

# Permutation-blind Bell scores and obstructions to maximal global randomness

Exact maximizers for two cyclic families and setting-complexity consequences

Alec Kriebel

with heavy assistance from ChatGPT 5.6 Sol

27 July 2026

## Abstract

We study how many measurement settings are needed for one Bell score to certify  $2 \log_2 d$  private random bits from projective  $d$ -outcome measurements. We do not determine the all-dimensional minimum, but prove four exact structural results. First, if either party has only one input, the complete behavior is local and has a compatible pure realization in which Eve guesses every joint output perfectly; thus both parties need at least two inputs. Second, we give a positive-factor theorem for a broad first-harmonic polar-linear class. Under explicit phase-product hypotheses, every permutation of the scalar maximizing phases produces an admissible order- $d$  maximizer with the same Bell-visible correlators, although its full target distribution can change. Third, the phase-permutation counterexamples previously found for the first cyclic family of Perito et al. also annihilate the sum-of-squares certificate of their second family. For both augmented families and every  $d \geq 4$ , an exact maximizer with trivial Eve obeys

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

At  $d = 4$ , an exact  $\mathbb{Q}(\zeta_{16})$  certificate gives  $G = 3/32 > 1/16$ . Finally, we compute all four ideal tables of the standard two-input qudit self-test and prove that a natural separately bounded third-setting repair cannot expose its common computational mutually unbiased basis. These results explain why several efficient designs fail, but they neither rule out nor construct an all-dimensional  $2 \times 2$  or  $2 \times 3$  protocol.

**Status.** This is an unrefereed, AI-assisted research note. The symbolic proof, discovery code, exact finite certificate, and independent checks are public for audit. The author is an independent amateur and cannot personally validate every technical step; expert review is required.

## 1 Framework and results

Fix an integer  $d \geq 2$ . Alice has projective measurements  $\{M_a^x\}_{a \in \mathbb{Z}_d}$ , Bob has  $\{N_b^y\}_{b \in \mathbb{Z}_d}$ , and Eve purifies their finite-dimensional state  $|\Psi\rangle_{ABE}$ . For a designated pair  $(x_*, y_*)$ , write

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

Maximal global private randomness means

$$\sigma_E^{ab} = \rho_E/d^2 \quad \text{for every } a, b, \quad \rho_E = \sum_{a,b} \sigma_E^{ab}. \quad (1)$$

This is stronger than the scalar equality  $p(a, b|x_*, y_*) = 1/d^2$ .

Let  $\mathfrak{M}_d$  denote the setting pairs for which one real linear Bell functional has a quantum maximum whose every realizing strategy satisfies (1). Our universal lower bound is:

**Theorem 1.1** (One-input impossibility). *For every  $d \geq 2$  and every finite  $m$ ,*

$$(1, m) \notin \mathfrak{M}_d, \quad (m, 1) \notin \mathfrak{M}_d.$$

*In fact, if Alice has one input, every complete nonsignalling behavior has a compatible pure projective realization satisfying*

$$G(AB|0, y, E) = 1$$

*for each Bob input  $y$ . The symmetric statement holds when Bob has one input.*

For  $d = 2$ , the lower bound is tight. The binary score

$$A_0B_0 - 2A_0B_1 + 2A_1B_0 + 2A_1B_1$$

has maximum  $3\sqrt{3}$  and certifies two private joint bits at  $(0, 0)$ . This is the  $\delta = \pi/6$  case, up to an output flip, of Woollorton, Brown, and Colbeck [4]; Appendix A records a short independent SOS check.

For  $d \geq 3$ , the exact minimum remains open. The strongest all-dimensional single-score construction located in our targeted audit has two Alice settings and  $d^2 + 1$  Bob settings [2]. Thus the rigorous setting bounds recorded here are

$$2 \leq m_A, \quad 2 \leq m_B,$$

with no claim that the known upper construction is minimal.

