RANK DEFECT IN COSET-2BGA CODES AT $n = 48$: AN EXHAUSTIVE CENSUS, AND A MODULE CRITERION THAT CANNOT HOLD

KOREA SUPERINTELLIGENCE LABS

Abstract. Coset-based two-block group algebra (coset-2BGA) codes replace the regular action of a group by its action on the cosets of a subgroup $H \leq G$; when H is not normal the two CSS parity checks of $Q_G^H(a,b)$ can have different ranks, and this *rank defect* is what controls the dimension. Lu, Guo, Liu and Yang (arXiv:2608.09115) study one instance — $G = \mathrm{SmallGroup}(72,30)$, $H \cong C_3$, $[G{:}H] = 24$, $n = 48$, $w_a = w_b = 4$ — announce a census of it, and conjecture that the defect is detected by a codimension-one submodule of $\mathbb{F}_2[G/H]$ containing $\langle a \rangle$ but not $\langle b \rangle$. We compute the joint rank distribution of the whole family: over all 9 430 575 normalised support pairs, 29 cells occur, 157 464 pairs have a rank defect, the defect takes the value 3 as well as 1, and the dimension k takes 23 distinct values from 2 to 36 rather than the two values the conjecture allows. We then show the conjecture's criterion cannot be satisfied: $\mathbb{F}_2[G/H]$ has exactly one codimension-one G-submodule and exactly three codimension-one $N_G(H)$-submodules, and every one of them contains every admissible $\langle b \rangle$, because $w_b = 4$ is even and b lives in a single orbit. Finally we give the distance distribution of the rank-defect stratum: of its 142 176 normalised pairs, 126 048 have $d \leq 4$, 14 592 have $d = 5$ and 1536 have $d \geq 6$. Every numerical statement below is machine-checked in Lean 4.

1. Introduction

Two-block CSS codes are defined by parity-check matrices $H_X = [\,A \mid B\,]$ and $H_Z = [\,-B^{\mathsf{T}} \mid A^{\mathsf{T}}\,]$ with A, B commuting square matrices, so that $H_X H_Z^{\mathsf{T}} = 0$ automatically [4, 5]. Taking A and B from the regular representation of a finite group gives the two-block group algebra (2BGA) codes of Lin and Pryadko [3]. Aydin, Tamo and Barg [2] generalise the construction by replacing the regular action with the action on cosets: for $H \leq G$ of index m and $N = N_G(H)$, the group G acts on the left of G/H and N acts on the right, the two actions commute, and for $a \in \mathbb{F}_2[G]$, $b \in \mathbb{F}_2[N]$ the code $Q_G^H(a,b)$ is the two-block CSS code on $n = 2m$ qubits with $A = L(a)$, $B = R(b)$. When $H \trianglelefteq G$ the construction reduces to the 2BGA code over G/H [2], and in the cyclic case the defect "vanishes identically" [1, §VII]; for a non-normal H it need not, and writing $k = n - \operatorname{rank} H_X - \operatorname{rank} H_Z$ in the form

$$k = 2\big(m - \operatorname{rank} H_X\big) + \big(\operatorname{rank} H_X - \operatorname{rank} H_Z\big)$$

of [1, eq. (4)] separates the generic contribution from the correction. We call $\operatorname{rank} H_Z - \operatorname{rank} H_X$ the *rank defect*.

Lu, Guo, Liu and Yang [1] devote Section VII of their paper on cyclic bicycle codes to one instance of the coset construction, chosen small enough to enumerate.

Date: August 30, 2026.

They fix

(1)
$$G = \mathrm{SmallGroup}(72,30), \quad H \cong C_3, \quad m = [G{:}H] = 24, \quad n = 48, \quad w_a = w_b = 4,$$

report that it was "enumerated exhaustively by computer into 123 equivalence classes under S_{48} coordinate permutation and the CSS X/Z swap" [1, §VII], and state two things about it. The first is a rank-degeneracy theorem, their Theorem 16: every code of the family with $d = 5$ has $\operatorname{rank} H_X = 19$, $\operatorname{rank} H_Z = 20$, $k = 9$, whence no $[[48, 10, 5]]$ code lies in the family. Its computer-assisted proof ends

> "All remaining classes — 110 with $d \leq 4$ and 6 with $d = 6$ — have full ranks $19+19$ and $k = 10$, so rank loss is tied to distance exactly 5, not to small or large distance as such."

The second is their Conjecture 17, labelled `conj:module` in the e-print source:

> "For this family, $\operatorname{rank} H_Z > \operatorname{rank} H_X$ iff the cyclic G-submodule $\langle a \rangle \subseteq \mathbb{F}_2[G/H]$ is contained in a proper submodule U with $\dim \mathbb{F}_2[G/H]/U = 1$, while $\langle b \rangle \not\subseteq U$. Whenever this happens the code has $k = 9$ and $d = 5$; otherwise $k = 10$ and $d \in \{3, 4, 6\}$."

