The automorphism group of an extremal [72, 36, 16] code does not contain \( Z_7, Z_3 \times Z_3, \) or \( D_{10}. \)

Thomas Feulner and Gabriele Nebe
By Maschke’s theorem [10, Theorem V.2.7] the group algebra \( F_2G \) is a commutative semisimple algebra, i.e. a direct sum of fields. More precisely
\[
F_2G \cong F_2 \oplus F_{2^{k_1}} \oplus \cdots \oplus F_{2^{k_t}}
\]
with \(|G| = \dim_{F_{2^t}} (F_2G) = 1 + k_1 + \cdots + k_t \) and \( k_i \geq 2 \) for \( i = 1, \ldots, t \). The projections \( e_0, e_1, \ldots, e_t \) onto the simple components of \( F_2G \) (the central primitive idempotents of \( F_2G \)) can be computed as explicit linear combinations of the group elements. For instance \( e_0 = \sum g \in G \), expressing the fact that the first summand corresponds to the trivial representation in which all group elements act as the identity. In general any \( g \in G \) defines an element
\[
ge_i \in F_2G e_i \cong F_{2^{k_i}} \]
of the extension field \( F_{2^{k_i}} \) of \( F_2 \) and then \( e_i = \sum g \in G a_0g \)
where \( a_0 = \text{trace}_{F_{2^{k_i}}/F_2}(g^{-1} e_i) \).

**Example 2.1:** Let \( G = <g, h> \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \). Since already \( F_4 \) contains an element of order 3
\[
F_2G \cong F_2 \oplus F_4 \oplus F_4 \oplus F_4 \oplus F_4.
\]
If \( h \) acts as the identity on \( F_2G e_i \cong F_4 \) and \( g \) as a primitive third root of unity, then the trace of \( g^i h e_i \) is 1 if \( i = 1, 2 \) and 0 if \( i = 0 \). So \( e_1 = (1 + h + h^2)(g + g^2) \). The coefficients of all the idempotents \( e_i \) are given in the following table:

|   | 1  | g  | g^2 | h  | gh | g^2h | h^2 | g^2h | g^2h^2 |
|---|----|----|-----|----|----|-------|-----|------|--------|
| e_0 | 1  | 1  | 1   | 1  | 1  | 1     | 1   | 1    | 1      |
| e_1 | 1  | 0  | 1   | 1  | 0  | 1     | 1   | 1    | 1      |
| e_2 | 0  | 0  | 0   | 1  | 1  | 1     | 1   | 1    | 1      |
| e_3 | 0  | 1  | 1   | 0  | 1  | 1     | 1   | 1    | 1      |
| e_4 | 0  | 1  | 1   | 1  | 0  | 1     | 1   | 1    | 1      |

The group algebra \( F_2G \) always carries a natural involuion \( \overline{\cdot} : F_2G \to F_2G, \sum g \in G a_0g \mapsto \sum g \in G a_0g^{-1} \).

If \(|G| > 1\) then this is an algebra automorphism of order 2. It permutes the central primitive idempotents \( \{e_0, \ldots, e_t\} \). We always have \( e_0 = e_i \) and order the idempotents such that
\[
e_i = e_i \quad \text{for} \quad i = 0, \ldots, r - 1
\]
\[
e_r + 2r - 1 = e_r + 2r \quad \text{for} \quad i = 1, \ldots, s
\]
where \( t = r + 2s \).

For later use we need explicit isomorphisms
\[
\overline{\varphi}_i : F_{2^{k_i}} \to F_2G e_i
\]
that are compatible with the involution \( \overline{\cdot} \). For \( i = 0 \) there is just one
\[
\overline{\varphi}_0 : F_2 \to F_2G e_0, 0 \mapsto 0, 1 \mapsto e_0.
\]

**Lemma 2.2:** (a) If \( i \geq 1 \) and \( e_i = e_r \) then \( k_i \) is even and there is a unique automorphism \( \sigma \in \text{Aut}(F_{2^{k_i}}) \) of order 2. Then
\[
\varphi_i(\sigma(a)) = \overline{\varphi_i(a)}
\]
for any isomorphism \( \varphi_i \) and all \( a \in F_{2^{k_i}} \).

(b) If \( i \neq e_i = e_r \), then \( k_i = k_j \) and we may and will define the pair \( (\varphi_i, \varphi_j) \) such that \( \varphi_j = \varphi_i \) so
\[
\varphi_j : F_{2^{k_j}} \to F_2G e_j, \varphi_j(a) = \overline{\varphi_i(a)}
\]
for all \( a \in F_{2^{k_j}} \).

**Proof:** (a) The fact that \( k_i \) is even is a special case of Fong’s theorem (see [11, Theorem VII.8.13]). In particular there is a unique automorphism \( \sigma \in \text{Aut}(F_{2^{k_i}}) \) of order 2. Since \( a \mapsto \overline{\varphi_i^{-1}(\varphi_i(a))} \) is an automorphism of \( F_{2^{k_i}} \) of order 1 or 2, we only need to show that this automorphism is not the identity. Since \( \{\overline{\varphi_i^{-1}(\varphi_i(e_i))} \mid g \in G \} \) generates \( F_{2^{k_i}} \), over \( F_2 \) and \( k_i \geq 2 \), there is some \( g \in G \) such that \( g e_i \neq e_i \). Then \( 1 \neq \overline{\varphi_i^{-1}(\varphi_i(e_i))} = a \in F_{2^{k_i}} \) is a non-trivial invertible element and hence has odd order. In particular \( a \neq a^{-1} \) and so
\[
\overline{\varphi_i^{-1}(\varphi_i(a))} = \varphi_i^{-1}(g^{-1} e_i) = a^{-1} \neq a.
\]
(b) Clearly \( k_i = k_j \) since under the assumption \( : F_2G e_i \to F_2G e_j \) is an isomorphism. The rest is obvious.

