A pure-state matched-basis information inequality violation in dimension five

Dev D. Goyal

28 October 2026; revised 1 November 2026

Abstract

This note defines a matched-identical-basis information comparison, motivated by the ECQC proposal of Iqbal [1]: the minimum sum from five of six mutually unbiased local settings is compared with the quantum mutual information of the state. In local dimension five, the normalized pure state $5^{-1/2}\sum_{x\in\mathbb{F}_5}|x\rangle|2x\rangle$ has quantum mutual information $2\log 5$. When both parties use the same computational basis or any of the five specified quadratic bases, the joint measurement table is a uniform permutation table with mutual information $\log 5$. Every selection of five settings therefore has sum $5\log 5$, exceeding the quantum-information budget by $3\log 5$, with ratio $5/2$. The proof verifies all six orthonormal bases, mutual unbiasedness, the actual Born probabilities, purity, and both reduced states. The basis family and identical-local-basis convention are explicit. A Lean formalization checks the dimension-five theorem for the actual state, bases, Born probabilities and entropies. Prior mixed-state ECQC counterexamples receive separate credit. Correspondence with an external ECQC proposal and historical novelty remain unverified. The same dimension-five counterexample was recorded publicly earlier, and no priority is claimed for it.

1 The question and prior work

Classical correlations obtained from several complementary measurements need not fit within a proposed quantum-information budget. The question here is whether the explicitly defined matched-basis bound below holds on pure states. The construction below shows a violation for a fixed complete six-basis family in dimension five. The mechanism is the exact identity $1+2^2=0$ in $\mathbb{F}_5$, which cancels every quadratic phase in the same-basis measurement amplitude.

For a bipartite density operator ρ, write

$$I(A:B)_\rho = S(\rho_A)+S(\rho_B)-S(\rho), \qquad S(\rho) = -\operatorname{Tr}(\rho\log\rho).$$

For a local basis measurement M performed by both parties, let $I(M^A:M^B)$ denote the Shannon mutual information of its joint Born distribution. All logarithms in this note are natural; division by $\log 2$ gives bits. The choice of base has no effect on the inequality.

For a finite probability distribution, $H(P)=-\sum_x P(x)\log P(x)$, with $0\log 0=0$. Classical mutual information is $H(P^A)+H(P^B)-H(P)$. Two orthonormal bases are mutually unbiased when every squared cross-basis overlap is $1/d$.

For a fixed complete collection $\mathcal{M}$ of $d+1$ mutually unbiased bases, define the score and the inequality to be tested by

$$E_d(\rho;\mathcal{M}) := \min_{\substack{\mathcal{S}\subset\mathcal{M}\\|\mathcal{S}|=d}} \sum_{M\in\mathcal{S}} I(M^A:M^B) \;\le\; I(A:B)_\rho. \tag{1}$$

The minimum discards one largest measurement mutual information. The collection is fixed; this definition does not optimize over other basis collections or local changes of basis.

The motivating ECQC proposal and pure-state question are attributed to Iqbal [1]. Wang, Wang, and Chen receive credit for the earlier mixed-state ECQC counterexamples attributed to their cited preprint [5]. These source comparisons, the precise published optimization, Bob's measurement convention, and current versions have not been verified here. A refutation of an external statement follows only if its definitions and quantifiers agree with (1) and the measurement model below. No unrestricted ECQC priority claim is made.

The theorem below violates (1) using identical local basis vectors on both parties. Bob uses the same basis vectors as Alice in each setting. Replacing his basis by a separately conjugated family changes the model. Section 6 describes the Lean formalization of the dimension-five theorem.

Earlier public work (note added 1 November 2026). On 31 October 2026 a check of public problem records found that the Omega Institute's public repository records the same counterexample: the state $5^{-1/2}\sum_x |x\rangle|2x \bmod 5\rangle$ with the same six mutually unbiased bases, used identically by both parties, giving the classical sum $5\log 5$ against the quantum mutual information $2\log 5$ [3]. That record, preregistered as issue #12896, was first committed on 4 October 2026, with a claimed Lean proof frozen the same day, about 25 days before this result was first committed to the author's repository. The conventional all-prime companion mentioned in Section 6 does not appear in that record. No originality or priority claim is made for the dimension-five counterexample.

