

When Complementary Measurements Count the Same Classical Bit Twice: Counterexamples to CQC, ECQC, and Complementarity-Based Certification

Jinbo Wang,¹ Qihang Wang,¹ and Kun Chen^{2,*}

¹*School of Mathematical Sciences, Peking University, Beijing 100871, China*

²*Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100190, China*

Complementary measurements can count the same classical information twice. We construct rank-two classical-classical states that violate the complementary-quantum correlation conjecture in every equal local dimension $d \geq 3$. A distinct two-branch source violates its complete-basis extension with an unbounded overrun along prime dimensions. The constructions also give false positives for specific quantum-correlation, steering, and conditional-probability criteria. A shared-bit source provides a simple null test for multibasis resource certification.

Introduction.—

Measuring a quantum system in one way can erase what was predictable in another. The extreme case is a pair of mutually unbiased bases (MUBs): a state with a certain outcome in one basis gives every outcome with equal probability in the other. This familiar expression of complementarity suggests a simple intuition: a classical source may coordinate Alice and Bob in one measurement basis, but should lose that coordination when both switch to a complementary basis. Correlations observed in both bases are then taken as evidence of a genuinely quantum shared resource. The complementary-quantum correlation (CQC) conjecture turns exactly this intuition into an additive information budget: correlations accessible in two MUBs are proposed to share a single budget set by the state's quantum mutual information (QMI) [1]. The same intuition appears in several concrete proposals: the extended CQC (ECQC) conjecture for complete MUB sets [2]; a criterion that sums matched conditional probabilities in complementary bases to detect entanglement [3]; and a claim that residual complementary-basis correlations certify one-sided semi-device-independent (1SSDI) steering [4]. It also motivates complementary-basis measures of quantum correlation and MUB entanglement witnesses [5, 6]. Experimentally, such multibasis scores are attractive because they can be estimated from a few local measurement settings, offering low-overhead routes to quantify correlations and certify entanglement or steering without full state tomography.

This intuition is natural for qubits but becomes subtle in higher dimensions. In the simplest qubit encoding, a source maps the bit K to the two X -basis states. The X measurement reads K exactly, while the mutually unbiased Z measurement gives the same 50:50 distribution for both states and erases it. For $d \geq 3$, however, there are many superpositions of $|x_1\rangle, \dots, |x_{d-1}\rangle$. Encode $K = 0$ in $|x_0\rangle$ and $K = 1$ in any such superposition. The binary test $X = 0$ versus $X \neq 0$ reads K perfectly, while different choices for the $K = 1$ state can have different Z -basis statistics. Choosing one whose Z distribution differs from that of $|x_0\rangle$ lets Z retain partial information about the same K . Any theoretical criterion or experimental

protocol that combines correlations from complementary bases as evidence of a quantum resource must therefore confront a common potential loophole: the same classical information may be counted more than once.

To test this potential loophole, we propose a two-branch classical null test. The test feeds a known classical control state ρ_d into a protocol while leaving its measurements and scoring rule unchanged. If ρ_d crosses a threshold claimed to certify a quantum resource, the criterion has a classical false positive. For every $d \geq 3$, construct ρ_d as follows. Let $Z = \{|j\rangle\}$ be the computational basis and let X be its Fourier MUB:

$$|u\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle, \quad |v\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \quad (1)$$

$$\rho_d = \frac{1}{2} |u\rangle\langle u|_A \otimes |v\rangle\langle v|_B + \frac{1}{2} |v\rangle\langle v|_A \otimes |u\rangle\langle u|_B.$$

To prepare ρ_d , sample a fair bit K before choosing the measurement setting. For $K = 0$, send $|u\rangle$ to Alice and $|v\rangle$ to Bob; for $K = 1$, swap them. Thus ρ_d is an equal mixture of two product preparations. Because $|u\rangle$ and $|v\rangle$ are orthogonal, it is classical-classical and its only shared correlation is K . Moreover, $|u\rangle = |x_0\rangle$, so X distinguishes the two preparations as $x = 0$ versus $x \neq 0$. Their Z -basis distributions also differ, allowing both bases to carry information about the same K .