**B. Invariant codes**

To study all self-dual codes \( C \subseteq F_2^g \) such that \( G \subseteq \text{Aut}(C) \), we view \( F_2^g \) as an \( F_2G \)-module where the elements \( g \in G \) act by right multiplication with the corresponding permutation matrix \( P_g \in F_2^{n \times n} \). So \( \sum g \in G a_g \in F_2G \) acts as \( \sum g \in G a_g P_g \in F_2^{n \times n} \). This way one obtains matrices \( E_i \in F_2^{n \times n} \) for the action of the idempotents \( e_i \in F_2G \), where \( E_iE_j = \delta_{ij}E_i \) and \( E_0 + \cdots + E_t = 1 \). Then \( F_2^g \) is the direct sum
\[
F_2^g = \bigoplus_{i=0}^{t} F_2^g E_i.
\]
The subspace \( F_2^g E_i \) is spanned by the rows of \( E_i \). It is an \( F_2G e_i \)-module, hence a vector space over the finite field \( F_{2^{k_i}} \). So we may choose \( \ell_i \) rows of \( E_i \), say \( (v_1, \ldots, v_{\ell_i}) \), to form an \( F_{2^{k_i}} \)-basis of \( F_2^{\ell_i} E_i \). We therewith obtain a non canonical isomorphism
\[
\varphi_i : F_{2^{k_i}} \cong F_2^{\ell_i} E_i, \varphi_i(a_1, \ldots, a_{\ell_i}) = \sum_{j=1}^{\ell_i} v_j \varphi_i(a_j)
\]
for \( i = 0, \ldots, t \), where the isomorphisms \( \varphi_i \) are as in Lemma 2.2.

Any \( G \)-invariant code \( C \), being an \( F_2G \)-submodule of \( F_2^g \), decomposes uniquely as
\[
C = \bigoplus_{i=0}^{t} C E_i = \bigoplus_{i=0}^{t} \varphi_i(C_i)
\]
for \( F_{2^{k_i}} \)-linear codes \( C_i \subseteq F_{2^{k_i}} \).

**Lemma 2.3:** The mapping
\[
\varphi : (C_0, C_1, \ldots, C_t) \mapsto \bigoplus_{i=0}^{t} \varphi_i(C_i)
\]
is a bijection between the set
\[
C_G := \{(C_0, C_1, \ldots, C_t) \mid C_i \subseteq F_{2^{k_i}} \}
\]
and the set of \( G \)-invariant codes in \( F_2^g \).

So instead of enumerating directly the \( G \)-invariant codes \( C \subseteq F_2^g \) we may enumerate all \( (t+1) \)-tuples of linear codes \( C_i \subseteq F_{2^{k_i}}^g \). Comparing the \( F_2 \)-dimension we get \( n = \sum_{i=0}^{t} k_i \ell_i \), so the length \( \ell_i \) is usually much smaller than \( n \).
C. Duality

We are interested in self-dual codes with respect to the standard inner product

\[ v \cdot w := \sum_{i=1}^{n} v_i w_i \]

on \( F_2^n \). This is invariant under permutations, so \( v g \cdot w g = v \cdot w \) for all \( v, w \in F_2^n \) and \( g \in S_n \). We hence obtain the equation

\[ v g \cdot w = v \cdot w g^{-1} \quad \text{for all } v, w \in F_2^n, g \in S_n. \]  

(2)

This tells us that the adjoint of a permutation \( g \) with respect to the inner product is \( g^{-1} \); for the natural involution \( \tau \) of \( F_2 G \). From Equation (2) we hence obtain that

\[ v a \cdot w = v \cdot w \tau a \quad \text{for all } v, w \in F_2^n, a \in F_2 G. \]

In particular the idempotents of \( F_2 G \) satisfy

\[ v E_I \cdot w E_J = v \cdot w E_J \tau E_I \quad \text{for all } v, w \in F_2^n. \]

(3)

Since \( E_J \tau E_I = 0 \) if \( E_I \neq E_J \) we hence obtain an orthogonal decomposition

\[ F_2^n = \bigoplus_{r=0}^{n} F_2^r E_i \bigoplus \bigoplus_{j=1}^{r} (F_2^r E_{r+2^j-1} \oplus F_2^r E_{r+2^j}) = \bigoplus_{r=0}^{n} F_2^r E_i \bigoplus \bigoplus_{j=1}^{r} (F_2^r E_{r+2^j-1} \oplus F_2^r E_{r+2^j}) \]

(4)

Definition 2.4: For \( 0 \leq i \leq r \) let \( \varphi_i : F_{2^i} \rightarrow F_{2^i} \) be the isomorphism from Equation (1). For \( 0 \leq i \leq r \) define the inner product

\[ h_i : F_{2^i}^d \times F_{2^i}^d \rightarrow F_2, h_i(c, c') := \varphi_i(c) \cdot \varphi_i(c') \]

and use \( h_i \) to define the dual of a code \( C_i \subseteq F_{2^i} \), as

\[ C_i^\perp := \{ v \in F_{2^i} \mid h_i(v, c) = 0 \quad \text{for all } c \in C_i \}. \]

