A sum-of-squares proof of the four-qubit Higuchi–Sudbery entropy bound

Dev D. Goyal

27 October 2026; revised 1 November 2026

Abstract

For a pure state of four qubits, the Higuchi–Sudbery problem [1] asks for the largest average von Neumann entropy across the three partitions into pairs. The proof shows that this average is at most $\log 2 + \frac{1}{2}\log 3$, with natural logarithms. The Higuchi–Sudbery state attains the bound. The proof gives an exact polynomial identity that bounds the sum of the third elementary symmetric functions of the three marginal spectra by 5/36. Its right side is a sum of 272 squared mixed cubics with positive integer weights. The identity holds for all sixteen complex amplitudes. A purity lower bound and a cubic majorant for $-x\log x$ then give the entropy inequality. The argument places no restriction on the one-qubit marginals. A companion Lean formalization includes the polynomial identity, the actual reduced-matrix eigenvalues, and an explicit state that attains the bound. The Omega Institute publicly committed a claimed Lean proof of the same bound, with an algebraically equivalent certificate, on 7 October 2026 [4]; no originality or priority claim is made for the result.

Priority and subsequent correspondence

Added 30 October 2026. On 30 October 2026, following my correspondence with Dr. Jef Pauwels, he informed me that the Omega Institute had recently announced a similar result. I was previously unaware of this work, and the novelty searches carried out by my research agents had not found it. The Omega Institute registered the problem on 5 October 2026 and publicly committed a claimed Lean proof on 7 October 2026 [4], before this manuscript was first published on 27 October 2026. A subsequent comparison showed that the two 272-term sum-of-squares certificates are algebraically equivalent. I acknowledge this earlier public work and the substantial overlap, and I make no originality or priority claim for the result. I have not independently checked the Omega Institute's Lean proof. The proof below and its formalization are unchanged.

1 The problem and the result

For a normalized pure state of four distinguishable qubits, let ρ_{AB}, ρ_{AC}, and ρ_{AD} denote the reduced density matrices on the indicated pairs. The notation uses natural logarithms, with

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i, \qquad 0\log 0 = 0,$$

where λ_i are the eigenvalues of ρ. The quantity to be maximized is

$$\mathcal{S}(\psi) = \frac{1}{3}\big(S(\rho_{AB}) + S(\rho_{AC}) + S(\rho_{AD})\big). \tag{1}$$

Higuchi and Sudbery introduced the candidate maximizing state in 2000 and gave evidence for global maximality [1]. Brierley and Higuchi proved that it is a local maximum [2]. Gour and Wallach proved the corresponding global entropy statement on their family $\mathcal{A}$ [3, Theorem 10(a)]; by their Theorem 5, that family, up to local unitaries, consists of states whose one-qubit marginals are all maximally mixed. The hypothesis $\psi \in \mathcal{A}$ is material. The unrestricted von Neumann entropy problem is not the statement of that theorem. Recent primary sources continue to distinguish the restricted theorem from the conjectured unrestricted optimum: see Pauwels and Gühne [5, Section IV.2 and Appendix A] and Collins [6, Section 3.2].

Theorem 1.1 (Balanced four-qubit entropy bound)**.** *For every normalized* $\psi \in (\mathbb{C}^2)^{\otimes 4}$*,*

$$\mathcal{S}(\psi) \le \log 2 + \frac{1}{2}\log 3. \tag{2}$$

Equality is attained by the Higuchi–Sudbery state in Section 6.

In base-two units the value is $1+\frac{1}{2}\log_2 3$, approximately 1.79248 bits. The proof uses the unrestricted degree-six inequality in Theorem 3.1, together with its explicit certificate. The purity lower bound is known. A direct algebraic proof makes its normalization and use explicit. The maximizing state, its marginal spectra, and the restricted result are due to prior work, and the unrestricted bound with an equivalent certificate was claimed earlier by the Omega Institute (see the priority note above). The Lean formalization described in Section 7 checks the polynomial identity, the bound for the eigenvalues of the actual reduced matrices, and the attaining state.

