Orthogonal Minimax Coherence, Conference-Matrix Rigidity, and Cyclotomic MUB Obstructions

Lluis Eriksson*

November 27, 2026

Abstract

We resolve the orthogonal minimax coherence problem $\mu_{\mathbb{R}}(d) := \min_{U \in O(d)} \max_{i,j} |U_{ij}|$ across the entire non-Hadamard residue class $d \equiv 2 \pmod 4$ and establish a sharp polynomial secant lower bound with spectral rigidity for all odd dimensions $d \geq 3$. First, combining a three-line pure-polynomial identity with a Hadamard three-row sign-parity obstruction, we prove $\mu_{\mathbb{R}}(d) \geq 1/\sqrt{d-1}$ for every $d = 4k+2 \geq 6$, together with a complete rigidity theorem: equality holds if and only if $\sqrt{d-1}\,U$ is a conference matrix up to column permutation. Pairing this rigidity with Paley constructions and Belevitch's sum-of-two-squares necessary condition yields an exact arithmetic dichotomy: $\mu_{\mathbb{R}}(d) = 1/\sqrt{d-1}$ for every conference-matrix order (realized rationally in $O(10,\mathbb{Q})$ and $O(26,\mathbb{Q})$), whereas strict inequality $\mu_{\mathbb{R}}(d) > 1/\sqrt{d-1}$ holds unconditionally whenever $d-1$ is not a sum of two squares ($d = 22, 34, 58, 70, 78, \ldots$). Second, for every odd $d \geq 3$, a pure-polynomial secant bound yields $\mu_{\mathbb{R}}(d) \geq 2/\sqrt{4d-3}$, strictly sharpening both the Welch bound $1/\sqrt{d}$ and the quadratic bound $\sqrt{2/(2d-1)}$. Analyzing the equality locus reduces attainment to a symmetric Seidel matrix satisfying $S^2 + S = (d-1)I_d$; zero trace forces $s = \sqrt{4d-3}$ to divide d and hence $s \mid 3$, proving that equality holds if and only if $d = 3$ ($\mu_{\mathbb{R}}(3) = 2/3$, rigidly attained by $I_3 - \frac{2}{3}J_3$) and strict inequality $\mu_{\mathbb{R}}(d) > 2/\sqrt{4d-3}$ holds for every odd $d \geq 5$. Via rational skew-Cayley transforms we construct exact rational circulant witnesses in $SO(5,\mathbb{Q})$ ($\mu = 6/11 < 3/5$) and $SO(7,\mathbb{Q})$ ($\mu = 1188/2437 < 5/7$). Third, translating these bounds to real mutually unbiased bases (MUBs) quantifies the unavoidable real two-basis coherence excess over the complex Welch bound $1/d$, contrasted against an exhaustive exact $\mathbb{Z}[\zeta_{24}]$ cyclotomic ring search over all $24^5 = 7{,}962{,}624$ normalized phase vectors unbiased to $\{I_6, F_6\}$ in $\mathbb{C}^6$, certifying exactly 12 rays forming 4 orthonormal bases whose distinct-ray overlaps lie strictly in $\{0, 1/3\}$ with zero pairs at $1/6$. A two-layer verification artifact accompanies the paper: Layer 1 formalizes the scalar-algebraic, parity, divisibility, and exact-witness arithmetic kernel in 20 constructive, axiom-free Lean 4.36.0 theorems (0 `sorry`, 0 `Classical.choice`); Layer 2 verifies all full matrix constructions, Belevitch classifications, and the exhaustive $\mathbb{Z}[\zeta_{24}]$ search in 16 zero-float Python certificates and 56 adversarial tests.

1 Introduction

For every integer $d \geq 1$, how delocalized can a d-by-d real orthogonal matrix be? Formally, define the *orthogonal minimax coherence*

$$\mu_{\mathbb{R}}(d) := \min_{U \in O(d)} \|U\|_{\max}, \qquad \|U\|_{\max} := \max_{1 \leq i,j \leq d} |U_{ij}|. \tag{1}$$

*Independent Researcher. Code, Lean 4.36.0 proofs, and zero-float certificates archived at https://github.com/lluiseriksson/orthogonal-minimax-coherence-and-conference-rigidity (`v1.0.0`, MIT / CC-BY-4.0, AIRR-FOUNDER-1.0). Manuscript and verification artifacts prepared with Google Antigravity assistance.

Since each row of $U \in O(d)$ has unit Euclidean norm, the Welch lower bound [13] gives $\mu_{\mathbb{R}}(d) \geq 1/\sqrt{d}$. Over $\mathbb{C}^d$, the discrete Fourier transform $F_d = \frac{1}{\sqrt{d}}(\omega_d^{jk})$ attains the unitary minimum $1/\sqrt{d}$ in every dimension. Over $\mathbb{R}^d$, equality $\mu_{\mathbb{R}}(d) = 1/\sqrt{d}$ holds if and only if a real Hadamard matrix of order d exists, which is impossible unless $d \in \{1, 2\}$ or $4 \mid d$. Outside Hadamard orders, the exact value of $\mu_{\mathbb{R}}(d)$ has remained largely open apart from the elementary dimension $d = 3$, where $\mu_{\mathbb{R}}(3) = 2/3$ is attained by the Householder reflection $I_3 - \frac{2}{3}J_3$.

The same quantity governs the geometry of real mutually unbiased bases (MUBs) [14, 4, 8]. For two orthonormal bases $\mathcal{B}_1, \mathcal{B}_2$ of $\mathbb{R}^d$ (or $\mathbb{C}^d$) with change-of-basis matrix U, the maximum squared transition probability is $\mu_2(\mathcal{B}_1, \mathcal{B}_2) := \max_{u \in \mathcal{B}_1, v \in \mathcal{B}_2} |\langle u, v\rangle|^2 = \|U\|_{\max}^2$. Thus $\mu_2^{\mathbb{R}}(d) := \min_{\mathcal{B}_1, \mathcal{B}_2} \mu_2(\mathcal{B}_1, \mathcal{B}_2) = \mu_{\mathbb{R}}(d)^2$ measures the optimal approximation to a pair of real MUBs when no Hadamard matrix of order d exists. In dimension $d = 6$, the smallest non-prime-power dimension where the maximal number of complex MUBs is famously conjectured to be 3 rather than 7 [3, 5, 6, 10], comparing the real obstruction ($\mu_2^{\mathbb{R}}(6) = 1/5 > 1/6$) against the complex cyclotomic obstruction highlights two sharply distinct algebraic mechanisms.

