Automorphisms of Order $2p$ in Binary Self-Dual Extremal Codes of Length a Multiple of 24

Martino Borello and Wolfgang Willems, Member, IEEE

Abstract—Let $C$ be a binary self-dual code with an automorphism $g$ of order $2p$, where $p$ is an odd prime, such that $g^p$ is a fixed point free involution. If $C$ is extremal of length a multiple of 24, all the involutions are fixed point free, except the Golay Code and eventually putative codes of length 120. Connecting module theoretical properties of a self-dual code $C$ with coding theoretical ones of the subcode $C\langle g^p \rangle$ which consists of the set of fixed points of $g^p$, we prove that $C$ is a projective $F_2 \langle g \rangle$-module if and only if a natural projection of $C\langle g^p \rangle$ is a self-dual code. We then discuss easy-to-handle criteria to decide if $C$ is projective or not. As an application, we consider in the last part extremal self-dual codes of length 120, proving that their automorphism group does not contain elements of order 38 and 58.

Index Terms—Automorphism group, self-dual codes.

I. INTRODUCTION

Binary self-dual extremal codes of length a multiple of 24 are binary self-dual codes with parameters $[24m, 12m, 4m + 4]$. They are interesting for various algebraic and geometric reasons; for example, they are doubly even [14] and all codewords of a fixed given nontrivial weight support a 5-design [1]. Very little is known about this family of codes: for $m = 1$, we have the Golay Code $G_{24}$, and for $m = 2$ there is the extended quadratic residue code $XQR_{48}$, but no other examples are known so far.

A classical way of approaching the study of such codes is through the investigation of their automorphism group. In this paper, we focus our attention to automorphisms of order $2p$, where $p$ is an odd prime. There are elements of this type in the automorphism group of $G_{24}$ and $XQR_{48}$, while it was recently proved [2] that for $m = 3$, no automorphisms of order 2p occur. The problem is totally open for $m > 3$. It is known [5] that for $m \not\equiv \{1, 5\}$, the involutions are fixed point free. So we will restrict our study to those automorphisms $g$ of order 2p whose $p$-power acts fixed point freely.

In the first part of this paper, we connect module theoretical properties of a self-dual code $C$ with coding theoretical ones of the subcode $C\langle g^p \rangle$ which consists of the fixed points of $g^p$. More precisely, we prove in Theorem 1 that $C$ is a projective $F_2 \langle g \rangle$-module if and only if a natural projection of $C\langle g^p \rangle$ is a self-dual code. In the second part, i.e., Section IV, we apply these results to the case $m = 5$. In particular, we prove that there are no automorphisms of order 2·19 and 2·29. All computations of the last part are carried out with Magma[6].

II. PRELIMINARIES

From now on, a code always means a binary linear code and $K$ always denotes the field $F_2$ with two elements. Let $C$ be a code and let $g \in \text{Aut}(C)$. We denote by $C(g) = \{c \in C \mid g^i c = c\}$ the subcode of $C$ consisting of all codewords which are fixed by $g$. It is easy to see that a codeword $c = (c_1, \ldots, c_n)$ is fixed by $g$ if and only if $c_i = c_{3i}$ for every $i \in \{1, \ldots, n\}$, i.e., if and only if $c$ is constant on the orbits of $g$.

Definition 1: For an odd prime $p$, let $s(p)$ denote the smallest $s \in \mathbb{N}$ such that $p \cdot 2^s - 1$. Note that $s(p)$ is the multiplicative order of 2 in $\mathbb{F}_p^*$.