2 Exact construction and theorem

Identify indices with $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, and let

$$\omega = e^{2\pi i/5}.$$

Define the normalized pure state

$$|\Psi\rangle = \frac{1}{\sqrt{5}} \sum_{x\in\mathbb{F}_5} |x\rangle_A |2x\rangle_B. \tag{2}$$

The same vector in computational notation is

$$|\Psi\rangle = \frac{|00\rangle + |12\rangle + |24\rangle + |31\rangle + |43\rangle}{\sqrt{5}}.$$

Take the computational basis M_∞ and the five quadratic bases

$$M_a = \{|a,k\rangle : k \in \mathbb{F}_5\}, \qquad |a,k\rangle = \frac{1}{\sqrt{5}} \sum_{x\in\mathbb{F}_5} \omega^{ax^2+kx}|x\rangle, \quad a \in \mathbb{F}_5. \tag{3}$$

The set $\mathcal{M} = \{M_\infty, M_0, M_1, M_2, M_3, M_4\}$ has six elements. Subscripts on the quadratic bases in this note are field indices. Section 4 gives an equivalent matrix representation.

Theorem 1 (Pure-state matched-basis violation)**.** *The five quadratic bases in (3) and the computational basis form a complete set of mutually unbiased orthonormal bases. For the state (2), every same-basis measurement has joint distribution*

$$P_M(i,j) = \begin{cases} 1/5, & j = 2i \pmod 5, \\ 0, & \textit{otherwise.} \end{cases} \tag{4}$$

Consequently,

$$I(M^A : M^B) = \log 5 \quad (M \in \mathcal{M}), \qquad I(A:B)_{|\Psi\rangle\langle\Psi|} = 2\log 5, \tag{5}$$

and

$$E_5(|\Psi\rangle\langle\Psi|; \mathcal{M}) = 5\log 5 > 2\log 5. \tag{6}$$

This is a counterexample to the displayed universal inequality on pure states. The excess is exactly $3\log 5$, and the ratio of the two sides is $5/2$. No assertion of minimal counterexample dimension is made.

3 Proof of Theorem 1

3.1 A fifth-root identity

For $c \in \mathbb{F}_5$,

$$\sum_{x\in\mathbb{F}_5} \omega^{cx} = \begin{cases} 5, & c = 0, \\ 0, & c \neq 0. \end{cases} \tag{7}$$

The zero case is immediate. In the other case, multiplication by c permutes $\mathbb{F}_5$, and

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0.$$

All exponent calculations below occur modulo five.

3.2 Orthonormality and mutual unbiasedness

For a fixed a,

$$\langle a, k|a, l\rangle = \frac{1}{5}\sum_x \omega^{(l-k)x} = \delta_{kl}$$

by (7). Thus each M_a is an orthonormal basis. Every computational coordinate of every vector in M_a has squared magnitude $1/5$, giving mutual unbiasedness with M_∞.

For two distinct quadratic bases, set $c = b - a \neq 0$ and $e = l - k$. Their unnormalized overlap is

$$G(c, e) = \sum_x \omega^{cx^2+ex}.$$

Writing $x = y + u$, expanding, and then applying (7),

$$\begin{aligned} |G(c,e)|^2 &= \sum_{u,y} \omega^{c((y+u)^2-y^2)+eu} \\ &= \sum_u \omega^{cu^2+eu} \sum_y \omega^{2cuy} \\ &= 5. \end{aligned}$$

Indeed, $2c \neq 0$ in $\mathbb{F}_5$, so the inner sum is zero unless $u = 0$, when it equals five. After the two factors $1/\sqrt{5}$ in the basis vectors, the squared overlap is $5/25 = 1/5$. All six bases are therefore pairwise mutually unbiased.

3.3 Normalization and reduced states

The map $x \mapsto 2x$ is a permutation of $\mathbb{F}_5$, and the five computational terms in (2) are orthogonal. Hence $\langle\Psi|\Psi\rangle = 1$.