Main Contributions

1. **Complete Resolution and Rigidity for $d \equiv 2 \pmod 4$ (Theorem 1).** We prove $\mu_{\mathbb{R}}(d) \geq 1/\sqrt{d-1}$ for every $d = 4k+2 \geq 6$ via a three-line pure-polynomial inequality and a Hadamard three-row sign-parity obstruction, with zero calculus. We further establish complete rigidity: $\|U\|_{\max} = 1/\sqrt{d-1}$ if and only if $\sqrt{d-1}\,U$ is a conference matrix [1, 9, 7] up to column permutation (closing all partial-zero cases $|N_0| \geq 3$, $|N_0| = 1$, and $|N_0| = 2$). Combining this rigidity with Paley constructions [11] and Belevitch's theorem [1, 2] yields an exact arithmetic dichotomy: $\mu_{\mathbb{R}}(d) = 1/\sqrt{d-1}$ for every conference-matrix order ($d = 6, 10, 14, 18, 26, 30, \dots$), while $\mu_{\mathbb{R}}(d) > 1/\sqrt{d-1}$ strictly whenever $d-1$ is not a sum of two squares ($d = 22, 34, 58, 70, 78, 94, \dots$).

2. **Secant Bound, Unique $d = 3$ Rigidity, and Rational Circulants for Odd d (Theorem 2).** For every odd $d \geq 3$, we prove $\mu_{\mathbb{R}}(d) \geq 2/\sqrt{4d-3}$ using a pure-polynomial secant identity. Analyzing the equality locus forces $2\mu^{-1}U$ (up to signed permutations) to take the form $I_d + 2S$ where S is a symmetric Seidel matrix [12] obeying $S^2 + S = (d-1)I_d$. Trace vanishing forces $s = \sqrt{4d-3}$ to be an integer dividing d, hence $s \mid (4d - s^2) = 3$, proving that equality holds if and only if $d = 3$ ($\mu_{\mathbb{R}}(3) = 2/3$) and strict inequality $\mu_{\mathbb{R}}(d) > 2/\sqrt{4d-3}$ holds for every odd $d \geq 5$. Using rational skew-Cayley transforms $(I - A)(I + A)^{-1}$, we construct explicit exact rational circulant witnesses in $SO(5, \mathbb{Q})$ ($\mu = 6/11$) and $SO(7, \mathbb{Q})$ ($\mu = 1188/2437$), beating the Householder reflections $3/5$ and $5/7$.

3. **Real MUB Defect vs. Exact $\mathbb{Z}[\zeta_{24}]$ MUB-6 Obstruction (Theorem 3).** We translate Theorems 1–2 into exact real two-basis MUB coherence excess bounds over $1/d$, and contrast them with an exhaustive exact ring computation in $\mathbb{Z}[\zeta_{24}] = \mathbb{Z}[x]/(x^8 - x^4 + 1)$ over all $24^5 = 7{,}962{,}624$ normalized 24th-root phase vectors unbiased to $\{I_6, F_6\}$. Exactly 12 rays survive, forming 4 orthonormal bases (an 8-regular orthogonality graph whose complement is $2K_{3,3}$) with distinct-ray overlaps strictly in $\{0, 1/3\}$ and zero pairs at the MUB-6 target $1/6$.

2 Minimax Coherence and Conference-Matrix Rigidity for $d \equiv 2 \pmod 4$

Recall that a $d \times d$ *conference matrix* C has 0 on the diagonal, ± 1 off the diagonal, and satisfies $C^\top C = (d-1)I_d$ [1, 9]. For $d \equiv 2 \pmod 4$, any conference matrix can be normalized to be

symmetric, and Belevitch's theorem [1, 2] states that a conference matrix of order $d \equiv 2 \pmod 4$ can exist only if $d-1 = a^2 + b^2$ is a sum of two integer squares.

Theorem 1 (Complete Minimax Coherence and Conference Rigidity for $d \equiv 2 \pmod 4$)**.** *Let $d = 4k+2 \geq 6$.*

(a) Unconditional lower bound: *For every $U \in O(d)$,*

$$\|U\|_{\max} \;\geq\; \frac{1}{\sqrt{d-1}}. \tag{2}$$

(b) Complete rigidity: *An orthogonal matrix $U \in O(d)$ attains $\|U\|_{\max} = 1/\sqrt{d-1}$ if and only if there exists a permutation matrix Π such that $\sqrt{d-1}\,U\Pi$ is a $d \times d$ conference matrix.*

(c) Belevitch–Paley arithmetic dichotomy: *Whenever a conference matrix of order d exists (in particular for every $d = q+1$ with $q \equiv 1 \pmod 4$ a prime power via the Paley construction, including rational orthogonal realizations $\frac{1}{3}C_{10} \in O(10, \mathbb{Q})$ and $\frac{1}{5}C_{26} \in O(26, \mathbb{Q})$), we have exact equality $\mu_{\mathbb{R}}(d) = 1/\sqrt{d-1}$. Conversely, whenever $d-1$ is not a sum of two integer squares (for instance $d \in \{22, 34, 58, 70, 78, 94\}$ and every $d \equiv 4, 7 \pmod 9$ with $d \equiv 2 \pmod 4$), strict inequality holds:*

$$\mu_{\mathbb{R}}(d) \;>\; \frac{1}{\sqrt{d-1}}. \tag{3}$$

Proof. We first record two elementary scalar facts for any real numbers $0 \leq x, y \leq \mu$:

$$xy - (x^2 + y^2 - \mu^2) = (\mu - x)(\mu - y) + x(\mu - x) + y(\mu - y) \geq 0, \tag{4}$$

$$x^2 + y^2 + xy \leq 3\mu^2. \tag{5}$$

Both (4) and (5) are immediate algebraic identities/bounds, with equality in (5) iff $x = y = \mu$, and equality in (4) for $x, y > 0$ iff $x = y = \mu$.

Proof of (a). Suppose for contradiction that $U \in O(d)$ has $\mu := \|U\|_{\max} < 1/\sqrt{d-1}$, so $(d-1)\mu^2 < 1$. For every entry U_{ij}, unit row norm implies

$$U_{ij}^2 = 1 - \sum_{\ell \neq j} U_{i\ell}^2 \geq 1 - (d-1)\mu^2 > 0, \tag{6}$$

so every entry of U is strictly nonzero and has a well-defined sign $\sigma_{ij} \in \{+1, -1\}$. Consider the first three rows r_1, r_2, r_3 of U (valid since $d \geq 6$). Multiplying column j by σ_{1j} preserves $O(d)$ and $\|U\|_{\max}$ while ensuring $\sigma_{1j} = +1$ for all $j \in \{1, \ldots, d\}$. Partition $\{1, \ldots, d\}$ by the sign pairs $(\sigma_{2j}, \sigma_{3j})$ into four cardinalities a, b, c, e corresponding to $(+,+), (+,-), (-,+), (-,-)$, so $a + b + c + e = d = 4k+2$. The counts of positive entrywise products among the three pairs of rows are $p_{12} = a + b$, $p_{13} = a + c$, and $p_{23} = a + e$, whose sum is

$$p_{12} + p_{13} + p_{23} = 2a + (a + b + c + e) = 2a + 4k + 2 \equiv 0 \pmod 2. \tag{7}$$

Since $3(2k+1) = 6k+3$ is odd, we cannot have $p_{12} = p_{13} = p_{23} = 2k+1$. Hence some pair of rows (u, v) among $\{r_1, r_2, r_3\}$ (after replacing v by $-v$ if necessary) satisfies $|P| = p \geq 2k+2$ and $|N| = q = d - p \leq 2k$, where $P := \{j : u_j v_j > 0\}$ and $N := \{j : u_j v_j < 0\}$ partition $\{1, \ldots, d\}$.

