AIRR.SCIENCE · ARR-2026-0HWK09032Q996SP0 v1 [Mathematics] 28 Nov 2026

Symmetric Rényi Entropic Uncertainty for Complex Hadamard Matrices: Hermite–ℓ^1 Concentration Envelopes, Möbius Symmetrization, and the Anomalous First-Order Phase Transition at $\alpha_c(N)$

Lluis Eriksson*

28 November 2026

Abstract

We establish a quantitative theory for the equal-index (symmetric) Rényi entropic uncertainty

$$U_\alpha(U) := \inf_{\|v\|_2=1} \Big(H_\alpha(|v|^2) + H_\alpha(|Uv|^2) \Big)$$

across every $N \times N$ complex Hadamard matrix $U \in \mathcal{H}_N$ (equivalently, every pair of mutually unbiased orthonormal bases in $\mathbb{C}^N$, including the discrete Fourier transform on any finite abelian group of order N, Walsh–Hadamard transforms $H_2^{\otimes k}$, and non-group complex Hadamard families). Unlike the Maassen–Uffink regime of Hölder-conjugate indices $\alpha^{-1}+\beta^{-1}=2$ where uncertainty grows as $\log N$, the symmetric functional $H_\alpha+H_\alpha$ collapses to a dimension-independent ceiling for every $\alpha > 1$, driven by the universal spike-plus-flat bisector states $v_{j,k} \propto e_j + e^{i\arg(U_{kj})}U^*e_k$. Four main theorems govern this phenomenon:

1. **Exact Universal Hermite–ℓ^1 Concentration Envelope (Theorem 2.2):** For every $\alpha > 1$, a Rolle-certified Hermite quadratic majorant $u^{2\alpha} \le Q_{\alpha,M,b}(u)$ on $[0, M]$ (factoring explicitly as $(u-b)^2(M-u)(M+u+2b) \ge 0$ at $\alpha = 2$) coupled with $\|Uv\|_\infty \le \|v\|_1/\sqrt{N}$ yields the closed-form two-point rational envelope $\|v\|_{2\alpha}^{2\alpha} \le \Psi_\alpha(N, x, y)$ with universal tail ceiling $b_1 \le y/\sqrt{N}$ and exact Cauchy–Schwarz ellipse boundary $2(\sqrt{N}x - y)^2/(N-2) + y^2 \le 1$.
2. **Möbius Symmetrization and Factor-of-Two Barrier Breaking (Theorem 3.3):** Holding $u = xy$ fixed and setting $w = x^2 + y^2$ turns the leading product into a Möbius function of w with exact negative determinant $-(\sqrt{N}u-1)^2(N - 2\sqrt{N}u + 1) < 0$, forcing maximization on the diagonal $x = y = \sqrt{u}$. Together with the exact endpoint factorization $4\sqrt{N}\,\mathcal{Q}(u_{\max}) = (\sqrt{N}-1)^2[(\alpha-2)\sqrt{N}-2]$, this yields an explicit finite-N lower bound for all $\alpha > 1$, proves the exact asymptotic limit

$$\lim_{N\to\infty} \inf_{U\in\mathcal{H}_N} U_\alpha(U) = \frac{2\alpha}{\alpha-1}\log 2 \qquad (\forall\, \alpha \ge 2),$$

strictly doubling both Deutsch's min-entropy barrier ($2\log 2$) and the Larsen–Ballester–Wehner traceless-Pythagoras barrier ($2\log 2$) at collision entropy $\alpha = 2$ ($4\log 2$ vs. $2\log 2$), and gives the dimension-independent lower bound $2\log(\alpha^{\alpha/(\alpha-1)}/(\alpha-1))$ for $\alpha \in (1, 2)$.

*Independent researcher, AIRR.SCIENCE. Correspondence: `editor@airr.science`. Authored with AI assistance (Google Antigravity) for proof exploration, Lean 4.36.0 formalization, computational verification, and manuscript drafting; evaluated by two distinct isolated frontier models under `AIRR-FOUNDER-1.0`.

3. **Exact Finite-N Sharpness and Rank-1 Necessity (Theorem 4.1):** We prove exact sharpness for $N = 2$ ($\|v\|_4^4\|Uv\|_4^4 \le (9 - \cos^2 4\theta)/16 \le 9/16$), for min-entropy $\alpha = \infty$ across arbitrary unitary overlap $c = \max_{j,k} |U_{jk}|$, and for collision entropy $\alpha = 2$ on the entire two-dimensional Landau–Pollak subspace family $\mathrm{span}\{e_j, U^* e_k\}$ for every $N \ge 2$ via a four-term strictly positive Bernstein polynomial identity. In sharp contrast, additive purity obeys $\|v\|_4^4 + \|Uv\|_4^4 \le 1 + 1/N$ via traceless Hilbert–Schmidt orthogonality, which is attained even by non-positive trace-one Hermitian operators, proving that no rank-free 2-design argument can surpass $2 \log 2$.
4. **Exact First-Order Phase Transition and Anomalous $1/(\log N)^2$ Scaling (Theorem 5.1):** The critical threshold $\alpha_c(N) > 1$ defined by $2H_{\alpha_c(N)}(v_+(N)) = \log N$ decreases strictly from the qubit point $\alpha_c(2) = 1.4313558812\ldots$ to 1^+ and obeys the even-power hyperbolic expansion

$$\alpha_c(N) \;=\; 1 + \frac{8\log 2}{(\log N)^2} + \frac{64(\log 2)^3}{3(\log N)^4} + O\!\left(\frac{1}{(\log N)^6}\right) \qquad (N \to \infty),$$

driven by exact double-root cancellation $\cosh(\frac{1}{2}\varepsilon \log N) = 2^{\varepsilon}(1 + O(N^{-1/2}))$ at $\alpha \to 1^+$.

Finally, we formulate Conjecture 6.1 on exact finite-N first-order sharpness across all $\alpha > 1$, supported by global optimization across DFT_N, Walsh–Hadamard, and non-group $F_4(\theta)$ matrices (discrepancy $\le 1.73 \times 10^{-13}$) and an explicit degree-2 rational single-vector decoupling weight $W_N(p)$. The exact algebraic core (25 declarations: 15 public theorems, 5 public definitions, 5 private helpers) is machine-checked in standalone Lean 4.36.0 (`0 sorry`, `0 grind`, `0 custom axioms`).

1 Introduction

Let $N \ge 2$ be an integer, and let $U \in U(N)$ be an $N \times N$ unitary matrix relating two orthonormal bases $\{e_j\}_{j=1}^N$ and $\{u_k = U^* e_k\}_{k=1}^N$ of $\mathbb{C}^N$. A unit vector $v \in \mathbb{C}^N$ ($\|v\|_2 = 1$) induces two probability distributions $p = (|v_1|^2, \ldots, |v_N|^2)$ and $q = (|(Uv)_1|^2, \ldots, |(Uv)_N|^2)$ on $\{1, \ldots, N\}$. For any Rényi order $\alpha \in [0, \infty]$, the Rényi entropy (in nats) is

$$H_\alpha(p) \;:=\; \frac{1}{1-\alpha} \log\left(\sum_{j=1}^N p_j^\alpha\right) \qquad (\alpha \notin \{0, 1, \infty\}),$$

extended by continuity to $H_1(p) = -\sum_j p_j \log p_j$ (Shannon entropy), $H_2(p) = -\log \|v\|_4^4$ (collision entropy), $H_\infty(p) = -\log \max_j p_j$ (min-entropy), and $H_0(p) = \log |\mathrm{supp}(p)|$. We call $U \in U(N)$ a *complex Hadamard matrix* (written $U \in \mathcal{H}_N$) if $|U_{jk}| = N^{-1/2}$ for all $1 \le j, k \le N$; equivalently, $\{e_j\}$ and $\{U^* e_k\}$ form a pair of mutually unbiased bases (MUBs) in $\mathbb{C}^N$ [10, 11]. Canonical examples include the discrete Fourier transform $\mathcal{F}_G$ on any finite abelian group G of order N, Walsh–Hadamard matrices $H_2^{\otimes k}$ ($N = 2^k$), and continuous non-group complex Hadamard families such as $F_4(\theta)$ [10].

1.1 The conjugate-index regime versus the symmetric regime

The Maassen–Uffink theorem [7] (extended to Rényi indices by Bialynicki-Birula [2] via Riesz–Thorin interpolation) establishes

$$H_\alpha(|v|^2) + H_\beta(|Uv|^2) \;\ge\; \log N \qquad \text{whenever } U \in \mathcal{H}_N,\ \frac{1}{\alpha} + \frac{1}{\beta} = 2. \tag{1}$$

At the Shannon point $\alpha = \beta = 1$, (1) gives $H_1(|v|^2) + H_1(|Uv|^2) \ge \log N$, attained by every basis vector e_j, every dual basis vector $U^* e_k$, and (for $U = \mathcal{F}_G$) every normalized subgroup or coset indicator $|H|^{-1/2}\mathbf{1}_{g+H}$. By monotonicity of $\alpha \mapsto H_\alpha$, the exact same lower bound $\log N$ holds for all symmetric indices $\alpha \in [0, 1]$.

For $\alpha > 1$, however, the Hölder conjugacy condition $\alpha^{-1} + \beta^{-1} = 2$ forces $\beta = \frac{\alpha}{2\alpha-1} < 1$, so (1) never bounds the equal-index (symmetric) uncertainty

$$U_\alpha(U) \;:=\; \inf_{\|v\|_2=1} \Big(H_\alpha(|v|^2) + H_\alpha(|Uv|^2) \Big). \tag{2}$$

In fact, $U_\alpha(U)$ behaves completely differently from $\log N$ for every $\alpha > 1$. Consider any of the N^2 *bisector states*

$$v_{j,k} \;:=\; \frac{e_j + e^{i\arg(U_{kj})} U^* e_k}{\sqrt{2(1 + N^{-1/2})}} \qquad (1 \le j, k \le N), \tag{3}$$

which bisect the angle $\theta_0 = \arccos(N^{-1/2})$ between e_j and $U^* e_k$. Both $|v_{j,k}|^2$ and $|Uv_{j,k}|^2$ have the exact same two-level spike-plus-flat distribution

$$p_0(N) \;=\; \frac{\sqrt{N}+1}{2\sqrt{N}}, \qquad p_1(N) \;=\; \frac{1}{2\sqrt{N}(\sqrt{N}+1)} \quad \text{(multiplicity } N-1), \tag{4}$$

with $\ell^{2\alpha}$-moment $S_\alpha(v_+(N)) := p_0(N)^\alpha + (N-1)p_1(N)^\alpha$. At collision entropy $\alpha = 2$, an exact factorization (verified in Lean 4.36.0 as `vplus_collision_identity`) yields

$$S_2(v_+(N)) \;=\; \frac{N + 3\sqrt{N} + 4}{4\sqrt{N}(\sqrt{N}+1)}, \qquad 2H_2(v_+(N)) \;=\; 2\log\!\left(\frac{4\sqrt{N}(\sqrt{N}+1)}{N + 3\sqrt{N} + 4} \right). \tag{5}$$

As $N \to \infty$, $p_0(N) \to 1/2$ while $(N-1)p_1(N)^\alpha = O(N^{1-\alpha}) \to 0$ for every $\alpha > 1$, so

$$U_\alpha(U) \;\le\; 2H_\alpha(v_+(N)) \;\longrightarrow\; \frac{2\alpha}{\alpha - 1} \log 2 \;<\; \infty \qquad (N \to \infty). \tag{6}$$

Thus, in stark contrast to the logarithmic divergence $\log N \to \infty$ at $\alpha \le 1$, symmetric Rényi uncertainty is universally bounded by a finite dimension-independent ceiling for every $\alpha > 1$.

1.2 Why existing bounds stall at $2\log 2$ and what this paper proves

For the qubit ($N = 2$), Zozor, Bosyk, and Portesi [12] characterized $U_\alpha(H_2)$ across all (α, β) and identified a critical transition at $\alpha_c(2) \approx 1.4314$. In general dimension $N \ge 3$, however, existing general-purpose uncertainty relations stall far short of the ceiling (6):

- **Deutsch's min-entropy bound [3]:** Since $H_\alpha \ge H_\infty$, Deutsch's bound gives $U_\alpha(U) \ge 2\log(\frac{2\sqrt{N}}{\sqrt{N}+1}) \to 2\log 2 \approx 1.3863$ for every $\alpha > 1$—missing the true collision-entropy ceiling $4\log 2 \approx 2.7726$ by a factor of 2 (a factor of 4 in collision probability).
- **Traceless-Pythagoras / 2-design bounds [6, 5, 1]:** For any $U \in \mathcal{H}_N$, Hilbert–Schmidt orthogonality of traceless measurement projections gives $\|v\|_4^4 + \|Uv\|_4^4 \le 1 + 1/N$. Applying AM–GM yields $\|v\|_4^4 \|Uv\|_4^4 \le \frac{1}{4}(1 + 1/N)^2$, hence $H_2 + H_2 \ge 2\log(\frac{2N}{N+1}) \to 2\log 2$—stalling at the exact same $2\log 2$ wall.
- **Direct-sum majorization [4, 8, 9]:** Bounding only the top coordinate $p_0 + q_0 \le 1 + N^{-1/2}$ allows a 2-point distribution $(p_0, 1-p_0, 0, \ldots, 0)$ whose collision sum is $p_0^2 + (1-p_0)^2 \to 1/2$, again stalling at $2\log 2$ as $N \to \infty$.

