

# Exact Quantum Values and Permutation-Blind Maximizers in Cyclic Bell Inequalities

Sharp operator bounds, equality structure, and limits of Bell-value randomness certification

Alec Kriebel

Independent Researcher

me@aleckriebel.com    ORCID: 0009-0001-9320-500X

9 August 2026

## Abstract

Perito, D’Avino, Jung, Mironowicz, Acín, and Augusiak introduced two cyclic Bell families designed for efficient certification of maximal global randomness. For the first reduced operator they proved the general bound  $d\sqrt{2}$ , supplied an attaining strategy of value  $2\csc(\pi/(2d))$ , and conjectured that this sharper value is exact. We prove that formula in every dimension; the polar-decomposition argument also applies to commuting-operator realizations. Its scalar equality phases yield two complementary structural results. Every attained finite-dimensional tensor-product exact maximizer of the first augmented family has, on the support of Alice’s reduced state, all  $d$  equality roots with equal multiplicity, so  $d$  divides the supported dimension. At the same time, conditional permutations of those phases generate a large orbit of exact maximizers invisible to all first-harmonic correlators in the score. For every  $d \geq 4$ , a final-two swap maximizes both augmented cyclic families while producing a nonuniform designated joint-output distribution. Thus maximal value of the displayed scalar functional alone does not certify the proposed uniform  $2\log_2 d$  bits or uniquely determine the canonical behavior. This does not challenge certification conditioned on the complete canonical behavior, nor determine the worst-case guessing probability. An exact  $d = 4$  certificate over  $\mathbb{Q}(\zeta_{16})$  accompanies the all-dimensional proofs.

## 1 Introduction

Bell inequalities can certify randomness without a model of the devices, but the conditioning data matter. A complete behavior  $p(a, b \mid x, y)$  contains far more information than one scalar Bell value. If a Bell maximum exposes a unique behavior, symmetries of the score may force uniform outputs and, with an operator-level argument, privacy against a purifying adversary. If the maximizing face contains several behaviors, the same symmetry argument need not apply to each of them [2, 3, 4].

Perito, D’Avino, Jung, Mironowicz, Acín, and Augusiak recently introduced two families built around cyclic Fourier correlators [1]. They defined the families, found explicit maximally-entangled strategies, and proved the general first-family bound  $d\sqrt{2}$ . Their strategy has value  $2\csc(\pi/(2d))$ ; they conjectured equality and confirmed it numerically through  $d = 6$  with the NPA hierarchy [5]. They also proved the exact value of the second reduced family by a sum-of-squares identity. Their symmetry analysis motivated maximal-global-randomness statements; for selected dimensions they evaluated Eve’s guessing probability numerically after fixing the complete canonical behavior. These are logically different inputs to a randomness problem.

| Topic                                | Originating work [1]                                                                                                                                     | This paper                                                                                                                                                                                                                           |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bell families                        | Introduced both cyclic families and their normalization                                                                                                  | Adopts the displayed Hermitian operator definitions, with a convention note                                                                                                                                                          |
| Attaining strategies                 | Supplied the canonical strategies and matching lower bounds                                                                                              | Rechecks admissibility and attainment exactly                                                                                                                                                                                        |
| First reduced value                  | Proved $\beta_q \leq d\sqrt{2}$ , supplied the lower value $2 \csc(\pi/(2d))$ , and conjectured equality; NPA evidence through $d = 6$                   | Proves the sharper all-dimensional upper bound and the $q = qa = qc$ equality                                                                                                                                                        |
| Second reduced value                 | Proved value $d$ by an SOS identity                                                                                                                      | Uses that SOS, including its commuting-operator reading                                                                                                                                                                              |
| Equality structure                   | Identified score symmetries and developed their randomness implications under a uniqueness hypothesis, without a complete maximizing-face classification | Proves the scalar phases, equal supported multiplicities for every attained finite-dimensional tensor-product exact maximizer of the first augmented family, and a conditional phase-permutation orbit with exact product hypotheses |
| Nonuniform phase-permuted maximizers | Focused on canonical realizations and their symmetry-based randomness implications                                                                       | Constructs biased exact maximizers of both augmented families for every $d \geq 4$                                                                                                                                                   |
| Canonical full behavior              | Randomness studied numerically in selected dimensions; second family self-tested at $d = 3$                                                              | Not contradicted                                                                                                                                                                                                                     |
| Scalar-value implication             | Maximal-violation certification proposed, with a uniqueness-based symmetry rationale                                                                     | Shows that the scalar maximum alone is insufficient for $d \geq 4$                                                                                                                                                                   |

Table 1: Attribution and logical scope. The present work does not claim the family definitions, canonical strategies, or second-family SOS.

The surrounding literature includes high-dimensional and modular Bell inequalities [6, 7, 8], self-testing from few measurements [9, 12], and analytic or algorithmic SOS constructions [11, 13]. Two contemporaneous works of the originating collaboration pursue all-dimensional global randomness and three-outcome noise robustness by different constructions [14, 15]. We use these works to set the attribution boundary; the family-specific polar bound and the phase-permuted maximizers below are not imported from them. To our knowledge, no prior work establishes either the first-family upper bound in this normalization or the nonuniform exact maximizers constructed here; the accompanying priority audit records the qualified search basis for that statement.

This paper unifies the exact-value and randomness questions through the equality phases of the first operator. The polar proof reduces its upper bound to a scalar roots-of-unity extremum. At equality the relative unitary may carry the full set of maximizing phases in different cyclic orders. Those orders leave the Bell-visible first harmonics unchanged, but they alter higher Fourier data and can change a complete output table. The same Bob observables also annihilate the sum-of-squares factors of Ref. [1], Eqs. (22)–(23), for the second family.

Our main conclusions are as follows.

1. The finite-dimensional tensor-product, approximate, and commuting-operator values of the first reduced cyclic operator are all  $2 \csc(\pi/(2d))$ .
2. Every attained finite-dimensional tensor-product exact maximizer of the first augmented family

has all equality roots with equal multiplicity on Alice's support; in particular,  $d$  divides that supported dimension.

3. A polar-linear permutation theorem gives explicit sufficient conditions under which phase permutations remain admissible maximizers and preserve the entire first-harmonic correlator matrix.
4. For each  $d \geq 4$ , one such maximizer has uniform local marginals but a nonuniform designated joint table. With trivial Eve this already gives a guessing probability strictly larger than  $1/d^2$ .
5. The same construction maximizes the second augmented cyclic family and has the same target table.
6. The result separates scalar Bell-value certification from certification conditioned on a fixed full behavior. It is not a claim about the exact worst-case guessing probability, the complete maximizing face, or the randomness of the canonical realization.

The exact value and support rigidity are proved in Sections 3–4; the explicit equality orbit is developed in Section 5; the two biased families are treated in Sections 6 and 7; and the randomness interpretation is isolated in Section 8. Section 9 collects the binary benchmark and sharply scoped low-setting design conditions.

## 2 Bell operators, behaviors, and randomness notions

Fix  $d \geq 2$ , write  $\omega = e^{2\pi i/d}$ , and identify outcomes with  $\mathbb{Z}_d$ . A projective  $d$ -outcome measurement  $\{M_a\}_{a \in \mathbb{Z}_d}$  is encoded by the order- $d$  unitary

$$A = \sum_{a=0}^{d-1} \omega^a M_a, \quad M_a = \frac{1}{d} \sum_{k=0}^{d-1} \omega^{-ak} A^k.$$

Zero spectral projections are allowed in the general definition. All explicit strategies below have the complete simple spectrum of  $d$ -th roots, so their outcomes are rank-one projectors.

For a matrix  $T$  written in the displayed computational basis,  $\bar{T}$  denotes entrywise complex conjugation, while  $T^T$  and  $T^\dagger$  denote its transpose and adjoint. The overbars in the separately defined names  $\bar{\mathcal{I}}_d$  and  $\bar{\mathcal{F}}_d$  indicate augmentation, not complex conjugation.

Let  $\mathcal{Q}_q$  denote the set of finite-dimensional tensor-product correlations, let  $\mathcal{Q}_{qa} = \overline{\mathcal{Q}_q}$ , and let  $\mathcal{Q}_{qc}$  denote the commuting-operator correlation set, in which Alice's and Bob's PVMs act on one Hilbert space and commute across parties. Thus

$$\mathcal{Q}_q \subseteq \mathcal{Q}_{qa} \subseteq \mathcal{Q}_{qc}.$$

For a Bell functional  $\mathcal{B}$ , write

$$\beta_\mu(\mathcal{B}) = \sup_{p \in \mathcal{Q}_\mu} \mathcal{B}(p), \quad \mu \in \{q, qa, qc\}.$$

The operator inequalities below hold in the commuting model; a matching finite-dimensional strategy then identifies all three values. The value theorem extends to the commuting-operator model because it is an operator inequality, whereas the support-rigidity and privacy results are stated only for finite-dimensional tensor-product strategies because their proofs use reduced-state supports,

Schmidt decompositions, and purifying-Eve conditional states; no commuting-operator analogue is claimed here.

For a behavior  $p(a, b \mid x, y)$ , a scalar Bell maximum fixes only one supporting hyperplane of the quantum correlation set. We distinguish:

- the value of a Bell functional;
- its full maximizing face;
- a selected canonical strategy and its canonical behavior;
- the complete observed behavior, including higher Fourier correlators;
- uniform observed target probabilities; and
- private randomness against a purifying adversary.

For a purification  $|\Psi\rangle_{ABE}$  and target settings  $(x_*, y_*)$ , let

$$\sigma_E^{ab} = \text{Tr}_{AB}[(M_a^{x_*} \otimes N_b^{y_*} \otimes \mathbf{1})|\Psi\rangle\langle\Psi|(M_a^{x_*} \otimes N_b^{y_*} \otimes \mathbf{1})].$$

Eve's guessing probability is

$$G(AB \mid x_*, y_*, E) = \max_{\{Q_{ab}\}} \sum_{a,b} \text{Tr}(Q_{ab} \sigma_E^{ab}).$$

For model-dependent optimizations below,  $\mathfrak{S}_q$  denotes finite-dimensional tripartite tensor-product strategies, including Eve's  $d^2$ -outcome guessing POVM;  $\mathfrak{S}_{qa}$  is the closure of the resulting finite extended correlations; and  $\mathfrak{S}_{qc}$  consists of a vector state and three party algebras on one Hilbert space that commute pairwise across parties, with Eve's guessing POVM in her algebra. This fixes the adversarial extension rather than leaving  $q$ ,  $qa$ , or  $qc$  implicit in a guessing quantity.

Maximal private global randomness means  $\sigma_E^{ab} = \rho_E/d^2$  for every  $a, b$ , and implies  $G = 1/d^2$ . Uniform probabilities are necessary but not sufficient for this operator-valued condition. Conversely, one explicit nonuniform target table, even with one-dimensional Eve, is enough to rule out maximal private randomness for that realization.

