

THE AUTOMORPHISM GROUP OF AN EXTREMAL $[72, 36, 16]$ CODE HAS ORDER AT MOST 2

TEJASVI SINGH TOMAR

ABSTRACT. Whether a binary doubly-even self-dual $[72, 36, 16]$ code exists is a question raised by Sloane in 1973. The automorphism group of such a code is known to be trivial or isomorphic to C_2 , C_3 , $C_2 \times C_2$ or C_5 . We exclude C_5 , $C_2 \times C_2$ and C_3 . For an automorphism of order 5 the fixed subcode is $e_8 \oplus e_8$, and minimum distance 16 becomes a condition on a 7×7 unitary matrix over $\mathbb{F}_{16}$. For a subgroup $\langle a, b \rangle \cong C_2 \times C_2$ the code is determined by a symmetric bilinear form on the contracted fixed code of a , which is one of the 41 self-dual $[36, 18, 8]$ codes. After a normalisation the form ranges over an affine space of dimension 63, 64 or 65, and minimum distance 16 becomes one syndrome condition for each word of weight 8, 10 or 12. For an automorphism of order 3 the code is determined by a Hermitian self-dual $[24, 12, 8]$ code over $\mathbb{F}_4$ and a labelling of its coordinates by the points of the extended Golay code. We classify these codes over $\mathbb{F}_4$: there are 26 924 931 of them up to monomial equivalence. Exhaustive computer searches show that none of the three reduced problems has a solution. Each search is confirmed by a second implementation, and tests on known codes recover them. Consequently the automorphism group of an extremal $[72, 36, 16]$ code is trivial or of order 2.

1. INTRODUCTION

A binary linear code $C = C^\perp \leq \mathbb{F}_2^n$ is *doubly-even self-dual*, or of Type II, if all its weights are divisible by 4. Its minimum weight satisfies $d \leq 4\lfloor n/24 \rfloor + 4$ [31] (see also [37, Sect. 9, Thm. 26]), and C is *extremal* if equality holds. Extremal codes of lengths 24 and 48 exist: the extended Golay code and the extended quadratic residue code of length 48. Whether an extremal code of length 72, that is, a doubly-even self-dual $[72, 36, 16]$ code, exists is a question of Sloane [38]. It is still open.

A series of papers restricts the automorphism group of such a code [5, 6, 8–11, 15, 19, 26, 33–36, 39, 40, 42]. Together they show that the automorphism group is trivial or isomorphic to C_2 , C_3 , $C_2 \times C_2$ or C_5 (see Borello’s survey [7, Thm. 6.3]). Two arXiv preprints that claimed stronger results were withdrawn by their authors [18, 27]. We exclude C_5 , $C_2 \times C_2$ and C_3 .

Theorem A. *A binary doubly-even self-dual $[72, 36, 16]$ code has no automorphism of order 5.*

Theorem B. *The automorphism group of a binary doubly-even self-dual $[72, 36, 16]$ code has no subgroup isomorphic to $C_2 \times C_2$.*

Theorem C. *A binary doubly-even self-dual $[72, 36, 16]$ code has no automorphism of order 3.*

Theorem D. *There are exactly 26 924 931 Hermitian self-dual $[24, 12, 8]$ codes over $\mathbb{F}_4$ up to monomial equivalence, and exactly 13 485 816 up to monomial equivalence and conjugation.*

Corollary. *The automorphism group of a binary doubly-even self-dual $[72, 36, 16]$ code is trivial or isomorphic to C_2 .*

Proof. By the list above the group is trivial or isomorphic to C_2 , C_3 , $C_2 \times C_2$ or C_5 . Theorems A, B and C exclude C_5 , $C_2 \times C_2$ and C_3 . □

2020 *Mathematics Subject Classification.* 94B05; 20B25, 05E18, 68V05.

Key words and phrases. Extremal self-dual codes, doubly-even codes, automorphism groups, Hermitian self-dual codes over $\mathbb{F}_4$, extended Golay code, classification, computer-assisted proof.

Theorem C confirms Conjecture 5.5 of the preprint [2], which predicts that the automorphism group of such a code is not generated by an automorphism of order 3.

The proofs of Theorems A–C reduce each statement to a finite search. For an automorphism of order 5 we show that the fixed subcode is $e_8 \oplus e_8$ with the two fixed points in different components. The code is then described by a 7×7 unitary matrix U over $\mathbb{F}_{16}$, and minimum distance 16 becomes a condition on the distances of a and of aU to the two copies of e_8 (Section 2). For a subgroup $\langle a, b \rangle \cong C_2 \times C_2$ we use results of Bouyuklieva and Nebe to write the code as $\{(z \mid z + y)\}$, with y in the contracted fixed code Y of a and z in a coset of Y determined by a symmetric bilinear form B on Y . The involution b is an automorphism exactly when B is invariant under the involution of Y induced by b . Swaps inside the cycles of a , including one swap that interchanges b and ab , normalise B further, and minimum distance 16 becomes one syndrome condition for each word of weight 8, 10 or 12 in Y (Section 3). For an automorphism of order 3 the fixed subcode is the tripled extended Golay code, and the rest of the code is a Hermitian self-dual $[24, 12, 8]$ code E over $\mathbb{F}_4$ placed on the cycles. Minimum distance 16 is then equivalent to three conditions on how the supports of the words of weight 8, 10 and 12 of E meet the octads and dodecads of the Golay code. We classify the codes E (Theorem D) and test each class with two exact programs for a labelling of its coordinates by the Golay points that satisfies these conditions (Section 4).

The proofs are computer-assisted. Statements marked $\dagger$ rest on a computer calculation. Tables 3, 4 and 5 list these calculations for Theorem A, Theorem B and Theorems C and D, with their re-checks: brute-force recounts, independent implementations, independent cross-checks, certificates for the last search level, and tests on known codes.

Conventions. All codes are binary unless stated otherwise. For $x \in \mathbb{F}_2^n$ we write $|x|$ for the weight, $\text{supp } x$ for the support and $\langle x, y \rangle = \sum_i x_i y_i$. We identify a set of coordinates with its characteristic vector, so that $|x \cap y|$ is the number of common coordinates of x and y . A permutation p of the coordinates acts by $(xp)_{p(i)} = x_i$, and $\text{Aut}(C)$ is the group of permutations p with $Cp = C$. Two codes are equivalent if a permutation maps one onto the other. Throughout, C denotes a doubly-even self-dual $[72, 36, 16]$ code. We use the identity $|x + y| = |x| + |y| - 2|x \cap y|$ without comment.

2. AUTOMORPHISMS OF ORDER 5

2.1. Decomposition. Let $g \in \text{Aut}(C)$ have order 5. By Conway and Pless [15] (see also [19, §V.A]), g has 14 cycles of length 5 and two fixed points. We number the coordinates so that the i -th cycle is $\{5i, \dots, 5i + 4\}$ for $0 \leq i \leq 13$, with g acting on it as the cyclic shift, and the fixed points are 70 and 71.

Let $F = \{v \in C : vg = v\}$, and let E be the set of $v \in C$ that vanish on the fixed points and have even weight on each cycle. Then $C = F \oplus E$ and $F \perp E$ [25, 43]. Both summands have a simple description.

- $F = \varphi_0(C_0)$, where $\varphi_0(a, x)$ repeats a_i on the i -th cycle and places $x \in \mathbb{F}_2^2$ on the fixed points. The code $C_0 \leq \mathbb{F}_2^{16}$ is self-dual [25], and $|\varphi_0(a, x)| = 5|a| + |x|$.
- $E = \varphi_1(C_1)$ with $C_1 \leq \mathbb{F}_{16}^{14}$. Here $\mathbb{F}_{16} = \mathbb{F}_2[t]/(t^4 + t^3 + t^2 + t + 1)$ is identified with the even-weight code of length 5 by $\psi(p(t)) = p(t)(t + t^2 + t^3 + t^4)$ in $\mathbb{F}_2[t]/(t^5 - 1)$, and φ_1 applies ψ on each cycle. Multiplication by t is the action of g . The code C_1 is $\mathbb{F}_{16}$ -linear and self-dual for the Hermitian form $\langle u, v \rangle = \sum_i u_i \bar{v}_i$ with $\bar{y} = y^4$ [19, Sect. II, Lemmas 2.2 and 2.5].

The norm $N(y) = y\bar{y} = y^5$ maps $\mathbb{F}_{16}^\times$ onto $\mathbb{F}_4^\times$. Its fibres are the three cosets of the group μ_5 of fifth roots of unity, which we call *norm classes*: class 1 is μ_5 , class 2 contains $1 + t$, and class 3 contains $1 + t^2$. For $y \neq 0$ we have $|\psi(y)| = 4$ if $y \in \mu_5$ and $|\psi(y)| = 2$ otherwise.

2.2. The fixed code.

Lemma 2.1. *Up to a permutation of the cycles and of the fixed points, $C_0 = e_8 \oplus e_8$, with one fixed point in each component.*

Proof. Each nonzero $(a, x) \in C_0$ satisfies $5|a| + |x| \geq 16$ and $5|a| + |x| \equiv 0 \pmod{4}$. Hence $|a| + |x| \equiv 0 \pmod{4}$ and $|a| \geq 3$, so C_0 is a doubly-even self-dual $[16, 8, 4]$ code. A word with $x = (1, 1)$ has $|a| \geq 6$, so no word of weight 4 in C_0 contains both fixed points. The doubly-even self-dual codes of length 16 are $e_8 \oplus e_8$ and d_{16}^+ . Indeed, $16!/|\text{Aut}(e_8 \oplus e_8)| + 16!/|\text{Aut}(d_{16}^+)| = 5\,791\,500 + 4\,054\,050 = 9\,845\,550 = \prod_{i=0}^6 (2^i + 1)$, which is the number of doubly-even self-dual codes of length 16. Each pair of coordinates of d_{16}^+ lies in a word of weight 4. In $e_8 \oplus e_8$ exactly the pairs inside one component do. The claim follows because $\text{Aut}(e_8)$ is transitive on the coordinates. This is equivalent to [19, Lemma 5.1]. $\square$

From now on $C_0 = e_8 \oplus e_8$. The cycles split into two sides A and B of seven cycles each. We number the cycles of each side $0, \dots, 6$ and regard them as the points of a Fano plane with lines

$$\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 0\}, \{5, 6, 1\}, \{6, 0, 2\}.$$

The words of e_8 on one side are the 16 pairs (S, x) , with S a set of cycles and x the value at the fixed point: $(\emptyset, 0)$, $(L, 1)$ and $(\bar{L}, 0)$ for the seven lines L , and $(\{0, \dots, 6\}, 1)$.

2.3. Reduction to a unitary matrix. For $v \in \mathbb{F}_{16}^7$ let $w_i = |\psi(v_i)|$ and

$$M(v) = \min_{(S, x)} \left(5|S| + x + \sum_{i \notin S} w_i - \sum_{i \in S} w_i \right),$$

the minimum over the 16 words (S, x) of e_8 . The expression in brackets is the weight, on one side, of $\varphi_0(S, x) + \varphi_1(v)$. Thus $M(v)$ is the distance from $\varphi_1(v)$ to the copy of e_8 on that side, and it depends only on the norm classes of the entries of v . Two properties follow at once from the definition. First, $M(v)$ is even, because $5|S| + x \equiv |S| + x \equiv 0 \pmod{2}$ for each word of e_8 and each w_i is even. Second, $M(v) \geq 2$ for $v \neq 0$: the term with $S = \emptyset$ is $\sum_i w_i \geq 2$, and every other term is at least $5|S| + x - 4|S| = |S| + x \geq 4$.

