The three-state root-fidelity entropy bound

Dev D. Goyal

29 October 2026; revised 1 November 2026

Abstract

For an ensemble of three finite-dimensional quantum states, its pairwise root fidelities form a positive matrix after weighting by the ensemble probabilities. The entropy of this matrix bounds the ensemble's Holevo quantity from above. The proof applies to arbitrary dimension, mixed and singular states, and zero probabilities. It first proves a three-block trace-norm comparison for entropy deficits. A simultaneous diagonal attainment construction, the scalar three-by-three absolute-value entropy comparison, and joint convexity of relative entropy give this comparison. A weighted-root Gram matrix then gives the ensemble bound. The result is the unrestricted inequality stated as Conjecture 1 by Fannes, de Melo, Roga, and Życzkowski [1]. A Lean formalization proves the theorem for actual positive semidefinite complex matrices of trace one, with spectral entropy and nuclear-norm root fidelity; it builds on credited QICLean foundations. A claimed Lean proof of the same conjecture was public earlier, and another group has reported a solution; the proofs have not been compared, and no priority is claimed.

Priority and subsequent correspondence

Added 30 October 2026. On 29 October 2026, following my correspondence with Dr. Wojciech Roga, one of the authors of the conjecture, he informed me that another group had contacted him several days earlier claiming to have solved the same conjecture using AI and Lean. I had been unaware of this parallel effort, and the novelty searches carried out by my research agents had not found it. I acknowledge this competing claimed solution. I have not seen it; the two proofs have not been compared, and neither mathematical equivalence nor priority has been conclusively established. The proof below and its formalization are unchanged.

Added 1 November 2026. On 31 October 2026, a check of public problem records found that the Omega Institute's public repository records a claimed Lean proof of the same conjecture, for three states of arbitrary dimension including singular states and zero weights, first committed on 19 October 2026 under issue #19184 [10]. This is about nine days before this result was first committed to the author's repository on 29 October 2026. The statements agree; the proofs have not been compared. I do not know whether this record is the competing claim that Dr. Roga described, and I do not assume so. I acknowledge this earlier public record and make no priority claim.

1 The ensemble bound

The Holevo quantity bounds the classical information that a measurement can extract from a quantum-state ensemble. The result below bounds it using three probabilities and three pairwise root fidelities. The matrix in the bound has size three regardless of the dimension of the states.

For a finite-dimensional positive semidefinite matrix T, use

$$\mathrm{S}(T) = -\sum_k \lambda_k(T) \log \lambda_k(T), \qquad 0 \log 0 = 0.$$

This definition also applies to matrices whose trace is not one. All logarithms are natural. Changing to any logarithm base greater than one multiplies every entropy in the result by the same positive constant. Section 6 describes the Lean formalization of the theorem, and Section 7 compares the result with prior work.

Theorem 1 (Three-state root-fidelity entropy inequality)**.** *Let ρ_1, ρ_2, ρ_3 be density matrices on any finite-dimensional complex Hilbert space. Let $p_i \geq 0$ and $\sum_{i=1}^3 p_i = 1$. Define*

$$\sigma = \sum_{i=1}^3 p_i \rho_i, \qquad C_{ij} = \sqrt{p_i p_j}\, \left\| \sqrt{\rho_i} \sqrt{\rho_j} \right\|_1 .$$

Then C is positive semidefinite with trace one, and

$$\mathrm{S}(\sigma) - \sum_{i=1}^3 p_i \mathrm{S}(\rho_i) \leq \mathrm{S}(C). \tag{1}$$

The matrix uses the *unsquared* root fidelity. Under the convention $F(\rho, \tau) = \left\| \sqrt{\rho}\sqrt{\tau} \right\|_1^2$, its entries are $C_{ij} = \sqrt{p_i p_j F(\rho_i, \rho_j)}$. Equation (1) is the unrestricted inequality stated as Conjecture 1, equation (18), in the published Fannes–de Melo–Roga–Życzkowski paper [1]. There is no assumption of commutativity, full rank, strictly positive probabilities, qubit dimension, or compatible polar unitaries.

The bound is attained when the state supports are mutually orthogonal. Then the off-diagonal root fidelities vanish, $C = \mathrm{diag}(p_1, p_2, p_3)$, and both sides of (1) equal $H(p) = -\sum_i p_i \log p_i$. It is also attained when all three states coincide: the Holevo quantity is zero and $C = vv^*$ for $v_i = \sqrt{p_i}$ has entropy zero. These examples do not give a complete equality characterization.

