Nonexistence of $(243, 121, 60)$ difference sets in $C_3 \times C_9 \times C_9$

P. Graham
https://orcid.org/0009-0007-8493-1505

October 25, 2026

Abstract

We prove, by exhaustive computation, that no $(243, 121, 60)$ difference set exists in $C_3 \times C_9 \times C_9$. Keita Baba settled this case first on October 4, 2026, by a SAT computation with a certificate accepted by a formally verified checker. We give an independent proof by a different method: a lifting search with the reduction checked in Lean. A difference set with these parameters is a 121-element subset whose ordered differences represent every nonzero group element exactly 60 times. Vera López and García Sánchez recorded this group-specific case as unresolved, and Gordon singled it out in his presentation on the La Jolla Difference Set Repository. The reduction builds on the classical multiplier and character methods of Hall, Menon and Turyn and the multiplier searches of Vera López and García Sánchez. A multiplier-fixed translate has thirteen points in the subgroup of elements annihilated by three. Moment identities, singleton congruences and affine normalizations reduce the problem to eight quotient multiplicity arrays. Complete ternary lifting searches exclude all eight. Lean proves the algebraic reduction, normalization, lifting coverage and pruning lemmas; the final formal nonexistence theorem assumes the search assertions established by the external integer computations.

1 Introduction

Keita Baba settled this case first on October 4, 2026, by a SAT computation with a certificate accepted by a formally verified checker [2]. The present paper gives an independent proof by a different method: a lifting search with the reduction checked in Lean.

Write $C_m = \mathbb{Z}/m\mathbb{Z}$ additively. For a subset P of an abelian group, put

$$d_P(g) = \big|\{(a, b) \in P \times P : a - b = g\}\big|.$$

A (v, k, λ) difference set in a group of order v is a subset D with $|D| = k$ and $d_D(g) = \lambda$ for every $g \neq 0$.

Theorem 1. *There is no subset $D \subseteq C_3 \times C_9 \times C_9$ such that $|D| = 121$ and*

$$\big|\{(a, b) \in D \times D : a - b = g\}\big| = 60 \qquad \textit{for every } g \neq 0.$$

Vera López and García Sánchez record these parameters in this group as unresolved in their Table 1, p. 105 of [15], with the question-mark convention of p. 101. Gordon singles out this case in [4, slide 38]; his repository's archived version 1.3 also lists $\mathrm{DS}(243, 121, 60, [3, 9, 9])$ as Open [5]. The neighboring abelian groups and the relevant published restrictions are reviewed in Appendix A.

Baba's proof uses multiplier 61, its 99 orbits, and a SAT encoding over all 49 cyclic quotients with 64,940 variables [2, Steps 1–5 and 8(a)]. The CaDiCaL refutation was accepted by cake_lpr, a

formally verified checker, and by lrat-check. A second route uses the 864 possible images in $G/3G$: one representative has a checked certificate, and all 864 instances were also solved separately, without individual certificates [2, Steps 6–8 and VERIFY, Sections 4–5]. Baba describes the work as written with AI assistance from Anthropic [2, repository README, Caveats].

Our independent proof uses a complete finite reduction and lifting exhaustion. A translate fixed by the multiplier still has many possible unions of orbits; the difficult step is to reduce these possibilities far enough that all lifts can be tested. Section 2 first obtains a fixed translate and the coset moment identities. Section 3 uses those identities to find its thirteen fixed points and the congruences they satisfy. A finite classification shows that all such thirteen-point sets lie in one orbit under the affine maps of Section 4. Section 5 then recovers the quotient multiplicities from the sums on its hyperplanes and reduces them to eight cases. Finally, Section 6 lifts each case by choosing orbits of length three in its cosets, pruning a partial choice whenever an ordered difference count exceeds 60. The proof depends on the external integer computations described in Section 7; the finite classification and the complete lifting search are computational steps.

The work uses the classical multiplier and character methods developed by Hall [6], Menon, Turyn, and others [12, Theorem 5], [14], and the systematic multiplier searches of Vera López and García Sánchez. It also benefits from the later nonexistence and field-descent theory of Arasu, Ma, Leung, Schmidt, and Miller [1, 10, 11, 12]. These contributions supply both the historical question and the algebraic framework for reducing it to a finite computation. The contributors to Lean, mathlib, and the declared library dependencies are also acknowledged for the formal-development infrastructure.