*Remark 2.1* (Normalization convention). Version 3 of Ref. [1] has a localized normalization discrepancy: the displayed reduced value in its Eq. (17) and its  $d = 3$  augmented value agree with the operator definition, while the formula printed beside its first augmented randomness conjecture contains an additional factor  $d$  in the denominator. We take the displayed Hermitian operator as authoritative. Thus the reduced and augmented values in our convention are respectively

$$M_d = 2 \csc\left(\frac{\pi}{2d}\right), \quad M_d + 1.$$

Appendix G records the corresponding adjoint conventions. Nothing in our argument uses the typographical discrepancy.

### 3 Exact value of the first cyclic operator

For commuting Alice and Bob unitaries define

$$\mathcal{I}_d = \sum_{y=0}^{d-1} \text{Re}[(A_0 + \omega^y A_1) B_y]. \quad (1)$$

In the tensor model the product in (1) means a tensor product. The order- $d$  relations are part of the Bell scenario, but will not be needed for the upper bound.

**Theorem 3.1** (Sharp commuting-operator value). *Let  $A_0, A_1, B_0, \dots, B_{d-1}$  be unitaries on an arbitrary complex Hilbert space and suppose  $[A_x, B_y] = 0$  for every  $x, y$ . Then*

$$\mathcal{I}_d \leq M_d \mathbf{1}, \quad M_d = 2 \csc\left(\frac{\pi}{2d}\right). \quad (2)$$

After imposing the order- $d$  measurement relations,

$$\boxed{\beta_q(\mathcal{I}_d) = \beta_{qa}(\mathcal{I}_d) = \beta_{qc}(\mathcal{I}_d) = M_d} \quad (d \geq 2).$$

The proof has two independent ingredients. The first is an operator identity that remains valid when a polar factor has a kernel.

**Lemma 3.2** (Polar positive-factor identity). *Let  $\mathcal{A}, \mathcal{B} \subseteq \mathcal{B}(\mathcal{H})$  be commuting unital  $*$ -algebras, let  $C \in \mathcal{A}$ , let  $C = V|C|$  be its canonical polar decomposition, and let  $B \in \mathcal{B}$  be unitary. Put*

$$P_{C,B} = |C^\dagger|^{1/2} - V|C|^{1/2}B.$$

Then

$$\frac{|C| + |C^\dagger|}{2} - \operatorname{Re}(CB) = \frac{1}{2}P_{C,B}^\dagger P_{C,B}. \quad (3)$$

*Proof.* Put  $\mathcal{M} = \mathcal{A}''$ , the von Neumann algebra generated by  $\mathcal{A}$ . Because  $C \in \mathcal{A}$ , continuous functional calculus places  $|C|$ , its square root, and  $(|C| + \varepsilon \mathbf{1})^{-1}$  in  $\mathcal{M}$  for every  $\varepsilon > 0$ . Strong closure then places its support projection there, since

$$\operatorname{supp}|C| = \lim_{\varepsilon \downarrow 0} |C|(|C| + \varepsilon \mathbf{1})^{-1}.$$

The canonical polar partial isometry belongs to the same algebra; explicitly,

$$V = \lim_{\varepsilon \downarrow 0} C(|C| + \varepsilon \mathbf{1})^{-1}.$$

Indeed, the right-hand side is  $V|C|(|C| + \varepsilon \mathbf{1})^{-1}$ , which converges strongly to  $V \operatorname{supp}|C| = V$ . Elementwise commutation of the two original algebras gives  $\mathcal{B} \subseteq \mathcal{A}'$ ; since  $\mathcal{M} = (\mathcal{A}')'$ , every element of  $\mathcal{M}$ , in particular  $V$  and the functional-calculus factors above, commutes with  $B$ . This is the only closure step needed in the commuting-operator model.

The initial projection  $V^\dagger V$  is the support projection of  $|C|$ , while polar functional calculus gives

$$|C^\dagger|^{1/2}V = V|C|^{1/2}, \quad |C^\dagger|^{1/2}V|C|^{1/2} = C.$$

Expanding yields

$$P_{C,B}^\dagger P_{C,B} = |C^\dagger| + |C| - CB - B^\dagger C^\dagger.$$

No inverse and no unitary extension of  $V$  has been used.  $\square$

The second ingredient is a scalar equality calculation; its elementary parity-split proof is included in Appendix A.

**Lemma 3.3** (Roots-of-unity extremum). *For  $z \in \mathbb{T}$ ,*

$$\sum_{y=0}^{d-1} |1 + \omega^y z| \leq M_d. \quad (4)$$

*Equality holds exactly when*

$$z^d = (-1)^{d-1}. \quad (5)$$

*Proof of Theorem 3.1.* Set

$$L_y = A_0 + \omega^y A_1, \quad U = A_0^\dagger A_1, \quad M_y = \mathbf{1} + \omega^y U.$$

Then  $L_y = A_0 M_y$ . The operator  $M_y$  is normal because

$$M_y^\dagger M_y = M_y M_y^\dagger = 2\mathbf{1} + \omega^y U + \omega^{-y} U^\dagger.$$

Consequently

$$|L_y| = |M_y|, \quad |L_y^\dagger| = A_0 |M_y| A_0^\dagger.$$

Put

$$F_d(U) = \sum_{y=0}^{d-1} |\mathbf{1} + \omega^y U|.$$

Continuous functional calculus for the unitary  $U$ , applied to Lemma 3.3, gives  $0 \leq F_d(U) \leq M_d \mathbf{1}$ . Summing Lemma 3.2 now gives

$$\mathcal{I}_d \leq \frac{1}{2} (F_d(U) + A_0 F_d(U) A_0^\dagger) \leq M_d \mathbf{1}.$$

All functional-calculus operators used here lie in the von Neumann algebra generated by Alice's observables and therefore commute with Bob's algebra by the argument in Lemma 3.2. Thus no tensor-factor decomposition, finite-dimensional trace, or cyclicity assumption enters the upper bound. The finite order- $d$  strategy rechecked in Appendix C attains  $M_d$ . The inclusions among  $q, qa, qc$  then prove all three equalities.  $\square$

For later equality arguments it is useful to retain the complete gap. If  $L_y = V_y |L_y|$ , define  $P_y = P_{L_y, B_y}$  and  $G = (M_d \mathbf{1} - F_d(U))^{1/2}$ . Then

$$\boxed{M_d \mathbf{1} - \mathcal{I}_d = \frac{1}{2} \sum_y P_y^\dagger P_y + \frac{1}{2} G^\dagger G + \frac{1}{2} (G A_0^\dagger)^\dagger (G A_0^\dagger).} \quad (6)$$

This is an operator identity, not a finite-level NPA certificate. At the operator level, scalar functional calculus also gives

$$F_d(U) = M_d \mathbf{1} \iff U^d = (-1)^{d-1} \mathbf{1}.$$

For an individual maximizing vector  $|\psi\rangle$ , however, the exact conclusion from (6) is only

$$P_y |\psi\rangle = 0 \quad (0 \leq y < d), \quad G |\psi\rangle = 0, \quad G A_0^\dagger |\psi\rangle = 0.$$

These vector-level relations do not yield a global relation for  $U$ , a description outside the state support, or a classification of all maximizing realizations. In finite dimension, however, the stabilizer supplied by the augmented term upgrades them to the support-level spectral restriction in Section 4.

**Corollary 3.4** (First augmented family). *For*

$$\bar{\mathcal{I}}_d = \mathcal{I}_d + \text{Re}(A_0 B_d)$$

*with a further order- $d$  Bob observable,*

$$\beta_q(\bar{\mathcal{I}}_d) = \beta_{qa}(\bar{\mathcal{I}}_d) = \beta_{qc}(\bar{\mathcal{I}}_d) = M_d + 1.$$

*Proof.* The upper bound follows from Theorem 3.1 and  $\text{Re}(A_0 B_d) \leq 1$ . The finite strategy in Appendix C, with the aligned added observable, attains equality.  $\square$

The exact formula gives a direct check against the numerical evidence in the originating paper:

| $d$ | Exact value $M_d$        | Decimal     | Source comparison   |
|-----|--------------------------|-------------|---------------------|
| 2   | $2\sqrt{2}$              | 2.828427... | analytic CHSH value |
| 3   | 4                        | 4.000000... | NPA 1 + $AB$        |
| 4   | $2\sqrt{4 + 2\sqrt{2}}$  | 5.226252... | NPA 1 + $AB$        |
| 5   | $2(1 + \sqrt{5})$        | 6.472136... | NPA level 2         |
| 6   | $2(\sqrt{6} + \sqrt{2})$ | 7.727407... | NPA level 2         |

Table 2: Low-dimensional exact values. The source NPA bounds, displayed there in truncated decimal form, agree with these values to the reported precision; its analytic  $d\sqrt{2}$  bound is tight only at  $d = 2$ .

Appendix C also derives the two source Fourier sums and the explicit qutrit Bob observable, fixing the phase, transpose, and complex-conjugation conventions rather than identifying the strategies only through their common value.

## 4 Finite-dimensional support-level equality rigidity

The equality certificate yields additional information at the precise scope below once the first cyclic operator is augmented by its aligned term. The following result concerns every attained finite-dimensional tensor-product exact maximizer of the first augmented family. It does not extend silently to  $qa$  or  $qc$ .

**Theorem 4.1** (Equal supported multiplicities). *Let a finite-dimensional tensor-product strategy with order- $d$  observables and state  $\rho_{AB}$  attain*

$$\langle \bar{\mathcal{I}}_d \rangle = M_d + 1.$$

*For a purification  $|\Psi\rangle_{ABE}$ , put*

$$\rho_A = \text{Tr}_{BE} |\Psi\rangle\langle\Psi|, \quad K = \text{supp } \rho_A, \quad U = A_0^\dagger A_1.$$

*Then  $K$  reduces the relative unitary  $U$ , and every root of  $z^d = (-1)^{d-1}$  occurs in  $\text{spec}(U|_K)$  with the same multiplicity. Consequently,*

$$d \mid \dim K.$$

*No conclusion is asserted on  $K^\perp$ , for approximate maximizers, or for general commuting-operator realizations.*

The proof, given in Appendix B, starts from the individual vanishing of every positive residual in (6) and of the augmented stabilizer. A Schmidt- support cancellation lemma moves those vector relations to  $K$ . Kernel- safe polar cancellation then makes each polar partial isometry unitary on  $K$ , adjacent half-angle phases produce one reflection for each equality root, and a rank inequality forces all root multiplicities to agree.

Equal supported multiplicities are necessary but do not imply a Weyl representation, uniqueness, or self-testing. In particular, every explicit permutation maximizer below has  $K = \mathbb{C}^d$  and is compatible with the theorem.

## 5 Equality phases and permutation blindness

The scalar equality set in (5) is a set, not an ordering. A Bell score built only from first powers can therefore fail to record how those phases are arranged along a weighted cycle. The following general statement isolates the exact sufficient conditions. It does not claim to classify every maximizer of every polar-linear functional.