Neither statement is accompanied by data: "the full census data and the structural analysis will be developed in a companion paper" [1, §VII], and the paper's list of open problems asks for a proof of the conjecture. As of 30 August 2026 no such companion paper had appeared: an arXiv author query for the first author, re-run on that date, returns after [1] a single later item, arXiv:2608.21852 of 22 August 2026, on quantum locally repairable codes.

This paper supplies the census and settles the conjecture. Write $\mathcal{F}$ for the set of *normalised support pairs* of the family (1): pairs (a, b) where $a \subseteq G$ has four elements including 1 and b is a set of four cosets of H in N including H itself. By the translation equivalence of [2] every code of the family is equivalent to $Q^H_G(a, b)$ for some $(a, b) \in \mathcal{F}$, and $|\mathcal{F}| = \binom{71}{3}\binom{11}{3} = 57\,155 \cdot 165 = 9\,430\,575$.

Results.

- **The census** (Theorem 3). The joint distribution of $(\operatorname{rank} H_X, \operatorname{rank} H_Z)$ over $\mathcal{F}$ occupies 29 cells (Table 1). The rank defect is nonzero on 157 464 pairs, split exactly 78 732/78 732 by sign; it takes the value 3 as well as 1; and k takes 23 distinct values from 2 to 36. Only 2.47% of $\mathcal{F}$ has $k = 10$ and 1.51% has $k = 9$, so the dichotomy "$k = 9 \ldots$ otherwise $k = 10$" describes under 4% of the family it is about.
- **The criterion cannot hold** (Theorem 6). The permutation module $\mathbb{F}_2[G/H]$ has exactly one codimension-one G-submodule, exactly three codimension-one N-submodules and exactly one codimension-one sub-bimodule; and for every one of the 495 admissible supports b, both the vector v_b and the whole image of $R(b)$ lie inside every one of them. The clause $\langle b \rangle \not\subseteq U$ is therefore unsatisfiable in this family, under each of the three readings of "submodule". The other half of the criterion is not degenerate in the same way: in the N-reading there are supports a with $\langle a \rangle \not\subseteq U$, so the first clause really does constrain a and it is only the second that can never be met.
- **Witnesses** (Theorem 10). Explicit members of the family, three of them of check weight 8, with $(\operatorname{rank} H_X, \operatorname{rank} H_Z, k, d) = (19, 20, 9, 2)$, with

$(20, 19, 9, 2)$, with $(9, 12, 27, 2)$ — rank defect 3 — and with $(19, 20, 9, 6)$, the last against "rank loss is tied to distance exactly 5".

- **The defect stratum's distances** (Theorem 11). Of the 142 176 normalised pairs with $\{\operatorname{rank} H_X, \operatorname{rank} H_Z\} = \{19, 20\}$ and $k = 9$, exactly 126 048 have $d \leq 4$, 14 592 have $d = 5$, and 1536 have $d \geq 6$. So 88.7% of that stratum fails the conjecture's "$d = 5$" conclusion, and 1536 of its members carry rank loss at distance at least 6.

What is confirmed, and what is left open. The refutation is of the conjecture and of the closing clause of the rank-degeneracy theorem, not of everything in [1, §VII]. The rank values that section quotes do occur in this family, and in quantity: the cells $(19, 19)$ and $\{(19, 20), (20, 19)\}$ together carry 374 936 normalised pairs, 3.98% of $\mathcal{F}$, and codes with a rank defect, $k = 9$ and $d = 5$ number 14 592. The theorem's own assertion — that every $d = 5$ code of the family has ranks $19, 20$ and $k = 9$ — is not contradicted by anything proved here; outside the $k = 9$ stratum we prove distances only at named codes, and our counts inside it do not separate the cells $(19, 20)$ and $(20, 19)$, so we do not test the orientation of that statement either. Remark 14 reports an unformalised computation consistent with it. What we could not reproduce is the partition into 123 classes (Remark 4), and we do not claim more about it than that. The mathematical question the family inherits is stated in Section 9: the defect is the failure of $\dim(\operatorname{im} L(a) \cap \operatorname{im} R(b))$ to be invariant under inversion of the supports, and a correct module criterion should be a statement about that intersection.

All counts below are counts of *normalised support pairs*. Distinct pairs in $\mathcal{F}$ can give equivalent codes, and we make no claim about the number of equivalence classes.