The next lemma is a well-known fact in modular representation theory. For those who are not familiar with representation theory, we recall here some of the notions we need. Let $G$ be a group. A projective indecomposable $KG$-module is a direct summand $W$ of the group algebra $KG$ which cannot be written as $W = W' \oplus W''$ with $KG$-modules $W' \neq \emptyset$. Such a module $W$ has a unique irreducible submodule, say $V$, called the socle of $W$, and a unique irreducible factor module which is isomorphic to $V$. We call $W$, which is (up to isomorphism) uniquely determined by $V$, the projective cover of $V$. Projective covers for irreducible modules always exist (actually they exist for any finite-dimensional $KG$-module). For these facts and some basics in modular representation theory (and only those are needed in this paper), the reader is referred to [12, Ch. VII].

Finally, note that the action of $G$ on a module is always from the right in this paper.

Lemma 1: Let $\nu = \frac{p - 1}{2}$, where $p$ is an odd prime, and let $G = \langle g \rangle$, a cyclic group of order $2p$. Then, we have the following.

a) There are $1 + \nu$ irreducible $KG$-modules $V_0, V_1, \ldots, V_\nu$, where $V_0 = K$ (the trivial module) and $d \cdot m_i = s(p)$ for $i \in \{1, \ldots, \nu\}$.

b) For $i = 0, \ldots, \nu$, the projective indecomposable cover $W_i$ of $V_i$ is a nonsplit extension $W_i = V_i \oplus V_i$ by $V_i$.

Furthermore

$$KG = W_0 \oplus W_1 \oplus \cdots \oplus W_\nu.$$ 

In order to understand codes with automorphisms of order $2p$, we need the following result on self-dual modules which
improves [13, Proposition 3.1]. Recall that a $KG$-module $V$ is self-dual if $V \cong V^*$ (as $KG$-modules). Here, $g \in G$ acts on $V^* = \text{Hom}_K(V, K)$ by

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

where $f \in V^*$, $g \in G$, and $v \in V$.

**Proposition 1:** Let $G = \langle g \rangle$ be a cyclic group of odd prime order $p$.

a) If $s(p)$ is even, then all irreducible $KG$-modules are self-dual.

b) If $s(p)$ is odd, then the trivial module is the only self-dual irreducible $KG$-module.

**Proof:**

a) Let $s(p) = 2t$ and let $E = F_{2^t}$ be the extension field of $K = \mathbb{F}_p$ of degree $2t$. Furthermore, let $W$ be an irreducible nontrivial $KG$-module. In particular, $W$ has dimension $2t$. By Theorem 1.18 and Lemma 1.15 in [12, Ch. VII], we have

$$W \otimes_K E = \oplus_{\alpha \in \text{Gal}(E/K)} V^\alpha$$

where $V$ is an irreducible $E$-$G$-module and $V^\alpha$ is the $\alpha$-conjugate module of $V$. The action of $g \in G$ on $V^\alpha$ is given by the matrix $(a_{ij}(g)^\alpha)$ if $g$ acts via the matrix $(a_{ij}(g))$ on $V$. Since $p | (2^t + 1)(2^t - 1)$ we get $p | 2^t + 1$. Clearly, the Galois group $\text{Gal}(E/K)$ of $E$ over $K$ (i.e., the group of field automorphisms of $E$ which leave the subfield $K$ elementwise fixed) consists of all automorphisms of the form $x \mapsto x^2$ where $0 \leq k \leq 2t - 1$ (see [11, Sec. 3.6]).

If $V = \langle \psi \rangle$, then $v \psi = \epsilon \psi$, where $\epsilon$ is a nontrivial $p$th root of unity in $E$. Since $p | 2^t + 1$, we obtain $\epsilon^{2^t + 1} = 1$; hence, $\epsilon^2 = \epsilon^{-1}$. Thus, there is an $\alpha \in \text{Gal}(E/K)$ such that $V^\alpha \cong V^\psi$ and (1) implies $W \cong W^\psi$.

b) Now let $s(p) = t$ be odd. As above, the irreducible module $W$ is self-dual if and only if $V^\alpha \cong V^\psi$ for some $\alpha \in \text{Gal}(F_{2^t}/K)$, or equivalently if and only if $\epsilon^\alpha = \epsilon^{-1}$. Suppose that such an $\alpha$ exists. Then, we may write $\epsilon^\alpha = \epsilon^2k$ where $0 \leq k \leq t - 1$. Hence, $\epsilon^{2k} = \epsilon^{-1}$ for some $0 \leq k \leq t - 1$, and therefore, $2k \equiv -1 \mod p$. Now $2^{2k} \equiv 1 \mod p$ forces $t = 2k$. Since $t$ is odd, we get $t \leq t - 1$, a contradiction.