Let  $R$  be a finite coefficient index set, let  $g_r(z) = \alpha_r + \beta_r z$ , and put

$$f(z) = \sum_{r \in R} |g_r(z)|, \quad M = \max_{z \in \mathbb{T}} f(z).$$

For order- $d$  observables define

$$\mathcal{J} = \sum_{r \in R} \operatorname{Re}[(\alpha_r A_0 + \beta_r A_1) B_r] + \operatorname{Re}(A_0 B_*). \quad (7)$$

**Theorem 5.1** (Conditional phase-permutation theorem). *Suppose there are labeled phases  $z_j, s_{rj} \in \mathbb{T}$ ,  $0 \leq j < d$ , such that*

$$f(z_j) = M, \quad \prod_j z_j = 1,$$

*and, for every  $r$ ,*

$$s_{rj} |g_r(z_j)| = g_r(z_j), \quad \prod_j s_{rj} = 1.$$

*At a zero of  $g_r$ ,  $s_{rj}$  may be any unitary extension phase. For every permutation  $\kappa$  of the labels, set on  $\mathbb{C}^d$*

$$\begin{aligned} A_0 &= X, & A_1 &= X \operatorname{diag}(z_{\kappa_j}), \\ B_r &= \overline{X \operatorname{diag}(s_{r, \kappa_j})}, & B_* &= X, \end{aligned} \quad (8)$$

*where  $X|j\rangle = |j+1 \bmod d\rangle$ , and use  $|\Phi_d\rangle = d^{-1/2} \sum_j |j, j\rangle$ . Then:*

- (i) every displayed observable is unitary, has  $d$ -th power  $\mathbf{1}$ , and has the full simple  $d$ -th-root spectrum;*
- (ii) the strategy attains the operator upper bound  $M + 1$  for (7); and*
- (iii) all local first moments and every complex first-harmonic correlator  $\langle A_x B_r \rangle$ ,  $\langle A_x B_* \rangle$  are independent of  $\kappa$ .*

*Proof.* With  $U = A_0^\dagger A_1$  and  $L_r = A_0 g_r(U) = V_r |L_r|$ , Lemma 3.2 and functional calculus give

$$(M+1)\mathbf{1} - \mathcal{J} = \frac{1}{2} \sum_r P_r^\dagger P_r + \frac{1}{2} R_*^\dagger R_* + \frac{1}{2} (H + A_0 H A_0^\dagger),$$

where

$$P_r = |L_r^\dagger|^{1/2} - V_r |L_r|^{1/2} B_r, \quad R_* = \mathbf{1} - A_0 B_*, \quad H = M\mathbf{1} - f(U) \geq 0.$$

Thus  $M+1$  is an operator upper bound.

For arbitrary nonzero weights  $t_j$ ,

$$(X \operatorname{diag}(t_j))^d = \left( \prod_j t_j \right) \mathbf{1}, \quad (9)$$

and its characteristic polynomial is  $t^d - \prod_j t_j$ . The product hypotheses therefore prove (i). Moreover, for each  $r$ , put

$$W_r = X \operatorname{diag}(s_{r,\kappa_j}), \quad E_r = \operatorname{supp}|L_r|.$$

Then

$$L_r = W_r |L_r|, \quad V_r = W_r E_r,$$

where  $V_r$  is the canonical polar partial isometry appearing in  $P_r$ . Consequently

$$V_r |L_r|^{1/2} = W_r E_r |L_r|^{1/2} = W_r |L_r|^{1/2};$$

the phases extending  $W_r$  on  $\ker L_r$  do not enter the positive residual. Since  $B_r = \overline{W_r}$ , one has  $B_r^T = W_r^\dagger$ , and therefore

$$V_r |L_r|^{1/2} B_r^T = W_r |L_r|^{1/2} W_r^\dagger = |L_r^\dagger|^{1/2}.$$

The vectorization identity

$$(R \otimes S)|\Phi_d\rangle = (RS^T \otimes \mathbf{1})|\Phi_d\rangle$$

now gives  $P_r|\Phi_d\rangle = 0$ , including when  $g_r(U)$  has a kernel. Moreover,  $f(U) = M\mathbf{1}$ , because every  $z_{\kappa_j}$  is a maximizing phase, and

$$(A_0 \otimes B_*)|\Phi_d\rangle = (X \otimes X)|\Phi_d\rangle = |\Phi_d\rangle.$$

Thus every factor in the displayed gap annihilates  $|\Phi_d\rangle$ , proving (ii). Finally, the maximally-entangled trace identity gives

$$\begin{aligned} \langle A_0 B_r \rangle &= \frac{1}{d} \sum_j \overline{s_{rj}}, & \langle A_1 B_r \rangle &= \frac{1}{d} \sum_j z_j \overline{s_{rj}}, \\ \langle A_0 B_* \rangle &= 1, & \langle A_1 B_* \rangle &= \frac{1}{d} \sum_j z_j. \end{aligned}$$

These are symmetric sums of the labeled data. Every local observable is a weighted shift and has zero trace. This proves (iii).  $\square$

The theorem explains both its power and its limit. It gives a concrete permutation orbit within a maximizing face, but it says nothing about maximizers whose relative spectrum is different, has different multiplicities, acts reducibly, or uses a kernel outside the stated phase data. Claims about the complete maximizing face require separate rigidity analysis.

## 6 Exact nonuniform maximizers of the first family

Put

$$\delta_d = \begin{cases} 0, & d \text{ odd}, \\ 1, & d \text{ even}, \end{cases} \quad z_k = \exp\left(\frac{\pi i(2k + \delta_d)}{d}\right). \quad (10)$$

These are precisely the roots in (5). For  $0 \leq y, k < d$ , define

$$s_{y,k} = \frac{1 + \omega^y z_k}{|1 + \omega^y z_k|}.$$

The denominator never vanishes. The polynomial  $t^d - (-1)^{d-1}$  gives

$$\prod_k z_k = 1, \quad \prod_k (1 + \omega^y z_k) = 2, \quad \prod_k s_{y,k} = 1. \quad (11)$$

Thus Theorem 5.1 applies with  $g_y(z) = 1 + \omega^y z$ .

For every permutation  $\kappa$ , the explicit first-family strategy is

$$\begin{aligned} A_0 &= X, & A_1 &= X Z_\kappa, & Z_\kappa &= \text{diag}(z_{\kappa_j}), \\ V_y &= X \text{diag}(s_{y,\kappa_j}), & B_y &= \overline{V_y}, & B_d &= X. \end{aligned} \quad (12)$$

Each observable defines a rank-one projective  $d$ -outcome measurement and

$$\langle \overline{\mathcal{I}}_d \rangle = M_d + 1.$$

The Bell-visible correlators are independent of the ordering. Explicitly, with  $\alpha_d = \csc(\pi/(2d))$ ,

$$\langle A_0 B_y \rangle = \frac{\alpha_d}{d}, \quad \langle A_1 B_y \rangle = \frac{\alpha_d \omega^{-y}}{d}, \quad \langle A_0 B_d \rangle = 1, \quad \langle A_1 B_d \rangle = 0. \quad (13)$$

The cyclic ordering  $\kappa_j = j$  reproduces the canonical first-harmonic behavior. Other orderings can change higher powers and full probabilities.

To calculate the designated pair  $(A_1, B_d)$ , set

$$q_0 = 1, \quad q_{j+1} = z_{\kappa_j} q_j, \quad \hat{q}_m = \sum_{j=0}^{d-1} q_j \omega^{mj}. \quad (14)$$

The product condition makes the sequence cyclic, so extend it by  $q_{j+d} = q_j$ , and put  $Q = \text{diag}(q_j)$ . The recurrence gives  $A_1 = Q X Q^\dagger$ . Define

$$|u_c\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{-cj} |j\rangle, \quad |v_a\rangle = Q |u_a\rangle.$$

Then

$$X |u_c\rangle = \omega^c |u_c\rangle, \quad A_1 |v_a\rangle = \omega^a |v_a\rangle,$$

so these are the outcome eigenvectors under the encoding  $A = \sum_a \omega^a M_a$ . The transpose of the outcome- $b$  projector of  $B_d = X$  is the projector onto  $\overline{u}_b = u_{-b}$ . Hence the maximally-entangled trace identity gives

$$\begin{aligned} p_\kappa(a, b \mid 1, d) &= \frac{1}{d} |\langle u_{-b} \mid v_a \rangle|^2 \\ &= \frac{1}{d^3} \left| \sum_{j=0}^{d-1} q_j \omega^{-(a+b)j} \right|^2 = \frac{|\hat{q}_{-(a+b)}|^2}{d^3}. \end{aligned} \quad (15)$$

Parseval gives  $\sum_m |\widehat{q}_m|^2 = d^2$ . Consequently both local marginals are exactly  $1/d$ , while the joint table is uniform if and only if every squared Fourier magnitude equals  $d$ .

The canonical ordering is Fourier-flat in every dimension. Indeed, for  $\kappa_j = j$ , the recurrence gives

$$q_j = \eta^{j(j-1+\delta_d)}, \quad \eta = e^{\pi i/d},$$

and the parity choice in  $\delta_d$  makes this formula cyclic. Reading indices cyclically, its autocorrelations are

$$R_t := \sum_{j=0}^{d-1} q_{j+t} \overline{q_j} = \eta^{t(t-1+\delta_d)} \sum_{j=0}^{d-1} \omega^{tj} = \begin{cases} d, & t = 0, \\ 0, & 1 \leq t < d. \end{cases}$$

Therefore

$$|\widehat{q}_m|^2 = \sum_{t=0}^{d-1} R_t \omega^{mt} = d$$

for every  $m$ , and the canonical target table is exactly  $1/d^2$ .

**Theorem 6.1** (Biased exact maximizers). *For every  $d \geq 4$ , choose the final-two swap*

$$\kappa = (0, 1, \dots, d-3, d-1, d-2). \quad (16)$$

*The strategy (12) attains  $M_d + 1$ , has uniform local marginals, and has a nonuniform target table. With one-dimensional Eve,*

$$G(AB \mid 1, d, E) \geq \frac{1}{d^2} + \frac{2 \sin(\pi/d) \sin(3\pi/d)}{d^2(d-1)} > \frac{1}{d^2}. \quad (17)$$

*Proof.* The second cyclic autocorrelation of (14) is

$$R_2 = \sum_j q_{j+2} \overline{q_j} = \sum_j z_{\kappa_j} \overline{z_{\kappa_{j+1}}}.$$

It vanishes for the cyclic ordering. The swap (16) gives

$$R_2 = (z_{d-1} - z_{d-2})(z_{d-3} - z_0), \quad |R_2| = 4 \sin(\pi/d) \sin(3\pi/d) > 0. \quad (18)$$

Hence the Fourier magnitudes are not all  $d$ .