## 2 Proof of the one-input impossibility

*Proof of Theorem 1.1.* Nonsignalling makes  $p(a) = \sum_b p(a, b|y)$  independent of  $y$ . For  $p(a) > 0$ , set

$$r_y(b|a) = \frac{p(a, b|y)}{p(a)};$$

for  $p(a) = 0$ , choose  $r_y(\cdot|a)$  arbitrarily. Introduce the finite hidden variable

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

Alice outputs the stored  $a$ , and Bob outputs the stored  $b_y$  on input  $y$ . Summing over the other entries gives

$$\sum_{\lambda: \lambda_A=a, \lambda_y=b} \mu(\lambda) = p(a)r_y(b|a) = p(a, b|y),$$

so this deterministic local model reproduces the complete behavior.

It has a finite-dimensional pure projective realization:

$$|\Psi'\rangle = \sum_{\lambda} \sqrt{\mu(\lambda)} |\lambda\rangle_A |\lambda\rangle_B |\lambda\rangle_E,$$

where Alice's and Bob's PVMs group the computational labels by  $a$  and  $b_y$ . Eve reads  $\lambda$  and knows both outputs for every target input, so  $G = 1$ . Exchanging Alice and Bob proves the symmetric claim.  $\square$

*Remark 2.1.* The theorem concerns the total number of test inputs. It does not say that a larger Bell test cannot use one designated generation input on each wing. It is the standard locality fact for a scenario with one input on one wing, written here because it gives the exact resource baseline. It is stronger than a one-score obstruction because the flagged realization reproduces the entire behavior.

### 3 A polar-linear permutation theorem

For an operator  $C$ , write  $|C| = (C^\dagger C)^{1/2}$  and  $\operatorname{Re} T = (T + T^\dagger)/2$ .

**Lemma 3.1** (Polar positive factor). *Let  $C = V|C|$  be the canonical polar decomposition and let  $B$  be unitary. Then*

$$\frac{|C| + |C|^\dagger}{2} \otimes \mathbf{1} - \operatorname{Re}(C \otimes B) = \frac{1}{2} P^\dagger P,$$

where

$$P = |C|^{1/2} \otimes \mathbf{1} - V|C|^{1/2} \otimes B.$$

*Proof.* The polar partial isometry satisfies  $V^\dagger V = s(|C|)$  and  $|C|^{1/2} V = V|C|^{1/2}$ . Consequently

$$|C|^{1/2} V|C|^{1/2} = V|C| = C,$$

while

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

Expanding  $P^\dagger P$ , with all tensor factors displayed, gives

$$|C| \otimes \mathbf{1} + |C|^\dagger \otimes \mathbf{1} - C \otimes B - C^\dagger \otimes B^\dagger.$$

No inverse and no extension of  $V$  to a unitary is used. □

Fix finitely many coefficient pairs  $\alpha_r, \beta_r \in \mathbb{C}$ , and set

$$g_r(z) = \alpha_r + \beta_r z, \quad f(z) = \sum_r |g_r(z)|, \quad M = \max_{|z|=1} f(z).$$

For unitaries  $A_0, A_1, B_r, B_*$ , define

$$\mathcal{J} = \sum_r \operatorname{Re}[(\alpha_r A_0 + \beta_r A_1) \otimes B_r] + \operatorname{Re}(A_0 \otimes B_*). \quad (2)$$

**Theorem 3.2** (Exact certificate and permutation blindness). *Put  $U = A_0^\dagger A_1$ ,  $C_r = A_0 g_r(U) = V_r |C_r|$ , and  $f(U) = \sum_r |g_r(U)|$ . Set*

$$\begin{aligned} P_r &= |C_r|^{1/2} \otimes \mathbf{1} - V_r |C_r|^{1/2} \otimes B_r, \\ G &= M \mathbf{1} - f(U), \\ R_* &= \mathbf{1} - A_0 \otimes B_*. \end{aligned}$$