For \( j = 1, \ldots, s \) let \( J : = r + 2j \) and define

\[ s_j : F_{2^r}^d \times F_{2^r}^{-d+j-1} \rightarrow F_2, s_j(c, c') := \varphi_j(c) \cdot \varphi_{j-1}(c'). \]

Then \( s_j \) defines the dual \( C_{j-1}^\perp \leq F_{2^{r+j-1}} \) of a code \( C_{j-1} \leq F_{2^{r+j-1}} \) as

\[ C_{j-1}^\perp := \{ v \in F_{2^{r+j-1}} \mid s_j(v, c) = 0 \quad \text{for all } c \in C_{j-1} \}. \]

Lemma 2.5: Let \( C = \varphi(C_0, \ldots, C_l) \subseteq F_2^n \) be some \( G \)-invariant code. Then the dual code is \( C^\perp = C^\perp \) where

\[ C^\perp = \varphi(C_0^\perp, C_1^\perp, \ldots, C_r^\perp, C_{r+2}^\perp, C_{r+1}^\perp, \ldots, C_l^\perp, C_{l-1}^\perp). \]

In particular the set of all self-dual \( G \)-invariant codes \( C \subseteq F_2^n \) is the image (under the bijection \( \varphi \) of Lemma 2.3) of the set

\[ C_{GD}^d := \{ (C_0, C_1, \ldots, C_l) \in C_G \mid C_i = C_i^\perp (0 \leq i \leq r) \}
\]

(5)

\[ C_{r+2}^\perp = C_{r+2}^\perp (j = 1, \ldots, (t-r)/2) \].

Proof: Comparing dimension it is enough to show that \( C^\perp \supseteq C' \). Since \( C = \bigoplus_{i=0}^{n} C_{E_i} \) and

\[ C' = \bigoplus_{j=0}^{r} \varphi_j(C_j^\perp) \oplus \bigoplus_{j=1}^{a} \varphi_{r+2^{j-1}}(C_{r+2}^\perp) \oplus \varphi_{r+2^j}(C_{r+2}^\perp) \]

it suffices to show that any element of \( CE_i \) is orthogonal to any component of \( C' \). So let \( c \in C_i \) and first assume that \( i \leq r \). By Equation (3)

\[ \varphi_i(c) \cdot \varphi_i(c') = 0 \quad \text{for all } j \neq i \text{ and } c' \in F_{2^b}. \]

For \( j = i \) we compute

\[ \varphi_i(c) \cdot \varphi_i(c') = h_i(c, c') \quad \text{for all } c' \in F_{2^b}. \]

This is 0 if \( c' \in C_i^\perp \).

Now assume that \( i = r + 2k \). Then Equation (3) yields

\[ \varphi_i(c) \cdot \varphi_i(c') = 0 \quad \text{for all } j \neq r + 2k - 1 \text{ and } c' \in F_{2^b}. \]

For \( j = r + 2k - 1 \) we have

\[ \varphi_{r+2k}(c) \cdot \varphi_{r+2k-1}(c') = s_k(c, c') \quad \text{for all } c' \in F_{2^b}. \]

This is 0 if \( c' \in C_{r+2k}^\perp \).

A similar argument holds for \( i = r + 2k - 1 \).

D. Weight

Enumerate the group elements so that \( G = \{ 1 = g_1, \ldots, g_q \} \subseteq S_n \) with \( q = |G| \). Then by assumption \( q \) is odd.

Lemma 2.6: Assume that \( G \leq S_n \) fixes the points \( m + 1, \ldots, n \) and that every element \( g \neq 1 \) acts without any fixed points on \( \{ 1, \ldots, m \} \). Then

\[ \ell_i = \ell = \frac{m}{q} \]

for all \( i > 0 \) and after reordering the elements in \( \{ 1, \ldots, m \} \) and therewith replacing \( G \) by a conjugate group we may assume that

\[ g_i(kq + 1) = kq + i \]

for all \( i = 1, \ldots, q, k = 0, \ldots, \ell - 1 \).

Proof: For \( j \in \{ 1, \ldots, m \} \) the stabiliser in \( G \) of \( j \) consists only of the identity and hence the orbit \( G_j = \{ g_1(j), \ldots, g_q(j) \} \) has length \( q \) and therefore \( m = \ell q \) is a multiple of the group order \( q = |G| \). From each of the \( \ell \) orbits choose some element \( j_k \). The reordering is now obviously

\[ (g_1(j_1), g_2(j_1), \ldots, g_q(j_1), g_1(j_2), \ldots, g_q(j_1)). \]

In this new group the permutation matrices \( P_i \) are block diagonal matrices with \( \ell \) equal blocks of size \( q \) and an identity matrix \( I_{n-m} \) of size \( n-m \) at the lower right corner. Also the idempotent matrices \( E_i \) are block diagonal

\[ E_0 = \text{diag}(B_0, \ldots, B_0, I_{n-m}) \]

\[ E_i = \text{diag}(B_i, \ldots, B_i, 0_{n-m}) \quad 1 \leq i \leq t. \]

