On extremal self-dual ternary codes of length 48

Gabriele Nebe
Lehrstuhl D für Mathematik, RWTH Aachen University
52056 Aachen, Germany
nebe@math.rwth-aachen.de

Abstract. All extremal ternary codes of length 48 that have some automorphism of prime order \( p \geq 5 \) are equivalent to one of the two known codes, the Pless code or the extended quadratic residue code.

Keywords: extremal self-dual code, automorphism group
MSC: primary: 94B05

1 Introduction.

The notion of an extremal code has been introduced in [8]. As Andrew Gleason [4] remarks one may use invariance properties of the weight enumerator of a self-dual code to deduce upper bounds on the minimum distance. Extremal codes are self-dual codes that achieve these bounds. The most wanted extremal code is a binary self-dual doubly even code of length 72 and minimum distance 16. One frequently used strategy is to classify extremal codes with a given automorphism, see [6] and [3] for the first papers on this subject.

Ternary codes have been studied in [7]. The minimum distance \( d(C) := \min\{\text{wt}(c) \mid 0 \neq c \in C\} \) of a self-dual ternary code \( C = C^\perp \leq \mathbb{F}_3^n \) of length \( n \) is bounded by

\[
d(C) \leq 3\lfloor \frac{n}{12} \rfloor + 3.
\]

Codes achieving equality are called extremal. Of particular interest are extremal ternary codes of length a multiple of 12. There exists a unique extremal code of length 12 (the extended ternary Golay code), two extremal codes of length 24 (the extended quadratic residue code \( Q_{24} := QR(23, 3) \) and the Pless code \( P_{24} \)). For length 36, the Pless code yields one example of an extremal code. [7] shows that this is the only code with an automorphism of prime order \( p \geq 5 \), a complete classification is yet unknown. The present paper investigates the extremal codes of length 48. There are two such codes known, the extended quadratic residue code \( Q_{48} \) and the Pless code \( P_{48} \). The computer calculations described in this paper show that these two codes are the only extremal ternary codes \( C \) of length 48 for which the order of the automorphism group is divisible by some prime \( p \geq 5 \). Theoretical arguments exclude all types of automorphisms that do not occur for the two known examples.
2 Automorphisms of codes.

Let $\mathbb{F}$ be some finite field, $\mathbb{F}^*$ its multiplicative group. For any monomial transformation $\sigma \in \text{Mon}_n(\mathbb{F}) := \mathbb{F}^* \wr S_n$, the image $\pi(\sigma) \in S_n$ is called the permutational part of $\sigma$. Then $\sigma$ has a unique expression as

$$\sigma = \text{diag}(\alpha_1, \ldots, \alpha_n)\pi(\sigma) = m(\sigma)\pi(\sigma)$$

and $m(\sigma)$ is called the monomial part of $\sigma$. For a code $C \leq \mathbb{F}^n$ we let

$$\text{Mon}(C) := \{ \sigma \in \text{Mon}_n(\mathbb{F}) \mid \sigma(C) = C \}$$

be the full monomial automorphism group of $C$.

We call a code $C \leq \mathbb{F}^n$ an orthogonal direct sum, if there are codes $C_i \leq \mathbb{F}^{n_i}$ $(1 \leq i \leq s > 1)$ of length $n_i$ such that

$$C \sim \bigoplus_{i=1}^{s} C_i = \{ (c_1^{(1)}, \ldots, c_{n_1}^{(1)}, \ldots, c_1^{(s)}, \ldots, c_{n_s}^{(s)} ) \mid c_i \in C (1 \leq i \leq s) \}.$$\[Lemma 2.1.\] Let $C \leq \mathbb{F}^n$ be not an orthogonal direct sum. Then the kernel of the restriction of $\pi$ to $\text{Mon}(C)$ is isomorphic to $\mathbb{F}^*$.