Then

$$(M+1)\mathbf{1} - \mathcal{J} = \frac{1}{2} \sum_r P_r^\dagger P_r + \frac{1}{2} R_*^\dagger R_* + \frac{1}{2} (G + A_0 G A_0^\dagger) \otimes \mathbf{1}. \quad (3)$$

Now let  $\omega = e^{2\pi i/d}$ . Suppose there are labeled phases  $z_j, s_{rj} \in \mathbb{T}$  satisfying

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

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

At a zero of  $g_r$ ,  $s_{rj}$  may be any unitary polar-extension phase. For every permutation  $\kappa$  of the labels, the strategy

$$\begin{aligned} A_0 &= X, & A_1 &= X \operatorname{diag}(z_{\kappa_j}), \\ B_r &= \overline{X \operatorname{diag}(s_{r,\kappa_j})}, & B_* &= X \end{aligned} \quad (4)$$

on  $|\Phi_d\rangle = d^{-1/2} \sum_j |j, j\rangle$  attains  $M+1$ , and every displayed observable has  $d$ -th power  $\mathbf{1}$ . All local first moments and the entire first-harmonic correlator matrix of (2) are independent of  $\kappa$ .

*Proof.* Since  $g_r(U)$  is normal,

$$|C_r| = |g_r(U)|, \quad |C_r^\dagger| = A_0 |g_r(U)| A_0^\dagger.$$

Functional calculus gives  $G \geq 0$ . Sum Lemma 3.1 over  $r$  and use

$$\mathbf{1} - \operatorname{Re}(A_0 \otimes B_*) = \frac{1}{2} R_*^\dagger R_*$$

to obtain (3).

For arbitrary weights  $t_j$ ,

$$(X \operatorname{diag}(t_j))^d = \left( \prod_j t_j \right) \mathbf{1}. \quad (5)$$

The two product hypotheses therefore prove every order relation in (4). Moreover,

$$\alpha_r A_0 + \beta_r A_1 = X \operatorname{diag}(g_r(z_{\kappa_j}))$$

has polar factor  $X \operatorname{diag}(s_{r,\kappa_j})$ . At a zero of  $g_r$ , this is a unitary extension of the canonical partial isometry; it agrees on the support of  $|C_r|$ , which is all that the positive factor uses. The maximally entangled trace identity

$$\langle \Phi_d | R \otimes S | \Phi_d \rangle = d^{-1} \operatorname{Tr}(RS^T)$$

then proves equality in every positive factor.

Finally,

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

These are symmetric sums of the labeled data. Every local observable is a weighted shift and hence has zero trace.  $\square$

**Corollary 3.3** (Exact randomness obstruction). *Use the spectral convention  $O = \sum_a \omega^a \Pi_a$ . For the target  $(A_1, B_*)$ , define*

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

Then

$$p_\kappa(a, b | 1, *) = \frac{|\hat{q}_{-(a+b)}|^2}{d^3}. \quad (6)$$

If the Fourier magnitudes are not constant, the trivial-Eve realization obeys

$$G(AB|1, *, E) \geq \frac{\max_m |\hat{q}_m|^2}{d^3} > \frac{1}{d^2}.$$

*Proof.* Equation (5) gives  $q_d = q_0$ . The eigenvectors of  $A_0 = X$  and  $A_1 = X \text{diag}(z_{\kappa_j})$  are respectively

$$u_c = d^{-1/2} \sum_j \omega^{-cj} |j\rangle, \quad v_a = d^{-1/2} \sum_j q_j \omega^{-aj} |j\rangle.$$

The transpose of Bob's outcome- $b$  projector is Alice's outcome- $(-b)$  projector for  $X$ . Taking their overlap proves (6). Parseval gives  $\sum_m |\hat{q}_m|^2 = d^2$ ; nonconstancy therefore forces one magnitude squared to exceed  $d$ .  $\square$

## 4 Both cyclic families admit biased maximizers

### 4.1 The first polar-linear family

Let

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

These are exactly the roots of  $z^d = (-1)^{d-1}$ .

