Computing this coefficient again via $W_2(y)$ we get $A_{12}^\pi = 10241 - 20\beta$, a contradiction. □

So far we have shown that automorphisms of order 3 act fixed point freely on the coordinates of C which completes part a) of Theorem A.

4 Order of the automorphism group and automorphisms of composite order

In this section we prove part b) and c) of Theorem A.

Proposition 7 *Let C be a binary code of length n. Suppose that for every automorphism of C of prime order p the number of p-cycles is not divisible by p and the number f of fixed points satisfies $f < p$. Then $p^2 \nmid |\mathrm{Aut}(C)|$.*

Proof: Suppose that $p^2 \mid |\mathrm{Aut}(C)|$. Thus, by Sylow's Theorem, there exists a subgroup $N \leq \mathrm{Aut}(C)$ with $|N| = p^2$. A group of that order is always abelian. If there is an automorphism, say σ, of order p^2, then the number of p-cycles of σ^p is divisible by p, a contradiction. Thus we may assume that all non-trivial elements in N have order p. In particular, $N = \langle \sigma, \theta \rangle$. Since σ and θ commute σ acts on the orbits of size p of θ. By assumption, the number of such orbits is not divisible by p. Thus σ fixes the elements of at least one orbit of θ, say Ω. It follows that $\theta = \sigma^k$ on Ω for some $k \in \mathbb{N}$. Thus $\theta\sigma^{-k}$, which is not the identity on the n coordinates, has at least p fixed points. This is a contradiction. $\Box$

Applying this in the particular situation of a binary self-dual extremal code of length 120 we get

Proposition 8 *Let C be a binary self-dual code with parameters $[120, 60, 24]$. Then $|\mathrm{Aut}(C)|$ divides $2^a \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 23 \cdot 29$, where $a \in \mathbb{N}_0$.*

Proof: Suppose that $p \mid |\mathrm{Aut}(C)|$, where $p \geq 3$ is a prime. Then, according to (2) and part a) of Theorem A, we have $(c, f) = (40, 0), (24, 0), (17, 1), (6, 6), (5, 5), (4, 4)$. Thus Proposition 7 implies $p^2 \nmid |\mathrm{Aut}(C)|$. $\Box$

Let σ be an automorphism of C of order $p \cdot r$ where p, r are primes. We say that σ is of type $p \cdot r$-$(s_1, s_2, s_3; f)$ if σ has s_1 p-cycles, s_2 r-cycles, s_3 pr-cycles and f fixed points. In particular, $n = s_1 p + s_2 r + s_3 pr + f$. In the special case $p = r$ we write p^2-$(s_1, s_2; f)$ where $n = s_1 p + s_2 p^2 + f$.

Lemma 9 [8] *Let C be a self-dual code and let p, r be different odd primes.*

- *a) If C has an automorphism of type $p \cdot r$-$(s_1, s_2, s_3; f)$, then the automorphism σ^r is of type p-$(s_1 + s_3 r; s_2 r + f)$ and σ^p is of type r-$(s_2 + s_3 p; s_1 p + f)$.*
- *b) If C has an automorphism of type p^2-$(s_1, s_2; f)$, then σ^p is of type p-$(s_2 p; s_1 p + f)$.*

Since by Proposition 7 there are no automorphisms of order p^2 for p an odd prime, the following completes the proof of Theorem A.

Lemma 10 *If σ is an automorphism of a self-dual $[120, 60, 24]$ code C of order $p \cdot r$ where p and r are different odd primes, then the order of σ is $3 \cdot 5$, $3 \cdot 19$ or $5 \cdot 23$ and its cycle structure is given by $3 \cdot 5$-$(0, 0, 8; 0)$, $3 \cdot 19$-$(2, 0, 2; 0)$ or $5 \cdot 23$-$(1, 0, 1; 0)$.*

Proof: Let $3 \leq p < r \leq 29$. In order to prove the Lemma we distinguish three cases.
Case $p = 3$:
In this case σ^r is an automorphism of type 3-$(s_1 + s_3 r; s_2 r + f)$. Thus $s_2 = f = 0$ and $s_1 + s_3 r = 40$, since we proved already that elements of order 3 have no fixed points. Thus