Applied without modification, this null source disproves CQC for every $d \geq 3$. A distinct rank-two classical-classical state, specified in the ECQC section, disproves ECQC at $d = 7$ with an aggregate overrun that grows without bound along prime dimensions [1, 2]. At $d = 3$, the same source violates the prediction that a complementary-basis quantum-correlation measure vanishes on classical-classical (CC) states [5], the claimed implication from that measure to 1SSDI steering [4], and a proposed separable conditional-probability interval [3]; a related full-rank $d = 4$ source also defeats the natural permutation-optimized repair of the latter. Beyond these specific failures, the same low-cost source provides a laboratory calibration: a threshold crossing in an otherwise unchanged data pipeline directly diagnoses classical overcounting. Passing this null test is necessary but not

sufficient; a final certificate must still bound every classical or separable source and every processing step allowed by its operational assumptions.

Two-Branch Classical Null Test.—

For a bipartite state ρ_{AB} , the quantum mutual information (QMI) is $I(A : B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$, where S is the von Neumann entropy. By contrast, $I(M^A : M^B)$ denotes the ordinary Shannon mutual information between the classical outcomes when Alice and Bob measure a basis M . The states $|u\rangle$ and $|v\rangle$ in Eq. (1) are orthogonal, so ρ_d is diagonal in a local product basis. It is therefore a rank-two CC state: its correlation is a pre-existing classical label, and the state is separable with zero discord in both directions. The global state and both marginals have nonzero spectrum $(1/2, 1/2)$, giving $I(A : B) = 1$ bit.

The loophole appears when correlations from different settings are added. For each setting x , data processing gives $I(A_x : B_x) \leq I(A : B) = 1$, but it does not bound the sum over x by one bit. Each setting is evaluated on a fresh copy of ρ_d , and both parties may change their readout with x . For our source, different MUB settings recover the same K , so their sum counts one classical bit more than once.

No quantum information is cloned, and MUB geometry remains intact. Mutual unbiasedness fixes the exact outcome distribution obtained by measuring a basis state in the other basis; it does not prevent different settings from grouping their outcomes so as to reveal the same classical variable. Multibasis correlations in nonproduct and zero-discord states were known [7, 8]; ρ_d shows that this redundancy can cross proposed quantum thresholds. Nor does the construction contradict information-exclusion bounds proved with one party's measurement fixed [9]: CQC and ECQC allow both parties to change their readout with the setting.

Counterexample to CQC.—

Let $Z = \{|j\rangle\}$ be the computational basis and $X = \{|x_k\rangle\}$ its Fourier MUB, $|x_k\rangle = d^{-1/2} \sum_j e^{2\pi i j k / d} |j\rangle$. The CQC conjecture asserts [1]

$$I(Z_A : Z_B) + I(X_A : X_B) \leq I(A : B). \quad (2)$$

It was proved for pure states, states with one maximally mixed subsystem, and all states when one measurement is minimally disturbing; extensive Monte Carlo searches found no violation [1]. Later work derived a sufficient condition covering additional states and proposed an extension to complete MUB families in prime dimensions [2].

