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

***Abstract*—A computer calculation with Magma shows that there is no extremal self-dual binary code C of length 72 that has an automorphism group containing either the dihedral group of order 10, the elementary abelian group of order 9, or the cyclic group of order 7. Combining this with the known results in the literature one obtains that the order of $\mathrm{Aut}(C)$ is either 5 or divides 24.**

***Index Terms*—extremal self-dual code, Type II code, automorphism group**

I. INTRODUCTION

LET $C = C^\perp \leq \mathbf{F}_2^n$ be a binary self-dual code of length n. Then all weights $\mathrm{wt}(c) := |\{i \mid c_i = 1\}|$ of codewords in C are even and C is called *doubly-even*, if $\mathrm{wt}(C) := \{\mathrm{wt}(c) \mid c \in C\} \subseteq 4\mathbf{Z}$. Doubly-even self-dual binary codes are also called *Type II* codes. Using invariant theory, one may show [12] that the minimum weight $d(C) := \min(\mathrm{wt}(C \setminus \{0\}))$ of a Type II code is bounded from above by $4 + 4\lfloor \frac{n}{24} \rfloor$. Type II codes achieving this bound are called *extremal*. Particularly interesting are the extremal codes of length a multiple of 24. There are unique extremal codes of length 24 (the extended binary Golay code $\mathcal{G}_{24}$) and 48 (the extended quadratic residue code QR_{48}), and each has a fairly big automorphism group (namely $\mathrm{Aut}(\mathcal{G}_{24}) \cong M_{24}$ and $\mathrm{Aut}(\mathrm{QR}_{48}) \cong \mathrm{PSL}_2(47)$) acting at least 2-transitively. The existence of an extremal code of length 72 is a longstanding open problem (see [15]). A series of papers investigates the automorphism group of a putative extremal code of length 72 excluding most of the subgroups of S_{72}. Continuing these investigations we have the following theorem, which is the main result of this paper:

Theorem 1.1: The automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code has order 5 or d where d divides 24.

Throughout the paper the *cyclic group* of order n is denoted by Z_n to reserve the letter C for codes. With D_{2n} we denote the *dihedral group* of order $2n$, S_n and A_n are the *symmetric* and *alternating* groups of degree n. $G \times H$ denotes the *direct product* of the two groups G and H and let $G \wr S_n$ denote the *wreath product* with normal subgroup $G \times G \ldots \times G$ and the symmetric group of degree n permuting the n components.

T. Feulner is with the Mathematics Department, University of Bayreuth, 95440 Bayreuth, Germany, e-mail: thomas.feulner@uni-bayreuth.de – supported by DFG priority program SPP 1489

G. Nebe is with the Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany, e-mail: nebe@math.rwth-aachen.de.

Manuscript received October, 2011; revised June, 2012.

The following is known about the automorphism group $\mathrm{Aut}(C)$ of a binary self-dual doubly-even $[72, 36, 16]$ code C:

By [4, Theorem 1] the group $\mathrm{Aut}(C)$ has order 5, 7, 10, 14, or d where d divides 18 or 24 or $\mathrm{Aut}(C) \cong A_4 \times Z_3$. The paper [16] shows that $\mathrm{Aut}(C)$ contains no element of order 9, [13, Corollary 3.6] excludes Z_{10} as subgroup of $\mathrm{Aut}(C)$. So to prove Theorem 1.1 it suffices to show that there are no such codes C for which $\mathrm{Aut}(C)$ contains D_{10} (Theorem 5.9), Z_7 (Theorem 4.2), or $Z_3 \times Z_3$ (Theorem 3.4). The necessary computations, which have been performed in Magma [1] using the methods of [7], are described in this paper.

II. THE GENERAL SETUP

Throughout this section we let $G \leq S_n$ be an abelian group of odd order.

The main strategy to construct self-dual G-invariant codes $C = C^\perp \leq \mathbf{F}_2^n$ is a bijection between these codes and tuples

$$(C_0, C_1, \ldots, C_r, C_{r+1}, C_{r+2}, \ldots, C_{r+2s})$$

of linear codes over extension fields of $\mathbf{F}_2$ that satisfy $C_0 = C_0^\perp$, $C_i = \overline{C_i}^\perp$ $(1 \leq i \leq r)$ and $C_{r+2i} = C_{r+2i-1}^\perp$ $(1 \leq i \leq s)$ for suitable inner products (see Lemma 2.5). Lower bounds on the minimum weight of C give rise to lower bounds on suitably defined weights for the codes C_i (see Lemma 2.7). This gives a method to enumerate G-invariant self-dual codes with high minimum weight.

To this aim we view the G-invariant codes $C \leq \mathbf{F}_2^n$ as $\mathbf{F}_2G$-submodules of the permutation module $\mathbf{F}_2^n$, where $\mathbf{F}_2G$ is the group algebra of G. By Maschke's theorem this is a commutative semisimple algebra and hence a direct sum of fields. The codes C_i arise as linear codes over these direct summands of $\mathbf{F}_2G$.

The underlying theory is well known and we do not claim to prove anything new in this section. However we try to be very explicit and therefore restrict to the special case that is relevant for the computations described in this paper. For the basic facts about representation theory of finite groups we refer the reader to [11, Chapter VII] and [10, Chapter V].

A. Abelian semisimple group algebras

G-invariant codes in $\mathbf{F}_2^n$ are modules for the group algebra

$$\mathbf{F}_2G := \{\sum_{g \in G} a_g g \mid a_g \in \mathbf{F}_2\}.$$

By Maschke's theorem [10, Theorem V.2.7] the group algebra $\mathbf{F}_2G$ is a commutative semisimple algebra, i.e. a direct sum of fields. More precisely

$$\mathbf{F}_2G \cong \mathbf{F}_2 \oplus \mathbf{F}_{2^{k_1}} \oplus \ldots \oplus \mathbf{F}_{2^{k_t}}$$

with $|G| = \dim_{\mathbf{F}_2}(\mathbf{F}_2G) = 1 + k_1 + \ldots + k_t$ and $k_i \geq 2$ for $i = 1, \ldots, t$. The projections $e_0, e_1, \ldots, e_t$ onto the simple components of $\mathbf{F}_2G$ (the central primitive idempotents of $\mathbf{F}_2G$) can be computed as explicit linear combinations of the group elements. For instance $e_0 = \sum_{g\in G} g$, 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

$$ge_i \in \mathbf{F}_2Ge_i \cong \mathbf{F}_{2^{k_i}}$$

of the extension field $\mathbf{F}_{2^{k_i}}$ of $\mathbf{F}_2$ and $e_i = \sum_{g\in G} a_g g$ where $a_g = \mathrm{trace}_{\mathbf{F}_{2^{k_i}}/\mathbf{F}_2}(g^{-1}e_i)$.