σ^3 is of type r-$(3s_3; 3s_1)$. According to (2), we get $r = 5$, $s_3 = 8$, $s_1 = 0$, or $r = 19$, $s_3 = s_1 = 2$. It follows that σ is of type $3 \cdot 5$-$(0, 0, 8; 0)$ or $3 \cdot 19$-$(2, 0, 2; 0)$.
Case $p = 5$:
Now σ^r is an automorphism of type 5-$(s_1 + s_3r; s_2r + f)$ and therefore $s_2 = f = 0$, $s_1 + s_3r = 24$, since elements of order 5 also have no fixed points. Thus σ^5 is of type r-$(5s_3; 5s_1)$. Looking again at (2), we see that $r = 23$ and $s_3 = s_1 = 1$ is the only possibility. It follows that σ is of type $5 \cdot 23$-$(1, 0, 1; 0)$.
Case $p > 5$:
Now σ^r is an automorphism of type p-$(s_1 + s_3r; s_2r + f)$ and the data in (2) lead to $s_2r + f = 1$, 4, 5 or 6. Since $r \geq 19$ we obtain $s_2 = 0$. Thus σ^p is of type r-$(s_3p; s_1p + f)$ where $s_3p = 4$, 5 or 6, which is not possible as $p > 5$. This proves that there are no possible automorphisms in this case. □

5 The structure of the automorphism group if all involutions act fixed point freely

The first author proved in [3] that involutions of the automorphism group of a binary self-dual extremal code C of length $n = 24m > 24$ permute the n coordinates without fixed points unless $n = 120$, the case we are considering in this paper. In the exceptional case involutions may have no fixed points or exactly 24 points. Throughout this section we assume that all involutions act fixed point freely. In this case Theorem A and the list in (2) show that all automorphisms have a unique cycle structure. This enables us to compute the order of $G = \mathrm{Aut}(C)$ via the Cauchy-Frobenius lemma ([13], 1A.6) which says that

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

is the number of orbits of G on the coordinates of C. Here $\mathrm{Fix}(g)$ denotes the number of fixed points of g. In order to compute t we only need to determine the number of automorphisms of prime order p for $p \geq 7$ since only those have fixed points assuming that involutions are fixed point free.

Let $\tau_p \in G$ of prime order $p \geq 7$. According to Sylow's theorem ([13], Corollary 1.17) the number of Sylow p-subgroups is given by

$$n_p = |G : N_G(\langle \tau_p \rangle)| \equiv 1 \pmod{p}.$$

If $\sigma \in N_G(\langle \tau_p \rangle)$ is an automorphism of prime order $r \neq p$ then $\sigma \tau_p \sigma^{-1} = \tau_p^s$ for some integer $0 \leq s < p$. Hence σ acts on the set $T = \{\Omega_{c+1}, \ldots, \Omega_{c+f}\}$ of fixed points of τ_p. Since $\mathrm{ord}(\sigma|_T) \mid \mathrm{ord}(\sigma) = r$ and $\mathrm{ord}(\sigma|_T) \leq f \leq 6$ (according to Theorem A and the list in (2)), we see that $r = 2$, 3, 5 or $\mathrm{ord}(\sigma|_T) = 1$. Finally the 2-part $|G|_2$ of $|G|$ is bounded by 8 since a Sylow 2-subgroup of G acts regularly on the coordinates in the considered case.

Lemma 11 *We have*

a) $n_{29} = 1,\ 2\cdot 3\cdot 5,\ 2^2\cdot 3\cdot 7\cdot 19,\ 2^3\cdot 3\cdot 23,\ 2^2\cdot 5\cdot 7\cdot 23$ *or* $3\cdot 5\cdot 19\cdot 23$.

b) $n_{23} = 1,\ 2^3\cdot 3,\ 2\cdot 5\cdot 7,\ 2^2\cdot 29,\ 2^3\cdot 5\cdot 19$ *or* $2^3\cdot 5\cdot 7\cdot 29$.

c) $n_{19} = 1,\ 5{\cdot}23,\ 3{\cdot}7{\cdot}29,\ 3{\cdot}5{\cdot}7{\cdot}23{\cdot}29,\ 2{\cdot}29,\ 2{\cdot}5{\cdot}23{\cdot}29,\ 2{\cdot}3{\cdot}5{\cdot}7,\ 2^2{\cdot}5,\ 2^2{\cdot}3{\cdot}5{\cdot}7{\cdot}29,\ 2^3{\cdot}5{\cdot}29$ *or* $2^3\cdot 3\cdot 23$.