Apply the null source in Eq. (1). In the X basis, $|u\rangle = |x_0\rangle$ always gives outcome 0, whereas $|v\rangle$ never does. Thus the binary question “zero or nonzero?” identifies K perfectly at either party, and $I(X_A : X_B) = 1$ bit. In the Z basis the outcome laws of $|u\rangle$ and $|v\rangle$ are

$$p = (1/d, \dots, 1/d), \quad q = (1/2, 1/2, 0, \dots, 0), \quad (3)$$

so that

$$P_Z(j, k) = \frac{1}{2}[p_j q_k + q_j p_k]. \quad (4)$$

This distribution is nonproduct for every $d \geq 3$, and its mutual information is

$$g_d = \frac{2}{d} \log_2 \frac{8d}{(d+2)^2} + \frac{d-2}{d} \log_2 \frac{2d}{d+2} > 0. \quad (5)$$

The quantity g_d is the residual Z -basis correlation generated by the same bit K already read perfectly in X ; it is not a second shared variable. Consequently, $I(X_A : X_B) + I(Z_A : Z_B) = 1 + g_d > 1 = I(A : B)$, disproving CQC for every $d \geq 3$. For qutrits the measured sum is

$$1 + \frac{1}{3} \log_2 \frac{3456}{3125} = 1.0484156759 \dots \text{ bits}. \quad (6)$$

The violation is strict and therefore survives sufficiently weak white noise, giving full-rank separable counterexamples.

Counterexample to ECQC.—

The complete-basis extension asks whether using all available complementarity restores an additive information budget. For a complete set $\mathcal{M}$ of $d+1$ MUBs in prime dimension, ECQC sums the d least-correlated bases—or, equivalently, discards one largest term—and asserts [2]

$$\min_{\substack{\mathcal{S} \subset \mathcal{M} \\ |\mathcal{S}|=d}} \sum_{M \in \mathcal{S}} I(M^A : M^B) \leq I(A : B). \quad (7)$$

For an odd prime d , let $\mathbb{F}_d$ denote integers modulo d . Take $M_\infty = Z$ and, for each $a \in \mathbb{F}_d$, define the quadratic basis $M_a = \{|a, b\rangle : b \in \mathbb{F}_d\}$ by

$$|a, b\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{2\pi i (aj^2 + bj)/d} |j\rangle, \quad a, b \in \mathbb{F}_d. \quad (8)$$

These $d+1$ bases form a complete MUB set. For ECQC, use instead

$$|u_d^E\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |v_d^E\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \quad (9)$$

and let ρ_d^E be the equal swapped product mixture obtained from Eq. (1) by replacing $|u\rangle, |v\rangle$ with $|u_d^E\rangle, |v_d^E\rangle$. This is again a rank-two CC state with $I(A : B) = 1$. The computational basis gives the same outcome law for $|u_d^E\rangle$ and $|v_d^E\rangle$, hence $I_{M_\infty} = 0$. In every quadratic MUB their laws are, up to a common cyclic relabeling,

$$p_j = \frac{1 + c_j}{d}, \quad q_j = \frac{1 - c_j}{d}, \quad c_j = \cos \frac{2\pi j}{d}. \quad (10)$$

Their swapped branches give

$$P_{jk}^{(d)} = \frac{1 - c_j c_k}{d^2}, \quad J_d := I(P^{(d)}). \quad (11)$$

Thus the $d + 1$ scores are $\{0, J_d, \dots, J_d\}$. ECQC retains the zero term and $d - 1$ copies of J_d , giving $E_d = (d - 1)J_d$. At $d = 7$,

$$\begin{aligned} J_7 &= 0.2079841266\dots, \\ E_7 &= 1.2479047596\dots > I(A : B) = 1. \end{aligned} \quad (12)$$

Supplemental Material [10] supplies the full derivations, exact tables, robustness constructions, and independent executable checks. In particular, J_d approaches a strictly positive integral along odd primes. Hence $d - 1$ retained quadratic bases each contribute an incomplete reading of the same branch bit, and E_d grows linearly along prime dimensions although the state contains only one bit of QMI. Complete MUB symmetry therefore amplifies redundant readouts into an unbounded aggregate overrun.