2 Coordinates and reduced matrices

Write the unnormalized state as

$$z = \sum_{a,b,c,d\in\{0,1\}} z_{abcd}|abcd\rangle, \qquad n = \|z\|^2 = \sum_{a,b,c,d} |z_{abcd}|^2.$$

For single-index formulas, z_{abcd} means $z_{8a+4b+2c+d}$. Define three flattenings, with rows and columns ordered lexicographically, by

$$(M_0)_{ab,cd} = z_{abcd}, \qquad (M_1)_{ac,bd} = z_{abcd}, \qquad (M_2)_{ad,bc} = z_{abcd}. \tag{3}$$

Let $\rho_j = M_j M_j^*$. These matrices are positive semidefinite and have trace n. When $n = 1$, they are the three density matrices in (1). For each of these reduced matrices A, with eigenvalues $\lambda_1, \dots, \lambda_4$, put

$$e_3(A) = \sum_{1\le i<j<k\le 4} \lambda_i\lambda_j\lambda_k.$$

Equivalently, $e_3(A)$ is the sum of the four principal minors of order three.

Lemma 2.1 (Cofactor expression)**.** *For every state vector* z *and each flattening* $M = M_j$ *in* (3)*,*

$$e_3(MM^*) = \sum_{\substack{I,J\subseteq\{0,1,2,3\}\\ |I|=|J|=3}} |\det M[I,J]|^2. \tag{4}$$

Proof. Sum the principal minors $\det((MM^*)[I,I])$ over the four three-element row sets I. For a fixed I, Cauchy–Binet expands this determinant as $\sum_{|J|=3} \det M[I,J] \det M^*[J,I]$. The second factor is the complex conjugate of the first, giving (4). □

3 An exact degree-six certificate

Theorem 3.1 (Third elementary symmetric function bound)**.** *For every $z \in (\mathbb{C}^2)^{\otimes 4}$, without a normalization assumption,*

$$\sum_{j=0}^{2} e_3(M_j M_j^*) \le \frac{5}{36}\|z\|^6. \tag{5}$$

The constant is sharp.

The proof consists of the following finite identity. The indexing and coefficients below specify the identity exactly.

3.1 Local integer rows

Each row in Table 1 is an integer-valued function on $\{0,1\}^3$. A triple such as 001 denotes its indicator function; all omitted values are zero.

Row	Nonzero values, expressed as indicators
S_0	000
S_1	$001 + 010 + 100$
S_2	$011 + 101 + 110$
S_3	111
T_0	$2 \cdot 001 - 010 - 100$
T_1	$011 + 101 - 2 \cdot 110$
A_0	$010 - 100$
A_1	$011 - 101$

Table 1: Integer rows defining the squared cubics.

Given a four-tuple of rows $r = (r_0, r_1, r_2, r_3)$, define

$$C_r(z) = \sum_{a,b,c \in \{0,1\}^4} \left(\prod_{j=0}^{3} r_j(a_j, b_j, c_j) \right) (-1)^{|c|} z_a z_b \overline{z_{\bar{c}}}. \tag{6}$$

Here $|c| = c_0 + c_1 + c_2 + c_3$, and $\bar{c}$ is the bitwise complement. Thus C_r has degree two in z and degree one in $\bar{z}$. The sign and complement in (6) are exactly those of $J^{\otimes 4}\bar{z}$, where $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

Fix a site $s \in \{0,1,2,3\}$, an index $r \in \{0,1,2,3\}$, and a bit $\epsilon_j \in \{0,1\}$ for each $j \neq s$. Define $P_{s,r,\epsilon}$ by taking row S_r at site s and row T_{ϵ_j} at each other site in (6). Define $Q_{s,r,\epsilon}$ as the sum of the three cubics obtained from this choice by replacing exactly two of its three T rows with the corresponding A rows. Finally, for $\epsilon \in \{0,1\}^4$, let W_ϵ be (6) with row A_{ϵ_j} at every site. Put

$$w_0 = w_3 = 3, \qquad w_1 = w_2 = 1. \tag{7}$$

The reconstruction recipe first forms the polynomial expression

$$R_{\text{recipe}}(z) = \sum_{s=0}^{3}\sum_{r=0}^{3} \sum_{\epsilon \in \{0,1\}^{\{0,1,2,3\}\setminus\{s\}}} w_r \left(|5P_{s,r,\epsilon} + 11 Q_{s,r,\epsilon}|^2 + 124 |Q_{s,r,\epsilon}|^2 \right) + 640 \sum_{\epsilon \in \{0,1\}^4} |W_\epsilon|^2.$$