Write $x_j := |u_j| \in (0, \mu]$ and $y_j := |v_j| \in (0, \mu]$. Using $\langle u, v \rangle = 0$, (4) on P, $\sum_{j=1}^{d}(x_j^2 + y_j^2) = 2$, and (5) on N:

$$\begin{aligned} 0 = \sum_{j \in P} x_j y_j - \sum_{j \in N} x_j y_j &\geq \sum_{j \in P}(x_j^2 + y_j^2 - \mu^2) - \sum_{j \in N} x_j y_j \\ &= 2 - p\mu^2 - \sum_{j \in N}(x_j^2 + y_j^2 + x_j y_j) \\ &\geq 2 - (p + 3q)\mu^2 = 2 - (d + 2q)\mu^2. \end{aligned} \tag{8}$$

Because $q \le 2k = (d-2)/2$, we have $d+2q \le 2(d-1)$, whence $2 \le 2(d-1)\mu^2$, i.e., $\mu^2 \ge 1/(d-1)$, contradicting $\mu < 1/\sqrt{d-1}$.

Proof of (b). If $\sqrt{d-1}\,U\Pi$ is a conference matrix, clearly $U \in O(d)$ and $\|U\|_{\max} = 1/\sqrt{d-1}$. Conversely, suppose $U \in O(d)$ attains $\mu = \|U\|_{\max} = 1/\sqrt{d-1}$. Call a row *zero-bearing* if it contains at least one zero entry, and let $Z \subseteq \{1,\dots,d\}$ be the set of zero-bearing rows and $N_0 := \{1,\dots,d\} \setminus Z$ the set of strictly nonzero rows.

Step 1 (Zero-bearing rows and distinct zero columns). If row $i \in Z$ has $U_{ij} = 0$, then $1 = \sum_{\ell \ne j} U_{i\ell}^2 \le (d-1)\mu^2 = 1$, forcing $|U_{i\ell}| = \mu$ for all $\ell \ne j$; thus every row in Z has a *unique* zero entry and $d-1$ entries in $\{\pm\mu\}$. Moreover, two distinct rows $i_1, i_2 \in Z$ cannot have their unique zero in the same column j: otherwise $\mu^{-2}\langle r_{i_1}, r_{i_2}\rangle$ would be a sum of $d-1 = 4k+1$ (odd) numbers in $\{\pm 1\}$, which can never equal 0. Therefore the zeros of Z occupy $|Z|$ distinct columns $C_Z \subseteq \{1,\dots,d\}$. Applying the same unit-norm argument to each column $c \in C_Z$ shows that every column $c \in C_Z$ has a unique zero (in Z) and all remaining $d-1$ entries in $\{\pm\mu\}$; in particular, every entry in $N_0 \times C_Z$ has magnitude μ.

Step 2 (Eliminating $|N_0| \ge 3$). If $|N_0| \ge 3$, every entry of any three rows in N_0 is strictly nonzero, so the exact sign-parity and polynomial derivation (8) applies verbatim to some pair $u, v \in N_0$ with $q \le 2k$. Since $2 - 2(d-1)\mu^2 = 0$, equality must hold throughout (8). Because $x_j, y_j > 0$ for all j, equality in (4) on P and in (5) on N forces $x_j = \mu$ for all $j \in \{1,\dots,d\}$, yielding $\|u\|_2^2 = d\mu^2 = d/(d-1) > 1$, a contradiction. Thus $|N_0| \le 2$.

Step 3 (Eliminating $|N_0| = 1$). If $N_0 = \{r_1\}$, let $C_0 = \{1,\dots,d\} \setminus C_Z = \{c_1\}$. By Step 1, row r_1 has $|C_Z| = d-1$ entries of magnitude μ, whose sum of squares is already $(d-1)\mu^2 = 1$. Hence $U_{r_1,c_1} = 0$, contradicting $r_1 \in N_0$.

Step 4 (Eliminating $|N_0| = 2$). If $N_0 = \{r_1, r_2\}$, let $C_0 = \{c_1, c_2\}$. By Step 1, row r_1 has $|C_Z| = d-2$ entries of magnitude μ, so $U_{r_1,c_1}^2 + U_{r_1,c_2}^2 = 1 - (d-2)\mu^2 = \mu^2$. Write $U_{r_1,c_1} = \mu\alpha$ and $U_{r_1,c_2} = \mu\beta$ with $\alpha^2 + \beta^2 = 1$ and $\alpha \ne 0$, $\beta \ne 0$. Since $|Z| = d-2 \ge 4$, pick any row $i \in Z$; let $j_i \in C_Z$ be its unique zero column. Row i has entries $\pm\mu$ in all $d-3 = 4k-1$ columns of $C_Z \setminus \{j_i\}$ and in c_1, c_2 (with signs $\sigma_1, \sigma_2 \in \{\pm 1\}$). Orthogonality $\langle r_1, r_i\rangle = 0$ divides by μ^2 to give

$$0 = m_i + \sigma_1\alpha + \sigma_2\beta, \tag{9}$$

where m_i is a sum of $4k-1$ (odd) numbers in $\{\pm 1\}$, hence an odd integer. Yet $(\sigma_1\alpha + \sigma_2\beta)^2 = \alpha^2 + \beta^2 + 2\sigma_1\sigma_2\alpha\beta = 1 + 2\sigma_1\sigma_2\alpha\beta \le 2 < 9$, so the odd integer m_i must satisfy $m_i^2 = 1$. Consequently $1 + 2\sigma_1\sigma_2\alpha\beta = 1$, forcing $\alpha\beta = 0$, contradicting $\alpha, \beta \ne 0$.

Therefore $N_0 = \emptyset$: every row and column contains a unique zero, and all off-zero entries lie in $\{\pm 1/\sqrt{d-1}\}$. Permuting columns to place the zeros on the diagonal makes $\sqrt{d-1}\,U\Pi$ a conference matrix.