If \( e_i = \sum_{k=1}^{q} \alpha_k g_k \), then the first row of \( B_i \) is \( \alpha_1, \ldots, \alpha_q \) and the other rows of \( B_i \) are obtained by suitably permuting these entries. The rank of the matrix \( B_i \) is exactly \( k_i \). Let

\[ \eta_i : F_2 G e_i \rightarrow \text{rowspace}(B_i), \sum_{k=1}^{q} \epsilon_k g_k e_i \mapsto (\epsilon_1, \ldots, \epsilon_q) B_i. \]

Then the isomorphism \( \varphi_i : F_{2^{b_i}} \rightarrow F_{2^{b_i}} E_i \leq F_{2^n} \) is defined by

\[ \varphi_i(c_1, \ldots, c_e) := (\eta_1(\varphi_1(c_1)), \eta_1(\varphi_1(c_2)), \ldots, \eta_1(\varphi_1(c_e))). \]
Lemma 2.7: In the situation above define a weight function 
\[ w_t : \mathbb{F}_{2^n} \to \mathbb{Z}_{\geq 0} \] 
by 
\[ w_t(x) := \text{wt}(\eta_t(\tilde{\varphi}_i(x))). \]
If \( i \geq 1 \) or \( m = n \), then 
\[ w_t : \mathbb{F}_{2^n} \to \mathbb{Z}_{\geq 0}, c \mapsto \sum_{k=1}^{\ell} w_t(c_k) \]
defines a weight function on \( \mathbb{F}_{2^n} \) such that the isomorphism 
\( \varphi_i \) is weight preserving.

Proof: We need to show that \( \text{wt}(\varphi_i(c)) = w_t(c) \) for all \( c \in \mathbb{F}_{2^n} \). But 
\[ \varphi_i((c_1, \ldots, c_d)) = (\eta_i(\tilde{\varphi}_i(c_1)), \eta_i(\tilde{\varphi}_i(c_2)), \ldots, \eta_i(\tilde{\varphi}_i(c_d)), 0^{n-m}) \]
and so the weight of \( \varphi_i(c) \) is the sum 
\[ \text{wt}(\varphi_i(c)) = \sum_{k=1}^{\ell} \text{wt}(\eta_i(\tilde{\varphi}_i(c_k))) = \sum_{k=1}^{\ell} w_t(c_k). \]

Remark 2.8: For \( m < n \) and \( i = 0 \), we need to modify the weight function because we work with \( \ell \) blocks of size \( q \) and \( n - m \) blocks of size 1. So here \( w_t : \mathbb{F}_{2^{n-m}} \to \mathbb{Z}_{\geq 0} \) 
\[ w_t(0, \ldots, 0) = q \text{wt}(c_1, \ldots, c_\ell) + \text{wt}(d_1, \ldots, d_{n-m}). \]

Remark 2.9: We will always work with \( G \)-equivalence classes of codes, where \( C, C' \leq \mathbb{F}_2^n \) are called \( G \)-equivalent, if there is some permutation 
\[ \pi \in S_{n,G} := \{ \pi \in S_n \mid \pi g = g \pi \text{ for all } g \in G \} \]
mapping \( C \) to \( C' \). In the situation of Lemma 2.6 the group 
\[ S_{n,G} \cong G \wr S_\ell \rtimes S_{n-m} \]
is obtained by the action of \( G \) on the blocks of size \( q \) and the symmetric group \( S_\ell \) permuting the \( \ell \) blocks of size \( q \). The group \( S_{n-m} \) permutes the last \( n - m \) entries. Via the isomorphism \( \varphi_i \) constructed in Lemma 2.7 the action of \( S_{n,G} \) on \( \mathbb{F}_2^n \) translates into the monomial action with monomial entries in the subgroup 
\[ \langle \varphi_i^{-1}(g e_i) \mid g \in G \rangle \leq \mathbb{F}_2^{n-1}. \]

Note that these are weight preserving automorphisms of the space \( \mathbb{F}_2^{n-1} \) for the weight function defined in Lemma 2.7.

Remark 2.10: For the weight preserving isomorphisms \( \varphi_i \) constructed in Lemma 2.7 the inner product \( h_i \) and \( s_j \) defined in Definition 2.4 are standard inner products: For \( 0 \leq i \leq r \) and \( c, c' \in \mathbb{F}_2^n \), 
\[ h_i(c, c') = \sum_{k=1}^{\ell} \eta_i(\tilde{\varphi}_i(c_k)) \cdot \eta_i(\tilde{\varphi}_i(c'_k)). \]

For \( 1 \leq j \leq s \) with \( J := r + 2j \), \( c \in \mathbb{F}_2^{2j}, c' \in \mathbb{F}_2^{2j-1} \), 
\[ s_j(c, c') = \sum_{k=1}^{\ell} \eta_j(\tilde{\varphi}_j(c_k)) \cdot \eta_{j-1}(\tilde{\varphi}_{j-1}(c'_k)) \]
be the fixed code of \( h \). Then \( g \) acts as an automorphism \( g' \) on the Golay code \( G \) and has no fixed points on the places of \( G \). Up to conjugacy in \( \text{Aut}(G) \) there is a unique such automorphism \( g' \). We use the notation of Section II for
$G' := \langle g' \rangle \leq S_{24}$. To distinguish the isomorphisms $\varphi_i$ from those defined by $G$, we use the letter $\psi$ instead of $\varphi$. As an $F_2(g')$ module the code $G$ decomposes as

$$G = \psi_0(D_0) \perp \psi_1(D_1).$$

Explicit computations show that $D_0 \cong h_8 \leq F_8^3$ is the extended Hamming code $h_8$ of length 8 and $D_1 \cong F_4 \otimes F_2$, $h_8$.