For the quantitative estimate put  $x_m = |\widehat{q}_m|^2 - d$  and  $\Delta = \max_m x_m$ . Fourier inversion at lag two gives

$$R_2 = \frac{1}{d} \sum_m x_m \omega^{-2m},$$

where the constant term vanishes for  $d \geq 4$ . Since the nonzero mean-zero sequence  $(x_m)$  has at most  $d-1$  positive entries,

$$d|R_2| \leq \sum_m |x_m| = 2 \sum_{x_m > 0} x_m \leq 2(d-1)\Delta.$$

With trivial Eve, always guessing a most likely pair gives  $G = (d+\Delta)/d^3$ . Substituting (18) proves (17).  $\square$

For  $d = 2, 3$ , every ordering in this particular permutation family is Fourier-flat. Indeed, for any permutation  $\kappa$ ,

$$R_1 = \sum_j q_{j+1} \overline{q_j} = \sum_j z_{\kappa_j} = \sum_k z_k = 0, \quad R_{d-t} = \overline{R_t}.$$

For  $d = 2$ ,  $R_1$  is the only nonzero-lag autocorrelation; for  $d = 3$ , the only such autocorrelations are  $R_1$  and  $R_2 = \overline{R_1}$ . Thus all nonzero-lag autocorrelations vanish and  $|\widehat{q}_m|^2 = d$  for every  $m$ . This leaves Bell-value rigidity in those dimensions unresolved.

## 7 Extension to the second augmented cyclic family

The second reduced family of Ref. [1] has a different Alice measurement set but compresses the same first-family Bob observables. Put  $\eta = e^{\pi i/d}$ , so  $\omega = \eta^2$ , and define

$$\lambda_\ell = \frac{(-1)^{\ell-1} \eta^{\ell(\ell-1)}}{d \sin(\pi(\ell - \frac{1}{2})/d)}, \quad 0 \leq \ell < d, \quad (19)$$

where  $(-1)^{-1} = -1$  at  $\ell = 0$ . For Bob's observables in (12), let

$$\widehat{B}_\ell = \sum_{y=0}^{d-1} \omega^{\ell y} B_y$$

and define the Hermitian functional

$$\mathcal{F}_d = \sum_{\ell=0}^{d-1} \operatorname{Re}(\overline{\lambda_\ell} A_\ell \widehat{B}_\ell), \quad \overline{\mathcal{F}}_d = \mathcal{F}_d + \operatorname{Re}(A_0 B_d). \quad (20)$$

**Lemma 7.1** (Coefficient normalization). *The coefficients in (19) satisfy*

$$\sum_{\ell=0}^{d-1} |\lambda_\ell|^2 = 1.$$

*Proof.* The logarithmic derivative of the sine product gives, away from its poles,

$$\sum_{k=0}^{d-1} \cot\left(x + \frac{k\pi}{d}\right) = d \cot(dx).$$

Differentiating yields the general identity

$$\sum_{k=0}^{d-1} \csc^2\left(x + \frac{k\pi}{d}\right) = d^2 \csc^2(dx). \quad (21)$$

At  $x = -\pi/(2d)$ , the right-hand side is  $d^2$ . Since the numerator of every  $\lambda_\ell$  has modulus one,

$$\sum_{\ell=0}^{d-1} |\lambda_\ell|^2 = \frac{1}{d^2} \sum_{\ell=0}^{d-1} \csc^2\left(\frac{\pi(\ell - \frac{1}{2})}{d}\right) = 1.$$

□

The SOS of Ref. [1], Eqs. (22)–(23), with prefactor  $1/(2d)$ , is short and load-bearing. Fourier orthogonality and unitarity of the  $B_y$ 's give

$$\sum_{\ell} \widehat{B}_{\ell}^{\dagger} \widehat{B}_{\ell} = d^2 \mathbf{1}, \quad \sum_{\ell} |\lambda_{\ell}|^2 = 1.$$

Thus, for  $P_{\ell} = d\lambda_{\ell} \mathbf{1} - A_{\ell} \widehat{B}_{\ell}$ ,

$$d\mathbf{1} - \mathcal{F}_d = \frac{1}{2d} \sum_{\ell=0}^{d-1} P_{\ell}^{\dagger} P_{\ell}. \quad (22)$$

The identity requires only cross-party commutation, so the source value also has the immediate commuting-operator reading

$$\beta_q(\mathcal{F}_d) = \beta_{qa}(\mathcal{F}_d) = \beta_{qc}(\mathcal{F}_d) = d, \quad \beta_q(\overline{\mathcal{F}}_d) = \beta_{qa}(\overline{\mathcal{F}}_d) = \beta_{qc}(\overline{\mathcal{F}}_d) = d + 1.$$

**Theorem 7.2** (Permutation maximizers of the second family). *For every permutation  $\kappa$ , define*

$$r_{\ell} = \eta^{-\ell(\ell-1+\delta_d)}, \quad D_{\ell} = r_{\ell} X \operatorname{diag}(\omega^{-\ell\kappa_j}), \quad A_{\ell} = \overline{D_{\ell}}. \quad (23)$$

*Together with the  $B_y$ 's in (12), these are order- $d$  observables and*

$$\widehat{B}_{\ell} = d\lambda_{\ell} D_{\ell}. \quad (24)$$

*They annihilate every factor in (22). With  $B_d = X$ , the augmented value is  $d + 1$ . For the swap (16), the target pair  $(A_1, B_d)$  has exactly the table (15) and the gap (17) for every  $d \geq 4$ . The complete matrix of complex first-harmonic correlators is independent of  $\kappa$ . Under the alternative source-appendix convention that adjoints all Bob observables, the target table is the same up to the harmless outcome inversion  $b \mapsto -b$ .*

*Proof.* For  $z_t = \eta^{2t+\delta_d}$ , write

$$s_{0,t} = \varepsilon_t \eta^{t+\delta_d/2}, \quad \varepsilon_t = \begin{cases} +1, & 2t + \delta_d < d, \\ -1, & 2t + \delta_d > d. \end{cases}$$

There is no equality case, and  $s_{y,t} = s_{0,t+y \bmod d}$ . The diagonal weight of  $\widehat{B}_{\ell}$  at a label  $t$  is therefore  $\omega^{-\ell t} S_{\ell}$ , with

$$S_{\ell} = \sum_t \omega^{\ell t \overline{s_{0,t}}}.$$

Let  $n = (d + 1 - \delta_d)/2$  and  $u_{\ell} = \eta^{2\ell-1}$ . Since  $u_{\ell}^d = -1$ , two geometric sums give

$$S_{\ell} = \eta^{-\delta_d/2} \left( \sum_{t=0}^{n-1} u_{\ell}^t - \sum_{t=n}^{d-1} u_{\ell}^t \right) = d\lambda_{\ell} r_{\ell}.$$

This is (24), including its phase.

By (9) and  $\sum_j \kappa_j = d(d-1)/2$ ,

$$D_{\ell}^d = (-1)^{\ell(\ell-1+\delta_d)+\ell(d-1)} \mathbf{1} = \mathbf{1},$$

because  $\ell(\ell + d - 2 + \delta_d)$  is even. Equation (24) gives

$$P_{\ell} |\Phi_d\rangle = d\lambda_{\ell} (\mathbf{1} - \overline{D_{\ell}} \otimes D_{\ell}) |\Phi_d\rangle = 0.$$

Also  $A_0 = X$ , so  $X \otimes X$  fixes  $|\Phi_d\rangle$ . Finally

$$A_1 = X \operatorname{diag}(\eta^{2\kappa_j + \delta_d}) = X \operatorname{diag}(z_{\kappa_j}),$$

which identifies the target table with (15). For  $0 \leq \ell, y < d$ , the trace identity and  $B_y^T = V_y^\dagger$  give

$$\begin{aligned} \langle A_\ell B_y \rangle &= \frac{\overline{r_\ell}}{d} \sum_j \omega^{\ell \kappa_j} \overline{s_{y, \kappa_j}} \\ &= \frac{\overline{r_\ell} \omega^{-\ell y}}{d} \sum_t \omega^{\ell t} \overline{s_{0, t}} \\ &= \lambda_\ell \omega^{-\ell y}, \end{aligned}$$

where the last equality uses  $S_\ell = d \lambda_\ell r_\ell$ . Likewise,

$$\langle A_\ell B_d \rangle = \frac{\overline{r_\ell}}{d} \sum_j \omega^{\ell \kappa_j} = \delta_{\ell 0}.$$

All local first moments vanish because the displayed Alice and Bob observables are weighted shifts. These formulas give the complete complex first-harmonic correlator matrix and show directly that it is independent of  $\kappa$ .  $\square$

The theorem uses the SOS of Ref. [1], Eqs. (22)–(23), to prove global optimality; merely annihilating a candidate collection of operators would not have sufficed. What is common to both families is the root ordering, the Bob cycle, and the target table. The second family additionally requires the exact Fourier phases in (23). No statement is made here about a complete classification of its maximizing face.

## 8 Randomness interpretation

For  $\mu \in \{q, qa, qc\}$  and either augmented family, define the model- indexed value-conditioned guessing quantity

$$G_{\text{val}}^\mu(d; \mathcal{B}) = \sup_{\substack{S \in \mathfrak{S}_\mu: \\ \langle \mathcal{B}_d \rangle_S = \beta_\mu(\mathcal{B}_d)}} G_S(AB \mid 1, d, E), \quad \mathcal{B} \in \{\overline{\mathcal{I}}, \overline{\mathcal{F}}\}. \quad (25)$$

The finite-dimensional construction embeds into both larger models, so Theorems 6.1 and 7.2 imply, for every such  $\mu$ ,

$$G_{\text{val}}^\mu(d; \mathcal{B}) \geq \frac{1}{d^2} + \frac{2 \sin(\pi/d) \sin(3\pi/d)}{d^2(d-1)} > \frac{1}{d^2} \quad (d \geq 4). \quad (26)$$

This is only a lower bound on the supremal adversarial guessing probability over the maximizing face. It comes from one explicit strategy with trivial Eve; the final-two swap is not claimed to be worst possible.

The scope can be stated in one sentence:

*The maximum scalar Bell value alone does not identify the canonical behavior or certify maximal global randomness across the entire maximizing face.*

This conclusion has a precise relationship to the originating conjecture. Conjecture 2 of Ref. [1] states that maximal violation of the first augmented functional certifies  $2 \log_2 d$  random bits for  $(x, y) = (1, d)$ . Its printed maximum contains the isolated normalization discrepancy described in Remark 2.1; for the displayed operator the actual maximum is  $M_d + 1$ . In that normalization, the constructed strategies prove that the scalar-value implication

$$\langle \bar{\mathcal{I}}_d \rangle = M_d + 1 \implies G(AB \mid 1, d, E) = \frac{1}{d^2}$$

is false for every  $d \geq 4$ . This is a counterexample to the displayed Bell-value claim in those dimensions, not a determination of the exact worst-case guessing probability and not a statement about protocols that condition on additional observed data.