Lemma 2.2. *The code C has minimum weight at least 16 if and only if*

$$(1) \quad M(c_A) + M(c_B) \geq 16 \quad \text{for every nonzero } c = (c_A, c_B) \in C_1.$$

Proof. Each word of C is $\varphi_0(u, u') + \varphi_1(c)$ with $(u, u') \in e_8 \oplus e_8$ and $c \in C_1$. Its weight is the sum of its weights on the two sides, and for fixed c the minimum over (u, u') is $M(c_A) + M(c_B)$. The nonzero words with $c = 0$ are the words $\varphi_0(a, x)$ with $0 \neq (a, x) \in e_8 \oplus e_8$. Their weight $5|a| + |x|$ is at least 16, because a word of weight 4 of $e_8 \oplus e_8$ contains at most one fixed point. $\square$

Lemma 2.3. *No nonzero $v \in \mathbb{F}_{16}^7$ with $\langle v, v \rangle = 0$ satisfies $M(\lambda v) \geq 16$ for all $\lambda \in \mathbb{F}_{16}^\times$.*

Proof. Let $W = \sum_i w_i$ and $W_L = \sum_{i \in L} w_i$. The terms with $S = \emptyset$, $S = \{0, \dots, 6\}$, $S = L$ and $S = \bar{L}$ show that $M(v) \geq 16$ implies $16 \leq W \leq 20$ and $(W - 4)/2 \leq W_L \leq W/2$ for each line L . Let $h = |\text{supp } v|$, and let n_1, n_2, n_3 be the numbers of entries in the three norm classes. Multiplication by λ permutes the norm classes cyclically, and $W = 2h + 2n_r$ when class r is mapped to μ_5 . Hence $8 \leq h + n_r \leq 10$ for $r = 1, 2, 3$. Summing over r gives $24 \leq 4h \leq 30$, so $h \in \{6, 7\}$. We have $\langle v, v \rangle = n_1 + n_2N(1+t) + n_3N(1+t^2)$, and $1, N(1+t), N(1+t^2)$ are the three nonzero elements of $\mathbb{F}_4$. Their only linear relation over $\mathbb{F}_2$ is that their sum is 0, so isotropy gives $n_1 \equiv n_2 \equiv n_3 \pmod{2}$.

If $h = 6$, then $(n_1, n_2, n_3) = (2, 2, 2)$, so $W = 16$ and $6 \leq W_L \leq 8$ after each scaling. Take a line through the zero entry. One of its other two entries must lie in μ_5 after each of the three scalings, which is impossible because the three scalings map different classes to μ_5 . If $h = 7$, then

(n_1, n_2, n_3) is a permutation of $(1, 3, 3)$. After the scaling that maps a class with three entries to μ_5 we have $W = 20$, and $8 \leq W_L \leq 10$ means that each line contains one or two of these three entries. No set of three points of the Fano plane meets every line in one or two points: a line meets itself in three points, and a non-collinear triple misses exactly one line. $\square$

Suppose that C_1 contains a nonzero word $c = (c_A, 0)$. Then $\lambda c \in C_1$ for all $\lambda \neq 0$, and $M(0) = 0$, so (1) gives $M(\lambda c_A) \geq 16$. Moreover $\langle c_A, c_A \rangle = \langle c, c \rangle = 0$. This contradicts Lemma 2.3, and the same argument applies to words $(0, c_B)$. Hence the projection of C_1 onto the coordinates of A is injective, so it is bijective, and $C_1 = \{(a, aU) : a \in \mathbb{F}_{16}^7\}$ for an invertible 7×7 matrix U . Since $\langle (a, aU), (a', a'U) \rangle = a(I + UU^*)a'^*$ with $U^* = \bar{U}^\top$, the code C_1 is Hermitian self-dual if and only if $UU^* = I$. Together with Lemma 2.2 this reduces Theorem A to a finite statement.

Proposition 2.4. *There is no 7×7 matrix U over $\mathbb{F}_{16}$ with $UU^* = I$ such that $M(a) + M(aU) \geq 16$ for every nonzero $a \in \mathbb{F}_{16}^7$.*

2.4. Symmetries and normal form. The following maps preserve unitarity and the condition of Proposition 2.4. Each of them is induced by a permutation of the 72 coordinates that maps $\varphi_0(e_8 \oplus e_8)$ to itself and normalises $\langle g \rangle$.

- (a) $U \mapsto D_1^{-1}UD_2$ with D_1, D_2 diagonal with entries in μ_5 (cyclic shifts inside cycles).
- (b) $U \mapsto P_1^{-1}UP_2$ with P_1, P_2 the permutation matrices of collineations of the Fano plane (automorphisms of $e_8 \oplus e_8$ that fix both fixed points).
- (c) The Frobenius map $y \mapsto y^2$ applied to all entries (the permutation $k \mapsto 2k$ inside each cycle, which conjugates g to a power of g).

The *pattern* of $v \in \mathbb{F}_{16}^7$ is the vector of norm classes of its entries, with 0 for a zero entry, read as the base-4 integer $\sum_j c_j 4^j$. The Frobenius map fixes class 1 and interchanges classes 2 and 3. The *key* of a row is the smallest pattern among its images under the collineations and the Frobenius map. The rows of U are indexed by the coordinates of A , which we process in the order 0, 1, 3, 2, 4, 5, 6. The row of the d -th coordinate in this order is the row at depth d .

Lemma 2.5. *Every matrix U as in Proposition 2.4 is mapped by the symmetries (a)–(c) to one with the following properties.*

- (i) *The row at depth 0 has the smallest key among all rows.*
- (ii) *The pattern of the row at depth 0 equals its key.*
- (iii) *Scan the nonzero entries row by row in order of depth, and within a row in order of column. Each scanned entry is an edge of a bipartite graph on the rows and columns. Every entry that joins two different components of the graph built from the earlier entries is the representative of its norm class. The representatives are 1, $1 + t$ and $1 + t^2$ for the classes 1, 2 and 3.*

Proof. Property (i) is reached by (b) on A , since the collineation group is transitive on points. Then (b) on B and (c) give (ii). These maps change no key, so (i) is kept. For (iii) we process the joining entries in scanning order. When an entry joins two components, we apply (a) with $D_1 = D_2$ equal to some $\zeta \in \mu_5$ on the rows and columns of the component being attached and to 1 elsewhere. This multiplies the joining entry by ζ or ζ^{-1} , so a suitable ζ moves it to the representative of its class. An entry with both ends inside one component is multiplied by $\zeta^{-1}\zeta = 1$ or by 1, so it does not change. Each earlier scanned nonzero entry touching the attached component lies inside it, so no earlier normalisation is undone. Scalings by μ_5 change no pattern, so (i) and (ii) are kept. $\square$

In particular, the first nonzero entry of each row is the representative of its class, since its row vertex is still isolated when it is scanned. All nonzero entries of the row at depth 0 have this

property. By (ii) the row at depth 0 is therefore determined by its key, and seven keys occur (Table 1).

2.5. The search. Every row u of U satisfies $\langle u, u \rangle = 1$. For a unit vector e_i we have $M(\lambda e_i) = |\psi(\lambda)|$, since the term with $S = \emptyset$ is $|\psi(\lambda)| \leq 4$ and every other term is at least $|S| + x \geq 4$. So the word $(\lambda e_i, \lambda u)$ of C_1 , with u the row of e_i , gives $M(\lambda u) \geq 16 - |\psi(\lambda)|$ for all $\lambda \neq 0$. Let R be the set of such rows. Then $|R| = 42\,437\,500^\dagger$. The search builds U row by row in order of depth. A candidate $u \in R$ for the row at depth d must satisfy three tests.

- (1) It is orthogonal to the earlier rows, its key is at least the key of the row at depth 0, and the rows so far satisfy condition (iii) of Lemma 2.5.
- (2) Pair test: $M(\lambda e_k + \mu e_d) + M(\lambda u_k + \mu u) \geq 16$ for the row u_k at each depth $k < d$ and all $\lambda, \mu \neq 0$. Here e_k and e_d are the unit vectors of the coordinates at depths k and d .
- (3) Full test: $M(a) + M(aU) \geq 16$ for every a supported on the coordinates at depths $0, \dots, d$ with $a_d \neq 0$, where aU uses the rows chosen so far.

Each test is a necessary condition for a solution, by Lemma 2.5 and Proposition 2.4. Three reductions keep the full test exact. Multiplying a by an element of μ_5 changes no pattern, so the coefficient a_d runs over one element of each norm class. Words with at most one nonzero coefficient at depths below d are covered by the definition of R and the pair test. Words with $M(a) \geq 14$ pass, because the rows are orthonormal, hence $aU \neq 0$ and $M(aU) \geq 2$.

TABLE 1. The search of §2.5. For each key (the pattern $c_0 \dots c_6$ of the row at depth 0): the number of rows of R with this key, the number of rows of R that are orthogonal to the row at depth 0 and pass the pair test with it (no normal-form condition), and the number of partial matrices with k rows in normal form that pass all tests. No partial matrix has six or seven rows.

key	pattern	rows in R	depth-1 rows	$k = 2$	$k = 3$	$k = 4$	$k = 5$
0	3211110	2 625 000	1 479 340	59 212	107 673 776	3 110 422 096	32
1	3222110	2 625 000	1 502 120	56 244	96 310 444	2 578 475 424	24
2	2211111	3 281 250	1 280 920	215 560	274 462 160	5 635 916 128	0
3	2222111	4 375 000	1 303 950	204 630	250 782 852	4 940 763 168	96
4	3322111	13 125 000	1 299 570	176 930	187 177 548	3 190 216 136	40
5	3132211	3 281 250	1 293 840	100 736	62 330 048	639 280 128	0
6	3322221	13 125 000	1 331 590	83 400	43 176 320	366 603 888	0
all		42 437 500		896 712	1 021 913 148	20 461 676 968	192

Proof of Proposition 2.4. By Lemma 2.5 a solution can be assumed to be in normal form. Its first k rows then form a partial matrix that passes all tests, for each k . The search finds no such partial matrix with six rows[†] (Table 1). $\square$

Proof of Theorem A. By Lemmas 2.1–2.3, an extremal code with an automorphism of order 5 yields a matrix as in Proposition 2.4, and no such matrix exists. $\square$

3. KLEIN FOUR-GROUPS

In this section $V = \langle a, b \rangle \leq \text{Aut}(C)$ is a subgroup isomorphic to $C_2 \times C_2$. The reduction uses three results from the literature, and the proof of Theorem B uses no other external input.

- (L1) Every involution in $\text{Aut}(C)$ is fixed-point-free [9].

(L2) Let $a \in \text{Aut}(C)$ be a fixed-point-free involution. Then C is a free $\mathbb{F}_2\langle a \rangle$ -module, and the fixed code $C(a) = \{c \in C : ca = c\}$, contracted to one coordinate for each cycle of a , is a self-dual [36, 18, 8] code [33, Thm. 3.1].

(L3) Up to equivalence there are exactly 41 self-dual [36, 18, 8] codes [1, 24].

With $u = 1 + a$ the group algebra $\mathbb{F}_2\langle a \rangle$ is the ring $\mathbb{F}_2 + u\mathbb{F}_2$, so (L2) says that C is a free linear code of length 36 over this ring. This formulation of codes with a fixed-point-free involution goes back to Dougherty, Gaborit, Harada and Solé [17]. By (L1) the elements a , b and ab are fixed-point-free.