Proof of (c). Because $O(d)$ is compact and $U \mapsto \|U\|_{\max}$ is continuous, $\mu_{\mathbb{R}}(d)$ is attained by some $U^* \in O(d)$. By (b), $\mu_{\mathbb{R}}(d) = 1/\sqrt{d-1}$ if and only if a conference matrix of order d exists. For every prime power $q \equiv 1 \pmod 4$, Paley's quadratic-residue construction [11] yields a symmetric conference matrix of order $d = q+1$; when q is an odd square ($q = 9, 25, 49, \dots$), $\frac{1}{\sqrt{q}} C_{q+1} \in O(q+1, \mathbb{Q})$ is rational orthogonal. Conversely, by Belevitch's theorem [1, 2], no conference matrix of order $d \equiv 2 \pmod 4$ exists unless $d-1$ is a sum of two squares, so compactness and (b) force strict inequality $\mu_{\mathbb{R}}(d) > 1/\sqrt{d-1}$. □

3 Odd Dimensions: Secant Bound, Spectral Rigidity, and Rational Circulants

For odd dimensions $d = 2k+1 \ge 3$, every pair of orthogonal rows automatically has an unbalanced sign partition ($|P| \ne |N|$) whenever all entries are nonzero, eliminating the need

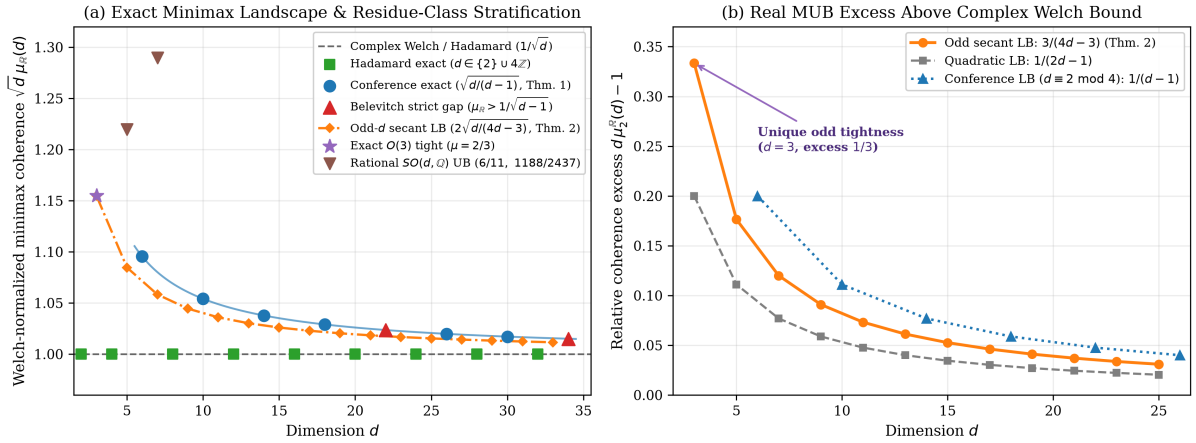

Figure 1: **Orthogonal minimax coherence landscape across residue classes.** (a) Welch-normalized coherence $\sqrt{d}\,\mu_{\mathbb{R}}(d)$ for $2 \le d \le 34$: Hadamard orders achieve 1, conference orders ($d \equiv 2 \pmod 4$, $d-1 = a^2+b^2$) achieve $\sqrt{d/(d-1)}$ (Theorem 1), red triangles mark the lower bound $\sqrt{d/(d-1)}$ at Belevitch-obstructed orders ($d = 22, 34$) where strict inequality $\mu_{\mathbb{R}}(d) > 1/\sqrt{d-1}$ holds, and odd orders satisfy the secant lower bound $2\sqrt{d/(4d-3)}$ (Theorem 2) with exact rational witnesses at $d = 3, 5, 7$. (b) Relative real two-basis MUB coherence excess $d\,\mu_2^{\mathbb{R}}(d) - 1$ comparing the odd secant bound $3/(4d-3)$, the quadratic bound $1/(2d-1)$, and the conference bound $1/(d-1)$.

for three rows. Replacing the quadratic bound (4) by an exact secant linearization of $\sqrt{\mu^2 - s}$ sharpens the lower bound uniformly and yields a complete spectral-divisibility rigidity theorem.

Theorem 2 (Odd-Dimension Secant Bound, Unique $d = 3$ Tightness, and Rational Witnesses)**.** *Let $d = 2k+1 \ge 3$ be odd.*

(a) Unconditional secant lower bound: *For every $U \in O(d)$,*

$$\|U\|_{\max} \;\ge\; \frac{2}{\sqrt{4d-3}} \;>\; \sqrt{\frac{2}{2d-1}} \;>\; \frac{1}{\sqrt{d}}. \tag{10}$$

(b) Unique $d = 3$ tightness via spectral divisibility: *Equality $\mu_{\mathbb{R}}(d) = 2/\sqrt{4d-3}$ holds if and only if $d = 3$ (where $\mu_{\mathbb{R}}(3) = 2/3$, rigidly attained up to signed row/column permutations by $I_3 - \frac{2}{3}J_3$). For every odd $d \ge 5$, strict inequality holds unconditionally:*

$$\mu_{\mathbb{R}}(d) \;>\; \frac{2}{\sqrt{4d-3}}. \tag{11}$$

(c) Exact rational circulant upper bounds: *Rational skew-Cayley transforms yield explicit special orthogonal circulant witnesses $U_5 = \frac{1}{11}\mathrm{circ}(3,6,2,-6,6) \in SO(5,\mathbb{Q})$ and $U_7 = \frac{1}{2437}\mathrm{circ}(-939,-522,1158,-384,1188,894,1042) \in SO(7,\mathbb{Q})$, certifying*

$$\frac{2}{\sqrt{17}} < \mu_{\mathbb{R}}(5) \le \frac{6}{11} < \frac{3}{5}, \qquad \frac{2}{5} < \mu_{\mathbb{R}}(7) \le \frac{1188}{2437} < \frac{5}{7}, \tag{12}$$

strictly improving the Householder upper bounds $(d-2)/d$.