2. The construction and the family

Coset-2BGA codes. Let G be a finite group, $H \leq G$ a subgroup of index m, and $N = N_G(H)$. On the set G/H of left cosets, G acts on the left by $L(g) : xH \mapsto gxH$ and N acts on the right by $R(g) : xH \mapsto xgH$, the latter well defined precisely because g normalises H. Both are permutations of the m cosets and they commute [2, Prop. II.2]. Extending L and R linearly to the group algebras, $a \in \mathbb{F}_2[G]$ and $b \in \mathbb{F}_2[N]$ give commuting $m \times m$ matrices $L(a)$, $R(b)$ over $\mathbb{F}_2$, and the coset-2BGA code is the two-block CSS code

$$Q_G^H(a, b): \qquad H_X = [\, L(a) \mid R(b) \,], \qquad H_Z = [\, R(b)^{\mathsf{T}} \mid L(a)^{\mathsf{T}} \,]$$

on $n = 2m$ qubits [2, Construction 1] (over $\mathbb{F}_2$ the sign in the definition of H_Z is immaterial). Its parameters are $k = n - \operatorname{rank} H_X - \operatorname{rank} H_Z$ and $d = \min(d_X, d_Z)$ [2, Prop. III.1], where throughout this paper d_X is the least weight of a vector of $\ker H_Z$ outside the row space of H_X and d_Z is the same with the roles exchanged; [2] attach the two labels the other way round, which changes neither d nor any statement below. Since $L(g)^{\mathsf{T}} = L(g^{-1})$ and $R(g)^{\mathsf{T}} = R(g^{-1})$ for permutation matrices, writing $a^\dagger$ for the support a with every element inverted we have

(2)
$$\operatorname{rank} H_X(a, b) = \dim\bigl(\operatorname{im} L(a) + \operatorname{im} R(b)\bigr), \qquad \operatorname{rank} H_Z(a, b) = \operatorname{rank} H_X(a^\dagger, b^\dagger),$$

so the rank defect changes sign under $(a, b) \mapsto (a^\dagger, b^\dagger)$, an involution of the family.

The instance. Throughout, $G = \mathrm{SmallGroup}(72, 30)$, of structure $C_3 \times ((C_6 \times C_2) \rtimes C_2)$, and H is a non-normal subgroup of order 3. In GAP [6] this group has three conjugacy classes of subgroups of order 3: two of them normal, and one of class length 2 whose normaliser has order 36. The last is H; [2] restrict their search to "non-Abelian groups and their non-normal subgroups", so it is theirs as well. Then $m = [G{:}H] = 24$, $n = 48$, $|N| = 36$ and $[N{:}H] = 12$. Because the two conjugates of H are distinct subgroups of prime order, $\mathrm{Core}_G(H) = 1$, so by [2, Prop. II.3] L is faithful — 72 distinct left actions — while R factors through N/H — 12 distinct right actions. This is also what the printed supports of [2] look like: for this group their a is $[1, 16, 57, 58]$, indices into a list of 72, and their b is $[1, 2, 3, 9]$, indices into a list of 12.

Accordingly a is a sum of $w_a = 4$ distinct elements of G and b a sum of $w_b = 4$ elements of N lying in four distinct cosets of H; the latter is the same as a weight-4 element of $\mathbb{F}_2[N/H]$, and we index the 12 cosets $0, \dots, 11$ in GAP's $\texttt{RightCosets}(N, H)$ order, the identity coset first. Elements of G are indexed $0, \dots, 71$ in GAP 4.11.1's $\texttt{Elements}(G)$ order. The 84 permutations of the 24 cosets that these actions produce are the only input data of the whole development; they are emitted by a GAP script that ships with it.

By [2, Lem. IV.1], $Q^H_G(a, b)$ is equivalent to $Q^H_G(a * g_a, g_b * b)$ for $g_a \in G$ and $g_b \in N$, so every code of the family is equivalent to one whose a contains 1 and whose b contains the identity coset. We call such a pair *normalised*, write $\mathcal{F}$ for the set of them, and record $|\mathcal{F}| = \binom{71}{3}\binom{11}{3} = 9\,430\,575$. Normalisation is a covering, not a transversal: it divides the $\binom{72}{4}\binom{12}{4}$ pairs by the factor $(72/4)(12/4) = 54$, and equivalent normalised pairs remain. Independently of [2, Lem. IV.1] one can see directly from (2) that both ranks are invariant under all four translations, using that $\operatorname{im} R(b)$ is $L(G)$-invariant and $\operatorname{im} L(a)$ is $R(N)$-invariant — both consequences of the two actions commuting.

The model is checked, not assumed. Everything below is a statement about the stored table of 84 permutations, so that table is checked first.

Proposition 1. *All 84 stored maps are permutations of the 24 cosets, and the identity occupies the first slot of each of the two blocks. For all $72 \cdot 12$ pairs $(g, h) \in G \times N/H$, $L(g)R(h) = R(h)L(g)$; consequently $H_X H_Z^{\mathsf{T}} = 0$ and every member of the family is a CSS code. The left action of G on the 24 cosets is transitive, the right action of N has exactly two orbits, and the two together are transitive.*

The commuting relation is [2, Prop. II.2] evaluated on every pair rather than argued, and the two orbit counts are what make the submodule counts of Theorem 6 exact. The permutation table is regenerated from GAP by the script mentioned above and agrees with the stored copy byte for byte.

