Nineteen qubits are necessary and sufficient for symmetric quantum codes correcting two errors

Yuxuan Zhang

10 November 2026 (version 1.0)

Abstract

We give a computer-assisted lower bound for two-dimensional quantum codes contained in the fully symmetric subspace of n qubits. If such a code corrects every error on at most two qubits, then $n \geq 19$. Together with the published nineteen-qubit construction, this determines the minimum length. The lower bound allows arbitrary complex Dicke coefficients and does not assume parity, a logical symmetry, or nondegenerate errors. For each $9 \leq n \leq 18$, exact rational certificates exclude a necessary semidefinite relaxation of the third moment of a code projector. The relaxation retains the standard representation of the three-copy permutation group and imposes positivity after partial time reversal. The smaller lengths follow from the quantum Singleton bound. All certificate coefficients are regenerated from angular-momentum identities; verification requires no numerical optimizer.

1 The minimum-length question

A permutation-invariant quantum code stores information in states fixed by every permutation of the physical qubits. Such states lie in $\mathrm{Sym}^n(\mathbb{C}^2)$, a space of dimension $n+1$ inside the 2^n-dimensional qubit Hilbert space. This structure is useful for collective-spin implementations, but it restricts how errors can be distinguished. The natural resource question is how many symmetric qubits are needed to correct two arbitrary errors.

We use pointwise permutation invariance: every code vector is fixed, not merely the code projector. An orthonormal logical basis therefore has the form

$$|a_L\rangle = \sum_{w=0}^{n} c_{a,w}\,|D_w^n\rangle\,, \qquad |D_w^n\rangle = \binom{n}{w}^{-1/2} \sum_{|x|=w} |x\rangle\,, \qquad a = 0, 1, \tag{1}$$

where the coefficients may be complex. Correcting arbitrary errors on two qubits is equivalent to detecting all Pauli operators of weight at most four. In projector notation the Knill–Laflamme condition is $PEP = c_E P$ for every such Pauli operator.

Theorem 1. *Let $\mathcal{Q} \subseteq \mathrm{Sym}^n(\mathbb{C}^2)$ have dimension two and distance at least five. Then $n \geq 19$. Consequently,*

$$n_{\min}^{\mathrm{PI}}(2) = 19.$$

The equality uses the existing nineteen-qubit construction of Aydin, Alekseyev and Barg [1, Section 7]. They solve the real Pollatsek–Ruskai equations with computer algebra and report interval certification of solutions. The lower bound here applies also outside that real, odd-length family. An earlier parameter-counting prediction for real covariant spin codes also gives nineteen [3, Section IV-C]. Bond et al. conjecture the general formula $n_{\min}^{\mathrm{PI}}(t) = 3t^2 + 3t + 1$ from numerical searches [2, Conjecture 3.1]. Theorem 1 treats $t = 2$; it makes no assertion about other values of t.

The decisive new exclusion is $n = 18$. The scalar $\mathfrak{su}(2)$ linear-programming framework goes back to Bumgardner [4]. Okada's Table 3.1 reports a dimension bound of 1 at distance five through $n = 17$, but 2.019 at $n = 18$ and 2.096 at $n = 19$ [5]. These last two bounds allow a logical qubit. Okada discusses exact-rational agreement for smaller instances without specifying a cutoff for the table. We supply separate exact certificates for every $9 \le n \le 18$, while crediting the earlier bounds rather than claiming all ten exclusions as new.

The proof replaces a putative code projector by a rotation-averaged third moment. Detection becomes a collection of linear constraints on that moment. Positivity, permutation symmetry and partial-transpose positivity impose semidefinite constraints. Every actual code satisfies them, so an exact infeasibility certificate excludes the code. The standard three-copy permutation component is retained: averaging $P^{\otimes 3}$ does not put it entirely in a symmetric tensor power. Scalar enumerators and their time-reversal inequalities [4, 5, 6, 7] supply additional necessary constraints. Higher-moment SDP bounds [8] and rational certificates [9] are established tools in quantum coding; the reduction and certificates here address this particular minimum-length question.