Proof: a) First observe that τ_p has exactly $f = 4$ fixed points. Therefore $r = 2$. Hence $n_{29} = \frac{|G|}{2^x\cdot 29} = 2^{a-x}\cdot 3^b\cdot 5^c\cdot 7^d\cdot 19^e\cdot 23^f$. Since $n_{29} \equiv 1 \pmod{29}$ we obtain exactly the six possibilities mentioned in a).
b) In this case we have $f = 5$ and therefore $r = 5$. Hence

$$n_{23} = \frac{|G|}{5^y\cdot 23} = 2^a\cdot 3^b\cdot 5^{c-y}\cdot 7^d\cdot 19^e\cdot 29^g.$$

Since $n_{23} \equiv 1 \pmod{23}$ exactly the six possibilities mentioned in b) may occur.
c) Now $f = 6$ and therefore $r = 2$ or $r = 3$. Hence

$$n_{19} = \frac{|G|}{2^x\cdot 3^z\cdot 19} = 2^{a-x}\cdot 3^{b-z}\cdot 5^c\cdot 7^d\cdot 23^f\cdot 29^g.$$

The congruence $n_{19} \equiv 1 \pmod{19}$ leads to the 11 possibilities in c). $\square$

Lemma 12

a) *If* $29 \mid |G|$ *then* $|G| = 2^a\cdot 29$ *or* $|G| = 2^a\cdot 3\cdot 5\cdot 29$ *where* $0 \le a \le 3$.

b) *If* $23 \mid |G|$ *then* $|G| = 5^c\cdot 23$ *or* $|G| = 2^3\cdot 3\cdot 5^c\cdot 23$ *where* $c = 0, 1$.

c) *If* $19 \mid |G|$ *then* $|G| = 2^a\cdot 3^b\cdot 19$ *or* $|G| = 2^a\cdot 3^b\cdot 5\cdot 19$ *where* $0 \le a \le 3$ *and* $b = 0, 1$.

d) *If* $7 \mid |G|$ *then* $|G| = 7$ *or* $2^3\cdot 7$.

Proof: a) Using Lemma 11, we see that $|G| = 2^a{\cdot}29,\ 2^a{\cdot}3{\cdot}5{\cdot}29,\ 2^a{\cdot}3{\cdot}7{\cdot}19{\cdot}29,\ 2^3{\cdot}3{\cdot}23{\cdot}29,\ 2^a\cdot 5\cdot 7\cdot 23\cdot 29$ or $2^a\cdot 3\cdot 5\cdot 19\cdot 23\cdot 29$. In the last three cases we have $n_{23} = 2^3\cdot 3\cdot 29$, $2^a\cdot 5^{1-y}\cdot 7\cdot 29$, or $2^a\cdot 3\cdot 5^{1-y}\cdot 19\cdot 29$. Since $n_{23} \equiv 1 \pmod{23}$ only $n_{23} = 2^3\cdot 5\cdot 7\cdot 29$ is possible which leads to $|G| = 2^3\cdot 5\cdot 7\cdot 23\cdot 29$. But in this case $n_7 = 2^3\cdot 5\cdot 23\cdot 29 \equiv 3 \pmod 7$, a contradiction. Thus 23 does not divide $|G|$. If $|G| = 2^a\cdot 3\cdot 7\cdot 19\cdot 29$ then $n_{19} = 2^{a-x}{\cdot}3^{1-y}{\cdot}7{\cdot}29$. Looking at the possibilities in Lemma 11 we see that $n_{19} = 3{\cdot}7{\cdot}29$. For n_7 we get $n_7 = 2^a\cdot 3\cdot 19\cdot 29 \equiv 2^a \pmod 7 \equiv 1 \pmod 7$, hence $a = 3$ since $a \ge 2$ in this case.