The generator divides by 16, expands each cubic, removes its integer common factor, and absorbs the square of that factor into its weight. The resulting finite list is named `sosData` in `HS/CertificateData.lean`, which assembles the explicit coefficient lists in `HS/CertificateParts/L00.lean` through `L16.lean`. It has 272 entries (v_ℓ, T_ℓ), where $v_\ell \in \{1, 3, 31, 93, 160\}$ and T_ℓ is a list of integer-index tuples (a, i, j, k). Define directly from these delivered lists

$$F_\ell(z) = \sum_{(a,i,j,k)\in T_\ell} a z_i z_j \overline{z_k}.$$

The row recipe permits an independent reconstruction of the data. The formal theorem takes the explicit coefficient lists as its definitions and checks the resulting identity directly. It does not verify the Python generator or rely on a formal proof of the recipe-to-table conversion.

Proposition 3.2 (Explicit-table polynomial identity)**.** *For all $z \in \mathbb{C}^{16}$, the delivered coefficient lists satisfy*

$$400n^3 - 2880 \sum_{j=0}^{2} \sum_{|I|=|J|=3} |\det M_j[I, J]|^2 = \sum_{\ell=1}^{272} v_\ell |F_\ell(z)|^2. \tag{8}$$

Proof. This is an identity of polynomials of bidegree $(3, 3)$ in the amplitudes and their conjugates. It can be checked by treating the sixteen amplitudes and sixteen formal conjugates as independent commuting variables. For precision, use the monomial basis

$$z_{i_1} z_{i_2} z_{i_3} \bar{z}_{j_1} \bar{z}_{j_2} \bar{z}_{j_3}, \qquad i_1 \le i_2 \le i_3, \quad j_1 \le j_2 \le j_3.$$

Expand n^3, expand each determinant by its six permutation terms, and expand each cubic from its explicit list T_ℓ. Multiplication and collection of coefficients give identical integer coefficients on the two sides of (8). Each side has exactly 1,968 nonzero collected coefficients; the difference has none.

The accompanying files supply all 272 cubics and all 48 determinants explicitly as coefficient lists. A separately implemented checker forms $M_j M_j^*$ and expands its principal order-three minors directly; it obtains the same polynomial before comparison with the squared cubics. Thus the identity is specified by finite formulas here and is independently reproducible without the optimization procedure used to find it. The companion Lean files check the polynomial equalities in the proof kernel. Section 7 describes the pinned environment and verification records.

The Lean development specifies the integer coefficient lists explicitly. Its kernel checks the resulting polynomial identity and its nonnegativity consequence; it does not assume that the Python generator, the discovery solver, or a representation-theoretic decomposition is correct. □

Proof of Theorem 3.1. Every summand on the right of (8) is nonnegative. Divide by 2880 and use $400/2880 = 5/36$, followed by Lemma 2.1. Sharpness follows from the explicit marginal spectrum in Section 6: its e_3 value is $5/108$ at each of the three cuts. □

3.2 Equivalent moment form

For a normalized state, set

$$q_k = \frac{1}{3} \sum_{j=0}^{2} \operatorname{Tr}(\rho_j^k), \qquad k = 2, 3. \tag{9}$$

Newton's identity, with $\operatorname{Tr} \rho_j = 1$, reads

$$6e_3(\rho_j) = 1 - 3 \operatorname{Tr}(\rho_j^2) + 2 \operatorname{Tr}(\rho_j^3). \tag{10}$$

Summing and applying (5) yields

$$q_3 \le \frac{3}{2} q_2 - \frac{13}{36}. \tag{11}$$

For an unnormalized vector the equivalent inequality is

$$12 \sum_j \mathrm{Tr}(\rho_j^3) + 13 n^3 \le 18 n \sum_j \mathrm{Tr}(\rho_j^2).$$

4 The purity lower bound

The argument also uses $q_2 \ge 1/3$, which is a known four-qubit purity bound. Its relation with the four-tangle appears explicitly in [3, Theorem 6]. The following coordinate identity provides a separate finite-algebra proof and fixes all normalization factors.