Proof. Proof of (a). Let $U \in O(d)$ with $\mu := \|U\|_{\max}$, and assume $\mu \le 2/\sqrt{4d-3}$ (otherwise (a) is immediate). Since $4(d-1) < 4d-3$, we have $(d-1)\mu^2 \le 4(d-1)/(4d-3) < 1$, so every entry satisfies $U_{ij}^2 \ge 1 - (d-1)\mu^2 > 0$ (strictly nonzero). Set $\Delta := d\mu^2 - 1$. Because d is odd, the

row entries cannot all equal $\pm 1/\sqrt{d}$ (else two rows would have inner product $\frac{1}{d}\sum_{j=1}^{d}(\pm 1) \neq 0$), so $0 < \Delta < \mu^2$. Let $r := \sqrt{\mu^2 - \Delta} = \sqrt{1-(d-1)\mu^2} > 0$ and $c := (\mu - r)/\Delta > 0$. Since $2c\mu - c^2\Delta = c(2\mu - (\mu - r)) = (\mu - r)(\mu + r)/\Delta = 1$, we have the exact polynomial identity

$$(\mu^2 - s) - (\mu - cs)^2 = c^2 s(\Delta - s) \geq 0 \qquad \forall\, s \in [0, \Delta], \tag{13}$$

with equality iff $s \in \{0, \Delta\}$. Taking square roots (as $\mu - cs \geq \mu - c\Delta = r > 0$) gives $\sqrt{\mu^2 - s} \geq \mu - cs$ on $[0, \Delta]$.

Now pick any two distinct rows u, v of U. Since all entries are nonzero and $d = 2k+1$ is odd, replacing v by $-v$ if necessary gives $|P| = p \geq k+1$ and $|N| = q = d - p \leq k$. Define $s_j := \mu^2 - u_j^2 \in [0, \Delta]$ and $t_j := \mu^2 - v_j^2 \in [0, \Delta]$, so $\sum_{j=1}^{d} s_j = \sum_{j=1}^{d} t_j = \Delta$. On P, multiplying $|u_j| \geq \mu - cs_j$ and $|v_j| \geq \mu - ct_j$ yields

$$|u_j v_j| \geq (\mu - cs_j)(\mu - ct_j) = \mu^2 - c\mu(s_j + t_j) + c^2 s_j t_j \geq \mu^2 - c\mu(s_j + t_j). \tag{14}$$

Summing (14) over $j \in P$, noting $\sum_{j\in P}(s_j + t_j) \leq 2\Delta$ and $c\Delta = \mu - r$, gives

$$\sum_{j \in P} |u_j v_j| \geq p\mu^2 - 2\mu c\Delta = (p-2)\mu^2 + 2\mu r. \tag{15}$$

On N, $\sum_{j\in N} |u_j v_j| \leq q\mu^2$. Since $\langle u, v\rangle = 0$ and $q - p \leq -1$, we obtain

$$2\mu r \leq (q - p + 2)\mu^2 \leq \mu^2 \implies 2r \leq \mu \implies 4(1-(d-1)\mu^2) \leq \mu^2, \tag{16}$$

which rearranges to $(4d-3)\mu^2 \geq 4$, proving $\mu \geq 2/\sqrt{4d-3}$. The strict comparisons $4/(4d-3) > 2/(2d-1) > 1/d$ hold for all $d \geq 3$ because $4(2d-1) - 2(4d-3) = 2 > 0$ and $4d - (4d-3) = 3 > 0$.

Proof of (b). Suppose $U \in O(d)$ attains equality $\mu = 2/\sqrt{4d-3}$. Then $r = \mu/2$, and for every pair of rows (u, v) (oriented so $p \geq k+1$), equality must hold in every step of (a): $p = k+1$, $q = k$; $s_j = t_j = 0$ for all $j \in N$; $\sum_{j\in P} s_j = \sum_{j\in P} t_j = \Delta$; $s_j, t_j \in \{0, \Delta\}$ by (13); and $s_j t_j = 0$ for all $j \in P$ by (14). Consequently, every row of U has *exactly one* entry of magnitude $r = \mu/2$ and $d-1$ entries of magnitude μ, and no two rows share the column of their $(\mu/2)$-entry.

Permuting columns so the $(\mu/2)$-entries lie on the diagonal, and scaling $M := \frac{2}{\mu}U$, we obtain an integer matrix M with diagonal entries $\sigma_{ii} \in \{\pm 1\}$, off-diagonal entries $2\sigma_{ij}$ ($\sigma_{ij} \in \{\pm 1\}$), and $MM^\top = (4d-3)I_d$. Multiplying row i by σ_{ii} preserves orthogonality and sets every diagonal entry of M to $+1$. For any distinct rows $i \neq j$, orthogonality $\langle M_i, M_j\rangle = 0$ gives

$$2(\sigma_{ij} + \sigma_{ji}) + 4\sum_{\ell \neq i,j} \sigma_{i\ell}\sigma_{j\ell} = 0 \implies \frac{\sigma_{ij} + \sigma_{ji}}{2} = -\sum_{\ell \neq i,j} \sigma_{i\ell}\sigma_{j\ell}. \tag{17}$$

Because $d-2$ is odd, the right-hand side is an odd integer; since $(\sigma_{ij} + \sigma_{ji})/2 \in \{-1, 0, +1\}$, it cannot be 0, forcing $\sigma_{ij} = \sigma_{ji}$ for all $i \neq j$. Thus $M = I_d + 2S$, where S is a symmetric Seidel matrix ($S = S^\top$, $S_{ii} = 0$, $S_{ij} \in \{\pm 1\}$ for $i \neq j$). Expanding $M^2 = (4d-3)I_d$ yields

$$I_d + 4S + 4S^2 = (4d-3)I_d \iff S^2 + S = (d-1)I_d. \tag{18}$$

Every eigenvalue of S therefore belongs to $\{\frac{-1+\sqrt{4d-3}}{2}, \frac{-1-\sqrt{4d-3}}{2}\}$, with integer multiplicities m_+, m_- summing to d. Since $\mathrm{tr}(S) = 0$,

$$0 = -\frac{d}{2} + (m_+ - m_-)\frac{\sqrt{4d-3}}{2} \implies (m_+ - m_-)\sqrt{4d-3} = d. \tag{19}$$

Because $d > 0$ and $m_+ - m_- \in \mathbb{Z}$, the quantity $s := \sqrt{4d-3} = d/(m_+ - m_-)$ is rational and its square $4d-3$ is an integer, so $s \in \mathbb{Z}_{>0}$ and $s \mid d$. Therefore $s \mid (4d - s^2) = 3$, forcing $s \in \{1, 3\}$. Since $d \geq 3$, $4d - 3 \geq 9$, so uniquely $s = 3$ and $d = 3$. At $d = 3$, $S^2 + S = 2I_3$ forces S to have