2 Scalar comparison in dimension three

An elementary proof of a known ingredient follows. Its entropy content occurs in the pure-state discussion of [1], using the spectral monotonicity studied by Mitchison and Jozsa [2].

Lemma 2. *If $A \succeq 0$ is a complex 3×3 matrix and $B = (|A_{ij}|)$, then $B \succeq 0$ and $\mathrm{S}(B) \geq \mathrm{S}(A)$. If $A \succ 0$, then $B \succ 0$.*

Proof. Write

$$A = \begin{pmatrix} a & u & v \\ \bar{u} & b & w \\ \bar{v} & \bar{w} & c \end{pmatrix}.$$

The principal minors of orders one and two are unchanged upon replacing entries by their absolute values. For the remaining principal minor,

$$\det B - \det A = 2\big(|uw\bar{v}| - \mathrm{Re}(uw\bar{v})\big) \geq 0.$$

The principal-minor criterion proves the claimed positivity statements.

First assume $A \succ 0$. Let x_1, x_2, x_3 and y_1, y_2, y_3 be the eigenvalues of A and B. Their first elementary symmetric functions agree because the traces agree. Their second elementary

symmetric functions agree because the sums of the principal minors of order two agree. Their third elementary symmetric functions satisfy $y_1y_2y_3 \geq x_1x_2x_3$. Hence, for all $t \geq 0$,

$$\prod_{k=1}^{3}(t+y_k) \geq \prod_{k=1}^{3}(t+x_k).$$

Define

$$Q(t) = \sum_{k=1}^{3}\big((t+y_k)\log(t+y_k) - (t+x_k)\log(t+x_k)\big).$$

The derivative is the logarithm of the ratio of the two products, so $Q'(t) \geq 0$. For each fixed $x > 0$,

$$(t+x)\log(t+x) = t\log t + x\log t + x + O(t^{-1}) \quad (t \longrightarrow \infty).$$

The common number of eigenvalues and their equal sums imply $Q(t) \longrightarrow 0$. Therefore $Q(0) \leq 0$, which is precisely $\mathrm{S}(B) \geq \mathrm{S}(A)$.

For singular A, apply the positive definite case to $A + \varepsilon I_3$. Its entrywise absolute-value matrix is $B + \varepsilon I_3$, since the diagonal entries of A are nonnegative. Continuity of $-x\log x$ at zero and continuity of finite-dimensional eigenvalues give the limit as $\varepsilon \downarrow 0$. □

Write δT for the ordinary diagonal matrix with the same diagonal as T. In particular, $\delta A = \delta B$ in Lemma 2. For positive definite matrices define the unnormalized relative entropy

$$\mathrm{D}(X\|Y) = \operatorname{Tr} X(\log X - \log Y).$$

The trace is real in this setting. Because $\log \delta A$ is diagonal,

$$\mathrm{D}(A\|\delta A) = \mathrm{S}(\delta A) - \mathrm{S}(A). \tag{2}$$

Consequently Lemma 2 gives

$$\mathrm{D}(B\|\delta B) \leq \mathrm{D}(A\|\delta A) \qquad (A \succ 0). \tag{3}$$

3 Simultaneous diagonal attainment

The following construction is the one in Li and Zhang's proof of their positivity theorem [3]. Neither that construction nor the positivity theorem is claimed as new here; Drury's earlier result is credited in their paper.

Lemma 3 (Li–Zhang construction)**.** *Let $G = (G_{ij})_{i,j=1}^{3} \succeq 0$ have square blocks of common size d. There are unitaries U_1, U_2, U_3 such that, with $U = U_1 \oplus U_2 \oplus U_3$ and $G' = UGU^*$, the scalar matrices*

$$A_r = \big((G'_{ij})_{rr}\big)_{i,j=1}^{3}, \qquad B_r = (|(A_r)_{ij}|), \qquad 1 \leq r \leq d,$$

satisfy

$$C = \sum_{r=1}^{d} B_r, \qquad C_{ij} = \|G_{ij}\|_1 . \tag{4}$$

Every A_r and B_r is positive semidefinite. If $G \succ 0$, they are positive definite.