**Lemma 4.1** (Sharp scalar sum).

$$\max_{|z|=1} \sum_{y=0}^{d-1} |1 + \omega^y z| = 2 \csc\left(\frac{\pi}{2d}\right) \quad (7)$$

has equality precisely when  $z^d = (-1)^{d-1}$ .

*Proof.* Write  $z = e^{2is}$ ,  $h = \pi/d$ , and  $a = h/2$ . Then the sum in (7) is

$$2G_d(s), \quad G_d(s) = \sum_{y=0}^{d-1} |\cos(s + yh)|,$$

and  $G_d$  has period  $h$ .

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

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

Its maximum is attained exactly at  $s \equiv 0 \pmod{h}$ , which is equivalent to  $z^d = 1$ .

If  $d = 2m$ , take  $0 \leq s \leq h$ . The first  $m$  cosines are nonnegative and the last  $m$  are nonpositive; an endpoint term may vanish. The two finite sums give

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

Its maximum is attained exactly at  $s \equiv a \pmod{h}$ , equivalently  $z^d = -1$ . Multiplying by two proves the result.  $\square$

Apply Theorem 3.2 with

$$g_y(z) = 1 + \omega^y z.$$

The polynomial  $t^d - (-1)^{d-1}$  gives

$$\prod_k z_k = 1, \quad \prod_k (1 + \omega^y z_k) = 2 > 0.$$

Thus the polar phases

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

have product one, and every root ordering is an order- $d$  maximizer of

$$\bar{\mathcal{I}}_d = \sum_{y=0}^{d-1} \operatorname{Re}[(A_0 + \omega^y A_1) \otimes B_y] + \operatorname{Re}(A_0 \otimes B_d)$$

with exact value

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

This recovers, in the general language above, the first-family counterexamples of Ref. [6].

## 4.2 The target bias

For  $d \geq 4$ , choose the final-two swap

$$\kappa = (0, 1, \dots, d-3, d-1, d-2). \quad (8)$$

The second cyclic autocorrelation of the sequence in Corollary 3.3 is

$$C_2 = \sum_j q_{j+2} \overline{q_j} = \sum_j z_{\kappa_j} \overline{z_{\kappa_{j+1}}}.$$

It vanishes in the canonical order, whereas (8) gives

$$C_2 = (z_{d-1} - z_{d-2})(z_{d-3} - z_0), \quad |C_2| = 4 \sin(\pi/d) \sin(3\pi/d) > 0. \quad (9)$$

Hence the target table is nonuniform.

For a quantitative bound, put

$$x_m = |\widehat{q}_m|^2 - d, \quad \Delta = \max_m x_m.$$

Then  $\sum_m x_m = 0$ , and Fourier inversion at lag two gives

$$C_2 = \frac{1}{d} \sum_m x_m \omega^{-2m}.$$

The nonzero mean-zero sequence  $x_m$  has at most  $d-1$  positive entries, so

$$d|C_2| \leq \sum_m |x_m| = 2 \sum_{x_m > 0} x_m \leq 2(d-1)\Delta.$$

Substitution in (6) proves

$$G(AB|1, d, E) \geq \frac{1}{d^2} + \frac{2 \sin(\pi/d) \sin(3\pi/d)}{d^2(d-1)}. \quad (10)$$

At  $d = 2, 3$ , every root ordering in this particular family is Fourier-flat.