**Corollary 8.1** (Behavior-level nonuniqueness). *For either augmented family and every  $d \geq 4$ , the maximal scalar value does not determine a unique behavior, even modulo local output relabelings.*

*Proof.* The canonical phase order has the uniform target table  $1/d^2$ , whereas the final-two swap has the nonuniform table of Theorems 6.1 and 7.2. A local output relabeling at either target input only permutes the entries of that table and therefore cannot turn a uniform table into a nonuniform one. Thus the two exact maximizers represent inequivalent behaviors under those relabelings.  $\square$

This behavior-level failure of uniqueness is the only self-testing-related consequence used here. We do not claim a classification under every strategy-level equivalence involving local isometries, ancillary systems, or transposition.

At  $d = 4$ , Appendix D gives  $\max_{a,b} p(a, b \mid 1, 4) = 3/32$ . For the displayed trivial-Eve realization its min-entropy is exactly

$$-\log_2(3/32) = 5 - \log_2 3 = 3.415037 \dots < 4. \quad (27)$$

Equivalently, if  $H_{\text{val}}^\mu(d; \mathcal{B}) := -\log_2 G_{\text{val}}^\mu(d; \mathcal{B})$ , then the scalar maximum certifies at most  $5 - \log_2 3$  bits in every model above. The number is an upper bound on value-only worst-case conditional min-entropy, not its exact optimized value.

It is equally important to state what does not follow. The result does not dispute a calculation that fixes the complete canonical behavior, and it does not show that the canonical strategy lacks maximal global randomness. In fact, the numerical program described in Appendix B.1 of Ref. [1] reconstructs the full distribution of the canonical strategy before optimizing Eve's guessing probability. The root-swapped strategy has different higher Fourier correlators and therefore does not satisfy those full-behavior constraints.

A full-behavior SDP may thus return  $G = 1/d^2$  for the canonical table while (26) holds for the scalar maximum. Passing from the first statement to the second would require uniqueness of the maximizing behavior, self-testing strong enough to control the target PVMs, or other statistics that exclude the phase-permuted realization. The source's  $d = 3$  self-testing theorem for the second family is outside our  $d \geq 4$  construction and is not challenged.

**Corollary 8.2** (No value-only endpoint robustness). *For either augmented family and every  $d \geq 4$ , there is no valid bound for all strategies of the form*

$$G(AB \mid 1, d, E) \leq \frac{1}{d^2} + f_d(\varepsilon), \quad f_d(\varepsilon) \longrightarrow 0,$$

where  $\varepsilon$  is only the Bell deficit from the maximum. More precisely, the asserted bound is required to hold for every strategy whose deficit is at most  $\varepsilon$ .

*Proof.* The biased exact maximizer has deficit zero, hence is feasible for every  $\varepsilon \geq 0$ , and has the fixed positive gap in (26). Bounds that use additional observed correlators or the complete behavior are not excluded.  $\square$

## 9 Benchmarks and design conditions for low-setting private randomness

The permutation mechanism is a design warning, not a universal lower bound on settings. This section separates one exact resource baseline, a complete binary benchmark, and a positive sufficient composition criterion from the still-open higher-dimensional problem.

**Proposition 9.1** (One-input certification baseline). *If either party has only one input, every finite-output nonsignalling behavior is local and admits a compatible finite-dimensional pure projective realization in which Eve guesses both outputs perfectly at every input pair. Therefore neither a scalar score nor even the complete behavior in such a scenario can device-independently force positive private global randomness against all compatible realizations.*

*Proof.* Suppose Alice has one input. Nonsignalling makes  $p(a) = \sum_b p(a, b | y)$  independent of  $y$ . For  $p(a) > 0$ , let  $r_y(b | a) = p(a, b | y)/p(a)$ , and choose an arbitrary conditional distribution when  $p(a) = 0$ . The hidden variable

$$\lambda = (a, b_1, \dots, b_{m_B}), \quad \mu(\lambda) = p(a) \prod_y r_y(b_y | a)$$

reproduces the whole behavior by outputting the stored entries. The pure state

$$\sum_{\lambda} \sqrt{\mu(\lambda)} |\lambda\rangle_A |\lambda\rangle_B |\lambda\rangle_E$$

with diagonal grouping PVMs realizes it. Eve reads  $\lambda$  and guesses perfectly. The other case is symmetric.  $\square$

This is a standard locality fact, and it concerns the total test-input alphabets. It does not say that a trusted one-input realization is intrinsically random or nonrandom, nor does it prevent a larger Bell test from having one designated generation input on each wing.

**Theorem 9.2** (Binary two-input benchmark). *For binary Hermitian unitaries with cross-party commutation, set*

$$\mathcal{W}_2 = A_0 B_0 - 2A_0 B_1 + 2A_1 B_0 + 2A_1 B_1.$$

*Its finite-dimensional tensor-product, approximate, and commuting-operator values are all  $3\sqrt{3}$ . Moreover, every attaining finite-dimensional tensor-product strategy, with arbitrary purifying Eve, satisfies at the target pair  $(x, y) = (0, 0)$*

$$\sigma_E^{ab} = \rho_E/4 \quad (a, b \in \mathbb{Z}_2).$$

*Hence  $G(AB | 0, 0, E) = 1/4$  and  $H_{\min}(AB | E) = 2$  bits.*

Appendix E gives a self-contained two-square SOS and operator-valued Fourier proof. The result is established prior art: after the output flip  $B_1 \mapsto -B_1$ , this is the  $\delta = \pi/6$  member of the Woollerton–Brown–Colbeck family [10]. We include the proof as a normalization and privacy benchmark, not as a novelty claim.

**Corollary 9.3** (Binary setting minimality). *In the finite-dimensional projective device-independent model considered here, two binary inputs per party suffice to certify two private global output bits. One input on either wing cannot force any private global randomness against all compatible realizations. Thus  $(2, 2)$  is componentwise minimal for this binary certification task.*

For general  $d$ , operator-valued Fourier coefficients make the privacy condition explicit. For target PVMs  $R = \{R_a\}$  and  $Q = \{Q_c\}$ , put

$$\hat{\sigma}_E(k, \ell) = \sum_{a,c} \omega^{ka+\ell c} \sigma_E^{a,c}, \quad \sigma_E^{a,c} = \frac{1}{d^2} \sum_{k,\ell} \omega^{-ka-\ell c} \hat{\sigma}_E(k, \ell).$$

Thus privacy is equivalent to  $\hat{\sigma}_E(0, 0) = \rho_E$  and  $\hat{\sigma}_E(k, \ell) = 0$  for every nonzero Fourier index. Observed uniformity tests only the scalar trace of these conditions.

**Lemma 9.4** (Private-MUB composition; sufficient criterion). *Let  $|\Psi\rangle_{ABE}$  be a finite-dimensional purification. Alice has two  $d$ -outcome PVMs  $P = \{P_b\}_{b \in \mathbb{Z}_d}$  and  $R = \{R_a\}_{a \in \mathbb{Z}_d}$ , and Bob has a  $d$ -outcome PVM  $Q = \{Q_c\}_{c \in \mathbb{Z}_d}$ . Let  $\pi$  be a permutation of  $\mathbb{Z}_d$  and define*

$$\tau_E^b = \text{Tr}_{AB}[(P_b \otimes \mathbf{1})|\Psi\rangle\langle\Psi|(P_b \otimes \mathbf{1})].$$

*Suppose, for every  $a, b$ , that*

$$\begin{aligned} \tau_E^b &= \rho_E/d, \\ (\mathbf{1} \otimes Q_{\pi(b)} \otimes \mathbf{1})|\Psi\rangle &= (P_b \otimes \mathbf{1})|\Psi\rangle, \\ (P_b R_a P_b \otimes \mathbf{1})|\Psi\rangle &= d^{-1}(P_b \otimes \mathbf{1})|\Psi\rangle. \end{aligned}$$

*Then the target pair  $(R, Q)$  obeys*

$$\sigma_E^{a, \pi(b)} = \rho_E/d^2 \quad \text{for every } a, b.$$

*The hypotheses are sufficient; no necessity or low-setting existence claim is made.*

*Proof.* Fix  $a, b$  and a Hermitian test operator  $T_E$ . Suppressing identity factors, projectivity, cross-party commutation, and the matching hypothesis give

$$\begin{aligned} \text{Tr}(T_E \sigma_E^{a, \pi(b)}) &= \langle \Psi | R_a Q_{\pi(b)} T_E Q_{\pi(b)} R_a | \Psi \rangle \\ &= \langle \Psi | P_b R_a P_b T_E | \Psi \rangle \\ &= \frac{1}{d} \langle \Psi | P_b T_E | \Psi \rangle = \frac{1}{d^2} \text{Tr}(T_E \rho_E). \end{aligned}$$

Equality against every Hermitian  $T_E$  proves the operator identity.  $\square$

The lemma identifies what a successful composition would have to certify: a private reference PVM, perfect matching to Bob, and a state-supported MUB sandwich. It does not itself construct a Bell functional enforcing those hypotheses.

Appendix F records two narrower observations retained from the setting-complexity study: the standard two-input qudit self-test has no uniform joint setting pair, and one natural separately bounded third-setting repair cannot expose its common computational mutually unbiased basis. The obstruction does not rule out a genuinely joint SOS, another MUB, another self-test, or an arbitrary  $(2, 3, d, d)$  Bell functional.

| Scenario or design            | Audited status                                                                                                            |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| $1 \times m$ or $m \times 1$  | Cannot DI-force private global randomness, even from the complete behavior (Proposition 9.1).                             |
| $2 \times 2$ , $d = 2$        | Achievable and componentwise setting-minimal (Theorem 9.2).                                                               |
| $2 \times 2$ , $d \geq 3$     | Open here; the standard ideal qudit realization has no uniform input pair.                                                |
| $2 \times 3$ , $d \geq 3$     | Open here; the direct perfect-anchor construction fails, and Proposition F.1 excludes one coefficientwise exposure route. |
| All-dimensional benchmark     | A current construction uses two Alice inputs and $d^2 + 1$ Bob inputs [14].                                               |
| Two augmented cyclic families | Their scalar maxima fail to force maximal global randomness for every $d \geq 4$ .                                        |

Table 3: Proved, conditional, and open low-setting regimes.

## 10 Discussion and open problems

The exact value theorem and the biased maximizers expose a structural distinction between optimality and rigidity. The first operator controls a sum of moduli of first-order linear functions of the relative unitary. Its score is sharp enough to determine the allowable scalar phases but not their cyclic order. That missing order is invisible to the Bell score and visible to the target output distribution.

Several questions are now sharply posed.