Let $\rho = |\Psi\rangle\langle\Psi|$. Tracing out either subsystem gives

$$\rho_A = \rho_B = \frac{1}{5} I_5. \tag{8}$$

For example,

$$\mathrm{Tr}_B\, \rho = \frac{1}{5} \sum_{x,y} |x\rangle\langle y|\, \langle 2y|2x\rangle = \frac{1}{5} \sum_x |x\rangle\langle x|.$$

The other partial trace follows in the same way, using that multiplication by two is bijective.

3.4 Every joint measurement table

In the computational basis, (4) follows immediately from (2).

For a quadratic basis M_a, the joint amplitude is

$$\begin{aligned} (\langle a, i| \otimes \langle a, j|)|\Psi\rangle &= \frac{1}{5\sqrt{5}} \sum_x \omega^{-ax^2 - ix - a(2x)^2 - j(2x)} \\ &= \frac{1}{5\sqrt{5}} \sum_x \omega^{-(i+2j)x}. \end{aligned} \tag{9}$$

The second equality uses the exact field identity $1 + 2^2 = 0$. By (7), the amplitude is $1/\sqrt{5}$ when $i + 2j = 0$, and zero otherwise. Since $2^2 = -1$, the equation $i + 2j = 0$ is equivalent to $j = 2i$. Taking the squared magnitude proves (4) for every quadratic setting.

With row and column order $0, 1, 2, 3, 4$, the common table is explicitly

$$P_M = \frac{1}{5} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{10}$$

3.5 Entropies and the strict violation

Both marginals of (10) are uniform. The joint table has exactly five nonzero entries, all $1/5$. Therefore

$$H(P_M^A) = H(P_M^B) = H(P_M) = \log 5,$$

and

$$I(M^A : M^B) = H(P_M^A) + H(P_M^B) - H(P_M) = \log 5.$$

The state ρ is a rank-one orthogonal projector, so its nonzero spectrum is (1) and $S(\rho) = 0$. Equation (8) gives $S(\rho_A) = S(\rho_B) = \log 5$, proving the quantum value in (5).

Every five-element subset of the six measurement settings has the same sum, $5 \log 5$; thus the minimum in (1) is exactly that value. Since $\log 5 > 0$, equation (6) is strict. This completes the proof.

In bits, the six individual scores are each approximately 2.3219280949, the matched-basis score is approximately 11.6096404744, and the quantum mutual information is approximately 4.6438561898. These decimal values are illustrations of the exact formulas, not inputs to the proof.

4 Equivalent matrix representation and source comparison

The displayed bases can also be written using the Fourier matrix F, the identity, and powers of

$$D = \mathrm{diag}(1, \omega, \omega^4, \omega^4, \omega), \qquad F_{xk} = \omega^{xk}/\sqrt{5}.$$

Because x^2 modulo five is $0, 1, 4, 4, 1$, the columns of $D^a F$ are exactly (3). The correspondence is:

Comparison label	Matrix	Label in this note
M_0	F	M_0
M_1	I_5	M_∞
M_2	DF	M_1
M_3	D^2F	M_2
M_4	D^3F	M_3
M_5	D^4F	M_4

Reindexing these six bases has no effect on the minimum over five-element subsets. The comparison labels record the convention attributed to Iqbal's Section 4.5.2 [1]; their identity with the published vectors and local measurement rule remains unverified. The matrix identities in this section follow directly from (3).

The state differs from the conventional $5^{-1/2} \sum_x |x, x\rangle$ by a fixed local permutation. This distinction matters because the measurement bases are fixed. The cancellation in (9) comes from the permutation in the state. It does not change either party's measurement rule.

5 Scope and attribution

The construction gives an exact pure-state violation for the displayed matched measurement family. It does not assert the smallest possible counterexample dimension. It also does not claim the first disproof of unrestricted ECQC: the mixed classical-classical counterexamples of Wang, Wang, and Chen are prior work [5].

Original two-basis complementary quantum correlation (CQC) is a separate question. Related contributions are attributed to Wang, Wang, and Chen [4] and Qian [2]. These later-work summaries and bibliographic details remain unverified. These attributions do not turn the present example into a new resolution of original CQC. The result here is the exact pure-state construction for the specified matched-basis settings. Its historical priority and the comparison with current source versions remain provisional.