Proof. Clearly $\mathbb{F}^*C = C$ since $C$ is an $\mathbb{F}$-subspace. Assume that $\sigma := \text{diag}(\alpha_1, \ldots, \alpha_n) \in \text{Mon}(C)$ with $\alpha_i \in \mathbb{F}^*$, not all equal. Let $\{\alpha_1, \ldots, \alpha_n\} = \{\beta_1, \ldots, \beta_s\}$ with pairwise distinct $\beta_i$. Then

$$C = \bigoplus_{i=1}^{s} \ker(\sigma - \beta_i \text{id})$$

is the direct sum of eigenspaces of $\sigma$. Moreover the standard basis is a basis of eigenvectors of $\sigma$ so this is an orthogonal direct sum. $\square$

In the investigation of possible automorphisms of codes, the following strategy has proved to be very fruitful ([6], [2]).

**Definition 2.2.** Let $\sigma \in \text{Mon}(C)$ be an automorphism of $C$. Then $\pi(\sigma) \in S_n$ is a direct product of disjoint cycles of lengths dividing the order of $\sigma$. In particular if the order of $\sigma$ is some prime $p$, then we say that $\sigma$ has cycle type $(t, f)$, if $\pi(\sigma)$ has $t$ cycles of length $p$ and $f$ fixed points (so $pt + f = n$).

**Lemma 2.3.** Let $\sigma \in \text{Mon}(C)$ have prime order $p$.

(a) If $p$ does not divide $|\mathbb{F}^*|$ then there is some element $\tau \in \text{Mon}_n(\mathbb{F})$ such that $m(\tau \sigma \tau^{-1}) = \text{id}$. Replacing $C$ by $\tau(C)$ we hence may assume that $m(\sigma) = 1$.

(b) Assume that $p$ does not divide char($\mathbb{F}$), $m(\sigma) = 1$, and $\pi(\sigma) = (1, \ldots, p) \cdots ((t - 1)p + 1, \ldots, tp)(tp + 1) \cdots (n)$. Then $C = C(\sigma) \oplus E$, where

$$C(\sigma) = \{ c \in C \mid c_1 = \ldots = c_p, c_{p+1} = \ldots = c_{2p}, \ldots, c_{(t-1)p+1} = \ldots = c_{tp} \}$$
is the fixed code of $\sigma$ and

$$E = \{ c \in C \mid \sum_{i=1}^{p} c_i = \sum_{i=p+1}^{2p} c_i = \ldots = \sum_{i=(t-1)p+1}^{tp} c_i = c_{tp+1} = \ldots = c_n = 0 \}$$

is the unique $\sigma$-invariant complement of $C(\sigma)$ in $C$.

(c) Define two projections

$$\pi_t : C(\sigma) \to F^t, \quad \pi_t(c) := (c_p, c_{2p}, \ldots, c_{tp})$$

$$\pi_f : C(\sigma) \to F^f, \quad \pi_f(c) := (c_{tp+1}, c_{tp+2}, \ldots, c_{tp+f})$$

So $C(\sigma) \cong (\pi_t(C(\sigma)), \pi_f(C(\sigma))) =: C(\sigma)^*$. If $C = C^\perp$ is self-dual with respect to $(x, y) := \sum_{i=1}^{n} x_i y_i$, then $C(\sigma)^* \leq F^{t+f}$ is a self-dual code with respect to the inner product $(x, y) := \sum_{i=1}^{t} px_i y_i + \sum_{j=t+1}^{t+f} x_j y_j$.

(d) In particular $\dim(C(\sigma)) = (t + f)/2$ and $\dim(E) = t(p - 1)/2$.

Proof. Part (a) follows from the Schur-Zassenhaus theorem in finite group theory. For the ternary case see [7, Lemma 1].

(b) and (c) are similar to [6, Lemma 2].

In the following we will keep the notation of the previous lemma and regard the fixed code $C(\sigma)$.

**Remark 2.4.** If $f \leq d(C)$ then $t \geq f$.

Proof. Otherwise the kernel $K := \ker(\pi_t) = \{(0, \ldots, 0, c_1, \ldots, c_f) \in C(\sigma)\}$ is a nontrivial subcode of minimum distance $\leq f < d(C)$.

The way to analyse the code $E$ from Lemma 2.3 is based on the following remark.