The proofs, the Lean formalization, the search code, the certificate checkers and the text were produced by AI models (from OpenAI and Anthropic), working under the author's direction. The result is computer-assisted and has not yet been reviewed by experts.

2 Multiplier fixedness and quotient moments

The multiplier theorem supplies the symmetry used throughout the proof; the moment identities then restrict the intersection numbers with cosets.

Use coordinates $G = C_3 \times C_9 \times C_9$ and put

$$H = G[3] = \{(x, 3u, 3w) : x, u, w \in C_3\},$$
$$K = 3G = \{(0, 3u, 3w) : u, w \in C_3\}.$$

Thus $|H| = 27$, $|K| = 9$, and $Q = G/K \cong C_3^3$. In particular, H and K are different subgroups.

Set

$$v = 243 = 3^5, \qquad k = 121, \qquad \lambda = 60, \qquad n = k - \lambda = 61, \qquad \exp(G) = 9.$$

Lemma 1. *If D is a difference set as in Theorem 1, then a translate D_0 satisfies $61D_0 = D_0$.*

Proof. The first multiplier theorem applies because G is abelian, $n = 61$ is prime, $61 > \lambda = 60$, and $\gcd(61, 243) = 1$. It gives $61D = D + g$ for some $g \in G$. This is also the $n_1 = 61$ specialization of Menon's multiplier theorem in Miller [12, Theorem 5]; see the classical character and multiplier theory in Turyn [14]. Put $s = \sum_{d \in D} d$. Summing the set identity gives $60s = 121g$. Multiplication by 121 has inverse multiplication by 7 on G, since $121 \cdot 7 \equiv 1 \pmod 9$. For $u = 7s$ we therefore have $60u = g$, whence

$$61(D - u) = D + g - 61u = D - u.$$

Take $D_0 = D - u$. □

In what follows, fixed means fixed by multiplication by 61, and a singleton is an orbit of this action having one point. The initial translating element u can be anywhere in G. Subsequent normalizing translations will lie in H. Multiplication by 61, equivalently by 7 modulo 9, has order three and fixed subgroup exactly H. Its scalar orbits consist of 27 singletons and 72 triples. Every fixed subset is a union of these orbits. A group automorphism commutes with scalar multiplication, and translation by $t \in H$ preserves fixedness because $60t = 0$.

A difference set has no nonzero translation period: if $D + h = D$, then $d_D(h) = 121$, contrary to 60 when $h \neq 0$. It follows that the fixed translates of a fixed difference set D_0 are exactly $D_0 + H$: fixedness of $D_0 + t$ implies that $60t$ is a period, hence $60t = 0$, whose solution set in G is H.

For later use, let $U \leq G$ and $r_U(a+U) = |D \cap (a+U)|$. Counting ordered pairs whose difference lies in U gives

$$\sum_{a+U} r_U(a+U) = 121, \qquad \sum_{a+U} r_U(a+U)^2 = 121 + 60(|U| - 1). \tag{1}$$

Projected autocorrelation counts ordered differences after passage to the quotient, with coset multiplicities retained. More generally, projected autocorrelation equals $121 + 60(|U| - 1)$ at zero and $60|U|$ elsewhere. For an index-three subgroup, the three coset counts consequently satisfy

$$t_0 + t_1 + t_2 = 121, \qquad t_0^2 + t_1^2 + t_2^2 = 4921, \qquad 0 \leq t_i \leq 81. \tag{2}$$

The complete integer solutions are the six permutations of $(36, 40, 45)$. This small finite assertion is checked both in the finite enumerations and in Lean.

3 The thirteen singleton points

The fixed points of the multiplier form H. We determine how a fixed difference set can meet H, then classify the resulting subsets under the affine maps specified in Section 4. The word legal below refers to those maps, whose linear parts are automorphisms and whose translations lie in H.