### 4.3 The second SOS-certified family

We now show that the same Bob observables maximize the second family of Ref. [1]. Put  $\eta = e^{\pi i/d}$ , so  $\omega = \eta^2$ , and let

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

This is  $\lambda_{0,\ell-1}$  in the source's cyclic indexing; the formula at  $\ell = 0$  is read literally with  $(-1)^{-1} = -1$ . For Bob's first-family observables, define

$$C_\ell = \sum_{y=0}^{d-1} \omega^{\ell y} B_y.$$

The Hermitian Bell functional is

$$\mathcal{F}_d = \sum_{\ell=0}^{d-1} \operatorname{Re}(\overline{\lambda_\ell} A_\ell \otimes C_\ell). \quad (11)$$

**Theorem 4.2** (Permutation maximizers of the second family). *For every permutation  $\kappa$ , define*

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

*Then every  $A_\ell$  and  $B_y$  has  $d$ -th power  $\mathbf{1}$ , and*

$$C_\ell = d \lambda_\ell D_\ell.$$

*The strategy on  $|\Phi_d\rangle$  attains*

$$\langle \mathcal{F}_d \rangle = d.$$

*With  $B_d = X$ , the augmented Hermitian functional*

$$\overline{\mathcal{F}}_d = \mathcal{F}_d + \operatorname{Re}(A_0 \otimes B_d)$$

*has value  $d+1$ . For the ordering (8), its target  $(A_1, B_d)$  has exactly the distribution (6), and hence obeys the strict gap (10) for every  $d \geq 4$ . Its complete matrix of complex first-harmonic correlators is independent of  $\kappa$ .*

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

$$s_0(z_r) = \varepsilon_r \eta^{r+\delta_d/2}, \quad \varepsilon_r = \begin{cases} +1, & 2r + \delta_d < d, \\ -1, & 2r + \delta_d > d. \end{cases}$$

There is no equality case. Also  $s_y(z_r) = s_0(z_{r+y \bmod d})$ . Therefore the diagonal weight of  $C_\ell$  at a label  $r$  is

$$\sum_y \omega^{\ell y} \overline{s_y(z_r)} = \omega^{-\ell r} S_\ell, \quad S_\ell = \sum_t \omega^{\ell t} \overline{s_0(z_t)}.$$

Let

$$n = \frac{d+1-\delta_d}{2}, \quad r_\ell = \eta^{2\ell-1}.$$

The first  $n$  signs  $\varepsilon_t$  are positive and the rest are negative, while  $r_\ell^d = -1$ . Two geometric sums give

$$\begin{aligned} S_\ell &= \eta^{-\delta_d/2} \left( \sum_{t=0}^{n-1} r_\ell^t - \sum_{t=n}^{d-1} r_\ell^t \right) \\ &= -\frac{2\eta^{-\delta_d/2} r_\ell^n}{1 - r_\ell} \\ &= \frac{(-1)^{\ell-1} \eta^{-\ell\delta_d}}{\sin(\pi(\ell - \frac{1}{2})/d)} = d\lambda_\ell q_\ell. \end{aligned}$$

This proves  $C_\ell = d\lambda_\ell D_\ell$ , including its phase.

The weighted-cycle identity (5) and  $\sum_j \kappa_j = d(d-1)/2$  give

$$D_\ell^d = q_\ell^d \omega^{-\ell \sum_j \kappa_j} \mathbf{1} = (-1)^{\ell(\ell-1+\delta_d)+\ell(d-1)} \mathbf{1} = \mathbf{1}.$$

Indeed,  $\ell(\ell+d-2+\delta_d)$  is even because  $d-2+\delta_d$  is odd. Thus the Alice observables are admissible.