Applying the Cauchy-Frobenius lemma we obtain

$$\begin{aligned} t &= \tfrac{120+6n_7+6\cdot 18n_{19}+4\cdot 28n_{29}}{2^3\cdot 3\cdot 7\cdot 19\cdot 29} \\ &= \tfrac{120+6\cdot 2^3\cdot 3\cdot 19\cdot 29+6\cdot 18\cdot 3\cdot 7\cdot 29+4\cdot 28\cdot 2^2\cdot 3\cdot 7\cdot 19}{2^3\cdot 3\cdot 7\cdot 19\cdot 29} = \tfrac{7}{2}, \end{aligned}$$

a contradiction. Therefore only the first two cases are possible, namely $|G| = 2^a\cdot 29$ or $2^a\cdot 3\cdot 5\cdot 29$ where $a = 0, 1, 2, 3$.

b) First note that $29 \nmid |G|$ as shown in a). Hence $n_{23} = 1,\ 2^3 \cdot 3,\ 2 \cdot 5 \cdot 7$ or $2^3 \cdot 5 \cdot 19$, by Lemma 11. Thus $|G| = 5^c \cdot 23,\ 2^3 \cdot 3 \cdot 5^c \cdot 23,\ 2 \cdot 5 \cdot 7 \cdot 23$ or $2^3 \cdot 5 \cdot 19 \cdot 23$. In the last case $n_{19} = 2^{3-x} \cdot 5 \cdot 23$ which froces $n_{19} = 5 \cdot 23$. It follows

$$t = \frac{120 + 6 \cdot 18 n_{19} + 5 \cdot 22 n_{23}}{2^3 \cdot 5 \cdot 19 \cdot 23} = \frac{120 + 6 \cdot 18 \cdot 5 \cdot 23 + 5 \cdot 22 \cdot 2^3 \cdot 5 \cdot 19}{2^3 \cdot 5 \cdot 19 \cdot 23} = \frac{11}{2},$$

a contradiction. If $|G| = 2 \cdot 5 \cdot 7 \cdot 23$ then $n_7 = 230 \equiv 6 \pmod 7$, a contradiction again. Thus $|G| = 5^c \cdot 23$ or $2^3 \cdot 3 \cdot 5^c \cdot 23$ where $c = 0, 1$.
c) In this case both 23 and 29 do not divide $|G|$. Thus according to Lemma 11 we have $n_{19} = 1,\ 2 \cdot 3 \cdot 5 \cdot 7$ or $2^2 \cdot 5$. It follows that $|G| = 2^a \cdot 3^b \cdot 19,\ 2^a \cdot 3 \cdot 5 \cdot 7 \cdot 19$ or $2^a \cdot 3^b \cdot 5 \cdot 19$. In the second case we have $n_7 = 2^a \cdot 3 \cdot 5 \cdot 19 \equiv 2^a \cdot 5 \not\equiv 1 \pmod 7$ for $0 \leq a \leq 3$. Thus $|G| = 2^a \cdot 3^b \cdot 19$ or $2^a \cdot 3^b \cdot 5 \cdot 19$ where $a = 0, 1, 2, 3$ and $b = 0, 1$.
d) By a), b) and c) we see that G is a $\{2, 3, 5, 7\}$-group, i.e., the only primes which may occur in the order of G are $2, 3, 5$ and 7. Since an element of order 7 has exactly one fix point we get $n_7 = \frac{|G|}{7}$. If $|G| = 2^a 3^b 5^c 7$ then the Cauchy-Frobenius Lemma yields

$$t = \frac{1}{2^a 3^b 5^c 7}(120 + \sum_{\mathrm{ord}(g)=7} 1) = \frac{1}{2^a 3^b 5^c 7}(120 + 6 n_7) = \frac{120}{2^a 3^b 5^c 7} + \frac{6}{7}$$

and $t \in \mathbb{N}$ forces

$$(a, b, c) = (0, 0, 0), (3, 0, 0), (0, 1, 1), (3, 1, 1).$$

If $(a, b, c) = (0, 1, 1)$ then $|G| = 3 \cdot 5 \cdot 7 = 105$. Using MAGMA we see that there are exactly two groups of order 105, all with $|N_G(\langle \tau_7 \rangle)| = 105 \neq 7$. In the latter case $(a, b, c) = (3, 1, 1)$ we have $|G| = 840$ and MAGMA shows that there are exactly 186 groups of order 840, all with $|N_G(\langle \tau_7 \rangle)| = 105, 840 \neq 7$. Therefore $|G| = 7$ or 56 . □

Lemma 13 *The only nonabelian composition factor which possibly occurs in* $\mathrm{Aut}(C)$ *is the alternating group* A_5.