**Remark 1:** According to [13, Lemma 3.5], we have $s(p)$ even if $p \equiv 3 \mod 8$ and $s(p)$ odd if $p \equiv -1 \mod 8$.

**Remark 2:** Since $KG \cong KG^*$ (see [12, Ch. VII, Lemma 8.23]), Lemma 1 and Proposition 1 imply the following.

a) If $s(p)$ is even, then

$$KG = W_0 \oplus W_1 \oplus \cdots \oplus W_\nu$$

with $W_i \cong W_i^*$ for all $i \in \{0, \ldots, \nu\}$.

b) If $s(p)$ is odd, then $\nu$ is even (put $\nu = 2t$) and

$$KG = W_0 \oplus W_1 \oplus \cdots \oplus W_{2t}$$

with $W_0 \cong W_0^*$ and $W_i \cong W_i^*$ for all $i \in \{1, \ldots, t\}$.

**III. AUTOMORPHISMS OF ORDER 2p IN SELF-DUAL CODES**

Throughout this section, let $C$ be a self-dual code of length $n$. In particular, $n$ is even. Suppose that $g \in \text{Aut}(C)$ is of order $2p$, where $p$ is an odd prime. Furthermore, suppose that the involution $g = g^p$ acts fix point freely on the $n$ coordinates. Without loss of generality, we may assume that $h = g^p = \{1, 2\} \cup \{3, 4\} \cup \{n - 1, n\}$.

We consider the maps $\pi = \pi_2 : C(h) \to K^\frac{n}{2}$, where

$$(c_1, c_2, c_3, \ldots, c_\frac{n}{2}) \to \{c_1, c_2, \ldots, c_\frac{n}{2}\}$$

and $\phi : C \to K^\frac{n}{2}$, where

$$(c_1, c_2, \ldots, c_{n-1}, c_n) \mapsto \{c_1 + c_2, \ldots, c_{n-1} + c_n\}.$$
whether $\pi(C(h))$ is self-dual or not. For completeness, we treat both cases $n \equiv 2 \mod 4$ and $n \equiv 0 \mod 4$.

Since $h$ acts fixed point freely, $g$ has $x \ 2p$-cycles and $w \ 2$-cycles, with

$$n = 2px + 2w.$$  

(2)

Thus, as a $K\langle g \rangle$-module, we have the decomposition

$$K^n = K\langle g \rangle \oplus \cdots \oplus K\langle g \rangle \oplus K(h) \oplus \cdots \oplus K(h).$$

Using Lemma 1 and $V_0 \cong K$, we get

$$K^n = \bigoplus_{y \text{ times}} V_0 \oplus \bigoplus_{x+w \text{ times}} V_0 \oplus \bigoplus_{y \text{ times}} V_0 \oplus \bigoplus_{z \text{ times}} V_0.$$ 

The action of $\langle g \rangle$ on $K^n$ and the self-duality of $C$ restrict the possibilities for $C$ as a subspace of $K^n$.

More precisely, we have the following.

**Proposition 2:** As a $K\langle g \rangle$-module, the code $C$ has the following structure:

$$C = \bigoplus_{y_0 \text{ times}} V_0 \oplus \bigoplus_{x \text{ times}} V_0 \oplus \bigoplus_{y \text{ times}} V_0 \oplus \bigoplus_{z \text{ times}} V_0 \oplus \bigoplus_{y \text{ times}} V_0 \oplus \bigoplus_{z \text{ times}} V_0 \oplus \cdots$$

where

1) $2y_0 + z_0 = x + w$.