For completeness, the coefficient identity

$$\sum_\ell |\lambda_\ell|^2 = 1$$

follows from

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

the derivative of the finite cotangent-sum identity. Fourier orthogonality and  $B_y^\dagger B_y = \mathbf{1}$  give

$$\sum_\ell C_\ell^\dagger C_\ell = d^2 \mathbf{1}.$$

Consequently, for arbitrary admissible observables,

$$P_\ell = d\lambda_\ell \mathbf{1} - A_\ell \otimes C_\ell$$

satisfies the exact SOS

$$d\mathbf{1} - \mathcal{F}_d = \frac{1}{2d} \sum_{\ell=0}^{d-1} P_\ell^\dagger P_\ell. \quad (12)$$

For our strategy,

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

Hence  $\langle \mathcal{F}_d \rangle = d$ . Since  $A_0 = X$  and  $(X \otimes X) |\Phi_d\rangle = |\Phi_d\rangle$ , the augmentation contributes one. Finally,

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

where the first equality is read entrywise in the weighted shift. Thus the target pair is literally the one in Corollary 3.3. Moreover,

$$\langle A_\ell \otimes B_y \rangle = \frac{\overline{q_\ell}}{d} \sum_{r=0}^{d-1} \omega^{\ell r} \overline{s_y(z_r)},$$

and  $\langle A_\ell \otimes B_d \rangle$  is obtained by deleting the  $\overline{s_y(z_r)}$  factor. These are symmetric sums over the complete root set, so every complex first harmonic is permutation-independent even though higher harmonics and the full target behavior need not be.  $\square$

*Remark 4.3* (Source conventions). Equations (11)–(12) match Eqs. (19), (22), and (23) of Ref. [1]. Its nearby Eq. (20) omits  $d\lambda_\ell$ , and the prose there omits Alice’s complex conjugation, which its theorem restores. We use a real part in the augmentation so that the Bell operator is Hermitian.

#### 4.4 An exact four-outcome certificate

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

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

The sequence in Corollary 3.3 is

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

Thus, for both augmented cyclic families,

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

The accompanying verifier works exactly in  $\mathbb{Q}[x]/(x^8 + 1)$ , reconstructs the published  $\lambda$ ’s, checks  $C_\ell = 4\lambda_\ell D_\ell$ , every fourth-power relation, the full SOS operator identity, both Bell values, and the displayed table.

**Corollary 4.4** (Value-only robustness is impossible). *For either augmented cyclic family and every  $d \geq 4$ , no valid value-only bound*

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

*can hold for all strategies with Bell deficit at most  $\varepsilon$ .*

*Proof.* The exact biased maximizer is feasible for every  $\varepsilon \geq 0$  and has the positive gap (10). This says nothing against bounds that condition on additional observed statistics.  $\square$

## 5 Why the standard $2 \times 2$ qudit route does not immediately work

The standard two-input self-test of a maximally entangled qudit [3] uses Fourier-phase bases. Directly from the geometric amplitude on  $|\Phi_d\rangle$ , its four joint tables have the form

$$p(a, b|x, y) = \frac{\sin^2(\pi\delta_{xy})}{d^3 \sin^2(\pi(a - b + \delta_{xy})/d)}, \quad (\delta_{xy}) = \begin{pmatrix} 1/4 & 3/4 \\ -1/4 & 1/4 \end{pmatrix}, \quad (13)$$

up to input swaps, conjugation, transposition, and output relabeling. Therefore every table has

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

None of the four setting pairs is uniform, for any  $d \geq 2$ . Its ideal joint min-entropy is

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

The existing self-test certifies  $\log_2 d$  local bits, not the desired  $2 \log_2 d$  global bits.

Suppose a third Bob setting is perfectly correlated with either one of Alice's two ideal bases by a separately bounded term. Its cross table with Alice's other basis has half-step offset:

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

Thus the direct “self-test plus perfect anchor” composition already has a nonuniform ideal maximizer. The qubit exception is exactly the case in which the two Alice bases are mutually unbiased.