3.1. The model. We label the coordinates (i, e) with $1 \leq i \leq 36$ and $e \in \mathbb{F}_2$ so that $a(i, e) = (i, e + 1)$. A vector $c \in \mathbb{F}_2^{72}$ is written $c = (u \mid v)$ with $u_i = c_{(i,0)}$ and $v_i = c_{(i,1)}$. The sets $\{(i, 0), (i, 1)\}$ are the cycles of a , and we call them *pairs*. The contracted fixed code of a is $Y = \{u : (u \mid u) \in C\}$. Its all-one word is denoted $\mathbf{1}$. Since Y is self-dual, all its weights are even and $\mathbf{1} \in Y$.

Definition 3.1. Let $Y \leq \mathbb{F}_2^{36}$ be self-dual and let B be a bilinear form on Y . Put

$$C_B = \{(z \mid z + y) : y \in Y, z \in \mathbb{F}_2^{36}, \langle z, y' \rangle = B(y, y') \text{ for all } y' \in Y\}.$$

Since $Y = Y^\perp$, the map $z \mapsto \langle z, \cdot \rangle|_Y$ from $\mathbb{F}_2^{36}$ to the dual space of Y is onto with kernel Y . Hence, for each $y \in Y$, the admissible z form a coset $z_0(y) + Y$, and $z_0 : Y \rightarrow \mathbb{F}_2^{36}$ can be chosen linear. Thus C_B is a linear code of dimension 36, and its words with $y = 0$ are the words $(x \mid x)$ with $x \in Y$.

Lemma 3.2. Let $a \in \text{Aut}(C)$ be a fixed-point-free involution, with coordinates labelled as above, and let Y be its contracted fixed code. Then $C = C_B$ for a unique bilinear form B on Y .

Proof. By (L2), Y is self-dual and C is a free $\mathbb{F}_2\langle a \rangle$ -module. In a free module the kernel and the image of $1 + a$ coincide, so $\{c + ca : c \in C\} = C(a)$. Let $\sigma(u \mid v) = u + v$. For $c = (u \mid v)$ we have $c + ca = (u + v \mid u + v)$, so $\sigma(c)$ is the contraction of $c + ca$. Hence $\sigma(C) = Y$, and the kernel of σ on C is $C(a) = \{(x \mid x) : x \in Y\}$. For $y \in Y$ choose $(z_y \mid z_y + y) \in C$. Then z_y is determined modulo Y , the map $y \mapsto z_y$ can be chosen linear, and $B(y, y') = \langle z_y, y' \rangle$ is a well-defined bilinear form on Y . By construction $C \subseteq C_B$, and both codes have dimension 36. The code C_B determines $z_0(y)$ modulo Y , hence B . $\square$

Lemma 3.3. Let $Y \leq \mathbb{F}_2^{36}$ be self-dual and let B be a bilinear form on Y .

- (a) Let $y \in Y$ have support S , and let $z \in z_0(y) + Y$. Then $|(z \mid z + y)| = |y| + 2|z \setminus S|$, where $|z \setminus S|$ is the number of coordinates outside S at which z is 1.
 - (b) C_B is self-dual if and only if B is symmetric.
 - (c) If B is symmetric, then C_B is doubly-even if and only if
- $$(2) \quad B(y, y) \equiv |y|/2 + B(y, \mathbf{1}) \pmod{2}$$
- for all y in a basis of Y .
- (d) The involution a is an automorphism of C_B , with contracted fixed code Y .

Proof. (a) On a pair $i \in S$ exactly one of z_i and $z_i + y_i$ equals 1. On a pair $i \notin S$ both equal z_i .

(b) For $c = (z \mid z + y)$ and $c' = (z' \mid z' + y')$ in C_B ,

$$\langle c, c' \rangle = \langle z, z' \rangle + \langle z + y, z' + y' \rangle = \langle z, y' \rangle + \langle y, z' \rangle + \langle y, y' \rangle = B(y, y') + B(y', y),$$

since $\langle y, y' \rangle = 0$. So C_B is self-orthogonal if and only if B is symmetric, and it has dimension 36.

(c) Let y , S and z be as in (a). Since $\mathbf{1} \in Y$ and $y \in Y$, we have $|z \setminus S| = |z| - |z \cap S| \equiv \langle z, \mathbf{1} \rangle + \langle z, y \rangle = B(y, \mathbf{1}) + B(y, y) \pmod{2}$. By (a), all words $(z \mid z + y)$ with a given y have weight divisible by 4 if and only if $q(y) = B(y, y) + B(y, \mathbf{1}) + |y|/2$ is even. For symmetric B the map q is additive

on Y modulo 2: the cross terms of $B(y + y', y + y')$ cancel, and $|y + y'|/2 = |y|/2 + |y'|/2 - |y \cap y'|$ with $|y \cap y'|$ even. Hence $q \equiv 0$ on Y if and only if $q \equiv 0$ on a basis.

(d) We have $(z \mid z + y)a = (z + y \mid z)$ and $z + y \in z_0(y) + Y$. The words fixed by a are those with $y = 0$. $\square$

3.2. The second involution. For a permutation β of $\{1, \dots, 36\}$ and $y \in \mathbb{F}_2^{36}$ we write $y\beta$ for the permuted vector, $(y\beta)_{\beta(i)} = y_i$.

Lemma 3.4. *Let $C = C_B$ as in Lemma 3.2, and let $b \in \text{Aut}(C)$ be an involution that commutes with a such that b and ab are fixed-point-free.*

- (a) *There are a fixed-point-free involution $\beta \in \text{Aut}(Y)$ and $t \in \mathbb{F}_2^{36}$ with $b(i, e) = (\beta(i), e + t_i)$ and $t_i = t_{\beta(i)}$.*
- (b) *After relabelling the two coordinates of some pairs, $t = 0$. The relabelling commutes with a , and the contracted fixed code of a is still Y .*
- (c) *If $t = 0$, then $b \in \text{Aut}(C_B)$ if and only if $B(y\beta, y'\beta) = B(y, y')$ for all $y, y' \in Y$.*

Proof. (a) Since b commutes with a , it maps pairs to pairs, so $b(i, e) = (\beta(i), e + t_i)$ for a permutation β . From $b^2 = 1$ we get $\beta^2 = 1$ and $t_i = t_{\beta(i)}$. If $\beta(i) = i$, then b fixes both coordinates of pair i (if $t_i = 0$) or acts on it as a (if $t_i = 1$), and then b or ab has a fixed point. Hence β is fixed-point-free. The involution b maps $C(a)$ to itself, and $(x \mid x)b = (x\beta \mid x\beta)$, so $Y\beta = Y$.

(b) For each β -orbit $\{i, j\}$ with $t_i = t_j = 1$, interchange the labels $(j, 0)$ and $(j, 1)$. If s denotes this interchange, then sbs maps (i, e) to (j, e) and (j, e) to (i, e) . The interchange commutes with a and fixes each word $(x \mid x)$.

(c) If $t = 0$, then $(z \mid z + y)b = (z\beta \mid z\beta + y\beta)$. This word lies in C_B if and only if $\langle z\beta, y'\beta \rangle = B(y\beta, y'\beta)$ for all $y' \in Y$, using $Y\beta = Y$. The left side equals $\langle z, y' \rangle = B(y, y')$. $\square$

3.3. Normalisation. For $T \subseteq \{1, \dots, 36\}$ let s_T interchange $(i, 0)$ and $(i, 1)$ for each $i \in T$. It commutes with a . Define the symmetric form

$$D_T(y, y') = |y \cap y' \cap T| \bmod 2 \quad (y, y' \in Y).$$

Lemma 3.5. *Let Y be self-dual, B a bilinear form on Y , and $\beta \in \text{Aut}(Y)$ a fixed-point-free involution. Let $b(i, e) = (\beta(i), e)$.*

- (a) *$C_{B s_T} = C_{B + D_T}$. Moreover $D_T(y, y) = D_T(y, \mathbf{1})$, so B satisfies (2) if and only if $B + D_T$ does.*
- (b) *If T is a union of β -orbits, then $s_T b s_T = b$. If T contains exactly one element of each β -orbit, then $s_T b s_T = ab$. In both cases D_T is β -invariant.*
- (c) *Let G be the span of the forms D_T for the sets T in (b). For $D \in G$ there is a permutation s that commutes with a and normalises $V = \langle a, b \rangle$ such that $C_{B+D} = C_{Bs}$. In particular, C_B is a doubly-even self-dual [72, 36, 16] code with $V \leq \text{Aut}(C_B)$ if and only if C_{B+D} is.*

Proof. (a) On a pair $i \in T$, s_T replaces $(z_i, z_i + y_i)$ by $(z_i + y_i, z_i)$. Hence $(z \mid z + y)s_T = (z' \mid z' + y)$ with $z' = z + (y \cap T)$, and $\langle z', y' \rangle = B(y, y') + |y \cap T \cap y'|$. The second claim holds because $D_T(y, y) = |y \cap T| = D_T(y, \mathbf{1})$.

(b) We have $s_T b s_T(i, e) = (\beta(i), e + [i \in T] + [\beta(i) \in T])$. The sum $[i \in T] + [\beta(i) \in T]$ is 0 for all i in the first case and 1 for all i in the second. Moreover $D_T(y\beta, y'\beta) = |y \cap y' \cap \beta(T)|$. In the first case $\beta(T) = T$. In the second case $\beta(T)$ is the complement of T , and $|y \cap y' \cap \beta(T)| = |y \cap y'| - |y \cap y' \cap T|$ is congruent to $|y \cap y' \cap T|$ modulo 2 because $|y \cap y'|$ is even.

(c) Since $s_T s_{T'} = s_{T \Delta T'}$ and $D_{T \Delta T'} = D_T + D_{T'}$, each $D \in G$ is D_T for a product $s = s_T$ of the swaps in (b). By (b), s commutes with a and conjugates b to b or ab , so $s^{-1}Vs = V$. By (a), $C_{Bs} = C_{B+D}$. $\square$

The 18 forms D_R , for R a β -orbit, sum to $D_{\{1,\dots,36\}} = 0$, because $|y \cap y'|$ is even. For each instance of §3.5 they span a space of dimension 17, and the form D_T of a set T with one element in each β -orbit lies outside this space, so $\dim G = 18^\dagger$.