2a) $2y_i + z_i = x$ for all $i \in \{1, \ldots, \nu\}$, if $s(p)$ is even, and

2b) $z_i = 2z_i$ and $y_i + y_{2i} + z_i = x$ for all $i \in \{1, \ldots, t\}$, if $s(p)$ is odd.

**Proof:** Since $C = C^\perp$, we see by a proof similar to that of [15, Proposition 2.3] that $K^n/C \cong C^\perp$. The conditions on the multiplicities are an easy consequence of this fact. Let us prove, for example, part 2b): if

$$C = \bigoplus_{y_0 \text{ times}} V_0 \oplus \bigoplus_{x \text{ times}} V_0 \oplus \bigoplus_{y \text{ times}} V_0 \oplus \bigoplus_{z \text{ times}} V_0 \oplus \cdots$$

then

$$K^n/C = \bigoplus_{x - z_i - y_i \text{ times}} V_i \oplus \bigoplus_{z_i \text{ times}} V_i \oplus \bigoplus_{y_i \text{ times}} V_i \oplus \bigoplus_{z_i \text{ times}} V_i \oplus \cdots$$

and since $V_i \cong V_2$,

$$C^\perp = \bigoplus_{y \text{ times}} V_0 \oplus \bigoplus_{x \text{ times}} V_0 \oplus \bigoplus_{y \text{ times}} V_0 \oplus \bigoplus_{z \text{ times}} V_0 \oplus \cdots$$

Thus, $z_i = 2z_i$ and $x - z_i - y_i = y_i$.

Proposition 2 implies that

$$\phi(C)^\perp = \pi(C(h)) = \pi \left( \bigoplus_{i=0}^{\nu} V_i \oplus \cdots \oplus V_i \right).$$

(3)

Since $\ker \phi = C(h)$, we furthermore have

$$\phi(C) \cong C'/\ker \phi \cong \bigoplus_{i=0}^{\nu} V_i \oplus \cdots \oplus V_i$$

which leads to

$$\phi(C)^\perp / \phi(C) \cong \bigoplus_{i=0}^{\nu} V_i \oplus \cdots \oplus V_i.$$ 

Taking dimensions, we get

$$\dim \phi(C)^\perp / \phi(C) = z_0 + s(p) \left( \sum_{i=1}^{\nu} z_i \right).$$

(4)

**Proposition 3:** With the notations used in Proposition 2, we have

a) $x \equiv w \mod 2$, if $n \equiv 0 \mod 4$,

b) $x \not\equiv w \mod 2$, if $n \equiv 2 \mod 4$.

Furthermore, if $s(p)$ is even, then

$$x \equiv z_1 \equiv \cdots \equiv z_\nu \mod 2.$$ 

**Proof:** a) and b) follow immediately from (2). The last fact is a consequence of $2y_i + z_i = x$, if $s(p)$ is even, which is stated in Proposition 2.

**Corollary 1:**

a) $\phi(C)^\perp / \phi(C)$ is of even dimension, if $n \equiv 0 \mod 4$,

b) $\phi(C)^\perp / \phi(C)$ is of odd dimension, if $n \equiv 2 \mod 4$.

**Proof:** First note that $s(p) \sum_{i=1}^{\nu} z_i \equiv 0 \mod 2$ whatever the parity of $s(p)$ is. In case $s(p)$ is odd, this follows from $z_i = z_i$ for $i \in \{1, \ldots, t \}$ (see Proposition 2). Furthermore, $z_0 = x + w \mod 2$; hence, $z_0$ is even if $4 \mid n$, and $z_0$ is odd if $n \equiv 2 \mod 4$, according to Proposition 3. Thus, (4) yields

$$\dim \phi(C)^\perp / \phi(C) \equiv z_0 \equiv 0 \mod 2, \text{ if } n \equiv 0 \mod 4$$
and
\[ \dim \phi(C) / \phi(C) \equiv z_0 \equiv 1 \mod 2, \text{ if } n \equiv 2 \mod 4. \]