**Remark 2.5.** Let $p \neq \text{char}(F)$ be some prime and $\sigma \in \text{Mon}_n(F)$ be an element of order $p$. Let

$$X^p - 1 = (X - 1)g_1 \ldots g_m \in F[X]$$

be the factorization of $X^p - 1$ into irreducible polynomials. Then all factors $g_i$ have the same degree $d = |(|F| + p\mathbb{Z})|$, the order of $|F|$ mod $p$.

There are polynomials $a_i \in F[X]$ $(0 \leq i \leq m)$ such that

$$1 = a_0 g_1 \ldots g_m + (X - 1) \sum_{i=1}^{m} a_i \prod_{j \neq i} g_j.$$

Then the primitive idempotents in $F[X]/(X^p - 1)$ are given by the classes of

$$\bar{e}_0 = a_0 g_1 \ldots g_m, \quad \bar{e}_i = a_i \prod_{j \neq i} g_j(X - 1), \quad 1 \leq i \leq m.$$
Let $L$ be the extension field of $F$ with $[L : F] = d$. Then the group ring
\[ F[X]/(X^p - 1) = F\langle \sigma \rangle \cong F \oplus L \oplus \ldots \oplus L \]
is a commutative semisimple $F$-algebra. Any code $C \leq F^n$ with an automorphism $\sigma \in \text{Mon}(C)$ is a module for this algebra. Put $e_i := \tilde{e}_i(\sigma) \in F[\sigma]$. Then $C = Ce_0 \oplus Ce_1 \oplus \ldots \oplus Ce_m$ with $Ce_0 = C(\sigma), E = Ce_1 \oplus \ldots \oplus Ce_m$. Omitting the coordinates of $E$ that correspond to the fixed points of $\sigma$, the codes $Ce_i$ are $L$-linear codes of length $t$.

Clearly $\dim_F(E) = d\sum_{i=1}^{m} \dim_L(Ce_i)$.

If $C$ is self-dual then $\dim(E) = t\frac{p-1}{2}$.

### 3 Extremal ternary codes of length 48.

Let $C = C^\perp \leq F_3^{48}$ be an extremal self-dual ternary code of length 48, so $d(C) = 15$.

#### 3.1 Large primes.

In this section we prove the main result of this paper.

**Theorem 3.1.** Let $C = C^\perp \leq F_3^{48}$ be an extremal self-dual code with an automorphism of prime order $p \geq 5$. Then $C$ is one of the two known codes. So either $C = Q_{48}$ is the extended quadratic residue code of length 48 with automorphism group
\[ \text{Mon}(C) = C_2 \times \text{PSL}_2(47) \text{ of order } 2^5 \cdot 3 \cdot 23 \cdot 47 \]
or $C = P_{48}$ is the Pless code with automorphism group
\[ \text{Mon}(C) = C_2 \times \text{SL}_2(23).2 \text{ of order } 2^6 \cdot 3 \cdot 11 \cdot 23. \]

**Lemma 3.2.** Let $\sigma \in \text{Mon}(C)$ be an automorphism of prime order $p \geq 5$. Then either $p = 47$ and $(t, f) = (1, 1)$ or $p = 23$ and $(t, f) = (2, 2)$ or $p = 11$ and $(t, f) = (4, 4)$.

**Proof.** For the proof we use the notation of Lemma 2.3. In particular we let $K := \ker(\pi_t) = \{(0, \ldots, 0, c_1, \ldots, c_f) \in C(\sigma)\}$ and put $K^* := \{(c_1, \ldots, c_f) \mid (0, \ldots, 0, c_1, \ldots, c_f) \in C(\sigma)\}$. Then
\[ K^* \leq F_3^f, \ d(K^*) \geq 15, \ dim(K^*) \geq \frac{f-t}{2}. \]

Moreover $tp + f = 48$.

**1) If** $t = 1$ **then** $p = 47$.

If $p = 47$, then $t = f = 1$.

So assume that $p < 47$ and $t = 1$. Then the code $E$ has length $p$ and dimension $(p - 1)/2$, therefore $p \geq d(C) = 15$. So $p \geq 17$ and $f \leq 48 - 17 = 31$. 

4
Then $K^* \leq \mathbb{F}_3^f$ has dimension $(f - 1)/2$ and minimum distance $d(K^*) \geq 15$. From the bounds given in [5] there is no such possibility for $f \leq 31$.