Example 2.1: Let $G = \langle g, h\rangle \cong Z_3 \times Z_3$. Since $\mathbf{F}_4$ contains an element of order 3

$$\mathbf{F}_2G \cong \mathbf{F}_2 \oplus \mathbf{F}_4 \oplus \mathbf{F}_4 \oplus \mathbf{F}_4 \oplus \mathbf{F}_4.$$

If h acts as the identity on $\mathbf{F}_2Ge_1 \cong \mathbf{F}_4$ and g as a primitive third root of unity, then the trace of $g^ih^je_1$ 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	gh^2	g^2h^2
e_0	1	1	1	1	1	1	1	1	1
e_1	0	1	1	0	1	1	0	1	1
e_2	0	0	0	1	1	1	1	1	1
e_3	0	1	1	1	0	1	1	1	0
e_4	0	1	1	1	1	0	1	0	1

The group algebra $\mathbf{F}_2G$ always carries a natural involution

$$^{-} : \mathbf{F}_2G \to \mathbf{F}_2G, \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g g^{-1}.$$

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 $\overline{e_0} = e_0$ and order the idempotents such that

$$\begin{array}{lll} \overline{e_i} = e_i & \text{for} & i = 0, \ldots, r \leq t \\ \overline{e_{r+2i-1}} = e_{r+2i} & \text{for} & i = 1, \ldots, s \end{array}$$

where $t = r + 2s$.

For later use we need explicit isomorphisms

$$\tilde{\varphi}_i : \mathbf{F}_{2^{k_i}} \to \mathbf{F}_2Ge_i$$

that are compatible with the involution $^{-}$. For $i = 0$ there is just one

$$\tilde{\varphi}_0 : \mathbf{F}_2 \to \mathbf{F}_2Ge_0, 0 \mapsto 0, 1 \mapsto e_0.$$

Lemma 2.2: (a) If $i \geq 1$ and $e_i = \overline{e_i}$ then k_i is even and there is a unique automorphism $\sigma \in \mathrm{Aut}(\mathbf{F}_{2^{k_i}})$ of order 2. Then

$$\tilde{\varphi}_i(\sigma(a)) = \overline{\tilde{\varphi}_i(a)}$$

for any isomorphism $\tilde{\varphi}_i$ and all $a \in \mathbf{F}_{2^{k_i}}$.

(b) If $e_i \neq \overline{e_i} = e_j$, then $k_i = k_j$ and we define the pair $(\tilde{\varphi}_i, \tilde{\varphi}_j)$ such that $\tilde{\varphi}_j = \overline{\tilde{\varphi}_i}$ so

$$\tilde{\varphi}_j : \mathbf{F}_{2^{k_j}} \to \mathbf{F}_2Ge_j, \tilde{\varphi}_j(a) = \overline{\tilde{\varphi}_i(a)}$$

for all $a \in \mathbf{F}_{2^{k_j}}$.

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 $\sigma \in \mathrm{Aut}(\mathbf{F}_{2^{k_i}})$ of order 2. Since $a \mapsto \tilde{\varphi}_i^{-1}(\overline{\tilde{\varphi}_i(a)})$ is an automorphism of $\mathbf{F}_{2^{k_i}}$ of order 1 or 2, we only need to show that this automorphism is not the identity. Since $\{\tilde{\varphi}_i^{-1}(ge_i) \mid g \in G\}$ generates $\mathbf{F}_{2^{k_i}}$ over $\mathbf{F}_2$ and $k_i \geq 2$, there is some $g \in G$ such that $ge_i \neq e_i$. Then $1 \neq \tilde{\varphi}_i^{-1}(ge_i) =: a \in \mathbf{F}^*_{2^{k_i}}$ is a non-trivial invertible element and hence has odd order. In particular $a \neq a^{-1}$ and so

$$\tilde{\varphi}_i^{-1}(\overline{\tilde{\varphi}_i(a)}) = \tilde{\varphi}_i^{-1}(g^{-1}e_i) = a^{-1} \neq a.$$

(b) Clearly $k_i = k_j$ since under the assumption $^{-} : \mathbf{F}_2Ge_i \to \mathbf{F}_2Ge_j$ is an isomorphism. The rest is obvious. ■

B. Invariant codes

To study all self-dual codes $C \leq \mathbf{F}_2^n$ such that $G \leq \mathrm{Aut}(C)$, we view $\mathbf{F}_2^n$ as an $\mathbf{F}_2G$-module where the elements $g \in G$ act by right multiplication with the corresponding permutation matrix $P_g \in \mathbf{F}_2^{n\times n}$. So $\sum_{g\in G} a_g g \in \mathbf{F}_2G$ acts as $\sum_{g\in G} a_g P_g \in \mathbf{F}_2^{n\times n}$. Thus one obtains matrices $E_i \in \mathbf{F}_2^{n\times n}$ for the action of the idempotents $e_i \in \mathbf{F}_2G$, where $E_iE_j = \delta_{ij}E_i$ and $E_0 + \ldots + E_t = 1$. Then $\mathbf{F}_2^n$ is the direct sum

$$\mathbf{F}_2^n = \bigoplus_{i=0}^{t} \mathbf{F}_2^n E_i.$$

The subspace $\mathbf{F}_2^nE_i$ is spanned by the rows of E_i. It is an $\mathbf{F}_2Ge_i$-module, hence a vector space over the finite field $\mathbf{F}_{2^{k_i}}$. So we may choose ℓ_i rows of E_i, say $(v_1, \ldots, v_{\ell_i})$, to form an $\mathbf{F}_{2^{k_i}}$-basis of $\mathbf{F}_2^nE_i$. Taking coordinates with respect to this basis defines an isomorphism

$$\varphi_i : \mathbf{F}_{2^{k_i}}^{\ell_i} \cong \mathbf{F}_2^nE_i, \varphi_i(a_1, \ldots, a_{\ell_i}) = \sum_{j=1}^{\ell_i} v_j\tilde{\varphi}_i(a_j) \qquad (1)$$

for $i = 0, \ldots, t$, where the isomorphisms $\tilde{\varphi}_i$ are as in Lemma 2.2.