1. Determine whether the support-level rigidity conditions, admissible phase permutations, direct sums, and irrelevant ancillary systems generate all attained finite-dimensional tensor-product exact maximizers of the first augmented family. First classify the minimal-support case  $\dim K = d$ . Theorem 4.1 then forces the equality-root spectrum to be simple; determine whether every such maximizer is equivalent, under the explicitly allowed symmetries, to a member of the permutation orbit of Theorem 6.1. Then separately characterize the  $qa$  and  $qc$  maximizing faces.
2. Determine the exact worst-case guessing probability at the Bell maximum; the bound (26) need not be tight.
3. Resolve the  $d = 2, 3$  maximizing faces for the first augmented family. The permutation orbit studied here is uniform in those dimensions.
4. Classify which phase permutations are related by local isometries and output relabelings, and which produce genuinely different full behaviors.
5. Find a low-setting modification whose Bell score controls the missing higher Fourier data, and determine whether it is rigid or robustly self-testing.
6. Develop robust bounds conditioned on a minimal set of extra correlators, rather than either one scalar score or the entire behavior.

The positive private-MUB criterion and the negative permutation-blindness mechanism point in the same direction: a successful low-setting score must control operator-valued adversarial information, not merely a scalar maximum or an unordered first-harmonic spectrum. These problems are natural opportunities for collaboration with the originating authors and the broader Bell-inequality community.

## Data, code, and historical versions

The source, exact certificates, and verification scripts are available in the public [Math repository](#), pinned for this revision at commit [609f8c6ffc083b665804890dd82fc739d414ea9d](#). From that directory, `./reproduce.sh` runs the mathematical checks, the two independent  $d = 4$  exact implementations, and clean manuscript and metadata builds; `manifest.sha256` records the package integrity hashes. Historical standalone versions remain accessible from the canonical paper page linked in that repository.

## AI-assistance disclosure

Generative-AI systems assisted with proof exploration, adversarial testing, code, literature-search organization, and drafting under Alec Kriebel’s direction. Alec Kriebel is the sole named author and takes responsibility for the manuscript and release. AI output was not treated as evidence: claims were retained only when accompanied by a written proof and replayable checks.

## A Proof of the scalar extremum

Write  $z = e^{2is}$ ,  $h = \pi/d$ , and  $a = h/2$ . Half of the sum in (4) is

$$G_d(s) = \sum_{y=0}^{d-1} |\cos(s + yh)|,$$

which has period  $h$ .

If  $d = 2m + 1$ , take  $-a \leq s \leq a$  and reindex by  $k = -m, \dots, m$ . Every angle lies in  $[-\pi/2, \pi/2]$ , so

$$G_d(s) = \sum_{k=-m}^m \cos(s + kh) = \csc(a) \cos s.$$

The maximum occurs exactly at  $s \equiv 0 \pmod{h}$ , equivalently  $z^d = 1$ .

If  $d = 2m$ , take  $0 \leq s \leq h$ . The first  $m$  cosines are nonnegative and the last  $m$  are nonpositive. Two finite sums give

$$G_d(s) = \sum_{y=0}^{m-1} \cos(s + yh) - \sum_{y=m}^{2m-1} \cos(s + yh) = \csc(a) \cos(s - a).$$

The maximum occurs exactly at  $s \equiv a \pmod{h}$ , equivalently  $z^d = -1$ . Multiplying by two proves Lemma 3.3, including the equality set.

## B Proof of support-level rigidity

We first isolate the finite-dimensional rank step.

**Lemma B.1** (Reflection-product rank bound). *Let  $T$  be unitary on an  $n$ -dimensional space and let  $E$  be an orthogonal projection of rank  $r$ . If*

$$T^d = \mathbf{1}, \quad (T(\mathbf{1} - 2E))^d = -\mathbf{1},$$

*then  $n \leq dr$ .*

*Proof.* Put  $R = \mathbf{1} - 2E$ . Factoring the ordered product gives

$$(TR)^d = T^d R_{d-1} \cdots R_0, \quad R_j = T^{-j} R T^j.$$

Thus  $-\mathbf{1} = R_{d-1} \cdots R_0$ . Each  $\mathbf{1} - R_j = 2T^{-j} E T^j$  has rank  $r$ , while repeated use of  $\mathbf{1} - AB = (\mathbf{1} - A) + A(\mathbf{1} - B)$  gives

$$\text{rank}(\mathbf{1} - R_{d-1} \cdots R_0) \leq \sum_{j=0}^{d-1} \text{rank}(\mathbf{1} - R_j) = dr.$$

The left side is  $\text{rank}(\mathbf{1}) = n$ . □

*Proof of Theorem 4.1.* Equality in the first reduced bound and in  $\text{Re}(A_0 B_d) \leq \mathbf{1}$  is forced separately. Every positive term in the augmented gap therefore vanishes on  $|\Psi\rangle$ :

$$P_y |\Psi\rangle = 0, \quad (M_d \mathbf{1} - F_d(U)) |\Psi\rangle = 0, \quad (A_0 B_d) |\Psi\rangle = |\Psi\rangle. \quad (28)$$

Here and below identity factors on the other parties are suppressed. The last relation follows from  $\mathbf{1} - \text{Re } W = \frac{1}{2}(\mathbf{1} - W)^\dagger(\mathbf{1} - W)$  for unitary  $W$ .

For every Alice operator  $R$ , a Schmidt decomposition across  $A : (BE)$  gives the support-cancellation equivalence

$$(R \otimes \mathbf{1}_{BE}) |\Psi\rangle = 0 \iff R|_K = 0. \quad (29)$$

Equivalently, the squared norm is  $\text{Tr}(\rho_A R^\dagger R)$ . This formulation includes nonfaithful  $\rho_A$  and makes no assertion on  $K^\perp$ . The middle relation in (28) therefore gives

$$K \subseteq L := \text{ran } \mathbf{1}_{\mathcal{Z}_d}(U), \quad \mathcal{Z}_d = \{z \in \mathbb{T} : z^d = (-1)^{d-1}\}.$$

The augmented stabilizer, after tracing out  $BE$ , gives  $\rho_A = A_0 \rho_A A_0^\dagger$ , hence  $A_0 K = K$ .

Write  $L_y = V_y |L_y|$  and define the possible kernel projection

$$E_y^{\text{bad}} = \mathbf{1}_{\{-\omega^{-y}\}}(U), \quad F_y = V_y V_y^\dagger = A_0 (\mathbf{1} - E_y^{\text{bad}}) A_0^\dagger.$$

The bad phase is not in  $\mathcal{Z}_d$ , because its  $d$ -th power is  $(-1)^d$ . Thus  $E_y^{\text{bad}} K = 0$ , and  $A_0 K = K$  gives  $F_y|_K = \mathbf{1}_K$ . Polar functional calculus factors the first residual as

$$P_y = |L_y^\dagger|^{1/2} (\mathbf{1} - V_y B_y).$$

The vector  $q_y = (\mathbf{1} - V_y B_y) |\Psi\rangle$  lies in  $\text{ran } F_y$  because  $F_y$  fixes the state's Alice support and  $F_y V_y = V_y$ . Equation (28) also puts  $q_y$  in  $\ker |L_y^\dagger|^{1/2} = \ker F_y$ . Therefore

$$(V_y B_y) |\Psi\rangle = |\Psi\rangle. \quad (30)$$

This cancellation uses neither an inverse nor a globally unitary extension of  $V_y$ .

The space  $K$  is contained in the initial support of  $V_y$ , so  $V_y$  is isometric there. Tracing (30) over  $BE$  yields  $\rho_A = V_y \rho_A V_y^\dagger$ , and hence  $V_y K = K$ . Thus  $S_y = A_0^\dagger V_y$  is unitary on  $K$ . On  $L$ , polar functional calculus gives

$$S_y = s_y(U), \quad s_y(z) = \frac{1 + \omega^y z}{|1 + \omega^y z|}, \quad s_y(z)^2 = \omega^y z.$$

It follows that  $U|_K = \omega^{-y}(S_y|_K)^2$ , so  $U(K) \subseteq K$ . Since  $U$  is unitary and  $K$  is finite-dimensional, this inclusion implies  $U(K) = K$ ; hence  $K$  reduces  $U$ . Let  $E_k$  be the spectral projection of  $U|_K$  corresponding to the root  $z_k$  in (10).

Put  $\eta = e^{\pi i/d}$ , read  $y+1$  modulo  $d$ , and let  $r_* = \lfloor (d-1)/2 \rfloor$ . Direct division of the adjacent half-angle phases gives

$$\overline{s_y(z_k)} s_{y+1}(z_k) = \begin{cases} -\eta, & [k+y]_d = r_*, \\ \eta, & [k+y]_d \neq r_*. \end{cases}$$

Consequently, for  $k(y) = [r_* - y]_d$ ,

$$S_y^\dagger S_{y+1} = \eta(\mathbf{1} - 2E_{k(y)}), \quad V_{y+1} = \eta V_y(\mathbf{1} - 2E_{k(y)}) \quad \text{on } K. \quad (31)$$

The map  $y \mapsto k(y)$  is a permutation of the root labels.

Since  $V_y$  is Alice-side and  $B_y$  is Bob-side, the two operators commute. Thus (30), together with  $B_y^d = \mathbf{1}$ , gives

$$V_y^d |\Psi\rangle = (V_y B_y)^d |\Psi\rangle = |\Psi\rangle.$$

Applying (29) to  $V_y^d - \mathbf{1}$  gives  $V_y^d|_K = \mathbf{1}_K$ . Since  $\eta^d = -1$ , (31) also gives

$$(V_y(\mathbf{1} - 2E_{k(y)}))^d = -\mathbf{1}_K.$$

Lemma B.1, with  $n = \dim K$ , yields  $n \leq d \operatorname{rank} E_k$  for every  $k$ . The  $E_k$ 's are mutually orthogonal and sum to  $\mathbf{1}_K$ , so their ranks sum to  $n$ . Every one of the  $d$  inequalities must be an equality:  $\operatorname{rank} E_k = n/d$  for all  $k$ . This proves the theorem.  $\square$

## C Rechecking the canonical attaining strategy

This appendix verifies the lower strategy supplied in Ref. [1] in a polar form. On  $\mathbb{C}^d$ , let

$$Z|j\rangle = \omega^j|j\rangle, \quad X|j\rangle = |j+1 \bmod d\rangle, \quad A_0 = Z, \quad A_1 = X.$$

Set

$$W_y = \omega^y Z^\dagger X, \quad H_y = |\mathbf{1} + W_y|, \quad Q_y = H_y^{-1}(\mathbf{1} + W_y^\dagger)Z^\dagger, \quad B_y = Q_y^T.$$

The weighted-shift action gives

$$W_y^d = (-1)^{d-1} \mathbf{1}, \quad \operatorname{spec}(W_y) = \{\lambda : \lambda^d = (-1)^{d-1}\}.$$

The spectrum is simple, and  $-1$  is absent; hence  $H_y$  is invertible. For  $L_y = Z + \omega^y X = Z(\mathbf{1} + W_y)$ ,

$$L_y = \underbrace{Z(\mathbf{1} + W_y)H_y^{-1}H_y}_{V_y}$$

is the polar decomposition, and  $Q_y = V_y^\dagger$  is unitary.