2) If $t = 2$ then $p = 23$.

Assume that $t = 2$. Since $2 \cdot p \leq 48$ we get $p \leq 23$ and if $p = 23$, then $(t, f) = (2, 2)$.

So assume that $p < 23$. The code $E$ is a non-zero code of length $2p$ and minimum distance $\geq 15$, so $2p \geq 15$ and $p$ is one of $11, 13, 17, 19$, and $f = 26, 22, 14, 10$. The code $K^* \leq \mathbb{F}_3^f$ has dimension $\geq f/2 - 1$ and minimum distance $\geq 15$. Again by [5] there is no such code.

3) $p \neq 13$.

For $p = 13$ one now only has the possibility $t = 3$ and $f = 9$. The same argument as above constructs a code $K^* \leq \mathbb{F}_3^f$ of dimension at least $(f + t)/2 - t = 3$ of minimum distance $\geq 15 > f$ which is absurd.

4) If $p = 11$, then $t = f = 4$.

Otherwise $t = 3$ and the code $K^*$ as above has length $15$, dimension $\geq 6$ and minimum distance $\geq 15$ which is impossible.

5) If $p = 7$ then $t = f = 6$.

Otherwise $t = 3, 4, 5$ and $f = 27, 20, 13$ and the code $K^*$ as above has dimension $\geq (f + t)/2 - t = 12, 8, 4$, length $f$, minimum distance $\geq 15$ which is impossible by [5].

6) $p \neq 7$.

Assume that $p = 7$, then $t = f = 6$ and the kernel $K$ of the projection of $C(\sigma)$ onto the first 42 components is trivial. So the image of the projection is $\mathbb{F}_3^6 \otimes \langle (1, 1, 1, 1, 1, 1) \rangle$, in particular it contains the vector $(1^7, 0^{35})$ of weight 7. So $C(\sigma)$ contains some word $(1^7, 0^{35}, a_1, \ldots, a_6)$ of weight $\leq 13$ which is a contradiction.

7) If $p = 5$ then $t = f = 8$ or $t = 9$ and $f = 3$.

Otherwise $t = 3, 4, 5, 6, 7$ and $f = 33, 28, 23, 18, 13$ and the code $K^* \leq \mathbb{F}_3^f$ has dimension $\geq (f + t)/2 - t = 15, 12, 9, 6, 3$ and minimum distance $\geq 15$ which is impossible by [5].

8) $p \neq 5$.

Assume that $p = 5$. Then either $t = 8$ and the projection of $C(\sigma)$ onto the first $8 \cdot 5$ coordinates is $\mathbb{F}_3^8 \otimes \langle (1, 1, 1, 1, 1) \rangle$ and contains a word of weight 5. But then $C(\sigma)$ has a word of weight $w$ with $5 < w \leq 5 + 8 = 13$ a contradiction.

The other possibility is $t = 9$. Then the code $E = E^\perp$ is a Hermitian self-dual code of length 9 over the field with $3^4 = 81$ elements, which is impossible, since the length of such a code is 2 times the dimension and hence even. \qed

**Lemma 3.3.** If $p = 11$ then $C \cong P_{48}$.

**Proof.** Let $\sigma \in \text{Mon}(C)$ be of order 11. Since $(x^{11} - 1) = (x - 1)gh \in \mathbb{F}_3[x]$ for irreducible polynomials $g, h$ of degree 5,

$$\mathbb{F}_3(\sigma) \cong \mathbb{F}_3 \oplus \mathbb{F}_{3^5} \oplus \mathbb{F}_{3^5}.$$  

Let $e_1, e_2, e_3 \in \mathbb{F}_3(\sigma)$ denote the primitive idempotents. Then $C = Ce_1 \oplus Ce_2 \oplus Ce_3$ with $C(\sigma) = Ce_1 = Ce_1^\perp$ of dimension 4 and $Ce_2 = Ce_3^\perp \leq (\mathbb{F}_{3^5} \oplus \mathbb{F}_{3^5})^4$. Clearly the projection of $C(\sigma)$ onto the first 44 coordinates is injective. Since all weights of $C$ are multiples of 3 and
≥ 15, this leaves just one possibility for $C(\sigma)$:

$$G_0 = (L_0 | R_0) := \begin{pmatrix}
1^{11} & 0^{11} & 0^{11} & 0^{11} \\
0^{11} & 1^{11} & 0^{11} & 0^{11} \\
0^{11} & 0^{11} & 1^{11} & 0^{11} \\
0^{11} & 0^{11} & 0^{11} & 1^{11}
\end{pmatrix} \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1
\end{pmatrix}.$$