2 A necessary third moment

Set $j = n/2$, $V = V_j = \mathrm{Sym}^n(\mathbb{C}^2)$, $N = n + 1$ and $K = 2$. Let P be a rank-K orthogonal code projector on V. In Condon–Shortley bases, the Hilbert–Schmidt orthonormal irreducible tensor operators are

$$(T_{lq})_{m,m'} = (-1)^{j-m'} \langle j, m; j, -m' \mid l, q \rangle. \tag{2}$$

Tensor rank l is contained in the degree-l collective-spin polynomials. Expanding these into single-qubit Pauli products shows that detection of weight at most four implies

$$PEP = \frac{\mathrm{Tr}(PE)}{K} P, \qquad E \in \mathrm{span}\{T_{lq} : 0 \le l \le 4\}. \tag{3}$$

This necessary direction suffices below. The full symmetric-power distance correspondence is proved in [6, Proposition B2].

Let U denote the spin-j representation and define

$$\Omega = \int_{\mathrm{SU}(2)} (UPU^*)^{\otimes 3} \, dU. \tag{4}$$

It is positive, has trace $K^3 = 8$, and commutes with both collective rotations and the permutation group S_3 on the three copies. Its fully antisymmetric part vanishes, since $\bigwedge^3 \mathrm{range}(P) = 0$.

Let F_{13} swap copies one and three. Direct contraction of indices gives

$$\mathrm{Tr}_3[(\mathbb{I} \otimes \mathbb{I} \otimes E) F_{13} P^{\otimes 3}] = PEP \otimes P.$$

Using (3), then rotating and averaging, yields

$$\mathrm{Tr}_3[(\mathbb{I} \otimes \mathbb{I} \otimes E)(F_{13} - \mathbb{I}/K)\Omega] = 0, \qquad 0 \le l(E) \le 4. \tag{5}$$

The rank-zero equations contain projector information and are included.

Define the spin-flip unitary $C\,|j, m\rangle = (-1)^{j+m}\,|j, -m\rangle$ and partial time reversal on the third copy by

$$\Theta_3(\Omega) = (\mathbb{I} \otimes \mathbb{I} \otimes C)\Omega^{T_3}(\mathbb{I} \otimes \mathbb{I} \otimes C^*). \tag{6}$$

Every term of (4) is a tensor product of positive matrices. Its partial transpose, and hence $\Theta_3(\Omega)$, is positive. Time reversal preserves rotational invariance and multiplies a rank-l operator on the third copy by $(-1)^l$.

Lemma 2. *A code with complex coefficients gives a real symmetric moment satisfying all the conditions above.*

Proof. Complex conjugation of the spin representation again ranges over the same representation of SU(2) in the chosen basis. The conjugated error space has the same tensor ranks. Thus $\overline{\Omega}$ is the moment associated with $\overline{P}$ and satisfies the same conditions. Averaging Ω with $\overline{\Omega}$ preserves positivity, partial-transpose positivity, trace, permutation symmetry and the linear detection equations. This averages moments; it does not replace P by its real part. □

3 All permutation-invariant positive blocks

Couple the first two spins to $a = 0, \dots, n$, then couple a and j to total spin J. The multiplicity basis is $|((jj)a, j)J, M\rangle$, with

$$I_J = \{a \in \mathbb{Z} : |J - j| \le a \le \min(n, J + j)\}.$$

The allowed J range from zero or one half to $3j$ in unit steps. Schur's lemma writes a rotationally invariant moment as

$$\Omega = \bigoplus_J X_J \otimes \mathbb{I}_{2J+1}, \qquad X_J \succeq 0. \tag{7}$$

The transpositions act on multiplicities by

$$D_J(a, a) = (-1)^{n-a}, \qquad R_J(a, b) = (-1)^n \sqrt{(2a + 1)(2b + 1)} \begin{Bmatrix} j & j & a \\ j & J & b \end{Bmatrix}. \tag{8}$$

Here D_J represents F_{12} and R_J represents F_{13}. They generate the six matrices of S_3.