Assume from now on that D_0 is fixed, and put $S = D_0 \cap H$. There are four projective nonzero linear forms on $(\bar{y}, \bar{z}) \in C_3^2$. For each, the two nonzero fibers contain only scalar triples, so their intersection counts with D_0 are divisible by three. Of $36, 40, 45$, only 40 is not divisible by three; thus the zero-fiber count is 40. Every point of H lies in all four zero fibers, and every point outside H lies in exactly one. Hence

$$4 \cdot 40 = 4|S| + (121 - |S|), \qquad |S| = 13.$$

Let a, b, c be the sizes of S in the three x-layers of H. They satisfy $a + b + c = 13$ and $0 \leq a, b, c \leq 9$. On $Q = G/K$, the three special cells $(x, 0, 0)$ contain only singleton points and have multiplicities a, b, c. Every other cell contains three scalar triples, so its multiplicity lies in $\{0, 3, 6, 9\}$. The $U = K$ instance of (1) gives

$$a^2 + b^2 + c^2 \equiv 601 \equiv 7 \pmod 9.$$

The x-quotient in (2) forces the residues of (a, b, c) modulo three to be a permutation of $(1, 0, 0)$. The complete list of layer triples satisfying these conditions consists of the permutations of $(4, 0, 9)$ and $(4, 3, 6)$.

For any $h \in H \setminus \{0\}$, the scalar action permutes the 60 ordered pairs in D_0^2 of difference h. Its fixed pairs have both endpoints in S; all remaining pair orbits have length three. Therefore

$$|S \cap (S + h)| \equiv 0 \pmod 3 \qquad (h \in H \setminus \{0\}). \tag{3}$$

A $(4, 0, 9)$ layer pattern has intersection four with its translate by $(1, 0, 0)$, so cannot satisfy (3).

A mask here is simply an encoding of a subset of H. The layer conditions above describe exactly

$$6\left[\binom{9}{4}+\binom{9}{4}\binom{9}{3}\binom{9}{6}\right]=5{,}335{,}092 \tag{4}$$

distinct subsets of H. For each candidate subset, the test evaluates $|S\cap(S+h)|$ for every $h\in H\setminus\{0\}$; these are the 26 congruences in (3). The factor six in (4) orders the three distinct layer sizes, and the binomial factors choose the points in each layer of nine points. The retained subsets are then compared as a set with the affine orbit of the specified representative. Exhaustive testing of all 26 congruences leaves exactly 7,776 masks. An enumeration scanning every one of the $\binom{27}{13}=20{,}058{,}300$ thirteen-point subsets independently reproduces both counts.

The surviving set of masks is exactly the orbit of S_0, specified in Appendix B, under the legal affine maps described below. Equality of these two finite sets, with normalization witnesses, establishes normalization; agreement of their cardinalities alone would not do so. Thus every hypothetical difference set has a fixed legal image with H-part exactly S_0.

4 Affine normalization

The normalizations must preserve both differences and fixedness under the multiplier. We give the coordinate maps and show why they do so. The letters a, b, c in this section are coefficients of a map; the three layer sizes used in Section 3 are fixed when the representative S_0 is chosen.

Use $F = A + t$ with $t = (t_0, 3t_1, 3t_2) \in H$, where

$$\begin{aligned} F(x,y,z) = \big(&ax+by+cz+t_0 \pmod 3,\\ &3dx+ey+fz+3t_1 \pmod 9,\\ &3gx+hy+iz+3t_2 \pmod 9\big). \end{aligned} \tag{5}$$

Here $a\not\equiv 0 \pmod 3$ and $B=\left(\begin{smallmatrix} e & f \\ h & i\end{smallmatrix}\right)$ is invertible modulo three. The parameters in the first coordinate and d, g, t_j are taken modulo three; entries of B have chosen lifts modulo nine.

The coordinate orders make A additive. Its induced map on $G/3G$ has block upper-triangular matrix with diagonal blocks a and $B \pmod 3$, so is invertible. If $A(p) = 0$, it follows that $p \in 3G = K$. On K, the map is again given by $B \pmod 3$, which is invertible; hence $p = 0$. Thus A is an automorphism. Translation preserves differences, and $60t = 0$ gives $F(61p) = 61F(p)$. Consequently F preserves the difference-set property and scalar fixedness.

For $b = c = 0$, the induced H-actions, writing its last two coordinates as a vector $\boldsymbol{u} \in C_3^2$, are

$$(x, \boldsymbol{u}) \longmapsto (ax + t_0, B\boldsymbol{u} + \boldsymbol{d}x + \boldsymbol{t}).$$

They form a group of order $2 \cdot 3 \cdot 48 \cdot 9 \cdot 9 = 23{,}328$. The factors count $a, t_0, B, \boldsymbol{d}, \boldsymbol{t}$, respectively. Each has an explicit full-G lift of (5). Here a lift extends the displayed action on H to the whole group G.