The cyclic code $Z$ of length 11 with generator polynomial $(x - 1)g$ (and similarly the one with generator polynomial $(x - 1)h$) has weight enumerator

$$x^{11} + 132x^5y^6 + 110x^2y^9$$

in particular it contains more words of weight 6 than of weight 9. This shows that the dimension of $C_{e_i}$ over $\mathbb{F}_3$ is 2 for both $i = 2, 3$, since otherwise one of them has dimension ≥ 3 and therefore contains all words $(0, 0, c, \alpha c)$ for all $c \in Z$ and some $\alpha \in \mathbb{F}_3^\ast$. Not all of them can have weight ≥ 15. Similarly one sees that the codes $C_{e_i} \leq \mathbb{F}_3^4$ have minimum distance 3 for $i = 2, 3$. So we may choose generator matrices

$$G_1 := \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix}, \quad G_2 := \begin{pmatrix} 1 & 0 & a' & b' \\ 0 & 1 & c' & d' \end{pmatrix}$$

with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_3)$ and $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = -\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-tr}$. To obtain $\mathbb{F}_3$-generator matrices for the corresponding codes $C_{e_2}$ and $C_{e_3}$ of length 48, we choose a generator matrix $g_1 \in \mathbb{F}_3^{5 \times 11}$ of the cyclic code $Z$ of length 11 with generator polynomial $(x - 1)g$, and the corresponding dual basis $g_2 \in \mathbb{F}_3^{5 \times 11}$ of the cyclic code with generator polynomial $(x - 1)h$. We compute the action of $\sigma$ (the multiplication with $x$) and represent this as left multiplication with $z_{11} \in \mathbb{F}_3^{5 \times 5}$ on the basis $g_1$. If $a = \sum_{i=0}^{4} a_i z_{11}^i \in \mathbb{F}_3^{5 \times 11}$ with $a_i \in \mathbb{F}_3$, then the entry $a$ in $G_1$ is replaced by $\sum_{i=0}^{4} a_i z_{11}^i g_1 \in \mathbb{F}_3^{5 \times 11}$. Analogously for $G_2$, where we use of course the matrix $g_2$ instead of $g_1$. Replacing the code by an equivalent one we may choose $a, b, c$ as orbit representatives of the action of $\langle -z_{11} \rangle$ on $\mathbb{F}_3^5$.

A generator matrix of $C$ is then given by

$$\begin{pmatrix} L_0 & R_0 \\ G_1 & 0 \\ G_2 & 0 \end{pmatrix}.$$

All codes obtained this way are equivalent to the Pless code $P_{48}$. \hfill \square

**Lemma 3.4.** If $p = 23$ then $C \cong P_{48}$ or $C \cong Q_{48}$.

**Proof.** Let $\sigma \in \text{Mon}(C)$ be of order 23. Since $(x^{23} - 1) = (x - 1)gh \in \mathbb{F}_3[x]$ for irreducible polynomials $g, h$ of degree 11,

$$\mathbb{F}_3(\sigma) \cong \mathbb{F}_3 \oplus \mathbb{F}_{3^{11}} \oplus \mathbb{F}_{3^{11}}.$$
By Lemma 2.3 the code 

\[ C(\sigma) = \langle (1^{23}, 0^{23}, 1, 0), (0^{23}, 1^{23}, 0, 1) \rangle. \]