Corollary 2: Let \( n \equiv 0 \mod 4 \) and let \( s(p) \) be even. If \( w \) is odd, then
\[ \dim C(h) = \dim \pi(C(h)) \geq \frac{n}{4} + \frac{s(p)\nu}{2} = \frac{n}{4} + \frac{p-1}{2}. \]

In particular, \( \phi(C) < \phi(C)^\perp \).

Proof: By Proposition 3, the condition 4 \mid n forces that \( w \) and \( x \) have the same parity. Thus, \( w \) odd implies that \( x \) is odd, and by Proposition 2, we get \( z_i > 1 \) for \( i = 1, \ldots, \nu \). Since
\[ \phi(C) \leq \phi(C)^\perp - \pi(C(h)) \leq K^\perp, \]
we have
\[ \dim \pi(C(h)) \geq \frac{n}{4} + \frac{1}{2} \dim \phi(C)^\perp / \phi(C). \]

Therefore, according to (4)
\[ \dim C(h) - \dim \pi(C(h)) \geq \frac{n}{4} + \frac{s(p)\nu}{2} - \frac{n}{4} - \frac{p-1}{2}. \]

Remark 5: We may ask whether the converse of Corollary 2 holds true; i.e., does \( \phi(C) < \phi(C)^\perp \) always implies that \( w \) is odd? This is not true. For instance, there exist self-dual \([36, 18, 8]\) codes and automorphisms of order 6 (note that \( s_2(3) \) is even) for which \( \pi(C(h)) \) is not self-dual, but \( w \) is even.

Corollary 3: Let \( n \equiv 0 \mod 4 \) and let \( s(p) \) be even. If \( g \) has an odd number of cycles of order 2, \( C \) is not projective as a \( K(g) \)-module.

Proof: If the number of 2-cycles of \( g \) is odd, then \( w \) is odd. Thus, by Corollary 2 and Theorem 1, the assertion follows.

To state further results, we need the following notation about the structure of the automorphisms.

Definition 2: We say that an automorphism of prime order \( p \) of a code is of type \( p-(\alpha, \beta) \) if it has \( \alpha \) \( p \)-cycles and \( \beta \) fixed points. Furthermore, an automorphism of order \( 2p \) is of type \( 2p-(\alpha, \beta, \gamma, \delta) \) if it has \( \alpha \) \( 2 \)-cycles, \( \beta \) \( p \)-cycles, \( \gamma \) \( 2p \)-cycles, and \( \delta \) fixed points.

Since \( \text{Aut}(C) \leq S_n \), the largest possible prime which may occur as the order of an automorphism of a self-dual code of length \( n \) is \( p = n - 1 \). If \( n \equiv 0 \mod 8 \), then \( s(p) \) is odd (see Remark 1). Obviously, in this case, we cannot have an automorphism of order \( 2p \).

Let \( C \) be an extremal self-dual code of length \( n \geq 48 \). According to [4, Th. 7], an automorphism of type \( p-(\alpha, \beta) \) with \( p > 5 \) satisfies \( \alpha \geq \beta \). Hence, the second largest possible prime \( p \) satisfies \( n = 2p + 2 \).

Corollary 4: Let \( C \) be a self-dual code of length \( n = 2p + 2 \), where \( p \) is an odd prime, and minimum distance is greater than 4. Suppose that involutions in \( \text{Aut}(C) \) are fixed point free. If \( s(p) \) is even, then \( \text{Aut}(C) \) does not contain an element of order \( 2p \).

In case \( C \) is doubly even, the condition \( s(p) \) even may be replaced by the condition \( p \neq -1 \mod 8 \).