Any G-invariant code C, being an $\mathbf{F}_2G$-submodule of $\mathbf{F}_2^n$, decomposes uniquely as

$$C = \bigoplus_{i=0}^{t} CE_i = \bigoplus_{i=0}^{t} \varphi_i(C_i)$$

for $\mathbf{F}_{2^{k_i}}$-linear codes

$$C_i \leq \mathbf{F}_{2^{k_i}}^{\ell_i}$$

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

$$\mathcal{C}_G := \{(C_0, C_1, \ldots, C_t) \mid C_i \leq \mathbf{F}_{2^{k_i}}^{\ell_i}\}$$

and the set of G-invariant codes in $\mathbf{F}_2^n$.

So instead of enumerating directly the G-invariant codes $C \leq \mathbf{F}_2^n$ we may enumerate all $(t + 1)$-tuples of linear codes $C_i \leq \mathbf{F}_{2^{k_i}}^{\ell_i}$. Comparing the $\mathbf{F}_2$-dimension we get $n = \sum_{i=0}^{t} k_i\ell_i$, so the length ℓ_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 $\mathbf{F}_2^n$. This is invariant under permutations, so $vg \cdot wg = v \cdot w$ for all $v, w \in \mathbf{F}_2^n$ and $g \in S_n$. We hence obtain the equation

$$vg \cdot w = v \cdot wg^{-1} \text{ for all } v, w \in \mathbf{F}_2^n, g \in S_n. \tag{2}$$

Thus the adjoint of a permutation g with respect to the inner product is $\overline{g} = g^{-1}$, for the natural involution $^{-}$ of $\mathbf{F}_2 G$. From Equation (2) we hence obtain that

$$va \cdot w = v \cdot w\overline{a} \text{ for all } v, w \in \mathbf{F}_2^n, a \in \mathbf{F}_2 G.$$

In particular the idempotents of $\mathbf{F}_2 G$ satisfy

$$vE_i \cdot wE_j = v \cdot wE_j\overline{E_i} \text{ for all } v, w \in \mathbf{F}_2^n. \tag{3}$$

Since $E_j\overline{E_i} = 0$ if $E_i \neq \overline{E_j}$ we obtain an orthogonal decomposition

$$\begin{array}{ll} \mathbf{F}_2^n & = \perp_{i=0}^r \mathbf{F}_2^n E_i \perp \perp_{j=1}^s (\mathbf{F}_2^n E_{r+2j-1} \oplus \mathbf{F}_2^n E_{r+2j}) = \\ & \perp_{i=0}^r \mathbf{F}_2^n E_i \perp \perp_{j=1}^s (\mathbf{F}_2^n \overline{E}_{r+2j} \oplus \mathbf{F}_2^n E_{r+2j}) \end{array} \tag{4}$$

Definition 2.4: For $0 \leq i \leq t$ let $\varphi_i : \mathbf{F}_{2^{k_i}}^{\ell_i} \to \mathbf{F}_2^n E_i$ be the isomorphism from Equation (1). For $0 \leq i \leq r$ define the inner product

$$h_i : \mathbf{F}_{2^{k_i}}^{\ell_i} \times \mathbf{F}_{2^{k_i}}^{\ell_i} \to \mathbf{F}_2, h_i(c, c') := \varphi_i(c) \cdot \varphi_i(c')$$

and use h_i to define the dual of a code $C_i \leq \mathbf{F}_{2^{k_i}}^{\ell_i}$ as

$$C_i^{\perp} := \{v \in \mathbf{F}_{2^{k_i}}^{\ell_i} \mid h_i(v, c) = 0 \text{ for all } c \in C_i\}.$$

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

$$s_j : \mathbf{F}_{2^{k_J}}^{\ell_J} \times \mathbf{F}_{2^{k_{J-1}}}^{\ell_{J-1}} \to \mathbf{F}_2, s_j(c, c') := \varphi_J(c) \cdot \varphi_{J-1}(c').$$

Then s_j defines the dual $C_{J-1}^{\perp} \leq \mathbf{F}_{2^{k_J}}^{\ell_J}$ of a code $C_{J-1} \leq \mathbf{F}_{2^{k_{J-1}}}^{\ell_{J-1}}$ as

$$C_{J-1}^{\perp} := \{v \in \mathbf{F}_{2^{k_J}}^{\ell_J} \mid s_j(v, c) = 0 \text{ for all } c \in C_{J-1}\}.$$

Lemma 2.5: Let $C = \varphi(C_0, \ldots, C_t) \leq \mathbf{F}_2^n$ be some G-invariant code. Then the dual code is $C^{\perp} = C'$ where

$$C' := \varphi(C_0^{\perp}, C_1^{\perp}, \ldots, C_r^{\perp}, C_{r+2}^{\perp}, C_{r+1}^{\perp}, \ldots, C_t^{\perp}, C_{t-1}^{\perp}).$$

In particular the set of all self-dual G-invariant codes $C = C^{\perp} \leq \mathbf{F}_2^n$ is the image (under the bijection φ of Lemma 2.3) of the set

$$\begin{array}{ll} \mathcal{C}_G^{sd} := & \{(C_0, C_1, \ldots, C_t) \in \mathcal{C}_G \mid C_i = C_i^{\perp} (0 \leq i \leq r) \\ & C_{r+2j} = C_{r+2j-1}^{\perp} (j = 1, \ldots, (t-r)/2)\}. \end{array}$$