Certification Failures and Scope.—

Quantum-correlation measure.— The same qutrit state tests more than a QMI conjecture. The Holevo correlation upper-bounds how much information Bob can obtain about Alice’s measurement result from his conditional quantum states. The measure $Q_2^{\rightarrow}$ maximizes this correlation over Alice’s basis and then over a MUB, interpreting the residual as “genuine quantum” correlation [5]. The proposal predicts $Q_2^{\rightarrow} = 0$ for classical–quantum (CQ) states, which include CC states. In Eq. (1), measuring Alice in X prepares orthogonal branch states for Bob and achieves the one-bit optimum. Yet the MUB Z gives

$$Q_2^{\rightarrow} \geq 0.1908745046\dots > 0 \quad (13)$$

on a CC state, directly violating that null property.

1SSDI steering.— Here steering asks whether the observed data can be explained by a bounded hidden variable on one side and pre-existing local quantum states on the other. Such an explanation is a local hidden-variable/local-hidden-state (LHV–LHS) model. A later work claimed universally that $Q_2^{\rightarrow} > 0$ demonstrates two-setting 1SSDI steering [4]. Here the two product branches in Eq. (1) are already an explicit two-valued LHV–LHS model, and its hidden-variable dimension 2 obeys the stipulated $2 \leq d_A = 3$. The state is therefore unsteerable in the stated model despite Eq. (13).

Conditional-probability entanglement score.— For a basis M , let a_i and b_i denote Alice’s and Bob’s outcomes assigned the same label i . The score $\mathcal{S}_M = \sum_i p(a_i|b_i)$ sums the probabilities that Alice obtains the paired outcome a_i conditioned on Bob obtaining b_i . It was conjectured that separable states obey $1 \leq \mathcal{S}_X + \mathcal{S}_Z \leq d + 1$ [3]. With the fixed same-index pairing used in that definition, the qutrit tables of Eq. (1) give $\mathcal{S}_X + \mathcal{S}_Z = 0.8$. The original work noted that the pairing is arbitrary but did not optimize it. Even the natural repair that maximizes over a separate outcome permutation in each setting fails at the upper end: an explicit full-rank separable $d = 4$ state gives $5.0710794\dots > 5$. The constructions and exhaustive assignment check are given in Sec. S4 of the Supplemental Material.

Scope.— The following claims fail: the universal CQC and ECQC bounds, the claimed CQ/CC-null property of $Q_2^{\rightarrow}$, its universal bridge to 1SSDI steering, and the conjectured conditional-probability interval. Where such a statement was a theorem or certification implication, the counterexample shows that its conclusion cannot hold universally. Entropic-uncertainty relations, the independently proved mutual-information entanglement criterion of Ref. [3], and other MUB witnesses with independent separable bounds [6, 11] remain intact. Nor is this a generic attack on QKD, device-independent security, or finite-key analysis; a cryptographic consequence requires its specified source, side-information, and adversary assumptions. Practically, the two-branch CC source can calibrate an unchanged protocol before quantum, steering, or cryptographic meaning is assigned to its score. Failure exposes a classical false positive; passing is only a necessary check, not a complete resource proof.

Discussion.—

Complementarity constrains fine-grained questions asked of one quantum system, but it does not stop separate experiments from rereading a classical common cause. This distinction is invisible in basis overlaps yet decisive for additive scores. Our null test makes it operational: multisetting certification should first survive the same classical source across its entire pipeline. A complete resource claim must then bound all allowed classical or separable sources; MUB geometry alone does not supply a common information budget.

The dimensional boundary is informative. For a qubit, the subspace orthogonal to $|x_0\rangle$ is spanned by $|x_1\rangle$, which has the same uniform Z statistics as $|x_0\rangle$. Our source therefore saturates rather than violates CQC at $d = 2$. Earlier numerical studies found no two-qubit counterexample [1], including subsequent tests based on sampling density matrices at fixed purity [12]. These results provided numerical evidence, but did not establish universal validity.