Remark 2. Section VII of [1] describes its family with "$a, b \in \mathbb{F}_2[G/H]$ sums of w_a, w_b coset permutations", which is less specific than [2, Construction 1]; we follow [2], under which a ranges over $\mathbb{F}_2[G]$ and b over $\mathbb{F}_2[N]$, as the printed supports of [2] for this group require. The printed supports of [1] require it too: the seven pairs listed in its Table IX have a-entries as large as 72 and b-entries no larger than 11, so there as well a is indexed in the 72 elements of G and b in the 12 cosets of H in N. The narrower reading in which a too is drawn from N/H is not the family in question: see Remark 14.

3. The census

Theorem 3. *Over the* $9\,430\,575$ *normalised support pairs of the family* (1), *the joint distribution of* $(\operatorname{rank} H_X, \operatorname{rank} H_Z)$ *is Table 1: exactly* 29 *cells are occupied, and the cell counts sum to* $9\,430\,575$*. Consequently:*

(1) $157\,464$ *normalised pairs —* 1.67% *— have* $\operatorname{rank} H_X \neq \operatorname{rank} H_Z$*, split exactly* $78\,732$ *with* $\operatorname{rank} H_Z > \operatorname{rank} H_X$ *and* $78\,732$ *with* $\operatorname{rank} H_X > \operatorname{rank} H_Z$*;*
(2) *the defect is not a* $0/1$ *invariant:* 24 *pairs have* $|\operatorname{rank} H_X - \operatorname{rank} H_Z| = 3$*;*
(3) $k = 48 - \operatorname{rank} H_X - \operatorname{rank} H_Z$ *takes exactly* 23 *distinct values, namely* $2, 4, 6, 8, 9, 10, 12, 13, 14, 16, 17, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 36$*;*
(4) $232\,760$ *normalised pairs have* $k = 10$ *and* $142\,176$ *have* $k = 9$.

Table 1. The joint rank census of the family (1) over all $9\,430\,575$ normalised support pairs. Cells in bold have a rank defect.

rank H_X	rank H_Z	k	pairs	rank H_X	rank H_Z	k	pairs
6	6	36	5	**15**	**16**	**17**	**3 264**
8	8	32	160	**16**	**15**	**17**	**3 264**
9	9	30	6	16	16	16	94 592
9	**12**	**27**	**12**	17	17	14	45 824
10	10	28	524	**17**	**18**	**13**	**4 032**
11	11	26	48	**18**	**17**	**13**	**4 032**
11	**12**	**25**	**24**	18	18	12	251 040
12	**9**	**27**	**12**	19	19	10	232 760
12	**11**	**25**	**24**	**19**	**20**	**9**	**71 088**
12	12	24	4 776	**20**	**19**	**9**	**71 088**
13	13	22	760	20	20	8	1 669 168
13	**14**	**21**	**312**	21	21	6	1 777 136
14	**13**	**21**	**312**	22	22	4	4 076 912
14	14	20	11 312	23	23	2	1 099 008
15	15	18	9 080				

Proof sketch. Exhaustive computation. For each of the $\binom{11}{3} = 165$ normalised b and each of the $\binom{71}{3} = 57\,155$ normalised a, the two 24×48 check matrices are built from the stored permutation table as arrays of 48-bit masks and their $\mathbb{F}_2$ ranks are computed by Gaussian elimination on the rows; the pair of ranks indexes a histogram. No equivalence reduction is used beyond the normalisation, and the histogram's total is checked against $|\mathcal{F}|$, so that no pair is lost or counted twice. Items (1)–(4) are read off the tabulated cells. The same census was produced first by an independent C program and agrees cell by cell; in the proof assistant it costs about 122 CPU-seconds. $\square$

The exact symmetry of the split in item (1) is forced by (2), since $\mathcal{F}$ is closed under $(a, b) \mapsto (a^\dagger, b^\dagger)$; the computation confirms it rather than uses it. Item (3) is already incompatible with the conjecture quoted in Section 1, which allows $k \in \{9, 10\}$ only: those two values account for $(232\,760 + 142\,176)/9\,430\,575 = 3.98\%$ of the family.

Remark 4. We could not reconcile the "123 equivalence classes" of [1, §VII] with the family as (1) defines it. The census assigns $k \notin \{9, 10\}$ to more than 96% of $\mathcal{F}$, whereas the proof of the rank-degeneracy theorem in [1] describes all 123 classes as having $k = 9$ (seven of them) or $k = 10$ (the remaining 116). Whatever set was enumerated there, its dimension spectrum is not that of $\mathcal{F}$. We claim nothing further about it: our results are statements about $\mathcal{F}$, and the classification of $\mathcal{F}$ is not attempted here.

4. The module criterion cannot be satisfied

Conjecture 17 of [1] predicts the sign of the rank defect from a codimension-one submodule $U \subseteq \mathbb{F}_2[G/H]$ with $\langle a\rangle \subseteq U$ and $\langle b\rangle \not\subseteq U$. Its second clause is empty in this family, for a reason that involves neither G nor the defect.