Proof: Comparing dimension it is enough to show that $C^{\perp} \supseteq C'$. Since $C = \bigoplus_{i=0}^t CE_i$ and

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

it suffices to show that every 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)

$$\varphi_i(c) \cdot \varphi_j(c') = 0 \text{ for all } j \neq i \text{ and } c' \in \mathbf{F}_{2^{k_j}}^{\ell}.$$

For $j = i$ we compute

$$\varphi_i(c) \cdot \varphi_i(c') = h_i(c, c') \text{ for all } c' \in \mathbf{F}_{2^{k_i}}^{\ell}.$$

This is 0 if $c' \in C_i^{\perp}$.
Now assume that $i = r + 2k$. Then Equation (3) yields

$$\varphi_i(c) \cdot \varphi_j(c') = 0 \text{ for all } j \neq r + 2k - 1 \text{ and } c' \in \mathbf{F}_{2^{k_j}}^{\ell}.$$

For $j = r + 2k - 1$

$$\varphi_{r+2k}(c) \cdot \varphi_{r+2k-1}(c') = s_k(c, c') \text{ for all } c' \in \mathbf{F}_{2^{k_j}}^{\ell}.$$

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 $G = \{1 = g_1, \ldots, g_q\} \leq S_n$ with $q = |G|$. By assumption q is odd.

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

$$\ell_i = \ell = \frac{m}{q}$$

for all $i > 0$. After reordering the elements in $\{1, \ldots, m\}$ and 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 stabilizer in G of j consists only of the identity and hence the orbit $Gj = \{g_1(j), \ldots, g_q(j)\}$ has length q and therefore $m = \ell q$ is a multiple of $q = |G|$. From each of the ℓ orbits choose some element j_k. The reordering is now obviously

$$(g_1(j_1), g_2(j_1), \ldots, g_q(j_1), g_1(j_2), \ldots, g_q(j_\ell)).$$

■

In this new group the permutation matrices P_g are block diagonal matrices with ℓ 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

$$\begin{array}{l} E_0 = \text{diag}(B_0, \ldots, B_0, I_{n-m}) \\ E_i = \text{diag}(B_i, \ldots, B_i, 0_{n-m}) \quad 1 \leq i \leq t. \end{array}$$

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

$$\eta_i : \mathbf{F}_2 G e_i \to \text{rowspace}(B_i), \sum_{k=1}^{q} \epsilon_k g_k e_i \mapsto (\epsilon_1, \ldots, \epsilon_q) B_i.$$

Then the isomorphism $\varphi_i : \mathbf{F}_{2^{k_i}}^{\ell} \to \mathbf{F}_2^n E_i \leq \mathbf{F}_2^n$ is defined by

$$\varphi_i(c_1, \ldots, c_\ell) := (\eta_i(\tilde{\varphi}_i(c_1)), \eta_i(\tilde{\varphi}_i(c_2)), \ldots, \eta_i(\tilde{\varphi}_i(c_\ell))).$$

Lemma 2.7: In the situation above define a weight function $w_i : \mathbf{F}_{2^{k_i}} \to \mathbf{Z}_{\geq 0}$ by

$$w_i(x) := \mathrm{wt}(\eta_i(\tilde{\varphi}_i(x))).$$

If $i \geq 1$ or $m = n$, then

$$\mathrm{wt}_i : \mathbf{F}_{2^{k_i}}^{\ell} \to \mathbf{Z}_{\geq 0}, c \mapsto \sum_{k=1}^{\ell} w_i(c_k)$$

defines a weight function on $\mathbf{F}_{2^{k_i}}^{\ell}$ such that the isomorphism φ_i is weight preserving.

Proof: We need to show that $\mathrm{wt}(\varphi_i(c)) = \mathrm{wt}_i(c)$ for all $c \in \mathbf{F}_{2^{k_i}}^{\ell}$. But $\varphi_i((c_1, \ldots, c_\ell))$

$$= (\eta_i(\tilde{\varphi}_i(c_1)), \eta_i(\tilde{\varphi}_i(c_2)), \ldots, \eta_i(\tilde{\varphi}_i(c_\ell)), 0^{n-m})$$

and so the weight of $\varphi_i(c)$ is the sum

$$\mathrm{wt}(\varphi_i(c)) = \sum_{k=1}^{\ell} \mathrm{wt}(\eta_i(\tilde{\varphi}_i(c_k))) = \sum_{k=1}^{\ell} w_i(c_k).$$

■

Remark 2.8: For $m < n$ and $i = 0$, we need to modify the weight function because we work with ℓ blocks of size q and $n - m$ blocks of size 1. So here $\mathrm{wt}_0 : \mathbf{F}_2^{\ell+(n-m)} \to \mathbf{Z}_{\geq 0}$

$$\mathrm{wt}_0(c_1, \ldots, c_\ell, d_1, \ldots, d_{n-m}) = \\ q\,\mathrm{wt}(c_1, \ldots, c_\ell) + \mathrm{wt}(d_1, \ldots, d_{n-m}).$$

Remark 2.9: We will always work with G-equivalence classes of codes, where $C, C' \leq \mathbf{F}_2^n$ 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

$$S_{n,G} \cong G \wr S_\ell \times S_{n-m}$$

is obtained by the action of G on the blocks of size q and the symmetric group S_ℓ permuting the ℓ blocks of size q. The group S_{n-m} permutes the last $n - m$ entries. Via the isomorphism φ_i constructed in Lemma 2.7 the action of $S_{n,G}$ on $\mathbf{F}_2^n E_i \cong \mathbf{F}_{2^{k_i}}^{\ell}$ translates into the monomial action with monomial entries in the subgroup

$$\langle \varphi_i^{-1}(ge_i) \mid g \in G \rangle \leq \mathbf{F}_{2^{k_i}}^{*}.$$

Note that these are weight preserving automorphisms of the space $\mathbf{F}_{2^{k_i}}^{\ell}$ for the weight function defined in Lemma 2.7.