The codes \( C_2 \) and \( C_3 \) are codes of length 2 over \( \mathbb{F}_{311} \) such that \( \dim(C_2) + \dim(C_3) = 2 \). Note that the alphabet \( \mathbb{F}_{311} \) is identified with the cyclic code of length 23 with generator polynomial \( (x-1)g \) resp. \( (x-1)h \). These codes have minimum distance \( 9 < 15 \), so \( \dim(C_2) = \dim(C_3) = 1 \) and both codes have a generator matrix of the form \( (1, t) \) (resp. \( (1, -t^{-1}) \)) for \( t \in \mathbb{F}_{311}^* \). Going through all possibilities for \( t \) (up to the action of the subgroup of \( \mathbb{F}_{311}^* \), of order 23) the only codes \( C \) for which \( C(\sigma) \) have minimum distance \( \geq 15 \) are the two known extremal codes \( P_{48} \) and \( Q_{48} \). \( \square \)

Lemma 3.5. If \( p = 47 \) then \( C \cong Q_{48} \).

**Proof.** The subcode \( C_0 := \{ c \in \mathbb{F}_3^{47} \mid (c, 0) \in C \} \) is a cyclic code of length 47, dimension 23 and minimum distance \( \geq 15 \). Since \( x^{47} - 1 = (x-1)gh \in \mathbb{F}_3[x] \) for irreducible polynomials \( g, h \) of degree 23, \( C_0 \) is the cyclic code with generator polynomial \( (x-1)g \) (or equivalently \( (x-1)h \)) and \( C = \langle (C_0, 0), 1 \rangle \leq \mathbb{F}_3^{48} \) is the extended quadratic residue code. \( \square \)

### 3.2 Automorphisms of order 2.

As above let \( C = C^\perp \leq \mathbb{F}_3^{48} \) be an extremal self-dual ternary code. Assume that \( \sigma \in \text{Mon}(C) \) such that the permutational part \( \pi(\sigma) \) has order 2. Then \( \sigma^2 = \pm 1 \) because of Lemma 2.1. If \( \sigma^2 = -1 \), then \( \sigma \) is conjugate to a block diagonal matrix with all blocks \( \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} =: J \) and \( C \) is a Hermitian self-dual code of length 24 over \( \mathbb{F}_9 \). Such automorphisms \( \sigma \) with \( \sigma^2 = -1 \) occur for both known extremal codes.

If \( \sigma^2 = 1 \), then \( \sigma \) is conjugate to a block diagonal matrix

\[ \sigma \sim \text{diag}(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^t, 1^f, (-1)^a) \]

for \( t, a, f \in \mathbb{N}_0, 2t + a + f = 48 \).

**Proposition 3.6.** Assume that \( \sigma \in \text{Mon}(C) \), \( \sigma^2 = 1 \) and \( \pi(\sigma) \neq 1 \). Then either \( (t, a, f) = (24, 0, 0) \) or \( (t, a, f) = (22, 2, 2) \). Automorphisms of both kinds are contained in \( \text{Aut}(P_{48}) \).

**Proof.** 1) Wlog \( f \leq a \).

Replacing \( \sigma \) by \( -\sigma \) we may assume without loss of generality that \( f \leq a \).

2) \( f - t \in 4\mathbb{Z} \).

By Lemma 2.3 the code \( C(\sigma)^* \leq \mathbb{F}_3^{4t+f} \) is a self-dual code with respect to the inner product \( (x, y) = -\sum_{i=1}^t x_i y_i + \sum_{j=1}^f x_j y_j \). This space only contains a self-dual code if \( f - t \) is a multiple
of 4.

3) \( t + f \in \{22, 24\} \).

The code \( C(\sigma)^t \leq \mathbb{F}_3^{t+f} \) has dimension \( \frac{t+f}{2} \) and minimum distance \( \geq 15/2 \) and hence minimum distance \( \geq 8 \). By [5] this implies that \( t + f \geq 22 \). Since \( t + a \geq t + f \) and \( (t + a) + (t + f) = 48 \) this only leaves these two possibilities.

4) \( t + f \neq 22 \).