The following proposition rules out a broader version of the same coefficientwise construction. 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

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

**Proposition 5.1** (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 third-setting term*

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

*can expose the computational PVM on the maximally entangled strategy through the common coefficientwise bound  $K_b \leq \Lambda \mathbf{1}$ .*

*Proof.* Write  $K = C + R C' R^\dagger$ , where  $C, C'$  are Hermitian circulants:

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

The eigenvector equations in column  $r$  are

$$c_m + \rho^{\nu_r(m)} c'_m = 0,$$

where  $\nu_r(m) \in [-r, d-1-r]$  is congruent to  $m \pmod{d}$ . Comparing each equation with its Hermitian conjugate forces

$$c_m = c'_m = 0 \quad \text{unless} \quad m \in \{1, \dots, s\} \cup \{d-s, \dots, d-1\}, \quad s = \min(r, d-1-r).$$

For the surviving modes, the ordinary and wrapped diagonals cancel except in the upper-right and lower-left  $s \times s$  corners. After grouping the first  $s$ , middle  $d-2s$ , and last  $s$  coordinates,

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

where  $T$  is upper-triangular Toeplitz. Its nonzero eigenvalues are  $\pm \sigma_j(T)$ . Hence a nonscalar  $K$  has spectrum on both sides of  $\kappa$ .

For the resulting bound  $\mathcal{L} \leq \Lambda \mathbf{1}$  to be saturated on  $|\Phi_d\rangle$  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 this impossible unless all relevant  $K_b$  are scalar, in which case the term constrains no measurement.  $\square$

*Remark 5.2.* Proposition 5.1 is deliberately narrow. It does not rule out a joint SOS, a different common MUB, a different two-input self-test, or an arbitrary  $2 \times 3$  Bell functional.

## 6 A sufficient private-MUB composition lemma

The preceding obstruction identifies a design route that fails, not the property a successful construction would need. The latter has a short operator-valued formulation.

**Lemma 6.1** (Private-MUB composition). *Let  $\{P_b\}$  and  $\{R_a\}$  be Alice PVMs and let  $\{Q_{\pi(b)}\}$  be a Bob PVM. Suppose, on a purification  $|\Psi\rangle_{ABE}$ ,*

- (i) *the Eve state conditioned on  $P_b$  equals  $\rho_E/d$ ;*
- (ii)  *$Q_{\pi(b)}|\Psi\rangle = P_b|\Psi\rangle$ ;*
- (iii)  *$P_b R_a P_b |\Psi\rangle = d^{-1} P_b |\Psi\rangle$ .*

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

$$\sigma_E^{a, \pi(b)} = \rho_E/d^2$$

*for every  $a, b$ .*

*Proof.* For every Hermitian test operator  $T_E$ , conditions (ii), cross-party commutation, and the projector relations 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.  $\square$

Thus a purification-stable self-test that yields a private reference basis and the state-supported MUB sandwich, plus a compatible third-setting equality condition, would solve the  $2 \times 3$  problem. State extraction alone, average scalar overlaps, and observed uniformity are insufficient.

## 7 Status of the measurement-resource problem

The exact conclusions of this note are summarized in Table 1.

| Scenario or design                | Rigorous status                                                                                                                          |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| $1 \times m$ or $m \times 1$      | Impossible even when the complete behavior is fixed (Theorem 1.1).                                                                       |
| $2 \times 2$ , $d = 2$            | Achievable and therefore setting-minimal; the score is known [4].                                                                        |
| $2 \times 2$ , $d \geq 3$         | Open here. The standard ideal qudit strategy has no uniform pair.                                                                        |
| $2 \times 3$ , $d \geq 3$         | Open here. The direct perfect-anchor composition fails, and Proposition 5.1 rules out one broader exposure route.                        |
| All-dimensional upper benchmark   | $2 \times (d^2 + 1)$ settings in Ref. [2]; the first $d^2$ Bob measurements have three outcomes and may be zero-padded when $d \geq 3$ . |
| First-harmonic polar-linear class | Exact conditional permutation obstruction under the hypotheses of Theorem 3.2.                                                           |
| Two augmented cyclic families     | Fail value-based maximal global randomness for every $d \geq 4$ .                                                                        |

Table 1: What is proved, and what remains open.