Proof: Let H be a nonabelian composition factor of G. If G is a $\{2, 3, 5\}$-group then $|G| \mid 2^3 \cdot 3 \cdot 5 = 120$ and H must be isomorphic to A_5. Thus we may assume that $p \mid |G|$ where $p = 7, 19, 23$ or 29. By Lemma 12, we have $|G| \leq 3480$. According to the classification of finite simple nonabelian groups, H must be a group in the following list.

$$\mathrm{A}_5,\ \mathrm{A}_6,\ \mathrm{PSL}(2, 8),\ \mathrm{PSL}(2, 11),\ \mathrm{PSL}(2, 13),\ \mathrm{PSL}(2, 17),\ \mathrm{A}_7,\ \mathrm{PSL}(2, 19).$$

Note that $\mathrm{PSL}(2, 11), \mathrm{PSL}(2, 13)$ and $\mathrm{PSL}(2, 17)$ can not occur since neither $11, 13$ nor 17 divide $|G|$. Furthermore $\mathrm{A}_6, \mathrm{A}_7, \mathrm{PSL}(2, 8), \mathrm{PSL}(2, 19)$ are not possible since $3^2 \nmid |G|$. Thus only the group A_5 is left. □

To sharpen the results of Lemma 12 we need the following fact.

Lemma 14 [2] *The automorphism group of an extremal self-dual code of length* 120 *does not contain elements of order* $2 \cdot 19$ *and* $2 \cdot 29$, *independent whether involutions have fixed points or not.*

Proposition 15 *Let $G = \mathrm{Aut}(C)$ where C is an extremal self-dual code of length 120. Suppose that all involutions of G act fixed point freely. Then we have.*

a) *If $29 \mid |G|$ then $|G| = 2^a \cdot 29$ where $0 \leq a \leq 2$.*

b) *If $23 \mid |G|$ then $|G| = 5^c \cdot 23$ or $|G| = 2^3 \cdot 5^c \cdot 23$ where $c = 0, 1$.*

c) *If $19 \mid |G|$ then $|G| = 2^a \cdot 3^b \cdot 19$ where $0 \leq a, b \leq 1$*

d) *If $7 \mid |G|$ then $|G| = 7$ or $2^3 \cdot 7$.*

e) *If G is a $\{2, 3, 5\}$-group then $|G| \leq 120$.*

Proof: In the proof we use the common notation $\mathrm{O}_p(G)$ for the largest normal p-subgroup of G.
a) By Lemma 12, we may suppose that $|G| = 2^a \cdot 3 \cdot 5 \cdot 29$ where $0 \leq a \leq 3$. If $\mathrm{O}_p(G) \neq 1$ for $p = 3, 5$ or 29 then G contains elements of order $3 \cdot 29$ or $5 \cdot 29$ in contrast to Theorem A, part c). Thus $p = 2$ and there is an element of order $2 \cdot 29$ which contradicts Lemma 14. The only possibility left is that A_5 is a normal subgroup in G according to Lemma 13. In this case we have again an element of order $2 \cdot 29$, hence a contradiction. It follows that $|G| = 2^a \cdot 29$ with $0 \leq a \leq 2$. Note that in case $a = 3$ there is an element of order $2 \cdot 29$.
b) This is part c) of Lemma 12.
c) According to Lemma 12, we first consider the case $|G| = 2^a \cdot 3^b \cdot 19$ with $0 \leq a \leq 3$ and $b = 0, 1$. Suppose that $a = 2$ or $a = 3$. Clearly, $\mathrm{O}_2(G) = 1$ otherwise there is an element of order $2 \cdot 19$ in contrast to Lemma 14. Furthermore $\mathrm{O}_{19}(G) = 1$ otherwise we get the same contradiction. Thus $\mathrm{O}_3(G) \neq 1$ since G is solvable, and we get an element of order $3 \cdot 19$. It follows $n_{19} = 2^x \equiv 1 \pmod{19}$ with $x = 1, 2$, a contradiction. Thus $|G| = 2^a \cdot 3^b \cdot 19$ where $0 \leq a, b \leq 1$.