We first treat the case \( f \leq 14 \). Then \( K^* \cong \ker(\pi_t) \) is a code of length \( f \leq 14 \) and minimum distance \( \geq 15 \) and hence trivial. So \( \pi_t \) is injective and

\[
C(\sigma) \cong D := \pi_t(C(\sigma)) \leq \mathbb{F}_3^t, \dim(D) = 11, \text{ and } d(D) \geq \left\lceil \frac{15 - f}{2} \right\rceil.
\]

Using [5] and the fact that \( f - t \) is a multiple of 4, this only leaves the cases \( (t, f) \in \{(19, 3), (21, 1)\} \). To rule out these two cases we use the fact that \( D \) is the dual of the self-orthogonal ternary code \( D^\perp = \pi_t(\ker(\pi_f)) \). The bounds in [9] give \( d(D) \leq 5 < \frac{15-3}{2} \) for \( t = 19 \) and \( d(D) \leq 6 < \frac{15-1}{2} \) for \( t = 21 \).

If \( f \geq 15 \), then \( t \leq 7 \) and \( K^* \cong \ker(\pi_t) \) has dimension \( f - t > 0 \) and minimum distance \( \geq 15 \). This is easily ruled out by the known bounds (see [5]).

5) If \( t + f = 24 \) then either \( (t, f) = (24, 0) \) or \( (t, f) = (22, 2) \).

Again the case \( f > t \) is easily ruled out using dimension and minimum distance of \( K^* \) as before. So assume that \( f \leq t \) and let \( D = \pi_t(C(\sigma)) \) as before. Then \( \dim(D) = 12 \) and using [5] one gets that

\[
(t, f) \in \{(24, 0), (22, 2), (20, 4)\}.
\]

Assume that \( t = 20 \). Then there is some self-dual code \( \Lambda = \Lambda^\perp \leq \mathbb{F}_3^{20} \) such that

\[
D^\perp = \pi_t(\ker(\pi_f)) \leq \Lambda = \Lambda^\perp \leq D.
\]

Clearly also \( d(\Lambda) \geq d(D) \geq 6 \), so \( \Lambda \) is an extremal ternary code of length 20. There are 6 such codes, none of them has a proper overcode with minimum distance 6. \( \square \)

**Remark 3.7.** If \( \sigma \in \text{Mon}(C) \) is some automorphism of order 4, then \( \sigma^2 = -1 \) or \( \sigma^2 \) has Type (24, 0, 0) in the notation of Proposition 3.6.

**Proof.** Assume that \( \sigma \in \text{Mon}(C) \) has order 4 but \( \sigma^2 \neq -1 \). Then \( \tau = \sigma^2 \) is one of the automorphisms from Proposition 3.6 and so \( \sigma \) is conjugate to some block diagonal matrix

\[
\sigma \sim \text{diag}(\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix})^{t/2}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{f/2}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{a/2}.
\]

If \( t = 22 \) and \( f = 2 \) then The fixed code of \( \sigma \) is a self-dual code in \( \langle (1, 1, 1, 1) \rangle^{t/2} \oplus \langle (1, 1) \rangle^{f/2} \) and \( C(\sigma)^* \leq \mathbb{F}_3^{t/2+f/2} \) is a self-dual code with respect to the form \( (x, y) := \sum_{i=1}^{t/2} x_i y_i - \sum_{i=t/2+1}^{t/2+f/2} x_i y_i \) which implies that \( t/2 - f/2 \) is a multiple of 4, a contradiction. \( \square \)

For the two known extremal codes all automorphisms \( \sigma \) of order 4 satisfy \( \sigma^2 = -1 \). It would be nice to have some argument to exclude the other possibility.
References

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput. 24 (1997) 235-265.

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

[3] J.H. Conway, 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 (1982) 143-156.

[4] A. M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, Actes, Congrès International de Mathématiques (Nice, 1970), Gauthiers-Villars, Paris, 1971, Vol. 3, 211-215.

[5] M. Grassi, Code Tables: Bounds on the parameters of various types of codes. http://www.codetables.de/

[6] W. C. Huffman, Automorphisms of codes with Applications to Extremal Doubly Even Codes of Length 48. IEEE Trans. Inform. Theory 28 (1982) 511-521.

[7] W. C. Huffman, On extremal self-dual ternary codes of lengths 28 to 40. IEEE Trans. Inform. Theory 38 (1992) 1395-1400.

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

[9] Annika Meyer, Maximal self-orthogonal codes of Type I-IV Advances in Mathematics of Communications 4 (2010) 579 - 596.