Proof: Suppose that \( g \) is an automorphism of order \( 2p \). Thus, \( g \) has a cycle of length \( 2p \) and one of length 2. As above let \( h = g^p \). By Corollary 2, we get
\[ \dim \pi(C(h)) \geq \frac{n}{4} + \frac{p-1}{2} = p. \]

Since \( \pi(C(h)) \leq K^\perp = K^{p+1} \), we see that \( \pi(C(h)) \) has minimum distance 1 or 2, a contradiction.

In case that \( C \) is doubly even, we only have to show that \( p \equiv 1 \mod 8 \) does not occur (see Remark 1). If \( p \equiv 1 \mod 8 \), then \( n = 2p + 2 + 4 \equiv 0 \mod 8 \), contradicting the Theorem of Gleason (see [11, Corollary 9.2.2]).

Corollary 5: Let \( C \) be an extremal self-dual code of length \( n = 24m \). Let \( g \in \text{Aut}(C) \) be an element of type \( 2p-(w, 0, x; 0) \).

If \( s(p) \) is even and \( w \) is odd, then \( p \leq \frac{n}{4} - 1 \).

Proof: By Corollary 2, \( \pi(C(h)) \) has parameters \([12m, \geq 6m + \frac{m-1}{2}, \geq 2m + 2]\). According to the Griesmer bound (see [11, Th. 2.7.4]), we have
\[ 12m \geq \sum_{i=0}^{6m+\frac{m-1}{2}} \left[ \frac{2m+2}{2^i} \right]. \]

This implies \( p < 6m - 1 - \frac{9}{4} \).

Clearly, the estimation in Corollary 5 is very crude for \( m \) large. For instance, if \( m = 5 \), the statement in Corollary 5 leads to \( p \leq 29 \), but computing all terms in the sum shows that \( p < 23 \).

IV. APPLICATION TO EXTREMAL SELF-DUAL CODES OF LENGTH 120

From now on, \( C \) is supposed to be a self-dual \([120, 60, 24]\) code. The following (see [7]) is the state of the art about the automorphisms of \( C \).

Automorphisms of odd prime order which may occur in \( \text{Aut}(C) \) are of type \( 29-(4, 4), 23-(5, 5), 19-(6, 6), 17-(7, 1), 5-(24, 0), \) or \( 3-(40, 0) \). Automorphisms of order 2 can only be of type \( 2-(48, 24) \) or \( 2-(60, 0) \). Automorphisms of possible composite odd order are of type \( 3 \cdot 5-(0, 0, 8; 0), 3 \cdot 19-(2, 0; 2; 0), \) or \( 5 \cdot 23-(1, 0, 1, 0) \).

Thus, we may ask about elements \( g \in \text{Aut}(C) \) of order \( 2p \), where \( p \) is an odd prime. Note that the involution \( h = g^p \) has no or exactly 24 fixed points, by [5].

Lemma 2: If the involution \( h \) has no fixed points, then \( g \) is of type
- \( 2 \cdot 29-(2, 0, 2; 0) \),
- \( 2 \cdot 19-(3, 0, 3; 0) \),
- \( 2 \cdot 5-(0, 0, 12; 0) \),
- \( 4 \) or \( 2 \cdot 3-(0, 0, 20; 0) \).

If \( h \) has 24 fixed points, then \( g \) is of type
- \( 2 \cdot 23-(2, 1, 2; 1) \),
- \( 2 \) or \( 2 \cdot 3-(0, 8, 16; 0) \).

Note that \( \text{Aut}(C) \) does not contain elements of order 2 · 7.

Proof: The proof is straightforward by considering the cycle structures using [7].
The above cycle structures show that only elements of order \(2 \cdot 19\) satisfy the hypothesis of Corollary 2. In this case, \(s(19)\) is even, and so we have

\[
\dim C(g^{19}) \geq \frac{120}{4} + \frac{19 - 1}{2} = 39.
\]

Thus, \(\pi_2(C(g^{19}))\) is a \([60, \geq 39, \geq 12]\) code. According to Grassl’s list [8], a \([60, \geq 39]\) code has minimum distance at most 10. Therefore, we can state the following.