The orbit of S_0 has size 7,776, so its stabilizer in this H-action group has order three.

Since the three layer sizes of S_0 are distinct, an S_0-stabilizing H-action has $a = 1, t_0 = 0$. Each of its three possibilities has nine (b, c) extensions. These induce 27 distinct permutations on Q, forming a group of order 27.

5 Quotient multiplicities

The sums over the thirteen projective families of hyperplanes determine all the intersection numbers with K-cosets. In this section a cell means a K-coset, indexed by its image in Q. The three special

cells are those indexed by $(x, 0, 0)$.

Normalize S to S_0 and define

$$r(q) = |D_0 \cap (q + K)| \qquad (q \in Q).$$

The notation now refers to the normalized fixed image of D_0. Its special entries $r(x, 0, 0)$ are $(4, 3, 6)$; initially each of the other 24 entries may be any of $0, 3, 6, 9$.

Choose one representative of each of the 13 projective nonzero forms $L : Q \to C_3$, by requiring its first nonzero coefficient to be 1, and put

$$t_L(j) = \sum_{L(q)=j} r(q).$$

If L ignores x, its zero fiber contains all thirteen singleton points; otherwise it contains the four points of the $x = 0$ singleton layer. Thus $t_L(0) \equiv 1 \pmod 3$ in both cases. Equation (2) forces

$$t_L(0) = 40, \qquad \{t_L(1), t_L(2)\} = \{36, 45\}. \tag{6}$$

For $p, q \in Q$, exactly thirteen of the forms have $L(p) = L(q)$ when $p = q$, and exactly four when $p \neq q$. Therefore

$$\sum_L t_L(L(q)) = 13r(q) + 4(121 - r(q)) = 484 + 9r(q). \tag{7}$$

The coefficient of $r(q)$ in (7) is nine, so the prescribed hyperplane sums determine $r(q)$ uniquely. The incidence inversion mentioned in the final proof is the recovery of r from these hyperplane sums. This identity proves completeness of the following finite procedure. Enumerate all $2^{13} = 8192$ ways of ordering $(36, 45)$ in (6); recover $r(q)$ from (7); retain integer coefficients between zero and nine, the special entries $(4, 3, 6)$, and nonspecial entries divisible by three. Every possible quotient array must occur, since its line assignments occur and the inversion recovers it uniquely.

Exactly 144 arrays survive. Each has projected autocorrelation 601 at zero and 540 at every nonzero element of Q, as required by (1) and its nonzero counterpart. Each has twelve nonspecial entries equal to three and twelve equal to six.

The divisibility condition in the finite procedure is the union-of-triples condition from Section 3. The group of 27 induced S_0-stabilizing quotient permutations partitions these arrays into eight orbits.

Their orbits are disjoint and their union is the full 144-array set. Each nine-digit string lists $r(x, \bar{y}, \bar{z})$ for fixed x, with $3\bar{y} + \bar{z} = 0, \ldots, 8$ in increasing order.

For each array an explicit legal map sends it to its representative while preserving S_0. These maps are part of the finite normalization witnesses.

6 Lifting and the proof of nonexistence

For each quotient representative, selecting multiplier orbits in the K-cosets gives a ternary tree. We first prove that these choices cover all possible sets and then give the rejection rule for its search.

Fix a case in Table 1. Each of its 24 nonspecial K-cosets has nine points, partitioned into three scalar triples. A multiplicity-three cell must select exactly one triple, and a multiplicity-six cell exactly two. In either case there are exactly three choices, namely all members of the appropriate $\binom{3}{1}$ or $\binom{3}{2}$ family.

Points and quotient cells are ordered lexicographically by their least nonnegative coordinate representatives. Number a cell's triples $0, 1, 2$ by their least encoded point. A digit j in a multiplicity-three cell selects triple j; in a multiplicity-six cell it omits triple j. Order the cells by placing the twelve six-cells first in increasing Q-index, followed by the twelve three-cells in increasing Q-index. Denote the resulting set for a case c and digit word $\boldsymbol{d} \in \{0, 1, 2\}^{24}$ by $\mathcal{L}(c, \boldsymbol{d})$.