We now use the isomorphisms $\psi_i$ constructed in Section II-B1) for the group $G = \langle g, h \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ and the idempotents $e_0, \ldots, e_4$ from Example 2.1. Since all the $e_i$ are invariant under the natural involution the extremal $G$-invariant code $C = C \perp \leq F_2^{22}$ decomposes as

$$C = \perp \varphi_i(C_1)$$

for some self-dual Type II code $C_0 \leq F_8^3$ and Hermitian self-dual codes $C_i \leq F_4^3$. Then all the $C_i$ (for $i = 1, 2, 3, 4$) are equivalent to the code $D_1$ from Remark 2.2 and hence $C_i \cong F_4 \otimes F_2$, $h_8$ for all $i = 1, 2, 3, 4$.

Remark 3.3: $C_i \cong F_4 \otimes F_2$, $h_8$ for all $i = 1, 2, 3, 4$. Moreover for all $i = 1, 2, 3, 4$ the code

$$\psi_0(C_0) \perp \psi_1(C_1) \cong G$$

is equivalent to the binary Golay code of length 24.

The main result of this section is the following theorem.

Theorem 3.4: There is no extremal self-dual Type II code $C$ of length 72 for which $\text{Aut}(C)$ contains $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Proof: For a proof we describe the computations that led to this result using the notation from above. To obtain all candidates for the codes $C_i$ we first fix a copy $C_0 \leq F_8^3$ of the Hamming code $h_8$. We then compute the orbit of $F_4 \otimes F_2$, $h_8$ under the full monomial group $F_2 \wr S_8$ and check for all these codes $C_i \leq F_8^3$ whether $\psi_0(C_0) \perp \psi_1(C_1)$ has minimum distance 8. This yields a list $L$ of 17, 496 candidates for the codes $C_i \leq F_2^{22}$.

Since there is up to equivalence a unique Golay code and this code has a unique conjugacy class of fixed-point free automorphisms $g'$ of order 3, we may choose a fixed representative for $C_0 \leq F_8^3$ and $C_1 \leq F_4^3$. The centralizer of $g'$ in the automorphism group of $G = \psi_0(C_0) \perp \psi_1(C_1)$ acts on $L$ with 138 orbits. Choosing representatives $C_2$ of these orbits, we obtain 138 doubly even binary codes

$$D = \varphi_0(C_0) \oplus \varphi_1(C_1) \oplus \varphi_2(C_2)$$

of length 72, dimension 20, and minimum distance $\geq 16$. These codes $D$ fall into 2 equivalence classes under the action of the full symmetric group $S_{72}$. The automorphism group of both codes $D$ contains up to conjugacy a unique subgroup $U \cong Z_3 \times Z_3$ that has 8 orbits of length 9 on $\{1, \ldots, 72\}$ and such that there are generators $g, h$ of $U$ each having a 12-dimensional fixed space on $D$. For both codes $D$ we compute the list

$$L_3(D) := \{C_3 \in L \mid d(D \oplus \varphi_3(C_3)) \geq 16\}$$

and similarly

$$L_4(D) := \{C_4 \in L \mid d(D \oplus \varphi_4(C_4)) \geq 16\}.$$
with $A_0 = A_0^\perp$ a Type I code and $A_2 = A_1^\perp$. The code $C_0$ is a full glue of $D_0^\perp / D_0$ and $F_2^2$.

$$C_0 = \{(a, 1, 1) \mid a \in A_0 \setminus D_0\} \cup \{(a, 0, 0) \mid a \in D_0\}$$

$$\cup \{(a, 1, 0) \mid a \in A_1 \setminus D_0\} \cup \{(a, 0, 1) \mid a \in A_2 \setminus D_0\}$$

For $a \in D_0^\perp$ and $x \in F_2^2$ the weight

$$\text{wt}(\varphi_0(a, x)) = 7 \text{wt}(a) + \text{wt}(x)$$

because $\varphi_0$ repeats the first 10 coordinates 7 times (see Remark 2.8) and leaves the last two unchanged. Since $\varphi_0(C_0)$ has minimum distance $\geq 16$, the set $A_1 \cup A_2$ needs to have minimum weight $> 2$. Since the weights in $D_0^\perp \setminus A_0$, the shadow of $A_0$ in the sense of [5, p. 1320], are $= \frac{42}{72}$ (mod 4), the minimum weight there needs to be 5. This forces $A_0$ to be equivalent to $F_2^5 \otimes \langle (1, 1) \rangle$.

**Theorem 4.2:** There is no extremal self-dual Type II code of length 72 that has an automorphism of order 7.

**Proof:** Based on the description of the code $D$ of length 70 above we use a computer search to show that no such code $D$ has minimum distance $\geq 16$. For this purpose we classify all codes in $C_1 \leq F_2^{10}$ such that $C_1$ and its dual $C_1^\perp$ both have minimum distance $\geq 4$, see [7] for more details. Furthermore, it is sufficient to consider only one of the two dual parameter sets $[10, k, d, d^\perp]$ and $[10, 10 - k, d^\perp, d]$ since the interchange of $C_1$ and $C_1^\perp$ leads to isomorphic codes.