Proof. Successive block-unitary conjugations make blocks 12 and 23 positive semidefinite: use their right polar decompositions, first changing block coordinate 2 and then block coordinate 3. The second change leaves block 12 fixed. Write the resulting block 13 as PW with $P \succeq 0$

and W unitary. Polar factors can be extended to unitaries even when the blocks are singular. Diagonalize W by a common internal unitary basis change in all three block coordinates. Blocks 12 and 23 remain positive, while block 13 becomes $\widetilde{P}\,\mathrm{diag}(z_r)$ with $|z_r| = 1$ and $\widetilde{P} \succeq 0$.

Thus, for each block, the sum of the absolute values of its diagonal entries equals its trace norm. For block 13 this is $\sum_r |\widetilde{P}_{rr} z_r| = \operatorname{Tr} \widetilde{P}$; the other blocks and their adjoints have the same property. Trace norms are unchanged by the unitary transformations, giving (4). Each A_r is a principal submatrix of G'. Apply Lemma 2 to finish. □

In particular, $C \succeq 0$ and $\operatorname{Tr} C = \operatorname{Tr} G$. The assertion that C is positive is established prior mathematics. The next section supplies the entropy comparison used to reach the original target.

4 The block entropy inequality

Let $\Delta G = G_{11} \oplus G_{22} \oplus G_{33}$ be pinching by the three outer block coordinates.

Theorem 4. *For every $G \succeq 0$ with three square blocks of common size $d \geq 1$, set $C_{ij} = \|G_{ij}\|_1$. Then*

$$\mathrm{S}(\delta C) - \mathrm{S}(C) \leq \mathrm{S}(\Delta G) - \mathrm{S}(G). \tag{5}$$

Proof. Positive definite case. Assume $G \succ 0$. Obtain U, G', A_r, B_r from Lemma 3. Let Φ pinch the internal coordinate r, retaining an entry between (i, r) and (j, s) exactly when $r = s$. This is a finite unitary average. Explicitly, with $\omega = \exp(2\pi \mathrm{i}/d)$, let $Z_k e_{i,r} = \omega^{kr} e_{i,r}$ for $0 \leq k < d$. Then

$$\Phi(T) = \frac{1}{d} \sum_{k=0}^{d-1} Z_k T Z_k^*.$$

The identity follows by summing the geometric progression $\sum_k \omega^{k(r-s)}$.

The proof uses joint convexity and unitary invariance of quantum relative entropy. These are established results, and their proofs are included in the checked prior-foundation dependency bundle. They imply

$$\mathrm{D}(G' \| \Delta G') \geq \mathrm{D}(\Phi(G') \| \Phi(\Delta G')). \tag{6}$$

After reordering coordinates, the two arguments on the right are $\bigoplus_r A_r$ and $\bigoplus_r \delta A_r$. Relative entropy is additive over direct sums, since matrix logarithms act separately on the summands. Therefore the right-hand side is $\sum_r \mathrm{D}(A_r \| \delta A_r)$.

Equation (3) yields

$$\sum_r \mathrm{D}(A_r \| \delta A_r) \geq \sum_r \mathrm{D}(B_r \| \delta B_r).$$

Joint convexity also yields the homogeneous finite-sum inequality

$$\mathrm{D}\left(\sum_r X_r \middle\| \sum_r Y_r \right) \leq \sum_r \mathrm{D}(X_r \| Y_r). \tag{7}$$

Indeed, apply joint convexity to the uniform averages and multiply by d, using $\mathrm{D}(tX \| tY) = t\mathrm{D}(X \| Y)$ for $t > 0$. Applying (7) to $X_r = B_r$, $Y_r = \delta B_r$, and using (4), gives the chain

$$\begin{aligned} \mathrm{D}(G \| \Delta G) &= \mathrm{D}(G' \| \Delta G') \\ &\geq \sum_r \mathrm{D}(A_r \| \delta A_r) \\ &\geq \sum_r \mathrm{D}(B_r \| \delta B_r) \\ &\geq \mathrm{D}(C \| \delta C). \end{aligned} \tag{8}$$

The first equality uses the fact that block-diagonal U satisfies $\Delta(UGU^*) = U(\Delta G)U^*$.

Finally, $\log \Delta G$ is block diagonal, so

$$\operatorname{Tr}(G \log \Delta G) = \operatorname{Tr}(\Delta G \log \Delta G).$$

It follows that $\mathrm{D}(G\|\Delta G) = \mathrm{S}(\Delta G) - \mathrm{S}(G)$. Use (2) for C to turn (8) into (5).