Remark 2.10: For the weight preserving isomorphisms φ_i constructed in Lemma 2.7 the inner product h_i and s_j defined in Definition 2.4 are (Hermitian) standard inner products: For $0 < i \leq r$ and $c, c' \in \mathbf{F}_{2^{k_i}}^{\ell}$ $h_i(c, c') =$

$$\sum_{k=1}^{\ell} \eta_i(\tilde{\varphi}_i(c_k)) \cdot \eta_i(\tilde{\varphi}_i(c'_k)) = \sum_{k=1}^{\ell} trace_{\mathbf{F}_{2^{k_i}}/\mathbf{F}_2}(c_k \sigma(c'_k))$$

where σ is the automorphism of $\mathbf{F}_{2^{k_i}}$ of order 2 (Lemma 2.2). For $1 \leq j \leq s$ with $J := r + 2j$, $c \in \mathbf{F}_{2^{k_J}}^{\ell}, c' \in \mathbf{F}_{2^{k_{J-1}}}^{\ell}$

$$s_j(c, c') = \sum_{k=1}^{\ell} \eta_J(\tilde{\varphi}_J(c_k)) \cdot \eta_{J-1}(\tilde{\varphi}_{J-1}(c'_k))$$

E. Strategy of computation

The computational strategy to enumerate representatives of the G-equivalence classes of all self-dual G-invariant codes $C = C^\perp \leq \mathbf{F}_2^n$ with minimum weight d is as follows: We successively enumerate the codes $C_0, C_1, \ldots$ such that $(C_0, \ldots, C_t) \in \mathcal{C}_G^{sd}$ yields a self-dual G-invariant code by Lemma 2.5. With Lemma 2.7 we control the minimum weight of $\varphi_i(C_i)$ using the suitable weight function wt_i on $\mathbf{F}_{2^{k_i}}^{\ell}$. We only continue with those codes $(C_0, \ldots, C_i)$ for which

$$\bigoplus_{j=0}^{i} \varphi_j(C_j) \leq \mathbf{F}_2^n$$

has minimum weight $\geq d$. Equivalence translates into the monomial equivalence from Remark 2.9. We have a simultaneous action of the monomial group

$$\mathcal{M} := \langle (\varphi_0^{-1}(ge_0), \ldots, \varphi_t^{-1}(ge_t)) \mid g \in G \rangle \wr S_\ell \times S_{n-m}.$$

If we have already found the tuple $(C_0, \ldots, C_i)$ then only the stabilizer in $\mathcal{M}$ of these $i + 1$ codes acts on the set of candidates for C_{i+1}.

III. The case $Z_3 \times Z_3$

From now on let $C \leq \mathbf{F}_2^{72}$ be a binary self-dual code with minimum distance 16. Then C is doubly-even (see [14]) and hence an extremal Type II code.

In this section we assume that $\mathrm{Aut}(C)$ contains a subgroup G isomorphic to $Z_3 \times Z_3$. By [3, Theorem 1.1] every element of order 3 in $\mathrm{Aut}(C)$ acts without fixed points on $\{1, \ldots, 72\}$, so G is conjugate in S_{72} to the subgroup $G = \langle g, h \rangle \leq S_{72}$ where

$$\begin{array}{rcl} g & = & (1,4,7)(2,5,8)(3,6,9)\ldots(66,69,72) \\ h & = & (1,2,3)(4,5,6)(7,8,9)\ldots(70,71,72) \end{array}$$

The following lemma gives the structure of the fixed code of any $1 \neq g \in G$.

Lemma 3.1: (cf. [9]) Let C be a Type II code of length 72 and minimum distance 16 and let $g \in \mathrm{Aut}(C)$ be an automorphism of order 3. Then the fixed code of g in C is equivalent to $\mathcal{G}_{24} \otimes \langle (1,1,1) \rangle$, where $\mathcal{G}_{24} \leq \mathbf{F}_2^{24}$ is the extended binary Golay code, the unique binary $[24, 12, 8]$-code.

Proof: We apply the methods of Section II to the group $\langle g \rangle \leq S_{72}$. Let $E_0 := 1 + P_g + P_g^2 \in \mathbf{F}_2^{72 \times 72}$. Then E_0 is the projection onto the fixed space of g, $\mathbf{F}_2^{72} E_0 \cong \varphi_0(\mathbf{F}_2^{24})$ and $CE_0 = \varphi_0(\mathcal{G})$ for some self-dual binary code $\mathcal{G} \leq \mathbf{F}_2^{24}$ (see Lemma 2.5). Since C is doubly-even, $\mathcal{G}$ is a Type II code. Moreover the minimum distance of $\varphi_0(\mathcal{G})$ is 3 times the minimum distance of $\mathcal{G}$ (see Lemma 2.7). Since $CE_0 \leq C$ has minimum distance ≥ 16, we conclude that the minimum distance of $\mathcal{G}$ is ≥ 6 and hence ≥ 8 since $\mathcal{G}$ is doubly-even. This shows that $\mathcal{G}$ is equivalent to the Golay code. ■

Remark 3.2: Let

$$C(h) := \{c \in C \mid ch = c\} \cong \mathcal{G} \otimes \langle (1,1,1) \rangle$$

be the fixed code of h. Then g acts as an automorphism g' on the Golay code $\mathcal{G}$ and has no fixed points on the places of $\mathcal{G}$. Up to conjugacy in $\mathrm{Aut}(\mathcal{G})$ 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 φ_i from those defined by G, we use ψ instead of φ. As an $\mathbf{F}_2\langle g' \rangle$ module the code $\mathcal{G}$ decomposes as

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

Explicit computations show that $D_0 \cong h_8 \leq \mathbf{F}_2^8$ is the extended Hamming code h_8 of length 8 and $D_1 \cong \mathbf{F}_4 \otimes_{\mathbf{F}_2} h_8$.