For each site s, let $z_0^{(s)}, z_1^{(s)} \in \mathbb{C}^8$ be the zero and one slices of the amplitude tensor, in the same order of the remaining bits. Define

$$d_s = \|z_0^{(s)}\|^2 - \|z_1^{(s)}\|^2, \qquad c_s = \sum_u (z_0^{(s)})_u \overline{(z_1^{(s)})_u},$$

and

$$H = z_0 z_{15} - z_1 z_{14} - z_2 z_{13} + z_3 z_{12} - z_4 z_{11} + z_5 z_{10} + z_6 z_9 - z_7 z_8. \tag{12}$$

Lemma 4.1 (Quartic purity identity)**.** *For every unnormalized four-qubit vector,*

$$\sum_{j=0}^{2} \mathrm{Tr}(\rho_j^2) - n^2 = \frac{1}{2} \sum_{s=0}^{3} (d_s^2 + 4|c_s|^2) + 2|H|^2. \tag{13}$$

Consequently $q_2 \ge 1/3$ when $n = 1$.

Proof. Substitute the flattenings (3) in the left side and the slice definitions and (12) in the right side. Expansion gives the same quartic polynomial. The identity is also valid with independent formal conjugate variables, and this is the version used for the direct ring calculation in the companion formalization. Every term on the right of (13) is nonnegative. Therefore the three purities sum to at least n^2; divide by three and set $n = 1$. □

5 An entropy bound from two moments

The remaining argument is a scalar interpolation calculation. The proof needs only the one-sided fourth-derivative statement below. Its hypotheses and conclusion agree with the corresponding Lean lemma.

Lemma 5.1 (A fourfold Rolle argument)**.** *Let $f_0, f_1, f_2, f_3, f_4 : (0, \infty) \to \mathbb{R}$ satisfy $f_j'(t) = f_{j+1}(t)$ for every $t > 0$ and $j = 0, 1, 2, 3$, and suppose $f_4(t) > 0$ for every $t > 0$. If $0 < a < b$ and*

$$f_0(a) = f_1(a) = f_0(b) = f_1(b) = 0,$$

then $f_0(x) \ge 0$ for every $x > 0$.

Proof. The conclusion at a, b is immediate. Suppose, for a contradiction, that $x > 0$ is distinct from a, b and $f_0(x) < 0$. Put

$$q(t) = (t-a)^2(t-b)^2, \qquad k = \frac{f_0(x)}{q(x)} < 0, \qquad g_j(t) = f_j(t) - kq^{(j)}(t) \quad (0 \le j \le 4).$$

Then $g_j' = g_{j+1}$ for $j = 0, 1, 2, 3$; moreover, g_0 vanishes at a, b, x and g_1 vanishes at a, b. The argument shows that g_1 has four *distinct* positive zeros. If $x < a$, Rolle's theorem applied on $[x, a]$ and $[a, b]$ supplies zeros $u \in (x, a)$ and $v \in (a, b)$; the four zeros are u, a, v, b. If $a < x < b$, the intervals $[a, x]$ and $[x, b]$ instead give four zeros a, u, v, b. If $b < x$, the intervals $[a, b]$ and $[b, x]$ give four zeros a, u, b, v.

Three further rounds of Rolle's theorem, first between consecutive zeros of g_1, then between the resulting zeros of g_2, and finally between the resulting zeros of g_3, produce a positive zero of g_4. All intervals used lie inside $(0, \infty)$; differentiability supplies the continuity needed by Rolle's theorem on each closed interval. This is impossible because

$$g_4(t) = f_4(t) - 24k > 0 \qquad (t > 0).$$

□

Let $L = \log 3$ and define

$$\begin{aligned} \alpha &= \frac{1}{2} - \frac{3}{8}L, & \beta &= \log 2 + 6L - \frac{11}{2}, \\ \gamma &= 18 - \frac{39}{2}L, & \delta &= 18(L-1), \end{aligned} \tag{14}$$

with $p(x) = \alpha + \beta x + \gamma x^2 + \delta x^3$.

