

No six-qubit distance-three code admits a transversal T gate

Yuxuan Zhang

Institute of Physics, École Polytechnique Fédérale de Lausanne (EPFL)
CH-1015 Lausanne, Switzerland

Department of Physics, Princeton University
Princeton, New Jersey 08544, USA

Version 1.0 — 28 September 2026

Abstract

We give a computer-assisted proof that no two-dimensional six-qubit code detecting every Pauli operator of weight at most two admits an exact logical T gate implemented by a product of single-qubit unitaries. The local factors may differ, their eigenbases and angles are unrestricted, and degenerate codes are included. The first step replaces any proposed gate by one whose local eigenvalue ratios are 64th roots of unity, without changing its action on the code. Exact moment separators and two off-diagonal error-detection contradictions then exclude the resulting finite cases. The certificate covers all 119,877,472 sorted order-64 angle vectors, using reductions that preserve the logical gate. Combined with the previously published seven-qubit construction, the result makes seven qubits the minimum block length under these assumptions. The proof, executable certificate, and independent coverage controls are supplied for examination.

1 Question and main result

Transversal gates limit the spread of errors between physical qubits. For a small code, however, specifying a desired logical gate need not leave any compatible error-correcting subspace. The six-qubit transversal- T question is a particularly concrete instance of this tension.

Let $\mathcal{P}_6 = \{I, X, Y, Z\}^{\otimes 6}$ be the phase-free Hermitian Pauli basis. A rank-two code detecting every error of weight at most two has an encoding isometry $V : \mathbb{C}^2 \rightarrow (\mathbb{C}^2)^{\otimes 6}$ satisfying

$$V^\dagger V = I_2, \quad V^\dagger E V = c_E I_2 \quad (E \in \mathcal{P}_6, \text{wt}(E) \leq 2). \quad (1)$$

These are the relevant Knill–Laflamme detection conditions [1]. They allow degeneracy. The desired transversal realization is

$$\left(\bigotimes_{j=0}^5 U_j \right) V = e^{i\phi} V T, \quad T = \text{diag}(1, e^{i\pi/4}), \quad U_j \in U(2). \quad (2)$$

No ancillary qubits, measurements, code switching, or additional transversal logical gates are part of this realization.

Zhang, Wu, Huang and Zeng introduced a subset-sum and linear-programming method for finding codes with prescribed diagonal transversal gates [2, Section 6.1]. Their Table 2 records numerical non-detection of the six-qubit cyclic-order-16 target, while Section 6.3.1 gives exact seven-qubit

examples with transversal T . He, Lu and Zeng subsequently classified twelve surviving seven-qubit candidates within a complementary binary-dihedral ansatz [3, Section IV and Appendices F–G]. Neither restricted classification nor numerical non-detection supplies an exclusion for arbitrary six-qubit codes and arbitrary local factors.

The QIQCOP question asks whether a genuinely nonadditive code can satisfy (1)–(2) [4]. We prove a stronger exclusion.

Theorem 1. *There is no isometry $V : \mathbb{C}^2 \rightarrow (\mathbb{C}^2)^{\otimes 6}$ and no $U_0, \dots, U_5 \in U(2)$ satisfying (1) and (2). In particular, the genuinely nonadditive code requested in QIQCOP problem `op_ddfbbe7ca0ead0c8` does not exist.*

The argument uses the published residue-support and moment-filter strategy. Its completeness comes from an arbitrary-angle reduction and an exhaustive exact exclusion, including the cases that pass the diagonal moment filter. No complementary relation between logical codewords is imposed.

2 Replacing arbitrary angles by a finite set

Write $a = V|0\rangle$ and $b = V|1\rangle$. A product change of basis preserves detection of every operator supported on at most two qubits, because the Paulis span each such operator space. Diagonalize the six local factors and remove their scalar phases. They become $\text{diag}(1, e^{2\pi i \theta_j})$, with arbitrary real θ_j .

Choose an occupied computational string in a and move it to 0^6 by local X operators. This changes signs of some angles and a global phase, but leaves the ratio of logical eigenvalues equal to $e^{2\pi i/8}$. After normalizing the first eigenvalue to one, every occupied string obeys

$$x \cdot \theta = \ell_x + \frac{\eta_x}{8}, \quad \ell_x \in \mathbb{Z}, \quad \eta_x = \begin{cases} 0 & x \in \text{supp}(a), \\ 1 & x \in \text{supp}(b). \end{cases} \quad (3)$$

The supports are disjoint because their eigenvalues differ.