It remains to check the measurement order. On the displayed spectrum put  $p(z) = (1+z)/|1+z|$ . Since  $Z^\dagger W_y Z = \omega^{-1} W_y$ ,

$$Q_y^d = \prod_{r=0}^{d-1} p(\omega^{-r} W_y)^\dagger.$$

For each eigenvalue  $\lambda$ , the corresponding scalar equals

$$\frac{\prod_r (1 + \omega^{-r} \lambda)}{\prod_r |1 + \omega^{-r} \lambda|} = \frac{1 - (-\lambda)^d}{|1 - (-\lambda)^d|} = 1.$$

Thus  $B_y^d = \mathbf{1}$ . The weighted-cycle characteristic polynomial shows that each  $d$ -th root occurs.

Finally,

$$\langle \Phi_d | L_y \otimes B_y | \Phi_d \rangle = \frac{1}{d} \text{Tr}(L_y V_y^\dagger) = \frac{1}{d} \text{Tr}(H_y).$$

The spectrum of  $W_y$  is the scalar equality set, so summing over  $y$  gives  $\langle \mathcal{I}_d \rangle = M_d$ . Taking the extra Bob observable  $B_d = Z^\dagger$  gives  $\langle Z \otimes Z^\dagger \rangle = 1$ , proving Corollary 3.4.

To identify this polar form with the source observables rather than only compare their values, write the source expansion as

$$B_y^{\text{src}} = \sum_{k=0}^{d-1} \lambda_{y,k}^{\text{src}} X^{k+1} Z^k, \quad \lambda_{y,k}^{\text{src}} = \frac{(-1)^k \omega^{k(k+1)/2} \omega^{-y(k+1)}}{d \sin(\pi(k + \frac{1}{2})/d)}.$$

Its discrete Fourier transform is

$$\sum_{y=0}^{d-1} \omega^{my} \lambda_{y,k}^{\text{src}} = d \lambda_{0,k}^{\text{src}} \delta_{k,m-1 \pmod{d}}.$$

At  $m = 0, 1$  this gives exactly

$$\sum_y B_y^{\text{src}} = \alpha_d Z^\dagger, \quad \sum_y \omega^y B_y^{\text{src}} = \alpha_d X, \quad \alpha_d = \csc\left(\frac{\pi}{2d}\right). \quad (32)$$

Thus the source strategy saturates the sum of the termwise polar bounds. Every  $L_y$  is invertible here, so equality in each positive polar deficit uniquely forces  $(B_y^{\text{src}})^T = V_y^\dagger$ . Hence  $B_y^{\text{src}} = Q_y^T = \overline{V_y}$ : the transpose and complex conjugation are fixed by  $\langle \Phi_d | R \otimes S | \Phi_d \rangle = d^{-1} \text{Tr}(RS^T)$ .

For  $d = 3$ , the coefficient formula reduces to

$$B_y = \frac{1}{3} (2Z^2 + 2\omega^{2y} X - \omega^{y+1} X^2 Z),$$

the explicit source observable, with  $\alpha_3 = 2$ . This appendix claims no new attaining strategy.

## D The exact four-outcome certificate

Let  $d = 4$ ,  $\zeta = e^{\pi i/8}$ , and  $\kappa = (0, 1, 3, 2)$ . Then

$$A_0 = X, \quad A_1 = X \text{diag}(\zeta^2, \zeta^6, \zeta^{14}, \zeta^{10}), \quad B_4 = X.$$

The first-family polar unitaries  $V_y = X \text{diag}(\zeta^{e_{y,0}}, \dots, \zeta^{e_{y,3}})$  are encoded by

| $y$ | $e_{y,0}$ | $e_{y,1}$ | $e_{y,2}$ | $e_{y,3}$ |                          |
|-----|-----------|-----------|-----------|-----------|--------------------------|
| 0   | 1         | 3         | 15        | 13        | $B_y = \overline{V_y}$ . |
| 1   | 3         | 13        | 1         | 15        |                          |
| 2   | 13        | 15        | 3         | 1         |                          |
| 3   | 15        | 1         | 13        | 3         |                          |

These are exact monomial matrices over  $\mathbb{Q}(\zeta_{16})$ , not numerical polar decompositions.

The recurrence (14) gives

$$q = (1, \zeta^2, -1, \zeta^6), \quad (|\widehat{q}_m|^2)_{m=0}^3 = (2, 6, 2, 6).$$

For both augmented families,

$$p(a, b \mid 1, 4) = \begin{cases} 1/32, & a + b \text{ even,} \\ 3/32, & a + b \text{ odd,} \end{cases} \quad G = 3/32 > 1/16. \quad (33)$$

For the displayed one-dimensional Eve this gives exactly  $H_{\min}(AB) = -\log_2(3/32) = 5 - \log_2 3$  bits, while the ideal uniform table would give four bits. One exact verifier reconstructs (33) from projectors and a separate Fourier calculation. An independent exact implementation reconstructs the source coefficients  $\lambda_{y,k}$ , proves  $\widehat{B}_\ell = 4\lambda_\ell D_\ell$ , checks all fourth-power relations, expands the full second-family SOS, and verifies values  $M_4 + 1$  and 5.

## E Binary two-input benchmark

We prove Theorem 9.2 directly, while crediting its prior-art origin in the main text. Cross-party identity factors are suppressed. The exact operator identity is

$$\begin{aligned} 3\sqrt{3}\mathbf{1} - \mathcal{W}_2 &= \frac{1}{2\sqrt{3}}(\sqrt{3}A_0 - B_0 + 2B_1)^2 \\ &\quad + \frac{1}{\sqrt{3}}(\sqrt{3}A_1 - B_0 - B_1)^2. \end{aligned} \quad (34)$$

Its expansion uses only  $A_x^2 = B_y^2 = \mathbf{1}$  and cross-party commutation. The two same-party Bob anticommutator terms cancel, so  $\mathcal{W}_2 \leq 3\sqrt{3}\mathbf{1}$  already in the commuting model.

If a finite-dimensional purified strategy attains equality, both squares annihilate  $|\Psi\rangle$ :

$$(B_0 - 2B_1)|\Psi\rangle = \sqrt{3}A_0|\Psi\rangle, \quad (B_0 + B_1)|\Psi\rangle = \sqrt{3}A_1|\Psi\rangle. \quad (35)$$

Define the Hermitian operators

$$X_A = \frac{A_0 + 2A_1}{\sqrt{3}}, \quad Z_B = \frac{B_0 - 2B_1}{\sqrt{3}}.$$

Solving (35) gives, explicitly as on-state relations,

$$B_0|\Psi\rangle = X_A|\Psi\rangle, \quad Z_B|\Psi\rangle = A_0|\Psi\rangle.$$

Cross-party commutation and unitarity imply  $X_A^2|\Psi\rangle = Z_B^2|\Psi\rangle = |\Psi\rangle$ . The exact identities

$$\{A_0, X_A\} = \sqrt{3}(X_A^2 - \mathbf{1}), \quad \{Z_B, B_0\} = \sqrt{3}(Z_B^2 - \mathbf{1})$$

therefore yield

$$\{A_0, X_A\}|\Psi\rangle = 0, \quad \{Z_B, B_0\}|\Psi\rangle = 0. \quad (36)$$

No global anticommutation relation is asserted.

Put  $S_A = X_A B_0$  and  $S_B = A_0 Z_B$ . These Hermitian operators stabilize the state. For every Hermitian Eve test  $T_E$ , cross-party commutation and (36) give

$$\begin{aligned}\langle A_0 T_E \rangle &= \langle S_A A_0 T_E \rangle = \langle X_A A_0 B_0 T_E \rangle = -\langle A_0 T_E S_A \rangle = -\langle A_0 T_E \rangle, \\ \langle B_0 T_E \rangle &= \langle S_B B_0 T_E \rangle = -\langle B_0 T_E S_B \rangle = -\langle B_0 T_E \rangle.\end{aligned}$$

Here the commuting factor  $B_0 T_E$ , respectively  $A_0 T_E$ , may be moved through the relevant on-state anticommutator; no global anticommutation is used. Finally,

$$\langle A_0 B_0 T_E \rangle = \langle A_0 X_A T_E \rangle.$$

The left side is real, while the complex conjugate of the right side is its negative by (36); hence the joint moment also vanishes. Thus all three nontrivial binary operator-valued Fourier coefficients are zero:

$$\langle A_0 T_E \rangle = \langle B_0 T_E \rangle = \langle A_0 B_0 T_E \rangle = 0.$$

For  $M_a^0 = (\mathbf{1} + (-1)^a A_0)/2$  and  $N_b^0 = (\mathbf{1} + (-1)^b B_0)/2$ , Fourier inversion gives

$$\begin{aligned}\mathrm{Tr}(T_E \sigma_E^{ab}) &= \frac{1}{4} (\mathrm{Tr}(T_E \rho_E) + (-1)^a \langle A_0 T_E \rangle + (-1)^b \langle B_0 T_E \rangle \\ &\quad + (-1)^{a+b} \langle A_0 B_0 T_E \rangle) = \frac{1}{4} \mathrm{Tr}(T_E \rho_E).\end{aligned}$$

Equality for every Hermitian  $T_E$  proves  $\sigma_E^{ab} = \rho_E/4$ .

For attainment, on  $|\Phi_2\rangle$  take

$$A_0 = Z, \quad A_1 = -\frac{1}{2}Z + \frac{\sqrt{3}}{2}X, \quad B_0 = X, \quad B_1 = -\frac{\sqrt{3}}{2}Z + \frac{1}{2}X.$$

All four observables square to  $\mathbf{1}$ , and the maximally entangled trace identity gives  $\langle \mathcal{W}_2 \rangle = 3\sqrt{3}$ . This finite strategy and (34) establish the  $q = qa = qc$  value; the preceding operator-valued calculation establishes the stated finite-dimensional privacy conclusion.

## F Scoped low-setting observations

The standard two-input maximally-entangled-qudit self-test [9] uses Fourier-phase bases. Up to input swaps, conjugation, transposition, and outcome relabeling, its four ideal tables have the form

$$p(a, b \mid x, y) = \frac{\sin^2(\pi \delta_{xy})}{d^3 \sin^2(\pi(a - b + \delta_{xy})/d)}, \quad (\delta_{xy}) = \begin{pmatrix} 1/4 & 3/4 \\ -1/4 & 1/4 \end{pmatrix}. \quad (37)$$

Every table has

$$p_{\max} = \frac{1}{2d^3 \sin^2(\pi/(4d))} > \frac{1}{d^2},$$

so no ideal input pair is uniform. Its ideal joint min-entropy is

$$\log_2 \left( 2d^3 \sin^2 \frac{\pi}{4d} \right) = \log_2 d + \log_2 \frac{\pi^2}{8} + o(1).$$

Perfectly anchoring a third Bob setting to either Alice basis leaves a cross table with

$$p_{\max}^{\mathrm{cross}} = \frac{1}{d^3 \sin^2(\pi/(2d))} > \frac{1}{d^2} \quad (d \geq 3).$$

The exception  $d = 2$  is precisely the mutually-unbiased qubit case.