Lemma 3. *Let E_J include the $+1$ eigenspace of D_J. Every positive, S_3-invariant block with no sign representation is the group average of $E_J H_J E_J^*$ for some $H_J \succeq 0$.*

Proof. An invariant block splits into trivial and standard components $X_{\text{triv}} + X_{\text{std}}$; the sign component is absent. On a standard irrep a transposition has one positive and one negative eigenvector, and the group average of its positive spectral projection is half the identity. On a trivial irrep the projection is the identity. Consequently the positive seed $E_J^*(X_{\text{triv}} + 2X_{\text{std}})E_J$ has group average equal to the original block after inclusion. This argument also retains arbitrary multiplicity matrices of the standard representation. □

We use rational coordinates to certify infeasibility. Define

$$\Delta(a, b, c)^2 = \frac{(a + b - c)!(a - b + c)!(-a + b + c)!}{(a + b + c + 1)!},$$
$$t_{Ja} = \sqrt{2a + 1}\, \Delta(j, j, a)\Delta(j, J, a). \tag{9}$$

All factorial arguments in allowed triangles are nonnegative integers. Choose a positive power of two q_{Ja} such that $d_{Ja} = (t_{Ja} q_{Ja})^2 \in [1, 4)$, and put $s_{Ja} = t_{Ja} q_{Ja}$. Writing $X_J = \operatorname{diag}(s_J) Z_J \operatorname{diag}(s_J)$ makes $R'_J = \operatorname{diag}(s_J)^{-1} R_J \operatorname{diag}(s_J)$ rational. Indeed, the four triangle factors in the Racah formula for the $6j$ symbol cancel the radicals in the diagonal scaling.

Let $W_{J,g}$ be the columns corresponding to $D_J = +1$ in the rational representation matrix of $g \in S_3$. Lemma 3 then gives the full parametrization

$$Z_J = \frac{1}{6} \sum_{g \in S_3} W_{J,g} H_J W_{J,g}^T, \quad H_J \succeq 0, \qquad \sum_J (2J + 1) \sum_{a \in I_J} d_{Ja} (Z_J)_{aa} = 8. \tag{10}$$

4 Detection and positivity in rational coordinates

4.1 Lifted detection

On the first two copies use the rank-l tensor $A^{(lq)}_{ab} : V_b \to V_a$ with matrix elements

$$(A^{(lq)}_{ab})_{m_a,m_b} = (-1)^{b-m_b}\langle a, m_a; b, -m_b \mid l, q\rangle.$$

It exists for $|a-b| \le l \le a+b$. The reduced contraction of (5) is

$$h^l_{Jab} = (2J+1)(-1)^{b+j+J}\begin{Bmatrix} a & j & J \\ j & b & l \end{Bmatrix}, \qquad \sum_J h^l_{Jab}[X_J R_J - X_J/K]_{ba} = 0. \tag{11}$$

This follows by inserting the coupled basis and performing a direct Clebsch–Gordan contraction. Rotational covariance pairs only equal tensor ranks, so the $q = 0$ contraction supplies the common reduced equation for all components. We retain every allowed pair a, b and every $l = 0, \dots, 4$.

For each test set

$$\begin{aligned} \kappa_{ab,l} &= \sqrt{(2a+1)(2b+1)}\,\Delta(j,j,a)\Delta(j,j,b)\Delta(a,b,l)\Delta(j,j,l), \\ c_{Jab,l} &= h^l_{Jab} s_{Ja} s_{Jb}/\kappa_{ab,l}. \end{aligned} \tag{12}$$

The numbers $c_{Jab,l}$ are rational: the Racah sum is multiplied by

$$(2J+1)(-1)^{b+j+J}\Delta(j,J,a)^2\Delta(j,J,b)^2 q_{Ja} q_{Jb}.$$

Dividing by the positive $\kappa_{ab,l}$ gives

$$\sum_J c_{Jab,l}[Z_J (R'_J)^T - Z_J/K]_{ba} = 0. \tag{13}$$

The transpose follows from the nonorthogonal scaling; replacing it by R'_J changes the constraint.