We now use the isomorphisms φ_i constructed in Section II-B for the group $G = \langle g, h \rangle \cong Z_3 \times Z_3$ 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 $C = C^\perp \leq \mathbf{F}_2^{72}$ decomposes as

$$C = \perp_{i=0}^4 \varphi_i(C_i) \text{ (see Lemma 2.5)}$$

for some self-dual Type II code $C_0 \leq \mathbf{F}_2^8$ and Hermitian self-dual codes $C_1, \ldots, C_4 \leq \mathbf{F}_4^8$ (see Remark 2.10). By Remark 3.2 all codes $C_i \leq \mathbf{F}_4^8$ (for $i = 1, 2, 3, 4$) are equivalent to the code D_1:

Remark 3.3: $C_i \cong \mathbf{F}_4 \otimes_{\mathbf{F}_2} h_8$ for all $i = 1, 2, 3, 4$. Moreover for all $i = 1, 2, 3, 4$ the code

$$\psi_0(C_0) \oplus \psi_i(C_i) \cong \mathcal{G}$$

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 $\mathrm{Aut}(C)$ contains $Z_3 \times Z_3$.

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 $C_0 \leq \mathbf{F}_2^8$ of the Hamming code h_8. We then compute the orbit of $\mathbf{F}_4 \otimes_{\mathbf{F}_2} h_8$ under the full monomial group $\mathbf{F}_4^* \wr S_8$ and check for all these codes $C_i \leq \mathbf{F}_4^8$ whether $\psi_0(C_0) \oplus \psi_1(C_i)$ has minimum distance 8. This yields a list $\mathcal{L}$ of $17,496$ candidates for the codes $C_i \leq \mathbf{F}_4^8$.

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 $C_0 \leq \mathbf{F}_2^8$ and $C_1 \leq \mathbf{F}_4^8$. The centralizer of g' in the automorphism group of

$$\mathcal{G} = \psi_0(C_0) \perp \psi_1(C_1)$$

acts on $\mathcal{L}$ 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 ≥ 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

$$\mathcal{L}_3(D) := \{C_3 \in \mathcal{L} \mid d(D \oplus \varphi_3(C_3)) \geq 16\}$$

and similarly

$$\mathcal{L}_4(D) := \{C_4 \in \mathcal{L} \mid d(D \oplus \varphi_4(C_4)) \geq 16\}.$$

The cardinalities are

$$|\mathcal{L}_3(D)| = |\mathcal{L}_4(D)| = 7146 \text{ or } 2940.$$

It takes about 2 days of computing time to go through the list of pairs $(C_3, C_4) \in \mathcal{L}_3(D) \times \mathcal{L}_4(D)$ and check whether $D \oplus \varphi_3(C_3) \oplus \varphi_4(C_4)$ has minimum distance ≥ 16 using Magma [1]. No extremal code is found. ■

IV. AUTOMORPHISMS OF ORDER SEVEN

Let $C = C^\perp \leq \mathbf{F}_2^{72}$ be an extremal Type II code. Assume that there is an element $g \in \mathrm{Aut}(C)$ of order 7. Then by [6, Theorem 6] the permutation $g \in S_{72}$ is the product of 10 seven-cycles. Without loss of generality we assume that

$$g = (1, \ldots, 7)(8, \ldots, 14) \cdots (83, \ldots, 70)$$

fixes the points 71 and 72, so in the notation of Lemma 2.7 $m = 70$. The central primitive idempotents

$$e_0 = \sum_{i=0}^{6} g^i, \;\; e_1 = g^4 + g^2 + g + 1, \;\; e_2 = g^6 + g^5 + g^3 + 1$$

of $\mathbf{F}_2\langle g \rangle$ satisfy

$$\overline{e_1} = e_2 \text{ and } \mathbf{F}_2\langle g \rangle e_i \cong \mathbf{F}_8 \text{ for } i = 1, 2.$$

In the notation of Section II the code C is of the form

$$C = \varphi_0(C_0) \perp \varphi_1(C_1) \oplus \varphi_2(C_1^\perp)$$

for some self-dual code

$$C_0 = C_0^\perp \leq \mathbf{F}_2^{10+2}$$

and $C_1 \leq \mathbf{F}_8^{10}$. To obtain weight preserving isomorphisms φ_i we consider the kernel D of the projection of C onto the last 2 coordinates. So let

$$D_0 := \{(c_1, \ldots, c_{10}) \mid (c_1, \ldots, c_{10}, 0, 0) \in C_0\}$$

and define $D := \varphi_0(D_0) \perp \varphi_1(C_1) \oplus \varphi_2(C_1^\perp) \leq \mathbf{F}_2^{70}$. Then

$$D = \{(c_1, \ldots, c_{70}) \mid (c_1, \ldots, c_{70}, 0, 0) \in C\}$$

is a doubly-even code of dimension 34 and minimum distance ≥ 16. Applying Lemma 2.7 and Lemma 2.5 to this situation one finds the conditions

$$\begin{array}{ll} D_0 \subset D_0^\perp \leq \mathbf{F}_2^{10} & \text{doubly even} \\ C_1 \leq \mathbf{F}_8^{10} & d(C_1) \geq 4, d(C_1^\perp) \geq 4. \end{array}$$

We hence compute the linear codes $C_1 \leq \mathbf{F}_8^{10}$ such that $d := d(C_1) \geq 4$ and the dual distance $d^\perp = d(C_1^\perp) \geq 4$. For each such code C_1 we check if the code

$$\tilde{C}_1 := \varphi_1(C_1) \oplus \varphi_2(C_1^\perp) \leq \mathbf{F}_2^{70}$$

has minimum distance ≥ 16.

Lemma 4.1: If C is an extremal Type II code then D_0 is equivalent to the maximal doubly-even subcode E of the 2-fold repetition code $\mathbf{F}_2^5 \otimes \langle (1,1) \rangle$.