Let $\mathcal{A} = \mathcal{A}(Y, \beta)$ be the affine space of symmetric, β -invariant bilinear forms on Y that satisfy (2). By Lemma 3.5 it is a union of cosets of G . Fix a basis $w_0, \dots, w_{17}$ of Y , and identify B with its Gram entries $B(w_i, w_j)$, $0 \leq i \leq j \leq 17$, in row-major order. Choose a basis of G in reduced echelon form whose pivots are the earliest possible entries. The *slice* $\mathcal{S} \subseteq \mathcal{A}$ consists of the forms whose entries at these $\dim G$ pivot positions vanish. Each coset of G in $\mathcal{A}$ meets $\mathcal{S}$ in exactly one form, and

$$N = \dim \mathcal{S} = \dim \mathcal{A} - \dim G.$$

3.4. The distance condition. For $y \in Y$ let $Y_y = \{x \in Y : x \cap y = \emptyset\}$ and fix a basis $x_1, \dots, x_m$ of Y_y . The *syndrome* of B at y is

$$s_y(B) = (B(y, x_1), \dots, B(y, x_m)) \in \mathbb{F}_2^m.$$

Let $E_8 = \{0, 2\}$, $E_{10} = \{1\}$ and $E_{12} = \{0\}$, and for $|y| \in \{8, 10, 12\}$ let

$$\text{Bad}(y) = \{(\langle e, x_1 \rangle, \dots, \langle e, x_m \rangle) : e \subseteq \{1, \dots, 36\} \setminus \text{supp } y, |e| \in E_{|y|}\}.$$

Lemma 3.6. *Assume that Y has minimum weight 8, and let $B \in \mathcal{A}$. Then C_B has minimum weight at least 16 if and only if $s_y(B) \notin \text{Bad}(y)$ for every $y \in Y$ of weight 8, 10 or 12.*

Proof. Let $S = \text{supp } y$ and $z \in z_0(y) + Y$. By Lemma 3.3, $(z \mid z + y)$ has weight $|y| + 2|z \setminus S|$, divisible by 4, so $|z \setminus S| \equiv |y|/2 \pmod{2}$. Since Y has minimum weight 8, either $y = 0$ or $|y| \geq 8$. For $y = 0$ the nonzero words have weight $2|z| \geq 16$. For $|y| \geq 16$ the weight is at least 16, and for $|y| = 14$ it is at least 14 and divisible by 4. Let $|y| \in \{8, 10, 12\}$. The weight is less than 16 exactly when $|z \setminus S| < (16 - |y|)/2$, and with the parity above this means $|z \setminus S| \in E_{|y|}$. As z runs over $z_0(y) + Y$, its restriction to the complement S^c runs over a coset of the punctured code $Y|_{S^c}$. A vector $e \in \mathbb{F}_2^{S^c}$ is orthogonal to $Y|_{S^c}$ if and only if its extension by zeros lies in $Y^\perp = Y$, that is, in Y_y . Hence e lies in this coset if and only if $\langle e, x_j \rangle = \langle z_0(y), x_j \rangle = B(y, x_j)$ for $j = 1, \dots, m$. So some word $(z \mid z + y)$ has weight less than 16 if and only if $s_y(B) \in \text{Bad}(y)$. $\square$

For $B \in \mathcal{A}$ the condition at $y\beta$, computed with the basis $x_1\beta, \dots, x_m\beta$ of $Y_{y\beta}$, coincides with the condition at y , because $B(y\beta, x_j\beta) = B(y, x_j)$ and $e \mapsto e\beta$ maps the patterns of $\text{Bad}(y)$ to those of $\text{Bad}(y\beta)$. One word from each orbit $\{y, y\beta\}$ therefore suffices. We call these words the *constraint words*. On the slice, $B \mapsto s_y(B)$ is an affine map $\mathbb{F}_2^N \rightarrow \mathbb{F}_2^m$.

3.5. Instances. Let $Y_1, \dots, Y_{41}$ be representatives of the 41 codes of (L3). An *instance* is a pair (Y_k, β) with β a fixed-point-free involution in $\text{Aut}(Y_k)$, taken from a fixed set of representatives of the conjugacy classes of such involutions in $\text{Aut}(Y_k)$. There are 119 instances[†]. One of the 41 codes has no fixed-point-free involution. A solution of an instance is a form $B \in \mathcal{S}(Y_k, \beta)$ with $s_y(B) \notin \text{Bad}(y)$ for every constraint word y .

Proposition 3.7. *A doubly-even self-dual $[72, 36, 16]$ code with a subgroup $C_2 \times C_2$ of automorphisms exists if and only if some instance has a solution.*

Proof. Let $V = \langle a, b \rangle \leq \text{Aut}(C)$. Label the coordinates as in §3.1. By Lemma 3.2, $C = C_B$, where Y is the contracted fixed code of a . A permutation π of the pairs with $Y\pi = Y_k$ lifts to $(i, e) \mapsto (\pi(i), e)$. The lift commutes with a and maps C to a code $C_{B'}$ over Y_k . By Lemma 3.4 we may assume $b(i, e) = (\beta(i), e)$. For $g \in \text{Aut}(Y_k)$, the lift of g commutes with a , fixes Y_k , and replaces β by $g^{-1}\beta g$. So β may be taken from the fixed set of representatives. Now B lies in $\mathcal{A}$ by Lemmas 3.3 and 3.4, and by Lemma 3.5 we may replace B by the form of $\mathcal{S}$ in $B + G$. By Lemma 3.6 this form is a solution.

Conversely, for a solution B the code C_B is doubly-even and self-dual (Lemma 3.3), has minimum weight 16 (Lemma 3.6 with the reduction to one word per orbit $\{y, y\beta\}$ that follows it), and has the automorphisms a and b (Lemmas 3.3 and 3.4). They generate a group $C_2 \times C_2$, since b moves the pairs. $\square$

For each instance we compute[†] $\dim \mathcal{A} \in \{81, 82, 83\}$ and $N \in \{63, 64, 65\}$. The value $N = 63$ occurs for 106 instances, $N = 64$ for 9 and $N = 65$ for 4. The involution β makes Y a module over $\mathbb{F}_2(\beta)$, and $r = \dim Y(1 + \beta)$ is 9 for 84 instances (then Y is free and $N = 63$), 8 for 31 instances ($N = 63$ or 64) and 7 for 4 instances ($N = 65$). Each instance has between 5 932 and 6 328 constraint words[†].

3.6. The searches. We decide each instance by an exhaustive search over $\mathcal{S} \cong \mathbb{F}_2^N$. The main algorithm enumerates the Gram matrix of B row by row. It has two implementations, I and II. Implementation II is independent of the other programs (Section 5).

Variables and levels. The conditions that define $\mathcal{S}$ are affine equations in the 171 Gram entries $B(w_i, w_j)$, $i \leq j$: β -invariance, (2) and the vanishing of the entries at the pivot positions of G . We bring them into reduced echelon form with pivots at the latest possible entries in row-major order. The N non-pivot entries are the variables. Each pivot entry is an affine function of earlier variables, so the entries in row t of the Gram matrix depend only on the variables in rows $0, \dots, t$. A variable in row t has *level* t , and k_t denotes the number of variables of level t . The syndrome s_y of a constraint word y is an affine function of the variables. Its level is the largest level of a variable that occurs in it (Implementation I) or the largest index i with w_i in the expansion of y (Implementation II, an upper bound for the former).

Nodes and removal of children. A node at level t is an assignment of all variables of level less than t . Its children are the 2^{k_t} assignments v of the variables of level t . For a constraint word y of level t we have $s_y = s_0 + L_y v$, where s_0 depends on the node and L_y is a fixed $m \times k_t$ matrix. For each $\mathbf{b} \in \text{Bad}(y)$, the children with $s_0 + L_y v = \mathbf{b}$ form either the empty set or a coset $v_0 + \ker L_y$. These children are removed from a bit vector of length 2^{k_t} . Implementation I instead runs through all children in Gray-code order when 2^{k_t} is at most $|\text{Bad}(y)| (2^{\dim \ker L_y} + 4)$. The surviving children are nodes at level $t + 1$. A node at level 18 satisfies every constraint and is a solution, and the programs report it.

Constraint sets and basis order. Implementation II uses the constraint words and the sets $E_{|y|}$ of Lemma 3.6. Implementation I uses one word from each orbit $\{y, y\beta\}$ of words of weight 8 to 14, with the larger sets $\{0, 1, \dots, (16 - |y|)/2 - 1\}$ in place of $E_{|y|}$. This gives the same solutions: by Lemma 3.3(c) the coset in the proof of Lemma 3.6 contains only vectors e with $|e| \equiv |y|/2 \pmod{2}$, so the additional patterns never match the syndrome of a form in $\mathcal{S}$. In particular, the words of weight 14 never remove a child. The order of the basis $w_0, \dots, w_{17}$ affects only the running time. Implementation I starts with a basis of the fixed space Y^β and then completes it. Each new basis vector maximises the number of words of weight at most 14 in the span, and is itself of weight at most 14 when possible. Implementation II chooses the first rows inside Y^β or inside $Y(1 + \beta)$ by a greedy rule and keeps the schedule with the smallest estimated work. It repeats every instance with a second basis order.

Splitting. For parallel runs, the nodes at a fixed level are numbered in depth-first order, and job j of P jobs expands the nodes whose number is congruent to j modulo P . Every job recomputes the levels above the split level, so each node at or below the split level is expanded by exactly one job.

A third solver. A guess-and-determine program provides a check by a different method. It uses only the 17-dimensional span of the forms D_R , so its search space has dimension $N + 1$ and contains two forms from each coset of G . Its variables are the coordinates of this space. For each constraint

word of weight at most 14 it keeps the m affine forms of s_y , reduced modulo the linear equations fixed so far, and the set of syndromes outside the bad set (with the larger sets of Implementation I) that are consistent with the linear relations among the reduced forms. It branches on the word with the smallest value of $\log_2(\text{number of consistent syndromes})/(\text{rank of the reduced forms})$, adds the equations of each consistent syndrome in turn, and propagates words with a single consistent syndrome. A branch ends when some word has no consistent syndrome. At a leaf the program solves all equations and checks every constraint word against the original forms.

Tests on known codes. The extended quadratic residue codes of lengths 48, 72 and 80 are doubly-even self-dual with minimum weights 12, 12 and $16^\dagger$ [37, Sect. 12.1]. Their automorphism groups contain $\text{PSL}(2, q)$ for $q = 47, 71, 79$. Since $q \equiv 3 \pmod{4}$, the involutions of $\text{PSL}(2, q)$ have no fixed points on the projective line, so a Klein four-subgroup acts freely on the coordinates. For such a subgroup we form Y and β as above and run the same programs with 16 replaced by the minimum weight of the code. If the reduction and the programs are correct, the form of the known code is among the solutions. At length 48 the searches are complete. At lengths 72 and 80 some variables are fixed to the values of the known code and the rest are searched.

Proof of Theorem B. By Proposition 3.7 it suffices that no instance has a solution. Both implementations of the level-wise search find no solution in any of the 119 instances[†], and the guess-and-determine program finds none in 113 of them[†] (Table 4). $\square$

4. AUTOMORPHISMS OF ORDER 3

In this section $\sigma \in \text{Aut}(C)$ has order 3. By Conway and Pless [15] and Bouyuklieva [10] (see also [19, Sect. III] and [7, Prop. 6.1]), σ has 24 cycles of length 3 and no fixed points. For extremal binary self-dual codes of length at least 72, Bouyuklieva, Russeva and Karataş [12] show that an automorphism of order 3 with c cycles of length 3 and f fixed points satisfies $c \geq f$. Bonnecaze, Bracco, Dougherty, Nochefranca and Solé [4] derive necessary conditions for the existence of a cubic [72, 36, 16] Type II code. Yorgov [41] announced in a talk abstract that the Hermitian code E of §4.1 has no generator matrix with entries in $\{0, 1\}$, a partial result that Theorem C supersedes.

4.1. Decomposition. We label the coordinates (i, j) with $1 \leq i \leq 24$ and $j \in \mathbb{Z}/3$ so that $\sigma(i, j) = (i, j+1)$. We identify $\mathbb{F}_2^3$ with $\mathbb{F}_2[x]/(x^3-1)$, so that σ acts on each cycle as multiplication by x . The words of even weight form the ideal generated by $1+x$. With identity element $x+x^2$ this ideal is a field with four elements, and multiplication by x acts on it as multiplication by its element x^2+1 , a root of y^2+y+1 . We write $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$ with $\bar{\omega} = \omega^2 = \omega+1$ and identify $\mathbb{F}_4$ with the even-weight words of length 3 by

$$\psi(1) = (0, 1, 1), \quad \psi(\omega) = (1, 0, 1), \quad \psi(\bar{\omega}) = (1, 1, 0).$$

Then multiplication by ω is the action of σ , and $|\psi(y)| = 2$ for $y \neq 0$. For $u, v \in \mathbb{F}_4$ we have $\langle \psi(u), \psi(v) \rangle = \text{Tr}(u\bar{v})$, where $\text{Tr}(y) = y+y^2$ and $\bar{v} = v^2$: both sides equal 1 exactly when u and v are nonzero and distinct.