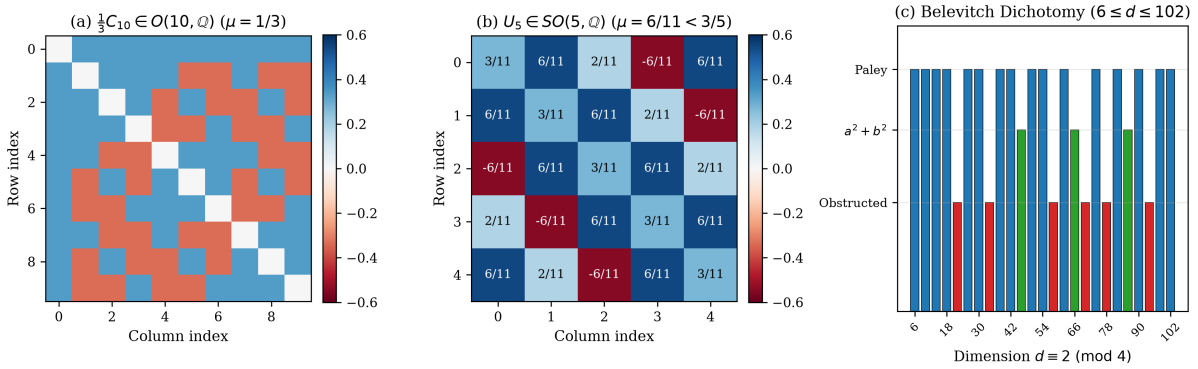

Figure 2: **Exact rational witnesses and Belevitch arithmetic dichotomy.** (a) Rational orthogonal Paley conference matrix $\frac{1}{3}C_{10} \in O(10, \mathbb{Q})$ achieving $\mu_{\mathbb{R}}(10) = 1/3$. (b) Exact rational circulant $U_5 \in SO(5, \mathbb{Q})$ achieving $\mu = 6/11 < 3/5$. (c) Belevitch dichotomy across all 25 dimensions $d \equiv 2 \pmod 4$ with $6 \le d \le 102$: Paley prime-power orders (blue), remaining sum-of-two-squares orders (green), and Belevitch-obstructed orders $d \in \{22, 34, 58, 70, 78, 94\}$ proving strict gap $\mu_{\mathbb{R}}(d) > 1/\sqrt{d-1}$ (red).

eigenvalues 1 (multiplicity 2) and -2 (multiplicity 1), hence $S = -(J_3 - I_3)$ up to diagonal sign conjugation, recovering $U = I_3 - \frac{2}{3}J_3$ uniquely up to signed permutations. For every odd $d \ge 5$, compactness of $O(d)$ then yields strict inequality $\mu_{\mathbb{R}}(d) > 2/\sqrt{4d-3}$.

Proof of (c). For any skew-symmetric $A \in \mathbb{Q}^{d\times d}$, the Cayley transform $U = (I_d - A)(I_d + A)^{-1}$ lies in $SO(d, \mathbb{Q})$. Taking circulant skew-symmetric generators on $\mathbb{Z}_5$ with $(a_1, a_2) = (1/2, -1)$ gives $U_5 = \frac{1}{11}\mathrm{circ}(3, 6, 2, -6, 6)$, satisfying $U_5^\top U_5 = I_5$, $\det(U_5) = +1$, and $\|U_5\|_{\max} = 6/11$. Taking $(a_1, a_2, a_3) = (4, -1, -2)$ on $\mathbb{Z}_7$ gives $U_7 = \frac{1}{2437}\mathrm{circ}(-939, -522, 1158, -384, 1188, 894, 1042) \in SO(7, \mathbb{Q})$ with $\|U_7\|_{\max} = 1188/2437$. Direct integer arithmetic confirms $4 \cdot 11^2 = 484 < 612 = 17 \cdot 6^2$, $6/11 < 3/5$, $2/5 < 1188/2437 < 5/7$. □

4 Real MUB Coherence Defect vs. Exact $\mathbb{Z}[\zeta_{24}]$ MUB-6 Obstruction

In quantum information theory, two orthonormal bases $\mathcal{B}_1, \mathcal{B}_2$ of $\mathbb{F}^d$ ($\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$) are mutually unbiased if $|\langle u, v\rangle|^2 = 1/d$ for all $u \in \mathcal{B}_1, v \in \mathcal{B}_2$ [14, 8]. While complex MUB pairs exist in every dimension via F_d, real MUB pairs fail whenever $d \notin \{1, 2\} \cup 4\mathbb{Z}$ [4]. In $\mathbb{C}^6$, pairs and triples of MUBs exist (including infinite continuous families of MUB-triplets [3, 10]), whereas no quadruple of MUBs has ever been found [5, 6]. We pair our exact real two-basis coherence defects with an exhaustive, zero-float algebraic certification of the 24th-root cyclotomic sector unbiased to $\{I_6, F_6\}$.

Theorem 3 (Real MUB Excess and Exhaustive $\mathbb{Z}[\zeta_{24}]$ MUB-6 Cyclotomic Obstruction)**.**

(a) Unavoidable real two-basis MUB coherence excess: *Over all pairs of orthonormal bases* $(\mathcal{B}_1, \mathcal{B}_2)$ *of* $\mathbb{R}^d$, *let* $\mu_2^{\mathbb{R}}(d) := \min_{\mathcal{B}_1,\mathcal{B}_2} \max_{u\in\mathcal{B}_1, v\in\mathcal{B}_2} \langle u, v\rangle^2$. *Then:*

$$\mu_2^{\mathbb{R}}(d) - \frac{1}{d} \ge \frac{1}{d(d-1)} \quad (d \equiv 2 \pmod 4,\ d \ge 6;\ \textit{strict if } d - 1 \ne a^2 + b^2), \tag{20}$$

$$\mu_2^{\mathbb{R}}(d) - \frac{1}{d} \ge \frac{3}{d(4d-3)} \quad (d \textit{ odd},\ d \ge 3;\ \textit{exact } 1/9 \textit{ at } d = 3,\ \textit{strict for } d \ge 5). \tag{21}$$

(b) Exhaustive $\mathbb{Z}[\zeta_{24}]$ MUB-6 sector classification: *Let* $\mathcal{V}_{24} \subset \mathbb{C}^6$ *be the subset of the* $24^5 = 7{,}962{,}624$ *normalized 24th-root phase vectors* $v = \frac{1}{\sqrt{6}}(1, \zeta_{24}^{e_1}, \ldots, \zeta_{24}^{e_5})^\top$ *($e_j \in \mathbb{Z}/24\mathbb{Z}$) that*

