

Maximal violation without maximal global randomness in a cyclic Bell family

Exact counterexamples in every dimension $d \geq 4$

Alec Kriebel

with heavy assistance from ChatGPT 5.6 Sol

26 July 2026

Abstract

Perito, D’Avino, Jung, Mironowicz, Acin, and Augusiak conjectured that maximal violation of an augmented cyclic Bell functional certifies $2 \log_2 d$ bits of global randomness. We disprove this Bell-value-based assertion for every $d \geq 4$. For each such d , a sparse weighted-shift strategy on $\mathbb{C}^d \otimes \mathbb{C}^d$, with no adversarial side information, attains the exact Bell maximum

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

while the designated joint output distribution is nonuniform. Quantitatively,

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

Both one-party marginals remain uniform, so the obstruction concerns global joint randomness rather than a local-output bias. At $d = 4$, a compact certificate over $\mathbb{Q}(\zeta_{16})$ gives probabilities $1/32$ and $3/32$, hence $G = 3/32 > 1/16$. We reproduce the exact Bell upper certificate, prove the infinite counterexample family from first principles, and provide an exact-arithmetic verifier for the finite witness. The construction does not challenge the separate numerical certificate for the fixed canonical full behavior, and every root ordering in this family is uniform at $d = 2, 3$.

Status. This is an unrefereed, AI-assisted research note. Its proof and exact certificate are public for audit but have not received independent expert review.

1 Definitions and result

Fix $d \geq 2$ and $\omega = e^{2\pi i/d}$. Alice has order- d unitaries A_0, A_1 , Bob has order- d unitaries $B_0, \dots, B_d$, and

$$\mathcal{I}_d = \frac{1}{2} \sum_{x=0}^1 \sum_{y=0}^{d-1} \left(\omega^{xy} A_x \otimes B_y + \omega^{-xy} A_x^\dagger \otimes B_y^\dagger \right), \quad (1)$$

$$\bar{\mathcal{I}}_d = \mathcal{I}_d + \frac{1}{2} \left(A_0 \otimes B_d + A_0^\dagger \otimes B_d^\dagger \right). \quad (2)$$

These are Eqs. (11) and (10), respectively, of Ref. [1]. Put

$$M_d = 2 \csc\left(\frac{\pi}{2d}\right). \quad (3)$$

The exact operator bound $\mathcal{I}_d \leq M_d \mathbf{1}$, proved in a companion note [2], gives

$$\bar{\mathcal{I}}_d \leq (M_d + 1) \mathbf{1}. \quad (4)$$

Section 2 recalls a self-contained proof.

For the output settings $x = 1, y = d$, let σ_E^{ab} be Eve's subnormalized conditional states. Their guessing probability is

$$G(AB \mid 1, d, E) = \max_{\{Q_{ab}\}} \sum_{a,b} \text{Tr}(Q_{ab} \sigma_E^{ab}).$$

Maximal private global randomness would require $\sigma_E^{ab} = \rho_E/d^2$, and hence $G = 1/d^2$.

For clarity, Conjecture 2 of Ref. [1] is printed as follows:

“The maximal violation of $\langle \bar{\mathcal{I}}_d \rangle$, which is equal to $2[d \sin(\pi/(2d))]^{-1} + 1$, certifies $2 \log d$ bits of randomness for settings $x = 1$ and $y = d$.”

Remark 1.1 (Normalization and scope of the refutation). The displayed functional (2) equals $\mathcal{I}_d + \text{Re}(A_0 \otimes B_d)$. Equation (17) of Ref. [1] gives M_d for its canonical unaugmented strategy, and $B_d = Z^\dagger$ makes the added term equal to one. The same paper states the resulting $d = 3$ value as $5 = M_3 + 1$, whereas its printed Conjecture 2 formula gives $7/3$. Thus the factor d in the printed denominator is an internal normalization typo; the evidently intended maximum is $M_d + 1$.

The precise assertion refuted below is the Bell-value implication

$$\langle \bar{\mathcal{I}}_d \rangle = M_d + 1 \implies G(AB \mid 1, d, E) = \frac{1}{d^2}. \quad (5)$$

This is the reading supported by the paper's abstract, introduction, and uniqueness-based symmetry argument. A narrower claim about the randomness of only the canonical *full behavior* is not refuted.