Let $F = \{c \in C : c\sigma = c\}$ and let $E(\sigma)$ be the set of words of C with even weight on each cycle. Then $C = F \oplus E(\sigma)$ [25, 43] (see also [8, Sect. 2]). The words of F are constant on cycles. We write $F = \{g^{(3)} : g \in G\}$, where $g^{(3)}$ repeats g_i on the i -th cycle. By [19, Lemma 3.1], $G \leq \mathbb{F}_2^{24}$ is equivalent to the extended Golay code. We call the words of weight 8 and 12 of G octads and dodecads. Moreover $E(\sigma) = \varphi(E)$, where φ applies ψ on each cycle and $E \leq \mathbb{F}_4^{24}$ is $\mathbb{F}_4$ -linear. Since $\langle \varphi(x), \varphi(y) \rangle = \text{Tr}(\sum_i x_i \bar{y}_i)$ and $E(\sigma)$ has dimension 24 over $\mathbb{F}_2$, the code E is a Hermitian self-dual [24, 12] code [25]. Its weights are even, because $\sum_i x_i \bar{x}_i \equiv \text{wt}(x) \pmod{2}$. Since $|\varphi(e)| = 2 \text{wt}(e)$, the minimum distance of E is at least 8. A Hermitian self-dual code

of length 24 has minimum distance at most $2\lfloor 24/6 \rfloor + 2 = 10$ [29], and a Hermitian self-dual $[24, 12, 10]$ code does not exist [28]. So E has minimum distance 8.

4.2. The distance condition.

Lemma 4.1. *For $g \in G$ and $e \in E$ with support S ,*

$$|g^{(3)} + \varphi(e)| = 3|g| + 2|S| - 4|g \cap S|.$$

Proof. On the i -th cycle the word $g^{(3)} + \varphi(e)$ has weight 0, 2, 3 or 1 according as (g_i, e_i) is $(0, 0)$, $(0, \neq 0)$, $(1, 0)$ or $(1, \neq 0)$. The sum over the cycles is $3|g \setminus S| + 2|S \setminus g| + |g \cap S|$. $\square$

Lemma 4.2. *Let $G \leq \mathbb{F}_2^{24}$ be equivalent to the extended Golay code, let $E \leq \mathbb{F}_4^{24}$ be a Hermitian self-dual code of minimum distance 8, and let $C = \{g^{(3)} : g \in G\} \oplus \varphi(E)$. Then C has minimum weight at least 16 if and only if the following hold.*

- (W8) *Every support of a word of weight 8 of E meets every octad in at most 6 points.*
- (W10) *No support of a word of weight 10 of E contains an octad.*
- (W12) *No support of a word of weight 12 of E is a dodecad.*

Proof. Let $g \in G$ and $e \in E$, not both zero, and put $w = \text{wt}(e)$ and $t = |g \cap \text{supp } e|$. If $e = 0$, the weight is $3|g| \geq 24$. If $g = 0$, it is $2w \geq 16$. Otherwise $|g| \in \{8, 12, 16, 24\}$, w is even with $8 \leq w \leq 24$, and by Lemma 4.1 the weight is at least 16 if and only if $4t \leq 3|g| + 2w - 16$. For $|g| = 8$ this reads $t \leq 2 + w/2$. It fails only for $w = 8, t \geq 7$ and for $w = 10, t = 8$, which are the cases excluded by (W8) and (W10). For $|g| = 12$ it reads $t \leq 5 + w/2$, and since $t \leq \min(12, w)$ it fails only for $w = 12, t = 12$, which (W12) excludes. For $|g| = 16$ it reads $t \leq 8 + w/2$, which holds because $t \leq \min(16, w)$. For $|g| = 24$ the weight is $72 - 2w \geq 24$. $\square$

For a Hermitian self-dual $[24, 12, 8]$ code E on a coordinate set X , an 8-subset of X is *forbidden* if it meets the support of a word of weight 8 in at least 7 points or lies in the support of a word of weight 10. A 12-subset is forbidden if it is the support of a word of weight 12. A *Golay code on X* is the image of the extended Golay code under a bijection from its 24 points onto X . It is *valid for E* if none of its octads and none of its dodecads is forbidden. Two codes over $\mathbb{F}_4$ are *monomially equivalent* if one is mapped onto the other by a permutation of the coordinates followed by multiplication of the coordinates by nonzero scalars. *Conjugation* applies $y \mapsto \bar{y}$ to every entry.

Proposition 4.3. *A doubly-even self-dual $[72, 36, 16]$ code with an automorphism of order 3 exists if and only if some Hermitian self-dual $[24, 12, 8]$ code over $\mathbb{F}_4$ has a valid Golay code on its coordinates. Whether such a Golay code exists depends only on the class of the code under monomial equivalence and conjugation.*

Proof. If $\sigma \in \text{Aut}(C)$ has order 3, then E is a Hermitian self-dual $[24, 12, 8]$ code and the labelled code G is valid for E by Lemma 4.2. Conversely, let E and a valid Golay code G on its coordinates be given, and put $C = \{g^{(3)} : g \in G\} \oplus \varphi(E)$. Then C has dimension $12 + 24 = 36$. Two tripled words are orthogonal because $3|g \cap g'|$ is even. A tripled word is orthogonal to $\varphi(E)$ because $\psi(y)$ has even weight. The code $\varphi(E)$ is self-orthogonal by the trace identity. So C is self-dual. Its generators $g^{(3)}$ and $\varphi(e)$ have weights $3|g|$ and $2\text{wt}(e)$, both divisible by 4, so C is doubly-even. It is invariant under σ , and it has minimum weight 16 by Lemma 4.2. A monomial map moves supports by its permutation and conjugation fixes them, so the forbidden sets of an equivalent code are the images of those of E . $\square$

4.3. Classification of the Hermitian self-dual [24,12,8] codes. Hermitian self-dual codes over $\mathbb{F}_4$ are classified up to length 20 [16, 21, 23, 29], and the extremal ones of length 22 are known [23] (see [20]). Theorem D classifies the codes of length 24 with minimum distance 8, the largest possible [28, 29]. We describe the method, which builds each code from one of its words of weight 8.

Let E be a Hermitian self-dual [24, 12, 8] code and $e_1 \in E$ a word of weight 8 with support S_1 . After scaling coordinates, e_1 is the all-one word $\mathbf{1}$ on S_1 . Let B be the complement of S_1 . The shortened code $E_B = \{e|_B : e \in E, e|_{S_1} = 0\}$ is a Hermitian self-orthogonal [16, 5, ≥ 8] code. The restriction of E to S_1 is $\mathbf{1}^\perp$, and the restriction to B is $E_B^\perp$. The map $e \mapsto (e|_{S_1} + \langle \mathbf{1} \rangle, e|_B + E_B)$ sends E onto the graph of a linear isometry θ between the six-dimensional spaces $\mathbf{1}^\perp / \langle \mathbf{1} \rangle$ and $E_B^\perp / E_B$, with their induced Hermitian forms, and E is the full preimage of this graph. Conversely, each such isometry θ defines a Hermitian self-dual code. It has minimum distance at least 8 if and only if, for every nonzero class $\bar{u}$ of $\mathbf{1}^\perp / \langle \mathbf{1} \rangle$, the minimum weights of the coset $\bar{u}$ in $\mathbb{F}_4^8$ and of the coset $\theta(\bar{u})$ in $\mathbb{F}_4^{16}$ add up to at least 8.

Both classification programs proceed in two stages.

- (i) The classes of Hermitian self-orthogonal [16, $k + 1, \geq 8$] codes are obtained from those of dimension k by adding one vector, one from each orbit of the automorphism group on the possible extensions. Up to monomial equivalence and conjugation there are 30, 393, 9 519 and 45 775 classes of dimension 2, 3, 4 and $5^\dagger$.
- (ii) For each code E_B of dimension 5, the isometries θ are enumerated up to the group $S_8 \times \mathbb{F}_4^\times$ acting on S_1 , subject to the Gram conditions and the minimum-weight condition above. The two programs use different enumerations. The second chooses the images of a basis one at a time, each minimal in its orbit under the stabiliser of the earlier ones. The first lists the images of the classes of the vectors $e_i + e_8$ ($i = 1, \dots, 7$) in increasing order and tests canonicity at the leaves. A code E obtained in this way is kept only if e_1 is a canonical word of weight 8 of E . The rule depends only on the multiset of intersection sizes of $\text{supp } e_1$ with the other supports of weight 8, so it is invariant under monomial maps and conjugation. Duplicates are removed with a canonical form under monomial equivalence. It is computed from a graph with three vertices per coordinate, for the scalings, and one vertex per word of a spanning set of codewords that is invariant under monomial maps. The class key of E is the smaller of the canonical forms of E and of its conjugate.

The rules for e_1 differ. The first program keeps a word for which a fixed hash of this multiset is largest and breaks ties by a canonical labelling, chosen so that the rule is invariant under conjugation. The second keeps the lexicographically smallest multiset without a tie-break and removes all duplicates by class keys. The two canonical forms are independent implementations of the same graph construction, both computed with nauty [32], and stage (i) uses the same method in both programs. The second program uses the canonical form of the first only to compare the final lists.

Proof of Theorem D. Both programs produce[†] 13 485 816 classes up to monomial equivalence and conjugation, with identical multisets of (class key, order of the monomial automorphism group, A_8 , self-conjugacy)[†]. Of these classes, 46 701 are self-conjugate, and each of the other 13 439 115 splits into two classes up to monomial equivalence. So the list gives $46\,701 + 2 \cdot 13\,439\,115 = 26\,924\,931$ classes up to monomial equivalence. It remains to show that the list has no repetitions and contains every class. We use five facts.

- (1) Every listed code is a Hermitian self-dual [24, 12, 8] code, with A_8 as listed[†].
- (2) An invariant of the supports of the words of weight 8, obtained by two rounds of colour refinement and invariant under monomial maps and conjugation, takes 13 485 816 distinct values on the list[†]. So no two listed codes are equivalent.

- (3) The listed orders of the monomial automorphism groups and the self-conjugacy flags are correct[†]. For 13 372 811 codes a discrete colouring of the coordinates and a connected hypergraph of supports force every monomial automorphism to be a scalar. The other 113 005 orders are computed with nauty.
- (4) Stage (i) is complete. Counting pairs of a code of dimension $k + 1$ and one of its subcodes of dimension k gives

$$\sum_{D'} \frac{(4^{k+1} - 1)/3}{|\text{Aut}_{\text{Mon}}(D')|} = \sum_D \frac{\text{ext}(D)}{|\text{Aut}_{\text{Mon}}(D)|},$$

where D' and D run over the classes up to monomial equivalence of dimension $k + 1$ and k , and $\text{ext}(D)$ is the number of codes of dimension $k + 1$ that contain D , counted directly from the cosets of D in $D^\perp$. The identity holds exactly for $k = 0, \dots, 4^\dagger$. Both sides are sums of positive terms, so by induction on k no class is missing at any dimension.