The reason all three methods stall at $2\log 2$ is geometric: a 2-sparse vector $(2^{-1/2}, 2^{-1/2}, 0, \ldots, 0)$ achieves large $\|v\|_4^4 = 1/2$, yet its ℓ^1 norm is only $\sqrt{2}$. This forces $\|Uv\|_\infty \le \|v\|_1/\sqrt{N} = \sqrt{2/N}$ and crushes $\|Uv\|_4^4 \le 2/N$. To achieve $O(1)$ mass in *both* bases simultaneously, the tail mass $1 - \|v\|_\infty^2$ must spread across $\Theta(N)$ coordinates to sustain $\|v\|_1 = \Theta(\sqrt{N})$, which drives the tail's $\ell^{2\alpha}$ contribution to $O(N^{1-\alpha})$.

In this paper we turn that ℓ^1–ℓ^∞ coupling into an exact analytical machine:

1. Section 2 derives the exact Hermite quadratic certificate (Lemma 2.1) and the closed-form two-point rational envelope $\Psi_\alpha(N,x,y)$ plus Cauchy–Schwarz ellipse envelope $\Phi_\alpha(N,x,y)$ (Theorem 2.2).
2. Section 3 proves the exact Möbius-in-w symmetrization identity (Lemma 3.1), the diagonal endpoint threshold $\alpha \geq 2 + 2/\sqrt{N}$ (Lemma 3.2), and our main universal finite-N and exact asymptotic uncertainty theorem (Theorem 3.3), establishing $\lim_{N\to\infty} \inf_{U\in\mathcal{H}_N} U_\alpha(U) = \frac{2\alpha}{\alpha-1}\log 2$ for every $\alpha \geq 2$ and breaking the $2\log 2$ wall by an exact factor of 2 at $\alpha = 2$.
3. Section 4 proves exact finite-N sharpness at $N = 2$, at $\alpha = \infty$ for arbitrary overlap c, and on the entire two-dimensional Landau–Pollak subspace family $\mathrm{span}\{e_j, U^* e_k\}$ for every $N \geq 2$ via a four-term strictly positive Bernstein polynomial identity, and proves why rank-1 positivity is strictly necessary to beat $2\log 2$ (Theorem 4.1).
4. Section 5 analyzes the first-order phase transition curve $\alpha_c(N)$, proving strict monotonicity and the anomalous even-power scaling $\alpha_c(N) = 1+8(\log 2)/(\log N)^2+64(\log 2)^3/(3(\log N)^4)+O((\log N)^{-6})$ (Theorem 5.1).
5. Section 6 formulates Conjecture 6.1, documents the single-vector rational decoupling weight $W_N(p)$, summarizes numerical verification across 44 global optimization runs, and records the machine-checked Lean 4.36.0 artifact manifest.

2 Exact Universal Hermite–ℓ^1 Concentration Envelopes

Throughout, we write $s := \sqrt{N} \geq \sqrt{2}$. For any unit vector $v \in \mathbb{C}^N$ and any $U \in \mathcal{H}_N$, set $w := Uv$, $x := \|v\|_\infty \in [s^{-1}, 1]$, and $y := \|w\|_\infty \in [s^{-1}, 1]$. Since $|U_{jk}| = s^{-1}$ for every j, k, the triangle inequality gives

$$\|v\|_1 \;\geq\; s\,y, \qquad \|w\|_1 \;\geq\; s\,x. \tag{7}$$

Equivalently, setting $u_j := |v_j| \in [0, x]$ (with $u_1 = x$ after permuting coordinates), the vector $u = (u_1, \ldots, u_N)$ satisfies $\sum_{j=1}^N u_j^2 = 1$ and $\sum_{j=1}^N u_j \geq sy$. By Cauchy–Schwarz on the $N-1$ tail entries $u_2, \ldots, u_N$,

$$sy - x \;\leq\; \sum_{j=2}^{N} u_j \;\leq\; \sqrt{(N-1)(1-x^2)} \quad\Longleftrightarrow\quad y \;\leq\; y_{\max}(x) \;:=\; \frac{x + \sqrt{(N-1)(1-x^2)}}{\sqrt{N}}. \tag{8}$$

We denote by $\mathcal{D}_N := \{(x,y) \in [s^{-1},1]^2 : y \leq y_{\max}(x)\}$ the symmetric Landau–Pollak feasible domain. Setting $x = \cos\theta$, $y = \cos\psi$ with $\theta, \psi \in [0, \theta_0]$ and $\theta_0 := \arccos(s^{-1}) \in [\pi/4, \pi/2)$, (8) is equivalently $\theta + \psi \geq \theta_0$, and squaring $(sy - x)^2 \leq (N-1)(1-x^2)$ gives the symmetric quadratic form

$$(x,y) \in \mathcal{D}_N \quad\Longleftrightarrow\quad x, y \in [s^{-1}, 1] \;\text{ and }\; x^2 + y^2 - \frac{2xy}{s} \;\leq\; 1 - \frac{1}{N}. \tag{9}$$

In particular, $xy \leq \cos^2(\theta_0/2) = \frac{s+1}{2s}$ on $\mathcal{D}_N$ (Deutsch's bound), and consequently

$$x^2 + y^2 \;\leq\; 1 + \frac{2xy - s^{-1}}{s} \;\leq\; 1 + \frac{1}{s} \qquad \forall\,(x,y) \in \mathcal{D}_N. \tag{10}$$

Lemma 2.1 (Exact Hermite Quadratic Certificate)**.** *Let $\alpha > 1$, $M > 0$, and $b \in [0, M)$. There exists a unique quadratic polynomial $Q_{\alpha,M,b}(u) = Au^2 + Bu + C$ satisfying the Hermite interpolation conditions*

$$Q_{\alpha,M,b}(b) = b^{2\alpha}, \qquad Q'_{\alpha,M,b}(b) = 2\alpha b^{2\alpha-1}, \qquad Q_{\alpha,M,b}(M) = M^{2\alpha}.$$

For every $u \in [0, M]$,

$$u^{2\alpha} \;\leq\; Q_{\alpha,M,b}(u), \tag{11}$$

with strict inequality for every $u \in [0, M] \setminus \{b, M\}$. At $\alpha = 2$, $Q_{2,M,b}$ takes the explicit form

$$Q_{2,M,b}(u) \;=\; (M^2 + 2bM + 3b^2)u^2 - 2b(M+b)^2 u + b^2 M(M+2b), \tag{12}$$

with exact algebraic deficit factorization

$$Q_{2,M,b}(u) - u^4 \;=\; (u-b)^2(M-u)(M+u+2b) \;\geq\; 0 \qquad \forall\, u \in [0, M]. \tag{13}$$

Proof. Uniqueness of the Hermite quadratic $Q_{\alpha,M,b}$ is immediate from Taylor's formula around b:

$$Q_{\alpha,M,b}(u) \;=\; b^{2\alpha} + 2\alpha b^{2\alpha-1}(u-b) + \frac{M^{2\alpha} - b^{2\alpha} - 2\alpha b^{2\alpha-1}(M-b)}{(M-b)^2}(u-b)^2.$$

When $b = 0$, $Q_{\alpha,M,0}(u) = M^{2\alpha-2}u^2 \geq u^{2\alpha}$ directly on $[0, M]$, with strict inequality on $(0, M)$. Assume now $b \in (0, M)$, and let $\Delta(u) := Q_{\alpha,M,b}(u) - u^{2\alpha}$ on $[0, M]$. Since $\alpha > 1$, $2\alpha > 2$, so Δ is C^2 on $[0, M]$ and C^∞ on $(0, M]$ with third derivative

$$\Delta'''(u) \;=\; -2\alpha(2\alpha-1)(2\alpha-2)u^{2\alpha-3} \;<\; 0 \qquad \forall\, u > 0.$$

Hence Δ'' is strictly decreasing on $(0, M]$. Because $\Delta(b) = \Delta(M) = 0$, Rolle's theorem gives $c_1 \in (b, M)$ with $\Delta'(c_1) = 0$. Since also $\Delta'(b) = 0$, Rolle's theorem gives $c_2 \in (b, c_1)$ with $\Delta''(c_2) = 0$. Strict monotonicity of Δ'' implies $\Delta'' > 0$ on $(0, c_2)$ and $\Delta'' < 0$ on $(c_2, M]$. Therefore Δ' is strictly increasing on $[0, c_2]$ and strictly decreasing on $[c_2, M]$. Because $\Delta'(b) = 0 = \Delta'(c_1)$ with $b < c_2 < c_1$, it follows that $\Delta' < 0$ on $(0, b)$, $\Delta' > 0$ on (b, c_1), and $\Delta' < 0$ on $(c_1, M]$. Consequently Δ strictly decreases from $\Delta(0) > 0$ to $\Delta(b) = 0$ on $[0, b]$, strictly increases on $[b, c_1]$, and strictly decreases from $\Delta(c_1) > 0$ to $\Delta(M) = 0$ on $[c_1, M]$. Thus $\Delta(u) > 0$ for all $u \in [0, M] \setminus \{b, M\}$. At $\alpha = 2$, expanding (13) directly yields (12) (machine-checked in Lean 4.36.0 as `hermite_quartic_identity`, `hermite_quartic_nonneg`, and `hermite_quartic_exact_nodes`). □

Theorem 2.2 (Universal Two-Point Rational Envelope and Cauchy–Schwarz Ellipse Envelope)**.** *Let $N \geq 2$, $s = \sqrt{N}$, $\alpha > 1$, and let $v \in \mathbb{C}^N$ be any unit vector with $x = \|v\|_\infty \in [s^{-1}, 1]$ and $y \in [s^{-1}, y_{\max}(x)]$ satisfying $\|v\|_1 \geq sy$.*

(a) ***Two-Point Rational Envelope (Ψ_α):*** *Whenever $sxy > 1$, set*

$$b_1(x, y) \;:=\; \frac{sxy - 1}{s(sx - y)}. \tag{14}$$

Then $0 < b_1(x, y) \leq \frac{y}{s} \leq \frac{1}{s} \leq x$ (with strict inequality $b_1(x, y) < x$ whenever $sxy > 1$, since $Nx^2 - 2sxy + 1 = (sx - y)^2 + (1 - y^2)$ vanishes only at $(x, y) = (s^{-1}, 1)$, where $sxy = 1$), and

$$\|v\|_{2\alpha}^{2\alpha} \;\leq\; \Psi_\alpha(N, x, y) \;:=\; \underbrace{\frac{N(1-y^2)\,x^{2\alpha}}{Nx^2 - 2sxy + 1}}_{A_\alpha(x,y)} + \underbrace{\frac{N(sx-y)^2\,b_1(x,y)^{2\alpha}}{Nx^2 - 2sxy + 1}}_{B_\alpha^{\mathrm{tail}}(x,y)}. \tag{15}$$

Moreover, the two pieces satisfy the universal elementary bounds

$$A_\alpha(x, y) \;\leq\; x^{2(\alpha-1)}, \qquad B_\alpha^{\mathrm{tail}}(x, y) \;\leq\; \frac{y^{2\alpha}}{N^{\alpha-1}} \;\leq\; N^{1-\alpha}. \tag{16}$$

(b) ***Exact Cauchy–Schwarz Tail Envelope (Φ_α):*** *For $N \geq 3$, let $R := 1 - x^2$ and $T := \max(0, sy - x)$. Whenever $T \geq \sqrt{R}$, every tail coordinate u_j ($j \geq 2$) satisfies the exact Cauchy–Schwarz ceiling*

$$u_j \;\leq\; M_{\mathrm{CS}}(x, y) \;:=\; \frac{T + \sqrt{(N-2)((N-1)R - T^2)}}{N-1}. \tag{17}$$

For any $(x,y) \in \mathcal{D}_N$ with $T \geq 0$, the algebraic inequality $x \leq M_{\mathrm{CS}}(x,y)$ holds if and only if (x,y) lies in the exact ellipse

$$\frac{2(sx-y)^2}{N-2} + y^2 \;\leq\; 1, \tag{18}$$

which automatically implies $x \leq 1/\sqrt{2}$. Whenever $x \geq M_{\mathrm{CS}}(x,y)$ and $T > \sqrt{R}$ (in particular for all $x \geq 1/\sqrt{2}$ with $T > \sqrt{R}$), applying Lemma 2.1 on the $N-1$ tail entries with $M = M_{\mathrm{CS}}$ and $b_0 := (T - M_{\mathrm{CS}})/(N-2) \geq 0$ gives the exact sharp envelope

$$\|v\|_{2\alpha}^{2\alpha} \;\leq\; \Phi_\alpha^{\mathrm{CS}}(N,x,y) \;:=\; x^{2\alpha} + M_{\mathrm{CS}}^{2\alpha} + (N-2)\, b_0^{2\alpha}, \tag{19}$$

attained with equality by $(x, M_{\mathrm{CS}}, b_0, \ldots, b_0)$. On the Landau–Pollak boundary $y = y_{\max}(x)$ (where $T = \sqrt{(N-1)R} > \sqrt{R}$), both envelopes coincide identically with $B_\alpha(x) := x^{2\alpha} + (N-1)^{1-\alpha}(1-x^2)^\alpha$.