Lemma 1. *If (1)–(2) has a solution, an equivalent code has the same logical gate implemented by*

$$D_k = \bigotimes_{j=0}^5 \text{diag}(1, e^{2\pi i k_j/64}), \quad 0 \leq k_0 \leq \dots \leq k_5 < 64, \quad (4)$$

with $\text{supp}(a) \subseteq \{x : k \cdot x = 0 \pmod{64}\}$ and $\text{supp}(b) \subseteq \{x : k \cdot x = 8 \pmod{64}\}$.

Proof. Form the binary matrix M whose rows are the occupied strings, and the vector h whose entries are the right-hand sides of (3). Then $M\theta = h$. Let $r = \text{rank } M$, so $1 \leq r \leq 6$, and choose r independent rows I and columns J such that $C = M[I, J]$ is invertible. Set $\theta'_J = C^{-1}h_I$ and set the other coordinates to zero. If a row of M is λM_I , consistency of the original real system gives the corresponding entry of h as λh_I . Thus $M\theta' = h$: all equations, including their fixed winding integers, are preserved. If $\Delta = |\det C|$, Cramer's rule gives $\theta'_j \in (8\Delta)^{-1}\mathbb{Z}$.

Border the matrix $\mathbf{1} - 2C$ by a first row and column of ones. The resulting $(r+1) \times (r+1)$ matrix H has entries in $\{\pm 1\}$ and $|\det H| = 2^r \Delta$. Hadamard's inequality gives

$$4^r \Delta^2 \leq (r+1)^{r+1} < 256 4^r \quad (1 \leq r \leq 6). \quad (5)$$

Consequently $\Delta < 16$. Write $\Delta = 2^v m$ with m odd; then $v \leq 3$. Choose an odd integer t with $mt = 1 \pmod{8}$ and set $q = mt$. Every $q\theta'_j$ has denominator dividing 2^{v+3} , hence dividing 64. Moreover $q = 1 \pmod{8}$, so raising the replacement gate to the q th power preserves its logical T

action. Reducing the exponents modulo 64 and permuting physical qubits gives (4). The code is unchanged by rational replacement and powering; the earlier local basis changes and permutations preserve its error-detection property. $\square$

There are exactly $\binom{69}{6} = 119,877,472$ possible sorted vectors in (4). The finite reduction does not require the original local angles to be rational.

3 Moment exclusions and denominator reduction

For $m \in \{8, 16, 32, 64\}$ define

$$A_k = \{x \in \{0, 1\}^6 : k \cdot x = 0 \pmod{m}\}, \quad B_k = \{x : k \cdot x = m/8 \pmod{m}\}. \quad (6)$$

The bit convention throughout is $x = \sum_{j=0}^5 2^j x_j$. The codewords may occupy proper subsets of these allowed supports.

Let $F(x)$ contain the constant 1, the six coordinates x_j , and the fifteen products $x_i x_j$ with $i < j$. From $x_j = (I - Z_j)/2$ and $x_i x_j = (I - Z_i - Z_j + Z_i Z_j)/4$, (1) implies

$$\sum_{x \in A_k} |a_x|^2 F(x) = \sum_{y \in B_k} |b_y|^2 F(y). \quad (7)$$

An integer vector c with $c \cdot F > 0$ on all of A_k and $c \cdot F < 0$ on all of B_k contradicts this equality. Checking the entire allowed supports makes the exclusion valid even when some amplitudes vanish.

Lemma 2. *If either of the disjoint allowed supports has at most two vertices, (7) cannot hold for normalized probability distributions.*

Proof. An empty support cannot contain a normalized codeword. The polynomial $Q(x) = \|x - u\|^2$ isolates a singleton $\{u\}$. For two distinct vertices u, v , put $d = v - u$ and

$$Q(x) = \|d\|^2 \|x - u\|^2 - ((x - u) \cdot d)^2. \quad (8)$$

It is nonnegative, has degree at most two, and vanishes exactly on the line $u + \mathbb{R}d$. A Boolean point on that line must have parameter 0 or 1, as is seen from any coordinate where u and v differ. Thus Q is zero on $\{u, v\}$ and strictly positive at every other Boolean vertex. Its expectations on two disjoint normalized supports cannot agree. Interchanging the supports gives the other case. $\square$