Lemma 5. *Let P be a group of permutations of a finite set X and $U \subseteq \mathbb{F}_2^X$ a P-invariant subspace of codimension 1. Then $U = \ker\varphi$ for a nonzero linear functional φ that is constant on the P-orbits; that is, φ is a sum of orbit indicator vectors, and $\varphi(v)$ is the sum of the parities of v on those orbits. Consequently every $v \in \mathbb{F}_2^X$ that is supported in a single P-orbit and has even weight lies in U.*

Proof. $\mathbb{F}_2^X/U$ is one-dimensional over $\mathbb{F}_2$, hence carries the trivial P-action, so the quotient map is a nonzero P-invariant functional φ with $U = \ker\varphi$. Writing $\varphi(v) = \sum_{x\in X}\varphi_x v_x$, invariance says $\varphi_{p(x)} = \varphi_x$ for every $p \in P$, i.e. φ is constant on orbits; hence $\varphi = \sum_O \varepsilon_O \mathbf{1}_O$ with $\varepsilon_O \in \mathbb{F}_2$ and $\varphi(v) = \sum_O \varepsilon_O |\operatorname{supp} v \cap O| \bmod 2$. □

Now b is a sum of four elements of N lying in four distinct cosets of H, so its image vector $v_b = \sum_{h\in b} e_{hH}$ has weight exactly 4 and is supported in the $R(N)$-orbit of the identity coset — one orbit, by Proposition 1. The same is true of every column of $R(b)$: the column at xH is $\{xhH : h \in b\}$, four distinct cosets inside the $R(N)$-orbit of xH. Under the left action of G there is only one orbit at all, and even weight again gives $\varphi(v) = 0$. So Lemma 5 applies in each reading, and $\langle b\rangle \subseteq U$ always. The computation verifies this where it lives, without using the lemma.

Theorem 6. *For the family* (1)*:*

1. *Of the 2^{24} linear functionals on $\mathbb{F}_2[G/H]$, exactly 2 are invariant under the left G-action, exactly 4 under the right N-action, and exactly 2 under both. Equivalently, $\mathbb{F}_2[G/H]$ has exactly one codimension-one G-submodule, exactly three codimension-one N-submodules, and exactly one codimension-one sub-bimodule.*
2. *For every one of the 495 weight-4 supports $b \subseteq N/H$ and every one of those submodules U: the image vector v_b lies in U, and so does every column of $R(b)$. Hence $\langle b\rangle \subseteq U$ for every codimension-one submodule U, under either reading of $\langle b\rangle$ — the submodule generated by v_b, or $\operatorname{im} R(b)$ — and under each of the three module structures.*
3. *The condition on a is not vacuous: there is a weight-4 support $a \subseteq G$ and a codimension-one N-submodule U with $v_a \notin U$. So $\langle a\rangle \subseteq U$ is a genuine restriction on a, while $\langle b\rangle \not\subseteq U$ is met by no b at all.*

Proof sketch. Item (1) is a brute-force enumeration of all $2^{24} = 16\,777\,216$ functionals, testing each against every one of the 72, respectively 12, respectively 84 stored permutations; the counts $2, 4, 2$ are returned, and a codimension-one submodule is the kernel of one of the nonzero ones. Item (2) runs over all $\binom{12}{4} = 495$ supports b — not only the normalised ones — and, for each, over all nonzero invariant functionals of each of the three actions, checking that the functional annihilates v_b and every column of $R(b)$. Item (3) exhibits a support a and an N-invariant functional not annihilating v_a; the search over $\binom{72}{4}$ supports stops at the first witness. Total cost about 94 CPU-seconds. No orbit argument enters the computation: the invariant functionals are enumerated, not derived. □

Corollary 7. *Conjecture 17 of* [1] *is false for the family it is about. Its right-hand side never holds, by Theorem 6(2), so it asserts that no member of the family has* $\operatorname{rank} H_Z > \operatorname{rank} H_X$*; but* 78 732 *normalised pairs do, by Theorem 3(1). Its closing clause fails as well: it confines* k *to* $\{9, 10\}$*, and* k *takes* 23 *values, by Theorem 3(3).*

Remark 8. The three readings are not equally generous, and the criterion fails in all of them. In the G-reading there is a single codimension-one submodule, the even-weight subspace (Theorem 6(1) with Proposition 1: the only nonzero invariant functional of a transitive action is the all-ones one). There the first clause holds for every a — v_a is a sum of four coset vectors, so it has even weight whether or not they collide — and the second for no b. The N-reading gives the criterion the most room, three submodules and a first clause that really constrains a, and only the second clause is impossible. Nothing in the argument uses which group G is: it uses that w_b is even and that b lies in one orbit, so it applies verbatim to any coset-2BGA family with even w_b.

Remark 9. "$\langle b\rangle$" is unambiguous here. The G-submodule generated by v_b is $\operatorname{span}\{L(g)v_b\} = \operatorname{span}\{R(b)e_{gH}\} = \operatorname{im} R(b)$, using that L and R commute (Proposition 1) and that G is transitive on the cosets; so the vector reading and the image reading of $\langle b\rangle$ agree. Theorem 6(2) certifies both in any case.