Proof. Part (a). Since $sxy > 1$ and $y \leq 1$, we have $sx > y^{-1} \geq 1 \geq y$, so $sx - y > 0$ and $b_1 > 0$. Cross-multiplying gives:

$$\begin{aligned}
b_1 \leq \frac{y}{s} &\iff sxy - 1 \leq sxy - y^2 \iff y^2 \leq 1, \\
b_1 \leq \frac{1}{s} &\iff sxy - 1 \leq sx - y \iff (1-y)(sx+1) \geq 0, \\
b_1 < x &\iff sxy - 1 < Nx^2 - sxy \iff Nx^2 - 2sxy + 1 = (sx-y)^2 + (1-y^2) > 0,
\end{aligned}$$

which holds for every $(x,y) \in \mathcal{D}_N$ with $sxy > 1$ (machine-checked in `tail_height_bounds`).

Now apply Lemma 2.1 with $M = x$ and $b = b_1 \in (0,x)$ to each $u_j = |v_j| \in [0,x]$. Define the unique weights $\lambda \in [0,1]$ and $1-\lambda$ of the two-point probability measure supported on $\{b_1, x\}$ having mean y/s and second moment $1/N$:

$$\lambda \;:=\; \frac{1-y^2}{Nx^2 - 2sxy + 1}, \qquad 1 - \lambda \;=\; \frac{(sx-y)^2}{Nx^2 - 2sxy + 1}. \tag{20}$$

Direct algebra verifies both moment identities:

$$\lambda x + (1-\lambda) b_1 \;=\; \frac{(1-y^2)x + (sx-y)(sxy-1)/s}{Nx^2 - 2sxy + 1} \;=\; \frac{y(Nx^2 - 2sxy + 1)}{s(Nx^2 - 2sxy + 1)} \;=\; \frac{y}{s},$$

and $\lambda x^2 + (1-\lambda) b_1^2 = 1/N$. To replace $\sum_{j=1}^N u_j$ by its lower bound sy, we verify that the linear coefficient $B = Q'_{\alpha,x,b_1}(0)$ of $Q_{\alpha,x,b_1}(u) = Au^2 + Bu + C$ is strictly negative. Writing $Q_{\alpha,x,b_1}(u) = b_1^{2\alpha} + 2\alpha b_1^{2\alpha-1}(u - b_1) + K(u-b_1)^2$ with $K = \frac{x^{2\alpha} - b_1^{2\alpha} - 2\alpha b_1^{2\alpha-1}(x-b_1)}{(x-b_1)^2} > 0$, we compute

$$B \;=\; Q'(0) \;=\; 2\alpha b_1^{2\alpha-1} - 2Kb_1 \;=\; \frac{2b_1}{(x-b_1)^2}\Big[\alpha b_1^{2\alpha-2}(x-b_1)^2 - \big(x^{2\alpha} - b_1^{2\alpha} - 2\alpha b_1^{2\alpha-1}(x-b_1)\big)\Big].$$

Simplifying the bracket gives

$$\alpha b_1^{2\alpha-2}(x^2 - b_1^2) - (x^{2\alpha} - b_1^{2\alpha}) \;=\; b_1^{2\alpha}\Big[\alpha(r^2-1) - (r^{2\alpha}-1)\Big] \quad \left(r := \frac{x}{b_1} > 1\right).$$

Let $\phi(t) := t^\alpha - 1 - \alpha(t-1)$ for $t = r^2 > 1$. Since $\alpha > 1$, $\phi(1) = 0$ and $\phi'(t) = \alpha(t^{\alpha-1} - 1) > 0$ on $(1,\infty)$, so $\phi(r^2) > 0$, hence $B < 0$ strictly. Therefore, summing $u_j^{2\alpha} \leq Au_j^2 + Bu_j + C$ over $j = 1, \ldots, N$ and using $\sum u_j^2 = 1$, $\sum u_j \geq sy$, and $B < 0$ gives

$$\sum_{j=1}^N u_j^{2\alpha} \;\leq\; A + B(sy) + NC \;=\; N\Big[\lambda\, Q_{\alpha,x,b_1}(x) + (1-\lambda)\, Q_{\alpha,x,b_1}(b_1)\Big] \;=\; N\big[\lambda x^{2\alpha} + (1-\lambda) b_1^{2\alpha}\big],$$

which is identically (15).

For (16), the first inequality follows directly from the algebraic identity (`leading_term_deficit_sq` in Lean)

$$(Nx^2 - 2sxy + 1) - N(1-y^2)x^2 \;=\; (sxy-1)^2 \;\geq\; 0,$$

giving $N(1-y^2)x^{2\alpha}/(Nx^2-2sxy+1) \leq x^{2(\alpha-1)}$. The second inequality follows from $1-\lambda \leq 1$ and $b_1 \leq y/s \leq 1/s$:

$$B_\alpha^{\text{tail}}(x,y) \;=\; N(1-\lambda)\, b_1^{2\alpha} \;\leq\; N(y/s)^{2\alpha} \;=\; \frac{y^{2\alpha}}{N^{\alpha-1}} \;\leq\; N^{1-\alpha}.$$

Part (b). Assume $T \geq \sqrt{R}$ and fix any tail index $j \geq 2$. Because $u_j \leq \sqrt{R} \leq T$, we have $\sum_{m\geq 2,\, m\neq j} u_m \geq T - u_j \geq 0$. Applying Cauchy–Schwarz to these $N-2$ remaining tail coordinates and squaring yields $(T-u_j)^2 \leq (N-2)(R-u_j^2)$, i.e., $(N-1)u_j^2 - 2Tu_j + T^2 - (N-2)R \leq 0$, whose larger root is $M_{\text{CS}}(x,y)$ in (17). Since $T = sy - x$ and $R = 1-x^2$, for any $(x,y) \in \mathcal{D}_N$ with $T \geq 0$ we have $(N-1)x \geq T$ (because $sy \leq Nx$), so the inequality $x \leq M_{\text{CS}}(x,y)$ is equivalent to $(N-1)x^2 - 2Tx + T^2 - (N-2)R \leq 0$. Expanding and completing the square (Lean: `xcap_ellipse_identity`):

$$2Nx^2 + Ny^2 - 4sxy \;=\; 2(sx-y)^2 + (N-2)y^2 \;\leq\; N-2,$$

which is (18). By Cauchy–Schwarz on $sx = (sx-y) + y$,

$$Nx^2 \;\leq\; \left(\frac{N-2}{2} + 1\right)\left(\frac{2(sx-y)^2}{N-2} + y^2\right) \;\leq\; \frac{N}{2},$$

so $x \leq 1/\sqrt{2}$ throughout the ellipse (18). Conversely, when $x \geq M_{\text{CS}}$ and $T > \sqrt{R}$, we have $b_0 = (T - M_{\text{CS}})/(N-2) \in (0, M_{\text{CS}})$ satisfying $M_{\text{CS}} + (N-2)b_0 = T$ and $M_{\text{CS}}^2 + (N-2)b_0^2 = R$. Applying Lemma 2.1 with $(M,b) = (M_{\text{CS}}, b_0)$ to the $N-1$ tail entries $u_2, \ldots, u_N \in [0, M_{\text{CS}}]$ (again with linear coefficient $B < 0$) yields (19). On $y = y_{\max}(x)$, $(N-1)R = T^2$, so $M_{\text{CS}} = b_0 = b_1 = \sqrt{R/(N-1)}$ and both envelopes equal $B_\alpha(x)$. □

3 Möbius Symmetrization and Breaking the $2\log 2$ Barrier

Applying Theorem 2.2(a) simultaneously to v and $w = Uv$ bounds the product $\|v\|_{2\alpha}^{2\alpha}\|Uv\|_{2\alpha}^{2\alpha}$ by $\Psi_\alpha(N,x,y)\Psi_\alpha(N,y,x)$. Remarkably, the leading product $A_\alpha(x,y)A_\alpha(y,x)$ admits an exact one-step symmetrization to the diagonal $x=y$ via a Möbius transformation in $w = x^2+y^2$.

Lemma 3.1 (Exact Möbius-in-w Symmetrization)**.** *For any $N \geq 2$ ($s = \sqrt{N}$), $\alpha > 1$, and $(x,y) \in \mathcal{D}_N$ with $u := xy \in (s^{-1}, \frac{s+1}{2s}]$, set $w := x^2+y^2 \in [2u, 1 - N^{-1} + 2u/s]$. Then*

$$A_\alpha(x,y)\, A_\alpha(y,x) \;=\; \frac{s^4(1+u^2-w)}{C(u) - D(u)\, w}\, u^{2\alpha}, \tag{21}$$

where $C(u) := s^4u^2 + 4s^2u^2 - 4su + 1$ and $D(u) := s^2(2su-1) > 0$. Its Möbius determinant satisfies the exact identity

$$D(u)(1+u^2) - C(u) \;=\; -(su-1)^2(s^2 - 2su + 1) \;<\; 0. \tag{22}$$

Consequently, for fixed $u \in (s^{-1}, \frac{s+1}{2s}]$, $w \mapsto A_\alpha(x,y)A_\alpha(y,x)$ is strictly decreasing on $[2u, 1 - N^{-1} + 2u/s]$, attaining its unique maximum at the diagonal $w = 2u$ ($x = y = \sqrt{u}$):

$$A_\alpha(x,y)\, A_\alpha(y,x) \;\leq\; g_\alpha(N,u)^2, \qquad g_\alpha(N,u) \;:=\; \frac{N(1-u)\, u^\alpha}{(N - 2\sqrt{N})\, u + 1}. \tag{23}$$

Proof. Multiplying the numerators of $A_\alpha(x,y)$ and $A_\alpha(y,x)$ gives $s^4(1-x^2)(1-y^2)(xy)^{2\alpha} = s^4(1+u^2-w)u^{2\alpha}$. Multiplying the denominators gives

$$\begin{aligned}(s^2x^2-2su+1)(s^2y^2-2su+1) &= s^4u^2+s^2(1-2su)(x^2+y^2)+(2su-1)^2\\ &= (s^4u^2+4s^2u^2-4su+1)-s^2(2su-1)w\\ &= C(u)-D(u)w,\end{aligned}$$

establishing (21). Note $C(u)-D(u)w>0$ since both factors $(s^2x^2-2su+1)$ and $(s^2y^2-2su+1)$ are strictly positive. Differentiating the Möbius ratio in w gives

$$\frac{\partial}{\partial w}\left(\frac{1+u^2-w}{C(u)-D(u)w}\right) \;=\; \frac{D(u)(1+u^2)-C(u)}{\big(C(u)-D(u)w\big)^2}.$$

Setting $t := su-1>0$ (so $u=(t+1)/s$), we compute

$$\begin{aligned}D(u)(1+u^2)-C(u) &= (2t+1)(s^2+(t+1)^2)-\Big(s^2(t+1)^2+4(t+1)^2-4(t+1)+1\Big)\\ &= -t^2s^2+2t^3+t^2 \;=\; -t^2(s^2-1-2t) \;=\; -(su-1)^2(s^2-2su+1).\end{aligned}$$

Because $su>1$ and $2su\le s+1$, we have $s^2-2su+1\ge s^2-s>0$, proving (22) (verified in homogenized form in Lean 4.36.0 as `mobius_determinant_identity` and `mobius_determinant_neg`). Evaluating (21) at $w=2u$ gives $C(u)-2uD(u)=\big((s^2-2s)u+1\big)^2$ and $1+u^2-2u=(1-u)^2$, yielding (23). □