Theorem 1.2 (Nonuniform exact maximizers). *For every integer $d \geq 4$, there is an explicit admissible strategy on $\mathbb{C}^d \otimes \mathbb{C}^d$, with $\mathcal{H}_E = \mathbb{C}$, such that*

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

but

$$G(AB \mid 1, d, E) \geq \frac{1}{d^2} + \frac{2 \sin(\pi/d) \sin(3\pi/d)}{d^2(d-1)} > \frac{1}{d^2}. \quad (6)$$

For the same strategy, each Alice and Bob marginal is uniform. Thus maximal violation does not force maximal observed joint uniformity, and therefore cannot force maximal private global randomness.

Corollary 1.3 (Failure of Bell-value certification). *Let $\mathbf{S}$ range over finite-dimensional strategies, including arbitrary quantum side information, and define*

$$G_{\text{val}}(d) = \sup_{\mathbf{S}: \langle \bar{\mathcal{I}}_d \rangle_{\mathbf{S}} = M_d + 1} G_{\mathbf{S}}(AB \mid 1, d, E).$$

For every $d \geq 4$,

$$G_{\text{val}}(d) \geq \frac{1}{d^2} + \frac{2 \sin(\pi/d) \sin(3\pi/d)}{d^2(d-1)} > \frac{1}{d^2}. \quad (7)$$

Proof. The strategy in Theorem 1.2 is feasible in the displayed supremum. Eve may ignore her system and always guess a most likely pair, so even guessing conditioned on that strategy's full observed behavior is at least $\max_{a,b} p(a, b \mid 1, d)$, which obeys (6). $\square$

The apparent tension with the $d = 4$ calculation in Ref. [1] is resolved by conditioning. Its Appendix B.1 fixes the full canonical behavior before optimizing Eve's guessing probability. Our strategy gives a different full behavior at the same maximum:

	canonical behavior	root-swapped behavior
$\langle \bar{\mathcal{I}}_4 \rangle$	$M_4 + 1$	$M_4 + 1$
Bell-visible first harmonics	identical	identical
$p(a, b \mid 1, 4)$	$1/16$ for all a, b	$1/32$ ($a + b$ even), $3/32$ ($a + b$ odd)

The equality of all correlators used by the Bell functional is proved in Corollary 3.2. Thus the originating fixed-behavior SDP may be correct while maximal Bell value alone fails to certify maximal randomness.

2 The exact Bell upper certificate

We reproduce the argument because global optimality is essential to the counterexample. Write

$$C_y = A_0 + \omega^y A_1, \quad U = A_0^\dagger A_1, \quad F_d(U) = \sum_{y=0}^{d-1} |1 + \omega^y U|.$$

Lemma 2.1 (Polar positive-factor identity). *Let $C = V|C|$ be the polar decomposition of a bounded operator on a Hilbert space; V may be a partial isometry. If B is unitary on another Hilbert space, then*

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

satisfies

$$\frac{|C| + |C^\dagger|}{2} \otimes \mathbf{1} - \operatorname{Re}(C \otimes B) = \frac{1}{2} P^\dagger P. \quad (8)$$

Proof. The initial projection $V^\dagger V$ is the support projection of $|C|$, while polar functional calculus gives $|C^\dagger|^{1/2} V = V|C|^{1/2}$. Consequently,

$$\begin{aligned} P^\dagger P &= |C^\dagger| \otimes \mathbf{1} + |C|^{1/2} V^\dagger V |C|^{1/2} \otimes B^\dagger B \\ &\quad - C \otimes B - C^\dagger \otimes B^\dagger \\ &= (|C| + |C^\dagger|) \otimes \mathbf{1} - C \otimes B - C^\dagger \otimes B^\dagger. \end{aligned}$$