5. Witnesses

A refutation by counting invites the question of what a violating code looks like, so we name four. Supports are given in the indexing of Section 2: a as a 4-subset of $\{0, \dots, 71\}$ and b as a 4-subset of $\{0, \dots, 11\}$.

Theorem 10. *Each of the following support pairs lies in* $\mathcal{F}$*, and the listed values of* $(\operatorname{rank} H_X, \operatorname{rank} H_Z, k, d)$ *are exact, the distances included.*

a	b	$\operatorname{rank} H_X$	$\operatorname{rank} H_Z$	k	d	*row weights* 8
$\{0, 1, 2, 37\}$	$\{0, 1, 2, 4\}$	19	20	9	2	*yes*
$\{0, 1, 2, 18\}$	$\{0, 1, 2, 4\}$	20	19	9	2	—
$\{0, 1, 2, 19\}$	$\{0, 1, 2, 4\}$	9	12	27	2	*yes*
$\{0, 6, 7, 46\}$	$\{0, 1, 2, 8\}$	19	20	9	6	*yes*

The last column records that every row of H_X *has weight* $w_a + w_b = 8$*, so that pair is a weight-*8 *member of the family* (1) *in the sense of* [1, §VII]*; it is verified for the three pairs marked, and not asserted for the second. The first pair also satisfies* $H_X H_Z^{\mathsf{T}} = 0$ *entry by entry.*

The first pair is the direct counterexample: it realises the conjecture's left-hand side, $\operatorname{rank} H_Z > \operatorname{rank} H_X$, while the right-hand side is unsatisfiable (Theorem 6), and its distance is 2, not the 5 that the conjecture asserts "whenever this happens". The second is its mirror, with the ranks exchanged. The third has rank defect 3 and $k = 27$. The fourth has a rank defect and distance exactly 6, against "rank loss is tied to distance exactly 5" in the proof of the rank-degeneracy theorem of [1]; Theorem 11 shows it is one of 1536 such normalised pairs.

Proof sketch. Each line is a direct computation from the definitions on one support pair: the check matrices are built from the stored permutations, the ranks are computed by Gaussian elimination, and the distance by information-set enumeration. For the latter, a reduced row-echelon basis of $\ker H_Z$ is computed and every combination of at most 7 basis vectors is enumerated: a codeword of weight w has at most w nonzero coordinates in the information set of such a basis, so this finds every codeword of weight at most 7, and the least weight found outside the row space of H_X is d_X; d_Z symmetrically, and $d = \min(d_X, d_Z)$. Each value above is therefore an exact distance and not an upper bound — the routine returns the sentinel 8 when no logical operator of weight at most 7 exists, and Proposition 13(3) checks that this sentinel behaves as described. □

6. Distances over the rank-defect stratum

The conjecture asserts $d = 5$ for every code with a rank defect, and the proof of the rank-degeneracy theorem asserts that every $d = 6$ code of the family has full ranks $19 + 19$. Both sentences are about the stratum

$$\mathcal{S} = \{(a, b) \in \mathcal{F} : \{\operatorname{rank} H_X, \operatorname{rank} H_Z\} = \{19, 20\}\}, \qquad |\mathcal{S}| = 142\,176,$$

which by Theorem 3 is exactly the set of normalised pairs with a rank defect and $k = 9$. We compute the distance of every one of its members.

Theorem 11. *Of the* 142 176 *normalised support pairs in* $\mathcal{S}$*, exactly* 126 048 *have* $d \le 4$*, exactly* 14 592 *have* $d = 5$*, and exactly* 1536 *have* $d \ge 6$*; the three counts sum to* $|\mathcal{S}|$*. Split over six ranges of the* 165 *normalised supports* b*, taken in lexicographic order, the counts are*

b	$d \le 4$	$d = 5$	$d \ge 6$	b	$d \le 4$	$d = 5$	$d \ge 6$
$[0, 28)$	23 904	2304	768	$[84, 112)$	3648	0	0
$[28, 56)$	22 104	2496	192	$[112, 140)$	23 328	3456	192
$[56, 84)$	22 872	1728	192	$[140, 165)$	30 192	4608	192

So 88.7% of the pairs in $\mathcal{S}$ have $d \le 4$ and only 10.3% have $d = 5$: the conjecture's "whenever this happens the code has $k = 9$ and $d = 5$" fails on nine codes in ten, in addition to failing on the 15 288 normalised pairs that have a rank defect and $k \ne 9$ (Table 1). And 1536 normalised pairs have a rank defect together with $d \ge 6$, against the closing clause of the rank-degeneracy theorem.