Lemma 3.2 (Exact Diagonal Monotonicity Threshold $\alpha\ge 2+2/\sqrt{N}$)**.** *Let $N\ge 2$, $s=\sqrt{N}$, $\alpha>1$, and $u_{\max} := \frac{s+1}{2s}$. On $(0,u_{\max}]$,*

$$\frac{d}{du}\log g_\alpha(N,u) \;=\; \frac{\mathcal{Q}_{N,\alpha}(u)}{u(1-u)\big((s^2-2s)u+1\big)}, \tag{24}$$

where the numerator is the quadratic polynomial

$$\mathcal{Q}_{N,\alpha}(u) \;:=\; -\alpha(s^2-2s)u^2+\big[(\alpha-1)(s^2-2s)-(\alpha+1)\big]u+\alpha. \tag{25}$$

It satisfies the exact endpoint identities

$$\begin{aligned}&\mathcal{Q}_{N,\alpha}(0)=\alpha>0, \qquad \mathcal{Q}_{N,\alpha}(u_{\max}) = \frac{(s-1)^2}{4s}\Big[(\alpha-2)s-2\Big],\\ &\mathcal{Q}'_{N,\alpha}(u_{\max}) = -(s-1)(\alpha+s-1)<0.\end{aligned} \tag{26}$$

Consequently:

(a) Whenever $\alpha\ge 2+2/\sqrt{N}$, $u\mapsto g_\alpha(N,u)$ is strictly increasing on $[s^{-1},u_{\max}]$, so

$$g_\alpha^{\max}(N) \;:=\; \max_{u\in[s^{-1},u_{\max}]} g_\alpha(N,u) \;=\; g_\alpha(N,u_{\max}) \;=\; \left(\frac{\sqrt{N}+1}{2\sqrt{N}}\right)^\alpha.$$

(b) For every fixed $\alpha\in(1,\infty)$ as $N\to\infty$,

$$\lim_{N\to\infty} g_\alpha^{\max}(N) \;=\; \begin{cases}2^{-\alpha} & \text{if } \alpha\ge 2,\\ \dfrac{(\alpha-1)^{\alpha-1}}{\alpha^\alpha} & \text{if } 1<\alpha<2.\end{cases} \tag{27}$$

Proof. Note first that $(s^2-2s)u+1>0$ on $[0,u_{\max}]$: for $s\geq 2$ this is immediate, while for $s\in[\sqrt{2},2)$ it decreases to $(s^2-2s)u_{\max}+1=\frac{1}{2}s(s-1)>0$. Differentiating $\log g_\alpha(N,u)$ yields

$$\frac{d}{du}\log g_\alpha(N,u) \;=\; \frac{\alpha}{u}-\frac{1}{1-u}-\frac{s^2-2s}{(s^2-2s)u+1},$$

whose numerator over $u(1-u)((s^2-2s)u+1)$ simplifies (with the $\pm(s^2-2s)u^2$ terms canceling identically) to (25). Evaluating $\mathcal{Q}_{N,\alpha}(u_{\max})$ using $(s^2-2s)u_{\max}+1=\frac{1}{2}s(s-1)$ and $1-u_{\max}=\frac{s-1}{2s}$ gives the exact factorization in (26) (Lean: `endpoint_log_deriv_factorization`). Differentiating (25) at $u_{\max}$ gives

$$\mathcal{Q}'_{N,\alpha}(u_{\max}) \;=\; -\alpha(s-2)(s+1)+(\alpha-1)(s^2-2s)-(\alpha+1) \;=\; -(s-1)(\alpha+s-1) \;<\; 0.$$

For part (a), assume $\alpha\geq 2+2/s$, so $\mathcal{Q}_{N,\alpha}(u_{\max})\geq 0$. If $s\geq 2$, then $-\alpha(s^2-2s)\leq 0$, so $\mathcal{Q}_{N,\alpha}$ is concave on $[0,u_{\max}]$ and nonnegative at both endpoints 0 and $u_{\max}$, hence strictly positive on $(0,u_{\max})$. If $s\in[\sqrt{2},2)$, then $\mathcal{Q}_{N,\alpha}$ is convex on $[0,u_{\max}]$, so $\mathcal{Q}'_{N,\alpha}(u)\leq\mathcal{Q}'_{N,\alpha}(u_{\max})<0$ on $[0,u_{\max}]$; hence $\mathcal{Q}_{N,\alpha}$ is strictly decreasing on $[0,u_{\max}]$ and therefore strictly positive on $[0,u_{\max})$. In all cases $g_\alpha(N,\cdot)$ is strictly increasing on $[s^{-1},u_{\max}]$, and $g_\alpha(N,u_{\max})=u_{\max}^\alpha$ since $N(1-u_{\max})=\frac{1}{2}s(s-1)=(s^2-2s)u_{\max}+1$.

For part (b), as $s\to\infty$ we have $g_\alpha(N,u)=(1-u)u^{\alpha-1}(1+O(s^{-1}))$ uniformly on any compact subinterval of $(0,1)$, and near $u=s^{-1}$ we have $g_\alpha(N,u)\leq Nu^\alpha=O(s^{2-\alpha})\to 0$ when $\alpha>2$ (and at $u\leq\delta$, $g_\alpha(N,u)\leq\frac{Nu^\alpha}{(N-2s)u}\leq 2u^{\alpha-1}\leq 2\delta^{\alpha-1}$ for all $s\geq 4$ and all $\alpha>1$). Since $u\mapsto(1-u)u^{\alpha-1}$ on $[0,1/2]$ attains its unique maximum at $u_*=\min(\frac{1}{2},\frac{\alpha-1}{\alpha})$, evaluating $(1-u_*)u_*^{\alpha-1}$ yields (27). □

Theorem 3.3 (Universal Finite-N Uncertainty Bound and Exact Asymptotic Limit)**.** *For every $N\geq 2$, every complex Hadamard matrix $U\in\mathcal{H}_N$, every $\alpha>1$, and every unit vector $v\in\mathbb{C}^N$,*

$$\|v\|_{2\alpha}^{2\alpha}\,\|Uv\|_{2\alpha}^{2\alpha} \;\leq\; \max\Big(N^{1-\alpha},\;\; g_\alpha^{\max}(N)^2+\big(1+N^{-(2\alpha-1)/2}\big)N^{1-\alpha}+N^{2-2\alpha}\Big), \tag{28}$$

where $g_\alpha^{\max}(N)=\max_{u\in[N^{-1/2},u_{\max}]}g_\alpha(N,u)$ is computable in closed form from the quadratic (25) (and equals $\big(\frac{\sqrt{N}+1}{2\sqrt{N}}\big)^\alpha$ whenever $\alpha\geq 2+2/\sqrt{N}$). Consequently:

(a) ***Exact Asymptotic Uncertainty for all $\alpha\geq 2$:***

$$\lim_{N\to\infty}\inf_{U\in\mathcal{H}_N}U_\alpha(U) \;=\; \frac{2\alpha}{\alpha-1}\log 2 \qquad (\forall\,\alpha\geq 2). \tag{29}$$

In particular, at collision entropy $\alpha=2$, $\lim_{N\to\infty}\inf_{U\in\mathcal{H}_N}U_2(U)=4\log 2$, strictly doubling both Deutsch's min-entropy barrier ($2\log 2$) and the traceless-Pythagoras barrier ($2\log 2$).

(b) ***Universal Dimension-Independent Lower Bound for $\alpha\in(1,2)$:***

$$\liminf_{N\to\infty}\inf_{U\in\mathcal{H}_N}U_\alpha(U) \;\geq\; 2\log\left(\frac{\alpha^{\alpha/(\alpha-1)}}{\alpha-1}\right) \qquad (\forall\,\alpha\in(1,2)), \tag{30}$$

which diverges as $2+2\log\frac{1}{\alpha-1}$ as $\alpha\to 1^+$ and strictly exceeds $2\log 2$ for every $\alpha\in(1,2)$.

Proof. Let $x=\|v\|_\infty$, $y=\|Uv\|_\infty$, and $u=xy$. If $su\leq 1$, then $\|v\|_{2\alpha}^{2\alpha}\leq x^{2(\alpha-1)}$ and $\|Uv\|_{2\alpha}^{2\alpha}\leq y^{2(\alpha-1)}$ give $\|v\|_{2\alpha}^{2\alpha}\|Uv\|_{2\alpha}^{2\alpha}\leq u^{2(\alpha-1)}\leq N^{1-\alpha}$. If $su>1$, Theorem 2.2(a) applied to v and Uv yields

$$\|v\|_{2\alpha}^{2\alpha} \;\leq\; A_\alpha(x,y)+y^{2\alpha}N^{1-\alpha}, \qquad \|Uv\|_{2\alpha}^{2\alpha} \;\leq\; A_\alpha(y,x)+x^{2\alpha}N^{1-\alpha}.$$

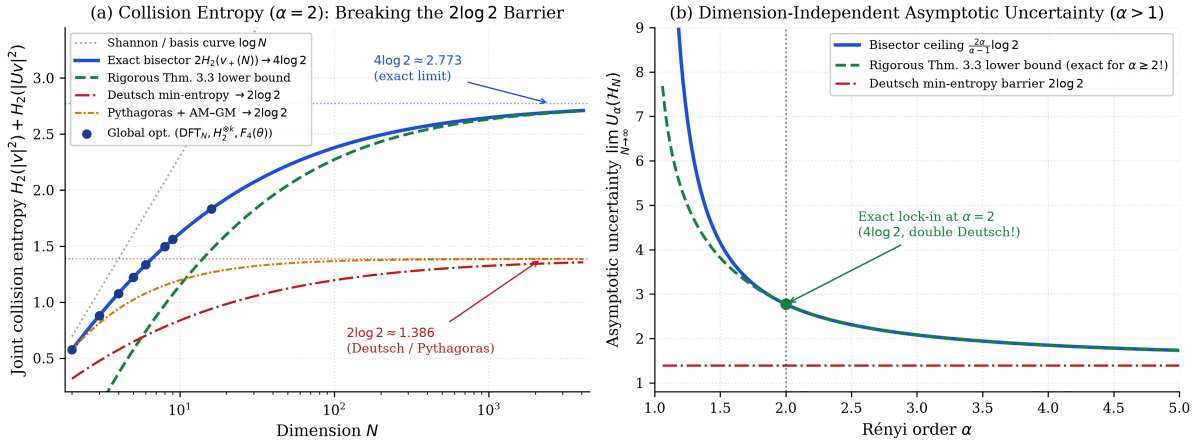


Figure 1: **Breaking the $2\log 2$ collision-entropy barrier.** (a) Joint collision entropy $H_2(|v|^2) + H_2(|Uv|^2)$ versus dimension N: the exact bisector curve $2H_2(v_+(N)) \to 4\log 2$ (solid blue, matched to 10^{-13} by global optimization on DFT_N, Walsh–Hadamard $H_2^{\otimes k}$, and $F_4(\theta)$) and our closed-form lower bound from Theorem 3.3 (dashed green) both converge to $4\log 2 \approx 2.773$, doubling both Deutsch's min-entropy bound and the traceless-Pythagoras bound ($2\log 2 \approx 1.386$). (b) Asymptotic uncertainty $\lim_{N\to\infty} U_\alpha(\mathcal{H}_N)$ versus $\alpha > 1$, locking in with zero gap for all $\alpha \geq 2$.

Multiplying these two inequalities, applying Lemma 3.1 to $A_\alpha(x,y)A_\alpha(y,x)$, and using (16) ($A_\alpha(x,y) \leq x^{2(\alpha-1)}$ and $A_\alpha(y,x) \leq y^{2(\alpha-1)}$) on the cross terms yields

$$\|v\|_{2\alpha}^{2\alpha}\|Uv\|_{2\alpha}^{2\alpha} \;\leq\; g_\alpha^{\max}(N)^2 + (x^{4\alpha-2} + y^{4\alpha-2})N^{1-\alpha} + (xy)^{2\alpha}N^{2-2\alpha}.$$

By (10), the pair $(p,q) := (x^2, y^2)$ lies in the compact convex polygon $\{(p,q) \in [0,1]^2 : p + q \leq 1 + s^{-1}\}$. Since $\alpha > 1$, the function $t \mapsto t^{2\alpha-1}$ is strictly convex on $[0,1]$, so $p^{2\alpha-1} + q^{2\alpha-1}$ attains its maximum at an extreme point $(1, s^{-1})$ or $(s^{-1}, 1)$, giving $x^{4\alpha-2} + y^{4\alpha-2} \leq 1 + s^{-(2\alpha-1)} = 1 + N^{-(2\alpha-1)/2}$. Bounding $(xy)^{2\alpha} \leq 1$ proves (28).