Lemma 2. *For a fixed case, the map $\boldsymbol{d} \mapsto \mathcal{L}(c, \boldsymbol{d})$ is a bijection onto all scalar-fixed subsets with singleton part S_0 and that quotient multiplicity array. Every such set has 121 points.*

Proof. The union of S_0 and the chosen cell options has size $13 + 12 \cdot 6 + 12 \cdot 3 = 121$, is scalar-fixed, and has the prescribed multiplicities. Conversely, any fixed set with those multiplicities intersects each cell in an invariant subset of the required size, hence in one of the three stated options. This proves surjectivity. Intersecting the union with each of the disjoint cells recovers its option and unique digit, proving injectivity. □

For each of the eight representatives, a full choice is a word of length 24 in three digits. Its first twelve digits determine a subtree, whose completions are all possible twelve-digit tails. Every full word has exactly one such prefix, so the subtrees partition the eight lifting families. Appendix C records their numerical indexing and the intervals I_r used to collect consecutive prefixes.

If $P \subseteq P'$, then $d_P(g) \leq d_{P'}(g)$ for every g. Thus a partial set for which some nonzero difference count exceeds 60 has no difference-set extension. This is the only difference-count rejection needed by the search. At a complete 121-point leaf,

$$\sum_{g \neq 0} d_P(g) = 121 \cdot 120 = 242 \cdot 60.$$

Consequently all counts being at most 60 is equivalent to every count being exactly 60.

For every prefix, depth-first search tries all three digits at each remaining position, unless the monotone rejection rule applies.

The exhaustive computations give zero difference-set leaves in each of the eight cases. Two searches using different difference-count representations agree, and a separately written third lifting program exhausts all the same ranges. The common finite inputs are checked by independent enumerations and by the formal coverage proof. The recorded counts and the certificate comparisons are in Appendix C and the checking notes.

Proof of Theorem 1. Suppose D were such a difference set. Lemma 1 gives a fixed translate. The singleton conditions and complete classification send its H-part legally to S_0. The incidence inversion places its quotient in the complete 144-array set, and a legal S_0-stabilizing map sends that array to Table 1. By Lemma 2, the resulting difference set is a leaf of that case. Its prefix lies in exactly one interval (10). Exhaustion rejects every leaf under that interval by tests that reject no difference set, a contradiction. □

7 Computational verification

The computation excludes every lift, while the formal proof establishes that every hypothetical difference set is one of these lifts. The following statements describe precisely how the two parts fit together.

The Lean definition of the group is the product of the three residue groups of moduli $3, 9, 9$. Its `IsDiffSet` predicate is exactly cardinality 121 and ordered-difference count 60 at every nonzero element. The singleton and quotient classifications are proved in Lean using finite tables; the programs separately enumerate the subsets and multiplicity arrays. For the final implication, each RangeClear(r) asserts that every lift with a prefix in the interval I_r fails to be a difference set. The intervals cover the prefix subtrees described in Section 6; their exact indexing and the full coverage statement are given in Appendix C.

In the equivalent range-assertion formulation checked in the formal development, `DS243.no_difference_set` states

$$(\forall r < 1038,\ \mathrm{RangeClear}(r)) \implies \neg\exists D \subseteq G,\ \mathrm{IsDiffSet}(D).$$

The conclusion is exactly Theorem 1: the product of residue groups is G, and IsDiffSet uses the cardinality and ordered differences in that theorem. The correspondence between the formal leaf table and the executable options, and the exhaustive range assertions, are external checks. The checking notes in the accompanying source bundle identify the exact formal statement types, the logical axioms and the reproduction commands.

Appendix A Known nonexistence criteria

These sources also put the question in perspective. For the same parameters, the other six abelian groups of order 243 are already recorded as follows; this is historical context, not a new proof of those entries:

group	recorded answer	attribution
C_{243}	No	Lander
$C_3 \times C_{81}$	No	Lander
$C_9 \times C_{27}$	No	Arasu–Ma
$C_3^2 \times C_{27}$	No	Vera López–García Sánchez
$C_3^3 \times C_9$	No	Vera López–García Sánchez
C_3^5	Yes	Paley's finite-field construction