In subsequent companion work, we proved the CQC inequality for every two-qubit state and every pair of mutually unbiased local bases on each subsystem, without restrictions on rank, marginals, or separability [13]. That proof combines a qubit information-exclusion tradeoff with data processing under local dephasing. Together with the explicit counterexamples constructed here for every $d \geq 3$, it establishes a sharp dimensional boundary for the universal CQC inequality on $\mathbb{C}^d \otimes \mathbb{C}^d$: it holds for all states at $d = 2$, whereas counterexamples exist in every dimension $d \geq 3$. The two works therefore resolve the two-basis CQC question across equal local dimensions; the ECQC and certification counterexamples remain separate conclusions of the present work.

Subsequent work by Qian [14] gives different rank-two separable families covering unequal dimensions $m \times n$ with $m, n \geq 3$, as well as qubit–qudit counterexamples and a state-dependent corrected inequality. Those re-

sults extend the dimensional scope of CQC failure. The present Letter instead isolates a classical null-test mechanism and its separate ECQC and resource-certification consequences; the equal-dimension boundary does not classify arbitrary unequal local dimensions.

K.C. acknowledges support from the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant No. XDB1680102. OpenAI GPT 5.6 Sol assisted with exploratory search, literature organization, and error checking. The authors directed these uses, independently verified the constructions, calculations, and source claims, and take responsibility for the scientific content.

Data and code availability.— No experimental data were generated. Independent executable certificates for all numerical values and counterexamples are available with the source of arXiv:2608.03828v3.

* Contact author: chenkun@itp.ac.cn

- [1] J. Schneeloch, C. J. Broadbent, and J. C. Howell, Uncertainty relation for mutual information, *Physical Review A* **90**, 062119 (2014).
- [2] H. Iqbal, On the CQC conjecture: A sufficient condition and an extension, *Quantum Information Processing* **25**, 250 (2026).
- [3] L. Maccone, D. Bruß, and C. Macchiavello, Complementarity and correlations, *Physical Review Letters* **114**, 130401 (2015).
- [4] C. Jebarathinam, D. Das, H.-Y. Ku, D. Sarkar, and H.-S. Goan, Operational simultaneous correlations in complementary bases of bipartite states via one-sided semi-device-independent steering, *Physical Review A* **111**, 062403 (2025).
- [5] S. Wu, Z. Ma, Z. Chen, and S. Yu, Reveal quantum correlation in complementary bases, *Scientific Reports* **4**, 4036 (2014).
- [6] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B. C. Hiesmayr, Entanglement detection via mutually unbiased bases, *Physical Review A* **86**, 022311 (2012).
- [7] Y. Guo and S. Wu, Quantum correlation exists in any non-product state, *Scientific Reports* **4**, 7179 (2014).
- [8] S. Kanjilal, A. Khan, C. Jebarathinam, and D. Home, Remote state preparation using correlations beyond discord, *Physical Review A* **98**, 062320 (2018).
- [9] S. Wu, U. V. Poulsen, and K. Mølmer, Correlations in local measurements on a quantum state, and complementarity as an explanation of nonclassicality, *Physical Review A* **80**, 032319 (2009).
- [10] See Supplemental Material at [URL will be inserted by publisher] for full derivations, supporting constructions, and executable-check documentation.
- [11] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Entropic uncertainty relations and their applications, *Reviews of Modern Physics* **89**, 015002 (2017).
- [12] P. M. Alsing, C. C. Tison, J. Schneeloch, R. J. Birrittella, and M. L. Fanto, Distribution of density matrices at fixed purity for arbitrary dimensions, *Physical Review Research* **4**, 043114 (2022).
- [13] J. Wang, Q. Wang, and K. Chen, Complementary quantum correlations are universal for qubits (2026), public preprint; author order updated in the jointly submitted companion Letter, arXiv:2608.04916 [quant-ph].
- [14] L. Qian, Separable counterexamples to complementary quantum correlations, and why random search missed them (2026), version 2, arXiv:2608.14806 [quant-ph].