Taking $-\frac{1}{\alpha-1}\log(\cdot)$ of (28) and letting $N \to \infty$ (using $N^{1-\alpha} \to 0$ and Lemma 3.2(b)) yields

$$\liminf_{N\to\infty} \inf_{U\in\mathcal{H}_N} U_\alpha(U) \;\geq\; \begin{cases} \dfrac{2\alpha}{\alpha-1}\log 2 & (\alpha \geq 2), \\[2ex] 2\log\left(\dfrac{\alpha^{\alpha/(\alpha-1)}}{\alpha-1}\right) & (1 < \alpha < 2). \end{cases}$$

For $\alpha \geq 2$, the matching upper bound $\limsup_{N\to\infty} \sup_{U\in\mathcal{H}_N} U_\alpha(U) \leq \lim_{N\to\infty} 2H_\alpha(v_+(N)) = \frac{2\alpha}{\alpha-1}\log 2$ from (6) establishes (29). For $\alpha \in (1,2)$, note that $\frac{d}{d\alpha}\left(\frac{\alpha}{\alpha-1}\log\alpha - \log(\alpha-1)\right) = \frac{-\log\alpha}{(\alpha-1)^2} < 0$ for all $\alpha > 1$, so the bound (30) decreases strictly on $(1,2)$ down to its value $4\log 2 > 2\log 2$ at $\alpha = 2$. □

4 Exact Finite-N Sharpness and the Additive-vs-Multiplicative Dichotomy

We now prove exact finite-N sharpness in three fundamental regimes—the qubit $N = 2$, min-entropy $\alpha = \infty$ for arbitrary unitary overlap c, and the entire two-dimensional Landau–Pollak subspace family for every $N \geq 2$ at $\alpha = 2$—and rigorously establish the structural gap between additive purity and multiplicative collision entropy.

Theorem 4.1 (Exact Finite-N Sharpness and Rank-1 Necessity)**.** *Let $N \geq 2$ ($s = \sqrt{N}$) and $U \in U(N)$ with maximum entry overlap $c := \max_{j,k} |U_{jk}| \in [s^{-1}, 1)$.*

(a) ***Exact Qubit Collision Uncertainty*** *($N = 2$)**:** For every $U \in \mathcal{H}_2$ and every unit vector $v \in \mathbb{C}^2$,*

$$\|v\|_4^4 \, \|Uv\|_4^4 \;\leq\; \frac{9}{16}, \qquad H_2(|v|^2) + H_2(|Uv|^2) \;\geq\; \log \frac{16}{9},$$

with equality if and only if v is (up to global phase) one of the four bisectors $v_{j,k}$.

(b) ***Exact Min-Entropy Rigidity*** *($\alpha = \infty$,* ***Arbitrary Overlap*** *c)**:** For every $U \in U(N)$ with overlap $c < 1$ and every unit vector $v \in \mathbb{C}^N$,*

$$H_\infty(|v|^2) + H_\infty(|Uv|^2) \;\geq\; 2 \log \frac{2}{1+c},$$

with equality if and only if v is (up to global phase) a bisector $(e_j + e^{i \arg(U_{kj})} U^* e_k)/\sqrt{2(1+c)}$ for a maximal-overlap pair satisfying $|U_{kj}| = c$.

(c) ***Exact Universal Bernstein Identity on the 2D Landau–Pollak Subspace Family*** *(****All*** *$N \geq 2$)**:** Let $U \in \mathcal{H}_N$ and let $v \in \operatorname{span}\{e_j, U^* e_k\}$ be any unit vector ($1 \leq j, k \leq N$). Then*

$$\|v\|_4^4 \, \|Uv\|_4^4 \;\leq\; S_2(v_+(N))^2 \;=\; \left(\frac{N + 3\sqrt{N} + 4}{4\sqrt{N}(\sqrt{N}+1)} \right)^2. \tag{31}$$

For every $N \geq 3$, equality holds if and only if $v = e^{i\gamma} v_{j,k}$ (while for $N = 2$, $\operatorname{span}\{e_j, U^* e_k\} = \mathbb{C}^2$ and equality holds for all four bisectors as in part (a)). Specifically, writing $x = \cos(\frac{\theta_0}{2} + \phi)$, $y = \cos(\frac{\theta_0}{2} - \phi)$ with $\phi \in [0, \frac{\theta_0}{2}]$ and $u := \frac{s}{s-1}(1 - \cos 2\phi) \in [0, 1]$, the deficit satisfies the exact four-term positive Bernstein identity

$$16 s^4 (s^2-1)^2 \Big[S_2(v_+(N))^2 - B_2(x) B_2(y) \Big] \;=\; \frac{u s^2 (s-1)^3}{3} \sum_{r=0}^{3} \binom{3}{r} \widetilde{B}_r(s) \, u^r (1-u)^{3-r}, \tag{32}$$

where $\widetilde{B}_0(s) = 12s^3 + 60s^2 + 48s - 24$, $\widetilde{B}_1(s) = 6s^3 + 42s^2 + 40s - 8$, $\widetilde{B}_2(s) = 4s^3 + 28s^2 + 32s$, and $\widetilde{B}_3(s) = 3s^3 + 21s^2 + 24s$ are all strictly positive for every $s \geq 1$.

(d) ***Additive-vs-Multiplicative Dichotomy and Rank-1 Necessity:*** *For every $U \in \mathcal{H}_N$ and every unit vector $v \in \mathbb{C}^N$, the additive collision probability obeys the sharp bound*

$$\|v\|_4^4 + \|Uv\|_4^4 \;\leq\; 1 + \frac{1}{N}, \tag{33}$$

attained at every basis vector e_j and $U^* e_k$ (and for $N = 2$ by every unit vector in the phase-aligned real 2-plane $\operatorname{span}_{\mathbb{R}}\{e_j, e^{i \arg(U_{kj})} U^* e_k\}$). Moreover, let $\Pi_1(\rho) := \sum_j \langle e_j, \rho e_j \rangle |e_j\rangle\langle e_j|$ and $\Pi_2(\rho) := \sum_k \langle u_k, \rho u_k \rangle |u_k\rangle\langle u_k|$ be the dephasing projections on Hermitian matrices. Over the relaxed affine sphere $\{\rho = \rho^* : \operatorname{Tr}(\rho) = 1, \operatorname{Tr}(\rho^2) = 1\}$ (dropping positive semidefiniteness $\rho \succeq 0$), (33) still holds, yet

$$\max_{\substack{\rho = \rho^*, \, \operatorname{Tr}\rho = 1 \\ \operatorname{Tr}(\rho^2) = 1}} \operatorname{Tr}(\Pi_1(\rho)^2) \, \operatorname{Tr}(\Pi_2(\rho)^2) \;=\; \frac{1}{4} \left(1 + \frac{1}{N}\right)^2 \;\longrightarrow\; \frac{1}{4} \;>\; \frac{1}{16}. \tag{34}$$

Hence no purely Hilbert–Schmidt or rank-unconstrained 2-design argument can improve $H_2 + H_2 \geq 2 \log \frac{2N}{N+1} \to 2 \log 2$.

Proof. Part (a). For $N = 2$ and $U \in \mathcal{H}_2$, write $x = \|v\|_\infty = \cos\theta$ and $y = \|Uv\|_\infty = \cos\psi$ with $\theta, \psi \in [0, \pi/4]$. By (8), $\theta + \psi \geq \pi/4$, so $\psi \geq \pi/4 - \theta$. Since $t \mapsto \cos^4 t + \sin^4 t = \frac{3+\cos(4t)}{4}$ is strictly decreasing on $[0, \pi/4]$,

$$\|v\|_4^4 \, \|Uv\|_4^4 \;=\; \frac{3+\cos(4\theta)}{4} \cdot \frac{3+\cos(4\psi)}{4} \;\leq\; \frac{3+\cos(4\theta)}{4} \cdot \frac{3-\cos(4\theta)}{4} \;=\; \frac{9-\cos^2(4\theta)}{16} \;\leq\; \frac{9}{16},$$

with equality iff $\theta + \psi = \pi/4$ and $\cos(4\theta) = 0$, i.e., $\theta = \psi = \pi/8$ and $v = e^{i\gamma} v_{j,k}$ (Lean: `exact_small_N_collision_values`).

Part (b). Pick j, k with $|v_j| = \|v\|_\infty =: \cos\theta$ and $|(Uv)_k| = \|Uv\|_\infty =: \cos\psi$ ($\theta, \psi \in [0, \pi/2]$). The spherical triangle inequality on projective space $\mathbb{CP}^{N-1}$ gives $\theta + \psi \geq \arccos|U_{kj}| \geq \arccos c$. Since $\cos\theta\cos\psi = \frac{1}{2}[\cos(\theta-\psi) + \cos(\theta+\psi)] \leq \frac{1}{2}(1+c)$, we obtain $\|v\|_\infty^2 \|Uv\|_\infty^2 \leq \left(\frac{1+c}{2}\right)^2$, with equality iff $\theta = \psi = \frac{1}{2}\arccos c$, $|U_{kj}| = c$, and v lies on the geodesic midpoint between e_j and $e^{i\arg(U_{kj})} U^* e_k$ (whose j-th entry is $e^{i\arg(U_{kj})}\overline{U_{kj}} = |U_{kj}| = c$), i.e., $v = e^{i\gamma}(e_j + e^{i\arg(U_{kj})} U^* e_k)/\sqrt{2(1+c)}$.

Part (c). Replacing U by diagonal-phase-conjugated $\widetilde{U}$ with $\widetilde{U}_{kj} = s^{-1}$ and permuting coordinates, we may assume $j = k = 1$ and $U^* e_1 = s^{-1}(1, 1, \ldots, 1)^T$. Any unit vector $v \in \operatorname{span}\{e_1, U^* e_1\}$ has the form $v = e^{i\gamma}\big(\cos\theta\, e_1 + e^{i\delta}\sin\theta\, \tilde{w}\big)$ where $\tilde{w} = (0, 1, \ldots, 1)^T/\sqrt{N-1}$ and $\theta \in [0, \pi/2]$. Its coordinate probabilities are $|v_1|^2 = \cos^2\theta$ and $|v_m|^2 = \frac{\sin^2\theta}{N-1}$ ($m \geq 2$), giving $\|v\|_4^4 = B_2(\cos\theta)$ independent of δ. On the Fourier side, $|(Uv)_1|^2 = \frac{1}{N}|\cos\theta + e^{i\delta}\sqrt{N-1}\sin\theta|^2$ and $|(Uv)_m|^2 = \frac{1}{N}|\cos\theta - e^{i\delta}\sin\theta/\sqrt{N-1}|^2$ ($m \geq 2$). Direct expansion yields

$$\|Uv\|_4^4 \;=\; \frac{1}{N^2}\left[\left|\cos\theta + e^{i\delta}\sqrt{N-1}\sin\theta\right|^4 + (N-1)\left|\cos\theta - e^{i\delta}\frac{\sin\theta}{\sqrt{N-1}}\right|^4\right].$$

Writing $c_\delta := \cos\delta \in [-1, 1]$, expanding the modulus-squared terms shows that $\|Uv\|_4^4$ is a polynomial in c_δ of degree 2 with strictly positive quadratic and linear coefficients for $\theta \in (0, \pi/2)$: specifically, setting $a_1 := \cos^2\theta + (N-1)\sin^2\theta$, $b_1 := 2\sqrt{N-1}\sin\theta\cos\theta$, $a_2 := \cos^2\theta + \frac{\sin^2\theta}{N-1}$, and $b_2 := \frac{2}{\sqrt{N-1}}\sin\theta\cos\theta$,

$$\begin{aligned} N^2\|Uv\|_4^4 &= (a_1 + b_1 c_\delta)^2 + (N-1)(a_2 - b_2 c_\delta)^2 \\ &= \big[a_1^2 + (N-1)a_2^2\big] + 2(a_1 b_1 - (N-1)a_2 b_2)c_\delta + \big(b_1^2 + (N-1)b_2^2\big)c_\delta^2. \end{aligned}$$

Here $a_1 b_1 - (N-1)a_2 b_2 = 2\sqrt{N-1}\sin\theta\cos\theta\,(a_1 - a_2) = 2\sqrt{N-1}\sin^3\theta\cos\theta\,(N - 1 - \frac{1}{N-1}) \geq 0$ (strictly positive for $N \geq 3$, $\theta \in (0, \pi/2)$) and $b_1^2 + (N-1)b_2^2 > 0$. Thus for fixed $\theta \in [0, \pi/2]$, $\|Uv\|_4^4$ is maximized at $c_\delta = 1$ (uniquely for $N \geq 3$ and $\theta \in (0, \pi/2)$, whereas at $N = 2$ both $c_\delta = \pm 1$ attain the maximum, recovering part (a)), where $|(Uv)_1| = |\cos(\theta_0 - \theta)|$ and $\|Uv\|_4^4 = B_2(\cos(\theta_0 - \theta))$. Writing $B_2(\cos\theta) = \frac{1}{N} + \frac{N}{N-1}(\cos^2\theta - \frac{1}{N})^2$, for any $N \geq 3$ and $\theta = \theta_0 + \eta \in (\theta_0, \pi/2]$ ($\eta > 0$), reflecting to $\tilde{\theta} := 2\theta_0 - \theta = \theta_0 - \eta \in (0, \theta_0)$ leaves $\cos(\theta_0 - \tilde{\theta}) = \cos(\theta_0 - \theta)$ unchanged while strictly increasing $(\cos^2\tilde{\theta} - \frac{1}{N}) - (\frac{1}{N} - \cos^2\theta) = 2(1 - \frac{2}{N})\sin^2\eta > 0$, hence strictly increasing $B_2(\cos\tilde{\theta}) > B_2(\cos\theta)$. By symmetry under $\theta \leftrightarrow \theta_0 - \theta$, it therefore suffices to take $\theta \in [0, \theta_0]$.