Lemma 3. *Suppose 16 divides m and at most two coefficients k_j are odd. A code supported as in (6) with logical T also admits the same logical gate with local ratios of order dividing $m/2$.*

Proof. Both residues in (6) are even. If exactly one coefficient is odd, its bit is zero on both supports; replace that coefficient by zero. If exactly two, say k_u, k_v , are odd, their bits agree on both supports. Replacing the two coefficients by $0, k_u + k_v \pmod{m}$ therefore preserves every phase on the code. All coefficients are now even. Divide them and the modulus by two. This leaves the physical phases on the code, and hence the exact logical T , unchanged. The all-even case requires only the final division. $\square$

This argument replaces the gate on its code space. It does not assert that the original gate has smaller order on the full physical space.

4 The order-eight exceptions

The certificate enumerates all $\binom{13}{6} = 1716$ sorted vectors in $\{0, \dots, 7\}^6$ and regenerates the sets in (6). There are 156 empty- B_k cases, 1551 cases excluded by exact integer moment separators, and nine remaining vectors. These nine pass to one of two support pairs by the local maps in Table 1. The compressed separator table is part of the executable certificate; every integer sign is checked after decompression.

k	Bit permutation	XOR mask	Pair
(1, 1, 3, 3, 3, 6)	(2, 3, 4, 5, 0, 1)	8	I
(1, 2, 2, 3, 4, 5)	(4, 3, 5, 1, 2, 0)	4	II
(1, 2, 5, 5, 5, 7)	(2, 3, 4, 1, 0, 5)	39	I
(1, 3, 4, 5, 6, 6)	(2, 1, 3, 4, 5, 0)	29	II
(2, 2, 4, 5, 5, 7)	(2, 3, 4, 0, 1, 5)	39	II
(2, 3, 3, 3, 7, 7)	(1, 2, 3, 0, 4, 5)	48	I
(2, 3, 3, 4, 6, 7)	(3, 1, 2, 0, 4, 5)	48	II
(3, 5, 5, 6, 7, 7)	(0, 1, 2, 3, 4, 5)	62	I
(4, 5, 5, 6, 6, 7)	(0, 1, 2, 3, 4, 5)	62	II

Table 1: For permutation π , first set $y_j = x_{\pi(j)}$, then XOR the displayed mask. Both ordered support sets map exactly to the indicated pair. No logical swap is needed.

4.1 Pair I

The supports are

$$A = \{8, 23, 39, 48, 59, 61, 62\},$$

$$B = \{1, 2, 4, 15, 24, 40, 55\}.$$

In increasing support order, the diagonal equations uniquely force

$$(|a_x|^2)_{x \in A} = \frac{1}{16}(5, 3, 3, 2, 1, 1, 1),$$

$$(|b_y|^2)_{y \in B} = \frac{1}{16}(1, 1, 1, 2, 3, 3, 5).$$

For completeness, the rational system has one normalization row for each support and, for each one- or two-element set S of bit positions, the row $(((-1)^{\sum_{j \in S} x_j})_{x \in A}, -((-1)^{\sum_{j \in S} y_j})_{y \in B})$. Its rank is 14; substituting the displayed vector verifies the unique solution exactly.

Consider $O = X_4(I + Z_0)/2$. It is a linear combination of detectable operators, but its only nonzero matrix element between these two supports is $\langle 8|O|24 \rangle = 1$. Therefore

$$0 = \langle a|O|b \rangle = \overline{a_8}b_{24}. \quad (9)$$

This contradicts $|a_8|^2 = 5/16$ and $|b_{24}|^2 = 3/16$.

4.2 Pair II

Here

$$A = \{2, 4, 27, 29, 39, 40, 48, 62\},$$

$$B = \{1, 15, 23, 24, 34, 36, 59, 61\}.$$

The analogous rational moment matrix has rank 15. Its entire affine solution space, in increasing support order, is

$$\begin{aligned} p &= (t, \frac{3}{16} - t, \frac{1}{4} - t, t + \frac{1}{16}, \frac{3}{16}, \frac{1}{8}, \frac{1}{8}, \frac{1}{16}), \\ q &= (\frac{1}{16}, \frac{1}{8}, \frac{1}{8}, \frac{3}{16}, t + \frac{1}{16}, \frac{1}{4} - t, \frac{3}{16} - t, t), \end{aligned}$$

with $0 \leq t \leq 3/16$ by nonnegativity. Exact row reduction, or a rank check together with substitution of a particular solution and its nonzero null direction, verifies this assertion.