Proof: Clearly $D_0 \leq \mathbf{F}_2^{10}$ is doubly-even and of dimension 4,

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

Parameters of C_1			Number of non-isomorphic candidates	
k	d	$d^\perp$	for C_1	for C_1 with $d(\tilde{C}_1) \geq 16$
3	8	4	1	1
4	4	4	81,717	657
4	5	4	1,854,753	8,657
4	6	4	490,382	2,632
5	4	4	61,487,808	145,918
5	5	4	3,742,898	10,769
5	5	5	3,014,997	9,216
Total			70,672,556	177,850

TABLE I
COMPUTATIONAL RESULTS FOR Z_7

with $A_0 = A_0^\perp$ a Type I code and $A_2 = A_1^\perp$. Then

$$C_0 = \{(a,1,1) \mid a \in A_0 \setminus D_0\} \dot\cup \{(a,0,0) \mid a \in D_0\} \dot\cup \{(a,1,0) \mid a \in A_1 \setminus D_0\} \dot\cup \{(a,0,1) \mid a \in A_2 \setminus D_0\}$$

For $a \in D_0^\perp$ and $x \in \mathbf{F}_2^2$ the weight

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

because φ_0 repeats the first 10 coordinates 7 times (see Remark 2.8) and leaves the last two unchanged. Since $\varphi_0(C_0)$ is doubly-even and has minimum distance ≥ 16 weights in $D_0^\perp \setminus A_0$ are > 1 and $\equiv 1 \pmod 4$ and hence ≥ 5. This forces A_0 to be equivalent to $\mathbf{F}_2^5 \otimes \langle(1,1)\rangle$. ■

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 ≥ 16. For this purpose we classify all codes in $C_1 \leq \mathbf{F}_8^{10}$ such that C_1 and its dual $C_1^\perp$ both have minimum distance ≥ 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 semi-linear isometry there are more than 70 million such codes. The condition that the minimum distance of the code $\tilde{C}_1 := \varphi_1(C_1) \oplus \varphi_2(C_1^\perp)$ is ≥ 16 reduces the number of codes to 177,850 codes that need to be tested, see Table I for details. For each of these codes $\tilde{C}_1$ we run through all 945 different binary codes $D_0 \leq \mathbf{F}_2^{10}$ that are equivalent to E from Lemma 4.1 and check whether the code $D := \varphi_0(D_0) \oplus \tilde{C}_1$ has minimum distance ≥ 16. No such code is found. ■

V. THE DIHEDRAL GROUP OF ORDER 10

A. Automorphisms of order 5

Let $C = C^\perp \leq \mathbf{F}_2^{72}$ be an extremal Type II code. Assume that there is some $g \in \mathrm{Aut}(C)$ of order 5. By [6, Theorem 6] the permutation $g \in S_{72}$ is the product of 14 five-cycles and we assume that

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

The primitive idempotents in $\mathbf{F}_2\langle g\rangle$ are

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

and $\mathbf{F}_2\langle g\rangle e_1 \cong \mathbf{F}_{16}$. As an $\mathbf{F}_2\langle g\rangle$ submodule of $\mathbf{F}_2^{72}$, the code C decomposes as

$$\varphi_0(C_0) \perp \varphi_1(C_1),\ \text{with } C_0 = C_0^\perp \leq \mathbf{F}_2^{16}, C_1 = C_1^\perp \leq \mathbf{F}_{16}^{14}.$$

As above let $D := \{(c_1,\dots,c_{70}) \mid (c_1,\dots,c_{70},0,0) \in C\}$. Then D is a doubly-even code in $\mathbf{F}_2^{70}$ of dimension 34 and minimum distance ≥ 16 and

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

for some doubly-even code $D_0 \leq \mathbf{F}_2^{14}$ 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 $A_0 \leq \mathbf{F}_2^{14}$ of minimum distance 4.

Proof: Clearly $D_0 \leq \mathbf{F}_2^{14}$ 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 4.1, code C_0 is a full glue of $D_0^\perp/D_0$ and $\mathbf{F}_2^2$. For $a \in D_0^\perp$ and $x \in \mathbf{F}_2^2$ the weight of

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

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

To obtain a weight preserving isomorphism $\varphi_1 : \mathbf{F}_{16}^{14} \to \mathbf{F}_2^{72}E_1$ as described in Lemma 2.7 we need to define the suitable weight function on the coordinates $c_k \in \mathbf{F}_{16}$.

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

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

For $c = (c_1,\dots,c_n) \in \mathbf{F}_{16}^n$ we let as usual $\mathrm{wt}_5(c) := \sum_{i=1}^n \mathrm{wt}_5(c_i)$.

B. The dihedral group of order 10

We now assume that $C = C^\perp \leq \mathbf{F}_2^{72}$ is an extremal Type II code such that

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

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

$$g = (1,2,3,4,5)(6,7,8,9,10)\dots(66,67,68,69,70),$$
$$h = (1,6)(2,10)(3,9)(4,8)(5,7)\dots(61,66)(62,70)(63,69)(64,68)(65,67)\cdot(71,72).$$

The centralizer in S_{72} of G is isomorphic to $D_{10} \wr S_7 \times \langle(71,72)\rangle$ and acts on the set of G-invariant codes.

Remark 5.3: Let e_0 and $e_1 = 1 + e_0 \in \mathbf{F}_2\langle g\rangle \leq \mathbf{F}_2G$ be as above. Then e_0 and e_1 are the central primitive idempotents in $\mathbf{F}_2G$. In particular $\langle h\rangle$ acts on the codes CE_0 and CE_1.

Remark 5.4: Explicit computations with Magma [1] 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 $\langle g\rangle$ 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

$$\mathcal{C}_0 := \{\varphi_0(C_0) \mid C_0 \in O_{14}\}.$$

To investigate the action of h on the Hermitian self-dual code $C_1 \le \mathbf{F}_{16}^{14}$ we recall the following theorem.

Theorem 5.5: ([13, Theorem 3.1]) The fixed code $C(h) := \{c \in C \mid ch = c\}$ of $\langle h\rangle$ is equivalent to $B \otimes \langle(1,1)\rangle$ for some self-dual code $B = B^{\perp} \le \mathbf{F}_2^{36}$ of minimum distance 8.

Let

$$\overline{} : \mathbf{F}_{16} \to \mathbf{F}_{16}, x \mapsto \overline{x} = x^4$$

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

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

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

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

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

Corollary 5.6: The code $X := \pi(C_1(h)) :=$

$$\{(x_1, \ldots, x_7) \mid (x_1, \overline{x_1}, \ldots, x_7, \overline{x_7}) \in C_1\} \le \mathbf{F}_{16}^7$$

is an $\mathbf{F}_4$-linear trace-Hermitian self-dual code $X = X^{\perp}$ where

$$X^{\perp} := \{v \in \mathbf{F}_{16}^7 \mid \sum_{i=1}^{7} \mathrm{trace}_{\mathbf{F}_{16}/\mathbf{F}_4} x_i \overline{v_i} = 0 \text{ for all } x \in X\}$$

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

$$C_1 = \Psi(X) := \langle (x_1, \overline{x_1}, \ldots, x_7, \overline{x_7}) \mid (x_1, \ldots, x_7) \in X\rangle_{\mathbf{F}_{16}}.$$

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

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

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

We call such a generator matrix *systematic*.