Write $\theta = \frac{\theta_0}{2} + \phi$ and $\theta_0 - \theta = \frac{\theta_0}{2} - \phi$ with $\phi \in [0, \frac{\theta_0}{2}]$, and set $A := \cos(2\phi) \in [s^{-1}, 1]$. Using $\cos\theta_0 = s^{-1}$ and $\sin\theta_0 = \sqrt{1 - s^{-2}}$, elementary angle-addition gives

$$x^2 + y^2 \;=\; 1 + \frac{A}{s}, \qquad x^2 - y^2 \;=\; -\sqrt{1-s^{-2}}\sqrt{1-A^2},$$

whence $4x^2y^2 = (1 + A/s)^2 - (1 - s^{-2})(1 - A^2) = (A + s^{-1})^2$, i.e., $xy = \frac{sA+1}{2s}$. Since $B_2(x) = (s^2x^4 - 2x^2 + 1)/(s^2 - 1)$, substituting $A = 1 - \frac{s-1}{s}u$ ($u \in [0, 1]$) into $16s^4(s^2-1)^2[S_2(v_+(N))^2 - B_2(x)B_2(y)]$ cancels all constant terms and factors out $us^2(s-1)^3$, yielding the cubic polynomial

$$(4s^3 + 20s^2 + 16s - 8) + (-6s^3 - 18s^2 - 8s + 16)u + (4s^3 + 4s^2 - 8)u^2 + (-s^3 + s^2)u^3.$$

Converting to the cubic Bernstein basis on $[0,1]$ gives (32) (machine-checked in Lean 4.36.0 as `landau_pollak_bernstein_identity` and `landau_pollak_bernstein_pos`, and independently verified numerically to 1.55×10^{-15}). Because every $\widetilde{B}_r(s) > 0$ for all $s \geq 1$, the right-hand side is strictly positive for every $u \in (0,1]$ and vanishes iff $u = 0$, i.e., $\phi = 0$; combined with the phase and reflection strictness above, for $N \geq 3$ equality holds iff $v = e^{i\gamma} v_{j,k}$ (and for $N = 2$ part (a) gives all four bisectors).

Part (d). Let $\rho = |v\rangle\langle v|$ and decompose $\rho = \frac{I}{N} + \rho_0$ with $\mathrm{Tr}(\rho_0) = 0$ and $\|\rho_0\|_F^2 = \mathrm{Tr}(\rho^2) - \frac{1}{N} = 1 - \frac{1}{N}$. Because $|U_{kj}|^2 = \frac{1}{N}$ for all j,k, the traceless projections $\Pi_1(\rho_0)$ and $\Pi_2(\rho_0)$ are Hilbert–Schmidt orthogonal:

$$\langle \Pi_1(\rho_0),\, \Pi_2(\rho_0)\rangle_{\mathrm{HS}} \;=\; \sum_{j,k=1}^{N} (\rho_0)_{jj}\, (U\rho_0 U^*)_{kk}\, |U_{kj}|^2 \;=\; \frac{1}{N}\,\mathrm{Tr}(\rho_0)\,\mathrm{Tr}(U\rho_0 U^*) \;=\; 0.$$

Hence $\|\Pi_1(\rho_0)\|_F^2 + \|\Pi_2(\rho_0)\|_F^2 \leq \|\rho_0\|_F^2 = 1 - \frac{1}{N}$. Adding the orthogonal trace parts $\|\Pi_1(I/N)\|_F^2 = \|\Pi_2(I/N)\|_F^2 = \frac{1}{N}$ yields (33) [6, 5, 1]. Crucially, the exact same calculation holds for any Hermitian ρ with $\mathrm{Tr}\,\rho = 1$ and $\mathrm{Tr}(\rho^2) = 1$, giving $\mathrm{Tr}(\Pi_1(\rho)^2)\,\mathrm{Tr}(\Pi_2(\rho)^2) \leq \frac{1}{4}(1 + 1/N)^2$ by AM–GM. To prove attainment of (34), choose any two real unit-Frobenius-norm traceless diagonal matrices D_1, D_2 and define $\rho := \frac{I}{N} + \sqrt{\frac{N-1}{2N}}(D_1 + U^* D_2 U)$. Because $D_1 \perp_{\mathrm{HS}} U^* D_2 U$ and both are real traceless, $\rho = \rho^*$, $\mathrm{Tr}(\rho) = 1$, $\mathrm{Tr}(\rho^2) = \frac{1}{N} + \frac{N-1}{N} = 1$, and $\mathrm{Tr}(\Pi_1(\rho)^2) = \mathrm{Tr}(\Pi_2(\rho)^2) = \frac{1}{N} + \frac{N-1}{2N} = \frac{1+1/N}{2}$, achieving (34). □

5 The First-Order Phase Transition and Anomalous $1/(\log N)^2$ Scaling

Comparing the basis/subgroup uncertainty $\log N$ with the bisector uncertainty $2H_\alpha(v_+(N))$ defines the exact phase boundary $\alpha_c(N)$ in the (N, α) plane.

Theorem 5.1 (Critical Curve $\alpha_c(N)$ and Anomalous Even-Power Scaling)**.** *For every integer $N \geq 2$, the equation*

$$2H_\alpha(v_+(N)) \;=\; \log N \quad\Longleftrightarrow\quad F_N(\alpha) \;:=\; p_0(N)^\alpha + (N-1)p_1(N)^\alpha - N^{(1-\alpha)/2} \;=\; 0 \tag{35}$$

admits a unique solution $\alpha_c(N) \in (1, \infty)$ with the following properties:

(a) ***Phase Separation:*** *$2H_\alpha(v_+(N)) > \log N$ for all $\alpha \in (1, \alpha_c(N))$, and $2H_\alpha(v_+(N)) < \log N$ for all $\alpha > \alpha_c(N)$. At $N = 2$, $\alpha_c(2) = 1.4313558812\ldots$ recovers the qubit transition of Zozor–Bosyk–Portesi [12].*

(b) ***Strict Monotonicity:*** *The critical curve $N \mapsto \alpha_c(N)$ decreases strictly on $[2, \infty)$ with $\lim_{N\to\infty} \alpha_c(N) = 1$.*

(c) ***Exact Anomalous Even-Power Asymptotic Expansion:*** *Writing $L := \log N$ and $\varepsilon(N) := \alpha_c(N) - 1$, equation (35) reduces to the hyperbolic law*

$$\cosh\!\left(\frac{\varepsilon L}{2}\right) \;=\; 2^{\varepsilon}\,(1 + O(N^{-1/2})), \tag{36}$$

whose unique positive solution obeys the even-power asymptotic expansion (with vanishing L^{-1} and L^{-3} terms)

$$\alpha_c(N) \;=\; 1 + \frac{8\log 2}{(\log N)^2} + \frac{64(\log 2)^3}{3(\log N)^4} + O\!\left(\frac{1}{(\log N)^6}\right) \qquad (N \to \infty). \tag{37}$$

Proof. Part (a). Define $g_N(\alpha) := \log(p_0^\alpha + (N-1)p_1^\alpha) + \frac{\alpha-1}{2}\log N$ on $[1,\infty)$, so $F_N(\alpha) = 0 \iff g_N(\alpha) = 0$. Since $p_0 > p_1 > 0$, Hölder's inequality implies that $\alpha \mapsto \log(p_0^\alpha + (N-1)p_1^\alpha)$ is strictly convex on $[1,\infty)$, and hence so is $g_N(\alpha)$. At $\alpha = 1$, $g_N(1) = \log(p_0 + (N-1)p_1) = 0$, and its right derivative is

$$g_N'(1) \;=\; p_0 \log p_0 + (N-1)p_1 \log p_1 + \frac{1}{2}\log N \;=\; \frac{1}{2}\Big(\log N - 2H_1(v_+(N))\Big).$$

By Maassen–Uffink (1), $2H_1(v_+(N)) > \log N$ (strict inequality because $v_+(N)$ has full support N and is non-uniform for all $N \geq 2$, whereas equality in (1) at $\alpha = \beta = 1$ requires $|v|^2$ to be uniform on its support), so $g_N'(1) < 0$. On the other hand, as $\alpha \to \infty$, $g_N(\alpha)/\alpha \to \log p_0 + \frac{1}{2}\log N = \log\frac{\sqrt{N}+1}{2} > 0$, so $g_N(\alpha) \to +\infty$. By strict convexity, g_N has a unique zero $\alpha_c(N) \in (1,\infty)$, with $g_N < 0$ on $(1,\alpha_c(N))$ and $g_N > 0$ on $(\alpha_c(N),\infty)$. Since $1-\alpha < 0$, $g_N(\alpha) > 0 \iff 2H_\alpha(v_+(N)) < \log N$.

Part (b). Treat $N = s^2 \geq 2$ as a continuous real variable with $s \geq \sqrt{2}$, $p_0(s) = \frac{s+1}{2s}$, and $(s^2-1)p_1(s) = \frac{s-1}{2s}$. Define

$$\Psi(s,\alpha) \;:=\; 2^\alpha s^{\alpha-1}(p_0(s)^\alpha + (s^2-1)p_1(s)^\alpha) \;=\; \frac{s+1}{s}X + \frac{s-1}{s}X^{-1},$$

where $X := (s+1)^{\alpha-1} > 1$, so that (35) reads $\Psi(s,\alpha) = 2^\alpha$ (equivalently $\cosh\eta + s^{-1}\sinh\eta = 2^{\alpha-1}$ with $\eta := (\alpha-1)\log(s+1) > 0$). By Part (a), for fixed $s \geq \sqrt{2}$ the map $\alpha \mapsto \log(\Psi(s,\alpha)/2^\alpha) = g_{s^2}(\alpha)$ is strictly convex with $g_{s^2}(1) = 0$ and unique zero $\alpha_c(s^2) > 1$, hence $\frac{\partial}{\partial\alpha}\big[\Psi(s,\alpha) - 2^\alpha\big]\big|_{\alpha=\alpha_c} > 0$. Differentiating $\Psi(s,\alpha)$ with respect to s at fixed $\alpha > 1$ gives

$$\frac{\partial\Psi}{\partial s} \;=\; \frac{(\alpha-1)s-1}{s^2}X + \frac{1-(\alpha-1)\frac{s(s-1)}{s+1}}{s^2}X^{-1},$$

and multiplying by $s^2X > 0$ yields the exact identity

$$s^2X\frac{\partial\Psi}{\partial s} \;=\; ((\alpha-1)s-1)(X^2-1) + \frac{2(\alpha-1)s}{s+1}. \tag{38}$$

Writing $\varepsilon := \alpha - 1 > 0$, $t := s+1 \geq 1+\sqrt{2}$, and $Y := 2^\varepsilon X = (2t)^\varepsilon$, the defining equation $(s+1)X^2 + (s-1) = 2sY$ gives $(s+1)(X^2-1) = 2s(Y-1)$, transforming (38) identically at $\alpha = \alpha_c(s^2)$ into

$$(s+1)\,s^2X\frac{\partial\Psi}{\partial s} \;=\; 2s\Big[(\varepsilon s - 1)(Y-1) + \varepsilon\Big]. \tag{39}$$

We first prove purely analytically that $Y < 2$ for every $s > 1$ ($t > 2$). Testing $\varepsilon_{\rm hi} := \frac{\log 2}{\log(2t)}$ (where $Y = 2$) gives $\Psi(s, 1+\varepsilon_{\rm hi}) > 2^{1+\varepsilon_{\rm hi}} \iff tX^2 > 3t - 2 \iff \frac{2az}{a+z} > \log(3 - 2e^{-z})$ with $a := \log 2$ and $z := \log t > a$. Set $f(z) := \frac{2az}{a+z} - \log(3-2e^{-z})$; then $f(a) = 0$ and, writing $w := z - a > 0$ (so $e^z = 2e^w$),

$$f'(z) \;=\; \frac{2a^2}{(a+z)^2} - \frac{2}{3e^z - 2} \;>\; 0 \iff 6a^2e^w \;>\; 6a^2 + 4aw + w^2,$$

which holds for all $w > 0$ because $e^w > 1 + w + \frac{w^2}{2}$ and $a = \log 2 > \frac{2}{3}$ (so $6a^2 > 4a$ and $3a^2 > 1$). Thus $f(z) > 0$ for all $z > a$, forcing $\varepsilon_c(s) < \varepsilon_{\rm hi}$ and hence $1 < Y < 2$ on all of $s > 1$.