This also shows explicitly why no invertibility assumption is needed. $\square$

Lemma 2.2 (Sharp scalar bound). *For $|z| = 1$,*

$$\sum_{y=0}^{d-1} |1 + \omega^y z| \leq M_d, \quad (9)$$

with equality exactly when

$$z^d = (-1)^{d-1}. \quad (10)$$

Proof. Write $z = e^{2is}$, $h = \pi/d$, and $a = h/2$. Half the left side 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 $s + kh$ lies in $[-\pi/2, \pi/2]$, since $a + mh = \pi/2$, and the finite cosine sum gives

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

Its 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 nonpositive; endpoints cause no ambiguity because the boundary cosine vanishes. Two finite cosine 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 occurs exactly at $s \equiv a \pmod{h}$, equivalently $z^d = -1$. Multiplying by two proves both claims. $\square$

Because $\mathbf{1} + \omega^y U$ is normal,

$$|C_y| = |\mathbf{1} + \omega^y U|, \quad |C_y^\dagger| = A_0 |\mathbf{1} + \omega^y U| A_0^\dagger.$$

Functional calculus and Lemma 2.2 give $F_d(U) \leq M_d \mathbf{1}$. Summing Lemma 2.1 therefore yields the exact gap decomposition

$$\boxed{M_d \mathbf{1} - \mathcal{I}_d = \frac{1}{2} \sum_{y=0}^{d-1} P_y^\dagger P_y + \frac{1}{2} \left[M_d \mathbf{1} - F_d(U) + A_0 (M_d \mathbf{1} - F_d(U)) A_0^\dagger \right] \otimes \mathbf{1}.} \quad (11)$$

Every term is positive. This proves $\mathcal{I}_d \leq M_d \mathbf{1}$ for arbitrary tensor-product unitaries on arbitrary Hilbert spaces, even without the order relations, and (4) follows from $\text{Re}(A_0 \otimes B_d) \leq \mathbf{1}$.

3 Weighted-shift maximizers

Let

$$X|j\rangle = |j + 1 \bmod d\rangle, \quad \delta_d = \begin{cases} 0, & d \text{ odd}, \\ 1, & d \text{ even}, \end{cases}$$

and enumerate the equality roots from Lemma 2.2 by

$$z_k = \exp\left(\frac{\pi i(2k + \delta_d)}{d}\right), \quad k = 0, \dots, d-1. \quad (12)$$

For any ordering $\kappa = (\kappa_0, \dots, \kappa_{d-1})$ of these roots, define

$$\begin{aligned} Z_\kappa &= \text{diag}(z_{\kappa_0}, \dots, z_{\kappa_{d-1}}), \\ s_{y,k} &= \frac{1 + \omega^y z_k}{|1 + \omega^y z_k|}, \\ S_y^\kappa &= \text{diag}(s_{y,\kappa_0}, \dots, s_{y,\kappa_{d-1}}), \\ H_y^\kappa &= \text{diag}(|1 + \omega^y z_{\kappa_0}|, \dots, |1 + \omega^y z_{\kappa_{d-1}}|). \end{aligned}$$

The denominators never vanish because -1 is not a root of $t^d - (-1)^{d-1}$.

Proposition 3.1 (Every root ordering gives a maximizer). *On $\mathbb{C}^d \otimes \mathbb{C}^d$, set*

$$\begin{aligned} A_0 &= X, & A_1 &= XZ_\kappa, \\ V_y &= XS_y^\kappa, & B_y &= \overline{V_y} \quad (0 \leq y < d), \\ B_d &= X, \end{aligned} \tag{13}$$

and use

$$|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j, j\rangle.$$

All observables are unitary, all have d -th power $\mathbf{1}$, and

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

Proof. The z_k are all roots of $t^d - (-1)^{d-1}$. Comparing the constant term and evaluating the polynomial at -1 give

$$\prod_k z_k = 1, \quad \prod_k (1 + \omega^y z_k) = 2. \tag{14}$$

Multiplication by ω^y merely permutes the roots. The second product is real and positive, so

$$\prod_k s_{y,k} = 1.$$

For arbitrary weights t_j ,

$$(X \text{diag}(t_0, \dots, t_{d-1}))^d = \left(\prod_j t_j \right) \mathbf{1}. \tag{15}$$

Equations (14)–(15) prove every order relation in (13); unitarity is immediate.