- (5) Counting pairs consisting of a code and one of its words of weight 8 up to scalars, once from the codes and once from the isometries, gives

$$\sum_E \frac{A_8(E)/3}{|\text{Aut}_{\text{Mon}}(E)|} = \sum_{E_B} \frac{N(E_B)}{|S_8 \times \mathbb{F}_4^\times| |\text{Aut}_{\text{Mon}}(E_B)|},$$

where the sums run over all classes up to monomial equivalence and $N(E_B)$ is the number of isometries θ over E_B that give minimum distance 8. The second program accumulates $N(E_B)$ before the acceptance test, and for every E_B its count agrees with that of the first program, whose enumeration is different[†]. The right side, computed from these counts, equals 526 493 209 678 523/322 560[†].

By (1)–(3), the left side of (5), evaluated over the list, is a sum of distinct terms of the full sum, and it also equals 526 493 209 678 523/322 560[†]. By (4) and (5) the right side is the full sum. All terms are positive, so the list contains every class. $\square$

Write $A_8 = 9\beta$ [3, Fact 5.1]. Table 2 gives the number of classes for each value of β and for each order of the monomial automorphism group[†]. These orders include the three scalar multiples of the identity. The largest group belongs to $G_{24} \otimes \mathbb{F}_4$, the code spanned over $\mathbb{F}_4$ by the extended Golay code, with $\beta = 253$ and $|\text{Aut}_{\text{Mon}}| = 3|M_{24}|$.

4.4. The labelling tests. By Proposition 4.3 and Theorem D, Theorem C amounts to a finite statement: none of the 13 485 816 classes has a valid Golay code. Each code E is tested by two exact programs. Both use only the forbidden sets of E . They rely on standard properties of the extended Golay code G_{24} and its automorphism group M_{24} . The nonzero weights of G_{24} are 8, 12, 16 and 24, and every 5-set of points lies in exactly one octad [14, Thm. 11 and Tables 10.1–10.2]. Since $|x + y| = |x| + |y| - 2|x \cap y|$ is again a weight, two distinct octads meet in 0, 2 or 4 points, and an octad and a dodecad meet in 2, 4 or 6 points. Every 4-set lies in exactly one sextet, a partition of the points into six 4-sets any two of which form an octad [13, Sect. 9]. The group M_{24} is 5-transitive of order $244\,823\,040 = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$ [14, Thms. 5 and 10]. The stabiliser of an octad O induces the alternating group on O , and the pointwise stabiliser of O is elementary abelian of order 16 and acts regularly on the complement of O [14, Thm. 10], [13, Sect. 10]. On the reference code used by the programs, the order of M_{24} , the order 48 of the pointwise stabiliser of five points of an octad, its action on the other three points, and the regularity of the pointwise stabiliser of the octad were also confirmed by computer[†]. A Golay code on X is $\pi(G_{24})$ for a bijection π from the points of G_{24} to X , and π and π' give the same code if and only if $\pi' = \pi m$ with $m \in M_{24}$.

We also use the octads disjoint from a given octad R . The only words of G_{24} supported in R are 0 and R , so the restriction of G_{24} to R has dimension 7, and the words of G_{24} that vanish on R

TABLE 2. Classes of Hermitian self-dual $[24, 12, 8]$ codes over $\mathbb{F}_4$ up to monomial equivalence and conjugation, by $\beta = A_8/9$ (left) and by the order of the monomial automorphism group (right). Both columns sum to 13 485 816.

β	classes	β	classes	Aut	classes	Aut	classes	Aut	classes
57	951 871	85	3 002	3	13 416 367	63	1	576	5
58	4 446 371	88	2 068	6	65 586	66	1	648	2
60	2 683 915	93	442	9	423	72	18	720	1
61	2 096 124	94	55	12	2 663	96	26	864	1
64	1 901 498	96	69	18	198	108	5	1 008	1
66	579 753	100	61	24	303	120	1	1 152	1
69	237 562	106	26	27	1	144	14	1 512	1
70	382 142	109	3	30	3	180	1	1 728	1
73	91 586	114	2	36	65	192	10	3 456	1
76	59 338	121	5	42	1	216	1	4 320	1
78	40 308	133	1	48	84	288	8	8 640	1
82	7 955	138	1	54	2	324	1	9 216	1
84	1 656	157	1	60	2	384	9	11 520	1
		253	1			432	1	27 648	1
								362 880	1
								734 469 120	1

form a 5-dimensional code D supported on the complement of R . Its weights are 0, 8 and 16, and it contains the word j whose support is the complement of R . In a generator matrix of D with first row j , the columns of the other four rows are 16 vectors of $\mathbb{F}_2^4$. Every nonzero linear form takes the value 1 on exactly 8 of them, since the corresponding word of D is neither 0 nor j . So the multiplicities of the columns have vanishing Fourier coefficients away from 0, and the columns are the 16 vectors of $\mathbb{F}_2^4$, each once. The 30 words of weight 8 of D , which are the octads disjoint from R , are then the affine hyperplanes of the affine space $\text{AG}(4, 2)$ on the complement of R (compare [13, Sect. 10] and [30, Sect. 5]).

Point placement. Fix an octad O_0 of G_{24} with points $p_1 < \dots < p_8$, a point $q_1 \notin O_0$, and five coordinates $c_1 < \dots < c_5$ of E .

Lemma 4.4. *Every Golay code on the coordinates of E is $\pi(G_{24})$ for exactly one bijection π with*

- (N1) $\pi(p_i) = c_i$ for $i = 1, \dots, 5$,
- (N2) $\pi(p_6) < \pi(p_7)$ and $\pi(p_6) < \pi(p_8)$,
- (N3) $\pi(q_1)$ is the smallest coordinate outside $\pi(O_0)$.

Proof. Let H be the pointwise stabiliser of $p_1, \dots, p_5$ in M_{24} . It has order 48 and fixes O_0 , the unique octad through these points. The alternating group on O_0 contains exactly three permutations that fix $p_1, \dots, p_5$, the rotations of p_6, p_7, p_8 , so H acts on these three points by rotations. The kernel K of this action is the pointwise stabiliser of O_0 , of order 16, so H induces all three rotations. Given π , choose $m_1 \in M_{24}$ with $\pi m_1(p_i) = c_i$ for $i \leq 5$, by 5-transitivity. The elements of $\pi m_1 H$ satisfy (N1), and they permute the three values at p_6, p_7, p_8 cyclically. So exactly one coset $\pi m_1 h_0 K$ satisfies (N2). On this coset the value at q_1 runs once through the coordinates outside $\pi(O_0)$, because K is regular on the complement of O_0 . So exactly one element also satisfies (N3). If π and πm both satisfy (N1)–(N3), then $m \in H$ by (N1), $m \in K$ by (N2), and $m = 1$ by (N3). $\square$

The first program places the points of G_{24} in a fixed order: $p_1, \dots, p_8$ as in (N1) and (N2), then the eight points of an octad Q disjoint from O_0 , starting with q_1 as in (N3), and then the eight points of the complement O^* of $O_0 \cup Q$, which is an octad because the sum of the all-one

word, O_0 and Q has weight 8. After each step, a coordinate is removed from the candidates of an unplaced point when some octad or dodecad, with all its other points placed, would receive a forbidden image. Forward checking of this kind removes no valid labelling. The octads inside $O_0 \cup Q$ are the 30 octads disjoint from O^* , namely O_0 , Q and 28 octads that meet each of them in four points. By the intersection numbers above, no dodecad lies inside $O_0 \cup Q$, and no octad or dodecad has exactly one point in O^* . So the placement of Q tests exactly these 30 octads, and the points of O^* start with all free coordinates as candidates. A complete bijection that passes all tests is a valid Golay code, and by Lemma 4.4 each valid Golay code is found exactly once.

Octad growth. The second program builds the Golay code on X as a code spanned by octads. Each step adds the unique octad through a chosen 5-set, the unique tetrad of a sextet that contains a chosen point, or the unique set of octads disjoint from an octad R . A candidate must keep the code doubly even with minimum weight at least 8, and each new word must be legal: a new octad must not be forbidden, and a new dodecad must not be the support of a word of weight 12. The first octad O_1 passes through a 5-set F_0 chosen from the supports of E . The second octad O_2 passes through $T \cup \{x\}$, with T a 4-subset of O_1 and $x \notin O_1$, and meets O_1 exactly in T . Then $A = O_1 \setminus T$ and $B = O_2 \setminus T$ are tetrads of the sextet of T . The program branches over the candidates for the tetrad C of this sextet that contains a chosen one of the remaining 12 points. These are the 4-sets C of remaining points that contain the chosen point and make $T \cup C$, $A \cup C$, $B \cup C$ and the complement R of $T \cup A \cup B \cup C$ octads that are not forbidden. In a Golay code, R is the union of the other two tetrads. The 30 octads disjoint from R are the hyperplanes of the affine space $\text{AG}(4, 2)$ on the complement of R . They span the 5-dimensional code D supported on the complement of R , and together with the all-one word of length 24 they span a code of dimension 6. They are the six unions of two of T, A, B, C and 24 octads that meet each of T, A, B, C in two points. The program enumerates every such structure whose octads are not forbidden, using tables of forbidden pairs computed from the supports of E . It also requires a split of R into two 4-sets each of which, in place of C , satisfies the same octad conditions and admits such a structure. In a Golay code the other two tetrads of the sextet form such a split. For each structure, the code of dimension 6 that it spans with the all-one word is extended one generator at a time. Each step adds the octad through the 5-set with the fewest candidates among up to 24 uncovered 5-sets $T' \cup \{x\}$, where T' is a 4-subset of the last octad added (of O_1 at the first extension step) and x lies outside that octad. If all of these 5-sets are covered, the first uncovered 5-set in a fixed order is used. Each new word of the code is checked when its generator is added. A word of weight 8 or 16 is accepted only if the octad, or the complementary octad, is not forbidden. A word of weight 12 is accepted only if neither it nor its complement is the support of a word of weight 12. Words of other weights are rejected. So at dimension 12 all 759 octads and 2576 dodecads of the code have been checked. Every step is complete: a Golay code that contains the partial structure has exactly one octad through the chosen 5-set, exactly one tetrad of the sextet of T through the chosen point and exactly one set of 30 octads disjoint from R , and these are among the candidates.

For codes with $|\text{Aut}_{\text{Mon}}(E)| > 3$, the first level runs only over representatives of the orbits of a group Γ of coordinate permutations on the octads through F_0 . The group Γ is induced on the coordinates by the automorphism group, computed with nauty [32], of a graph with three vertices per coordinate, for the scalings, and one vertex for each word of weight 8 of E . The vertices of the coordinates of F_0 form a separate cell, so that Γ fixes F_0 as a set. When the words of weight 8 span E , Γ is the setwise stabiliser of F_0 in $\text{Aut}_{\text{Mon}}(E)$, acting by its coordinate permutations, and the reduction is sound because automorphisms of E preserve the forbidden sets. Among the 69 449 classes with $|\text{Aut}_{\text{Mon}}(E)| > 3$, exactly two have words of weight 8 that span only a subcode of dimension 11 ($|\text{Aut}_{\text{Mon}}(E)| = 288$, $\beta = 57$ and $|\text{Aut}_{\text{Mon}}(E)| = 9216$, $\beta = 93$)[†]. For these two classes the reduction is still valid, because the group used preserves all supports of weight 8, 10

and 12 of both codes[†]. The octad-growth computation of §4.5, which the proof uses, also applies the reduction to these two classes. Re-tests without it find no solution[†]. The point-placement program uses no reduction by automorphisms of E .