4.2 Scalar enumerators

Use the unnormalized enumerators

$$A_l = \sum_q |\operatorname{Tr}(PT_{lq})|^2, \qquad B_l = \sum_q \operatorname{Tr}(PT^*_{lq} P T_{lq}). \tag{14}$$

They obey $A_l \ge 0$ and $B_l - A_l/K \ge 0$. The latter is Hilbert–Schmidt Cauchy–Schwarz on the code subspace. In these conventions the intrinsic MacWilliams transform is

$$B = MA, \qquad M_{la} = (-1)^{n+a+l}(2l+1)\begin{Bmatrix} j & j & a \\ j & j & l \end{Bmatrix}. \tag{15}$$

These formulas are the scalar SU(2) specialization of the enumerator theory in [6, 7]. The two-copy moment $\operatorname{Tr}_3 \Omega/K$ gives

$$A_l = \frac{1}{K}\sum_J (2J+1)\sum_a f_{la} d_{Ja}(Z_J)_{aa}, \qquad f_{la} = (-1)^{n+a}(2l+1)\begin{Bmatrix} j & j & a \\ j & j & l \end{Bmatrix}. \tag{16}$$

Here $A_0 = K^2/N$ and $\sum_l A_l = K$. Time reversal preserves positivity of P and multiplies its rank-l component by $(-1)^l$. Applying the polarized completely positive twirl inequalities to P and its time reversal gives the shadow inequalities

$$M \operatorname{diag}((-1)^l) A \ge 0. \tag{17}$$

All these inequalities are linear in the seed matrices through (16).

4.3 Partial time reversal

For fixed a, b, expand an invariant operator in the contractions $\sum_q (-1)^q A^{(lq)}_{ab} \otimes T_{l,-q}$. Their reduced matrix elements are $(2l+1)h^l_{Jab}/(2J+1)$. The $6j$ orthogonality relations invert this expansion, while time reversal contributes $(-1)^l$. Thus

$$(\Theta_3 X)_{J,ab} = \sum_{J'} L_{ab}(J,J') X_{J',ab}, \qquad L_{ab}(J,J') = \sum_l \frac{(-1)^l (2l+1) h^l_{Jab} h^l_{J'ab}}{2J+1}, \tag{18}$$

where $|a-b| \le l \le \min(n, a+b)$. The scaled blocks Y_J of $\Theta_3\Omega$ therefore satisfy

$$\begin{aligned} (Y_J)_{ab} &= \sum_{J'} T_{ab}(J,J')(Z_{J'})_{ab}, \\ T_{ab}(J,J') &= \sum_l \frac{(-1)^l (2l+1) \kappa^2_{ab,l} c_{Jab,l} c_{J'ab,l}}{(2J+1) d_{Ja} d_{Jb}}. \end{aligned} \tag{19}$$

The transform is rational and involutive. Since Θ_3 commutes with F_{12}, each Y_J splits into the two parities of a; both blocks must be positive. It need not commute with the other transpositions and need not have a vanishing sign component.

5 Ten exact exclusion certificates

Flatten the independent upper-triangular seed entries into x. Equations (10) and (13) give $\mathsf{A}x = b$, where $b = (8, 0, \ldots, 0)^T$. Collect the scalar and shadow inequalities in $Gx \ge 0$, and write $L_k(x)$ for the two parity blocks of the Y_J. Every code supplies a feasible point of

$$\mathsf{A}x = b, \qquad Gx \ge 0, \qquad H_J(x) \succeq 0, \qquad L_k(x) \succeq 0. \tag{20}$$

Sufficiency of this relaxation for constructing a code is not needed.

For each $n = 9, \ldots, 18$ the accompanying file `certificate-ppt-nN.json` supplies rational y, scalar multipliers λ and matrices Q_k. The checker computes the seed slack matrices S_J from the exact identity

$$y^T \mathsf{A}x - \lambda^T G x - \sum_k \operatorname{Tr}(Q_k L_k(x)) = \sum_J \operatorname{Tr}(S_J H_J(x)). \tag{21}$$

This identity holds for every symmetric seed; off-diagonal linear coefficients are divided by two in the trace pairing. Direct rational arithmetic verifies

$$\lambda \ge 0, \qquad Q_k \succ 0, \qquad S_J \succ 0, \qquad y^T b < 0. \tag{22}$$

Positive definiteness is checked by exact LDL^T pivots. If (20) were feasible, every term on the right after rearranging (21) would be nonnegative, contradicting $y^T b < 0$.

The ten certificates contain 435 nonnegative scalar multipliers and 2,496 positive matrix pivots. Each $y^T b$ is a negative rational; for example, at $n = 18$ it is

$$-\frac{2475880078571389911855372369749 01}{2475880078570760549798248448000000}.$$

Floating-point solver results guided the search, but their residuals and statuses do not enter the exclusion. The checker regenerates the coefficients from n, recomputes the dual slacks and checks their exact signs. It reads no cached coefficient matrices.