The source for the complete list and its attributions is Gordon [5].[1] For $C_3 \times C_{81}$ the two records give different attributions; the displayed table follows Gordon, while the following description follows the 1997 table. The 1997 table credits the negative entry for C_{243} to Lander's Theorem 4.38 [8] with $q = 3$ (its reference 10). For $C_3 \times C_{81}$, $C_3^2 \times C_{27}$, and $C_3^3 \times C_9$, it uses method 21, multiplier-orbit enumeration with multiplier 61. Here 21 is the table marker used in the source for that enumeration. Arasu and Ma [1] subsequently resolved $C_9 \times C_{27}$. For C_3^5, Paley's quadratic-residue construction [13] in the additive group of $\mathbb{F}_{243}$ gives the stated parameters. The 1997 table cites Emma Lehmer [9] for its positive entry. The nonexistence at issue here concerns the group $C_3 \times C_9 \times C_9$, settled first by Baba [2].

The parameter identity $k(k-1) = \lambda(v-1)$ holds. The odd-order Bruck–Ryser–Chowla equation $61x^2 - 60y^2 = z^2$ has the nonzero solution $x = y = z = 1$. These elementary necessary conditions do not exclude the parameters.

Turyn's character restrictions [14] allow this application: $\mathrm{ord}_3(61) = 1$ is odd. At the nontrivial character orders 3 and 9, the prime 61 is not self-conjugate. Indeed, its powers modulo 3 equal 1, and modulo 9 cycle through $7, 4, 1$, never -1. Obstructions requiring a common prime divisor of n and v have no such prime here; in particular that ingredient of the Lander-type restrictions in Leung–Ma–Schmidt [10] is absent.

In the following paragraph F denotes the published field-descent function, rather than an affine map. For the field-descent function of Leung and Schmidt [11, Definition 2.6], one obtains $F(9, 61) = 3$. Here $\mathrm{ord}_3(61) = 1$ and $61 \not\equiv 1 \pmod 9$, so the exponent $b_3 = 1$ is permitted in that definition. Taking their factor A to be the entire group and the complementary factor trivial,

[1] This small status summary is selected and reformatted from Daniel M. Gordon's repository data, copyright 2024 Daniel M. Gordon, under CC BY 4.0. Group notation and presentation are changed; the source status values are unchanged. No endorsement is implied.

Theorem 4.3 gives

$$\exp(G) \le 243\sqrt{\frac{3^2}{4\cdot 61\cdot\varphi(3)}} = \frac{729}{\sqrt{488}} \approx 33.0003,$$

which permits exponent 9. Their Theorem A [11, Theorem A] cannot instead split off a C_9 factor: its coprimality condition would require $\gcd(9, \exp(C_3 \times C_9)) = 1$, whereas this gcd is 9. Theorem 4.1 [11, Theorem 4.1] requires a cyclic Sylow subgroup, also absent here.

Arasu and Ma's 2001 nonexistence result [1] resolves $C_9 \times C_{27}$. The relevant theorem, as explicitly restated and extended by Miller [12, Theorems 1 and 3], assumes

$$G = C_{p^e} \times J, \qquad e \ge 2, \qquad \exp(\mathrm{Syl}_p J) < p^e.$$

The displayed group hypothesis is from Miller's Theorem 1; his Theorem 3 gives the subsequent multiplier bound. Splitting off C_9 in the present group leaves another C_9, so the strict exponent inequality fails. The forbidden-multiplier congruences would demand both $t \equiv 4 \pmod 9$ and $t \equiv 1 \pmod 9$. Although the older numerical condition $4(p-1)n = 488 > 243$ holds, it cannot repair the failed group hypothesis.

Chen, Xiang, and Sehgal [3] study skew Hadamard abelian difference sets, which satisfy the additional partition $G = \{0\} \dot\cup D \dot\cup (-D)$. The present parameters do not supply this hypothesis. Consequently a skew-only exponent bound cannot be applied to the ordinary difference-set question.

For the following comparison the defect is $d = v-k$, the notation of He and Wu[7, Theorem 4.7]. Recent work on signed difference sets by He and Wu [7] includes ordinary difference sets but does not yield this exclusion by the criteria considered here. Their Theorem 3.2 has the same failed self-conjugacy test for 61; Theorem 4.2 requires even v; Theorem 4.4 requires $k = v - 1$; and Theorem 4.7 requires an elementary abelian group and a defect bound, whereas this group is not elementary abelian and the defect is $d = 122 > 5$.