Proof sketch. Exhaustive computation over $\mathcal{F}$ with a filter: for every normalised pair the two ranks are computed as in Theorem 3, and when $k = 9$ — equivalently $(a, b) \in \mathcal{S}$ — the distance is computed by the information-set enumeration of Section 5 with the search depth capped at 5. The three classes are therefore "$d \le 4$", "$d = 5$" and "no logical operator of weight at most 5 exists", the last being the class we report as $d \ge 6$; it is a genuine lower bound and we make no claim that those 1536 codes have $d = 6$ exactly, although the witness of Theorem 10 is one of them and does. The sweep was split into six chunks by ranges of the 165 normalised b, which partition them; the six chunk statements are proved separately and added. Cost about 1.7 CPU-hours in the proof assistant and 160 CPU-seconds for an independent C implementation, which agrees chunk by chunk. □

7. Reproduced from the literature

Nothing in this section is new. It records the part of the surrounding literature that the same development verifies, because the value of a refutation depends on the refuting model being the right one.

Proposition 12. *The family* (1) *contains a* $[[48, 10, 6]]$ *code with all* H_X *row weights equal to* 8*: for* $a = \{0, 1, 14, 24\}$*,* $b = \{0, 1, 2, 8\}$ *one has* $\operatorname{rank} H_X = \operatorname{rank} H_Z = 19$*,* $k = 10$*, and* $d_X = d_Z = 6$ *exactly. That is the parameter set* [2] *report for this group, obtained here from their construction rather than read off their table. The printed support indices of* [2] *do not transfer to our indexing: their a for that code, read in GAP 4.11.1's* `Elements`(G) *order, together with their own b, gives* $\operatorname{rank} H_X = \operatorname{rank} H_Z = 20$*,* $k = 8$*,* $d = 4$*, and irregular row weights.*

The relevant row of [2] is

$$48 \quad 10 \quad 6 \quad C_3 \times ((C_6 \times C_2) \rtimes C_2) \quad C_3 \quad [1, 16, 57, 58] \quad [1, 2, 3, 9] \quad 72 \quad 30 \quad 9,$$

in the weight-8 block of their Table VI of additional code examples, whose caption states "Distances reported with a $\leq$ symbol represent upper bounds obtained using QDistRnd with 10^6 iterations. All other distances are exact." The b-half of the dictionary transfers verbatim — their $[1, 2, 3, 9]$ is our $\{0, 1, 2, 8\}$, so the `RightCosets`(N, H) order used here agrees with the `LeftCosets`$(N_G(H), H)$ order of [2] — while the a-half does not. Table VI's own caption fixes no index convention; the one it inherits is that of their Table II, whose caption makes the last three entries of the row the pair (ℓ, m) of `SmallGroup`(ℓ, m) together with an index s into the list of *non-normal* subgroups of G — so their H here is a non-normal C_3 — and says that the printed group-algebra integers "correspond to the indices of the respective coset representatives in the lists `LeftCosets(G, Core(G,H))` and `LeftCosets(Normalizer(G,H), H)`". Here $\operatorname{Core}_G(H) = 1$, so the first of those lists is a list of the 72 elements of G in an order we could not reproduce under GAP 4.11.1; reading the printed indices in `Elements`(G) order instead gives the $[[48, 8, 4]]$ code of Proposition 12. The construction is unambiguous and nothing above depends on the dictionary; only the reproduction of a printed example does.

We note, without drawing any conclusion from it, that the GAP version is reported inconsistently in [2]: the captions of their Tables II and IV name Version 4.14.0 — the first for the subgroup list that fixes the column s, the second for the `Elements`(G) ordering used there — while their bibliography entry for GAP names Version 4.13.0. Which of the two produced the coset lists of Table II is therefore not determined by the paper, and we have not asked.

Proposition 13. *The following controls hold for the family* (1)*.*

1. *Two claims that are too large are refuted: "*$\operatorname{rank} H_X = \operatorname{rank} H_Z$ *for every member of the family" and "the rank defect is at most* 1*" both fail, on the first and third witnesses of Theorem 10.*
2. *Two claims that are too small are refuted: "no member has* $d \geq 6$*" and "every member has* $k \leq 10$*" both fail.*
3. *The distance routine does not truncate: for the code of Proposition 12 it returns the sentinel* 5 *at search depth* 4 *— no logical operator of weight at most* 4 *— and the value* 6 *at depths* 6 *and* 7 *alike, so a reported* 6 *is a distance and not a cap.*

(4) *The hypothesis "all H_X row weights are 8" is not vacuous: it holds for the first witness of Theorem 10 and fails for the support pair carrying the printed indices of* [2].

Item (1) deserves a word: those two statements are exactly what the conjecture's unsatisfiable criterion would impose on the whole family, so refuting them is Corollary 7 read from the other side, and it is refuted by a single explicit code rather than by a census.

Remark 14 (computations outside the formal development). Three computations were run only in C and are *not* machine-checked; nothing above depends on them, and we record them for orientation. (i) Over all 232 760 normalised pairs with $k = 10$, no code has $d = 5$ — which is the corollary [1] draws from its rank-degeneracy theorem, that no $[[48, 10, 5]]$ code lies in this family — and 3456 have $d \geq 6$. (ii) In the narrower reading of the family discussed in Remark 2, with a drawn from N/H as well as b, there are $\binom{11}{3}^2 = 27\,225$ normalised pairs, none of which has a rank defect and none of which has $k \in \{9, 10\}$; so that reading is not the set [1, §VII] enumerated either. (iii) The distances of the remaining $9.29 \cdot 10^6$ normalised pairs, with $k \notin \{9, 10\}$, were priced at about 18 CPU-minutes and not run.