There is a broader but still scoped obstruction. Let  $F$  be the Fourier matrix,  $\rho = e^{\pi i/d}$ , and  $R = \text{diag}(1, \rho, \dots, \rho^{d-1})$ . The real Hermitian operator system generated by the two ideal Alice PVMs is

$$\mathcal{S} = \{F \text{diag}(x) F^\dagger + R F \text{diag}(y) F^\dagger R^\dagger : x, y \in \mathbb{R}^d\}.$$

**Proposition F.1** (Computational-MUB exposure obstruction). *If  $K \in \mathcal{S}$  has a computational vector  $e_r$  as an eigenvector with eigenvalue  $\kappa$ , then either  $K = \kappa \mathbf{1}$ , or  $\kappa$  is neither the largest nor the smallest eigenvalue of  $K$ . Consequently, no nontrivial separately bounded term*

$$\mathcal{L} = \sum_b K_b \otimes Q_b, \quad K_b \in \mathcal{S},$$

can expose the computational PVM on  $|\Phi_d\rangle$  through a coefficientwise spectral upper bound.

*Proof.* Write  $K = C + RC'R^\dagger$ , with  $C, C'$  Hermitian circulants. Index rows and columns by  $0, \dots, d-1$ , and write

$$C_{jk} = c_{j-k}, \quad C'_{jk} = c'_{j-k},$$

where the coefficient subscripts are understood modulo  $d$ , while the exponent in

$$(RC'R^\dagger)_{jk} = \rho^{j-k} c'_{j-k}$$

uses the ordinary integer difference  $j-k$ . The diagonal equation gives  $c_0 + c'_0 = \kappa$ . The off-diagonal components of  $Ke_r = \kappa e_r$ , first with  $j = r+t$  and then with  $j = r-t$ , are

$$\begin{aligned} c_t + \rho^t c'_t &= 0 & (1 \leq t \leq d-1-r), \\ c_{d-t} + \rho^{-t} c'_{d-t} &= 0 & (1 \leq t \leq r). \end{aligned}$$

Put  $s = \min(r, d-1-r)$ . Since  $C$  and  $C'$  are Hermitian,

$$c_{d-t} = \overline{c_t}, \quad c'_{d-t} = \overline{c'_t} \quad (1 \leq t \leq d-1).$$

Conjugating the second indexed family and combining it with the first therefore gives

$$c_t + \rho^t c'_t = 0 \quad (1 \leq t \leq \max(r, d-1-r) = d-1-s).$$

For  $s+1 \leq t \leq d-1$ , the index  $u = d-t$  satisfies  $1 \leq u \leq d-1-s$ . Applying the preceding equation at  $u$  and taking its Hermitian conjugate gives

$$c_t + \rho^{t-d} c'_t = 0.$$

Because  $\rho^d = -1$ , this is

$$c_t - \rho^t c'_t = 0 \quad (s+1 \leq t \leq d-1).$$

On the common index range

$$s+1 \leq t \leq d-1-s$$

(which may be empty), adding and subtracting the last two equations shows directly that

$$c_t = c'_t = 0.$$

Thus only the off-diagonal cyclic modes  $t \in \{1, \dots, s\} \cup \{d-s, \dots, d-1\}$  can survive, with both sets empty when  $s = 0$ .

For  $1 \leq t \leq s$ , the relation  $c_t + \rho^t c'_t = 0$ , and its Hermitian conjugate, cancel the entries having ordinary differences  $t$  and  $-t$ . The only surviving occurrences are therefore the wraparound differences  $t - d$  and  $d - t$ . Set

$$a_t := c_t + \rho^{t-d} c'_t = c_t - \rho^t c'_t = 2c_t \quad (1 \leq t \leq s).$$

After grouping the first  $s$ , middle  $d - 2s$ , and last  $s$  coordinates, the upper-right corner has entries

$$T_{pq} := (K - \kappa \mathbf{1})_{p, d-s+q} = \begin{cases} a_{s+p-q}, & 0 \leq p \leq q \leq s-1, \\ 0, & 0 \leq q < p \leq s-1. \end{cases}$$

Hence  $T$  is an  $s$ -by- $s$  upper-triangular Toeplitz matrix, and Hermiticity supplies the lower-left corner:

$$K - \kappa \mathbf{1} = \begin{pmatrix} 0 & 0 & T \\ 0 & 0 & 0 \\ T^\dagger & 0 & 0 \end{pmatrix}.$$

On the first and last coordinate blocks this is  $\begin{pmatrix} 0 & T \\ T^\dagger & 0 \end{pmatrix}$ . If  $s = 0$ , the preceding vanishing already gives  $K = \kappa \mathbf{1}$ . If  $s > 0$  and  $T = 0$ , then  $T_{0, s-t} = a_t = 0$  for every  $1 \leq t \leq s$ . Hence  $c_t = 0$  by  $a_t = 2c_t$ , and  $c'_t = 0$  by  $c_t + \rho^t c'_t = 0$ . Hermiticity eliminates the modes  $d - s, \dots, d - 1$ , while the middle modes already vanish; together with  $c_0 + c'_0 = \kappa$ , this gives  $K = \kappa \mathbf{1}$ . Thus a nonscalar  $K$  forces  $T \neq 0$ . An SVD of  $T$  shows that this block matrix has nonzero eigenvalues  $\pm \sigma_j(T)$ . Hence a nonscalar  $K$  has spectrum on both sides of  $\kappa$ .

To saturate a coefficientwise upper bound on the maximally entangled state with computational  $Q_b$ , every computational outcome has nonzero weight and the corresponding  $e_b$  must be a maximal eigenvector of  $K_b$ . The first part makes that impossible unless all relevant  $K_b$  are scalar, in which case the term constrains no measurement.  $\square$

Proposition F.1 rules out only this separately bounded local- spectral route. It is not a no-go theorem for  $(2, 3, d, d)$ , and it is not used in any cyclic-family conclusion.

## G Source conventions and claim boundary

Our first-family definition (1) follows the displayed main-text operator definition in Ref. [1]. A nearby appendix writes one Bob adjoint differently while its subsequent calculation follows the main convention. Replacing every Bob observable by its adjoint transports between the two notations, but mixing them within one formula does not. We therefore state every adjoint explicitly and test the Fourier orientation.

For the second family, (20) matches the Hermitian content of the source definition and the SOS of Ref. [1], Eqs. (22)–(23), with prefactor  $1/(2d)$ . The source text adjacent to the canonical construction briefly omits Alice's entrywise conjugation, while its theorem includes it. Our choice  $A_\ell = \overline{D_\ell}$  is the one that annihilates the displayed SOS on  $|\Phi_d\rangle$ .

If instead every Bob observable in the source appendix is written with an adjoint, set  $B'_y = B_y^\dagger$  and  $B'_d = B_d^\dagger$ . This is Bob's outcome inversion: it sends  $p(a, b)$  to  $p(a, -b)$  while preserving the maximum, nonuniformity, and guessing probability. It cannot be mixed termwise with the no-adjoint convention used in (20).

The source's numerical guessing-probability table explicitly fixes the full canonical distribution. Our scalar-value conclusion should therefore not be read as a criticism of that calculation. The literal maximal-violation conjecture and the fixed-behavior numerical experiment have different logical hypotheses; the present construction separates them.

## References

- [1] I. Perito, R. D’Avino, M. Jung, P. Mironowicz, A. Acín, and R. Augusiak, Bell inequalities tailored to optimal global randomness certification, *arXiv:2606.21362v3* (2026), <https://arxiv.org/abs/2606.21362v3>.
- [2] C. Dhara, G. Pretico, and A. Acín, Maximal quantum randomness in Bell tests, *Phys. Rev. A* **88**, 052116 (2013), <https://doi.org/10.1103/PhysRevA.88.052116>.
- [3] O. Nieto-Silleras, S. Pironio, and J. Silman, Using complete measurement statistics for optimal device-independent randomness evaluation, *New J. Phys.* **16**, 013035 (2014), <https://doi.org/10.1088/1367-2630/16/1/013035>.
- [4] J.-D. Bancal, L. Sheridan, and V. Scarani, More randomness from the same data, *New J. Phys.* **16**, 033011 (2014), <https://doi.org/10.1088/1367-2630/16/3/033011>.
- [5] M. Navascués, S. Pironio, and A. Acín, Bounding the set of quantum correlations, *Phys. Rev. Lett.* **98**, 010401 (2007), <https://doi.org/10.1103/PhysRevLett.98.010401>.
- [6] H. Buhrman and S. Massar, Causality and Tsirelson’s bounds, *Phys. Rev. A* **72**, 052103 (2005), <https://doi.org/10.1103/PhysRevA.72.052103>.
- [7] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, Bell inequalities tailored to maximally entangled states, *Phys. Rev. Lett.* **119**, 040402 (2017), <https://doi.org/10.1103/PhysRevLett.119.040402>.
- [8] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems, *Quantum* **3**, 198 (2019), <https://doi.org/10.22331/q-2019-10-24-198>.
- [9] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, Self-testing quantum systems of arbitrary local dimension with minimal number of measurements, *npj Quantum Information* **7**, 151 (2021), <https://doi.org/10.1038/s41534-021-00490-3>.
- [10] L. Woollerton, P. Brown, and R. Colbeck, Tight analytic bound on the trade-off between device-independent randomness and nonlocality, *Phys. Rev. Lett.* **129**, 150403 (2022), <https://doi.org/10.1103/PhysRevLett.129.150403>.
- [11] V. Barizien, P. Sekatski, and J.-D. Bancal, Custom Bell inequalities from formal sums of squares, *Quantum* **8**, 1333 (2024), <https://doi.org/10.22331/q-2024-05-02-1333>.
- [12] I. Klep, N. Leijenhorst, and V. Magron, Robust self-testing with CHSH mod 3, *arXiv:2604.03700v1* (2026), <https://arxiv.org/abs/2604.03700v1>.
- [13] L. Coccia, M. Padovan, and G. Vallone, Systematic derivation of Tsirelson bounds in arbitrary dimensions, *arXiv:2606.21626v1* (2026), <https://arxiv.org/abs/2606.21626v1>.
- [14] M. Farkas, P. Mironowicz, and R. Augusiak, Maximal global device-independent randomness from projective measurements in every dimension, *arXiv:2606.21369v2* (2026), <https://arxiv.org/abs/2606.21369v2>.

- [15] R. D'Avino, I. Perito, P. Mironowicz, A. Acín, and R. Augusiak, Noise robustness of three outcome Bell certified quantum randomness, *arXiv:2606.21371v2* (2026), <https://arxiv.org/abs/2606.21371v2>.