4.5. Results. The point-placement program decided each of the 13 485 816 classes exactly once[†] and found no valid Golay code for any of them. The octad-growth run was split into parts. Every class was decided exactly once in the part to which it was assigned[†], and no solution was found. Table 5 lists the coverage checks. The point-placement program visited 4.37×10^{14} nodes in total.

Proof of Theorem C. By Proposition 4.3 and Theorem D it suffices that none of the 13 485 816 classes has a valid Golay code. Each of the two labelling programs decided every class and found no valid Golay code[†]. $\square$

Remark 4.5. The proofs of Theorems C and D use four published results that are neither re-proved nor checked by computer here: the absence of fixed points [10], the bound $d \leq 2\lfloor n/6 \rfloor + 2$ for Hermitian self-dual codes of length n [29], the non-existence of a Hermitian self-dual [24, 12, 10] code [28], and the uniqueness of the extended Golay code, which enters through [19, Lemma 3.1]. The computational inputs to the double count are described in facts (3) and (5) of the proof of Theorem D. A class could escape the labelling tests only if both programs failed on it.

5. VERIFICATION

The computations marked [†] in Sections 2–4 were re-checked. The re-checks test the reductions of Sections 2–4 on explicit codes, repeat each search with a second program, and check the coverage of the runs that were split into parts. Each table lists re-checks of the main runs, that is, the runs whose output the proof uses. Tests of individual components are listed in the README of the archive. Table 3 lists the checks for Theorem A, Table 4 those for Theorem B, and Table 5 those for Theorems C and D. We call an implementation independent if it shares no code with the program it checks, and a cross-check a re-examination of a reduction or a program in which the quantities reproduced are recomputed, with independently written code unless stated otherwise. Implementation II (§3.6) was written from a statement of the problem, and the independent implementation of Table 3 from the statement of Proposition 2.4. Planted solutions are known solutions inserted into an instance, and a removal certificate certifies that a child of a search node is removed. Node counts of searches split into parts count each node once, including the first levels that every part recomputes.

Table 3: Verification of Theorem A. Items marked [†] belong to the order-5 cross-check, described in the first row.

Check	Outcome
Independently written field arithmetic, e_8 , M , $\text{GL}(3, 2)$, normal form and enumeration of orthogonal complements [†] were used to recompute all depth-1 counts, to re-run parts of the search, one of them node by node (13 254 989 nodes), and to re-check 50 of the 192 five-row nodes, also without symmetry rules. In addition, a sample of 7 849 nodes with 2 to 5 rows was checked.	The counts agree with the main run, none of these five-row nodes has a sixth row, and the sampled nodes show no disagreement.
Lemma 2.1: the placements of the two fixed points compatible with the weight conditions were enumerated.	There are 64 in $e_8 \oplus e_8$, all in different components, and none in d_{16}^+ .
Lemma 2.3: exceptional isotropic vectors were searched for by the search program (all 2^{28} vectors), by the cross-check code (all 4^7 patterns) [†] and by the independent implementation below (all 2^{28} vectors).	None of the three finds one.

Table 3, continued

Check	Outcome
$ R $, the seven keys with their orbit sizes, and the depth-1 column of Table 1 were recomputed by the cross-check code (812 patterns) [‡] and by the independent implementation (also by brute force over all 2^{28} vectors).	Both reproduce all values.
The independent implementation (Section 5), with its own normal form, searched for solutions. Its numbers of nodes with 2, 3, 4, 5, 6 rows are 130 857, 81 715 595, 1 248 185 306, 8 and 0. Its eight five-row nodes were re-checked by independently written code (480 candidates).	It finds no solution.
A variant of the search program without two shortcuts, the skipping of words with $M(a) \geq 14$ in the full test and a filter at depth 1 that the normal form implies, was run on part of the search.	Its node counts agree with the main run at each depth.
Last level: each of the 192 five-row nodes was re-validated, and the 60 vectors of norm 1 in its orthogonal complement were tested as sixth rows against every word, by independently written code.	All 11 520 candidates fail.
Parity: the search runs as 224 jobs with 8 threads each, one job for each of the seven keys and each of 32 classes of a hash of the row at depth 1. The transposition (2 4) of the coordinates of A preserves the traces of all lines on $\{0, 1, 2, 3, 4\}$ and pairs the five-row nodes, and the five-row nodes of each job were counted.	The count is even in every job.

 Table 4: Verification of Theorem B. Implementations I and II are the two level-wise programs of §3.6, and the third solver is the guess-and-determine program. The first two rows describe the Implementation I cross-check and the third-solver cross-check. Items marked [‡] belong to the third-solver cross-check.

Check	Outcome
Implementation I cross-check (instance generator and search program): all 119 instances were re-derived and regenerated, and coincide exactly with those searched, explicit words of weight 8 or 12 were exhibited for every removal of six small instances (111 812), the length-48 test was run, with 64 solutions in both programs, and the search was re-run completely. In addition, samples were checked: 2 800 codes built from random forms and from forms at the deepest levels reached by the search, in which every violated constraint carries a word of weight less than 16 and every such word lies over a violated constraint; explicit words of weight 8 or 12 for 274 483 removals (577 894 completions); 17 832 sub-instance tests against an independent naive search program (2.67×10^8 nodes compared); 312 295 260 nodes of the re-run, re-evaluated naively.	The instances coincide with those searched, every checked removal is justified by a word of weight 8 or 12, every checked node agrees with the naive evaluation, and the re-run reproduces every per-level count and finds no solution.
Third solver [‡] : its solution sets were compared with brute force on 30 sub-instances with planted solutions (501 solutions, with and without splitting the search), 7 tests were run on instances with $N + 1 \in \{65, 66\}$ in which some variables are fixed to given values, node accounting was checked for split searches on five instances, about 61 000 run-time invariant checks were made, and unit propagation at the root was recomputed by the cross-check code.	The solution sets agree with brute force, the node accounting is exact, and no invariant check fails.
The 41 codes of (L3), from the database [22], were checked for self-duality and minimum weight 8, and their pairwise inequivalence by canonical forms of the graph on the coordinates and the words of weights 8 and 10 [‡] . Implementation II also checked self-duality and minimum weight.	All 41 codes are self-dual with minimum weight 8, and they are pairwise inequivalent.

Table 4, continued

Check	Outcome
$\text{Aut}(Y_k)$ was computed by nauty [32] with two graph encodings. The generators were checked to be automorphisms, and the order of the group they generate was compared with the order reported by nauty (independent parser)[‡].	For all 41 codes the two encodings agree, the generators are automorphisms, and the group they generate has the reported order.
The conjugacy classes of fixed-point-free involutions were recomputed by the cross-check code[‡] and by Implementation II.	Both find 119 in total, and one code has none.
Implementations I and II computed $\dim G = 18$ and N for each instance.	They agree, with $N = 63, 64, 65$ for 106, 9 and 4 instances.
Implementation I was run on all 119 instances: 6.08×10^{10} nodes in total. The seven largest instances have $9.79\text{--}10.08 \times 10^9$ nodes (five of them), 5.33×10^9 and 5.40×10^9 nodes. The last has 18 nodes in Implementation II and is refuted at the root by the unit propagation of the third solver. Implementation I does no propagation. All other instances have at most 3.59×10^8 nodes each.	It finds no solution.
Implementation II was run on all 119 instances: 4.78×10^{10} nodes in total, five instances with $9.35\text{--}9.74 \times 10^9$ nodes each, the others at most 1.03×10^7 nodes each, deepest level reached 14 of 18. A second run used a different basis order for every instance, with $9.66\text{--}10.05 \times 10^9$ nodes for the five largest instances.	Neither run finds a solution.
The third solver was run on the 113 instances other than the six with the largest trees in Implementation II: 2.37×10^8 nodes in total. Runs are split at depth 5 into 16 jobs as in §3.6, and one instance at depth 6 into 64 jobs.	It finds no solution.
Removal certificates for Implementation II: for a removed child, an independent checker exhibits a word of weight less than 16 and checks that it lies in the code for three completions of the remaining variables. This was done for all removals of 35 instances (132 834 removals, equal to the counts of the search). In addition, a sample of 23 501 removals over all 119 instances was checked, with words y of weights 8, 10 and 12.	Every certificate is valid.
The coverage of the split searches of Implementation II was checked for its five largest instances.	Every part ran to completion, and the level-9 nodes expanded by the parts sum to 65 536 for each instance.

Table 5: Verification of Theorems C and D. The two classification programs and the two labelling programs are those of §4.3 and §4.4. Items marked † belong to the order-3 cross-check, described in the first row.

Check	Outcome
Order-3 reduction and programs † : the reduction was checked on 27 explicit codes of length 72. For the classification, steps (1)–(4) of the proof of Theorem D were recomputed and step (5) was evaluated from the counts of the two programs. Both labelling programs were checked by inspection of the source code, an independently computed reference and an independent solver, which finds no valid labelling for 5 711 classes, among them $G_{24} \otimes \mathbb{F}_4$, all 3 862 classes with $9 \leq \text{Aut}_{\text{Mon}} < 3 M_{24} $ and all 225 with $\beta \geq 94$. The coverage of the main runs was checked with independent checkers.	The reduction holds on these codes, the classification steps are confirmed, and the coverage of the main runs is complete.
<i>Classification (Theorem D)</i>	
Stage (i) was run by both programs: 30, 393, 9 519, 45 775 classes of dimension 2, 3, 4, 5. Class keys were compared at dimensions 4 and 5, and at dimension 5 also the multisets of (key, $ \text{Aut}_{\text{Mon}} $, self-conjugacy).	The two programs agree in all these comparisons.
Isometry search: the first program visits 5.74×10^9 leaves, of which 2.87×10^9 are canonical, and accepts 1.60×10^7 codes. The second program finds 2.872×10^9 orbits of isometries, 3.474×10^{14} isometries in total, and accepts 18 738 263 codes.	Both give 13 485 816 classes, with identical multisets of (key, $ \text{Aut}_{\text{Mon}} $, A_8 , self-conjugacy).
Step (1) of the proof of Theorem D † : every listed code was checked for self-orthogonality, rank 12, no nonzero word of weight less than 8, and the listed A_8 .	All 13 485 816 codes pass.
Step (2) † : the support invariant was computed for every listed code.	It takes 13 485 816 distinct values.
Step (3) † : the automorphism groups and self-conjugacy flags were recomputed.	13 372 811 groups are certified directly and 113 005 by nauty, and all agree with the list.
Step (4) † was checked with independently computed extension counts and automorphism groups, and by a second independent implementation. Independent canonical keys of the classes of dimension 4 and 5 were computed.	The identity holds exactly for $k = 0, \dots, 4$ (for $k = 0$, $\text{ext}(0) = 713\,843\,361$; for $k = 4$ both sides equal 23 376 798 468 859/2 903 040), and the keys are distinct.
The counts $N(E_B)$ of the two programs were compared for all 45 775 codes E_B . The first program counts orbits of $S_8 \times \mathbb{F}_4^\times$, which acts faithfully on $\mathbf{1}^\perp/\langle \mathbf{1} \rangle$ and so freely on the isometries, and its count is 120 960 times the number of orbits. A third, plain count was made on 13 codes E_B , four of them with $N(E_B) = 0$.	The two counts agree for all 45 775, with the same $ \text{Aut}_{\text{Mon}}(E_B) $ and self-conjugacy, and the plain count agrees on the 13.
Step (5) was evaluated in rational arithmetic: the left side from the list, with the recomputed values † of A_8 and $ \text{Aut}_{\text{Mon}} $, and the right side from the counts of each program.	All values equal 526 493 209 678 523/322 560.
<i>Labelling (Theorem C)</i>	

Table 5, continued

Check	Outcome
The main run of the point-placement program covered all 13 485 816 classes, with coverage checked by two independent programs.	No valid Golay code was found for any class. All 13 485 816 classes are covered, none is missing or duplicated, no decision concerns a class outside the list, and no errors were reported. For each class, the program’s count of words of weight 8 up to scalars equals $A_8/3$, and the code it tested agrees with the list (compared by hashes).
The main run of the octad-growth program covered all 13 485 816 classes, with coverage checked by two independent programs.	No solution was found. Each class was decided exactly once in the part to which it was assigned, and the run produced no output other than these decisions.
Symmetry reduction for the two classes of §4.4 whose words of weight 8 span 11 dimensions ($ \text{Aut}_{\text{Mon}} = 288$, $A_8 = 513$ and $ \text{Aut}_{\text{Mon}} = 9216$, $A_8 = 837$): the validity of the group used in the main run was checked, and both classes were re-tested without the reduction, both with the program of §4.5 and with a variant that switches the reduction off when the words of weight 8 do not span the code.	The reduction is valid, and neither re-test finds a solution.
$G_{24} \otimes \mathbb{F}_4$ ($\beta = 253$), with its coordinates in random order and in the order of the reference Golay code, and as a double-circulant code, was tested by point placement (1.52×10^9 nodes per run), by a variant of the octad-growth program without the symmetry reduction, by the octad-growth program with the reduction and by the independent solver [‡] without it (1.66×10^9 nodes).	No run finds a solution.