Singular case. For $\varepsilon > 0$ apply the proved result to $G_\varepsilon = G + \varepsilon I_{3d}$. The off-diagonal blocks are unchanged. For each diagonal block, positivity gives

$$\|G_{ii} + \varepsilon I_d\|_1 = \operatorname{Tr} G_{ii} + d\varepsilon.$$

Its norm-compression matrix is consequently $C_\varepsilon = C + d\varepsilon I_3$. Also $\Delta G_\varepsilon = \Delta G + \varepsilon I_{3d}$ and $\delta C_\varepsilon = \delta C + d\varepsilon I_3$. All four entropy terms converge as $\varepsilon \downarrow 0$ by the continuity of finite-dimensional entropy. This proves the assertion with no rank or nonzero-block restriction. □

5 Reduction to a three-state ensemble

Proof of Theorem 1. Form the rectangular matrix

$$X = [\sqrt{p_1}\sqrt{\rho_1} \quad \sqrt{p_2}\sqrt{\rho_2} \quad \sqrt{p_3}\sqrt{\rho_3}], \qquad G = X^*X.$$

Then $XX^* = \sigma$. The nonzero eigenvalues of X^*X and XX^* coincide, with multiplicity. Since zero eigenvalues contribute zero to entropy, $\mathrm{S}(G) = \mathrm{S}(\sigma)$. Furthermore,

$$G_{ij} = \sqrt{p_i p_j}\sqrt{\rho_i}\sqrt{\rho_j}, \qquad G_{ii} = p_i\rho_i.$$

Thus its norm-compression matrix is exactly C from the theorem. Lemma 3 proves $C \succeq 0$, and $C_{ii} = p_i$ proves $\operatorname{Tr} C = 1$.

Let $H(p) = -\sum_i p_i \log p_i$. Direct-sum additivity and the scaling identity $\mathrm{S}(p_i\rho_i) = p_i\mathrm{S}(\rho_i) - p_i \log p_i$ give

$$\mathrm{S}(\Delta G) = H(p) + \sum_i p_i \mathrm{S}(\rho_i), \qquad \mathrm{S}(\delta C) = H(p).$$

The scaling identity is interpreted continuously at $p_i = 0$. Substitute these identities in Theorem 4 and cancel $H(p)$:

$$H(p) - \mathrm{S}(C) \le H(p) + \sum_i p_i \mathrm{S}(\rho_i) - \mathrm{S}(\sigma).$$

Rearrangement gives (1). □

The block formulation is a useful structural form of the same result. It is not counted here as a second independent research breakthrough. The argument makes essential use of the three-by-three absolute-value lemma; it does not establish an analogous statement for an arbitrary number of states.

6 Formalization and reproduction

The accompanying Lean declaration is `Fidelity.holevo_le_entropy_rootFidelityMatrix`. Its hypotheses are exactly nonnegative real weights summing to one and three positive semidefinite complex matrices of trace one on a common finite index type. The formal proof derives nonemptiness of this type from trace one. It imposes no commutativity, rank, dimension, or polar-compatibility restriction.

Entropy is the spectral sum of $-x \log x$. The definition `Fidelity.nuclear A` is the real part of $\operatorname{Tr} \sqrt{A^* A}$; its equality with the QIC trace norm on finite ordinal indices is proved. The formal scalar comparison uses an exponential witness and the Gibbs variational inequality for positive definite three-by-three matrices. It supplies the positive definite part of Lemma 2. The formal block proof handles singular matrices by regularization. It does not formalize the derivative calculation printed here. The remaining formal steps follow the block argument and Gram reduction.

The dependency bundle contains 42 prior QICLean source modules [9] from commit

`acda92aa70e69b37507e422bceb5414036859fe6`.

The bundle retains their proofs, copyright notices, and Apache 2.0 license. These foundations are credited prior work. The local proof combines 25 modules. The pinned compiler is Lean 4.35.0-rc3, commit

`470d5ce1400764999581fd26d5d72b00d990b0f4`.

Mathlib is pinned to

`c55e6e786f49471c72fbddbec5415808896aec1e`.

The reproduction files retain all transitive package revision pins.

From the proof directory, run

```
python3 fetch_mathlib_cache.py
lake build FullCandidate
lake lean Audit.lean
```

The audit prints the fully quantified theorem and its transitive axioms. The accepted logical foundations are `propext`, `Classical.choice`, and `Quot.sound`.