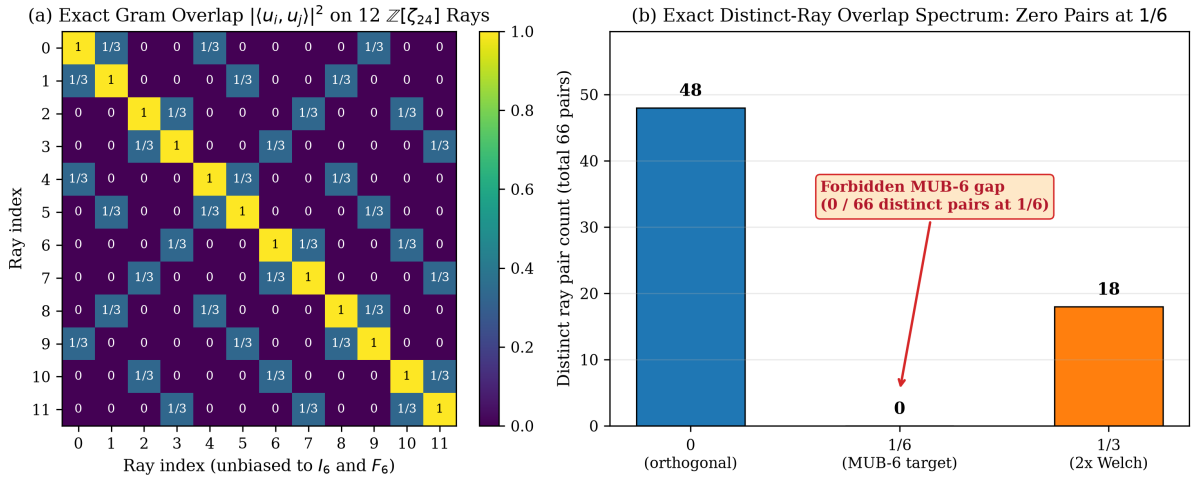

Figure 3: **Exhaustive $\mathbb{Z}[\zeta_{24}]$ cyclotomic MUB-6 obstruction.** (a) Exact Gram overlap matrix $|\langle u_i, u_j\rangle|^2$ across all 12 rays in $\mathcal{V}_{24}$ unbiased to $\{I_6, F_6\}$. (b) Distinct-ray overlap distribution (48 orthogonal pairs at 0, 18 pairs at 1/3, and strictly 0 pairs at the MUB-6 target 1/6).

are unbiased to both I_6 and the 6-point Fourier basis F_6. Exhaustive exact arithmetic in the cyclotomic ring $\mathbb{Z}[\zeta_{24}] \cong \mathbb{Z}[x]/(x^8 - x^4 + 1)$ certifies:

(i) $|\mathcal{V}_{24}| = 12$ *exactly;*

(ii) *the orthogonality graph on $\mathcal{V}_{24}$ is 8-regular (complement isomorphic to $2K_{3,3}$) and contains exactly 4 orthonormal bases (6-cliques);*

(iii) *across all $\binom{12}{2} = 66$ distinct pairs in $\mathcal{V}_{24}$, the exact squared overlap spectrum is $\{0$ (48 pairs), $1/3$ (18 pairs)$\}$, and across all 216 vector pairs between distinct bases the spectrum is $\{0$ (132), $1/3$ (72), 1 (12)$\}$. In particular,* zero *pairs attain $|\langle u, v\rangle|^2 = 1/6$: no fourth basis unbiased to $\{I_6, F_6\}$ and any third basis in $\mathcal{V}_{24}$ exists within the 24th-root cyclotomic sector.*

Proof. Part (a) follows directly by squaring Theorems 1 and 2 since $\mu_2^{\mathbb{R}}(d) = \mu_{\mathbb{R}}(d)^2$ and $\frac{1}{d-1} - \frac{1}{d} = \frac{1}{d(d-1)}$, $\frac{4}{4d-3} - \frac{1}{d} = \frac{3}{d(4d-3)}$.

For (b), note that the (j,k)-entry of $\sqrt{6}\,F_6$ is $\omega_6^{jk} = \zeta_{24}^{4jk}$. Unbiasedness of $v = \frac{1}{\sqrt{6}}(\zeta_{24}^{e_j})_{j=0}^5$ ($e_0 = 0$) to F_6 is equivalent in $\mathbb{Z}[\zeta_{24}]$ to $|S_k|^2 = 6$ for $k = 0, \ldots, 5$, where $S_k := \sum_{j=0}^5 \zeta_{24}^{e_j - 4jk}$. Splitting $S_k = E_k + O_k$ into even ($j \in \{0,2,4\}$) and odd ($j \in \{1,3,5\}$) indices satisfies $S_{k+3} = E_k - O_k$ for $k = 0, 1, 2$ because $\zeta_{24}^{-12j} = (-1)^j$. By the parallelogram law in $\mathbb{Z}[\zeta_{24}]$,

$$|S_k|^2 + |S_{k+3}|^2 = 2(|E_k|^2 + |O_k|^2) = 12 \implies |E_k|^2 + |O_k|^2 = 6 \qquad (k = 0, 1, 2). \tag{22}$$

This exact necessary invariant permits a lossless meet-in-the-middle partition of all $24^5 = 7{,}962{,}624$ phase tuples: indexing all $24^2 = 576$ even pairs (e_2, e_4) by $(|E_0|^2, |E_1|^2, |E_2|^2) \in \mathbb{Z}[\zeta_{24}]^3$ and matching against all $24^3 = 13{,}824$ odd triples (e_1, e_3, e_5) with complementary norm triple $(6 - |E_k|^2)_{k=0}^2$, then checking $|E_k \pm O_k|^2 = 6$ exactly in $\mathbb{Z}[x]/(x^8 - x^4 + 1)$. The exhaustive search (Certificate `cert16`) returns exactly 12 rays, partitions into two blocks of $3 + 3$ rays generating $2 \times 2 = 4$ orthonormal bases, and certifies every exact squared inner product in $\{0, 1/3\}$ for distinct rays. □

5 Formal Verification Architecture and Scope

To prevent ambiguity between machine-checked proof scope and computational certification, our artifact separates two complementary verification layers:

Table 1: Summary of exact minimax coherence bounds, witnesses, and arithmetic regimes verified across Certificates `cert01`–`cert15`.