The maximal dimension of such a code $C_1$ is 7. Up to semilinear isometry there are more than 70 million such codes. The condition that the minimum distance of the code $C_1 := \varphi_1(C_1) \oplus \varphi_2(C_1^\perp)$ is $\geq 16$ reduces the number of codes to about 180,000 codes that need to be tested, see Table I for details. For each of these codes $C_1$ we run through all 945 different binary codes $D_0 \leq F_2^{10}$ that are equivalent to $E$ from Lemma 4.1 and check whether the code $D := \varphi_0(D_0) \oplus C_1$ has minimum distance $\geq 16$. No such code is found.

### V. The Dihedral Group of Order 10

#### A. Automorphisms of order 5.

Let $C = C_1^\perp \leq F_2^{72}$ be an extremal Type II code. Assume that there is some element $g \in \text{Aut}(C)$ of order 5. Then by [6, Theorem 6] the permutation $g \in S_{72}$ is the product of 14 five-cycles and we assume that

$$g = (1, 2, 3, 4, 5)(6, 7, 8, 9, 10) \ldots (66, 67, 68, 69, 70)$$

The primitive idempotents in $F_2^2$ are

$$e_0 = \sum_{i=0}^4 g_i, \quad e_1 = 1 + e_0 = g + g^2 + g^3 + g^4$$

and $F_2^2(e_1) \cong F_{16}$. As an $F_2^2(e_1)$ submodule of $F_2^{72}$, the code $C$ decomposes as

$$\varphi_0(C_0) \perp \varphi_1(C_1), \quad \text{with } C_0 = C_0^\perp \leq F_2^{16}, C_1 = C_1^\perp \leq F_1^{14}.$$ 

As above let $D := \{c_1, \ldots, c_{70}\} \mid \{c_1, \ldots, c_{70}, 0, 0\} \in C$. Then $D$ is a doubly-even code in $F_2^{70}$ of dimension 34 and minimum distance $\geq 16$ and

$$D = \varphi_0(D_0) \perp \varphi_1(C_1)$$

for some doubly-even code $D_0 \leq F_2^{14}$ of dimension 4.

**Lemma 5.1:** If $C$ is an extremal Type II code then $D_0$ is equivalent to the maximal doubly-even subcode $E$ of the unique self-dual code $A_0 \leq F_2^{14}$ of minimum distance 4.

**Proof:** Clearly $D_0 \leq F_2^{14}$ is doubly-even and of dimension 6,

$$D_0^\perp > A_0, A_1, A_2 > D_0$$

with $A_0 = A_0^\perp$ a Type I code and $A_2 = A_1^\perp$. As in the proof of Lemma 5.1 code $C_0$ is a full glue of $D_0^\perp / D_0$ and $F_2^2$. For $a \in D_0^\perp$ and $x \in F_2^2$ the weight of

$$\varphi_0(a, x) \in \varphi_0(C_0) \leq C$$

is $5 \text{wt}(a) + \text{wt}(x)$. Since $\varphi_0(C_0)$ has minimum distance $\geq 16$, the code $A_0$ needs to have minimum weight $\geq 4$. Explicit computations show that there is up to equivalence a unique such code $A_0$.

To obtain a weight preserving isomorphism $\varphi_1 : F_2^{14} \rightarrow F_2^2 E_1$ as described in Lemma 2.4 we need to define the suitable weight function on the coordinates $c_k \in F_{16}$.

**Definition 5.2:** Let $\xi \in F_{16}^*$ denote a primitive 5th root of unity. The 5-weight of $x \in F_{16}$ is

$$\text{wt}_5(x) := \begin{cases} 0 & x = 0 \\ 4 & x \in \langle \xi \rangle \leq F_{16}^* \\ 2 & x \in F_{16}^* \setminus \langle \xi \rangle \end{cases}$$

For $c = (c_1, \ldots, c_n) \in F_{16}^n$ we let as usual $\text{wt}_5(c) := \sum_{i=1}^n \text{wt}_5(c_i)$.

### B. The dihedral group of order 10.

We now assume that $C = C_1^\perp \leq F_2^{72}$ is an extremal Type II code such that

$$D_{10} \cong G := \langle g, h \rangle \leq \text{Aut}(C)$$

where $g$ is the element of order 5 from above and the order of $h$ is 2. By any automorphism of order 2 of $C$ acts without fixed points, so we may assume wlog that

$$g = (1, 2, 3, 4, 5)(6, 7, 8, 9, 10) \ldots (66, 67, 68, 69, 70),$$

$$h = (1, 6)(2, 10)(3, 9)(4, 8)(5, 7) \ldots$$

$$(61, 66)(62, 70)(63, 69)(64, 68)(65, 67) \cdot (71, 72).$$

The centralizer in $S_{72}$ of $G$ isomorphic to $D_{10} \rtimes S_7 \times \langle (71, 72) \rangle$ acts on the set of $G$-invariant codes.
Remark 5.3: Let $e_0$ and $e_1 = 1 - e_0 \in \mathbb{F}_2(g) \leq \mathbb{F}_2G$ be as above. Then $e_0$ and $e_1$ are the central primitive idempotents in $\mathbb{F}_2G$. In particular $\langle h \rangle$ acts on the codes $CE_0$ and $CE_1$.