**Proposition 4:** The automorphism group of an extremal self-dual \([120, 60, 24]\) code does not contain elements of order 38.

Next we consider automorphisms of order 58. By Lemma 2, we know that \(g\) is of type \(2 : 29\)\((2, 0, 2; 0)\). Therefore, \(g^2\) is of type \(29\{-4, 4\}\) and \(g^{29}\) is of type \(2\{-60, 0\}\). Thus, without loss of generality, we may assume that

\[
g^2 = (1, \ldots, 29)(30, \ldots, 58)(59, \ldots, 87)(88, \ldots, 116)
\]

and

\[
g^{29} = (1, 30) \ldots (59, 88) \ldots (117, 118)(119, 120).
\]

If \(\pi_{29} : C(g^2) \to F_2^5\) is defined by

\[
(v_1, \ldots, v_{120}) \mapsto (v_1, v_{30}, v_{59}, v_{88}, v_{117}, v_{118}, v_{119}, v_{120})
\]

then \(\pi_{29}(C(g^{29}))\) is a self-dual \([8, 4]\) code according to [10], and clearly, the minimum distance must be greater than or equal to 4, since \(C\) is doubly even. It is well known that, up to equivalence, the only code with such parameters is the extended Hamming code \(H_{13}\).

According to Lemma 1, the structure of the ambient space \(K_{120}\), viewed as a module for the group \(g\), is as follows:

\[
K_{120} = K K K K K V V \oplus V V
\]

where \(\dim V = 28\). Since \(C(g^2)\) has dimension 4, the code \(C(g) = (C(g^2))(g^{29})\) has dimension at least 2. By calculations, we verify that

\[
\dim((\pi_{29}(A))(g)) \leq 2
\]

for every \(A \in H_{120}^{29}\), which denotes the set of all self-dual \([8, 4, 4]\) codes. Note that there are only a few computations since \(H_{120}^{29} = \frac{[S_5]}{\text{Aut}[S_5]} = 30\). Thus, \(\dim C(g) = 2\) and there are only two possible structures for \(C\), namely

a) \(C = K K \ominus V \oplus V\) or

b) \(C = K K K K K V\).

Next, we look at \(C(g^{29})\) which may be written as \(C(g^{29}) = B \otimes \{1, 1\}\), where \(B = \pi_2(C(g^{29}))\) is a \([60, \geq 30; \geq 12]\) code. In case a), we have \(\dim B = 58\), a contradiction. Thus, case b) occurs. According to Theorem 1, \(C\) is projective and \(B\) is a self-dual \([60, 30, 12]\) code. Furthermore, \(B\) has an automorphism of type \(29\{-2, 2\}\).

**Proposition 5:** Every self-dual \([60, 30, 12]\) code \(B\) with an automorphism of type \(29\{-2, 2\}\) is bordered double-circulant. There are (up to equivalence) three such codes.

**Proof:** We can easily determine the submodule of \(B\) fixed by the given automorphism and then do an exhaustive search with Magma on its complement in \(K^{(d)}\) (following the methods described in [10] and considering the complement as a vector space over \(F_{2^d}\)). In fact, it turns out that \(B\) is equivalent to one of the three bordered double-circulant singly even codes of length 60 classified by Harada et al. [9].

It is computationally easy to check that there are exactly 14 conjugacy classes of elements of type \(29\{-2, 2\}\) in \(\text{Aut}(B)\) for each of the three possibilities for \(B\).