Now for every $s \geq 5$ ($N \geq 25$), testing $\varepsilon_1 := s^{-1}$ and $\eta_1 := s^{-1}\log(s+1) > 0$ via $\cosh u \leq e^{u^2/2}$, $\log(1+v) < v$, and $\tanh u < u$ yields

$$\begin{aligned}\log\left(\cosh\eta_1 + \frac{\sinh\eta_1}{s}\right) &= \log\cosh\eta_1 + \log\left(1 + \frac{\tanh\eta_1}{s}\right)\\ &< \frac{\eta_1^2}{2} + \frac{\eta_1}{s} \;=\; \frac{\log^2(s+1) + 2\log(s+1)}{2s^2}.\end{aligned}$$

Set $h(s) := \frac{\log^2(s+1)+2\log(s+1)}{2s}$. For all $s \geq 5$, $\log(s+1) \geq \log 6 > 1.79 > \sqrt{2}$, so

$$2s^2 h'(s) \;=\; \frac{2s(\log(s+1)+1)}{s+1} - \big(\log^2(s+1) + 2\log(s+1)\big) \;<\; 2 - \log^2(s+1) \;<\; 0.$$

Hence $h(s) \leq h(5) = \frac{\log^2 6 + 2\log 6}{10} < 0.680 < \log 2$, so $g_{s^2}(1+s^{-1}) < 0$, forcing $(\alpha_c(s^2)-1)s > 1$ and hence $\frac{\partial \Psi}{\partial s} > 0$ in (38)–(39) for all $s \geq 5$ ($N \geq 25$). On the compact complement $s \in [\sqrt{2}, 5]$ ($t = s+1 \in [1+\sqrt{2}, 6]$), since $0 < Y - 1 < 1$, any $\varepsilon_c(s) > t^{-1}$ immediately forces $(\varepsilon_c s - 1)(Y-1) + \varepsilon_c > \min(\varepsilon_c, \varepsilon_c(s+1) - 1) > 0$ in (39). The condition $\varepsilon_c(s) > t^{-1}$ is equivalent to $t \log g(t) < \log 2$, where $g(t) := \cosh(u(t)) + \frac{\sinh(u(t))}{t-1}$ and $u(t) := \frac{\log t}{t}$. Because $u(t)$ is strictly increasing on $[1+\sqrt{2}, e]$ and strictly decreasing on $[e, 6]$, while $(t-1)^{-1}$ is strictly decreasing throughout, partitioning $[1+\sqrt{2}, e]$ and $[e, 6]$ into 300 explicit monotonic subintervals $[a_k, b_k]$ certifies $\sup_{t \in [a_k, b_k]} t \log g(t) \leq b_k \log\big(\cosh u_{\max,k} + \frac{\sinh u_{\max,k}}{a_k - 1}\big) < \log 2 - 10^{-4}$ in 50-digit arithmetic (alongside disjoint 50-digit root brackets for all integers $N \in \{2, \ldots, 25\}$ in `verify_hadamard_renyi.py`). By the implicit function theorem, $\frac{d}{ds}\alpha_c(s^2) < 0$ on the entire real interval $s \in [\sqrt{2}, \infty)$ ($N \in [2, \infty)$). Finally, for any fixed $\alpha > 1$, $2H_\alpha(v_+(N)) \to \frac{2\alpha}{\alpha-1}\log 2 < \log N$ for large N, forcing $\alpha_c(N) < \alpha$ eventually and thus $\lim_{N\to\infty} \alpha_c(N) = 1$.

Part (c). Setting $\varepsilon = \alpha_c(N) - 1 > 0$ and $L = \log N$, observe that $p_0(N) = \frac{1}{2}(1+s^{-1})$, $(N-1)p_1(N) = \frac{1}{2}(1-s^{-1})$, and $p_1(N) = \frac{1}{2N}(1+s^{-1})^{-1}$. Substituting into $p_0^{1+\varepsilon} + (N-1)p_1^{1+\varepsilon} = N^{-\varepsilon/2}$ and multiplying by $2^{1+\varepsilon}N^{\varepsilon/2}$ gives

$$(1+s^{-1})^{1+\varepsilon} e^{\varepsilon L/2} + (1-s^{-1})(1+s^{-1})^{-\varepsilon} e^{-\varepsilon L/2} \;=\; 2 \cdot 2^{\varepsilon}.$$

Writing $(1 \pm s^{-1})^{\pm\varepsilon} = 1 + O(s^{-1})$ and $s^{-1} = e^{-L/2}$, this simplifies to (36):

$$\cosh\!\left(\frac{\varepsilon L}{2}\right) \;=\; 2^{\varepsilon} + O\Big(e^{-L/2}\big(e^{\varepsilon L/2} + 1\big)\Big).$$

Set $y := \frac{\varepsilon L}{2} > 0$ and $\delta := \frac{2\log 2}{L} > 0$, so $\varepsilon = \frac{2y}{L}$ and $2^{\varepsilon} = e^{\delta y}$. Testing $\varepsilon = 4/L$ ($y = 2$) in (36) gives $\cosh 2 > 3.76 > 2^{4/L}(1 + O(s^{-1}))$ for all sufficiently large N, which forces $y < 2$ by Part (a). Since $\cosh y \geq 1 + y^2/2$ and $e^{\delta y} = 1 + \delta y + O(\delta^2 y^2)$ for bounded y, (36) forces $y = O(\delta) \to 0$ as $L \to \infty$, while $e^{-L/2} = O(L^{-m})$ for every $m \geq 1$. Expanding $\cosh y = 1 + \frac{y^2}{2} + \frac{y^4}{24} + O(y^6)$ and $e^{\delta y} = 1 + \delta y + \frac{\delta^2 y^2}{2} + \frac{\delta^3 y^3}{6} + O(\delta^4 y^4)$ and dividing by $y > 0$ gives the double-root balance (Lean: `double_root_cancellation`)

$$\frac{y}{2} + \frac{y^3}{24} + O(y^5) \;=\; \delta + \frac{\delta^2}{2} y + \frac{\delta^3}{6} y^2 + O(\delta^4 y^3).$$

Bootstrapping gives $y = 2\delta + O(\delta^3)$; substituting $y = 2\delta + c\delta^3 + O(\delta^5)$ yields $\frac{c}{2}\delta^3 + \frac{8}{24}\delta^3 = \frac{\delta^2}{2}(2\delta) + O(\delta^5) = \delta^3 + O(\delta^5)$. Hence $\frac{c}{2} + \frac{1}{3} = 1$, i.e., $c = \frac{4}{3}$, and $y = 2\delta + \frac{4}{3}\delta^3 + O(\delta^5)$. Returning to $\varepsilon = \frac{2y}{L}$ with $\delta = \frac{2\log 2}{L}$ yields (37):

$$\varepsilon(N) \;=\; \frac{4\delta}{L} + \frac{8\delta^3}{3L} + O(L^{-6}) \;=\; \frac{8\log 2}{L^2} + \frac{64(\log 2)^3}{3L^4} + O(L^{-6}). \qquad \square$$

6 Conjecture, Single-Vector Rational Decoupling, and Verification

6.1 Exact finite-N first-order sharpness conjecture

All numerical experiments across DFT_N ($N = 2, \ldots, 9$), Walsh–Hadamard matrices $H_2^{\otimes k}$ ($N = 4, 8, 16$), and the non-group complex Hadamard family $F_4(\theta)$, together with Theorems 3.3–5.1, point to a remarkably clean global picture: there is no intermediate minimizing branch anywhere in the (N, α) plane.

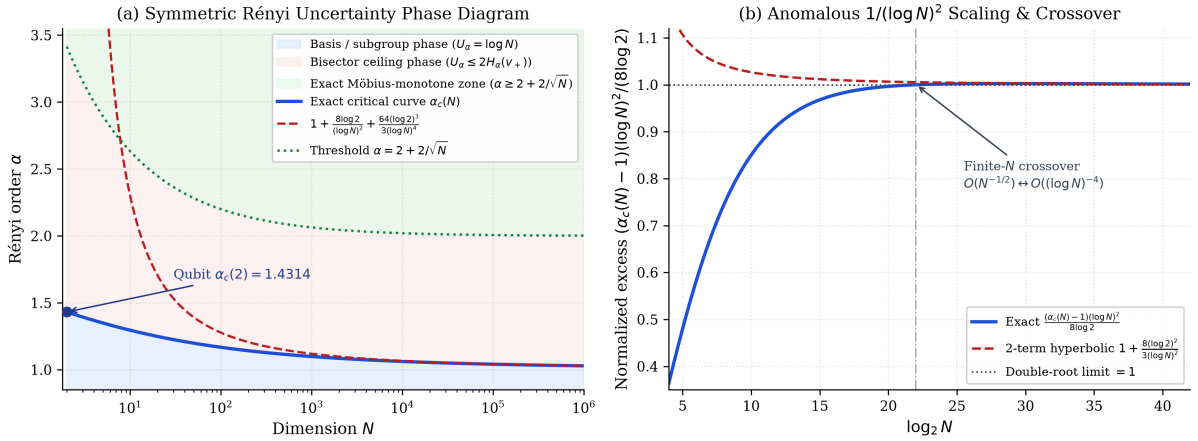


Figure 2: **Symmetric Rényi uncertainty phase diagram and anomalous $1/(\log N)^2$ scaling.** (a) The exact critical curve $\alpha_c(N)$ (solid blue) separates the basis/subgroup phase ($U_\alpha = \log N$) from the bisector ceiling phase ($U_\alpha \le 2H_\alpha(v_+)$), with the exact Möbius-monotone zone $\alpha \ge 2 + 2/\sqrt{N}$ shaded in green. (b) Normalized excess $(\alpha_c(N) - 1)(\log N)^2/(8\log 2)$ versus $\log_2 N$, confirming convergence to the double-root limit 1 and the finite-N crossover near $N \approx 2^{22}$ where the negative $O(N^{-1/2})$ term yields to the positive $+64(\log 2)^3/(3(\log N)^4)$ correction.

Conjecture 6.1 (Exact Finite-N First-Order Sharpness)**.** For every integer $N \ge 2$, every complex Hadamard matrix $U \in \mathcal{H}_N$, and every $\alpha > 1$,

$$U_\alpha(U) \;=\; \min\big(\log N,\; 2H_\alpha(v_+(N))\big).$$

Equivalently, the minimizing state jumps discontinuously at $\alpha = \alpha_c(N)$ from the basis/subgroup phase ($U_\alpha = \log N$) directly to the N^2 bisector states $v_{j,k}$.