Moreover,

$$A_0 + \omega^y A_1 = X(\mathbf{1} + \omega^y Z_\kappa) = V_y H_y^\kappa,$$

which is its polar decomposition. The maximally entangled trace identity

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

and $B_y^T = V_y^\dagger$ give

$$\langle \mathcal{I}_d \rangle = \frac{1}{d} \sum_{j,y} |1 + \omega^y z_{\kappa_j}| = \frac{1}{d} \sum_j M_d = M_d.$$

Finally, $X \otimes X$ fixes $|\Phi_d\rangle$, so the added correlator equals one. The upper bound (4) proves global optimality. $\square$

Corollary 3.2 (The Bell-visible correlators do not see the root ordering). *Every ordering κ in Proposition 3.1 gives the same complex first-harmonic correlators occurring in $\overline{\mathcal{I}}_d$.*

Proof. For $0 \leq y < d$, the maximally entangled trace identity gives

$$\begin{aligned}\langle A_0 \otimes B_y \rangle_\kappa &= \frac{1}{d} \operatorname{Tr} \left((S_y^\kappa)^\dagger \right), \\ \langle A_1 \otimes B_y \rangle_\kappa &= \frac{1}{d} \operatorname{Tr} \left(Z_\kappa (S_y^\kappa)^\dagger \right).\end{aligned}$$

Both traces are sums over the complete, unordered root set and hence are independent of κ . More explicitly, the root set is invariant under conjugation and

$$s_{0,k} + \overline{s_{0,k}} = |1 + z_k|.$$

Lemma 2.2 therefore gives $\sum_k s_{0,k} = \sum_k \overline{s_{0,k}} = \csc(\pi/(2d))$. Reindexing the roots for general y , and using $z_k \overline{s_{y,k}} = \omega^{-y} s_{y,k}$, yields

$$\begin{aligned}\langle A_0 \otimes B_y \rangle_\kappa &= \frac{1}{d \sin(\pi/(2d))}, \\ \langle A_1 \otimes B_y \rangle_\kappa &= \frac{\omega^{-y}}{d \sin(\pi/(2d))}.\end{aligned}\tag{16}$$

These agree with the reference canonical strategy (only the $k = d-1$ and $k = 0$ terms, respectively, survive the trace in its Eq. (45)). The added correlator $\langle A_0 \otimes B_d \rangle_\kappa = 1$ is also independent of the ordering, while $\langle A_1 \otimes B_d \rangle_\kappa = d^{-1} \operatorname{Tr} Z_\kappa = 0$. Thus even the first harmonic of the unused target-setting pair is identical; all conjugate first harmonics are identical as well. $\square$

4 The designated output distribution

The eigenvectors of $A_0 = X$ and $A_1 = XZ_\kappa$ can be written

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

where

$$q_0 = 1, \quad q_{j+1} = z_{\kappa_j} q_j.\tag{17}$$

The sequence is cyclic because $\prod_k z_k = 1$. Put

$$\hat{q}_m = \sum_{j=0}^{d-1} q_j \omega^{mj}.$$

The transpose of the outcome- b projector of $B_d = X$ is the outcome- $(-b)$ projector of A_0 . Hence

$$p(a, b \mid 1, d) = \frac{1}{d} |\langle u_{-b}, v_a \rangle|^2 = \frac{|\hat{q}_{-(a+b)}|^2}{d^3}.\tag{18}$$

Parseval gives $\sum_m |\hat{q}_m|^2 = d^2$. As $a + b$ traverses all residues when either output is fixed, (18) immediately implies

$$\sum_b p(a, b \mid 1, d) = \sum_a p(a, b \mid 1, d) = \frac{1}{d}.\tag{19}$$

For $d \geq 4$, choose

$$\kappa = (0, 1, \dots, d-3, d-1, d-2), \quad (20)$$

the canonical ordering with its final two entries exchanged. Consider the second cyclic autocorrelation

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

For the canonical ordering this sum vanishes. Exchanging the last two entries changes only the affected summands and gives

$$C_2 = (z_{d-1} - z_{d-2})(z_{d-3} - z_0), \quad |C_2| = 4 \sin(\pi/d) \sin(3\pi/d) > 0. \quad (21)$$

Thus the Fourier magnitudes cannot all equal d , so the joint table is not uniform.