Source-access qualifications for these historical comparisons are recorded in the accompanying checking notes.

Appendix B Finite classification data

The following data specify the representative used in the main proof and record the finite classification checks.

For an explicit finite encoding, the point $(x, 3u, 3w) \in H$ has mask bit $9x + 3u + w$, with bit zero the least significant bit.

$$S_0: \quad \text{mask } 24909666, \qquad (a,b,c) = (4,3,6), \tag{8}$$

A separate depth-first enumeration assigns $\{0,3,6,9\}$ to the 24 nonspecial cells and enforces all index-three moment triples, without assuming which fiber has count 40. It gives exactly the same set of 144 arrays.

Representatives in the order used for lifting are given in Table 1.

The orbit sizes are

$$27, 27, 9, 9, 27, 27, 9, 9;$$

their stabilizers in the induced 27-element group have orders $1, 1, 3, 3, 1, 1, 3, 3$.

B.1 A centered coset invariant

For the centered fixed translate, let

$$m(v) = |D_0 \cap (v + H)| \qquad (v \in G/H \cong C_3^2).$$

case c	orbit size	$x=0$	$x=1$	$x=2$
0	27	463666333	366636636	633336336
1	27	463663363	366633666	633333366
2	9	436666333	366663663	633363363
3	9	436636336	366633666	633333366
4	27	463666333	363633633	663366366
5	27	436666333	336633633	636366366
6	9	463666333	366366663	633363633
7	9	463636336	366336666	633333636

Table 1: The eight quotient multiplicity representatives.

We have $m(0) = 13$. The zero fiber for each of the four directions on G/H has count 40, so

$$m(v) + m(-v) = 27 \qquad (v \neq 0).$$

After singleton normalization, $m(v) = \sum_x r(x, v)$. The complete quotient classification gives $m(v) \in \{9, 12, 15, 18\}$ for $v \neq 0$. Legal normalizations induce an invertible linear map on G/H, so these statements transfer back to the centered fixed translate. Each opposite pair is consequently $\{9, 18\}$ or $\{12, 15\}$.

The $U = H$ moment identity is

$$\sum_v m(v)^2 = 121 + 60 \cdot 26 = 1681.$$

If j of the four opposite pairs are $\{9, 18\}$, then

$$1681 - 13^2 = j(9^2 + 18^2) + (4 - j)(12^2 + 15^2) = 1476 + 36j.$$

Thus $j = 1$: the eight off-H cosets have multiplicities

$$9, 18, 12, 12, 12, 15, 15, 15, \tag{9}$$

with one opposite pair $\{9, 18\}$ and three $\{12, 15\}$. All 144 arrays satisfy this invariant.

Appendix C Search data and indexing

Split each 24-digit word after twelve digits. With leading zeroes retained, give its first half the big-endian rank

$$p = \sum_{j=0}^{11} d_j 3^{11-j}, \qquad \mathrm{id} = c\,3^{12} + p.$$

The complete ID domain has size

$$N = 8 \cdot 3^{12} = 4{,}251{,}528,$$

and is partitioned into 1,038 intervals

$$I_r = [4096r, \min(4096(r+1), N)), \qquad 0 \leq r < 1038. \tag{10}$$

Each ID specifies the full cylinder of all 3^{12} possible tails. Different prefixes define disjoint cylinders and every full digit word has exactly one prefix, so these cylinders partition all eight trees.

In digits(id, $\boldsymbol{t}$), the first twelve entries and the tail are concatenated. Here the first twelve digits are the leading-zero-preserving base-three expansion of id mod531441 and the last twelve are $\boldsymbol{t}$.

The formal coverage implication says: if D is a difference set, then there exist $u \in G$, a word w of legal affine maps, an integer $r < 1038$, an $\mathrm{id} \in I_r$, and a twelve-digit tail $\boldsymbol{t}$ such that

$$F_w(D-u) = \mathcal{L}\left(\left\lfloor \frac{\mathrm{id}}{531441} \right\rfloor, \mathrm{digits}(\mathrm{id}, \boldsymbol{t})\right). \tag{11}$$

The map F_w is an additive automorphism followed by a translation in H. For an interval I_r, define the semantic assertion

$$\begin{aligned} \mathrm{RangeClear}(r): \quad & \text{for every } \mathrm{id} \in I_r \text{ and every twelve-digit tail } \boldsymbol{t}, \\ & \mathcal{L}\left(\left\lfloor \frac{\mathrm{id}}{531441} \right\rfloor, \mathrm{digits}(\mathrm{id}, \boldsymbol{t})\right) \text{ is not a difference set.} \end{aligned} \tag{12}$$

The formal nonexistence result is conditional on the family

$$\forall r < 1038, \qquad \mathrm{RangeClear}(r).$$

The recorded exhaustive searches have the following totals.

depth-twelve prefixes	4,251,528
search nodes	108,733,222,341
difference-set leaves	0.