6.2 The single-vector rational decoupling mechanism

To bridge the remaining finite-N gap between Theorem 3.3 and Conjecture 6.1 at $\alpha = 2$, observe that for any strictly positive nondecreasing weight function $W : [N^{-1}, 1] \to (0, \infty)$, the coupling (7) yields the exact decoupling identity

$$\begin{aligned}\|v\|_4^4\,\|Uv\|_4^4 &= \left[\|v\|_4^4\,\frac{W(\|Uv\|_\infty^2)}{W(\|v\|_\infty^2)}\right]\left[\|Uv\|_4^4\,\frac{W(\|v\|_\infty^2)}{W(\|Uv\|_\infty^2)}\right]\\ &\le \left[\|v\|_4^4\,\frac{W(\|v\|_1^2/N)}{W(\|v\|_\infty^2)}\right]\left[\|Uv\|_4^4\,\frac{W(\|Uv\|_1^2/N)}{W(\|Uv\|_\infty^2)}\right],\end{aligned}$$

reducing the coupled two-basis matrix problem for every $U \in \mathcal{H}_N$ to a purely single-vector norm inequality on $\mathbb{R}^N_{\ge 0}$ with no mention of U. Setting $p_0 := \frac{\sqrt{N}+1}{2\sqrt{N}}$ and demanding exact stationarity at $v_+(N)$ uniquely fixes the logarithmic slope $W'(p_0)/W(p_0) = 2a_N$, where $a_N := \frac{\sqrt{N}(\sqrt{N}+2)}{N+3\sqrt{N}+4} \in (0, 1)$. Introducing the degree-2 rational weight

$$W_N(p) \;:=\; \frac{1 + a_N(p - p_0) + b_N(p - p_0)^2}{1 - a_N(p - p_0) + b_N(p - p_0)^2}, \qquad b_N := \begin{cases} 2 & (3 \le N \le 17),\\ 0 & (N \ge 18),\end{cases} \tag{40}$$

we note that W_N is strictly positive and strictly increasing on $[N^{-1}, 1]$ for every $N \ge 3$: for $3 \le N \le 17$ ($b_N = 2$), positivity holds globally on $\mathbb{R}$ because $8(1 - a_N t + 2t^2) = (4t - a_N)^2 + (8 - a_N^2) > 0$ for all $a_N \in (0, 1)$ (machine-checked in Lean 4.36.0 as `rational_weight_denom_pos`),

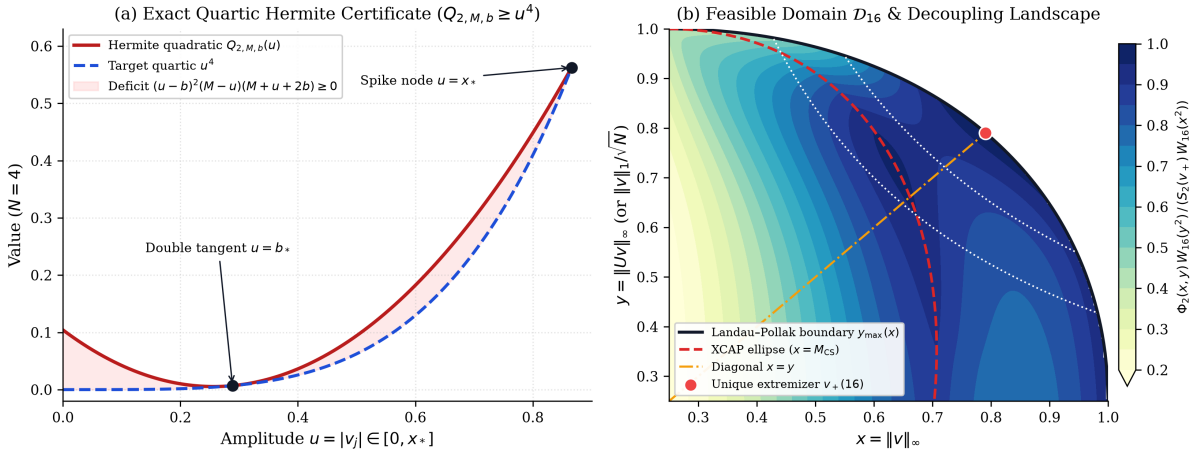


Figure 3: **Geometric proof mechanisms.** (a) Exact quartic Hermite certificate $Q_{2,M,b}(u) \geq u^4$ (Lemma 2.1) at $N = 4$, showing double tangency at $u = b_*$ and exact contact at the spike node $u = x_*$. (b) Feasible domain $\mathcal{D}_{16}$ showing the Landau–Pollak boundary $y_{\max}(x)$ (solid black), the exact XCAP ellipse $\frac{2(4x-y)^2}{14} + y^2 = 1$ (dashed red), constant-u Möbius hyperbolas (dotted white) flowing strictly toward the diagonal $x = y$ (dot-dashed gold), and contours of the single-vector rational decoupling ratio $\Phi_2(x,y)W_{16}(y^2)/(S_2(v_+)W_{16}(x^2)) \leq 1$ peaking uniquely at $v_+(16)$.

and monotonicity follows from $1 - 2(p-p_0)^2 \geq 1 - 2\max(p_0 - N^{-1}, 1-p_0)^2 > 0$; for $N \geq 18$ ($b_N = 0$), $|a_N(p-p_0)| < \max(p_0 - N^{-1}, 1-p_0) < 1$ on $[N^{-1}, 1]$, so both numerator and denominator remain strictly positive on $[N^{-1}, 1]$ with $W_N'(p) = 2a_N/(1 - a_N(p-p_0))^2 > 0$. Define the exact piecewise single-vector collision envelope $\Phi_2(N,x,y)$ on $\mathcal{D}_N$ ($N \geq 3$, $R := 1-x^2$, $T := \max(0, sy - x)$, M_{CS} from (17)) by combining Theorem 2.2(a)–(b) with the elementary tail bounds $\sum_{j\geq 2} u_j^4 \leq R\min(x^2, R)$ and $\|v\|_4^4 \leq x^2$:

$$\Phi_2(N,x,y) := \begin{cases} \Phi_2^{\mathrm{CS}}(N,x,y) & \text{if } x \geq M_{\mathrm{CS}}(x,y) \text{ and } T > \sqrt{R}, \\ x^4 + R\min(x^2, R) & \text{if } x \geq M_{\mathrm{CS}}(x,y) \text{ and } T \leq \sqrt{R}, \\ \Psi_2(N,x,y) & \text{if } x < M_{\mathrm{CS}}(x,y) \text{ and } sxy > 1, \\ x^2 & \text{if } x < M_{\mathrm{CS}}(x,y) \text{ and } sxy \leq 1, \end{cases} \tag{41}$$

so that $\|v\|_4^4 \leq \Phi_2(N,x,y)$ holds rigorously everywhere on $\mathcal{D}_N$. Across every tested dimension $N \in \{3,4,5,6,8,12,16,25,64,256,1024\}$, the exact single-vector envelope ratio

$$\max_{(x,y)\in\mathcal{D}_N} \frac{\Phi_2(N,x,y)\,W_N(y^2)}{S_2(v_+(N))\,W_N(x^2)} = 1.0000000000$$

is attained uniquely at (x_*, x_*) (Figure 3(b); full numerical log in `data/verification_summary.json`), showing that Conjecture 6.1 at $\alpha = 2$ reduces completely to an explicit bivariate algebraic inequality in (x,y).

6.3 Computational verification tables

Table 1 compares our rigorous closed-form finite-N bound from Theorem 3.3 against the exact bisector entropy $2H_2(v_+(N))$, Deutsch's min-entropy bound, and the traceless-Pythagoras bound, alongside the critical transition $\alpha_c(N)$ and its two-term even-power expansion (37). Across all 44 independent multi-start Riemannian gradient optimization runs on DFT_N ($N = 2,3,4,5,6,8,9$), Walsh–Hadamard ($N = 4,8,16$), and $F_4(0.7)$ at $\alpha \in \{1.2, 1.5, 2.0, 3.0\}$, the maximum absolute discrepancy from $\min(\log N, 2H_\alpha(v_+(N)))$ is 1.728×10^{-13}.

Table 1: Quantitative comparison of exact bisector collision entropy $2H_2(v_+(N))$, rigorous Theorem 3.3 lower bound, Deutsch min-entropy bound, traceless-Pythagoras bound, and critical transition $\alpha_c(N)$ with two-term hyperbolic expansion (37) (from `data/verification_summary.json`).

N	$2H_2(v_+)$	Thm. 3.3 ($\alpha = 2$)	Deutsch	Pythag.+AM–GM	$\alpha_c(N)$	2-term rel. err.
2	0.575364	—†	0.316694	0.575364	1.43135588	—
4	1.077993	0.363964	0.575364	0.940007	1.36813866	—
8	1.497525	0.978584	0.780828	1.150728	1.31187054	—
16	1.832581	1.469069	0.940007	1.265045	1.26310681	—
64	2.282344	2.133868	1.150728	1.355286	1.18693295	8.42×10^{-1}
256	2.523993	2.475513	1.265045	1.378497	1.13417409	4.00×10^{-1}
1024	2.647778	2.633962	1.324751	1.384342	1.09814422	2.07×10^{-1}
16384	2.741342	2.740394	1.370730	1.386172	—	—
2^{16}	2.756964	2.756724*	1.378497	1.386264	1.04407354	3.36×10^{-2}
2^{26}	2.772100	2.772100*	1.386050	1.386294	1.01711337	1.59×10^{-3}
2^{40}	2.772585	2.772585*	1.386292	1.386294	1.00722539	1.53×10^{-5}
∞	$4 \log 2$	$4 \log 2$	$2 \log 2$	$2 \log 2$	1	0

†At $N = 2$, Theorem 4.1(a) gives the exact bound $\log(16/9) \approx 0.575364$ directly. At $\alpha = 3$ and $\alpha = 4$, Theorem 3.3 matches $2H_\alpha(v_+(N))$ to within 2.5×10^{-5} and 6×10^{-8} already at $N = 1024$. *Evaluated directly from (28); for $N \geq 2^{26}$ the gap from $2H_2(v_+(N))$ is below 10^{-6}.

6.4 Formal Lean 4.36.0 verification and reproducibility

All core polynomial and denominator-cleared algebraic identities underlying Lemmas 2.1, 3.1, 3.2 and Theorems 2.2, 4.1, 5.1 are formally verified in standalone Lean 4.36.0 (25 total declarations: 15 public theorems, 5 public definitions, 5 private helpers; zero Mathlib, zero `sorry`, zero `grind`, zero custom axioms, compiled with `-DwarningAsError=true` and `lake build`). The 15 certified public theorems cover:

- *Hermite quartic certificate:*
  `hermite_quartic_identity`, `hermite_quartic_nonneg`, `hermite_quartic_exact_nodes`;
- *Rational envelope & XCAP ellipse:*
  `leading_term_deficit_sq`, `tail_height_bounds`, `xcap_ellipse_identity`;
- *Möbius symmetrization & endpoint threshold:*
  `mobius_determinant_identity`, `mobius_determinant_neg`, `endpoint_log_deriv_factorization`;
- *Finite-N Bernstein sharpness:*
  `vplus_collision_identity`, `exact_small_N_collision_values`,
  `landau_pollak_bernstein_identity`, `landau_pollak_bernstein_pos`;
- *Scaling & decoupling:*
  `double_root_cancellation`, `rational_weight_denom_pos`.

All archived artifacts are publicly available in the AIRR repository (https://github.com/arr-research/arr-research.github.io) under CC-BY-4.0 (manuscript) and MIT (code and data):

- `src/lean/HadamardRenyiCore.lean` (28,238 bytes)
  SHA-256: `a2ed18cb306dae795661056857728ffd3c777951f3ac2f182edc5fe43db54969`
- `src/python/verify_hadamard_renyi.py` (30,584 bytes)
  SHA-256: `4392ce2583b5d49cb3df09990c0a65ba277c948da7f036c25fd9266b23fb38a5`
- `data/verification_summary.json` (20,682 bytes)
  SHA-256: `ef77245574dfc473e66c2668e6f144a9181c3f5a11398c0712011beb28affb79`

References

[1] Manuel A. Ballester and Stephanie Wehner. Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases. *Physical Review A*, 75(2):022319, 2007.

[2] Iwo Bialynicki-Birula. Formulation of the uncertainty relations in terms of the Rényi entropies. *Physical Review A*, 74(5):052101, 2006.

[3] David Deutsch. Uncertainty in quantum measurements. *Physical Review Letters*, 50(9):631–633, 1983.

[4] Shmuel Friedland, Vlad Gheorghiu, and Gilad Gour. Universal uncertainty relations. *Physical Review Letters*, 111(23):230401, 2013.

[5] I. D. Ivanovic. An inequality for the sum of entropies of unbiased quantum measurements. *Journal of Physics A: Mathematical and General*, 25(7):L363–L364, 1992.

[6] Ulf Larsen. Superspace formulation of the complementarity principle. *Journal of Physics A: Mathematical and General*, 23(7):1041–1051, 1990.

[7] Hans Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Physical Review Letters*, 60(12):1103–1106, 1988.

[8] Zbigniew Puchała, Łukasz Rudnicki, and Karol Życzkowski. Majorization entropic uncertainty relations. *Journal of Physics A: Mathematical and Theoretical*, 46(27):272002, 2013.

[9] Łukasz Rudnicki, Zbigniew Puchała, and Karol Życzkowski. Strong majorization entropic uncertainty relations. *Physical Review A*, 89(5):052115, 2014.

[10] Wojciech Tadej and Karol Życzkowski. A concise guide to complex Hadamard matrices. *Open Systems & Information Dynamics*, 13(2):133–177, 2006.

[11] Stephanie Wehner and Andreas Winter. Entropic uncertainty relations—a survey. *New Journal of Physics*, 12(2):025009, 2010.

[12] Steeve Zozor, Gustavo Martín Bosyk, and Mariela Portesi. On a generalized entropic uncertainty relation in the case of the qubit. *Journal of Physics A: Mathematical and Theoretical*, 46(46):465301, 2013.