For the quantitative gap, 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

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

Here the subtracted constant contributes zero because $d \geq 4$ and $\sum_m \omega^{-2m} = 0$. The nonzero mean-zero sequence x_m has at most $d-1$ positive entries. Therefore

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

and

$$\Delta \geq \frac{d|C_2|}{2(d-1)}.$$

With trivial Eve, the optimal guessing strategy selects a most likely output pair, so

$$G = \max_{a,b} p(a, b \mid 1, d) = \frac{d + \Delta}{d^3}.$$

Substitution of (21) proves (6) and Theorem 1.2.

Remark 4.1 (Why this mechanism begins at $d = 4$). Every root ordering in Proposition 3.1 has a flat target table for $d = 2, 3$. For $d = 2$, one has $q = (1, \pm i)$, whose two Fourier magnitudes squared both equal 2. For $d = 3$, write an arbitrary root ordering as (a, b, c) . Since $abc = 1$ and $a + b + c = 0$, the sequence $q = (1, a, ab)$ has nontrivial cyclic autocorrelation

$$a + b + \overline{ab} = a + b + c = 0$$

and its conjugate also vanishes. Hence all three Fourier magnitudes squared equal 3. This family therefore leaves the $d = 2, 3$ maximizing faces unresolved.

5 A sparse exact four-outcome certificate

Let $\zeta = e^{\pi i/8}$, so $\mathbb{Q}(\zeta) \cong \mathbb{Q}[x]/(x^8 + 1)$. At $d = 4$, choose $\kappa = (0, 1, 3, 2)$. Proposition 3.1 becomes

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

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

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

These sparse monomial formulas are exact matrices over $\mathbb{Q}(\zeta_{16})$; no numerical polar decomposition is part of the certificate.

The sequence (17) is

$$q = (1, \zeta^2, -1, \zeta^6).$$

With $\omega = i$, direct finite Fourier transformation gives

$$\hat{q} = (i\sqrt{2}, 2 + i\sqrt{2}, -i\sqrt{2}, 2 - i\sqrt{2}), \quad (|\hat{q}_m|^2)_m = (2, 6, 2, 6).$$

Equation (18) therefore gives

$$p(a, b \mid 1, 4) = \begin{cases} 1/32, & a + b \text{ even,} \\ 3/32, & a + b \text{ odd.} \end{cases} \quad (22)$$

Consequently,

$$G(AB \mid 1, 4, E) = \frac{3}{32} > \frac{1}{16}, \quad H_{\min}(AB \mid E) = 5 - \log_2 3 < 4.$$

The independent verifier reconstructs the observables from the displayed exponents and checks, using exact rational arithmetic modulo $x^8 + 1$, all unitarity and fourth-order relations, all polar factorizations, the original Bell expression, both probability calculations, uniform marginals, the strict guessing gap, and the exact equality of every first harmonic for all settings between the cyclic and root-swapped $d = 4$ strategies.

6 Consequences, verification, and scope

1. After correcting the normalization typo described in Remark 1.1, the Bell-value reading of Conjecture 2 of Ref. [1] is false for every $d \geq 4$.
2. The obstruction needs neither a direct sum nor an Eve-held flag. It occurs on one $d \times d$ block, on a maximally entangled state, while both local marginals remain uniform.
3. The Bell maximum does not determine a unique target behavior in these dimensions. Hence the uniqueness premise of the paper's symmetry argument fails, and the first augmented family cannot self-test a unique maximizing correlation.

4. No upper bound based only on the Bell value or Bell deficit can converge to $1/d^2$ as the deficit tends to zero. Indeed, if $G_{\text{val}}(d, \varepsilon)$ is the supremum of the guessing probability over strategies with $\langle \bar{\mathcal{I}}_d \rangle \geq M_d + 1 - \varepsilon$, the exact witness is feasible for every $\varepsilon \geq 0$, so the lower bound in (7) holds for every ε . Bounds using additional observed statistics are not excluded.
5. The complete maximizing face, its worst guessing probability, and the maximal-violation randomness question for $d = 2, 3$ remain unresolved here. The Appendix proves only a multiplicity restriction, not a classification.