Proof: The condition on the minimum 5-weight implies that there is at least one column with two $\mathbf{F}_4$-linearly independent entries. Use the group action of $\mathrm{GL}_7(\mathbf{F}_4) \times (D_{10} \wr S_7)$ to map this column to $(0, \ldots, 0, 1, \xi)^T$ 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 $\mathrm{Aut}(C)$ contains the dihedral group of order 10.

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

Let Ψ be the map from the $\mathbf{F}_4$-linear codes in $\mathbf{F}_{16}^7$ to the $\mathbf{F}_{16}$-linear codes in $\mathbf{F}_{16}^{14}$ from Corollary 5.6. Let $\mathcal{C}_0$ be the list of 1920 codes of length 72 from Remark 5.4 and let $\mathcal{X}$ denote a system of representatives of $D_{10} \wr S_7$ equivalence classes of trace-Hermitian self-dual codes $X \le \mathbf{F}_{16}^7$ with minimal 5-weight at least 8. Then

$$C \cong \varphi_0(C_0) \oplus \varphi_1(\Psi(X)) \text{ for some } C_0 \in \mathcal{C}_0 \text{ and some } X \in \mathcal{X}.$$

For the proof of the theorem we summarize our construction method for all systematic generator matrices of $\mathbf{F}_4$-linear trace-Hermitian self-dual codes $X \le \mathbf{F}_{16}^7$ with minimal 5-weight at least 8 up to equivalence under $D_{10} \wr S_7$. Furthermore, we restrict to these codes that might be extended by a binary code $C_0 \in \mathcal{C}_0$ such that $\varphi_0(C_0) \oplus \varphi_1(\Psi(X))$ has minimum distance ≥ 16.

The construction starts with the first row and iteratively adds a further row fulfilling the conditions on the systematic form. A backtracking approach is applied: whenever the condition on the 5-weight or self-orthogonality is violated, the code $\langle \Gamma_{1,*}, \ldots, \Gamma_{i-1,*}\rangle_{\mathbf{F}_4}$ is isomorphic to some other code already examined or there is no code C_0 such that $\varphi_0(C_0) \oplus \varphi_1(\Psi(\langle \Gamma_{1,*}, \ldots, \Gamma_{i-1,*}\rangle_{\mathbf{F}_4}))$ has minimum distance ≥ 16.

The following observations are used to speed up the computations:

- Each element in $\mathbf{F}_{16}^7$ is self-orthogonal under the trace-Hermitian inner product.
- Each row $\Gamma_{i,*}$ must have minimum 5-weight at least 8. Since the 5-weight is not constant under scalar multiplication by elements $\mu \in \mathbf{F}_4^*$ we also have to test $\mathrm{wt}_5(\mu\Gamma_{i,*})$. This reduces the candidates for the first row to 3525 vectors. There are 15705 candidates for the other rows.
- The action of $\mathbf{F}_4^* \times (D_{10} \wr S_7)$ 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 $\langle \Gamma_{1,*}, \ldots, \Gamma_{i-1,*}\rangle_{\mathbf{F}_4}$.
- If some candidate v for row i is either not trace-Hermitian orthogonal to some preceding row $\Gamma_{j,*}, j \le i-2$ or the minimum 5-weight of $\langle v, \Gamma_{1,*}, \ldots, \Gamma_{i-2,*}\rangle_{\mathbf{F}_4}$ 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 $\mathcal{L}^{(0)} = \mathcal{C}_0$ 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

$$\mathcal{L}^{(i)} := \{C_0 \in \mathcal{L}^{(i-1)} : d\left(\varphi_0(C_0) \oplus \varphi_1(\Psi(\langle \Gamma_{1,*}, \ldots, \Gamma_{i,*}\rangle_{\mathbf{F}_4}))\right) \ge 16\}.$$

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

k	Number of non-isomorphic candidates for first k rows
1	6
2	463
3	4,885
4	856,804
5	416,899
6	306
7	4

TABLE II
COMPUTATIONAL RESULTS FOR D_{10}

We test if a code is isomorphic to one that is already processed by calculating unique orbit representatives using a modification of [8]. This computation returns at the same time without any additional effort the stabilizer of $\langle \Gamma_{1,*}, \ldots, \Gamma_{i,*} \rangle_{\mathbf{F}_4}$ in $D_{10} \wr S_7$. The computations have been performed in Magma [1] 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 $\mathbf{F}_4$-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 $\mathcal{L}^{(7)}$ of candidates for C_0 are empty.

In contrast to [7] 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 $C_0 \in \mathcal{C}_0$. ∎

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 and nonexistence results for linear codes with prescribed minimum distances.* Designs, Codes, and Cryptography, DOI: 10.1007/s10623-012-9700-8

[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) 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)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, *A Putative Doubly Even [72, 36, 16] Code Does Not Have an Automorphism of Order 9.* IEEE Trans. Inform. Theory 58 (2012) 159-163

Thomas Feulner Thomas Feulner was born in Germany in 1982. He received the Diploma degree in mathematics from the University of Bayreuth, Bayreuth, Germany in 2008. Since then, he is working as a research assistant at the University of Bayreuth, Germany. His research interests cover coding theory, cryptography and group actions on combinatorial structures.

Gabriele Nebe Gabriele Nebe received her PhD in mathematics from the RWTH Aachen university in 1995. She was assistant professor in Aachen (1995-2000), professor in Ulm (2000-2004) and is now professor at the RWTH Aachen university. She had visiting positions in Bordeaux, Harvard, EPFL, Sydney and AT&T Shannon Labs. Her research interests include representation theory of finite groups, lattices, spherical designs, and modular forms, and the analogues in coding theory.