References

[1] K. T. Arasu and S. L. Ma, *A nonexistence result on difference sets, partial difference sets and divisible difference sets*, Journal of Statistical Planning and Inference **95** (2001), 67–73. doi:10.1016/S0378-3758(00)00278-0.

[2] Keita Baba, *No (243, 121, 60) difference set in $\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9$*, in *Answers to seven open questions (2026)*, October 4, 2026, repository `kei825/open-questions-2026`, commit `d40fc3a3`. https://github.com/kei825/open-questions-2026/tree/d40fc3a3ac538e08e1bc31cf45b5d1204a2c34c8/space/difference-set-243. Repository README (Caveats): https://github.com/kei825/open-questions-2026/blob/d40fc3a3ac538e08e1bc31cf45b5d1204a2c34c8/README.md.

[3] Y. Q. Chen, Q. Xiang, and S. K. Sehgal, *An exponent bound on skew Hadamard abelian difference sets*, Designs, Codes and Cryptography **4** (1994), 313–317. doi:10.1007/BF01388647.

[4] Daniel M. Gordon, *The La Jolla Difference Set Repository*, presentation, August 3, 2019, slides 11 and 38 (slide 38 is physical PDF page 49). Wayback Machine snapshot, May 2, 2024: https://web.archive.org/web/20240502201448/https://cargo.wlu.ca/ArasuFest/ArasuFest_talks/Dan_Gordon.pdf.

[5] Daniel M. Gordon, *La Jolla Difference Sets Repository*, archived dataset, version 1.3, April 24, 2026. doi:10.5281/zenodo.19740740. Repository and definition of entries: https://dmgordon.org/difference-sets/.

[6] Marshall Hall Jr., *A Survey of Difference Sets*, Proceedings of the American Mathematical Society **7** (1956), 975–986. doi:10.1090/S0002-9939-1956-0082502-7.

[7] Zhiwen He and Jiayan Wu, *Nonexistence results and constructions for signed difference sets*, preprint, arXiv:2608.22936v2, September 20, 2026 (first version August 24, 2026). https://arxiv.org/abs/2608.22936v2.

[8] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, London Mathematical Society Lecture Note Series, vol. 74, Cambridge University Press, Cambridge, 1983. doi:10.1017/CBO9780511662164.

[9] Emma Lehmer, *On residue difference sets*, Canadian Journal of Mathematics **5** (1953), 425–432. doi:10.4153/CJM-1953-047-3.

[10] K. H. Leung, S. L. Ma, and B. Schmidt, *Nonexistence of abelian difference sets: Lander's conjecture for prime power orders*, Transactions of the American Mathematical Society **356** (2004), 4343–4358. doi:10.1090/S0002-9947-03-03365-8.

[11] K. H. Leung and B. Schmidt, *The Field Descent Method*, Designs, Codes and Cryptography **36** (2005), 171–188. doi:10.1007/s10623-004-1703-7.

[12] Niklas Miller, *Forbidden multipliers in abelian difference sets*, preprint, arXiv:2511.10231v1, November 13, 2025. `https://arxiv.org/abs/2511.10231v1`.

[13] R. E. A. C. Paley, *On Orthogonal Matrices*, Journal of Mathematics and Physics **12** (1933), 311–320. doi:10.1002/sapm1933121311.

[14] R. J. Turyn, *Character sums and difference sets*, Pacific Journal of Mathematics **15** (1965), 319–346. doi:10.2140/pjm.1965.15.319.

[15] A. Vera López and M. A. García Sánchez, *On the existence of abelian difference sets with* $100 < k \leq 150$, Journal of Combinatorial Mathematics and Combinatorial Computing **23** (1997), 97–112; Table 1, p. 105. Publisher's article record.