Using this, we are able to do an exhaustive search for \(C\) along the methods used in [2]. Without repeating all the details, we just recall the two main steps of the search. First, we determine a set, say \(\mathcal{L}\), such that there exists a \(t \in S_{120}\) and \(L \in \mathcal{L}\) such that \((C(g^2) + C(g^{29}))t = L\) and \(g^t = g\). It turns out that \(|\mathcal{L}| = 42\). In the second step, we construct all possible codes \(C\) from the knowledge of its socle as in [2, Sec. VI]. By checking the minimum distance, we see that in all cases the codes are not extremal which proves the following.

**Proposition 6:** The automorphism group of an extremal self-dual \([120, 60, 24]\) code does not contain elements of order 58.

**Acknowledgment**

The first author likes to express his gratitude to his supervisors F. Dalla Volta and M. Sala. Both authors are indebted to the Dipartimento di Matematica e Applicazioni at Milano and the Institut für Algebra und Geometrie at Magdeburg for hospitality and excellent working conditions, while this paper has mainly been written. Laboratorio di Matematica Industriale e Crittografia di Trento deserves thanks for the help in the computational part.

**References**

[1] E. F. Assmuss and H. F. Mattson, “New 5-designs,” *J. Combin. Theory*, vol. 6, pp. 122–151, 1969.

[2] M. Borello, “The automorphism group of a self-dual \(72, 35, 16\) binary code does not contain elements of order 6,” *IEEE Trans. Inf. Theory*, vol. 58, no. 12, pp. 7240–7245, Dec. 2012.

[3] S. Bouyuklieva, “A method for constructing self-dual codes with an automorphism of order 2,” *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 496–504, Mar. 2000.

[4] S. Bouyuklieva, A. Malevich, and W. Willems, “Automorphisms of extremal self-dual codes,” *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2091–2096, May 2010.

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

[6] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system I: The user language,” *J. Symbol. Comput.*, vol. 24, pp. 235–265, 1997.

[7] J. de la Cruz, “Über die Automorphismengruppe Extremaler Codes der Längen 96 und 120,” Ph.D. dissertation, Otto-von-Guericke Univ. Magdeburg, Magdeburg, Germany, 2012.

[8] M. Grassl, Bounds on the Minimum Distance of Linear Codes and Quantum Codes 2012 [Online]. Available: www.codetables.de

[9] M. Harada, T. A. Gulliver, and H. Kaneta, “Classification of extremal double-circulant self-dual codes of length up to 62,” *Discrete Math.*, vol. 188, pp. 127–136, 1998.

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

[11] W. C. Huffman, and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[12] B. Huppert and N. Blackburn, *Finite Groups II*. New York, NY, USA: Springer, 1982.
[13] C. Martínez-Pérez and W. Willems, “Self-dual codes and modules of finite groups in characteristic two,” IEEE Trans. Inf. Theory, vol. 50, no. 8, pp. 67–78, Aug. 2004.

[14] E. M. Rains, “Shadow bounds for self-dual codes,” IEEE Trans. Inf. Theory, vol. 44, no. 1, pp. 134–139, Jan. 1998.

[15] W. Willems, “A note on self-dual group codes,” IEEE Trans. Inf. Theory, vol. 48, no. 12, pp. 3107–3109, Dec. 2002.

Martino Borello received the master’s degree in 2010 from Università degli Studi di Milano. Since 2011 he has been a Ph.D. student in Università degli Studi di Milano Bicocca. His primary research interest is algebraic coding theory.

Wolfgang Willems (M’00) received the Diploma in 1974 and the Ph.D. 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, University of Mainz. During 1986–1987 and 1989–1991, he was a Visiting Professor at the University of Essen, Germany, and the Institute of Experimental Mathematics, Essen. In 1996, he was an Acting Professor at the Otto-von-Guericke University, Magdeburg, Germany. Since 1998, he has been a Professor for “Pure Mathematics” at the University of Magdeburg and since 2010, also Professor Honorario at the Universidad del Norte, Barranquilla, Colombia. His primary research interests are algebraic coding theory and representation theory of finite groups.