The state differs from the usual maximally entangled state by a local permutation, while the measurement bases remain fixed. This distinction is essential to the phase cancellation. The result makes no claim about quantum capacity, cryptographic security, experimental implementation, or a classification of all dimensions or measurement families.

6 Formal verification and reproducibility

The formal project uses Lean 4.19.0 and mathlib revision

`c44e0c8ee63ca166450922a373c7409c5d26b00b`.

The state is an actual normalized vector; its density matrix is its outer product. Both reduced matrices are partial traces. Von Neumann entropy is defined through continuous functional calculus of the matrices. The measurement probabilities are squared magnitudes of the actual Born amplitudes, then proved equal to the permutation table. Thus the entropy calculation is connected to the quantum state and measurements, rather than assumed for an unrelated table.

The principal declarations, in namespace `ECQC5`, are

```
pure_state_ECQC_counterexample
no_actual_five_setting_budget
actualScore_bits_violation
```

The complete source was freshly rebuilt with Lean 4.19.0 on 28 October 2026. A separate audit with `--trust=0` checked eight named endpoints, including basis unitarity, mutual unbiasedness, the Born-table identity, quantum mutual information, and density-matrix positivity. The build and audit succeeded. All eight reports contain only `propext`, `Classical.choice`, and `Quot.sound`. The proof sources and pins were unchanged during checking. A declaration map and reproduction commands accompany this paper. Formal checking does not establish historical novelty, source attribution, expert validation, or an external conjecture identification.

A supplementary exact cyclotomic arithmetic check covered 125 orthogonality identities, 375 unbiasedness identities, 125 quadratic Born probabilities, and 100 negative-control checks for the ordinary maximally entangled state. These are finite exact checks. They support the explicit arithmetic and do not replace the formal density-matrix and entropy proof. The all-prime companion note proves an unbounded-ratio extension by a conventional argument. The Lean package covers dimension five only.

7 Research process and AI disclosure

This work is fully autonomous agentic research. Automated systems produced the research, proofs, formalization, and earlier versions of this manuscript. Opus 5.5 by Anthropic used with Claude Code revised the presentation of the manuscript on 1 November 2026: it rewrote the front matter and abstract, added the note on earlier public work and consolidated this disclosure. The revision does not change the mathematics. Dev D. Goyal is responsible for publication. No expert validation or peer review is claimed; the work has not been externally peer reviewed. The formal scope is stated in Section 6, and the limits of the source comparison in the section on scope and attribution.

References

[1] H. Iqbal. On the CQC conjecture: a sufficient condition and an extension. *Quantum Information Processing*, 25, 2026. Unverified source-context metadata. Article 250. Published 10 July 2026. DOI: 10.1007/s11128-026-05258-2. Conjecture 3.1, equation (6), Sections 4.5.2 and 5.

[2] L. Qian. Separable counterexamples to complementary quantum correlations, and why random search missed them. arXiv:2608.14806, https://arxiv.org/abs/2608.14806, 2026. Unverified source-context metadata. 14 August 2026.

[3] The Omega Institute. Problem dossier on the pure-state ECQC specialization (issue #12896). Public repository `the-omega-institute/trureturing`, first committed 4 October 2026, https://github.com/the-omega-institute/trureturing/blob/a47aa292ae5090e6c9681bf6d41c5e5f6e9b9dcf/Problems/iqbal-2025-pure-state-ecqc.md.

[4] J. Wang, Q. Wang, and K. Chen. Complementary quantum correlations are universal for qubits. arXiv:2608.04916v1, https://arxiv.org/abs/2608.04916v1, 2026. Unverified source-context metadata. 5 August 2026.

[5] J. Wang, Q. Wang, and K. Chen. When complementary measurements count the same classical bit twice: Counterexamples to CQC, ECQC, and complementarity-based certification. arXiv:2608.03828v3, https://arxiv.org/abs/2608.03828v3, 2026. Unverified source-context metadata. 25 September 2026. Section IV, equation (7), Appendix B, and Section VI.