Now suppose, according to Lemma 12, that $|G| = 2^a \cdot 3^b \cdot 5 \cdot 19$ where $0 \leq a \leq 3$ and $b = 0, 1$. Suppose that $3 \mid |G|$. Clearly, $\mathrm{O}_p(G) = 1$ for $p = 5$ and $p = 19$ since otherwise there exists an element of order $5 \cdot 19$, in contrast to Theorem A. Furthermore $\mathrm{O}_2(G) = 1$ since there are no elements of order $2 \cdot 19$, by Lemma 14. If $\mathrm{O}_3(G) \neq 1$ then G is solvable. Thus there exists a subgroup H of G with $|H| = 15$ (a so-called $\{5, 19\}$-Hall subgroup). But such a group is cyclic, i.e. there is an element of order $5 \cdot 19$, a contradiction to Theorem A again. Finally, if A_5 is involved in $\mathrm{Aut}(C)$ then it must be a normal subgroup of $\mathrm{Aut}(C)$ and elements of order 19 centralize A_5, a contradiction. This shows that $3 \nmid |G|$ in the considered case. Thus $|G| = 2^a \cdot 5 \cdot 19$ and G is solvable. Since $\mathrm{O}_2(G) = 1$ we get an element of order $5 \cdot 19$, a contradiction to Theorem A. In summary, the case $|G| = 2^a \cdot 3^b \cdot 5 \cdot 19$ does not occur. □

Remark 16 a) Lemma 13 and Proposition 15 together show that $\mathrm{Aut}(C)$ is solvable if a prime $p \geq 7$ divides $|G|$.
b) The largest group occurring in Proposition 15 has order 920.
c) In case a) the Sylow 29-subgroup must be normal, in case c) the Sylow 2-subgroup is elementary abelian and normal.

Remark 17 In this section we assumed that all involutions do not have foxed points. To prove that this is always true seems to be quite challenging since ideas beyond those which are used in [3] are missing.

References

[1] M. Borello, *The automorphism group of an extremal* $[72, 36, 16]$ *code does not contain an element of order* 6, IEEE Trans. Inform. Theory 58 (2012) 7240-7245.

[2] M. Borello and W. Willems, *Automorphisms of order* $2p$ *in a binary self-dual extremal code of length a multiple of* 24, to appear IEEE Trans. Inf. Theory, `arXiv:1209.5071v1`.

[3] 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.

[4] J.H. Conway and N.J.A. Sloane, *A New Upper Bound on the Minimal Distance of Self-Dual Codes*, IEEE Trans. Inform. Theory 36 (1990) 1319-1333.

[5] J. de la Cruz and W. Willems, *On extremal self-dual codes of length* 96, IEEE Trans. Inform. Theory 57 (2011) 6820-6823.

[6] J. de la Cruz, *On extremal self-dual codes of length* 120, `arXiv:1302.0033v1`. to appear

[7] J. de la Cruz, *Über die Automorphismengruppe extremaler Codes der Längen* 96 *und* 120, PhD Thesis, Magdeburg, 2012. Online `http://edoc2.bibliothek.uni-halle.de/hs/content/titleinfo/20281`

[8] R. Dontcheva, A.J. van Zanten, and S. Dodunekov, *Binary Self-Dual Codes With Automorphisms of Composite Order*, IEEE Trans. Inform. Theory 50 (2004) 311-318.

[9] M. El-Khamy and R. J. McEliece, *The partition weight enumerator of MDS codes and its applications*, International Symposium on Information Theory 2005, `arXiv.org/pdf/cs.IT/0505054.pdf`.

[10] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, `http://www.codetables.de`.

[11] 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 (2003) 53-59.

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

[13] I.M. Isaacs, Finite group theory, Graduate Studies in Mathematics 92, AMS, Providence 2008.

[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] J. Simonis, *MacWilliams identities and coordinate partitions*, Linear Algebra Appl. 216 (1995) 81-91.