The general SDP discussion in the source preprint permits either a full target distribution or a Bell constraint, but its Appendix B.1 calculation fixes the *full canonical probability distribution*. That calculation can support randomness of the fixed canonical behavior without excluding another behavior at the same Bell maximum. The strategy above supplies exactly such a behavior, and its own full behavior is nonuniform. This note does not dispute the separate protocols of Farkas, Mironowicz, and Augusiak [3], nor the distinct three-outcome robustness study of D’Avino et al. [4].

The accompanying package contains the TeX source, the exact $\mathbb{Q}(\zeta_{16})$ verifier, a compact machine-readable certificate, the all-dimensional constructor and symbolic family certificate, floating point regressions for $d = 2, \dots, 12$, a direct source-convention full-behavior comparison, historical discovery code, claims and assumptions ledgers, failed approaches, a research log, and SHA-256 hashes. The finite programs support the proof but do not formally quantify over all d .

A targeted search on 26 July 2026 found no public equivalent of the weighted-shift counterexample. This does not establish absolute novelty: unindexed, unpublished, or concurrent work may exist. The appropriate priority wording is therefore “to the best of our knowledge.” No external contact occurred during the derivation or priority audit. Alec Kriebel reports that he previously emailed Ignacio Perito about the companion Conjecture 1 result; no reply had been received when this revision was prepared.

The proof architecture, derivations, manuscript, verification code, and literature audit were developed with heavy assistance from ChatGPT 5.6 Sol under Alec Kriebel’s direction. Alec Kriebel is the named human author but cannot independently validate the mathematical claims. Independent expert checking remains necessary.

A A support-level multiplicity restriction

This appendix records a structural consequence that is not needed for the counterexample.

Lemma A.1 (Reflection-product rank bound). *Let T be a 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 $R = \mathbf{1} - 2E$. The ordered product is

$$(TR)^d = T^d (T^{-(d-1)} R T^{d-1}) \cdots (T^{-1} R T) R.$$

Thus $-\mathbf{1} = R_{d-1} \cdots R_0$, where $R_j = T^{-j} R T^j$. Each defect $\mathbf{1} - R_j = 2T^{-j} E T^j$ has rank r . For arbitrary operators $R_1, \dots, R_d$,

$$\text{rank}(\mathbf{1} - R_1 \cdots R_d) \leq \sum_{j=1}^d \text{rank}(\mathbf{1} - R_j),$$

by repeatedly using $\mathbf{1} - AB = (\mathbf{1} - A) + A(\mathbf{1} - B)$. Each reflected defect has rank r ; the left side is $\text{rank}(2\mathbf{1}) = n$. $\square$

Proposition A.2 (Equal supported multiplicities). *Let a finite-dimensional admissible strategy and state $|\Psi\rangle_{ABE}$ attain $\langle \bar{\mathcal{I}}_d \rangle = M_d + 1$. Put*

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

On K , all d roots of $z^d = (-1)^{d-1}$ occur as eigenvalues of U with the same multiplicity. In particular,

$$d \mid \dim K.$$

No statement is made about unused sectors orthogonal to K .

Proof. Equality in the two bounds $\langle \mathcal{I}_d \rangle \leq M_d$ and $\langle \text{Re}(A_0 \otimes B_d) \rangle \leq 1$ is forced separately. Every positive term in (11) therefore vanishes on the state:

$$P_y |\Psi\rangle = 0, \tag{23}$$

$$(M_d \mathbf{1} - F_d(U)) \otimes \mathbf{1} |\Psi\rangle = 0, \tag{24}$$

$$(A_0 \otimes B_d \otimes \mathbf{1}_E) |\Psi\rangle = |\Psi\rangle. \tag{25}$$

The last implication uses $\mathbf{1} - \text{Re } W = \frac{1}{2}(\mathbf{1} - W)^\dagger(\mathbf{1} - W)$ for unitary W .