Use two-qubit matrix units mapping the bit patterns $(0, 1)$ to $(1, 0)$ on positions $(4, 2)$ and $(5, 3)$, respectively, and $(0, 0)$ to $(1, 1)$ on positions $(1, 0)$. Their cross-support transitions are respectively

$$\{(27, 15), (48, 36)\}, \quad \{(39, 15), (48, 24)\}, \quad \{(27, 24), (39, 36)\}.$$

Matrix units are complex linear combinations of the relevant Paulis, so their off-diagonal compressions vanish. Put $u_x = \overline{a_x}$ and $v_y = b_y$. We obtain

$$\begin{aligned} u_{27}v_{15} + u_{48}v_{36} &= 0, \\ u_{39}v_{15} + u_{48}v_{24} &= 0, \\ u_{27}v_{24} + u_{39}v_{36} &= 0. \end{aligned} \tag{10}$$

All six amplitudes are nonzero, including at the endpoints of the allowed interval: the two variable squared moduli are $1/4 - t \geq 1/16$, and the others are $3/16$ or $1/8$. The first two equations give $u_{27}/u_{39} = v_{36}/v_{24}$; the third gives its negative. This is impossible over $\mathbb{C}$. Table 1 therefore closes all nine exceptions, without any real-amplitude or phase restriction.

5 Complete higher-order coverage

At modulus 16, an all-even vector reduces directly to modulus 8. For the 52,548 vectors with an odd coefficient, the standalone check finds 4844 empty second supports. The remaining 47,704 tuples produce 32,975 distinct ordered support pairs, all of which have exact integer moment separators. This enumeration is regenerated with `combinations_with_replacement`; its coordinate-sum checksum is 2,369,808. Thus every order-dividing-16 gate is excluded.

For $m = 32$ and then $m = 64$, the mutually exclusive branches are shown in Table 2. The first two reduce to the previously excluded modulus by Lemma 3. Empty supports and supports of size at most two are excluded by Lemma 2. Every remaining ordered support pair is covered by a checked integer separator.

5.1 An exact enumeration with bounded storage

The program writes a sorted tuple as (a, b, c, d, e, f) . For each b , it enumerates all suffixes $b \leq c \leq d \leq e \leq f < m$ and then takes $a = 0, \dots, b$. Every sorted tuple occurs once. For each suffix i , let $L_{r,i}$ be the 16-bit mask of four-bit words whose dot product with that suffix is $r \pmod{m}$. All sixteen words are evaluated with integer arithmetic.

Define $S(u) = \sum_{j: \text{bit}_j(u)=1} 2^{4j}$. For $t \in \{0, 1, 2, 3\}$ put $s_t = a \text{ bit}_0(t) + b \text{ bit}_1(t)$. The two complete six-bit support masks are

$$A = \bigvee_{t=0}^3 (S(L_{-s_t, i}) \ll t), \quad B = \bigvee_{t=0}^3 (S(L_{m/8-s_t, i}) \ll t), \tag{11}$$

Class	$m = 32$	$m = 64$
All coefficients even	54,264	2,324,784
Exactly one or two odd coefficients	775,200	39,709,824
Empty second support	297,784	31,518,100
One support has size at most two	940,779	44,459,312
Residual tuples	256,757	1,865,452
Total sorted tuples	2,324,784	119,877,472
Distinct residual support pairs	89,598	139,817
Uncertified residual pairs	0	0

Table 2: The first five rows partition all sorted tuples, in the displayed branch order. Distinct support pairs are deduplicated only after this partition. Every residual pair passes an exact strict-sign check.

where residue indices are taken modulo m . Indeed, the full word is $t + 4w$, so its bit position in the mask is exactly $t + 4w$. The largest position is 63. Complete ordered pairs of unsigned 64-bit masks are compared for equality; no approximate hash is used.

The code checks the multiset counts and the partition sums. The coordinate checksums are 216,204,912 at modulus 32 and 22,656,842,208 at modulus 64, each equal to half the tuple count times $6(m - 1)$. These checks support the explicit enumeration; a matching count alone would not establish completeness.