No universal impossibility theorem for  $2 \times 2$  at  $d > 2$  is proved. In particular, the spectrum-permutation theorem is class-specific. Nor do the negative ideal-strategy calculations preclude a different constant-setting self-test. The minimum-setting law requested at the start of this program therefore remains unresolved.

The useful positive outcome is a sharper design criterion: a successful Bell score must constrain operator-valued higher information, not merely an unordered relative spectrum or first-harmonic correlators. One exact route would be to prove the hypotheses of Lemma 6.1; another would be a direct operator-valued Fourier cancellation proof requiring less than full self-testing.

## 8 Verification and scope

The public package contains:

- this analytic manuscript and a machine-readable family certificate;
- independent, dependency-free checks of the binary SOS and standard qudit probability tables;
- discovery code for the second-family Fourier construction through  $d = 12$ ;
- an independent exact  $\mathbb{Q}(\zeta_{16})$  verifier for  $d = 4$ ;
- claims and assumptions ledgers, failed approaches, a research log, and a targeted prior-art audit.

The programs are secondary checks and do not formally quantify over every  $d$ .

A targeted primary-source search found no all-dimensional  $2 \times 2$  or  $2 \times 3$  single-score protocol with the required projective  $d$ -outcome global-private conclusion, and no equivalent published permutation theorem for the second cyclic family. This is not proof of worldwide priority. Unindexed, unpublished, or concurrent work may exist. The standard two-input self-test itself identifies global  $2 \log_2 d$  randomness as an open direction [3].

The derivations, manuscript, code, and literature audit were produced with heavy assistance from ChatGPT 5.6 Sol under Alec Kriebel's direction. No AI system is an author or bears responsibility for the claims. Alec Kriebel is the named human author and takes responsibility for releasing the artifacts, while explicitly requesting independent expert validation.

## A Binary benchmark

For binary Hermitian unitaries, set

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

The exact identity

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

proves the maximum  $3\sqrt{3}$ , with cross-party tensor identities suppressed only in this display. Equality yields

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

Putting  $X_A = (A_0 + 2A_1)/\sqrt{3}$  and  $Z_B = (B_0 - 2B_1)/\sqrt{3}$  gives, on the state,

$$B_0 = X_A, \quad Z_B = A_0, \quad \{A_0, X_A\} = 0, \quad \{Z_B, B_0\} = 0.$$

The two associated cross-party stabilizers make  $\langle A_0 T_E \rangle$ ,  $\langle B_0 T_E \rangle$ , and  $\langle A_0 B_0 T_E \rangle$  vanish for every Hermitian  $T_E$ . These are exactly the three nontrivial binary operator-valued Fourier coefficients, so  $\sigma_E^{ab} = \rho_E/4$ .

## 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/2606.21362>.
- [2] M. Farkas, P. Mironowicz, and R. Augusiak, Maximal global device-independent randomness from projective measurements in every dimension, *arXiv:2606.21369* (2026), <https://arxiv.org/abs/2606.21369>.
- [3] 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>.
- [4] L. Woollorton, P. Brown, and R. Colbeck, Tight analytic bound on the trade-off between device-independent randomness and nonlocality, *Physical Review Letters* **129**, 150403 (2022), <https://doi.org/10.1103/PhysRevLett.129.150403>.
- [5] A. Kriebel, The exact quantum value of a cyclic Bell operator, provisional AI-assisted research note (2026), <https://aleckriebel.github.io/Math/papers/cyclic-bell-tsirelson-bound/>.
- [6] A. Kriebel, Maximal violation without maximal global randomness in a cyclic Bell family, provisional AI-assisted research note (2026), <https://aleckriebel.github.io/Math/papers/cyclic-bell-randomness-counterexample/>.
- [7] 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>.
- [8] E. Coccia, S. Padovan, and G. Vallone, Systematic derivation of Tsirelson bounds in arbitrary dimensions, *arXiv:2606.21626* (2026), <https://arxiv.org/abs/2606.21626>.