d	Class	Lower bound $\mu_{\mathbb{R}}(d)$	Exact / upper witness	Status	Excess $\mu_2^{\mathbb{R}} - \frac{1}{d}$
3	odd	$2/3$	$I_3 - \frac{2}{3}J_3$	Exact tight (Thm. 2)	$1/9$
5	odd	$2/\sqrt{17}$ (strict)	$\frac{1}{11}\mathrm{circ}(3,6,2,-6,6)$	$\in (2/\sqrt{17},\, 6/11]$	$> 3/85$
6	2 mod 4	$1/\sqrt{5}$	$\frac{1}{\sqrt{5}}C_6$ (Paley $p=5$)	Exact tight (Thm. 1)	$1/30$
7	odd	$2/5$ (strict)	$\frac{1}{2437}\mathrm{circ}(\dots)$	$\in (2/5,\, 1188/2437]$	$> 3/175$
10	2 mod 4	$1/3$	$\frac{1}{3}C_{10} \in O(10,\mathbb{Q})$	Exact rational tight	$1/90$
14	2 mod 4	$1/\sqrt{13}$	$\frac{1}{\sqrt{13}}C_{14}$ (Paley $p=13$)	Exact tight	$1/182$
18	2 mod 4	$1/\sqrt{17}$	$\frac{1}{\sqrt{17}}C_{18}$ (Paley $p=17$)	Exact tight	$1/306$
22	2 mod 4	$1/\sqrt{21}$ (strict)	Belevitch ($21 \neq a^2+b^2$)	Strict gap $> 1/\sqrt{21}$	$> 1/462$
26	2 mod 4	$1/5$	$\frac{1}{5}C_{26} \in O(26,\mathbb{Q})$	Exact rational tight	$1/650$
30	2 mod 4	$1/\sqrt{29}$	$\frac{1}{\sqrt{29}}C_{30}$ (Paley $p=29$)	Exact tight	$1/870$
34	2 mod 4	$1/\sqrt{33}$ (strict)	Belevitch ($33 \neq a^2+b^2$)	Strict gap $> 1/\sqrt{33}$	$> 1/1122$

- **Layer 1 — Constructive Lean 4.36.0 Kernel** (`lean/OrthogonalMinimaxCoherence.lean`): Twenty theorems compiled with `lean -DwarningAsError=true`, zero external dependencies, zero `sorry`, and zero `Classical.choice` (audited via `#print axioms`). Layer 1 machine-checks the complete scalar-algebraic, parity, divisibility, and exact-witness arithmetic kernel: polynomial identity (4) and non-negativity (`thm01`–`thm03`), the Hadamard three-row sign-parity obstruction and $d = 4k+2$ coherence inequality (`thm04`–`thm07`), the odd-dimension secant identity (13) and dominance over quadratic/Welch bounds (`thm08`–`thm10`), the unique $d = 3$ spectral-divisibility theorem $s^2 = 4d - 3 \wedge s \mid d \Rightarrow d = 3$ (`thm11`), exact rational orthogonality and entry inequalities for U_3, U_5, U_7 (`thm12`–`thm14`), infinite Belevitch mod-9 and mod-49 sum-of-two-squares obstructions (`thm15`–`thm18`), rational conference squares (`thm19`), and MUB coherence excesses (`thm20`). The finite-sum matrix/vector aggregation steps (such as summing (4) over P, N, applying matrix orthogonality to $N_0 \times C_Z$, and taking eigenvalues/trace of S) are proved in full mathematical detail in Sections 2–3.

- **Layer 2 — Zero-Float Exact Python Verifier** (`verification/verify_orthogonal_coherence.py`): An AST-audited pure standard-library verifier using strictly `int` and `fractions.Fraction` (zero floating-point operations, zero numeric division or exponentiation, zero `limit_denominator`), emitting 16 SHA-256 certificates under `certificates/MANIFEST.json` and validated by 56 adversarial `pytest` checks. Layer 2 independently verifies Paley conference matrices for $d \in \{6, 10, 14, 18, 26, 30, 38, 42, 54, 62\}$ (including GF(9) and GF(25) constructions), the complete Belevitch classification for $6 \leq d \leq 102$, exact matrix orthogonality for U_3, U_5, U_7 (together with $\det(U_3) = -1$ and $\det(U_5) = \det(U_7) = +1$ in the adversarial test suite), the spectral-divisibility scan for all odd $d \leq 1001$ in Certificate `cert13` (extended to $d \leq 5001$ in `tests/test_adversarial.py`), and the exhaustive 24^5-vector $\mathbb{Z}[\zeta_{24}]$ ring search of Theorem 3(b).

Remark 1 (Open Directions). Two sharp open questions remain directly highlighted by Theorems 1 and 2: (i) determining the exact value of $\mu_{\mathbb{R}}(5) \in (2/\sqrt{17},\, 6/11]$ (and general odd $\mu_{\mathbb{R}}(2k+1)$ for $k \geq 2$), where our spectral-divisibility obstruction rules out $2/\sqrt{4d-3}$ uniformly; and (ii) quantifying the Belevitch coherence gap $\mu_{\mathbb{R}}(d) - 1/\sqrt{d-1} > 0$ at the first obstructed order $d = 22$, where conference-matrix rigidity proves no zero-diagonal $\pm 1/\sqrt{21}$ minimizer can exist.

References

[1] V. Belevitch, *Theory of $2n$-terminal networks with applications to conference telephony*, Electr. Commun. **27** (1950), 231–244.

[2] V. Belevitch, *Conference networks and Hadamard matrices*, Ann. Soc. Sci. Bruxelles Sér. I **82** (1968), 13–32.

[3] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej, and K. Życzkowski, *Mutually unbiased bases and Hadamard matrices of order six*, J. Math. Phys. **48** (2007), 052106.

[4] P. O. Boykin, M. Sitharam, M. Tarifi, and P. Wocjan, *Real mutually unbiased bases*, arXiv:quant-ph/0502024 (2005).

[5] S. Brierley and S. Weigert, *Maximal sets of mutually unbiased quantum states in dimension 6*, Phys. Rev. A **78** (2008), 042312.

[6] S. Brierley and S. Weigert, *Constructing mutually unbiased bases in dimension six*, Phys. Rev. A **79** (2009), 052316.

[7] P. Delsarte, J. M. Goethals, and J. J. Seidel, *Orthogonal matrices with zero diagonal. II*, Canad. J. Math. **23** (1971), 816–832.

[8] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, *On mutually unbiased bases*, Int. J. Quantum Inform. **8** (2010), 535–640.

[9] J. M. Goethals and J. J. Seidel, *Orthogonal matrices with zero diagonal*, Canad. J. Math. **19** (1967), 1001–1010.

[10] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, and M. Weiner, *A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6*, J. Phys. A: Math. Theor. **42** (2009), 245305.

[11] R. E. A. C. Paley, *On orthogonal matrices*, J. Math. Phys. **12** (1933), 311–320.

[12] J. J. Seidel, *A survey of two-graphs*, in *Colloquio Internazionale sulle Teorie Combinatorie (Roma, 1973)*, Tomo I, Accad. Naz. Lincei (1976), 481–511.

[13] L. R. Welch, *Lower bounds on the maximum cross correlation of signals*, IEEE Trans. Inform. Theory **20** (1974), 397–399.

[14] W. K. Wootters and B. D. Fields, *Optimal state-determination by mutually unbiased measurements*, Ann. Physics **191** (1989), 363–381.