5.2 What the numerical optimizer is allowed to do

For an uncovered pair, a linear program proposes coefficients of a separating polynomial. Scaled coefficients are rounded to integers, after which every polynomial value on all 64 vertices is recomputed with unbounded Python integers. An exclusion is accepted only when its signs are strictly correct over both entire supports. A verified polynomial may cover additional pairs, but only through exact inclusion in its positive and negative vertex sets. Failure to obtain a certificate for even one pair aborts the check. No solver status, tolerance, floating residual, or time limit is interpreted as an exclusion.

The certificate verifies zero unresolved pairs in both columns of Table 2. Order 8, then 16, then 32, then 64 is therefore excluded. Lemma 1 completes the proof of Theorem 1.

6 Consequences, checks, and limitations

Corollary 1. *Seven is the minimum block length for a two-dimensional qubit code detecting all weight-at-most-two errors and admitting an exact transversal logical T of the form considered here.*

Proof. A code on fewer than six qubits could be embedded into six qubits by adjoining fixed product states and extending its local gate by identities. The scalar compression property for errors of weight at most two is preserved, contradicting Theorem 1. The seven-qubit construction of Ref. [2, Section 6.3.1] supplies the upper bound. $\square$

The six-qubit exclusion concerns the logical phase of projective order eight. It does not exclude the published six-qubit construction with a different non-Clifford phase of projective order five [2, Section 4.1], or protocols outside the stated transversal model.

The supplement contains the frozen complete proof, the standalone `exact-check.py`, and independent controls. The main check was run with Python 3.12.13, NumPy 2.5.3, SciPy 1.18.1, and SymPy 1.14.0 in the existing network-disabled Docker verifier. It uses no external project files or compiled helper. Separate enumeration programs, using direct subset recurrence and Gray-code traversal, regenerated the same residual pair sets. Saved integer witnesses were also checked without an optimizer. As a positive boundary control, the known seven-qubit example was reconstructed and all 211 Pauli compressions of weight at most two, together with its transversal phase, were checked exactly.

The distinction between analytic proof and computation matters. The program certifies finite arithmetic and coverage; it does not formally prove the arbitrary-angle reduction in a proof assistant. Two distinct frozen AI reviews and independent controls form the project’s internal verification process. They do not constitute human peer review or catalog acceptance. A focused comparison found no full six-qubit exclusion in the closest primary sources, but historical priority remains unverified.

AI assistance and writing procedure. The argument and computational certificates were developed with GPT-6 Astra using the Inspect AI rolling-state research workflow, with coordinator reconstruction and separate frozen reviews. AI assistance included mathematical reasoning, programming, verification, source comparison and exposition. The K-Dense scientific-writing procedure [5] was used for the evidence outline, numerical consistency checks and disclosure. No claim of independent human verification is made.

Availability. The manuscript, source, and verification archive accompany the author’s [research note](#). The background references below are separate from this manuscript’s own research record.

References

- [1] E. Knill and R. Laflamme, Theory of quantum error-correcting codes, *Physical Review A* **55**, 900–911 (1997). [doi:10.1103/PhysRevA.55.900](#).
- [2] C. Zhang, Z. Wu, S. Huang and B. Zeng, *Transversal Gates in Nonadditive Quantum Codes*, [arXiv:2504.20847](#), version 1, 29 April 2025. Sections 4.1, 6.1 and 6.3.1; Table 2.
- [3] X. He, S. Lu and B. Zeng, *Co-Designing Quantum Codes with Transversal Diagonal Gates via Multi-Agent Systems*, [arXiv:2510.20728](#), version 3, 6 April 2026. Section IV and Appendices F–G.
- [4] QIQCOP, *Non-additive $((6, 2, 3))$ qubit code with transversal T* , problem `op_ddfbbe7ca0ead0c8`, formulation last edited 15 September 2026, accessed 28 September 2026. https://qiqc-op.com/problem/op_ddfbbe7ca0ead0c8/.
- [5] T. Kassis, V. Agarwal, Y. He, D. Patel and A. M. Brueckner, *Scientific Agent Skills: A Library of Procedural Knowledge for Research Agents* (2026). [arXiv:2609.00065](#). Current record checked 28 September 2026; version 2 dated 2 September 2026.