Running times. The wall-clock times of the parallel parts of the order-5 search sum to 64.5 hours (about 516 thread-hours), and the independent implementation of Table 3 ran for 22.1 CPU-hours. For Theorem B, Implementation I took 288 835 CPU-seconds in total, and Implementation II took 131 678 CPU-seconds in its first run and, in its second run, 134 550 CPU-seconds for the five largest instances and 5 200 CPU-seconds for 111 others. The third solver took 3 889 321 CPU-seconds in total. For Theorem C, the per-class wall-clock times of the point-placement program sum to 68 507 615 s (5.08 s per class), and the slowest class, $G_{24} \otimes \mathbb{F}_4$, took 2 274.3 s. The octad-growth run took about 17 700 CPU-hours. On $G_{24} \otimes \mathbb{F}_4$, a variant of the octad-growth program without the symmetry reduction took 15 336–15 803 s per run, and the octad-growth program with the reduction took 63 s.

DATA AND CODE AVAILABILITY

The programs, instance files, logs and certificates are archived at doi:10.5281/zenodo.23603746. For Theorem A they comprise the search program, the brute-force tester, the planted test, the 192 five-row nodes with their check, and the independent implementation. For Theorem B they

comprise the instance generators, the instance files, the two level-wise programs, the guess-and-determine program, the test scripts, the per-instance logs and the removal certificates (named kill certificates in the archive files). The 41 codes are taken from the database of Harada and Munemasa [22]. For Theorems C and D the files comprise the list of the 13 485 816 classes (for each class a canonical generator matrix, the order of the monomial automorphism group, A_8 and a self-conjugacy flag), the two classification programs, the two labelling programs with their tests, and the per-class results of both main runs. The README of the archive describes how the runs were executed.

REFERENCES

1. C. Aguilar Melchor and P. Gaborit, *On the classification of extremal $[36, 18, 8]$ binary self-dual codes*, IEEE Trans. Inform. Theory **54** (2008), no. 10, 4743–4750.
2. M. Altunbulak, F. Altunbulak Aksu, R. Hafezieh, and İ. Tuvay, *On the permutation automorphisms of binary cubic codes*, arXiv:2402.10667, 2026, Version 3, 6 January 2026.
3. M. Araya and M. Harada, *Some restrictions on the weight enumerators of near-extremal ternary self-dual codes and quaternary Hermitian self-dual codes*, Des. Codes Cryptogr. **91** (2023), no. 5, 1813–1843.
4. A. Bonnet, A. D. Bracco, S. T. Dougherty, L. R. Nochefranca, and P. Solé, *Cubic self-dual binary codes*, IEEE Trans. Inform. Theory **49** (2003), no. 9, 2253–2259.
5. M. Borello, *The automorphism group of a self-dual $[72, 36, 16]$ binary code does not contain elements of order 6*, IEEE Trans. Inform. Theory **58** (2012), no. 12, 7240–7245.
6. ———, *The automorphism group of a self-dual $[72, 36, 16]$ code is not an elementary abelian group of order 8*, Finite Fields Appl. **25** (2014), 1–7.
7. ———, *On automorphism groups of binary linear codes*, Topics in Finite Fields, Contemp. Math., vol. 632, Amer. Math. Soc., Providence, RI, 2015, pp. 29–41.
8. M. Borello, F. Dalla Volta, and G. Nebe, *The automorphism group of a self-dual $[72, 36, 16]$ code does not contain S_3 , A_4 or D_8* , Adv. Math. Commun. **7** (2013), no. 4, 503–510.
9. S. Bouyuklieva, *On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length $24m$* , Des. Codes Cryptogr. **25** (2002), no. 1, 5–13.
10. ———, *On the automorphism group of a doubly-even $(72, 36, 16)$ code*, IEEE Trans. Inform. Theory **50** (2004), no. 3, 544–547.
11. S. Bouyuklieva, E. A. O’Brien, and W. Willems, *The automorphism group of a binary self-dual doubly even $[72, 36, 16]$ code is solvable*, IEEE Trans. Inform. Theory **52** (2006), no. 9, 4244–4248.
12. S. Bouyuklieva, R. Russeva, and E. Karataş, *On some automorphisms of order 3 of the extremal binary codes*, Electron. Notes Discrete Math. **57** (2017), 73–78.
13. J. H. Conway, *The Golay codes and the Mathieu groups*, Sphere Packings, Lattices and Groups, Springer, New York, third ed., 1999, pp. 299–330.
14. ———, *Three lectures on exceptional groups*, Sphere Packings, Lattices and Groups, Springer, New York, third ed., 1999, pp. 267–298.
15. J. H. Conway and 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), no. 2–3, 157–162.
16. J. H. Conway, V. Pless, and N. J. A. Sloane, *Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16*, IEEE Trans. Inform. Theory **25** (1979), no. 3, 312–322.
17. S. T. Dougherty, P. Gaborit, M. Harada, and P. Solé, *Type II codes over $\mathbf{F}_2 + u\mathbf{F}_2$* , IEEE Trans. Inform. Theory **45** (1999), no. 1, 32–45.
18. S. T. Dougherty, S. Karadeniz, and B. Yildiz, *The automorphism group of the doubly-even $[72, 36, 16]$ code can only be of order 1, 3 or 5*, arXiv:1303.4920, 2013, Withdrawn by the authors (v2, 25 March 2013).
19. T. Feulner and G. Nebe, *The automorphism group of an extremal $[72, 36, 16]$ code does not contain Z_7 , $Z_3 \times Z_3$, or D_{10}* , IEEE Trans. Inform. Theory **58** (2012), no. 11, 6916–6924.
20. M. Harada, *A method for constructing quaternary Hermitian self-dual codes and an application to quantum codes*, Des. Codes Cryptogr. **92** (2024), no. 10, 2927–2948.
21. M. Harada, C. Lam, A. Munemasa, and V. D. Tonchev, *Classification of generalized Hadamard matrices $H(6, 3)$ and quaternary Hermitian self-dual codes of length 18*, Electron. J. Combin. **17** (2010), R171.
22. M. Harada and A. Munemasa, *Database of self-dual codes*, <https://www.math.is.tohoku.ac.jp/~mharada/selfdualcodes.htm>, Binary page research/codes/sd2.htm (length 36, minimum weight 8: 41 codes); Hermitian $GF(4)$ page research/codes/hsd4.htm. Accessed 20 October 2026.

23. ———, *Classification of quaternary Hermitian self-dual codes of length 20*, IEEE Trans. Inform. Theory **57** (2011), no. 6, 3758–3762.
24. ———, *Classification of self-dual codes of length 36*, Adv. Math. Commun. **6** (2012), no. 2, 229–235.
25. 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.
26. W. C. Huffman and V. Yorgov, *A $[72, 36, 16]$ doubly even code does not have an automorphism of order 11*, IEEE Trans. Inform. Theory **33** (1987), no. 5, 749–752, Correspondence.
27. G. Janusz, *Solution of the $[72, 36, 16]$ problem*, arXiv:2210.02551, 2022, Withdrawn by the author (v2, 9 November 2022).
28. C. W. H. Lam and V. Pless, *There is no $(24, 12, 10)$ self-dual quaternary code*, IEEE Trans. Inform. Theory **36** (1990), no. 5, 1153–1156.
29. F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward, *Self-dual codes over $GF(4)$* , J. Combin. Theory Ser. A **25** (1978), no. 3, 288–318.
30. F. J. MacWilliams and N. J. A. Sloane, *The Golay codes*, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977, pp. 634–650.
31. C. L. Mallows and N. J. A. Sloane, *An upper bound for self-dual codes*, Information and Control **22** (1973), no. 2, 188–200.
32. B. D. McKay and A. Piperno, *Practical graph isomorphism, II*, J. Symbolic Comput. **60** (2014), 94–112.
33. 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 Appl. **18** (2012), no. 3, 563–566.
34. E. A. O’Brien and W. Willems, *On the automorphism group of a binary self-dual doubly even $[72, 36, 16]$ code*, IEEE Trans. Inform. Theory **57** (2011), no. 7, 4445–4451.
35. V. Pless, *23 does not divide the order of the group of a $(72, 36, 16)$ doubly even code*, IEEE Trans. Inform. Theory **28** (1982), no. 1, 113–117, Correspondence.
36. V. Pless and J. G. Thompson, *17 does not divide the order of the group of a $(72, 36, 16)$ doubly even code*, IEEE Trans. Inform. Theory **28** (1982), no. 3, 537–541, Correspondence.
37. E. M. Rains and N. J. A. Sloane, *Self-dual codes*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), Elsevier, Amsterdam, 1998, pp. 177–294.
38. N. J. A. Sloane, *Is there a $(72, 36)$ $d = 16$ self-dual code?*, IEEE Trans. Inform. Theory **19** (1973), no. 2, 251, Correspondence.
39. N. Yankov, *A putative doubly even $[72, 36, 16]$ code does not have an automorphism of order 9*, IEEE Trans. Inform. Theory **58** (2012), no. 1, 159–163.
40. V. Yorgov, *On the automorphism group of a putative code*, IEEE Trans. Inform. Theory **52** (2006), no. 4, 1724–1726.
41. ———, *On automorphisms of order three of a putative $[72, 36, 16]$ binary self-dual code*, Talk abstract, 30th Midwestern Conference on Combinatorics and Combinatorial Computing (MCCCC30), Illinois State University, Normal, IL, October 2016, <https://about.illinoisstate.edu/MCCCC30/files/2019/11/Yorgov.pdf>.
42. V. Yorgov and D. Yorgov, *The automorphism group of a self-dual $[72, 36, 16]$ code does not contain Z_4* , IEEE Trans. Inform. Theory **60** (2014), no. 6, 3302–3307.
43. V. I. Yorgov, *Binary self-dual codes with automorphisms of odd order*, Problemy Peredachi Informatsii **19** (1983), no. 4, 11–24, In Russian.

ORCID: <https://orcid.org/0000-0003-4668-3639>