8. Verification

Every numerical statement above — the census and each of its readings, the three functional counts and the two submodule sweeps, each witness with its ranks, dimension and distance, each of the six distance chunks and their sum, and every control — has been formalised and checked in Lean 4 [7]; repository reference to be added at submission. The development is self-contained: it defines the coset action as an array of 84 permutations of $\{0, \ldots, 23\}$, the $\mathbb{F}_2$ linear algebra on 48-bit masks (rank, kernel basis, row span, minimum logical weight) and the sweeps directly on `Nat`/`Array UInt64`, and imports no external library, in particular no object of Mathlib, so that the enumerations can be evaluated by the compiler. The sweeps are discharged by compiled evaluation (`native_decide`), which adds one evaluation axiom per declaration; an audit of the axiom set of every statement cited above found nothing beyond `propext`, `Classical.choice`, `Quot.sound` and those evaluation axioms — in particular no incomplete proof. The arithmetic that adds the six chunks of Theorem 11 uses no evaluation axiom at all. Three ingredients are by hand and are marked where they occur: Lemma 5, the identities (2), and the translation equivalence quoted from [2, Lem. IV.1]; each of them consumes only finite data that is itself checked, and none is needed for the refutation, which rests on Theorem 6(2) and Theorem 3(1) alone. Independent C implementations of the census, the distance sweep and the witnesses agree with the checked values throughout, and the permutation table is regenerated from GAP and compared byte for byte.

9. Open questions

(1) *What is the right criterion?* By (2),

$$\operatorname{rank} H_Z - \operatorname{rank} H_X = \dim\bigl(\operatorname{im} L(a) \cap \operatorname{im} R(b)\bigr) - \dim\bigl(\operatorname{im} L(a^\dagger) \cap \operatorname{im} R(b^\dagger)\bigr),$$

so the rank defect measures the failure of the intersection dimension to be invariant under inversion of the supports. Since $\operatorname{im} L(a)$ is an N-submodule and $\operatorname{im} R(b)$ a G-submodule, a module-theoretic criterion for the defect should be a statement about that intersection. Finding one — and one that survives the parity obstruction of Lemma 5 — is the question this family inherits from [1].

(2) *The rest of the family.* The distance distribution is known here for the stratum $\mathcal{S}$ only. The $k = 10$ stratum has been swept outside the formal development (Remark 14); the remaining $9.29 \cdot 10^6$ normalised pairs, where k ranges over 21 further values, are unmeasured.

(3) *Is the defect coset-theoretic or non-abelian?* [1, §VII] says the defect "vanishes identically in the cyclic case and can be nonzero for nontrivial coset actions", which locates it in the coset construction. The two *normal* subgroups of order 3 of the same G give ordinary 2BGA codes over non-abelian groups of order 24, a setting the coset construction has left behind but non-commutativity has not. A census of those two families is cheap, is not attempted here, and would separate the two possible sources of the phenomenon.

(4) *The announced census.* If the companion paper promised in [1, §VII] appears, reconstructing which set its 123 classes partition would settle whether the two censuses are about the same family (Remark 4).

References

[1] L. Lu, G. Guo, Y. Liu and R. Yang, *Quantum Bicycle LDPC Codes with High kd^2/n from Divisor-Driven Search*, arXiv:2608.09115v1 (10 August 2026). All quotations, and all section, equation, theorem and table numbers, are as printed in the typeset v1 PDF, consulted 30 August 2026, on which date v1 was the only version.

[2] A. Aydin, I. Tamo and A. Barg, *Breaking the bicycle frame: Coset-based quantum LDPC codes*, arXiv:2606.17268v1 (15 June 2026). The construction, proposition, lemma and table numbers cited here are as printed in the typeset v1 PDF, consulted 30 August 2026, on which date v1 was the only version.

[3] H.-K. Lin and L. P. Pryadko, *Quantum two-block group algebra codes*, Phys. Rev. A **109** (2024), no. 2, 022407.

[4] A. A. Kovalev and L. P. Pryadko, *Quantum Kronecker sum-product low-density parity-check codes with finite rate*, Phys. Rev. A **88** (2013), no. 1, 012311.

[5] D. J. C. MacKay, G. Mitchison and P. L. McFadden, *Sparse-graph codes for quantum error correction*, IEEE Trans. Inform. Theory **50** (2004), no. 10, 2315–2330.

[6] The GAP Group, *GAP — Groups, Algorithms, and Programming*, `https://www.gap-system.org`. The group data used here was generated with Version 4.11.1. [2] name Version 4.14.0 in the captions of their Tables II and IV and Version 4.13.0 in their bibliography entry for GAP.

[7] L. de Moura and S. Ullrich, *The Lean 4 Theorem Prover and Programming Language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science, Springer, 2021, pp. 625–635.