Remark 5.4: Explicit computations with MAGMA show that the automorphism group of the code $A_0$ from Lemma 5.1 contains a unique conjugacy class of elements $x$ of order 2 that have 7 orbits. Therefore the action of $h$ on the fixed code of $\langle q \rangle$ is uniquely determined. Let $U$ be the centralizer of $x$ in the full symmetric group of degree 14. Then the $U$-orbit $O_{14}$ of $A_0$ has length 1920. Let

$$C_0 := \{ \varphi_0(C_0) \mid C_0 \in O_{14} \}.$$  

To investigate the action of the element $h$ on the Hermitian self-dual code $C_1 \leq \mathbb{F}_{14}^{14}$ we recall the following theorem.

Theorem 5.5: ([13] Theorem 3.1) The fixed code $C(h) := \{ c \in C \mid ch = c \} \cup \langle h \rangle$ is equivalent to $B \otimes ((1, 1))$ for some self-dual code $B = B^\perp \leq \mathbb{F}_{16}^{36}$ of minimum distance 8.

Let

$$\varphi: \mathbb{F}_{16} \rightarrow \mathbb{F}_{16}, x \mapsto x^4$$

be the nontrivial Galois automorphism of $\mathbb{F}_{16}$ with fixed field $\mathbb{F}_4$. Then the action of $h$ is given by

$$(x_1, y_1, x_2, y_2, \ldots, x_7, y_7)h = (y_1, \overline{x_1}, y_2, \overline{x_2}, \ldots, y_7, \overline{x_7}).$$

Note that this action is only $\mathbb{F}_4$-linear. In particular the fixed code of $\langle h \rangle$ is

$$C_1(h) = \{(x_1, \overline{x_1}, \ldots, x_7, \overline{x_7}) \in C_1 \}$$

only an $\mathbb{F}_4$-linear code in $\mathbb{F}_{16}^{14}$.

Corollary 5.6: The code $X := \pi(C_1(h)) := \{(x_1, \ldots, x_7) \mid (x_1, \overline{x_1}, \ldots, x_7, \overline{x_7}) \in C_1 \} \leq \mathbb{F}_{16}^7$ is an $\mathbb{F}_4$-linear trace-Hermitian self-dual code $X = X^\perp$ where

$$X^\perp := \{ v \in \mathbb{F}_{16}^7 \mid \sum_{i=1}^7 \text{tr}(v_{16}^i, x_i, \overline{x_i}) = 0 \text{ for all } x \in X \}$$

such that the minimal 5-weight of $X$ is at least 8. Since $\dim_{\mathbb{F}_4}(X) = 7 = \dim_{\mathbb{F}_{16}}(C_1)$, the $\mathbb{F}_{16}$ linear code $C_1 \leq \mathbb{F}_{16}^{14}$ is obtained from $X$ as

$$C_1 = \Psi(X) := \langle (x_1, \overline{x_1}, x_7, \overline{x_7}) \rangle \times (x_1, \ldots, x_7) \in X \rangle \mathbb{F}_{16}.$$

Remark 5.7: If $\varphi: x \mapsto x^4$ denotes the Galois automorphism of $\mathbb{F}_{16}$ with fixed field $\mathbb{F}_4$, then $\text{wt}_5(x) = \text{wt}_5(\overline{x})$ for all $x \in \mathbb{F}_{16}$. Let $\xi$ denote a fixed element of order 5 in $\mathbb{F}_{16}^*$. Then $D_{10} = \langle \xi, \overline{\xi} \rangle$ acts $\mathbb{F}_{16}$-linearly on $\mathbb{F}_{16}$ and preserves the 5-weight and trace-Hermitian orthogonality.

Lemma 5.8: An $\mathbb{F}_4$-linear code $X \leq \mathbb{F}_{16}^7$ with minimal 5-weight at least 8 is equivalent (under $D_{10} \otimes S_7$) to a code with generator matrix of the following type:

$$\Gamma := \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \xi & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, a \in (\mathbb{F}_4 : \xi)^6, B \in \mathbb{F}_{16}^{7 \times 3}$$

We will call such a generator matrix systematic.

Proof: The condition on the minimal 5-weight implies that there is at least one column with two $\mathbb{F}_4$-linearly independent entries. Use the group action of $\text{GL}_7(\mathbb{F}_4) \times (D_{10} \otimes S_7)$ to map this column to $\{0, \ldots, 0, 1, \xi, \overline{\xi} \}$ and move the column to the front. Similar arguments can be applied to the derived code shortened at position 1 and $\{1, 2 \}$, respectively.

Theorem 5.9: There is no extremal self-dual Type II code $C$ of length 72 such that $\text{Aut}(C)$ contains the dihedral group of order 10.

Proof: Assume that there is such a code $C$ with $\text{Aut}(C) \geq \langle g, h \rangle = G \cong D_{10}$.

Let $\Psi$ be the map from the $\mathbb{F}_4$-linear codes in $\mathbb{F}_{16}^7$ to the $\mathbb{F}_{16}$-linear codes in $\mathbb{F}_{16}^{14}$ from Corollary 5.6. Let $C_0$ be the list of 1920 codes of length 72 from Remark 5.4 and let $X$ denote a system of representatives of $D_{10} \otimes S_7$ equivalence classes of trace-Hermitian self-dual codes $X \leq \mathbb{F}_{16}^7$ with minimal 5-weight at least 8. Then

$$C \cong \varphi_0(C_0) \oplus \varphi_1(\Psi(X))$$

for some $C_0 \in C_0$ and some $X \in X$.