The companion sources, dependency pins, verifier, and licenses are distributed in the Math and Theory collection: https://github.com/dvgyl/math-and-theory.

7 Relation to prior work

The inequality is Conjecture 1, equation (18), of Fannes, de Melo, Roga, and Życzkowski [1]. Their paper gives the pure-state result and weaker bounds obtained by reducing the off-diagonal fidelities. Zhang, Wu, and Fei [4] prove the target under a compatibility condition on three polar unitaries. The present statement has no such condition.

The scalar entropy comparison is known from the pure-state analysis in [1] and the spectral monotonicity in [2]. The simultaneous diagonal construction and positivity theorem are due to Li and Zhang [3], who credit Drury's earlier positivity result. Joint convexity, entropy continuity, and the Gram-spectrum identity are also prior results. The entropy comparison for the block trace-norm matrix is the step that connects these ingredients to the full ensemble inequality. It is a structural form of the same result, rather than a second independent contribution.

Related polar reduction, dephasing, and convexity methods appear in Tang and coauthors [8] for a different triangular-block entropy inequality. Theorem 4.2 and Appendix A of that source do not state the three-block trace-norm comparison proved here. Priority is not certified by the

available literature review; see also the priority note at the beginning of this paper. In particular, the complete texts of [5, 6, 7] were not available for comparison. An accessible-information bound alone does not imply a bound on the Holevo quantity. These access limits leave possible overlap unresolved; they do not change the theorem proved here.

8 Research process and AI disclosure

This work is fully autonomous agentic AI research. AI systems developed the mathematical argument, formal proofs, and earlier versions of this manuscript. Opus 5.5 by Anthropic used with Claude Code revised the presentation of the manuscript on 1 November 2026: it rewrote the front matter and abstract, added the dated note on the Omega Institute record and consolidated this disclosure. The revision does not change the mathematics. Dev D. Goyal is responsible for publication. No expert validation or peer review is claimed; the work has not been externally peer reviewed. The formal scope is stated in Section 6; credited prior work and the limits of the literature comparison are stated in Section 7.

References

[1] M. Fannes, F. de Melo, W. Roga, and K. Życzkowski, *Matrices of fidelities for ensembles of quantum states and the Holevo quantity*, Quantum Information and Computation **12** (2012), 472–489. doi:10.26421/QIC12.5-6-8; arXiv:1104.2271.

[2] G. Mitchison and R. Jozsa, *Towards a geometrical interpretation of quantum information compression*, Physical Review A **69** (2004), 032304. doi:10.1103/PhysRevA.69.032304; arXiv:quant-ph/0309177.

[3] C.-K. Li and F. Zhang, *Positivity of partitioned Hermitian matrices with unitarily invariant norms*, Positivity **19** (2015), 439–444. arXiv:1407.0331v3.

[4] L. Zhang, J. Wu, and S.-M. Fei, *Universal upper bound for the Holevo information induced by a quantum operation*, 2012 preprint, Theorem 3.4. arXiv:1110.5979v3.

[5] L. Klotz and C. Mädler, *An Addendum to a Paper by Li and Zhang*, in Operator Theory: Advances and Applications **263** (2018), 387–392. doi:10.1007/978-3-319-68849-7_15.

[6] Y. Sun, S. Luo, and X. Lei, *Gram Matrices of Mixed-State Ensembles*, International Journal of Theoretical Physics **60** (2021), 3211–3224. doi:10.1007/s10773-021-04908-8.

[7] W. Gao and S. Yu, *Alternative upper bound for accessible information and wave-particle duality*, Physical Review A **114** (2026), 012466. doi:10.1103/ks9d-73dp.

[8] Z. Tang, C. Zhu, G. Bai, and X. Wang, *Classical Capacity and Entanglement Cost of the Amplitude Damping Channel*, 2026 preprint. arXiv:2609.28592v1.

[9] QICLean contributors, *QICLean*, source repository. Pinned source tree. The source retains its Apache 2.0 license and individual copyright notices.

[10] The Omega Institute, problem dossier on the Fannes–de Melo–Roga–Życzkowski root-fidelity Holevo bound (issue #19184), public repository `the-omega-institute/trureturing`; claimed Lean proof first committed 19 October 2026. `https://github.com/the-omega-institute/trureturing/blob/81743e5d0ee1b300b9b36a2c3dbe15d05d39c993/Problems/fannes-demelo-roga-zyczkowski-2012-root-fidelity-holevo-bound.md`.