For $n \le 8$, the quantum Singleton bound already excludes a two-dimensional distance-five code. One can see the obstruction directly: for $5 \le n \le 8$, correction of every four-qubit erasure would recover the logical state from either of two disjoint sets of $n-4$ qubits, violating no-cloning. For $n \le 4$, detection of every weight-at-most-four Pauli is detection of the full operator algebra, impossible for a rank-two code. These arguments together with the ten certificates exclude every $n \le 18$. No monotonicity of symmetric-code existence in n is assumed. The published nineteen-qubit existence result completes Theorem 1.

n	Scalar multipliers	Q_k positive pivots	S_J positive pivots
9	30	75	40
10	33	91	48
11	36	108	57
12	39	127	67
13	42	147	77
14	45	169	88
15	48	192	100
16	51	217	113
17	54	243	126
18	57	271	140

Table 1: Exact certificate checks, one for each excluded length.

6 Reproducibility and scope of review

The source package contains the rational coefficient generators, ten certificates, their exact expected outputs, the original problem statement and a runner that checks hashes and copies the computational inputs into an initially empty directory. Running `python reproduce.py` regenerates and verifies all ten systems without an optimizer. The pinned Python dependencies are NumPy, SymPy and gmpy2. Timing and floating-point displays of pivot sizes are excluded from the exact comparison.

The analytic issue is whether every admissible code enters the relaxation. Lemma 2, Lemma 3, (5) and (19) carry that conclusion; successful certificate replay alone cannot establish it. The derivation has finite controls using direct Clebsch–Gordan contractions, independently formed partial transposes and known codes. A separate model context reviewed these analytic steps and the primary literature, independently checked the coefficients, and tested the moment constraints on complex projectors and a known twenty-one-qubit distance-five code. Its report and controls accompany the release. It found no fatal issue and supported full original coverage; external expert review remains outstanding.

The result concerns a logical qubit in the fully symmetric physical-qubit subspace. It permits complex coefficients, both length parities and degenerate error correction. It does not bound the length of unrestricted quantum codes, determine a family for every number of errors, or assert that every optimal symmetric code has Pollatsek–Ruskai symmetry.

Human and AI contributions. The author directed the research and designed the workflow for problem selection, derivation and checking. AI systems developed the candidate argument, searched primary literature, generated and checked computational certificates, and drafted the manuscript under that direction. Review by a fresh model context is distinct from external expert review and formal proof verification.

References

[1] A. Aydin, M. A. Alekseyev and A. Barg, "A family of permutationally invariant quantum codes," *Quantum* **8**, 1321 (2024). doi:10.22331/q-2024-04-30-1321; arXiv:2310.05358v3.

[2] L. J. Bond, J. Minář, M. Ozols, A. Safavi-Naini and V. Visnevskyi, "Permutation-invariant codes: a numerical study and qudit constructions," arXiv:2603.10981v1 (2026).

[3] E. Kubischta and I. Teixeira, "Permutation-Invariant Quantum Codes with Transversal Generalized Phase Gates," *IEEE Transactions on Information Theory* **71**, 485–498 (2025). arXiv:2310.17652v3.

[4] C. Bumgardner, "Codes in W*-metric Spaces: Theory and Examples," arXiv:1205.4517v1 (2012).

[5] R. S. Okada, "A Quantum Analog of Delsarte's Linear Programming Bounds," Ph.D. dissertation, University of California, Davis (2023), arXiv:2502.14165v1 (2025).

[6] E. Kubischta and I. Teixeira, "MacWilliams Identities for Intrinsic Quantum Codes," arXiv:2604.16023v2 (2026).

[7] I. Teixeira, "Orthogonal Polynomials and the MacWilliams Transform for Permutation-Invariant Qudit Codes," arXiv:2605.15372v1 (2026).

[8] G. Angl'es Munné, A. Nemec and F. Huber, "SDP bounds on quantum codes," arXiv:2408.10323v2 (2025).

[9] G. Anglès Munné and F. Huber, "SDP bounds on quantum codes: rational certificates," arXiv:2603.19901v1 (2026).