For the proof of the theorem we summarize our construction method for all systematic generator matrices of $\mathbb{F}_4$-linear trace-Hermitian self-dual codes $X \leq \mathbb{F}_{16}^7$ with minimal 5-weight at least 8 up to equivalence under $D_{10} \otimes S_7$. Furthermore, we restrict ourselves to these codes that might be extended by a binary code $C_0 \in C_0$ such that $\varphi_0(C_0) \oplus \varphi_1(\Psi(X))$ has minimum distance $\geq 16$.

The following observations are used for speeding up the computations:

- Each element in $\mathbb{F}_{16}^*$ is self-orthogonal under the trace-Hermitian inner product.
- We further know that each row $\Gamma_i$ must have minimum 5-weight at least 8. Since the 5-weight is not constant under scalar multiplication by elements $\mu \in \mathbb{F}_4^*$ we also have to test $\text{wt}_5(\mu \Gamma_i)$. This reduces the candidates for the first row to 3525 vectors. There are 15705 candidates for the other rows.
- The action of $\mathbb{F}_4^* \times (D_{10} \otimes S_7)$ partitions these 3525 vectors into 6 orbits. It is sufficient to start with only one representative for each orbit.
- Similarly, for the $i$-th row it is sufficient to add only representatives under the action of the stabilizer of the code $\langle \Gamma_1, \ldots, \Gamma_{i-1} \rangle \mathbb{F}_4$.
- If some candidate $v$ for row $i$ is either not trace-Hermitian orthogonal to some preceding row $\Gamma_j$, $j \leq i - 2$ or the minimum 5-weight of $(v, \Gamma_1, \ldots, \Gamma_{i-2}) \mathbb{F}_4$ is less than 8, we know that the corresponding permuted vector is not allowed to be a candidate for row $i + 2$ and $i + 4$, respectively.
- In the beginning there is a set $\mathcal{L}(0) = C_0$ of 1920 binary codes which may play the role of $C_0$. In each step $i$ of
the iteration we may iteratively update this set by setting
\[ L^{(i)} := \{ C_0 \in L^{(i-1)} : d \left( \varphi_0(C_0) \oplus \varphi_1(\Psi(\Gamma_{i_{1*}}, \ldots, \Gamma_{i_{s*}}F_4)) \right) \geq 16 \} \]

If \( L^{(i)} \) is empty we can skip this branch.

The test if there is another code already examined, which is isomorphic to the actual code is done by the calculation of unique orbit representatives by a modification of [8]. This computation returns at the same time without any additional effort the stabilizer of \( \langle \Gamma_{i_{1*}}, \ldots, \Gamma_{i_{s*}}F_4 \rangle \) in \( D_{10} \wr S_7 \). The computations have been performed in Magma [11] and needed about 70 days CPU time. The number of non isomorphic candidates on level \( i \) which appeared during our backtracking approach may be found in Table II. These numbers count \( F_4 \)-linear trace-Hermitian self-orthogonal codes which fulfill the condition on the given systematic form, the 5-weight and self-orthogonality. The test on the extendability by \( C_0 \) is executed after the isomorphism rejection. Hence, the numbers may vary for different backtracking approaches. For the remaining 4 candidates at level \( i = 7 \) the corresponding lists \( L^{(7)} \) of candidates for \( C_0 \) are empty.

In contrast to [11] applied in Section IV we preferred a row-wise generation of the generator matrix in this case, since this gives us the possibility to check the existence of a valid code \( C_0 \in C_0 \).

### REFERENCES

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*. J. Symbolic Comput., 24(3-4):235-265, 1997

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

[3] S. Bouyuklieva, *On the automorphism group of a doubly-even \( (72, 36, 16) \) code*. IEEE Trans. Inform. Theory 50 (2004), no. 3, 544–547.

[4] E.A. O’Brien, W. Willems, *On the automorphism group of a binary self-dual doubly-even \( (72, 36, 16) \) code*. IEEE Trans. Inform. Theory 57 (2011) 4445-4451.

[5] J. H. Conway, N.J.A. Sloane, *A new upper bound on the minimal distance of self-dual codes*. IEEE Trans. Inform. Theory 36 (1990) 1319-1333.

[6] 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.

[7] T. Feulner, *Classification of linear codes with prescribed minimum distance and new upper bounds*. Servei de Publicacions UAB, Congressos 5 (2011), 105-110.

[8] T. Feulner, *The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes*. Adv. Math. Commun. 3 (2009), 363-383.

[9] W. C. Huffman, *Automorphisms of codes with Applications to Extremal Doubly Even Codes of Length 48*. IEEE Trans. Inform. Theory 28 (1982), no. 3, 511–521.

[10] B. Huppert, *Endliche Gruppen I*. Springer Verlag (1967)

[11] B. Huppert, N. Blackburn, *Finite groups II*. Springer Verlag (1982)

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

[13] G. Nebe, *An extremal \( [72, 36, 16] \) binary code has no automorphism group containing \( Z_2 \times Z_4 \), \( Q_8 \), or \( Z_{10} \). Finite Fields and Their Applications 18 (2012) 563-566.

[14] E.M. Rains, *Shadow bounds for self-dual codes*. IEEE Trans. Inform. Theory 44 (1998), no. 1, 134–139.

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

[16] N. Yankov, *On the doubly even \( [72, 36, 16] \) codes having an automorphism of order 9*. IEEE Trans. Inform. Theory (to appear)