For any Alice operator R ,

$$(R \otimes \mathbf{1}) |\Psi\rangle = 0 \iff R|_K = 0, \tag{26}$$

as follows from a Schmidt decomposition across $A : (BE)$. Thus (24) places K inside the equality spectral subspace

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

Equation (25) gives $A_0 K = K$.

We next justify a cancellation in (23) without assuming that a polar factor is globally invertible. Let $C_y = V_y |C_y|$ be the canonical polar decomposition, let

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

The bad phase is not in $\mathcal{Z}_d$, so $E_y^{\text{bad}} K = 0$. Together with $A_0 K = K$, this gives $F_y|_K = \mathbf{1}_K$. Also $F_y V_y = V_y$, because F_y is the final support of the polar partial isometry. Since

$$P_y = (|C_y^\dagger|^{1/2} \otimes \mathbf{1})(\mathbf{1} - V_y \otimes B_y),$$

the vector

$$q_y = (\mathbf{1} - V_y \otimes B_y \otimes \mathbf{1}_E) |\Psi\rangle$$

belongs to $\text{ran } F_y \otimes \mathcal{H}_{BE}$. Equation (23) places the same vector in the kernel of $|C_y^\dagger|^{1/2} \otimes \mathbf{1}$, which is orthogonal to that range. Hence $q_y = 0$, or

$$(V_y \otimes B_y \otimes \mathbf{1}_E) |\Psi\rangle = |\Psi\rangle. \tag{27}$$

The space K lies in the initial support of V_y , so the polar factor is an isometry there. Tracing (27) over BE gives $\rho_A = V_y \rho_A V_y^\dagger$, and therefore $V_y K = K$. Hence

$$S_y = A_0^\dagger V_y$$

preserves K . On L , 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 $U = \omega^{-y} S_y^2$ preserves K . We may now let E_k denote the spectral projections of $U|_K$ for the d roots in $\mathcal{Z}_d$.

Put $\eta = e^{\pi i/d}$, and read $y+1$ modulo d , so $S_d = S_0$ and $V_d = V_0$ in the next relation. Comparing adjacent half-angle phases can be done explicitly. For residues $[r]_d \in \{0, \dots, d-1\}$, put

$$r_* = \left\lfloor \frac{d-1}{2} \right\rfloor, \quad \epsilon_r = \begin{cases} +1, & 2r + \delta_d < d, \\ -1, & 2r + \delta_d > d. \end{cases}$$

Equality cannot occur in this definition. Since $\omega^y z_k = z_{[k+y]_d}$ and

$$\frac{1 + z_r}{|1 + z_r|} = \epsilon_r \exp\left(\frac{\pi i(2r + \delta_d)}{2d}\right),$$

direct division of adjacent phases, including the wrap from $d-1$ to 0, 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, with $k(y) = [r_* - y]_d$,

$$S_y^\dagger S_{y+1} = \eta(\mathbf{1} - 2E_{k(y)}), \quad V_{y+1} = \eta V_y(\mathbf{1} - 2E_{k(y)}), \quad (28)$$

and $y \mapsto k(y)$ is a permutation of the d root labels. Raising (27) to the d -th power, using $B_y^d = \mathbf{1}$, and applying (26) gives $V_y^d = \mathbf{1}$ on K . Since $\eta^d = -1$, equation (28) gives

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

Lemma A.1, with $n = \dim K$, yields

$$n \leq d \operatorname{rank} E_k$$

for every k . But the E_k sum to $\mathbf{1}_K$, so their ranks sum to n . Every inequality must therefore be an equality: $\operatorname{rank} E_k = n/d$ for all k . $\square$

Remark A.3. Proposition A.2 is restricted to exact maximizers of the *augmented* functional because the proof uses the A_0 - B_d stabilizer. Equal multiplicities do not imply a Weyl representation, uniqueness, or self-testing; the weighted-shift family is the obstruction.

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] A. Kriebel, The exact quantum value of a cyclic Bell operator, provisional AI-assisted research note (2026), public note and source package: <https://aleckriebel.github.io/Math/papers/cyclic-bell-tsirelson-bound/>.

- [3] 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/2606.21369>.
- [4] 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/2606.21371>.