The required elementary logarithmic bounds are

$$1 < \log 3 < \frac{6}{5}. \tag{15}$$

To check them using exactly the rational comparisons in the Lean proof, use $1 - t^{-1} \le \log t \le t - 1$ for $t > 0$ together with

$$\left(\frac{12}{11}\right)^{12} < 3 < \left(\frac{23}{20}\right)^{8}.$$

The first comparison and monotonicity of the logarithm give

$$1 = 12\left(1 - \frac{11}{12}\right) \le 12 \log \frac{12}{11} < \log 3.$$

The second gives

$$\log 3 < 8 \log \frac{23}{20} \le 8\left(\frac{23}{20} - 1\right) = \frac{6}{5}.$$

In particular,

$$\alpha > 0, \qquad \delta > 0, \qquad \gamma + \frac{3}{2}\delta = \frac{15}{2}\log 3 - 9 < 0. \tag{16}$$

Lemma 5.2 (Scalar entropy majorant)**.** *For all $x \ge 0$, with $0 \log 0 = 0$,*

$$-x \log x \le p(x). \tag{17}$$

The two sides agree at $x = 1/6$ and $x = 1/2$.

Proof. For $x > 0$, take $f_0(x) = p(x) + x \log x$, with derivative chain

$$\begin{aligned} f_1(x) &= \beta + 2\gamma x + 3\delta x^2 + \log x + 1, \\ f_2(x) &= 2\gamma + 6\delta x + \frac{1}{x}, \\ f_3(x) &= 6\delta - \frac{1}{x^2}, \\ f_4(x) &= \frac{2}{x^3} > 0. \end{aligned}$$

Substitution of (14), together with $\log(1/6) = -\log 2 - \log 3$ and $\log(1/2) = -\log 2$, gives

$$f_0(1/6) = f_1(1/6) = f_0(1/2) = f_1(1/2) = 0.$$

Lemma 5.1 therefore gives $f_0(x) \geq 0$ for all $x > 0$, which is (17). The same substitutions prove equality at the two specified points. At $x = 0$ the left-hand side is zero and $p(0) = \alpha > 0$ by (15), so the inequality holds there as well. □

Proof of the upper bound in Theorem 1.1. Apply (17) to each of the four nonnegative eigenvalues of each density matrix. Their sum is one, so

$$S(\rho_j) \leq 4\alpha + \beta + \gamma \operatorname{Tr}(\rho_j^2) + \delta \operatorname{Tr}(\rho_j^3).$$

Averaging and using (11), with $\delta > 0$, yields

$$\mathcal{S}(\psi) \leq 4\alpha + \beta + (\gamma + \tfrac{3}{2}\delta) q_2 - \tfrac{13}{36}\delta.$$

The coefficient of q_2 is negative by (16); hence Lemma 4.1 gives

$$\begin{aligned} \mathcal{S}(\psi) &\leq 4\alpha + \beta + \tfrac{1}{3}(\gamma + \tfrac{3}{2}\delta) - \tfrac{13}{36}\delta \\ &= \log 2 + \tfrac{1}{2}\log 3, \end{aligned}$$

where the last equality is substitution of (14). □

6 Normalization and attainment

Let $\omega = (-1 + i\sqrt{3})/2$ and set

$$|\mathrm{HS}\rangle = \frac{1}{\sqrt{6}} \left[|0011\rangle + |1100\rangle + \omega(|0101\rangle + |1010\rangle) + \omega^2(|0110\rangle + |1001\rangle) \right]. \tag{18}$$

The six basis vectors are distinct and the six coefficients have modulus $1/\sqrt{6}$, so the state is normalized. For exact real arithmetic the same vector has two amplitudes equal to 2, two equal to $-1 + i\sqrt{3}$, and two equal to $-1 - i\sqrt{3}$, all divided by $\sqrt{24}$. This is the representation used in the formal witness.

For the cut $AB|CD$, the unnormalized flattening of the bracketed expression in (18) is

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & \omega & \omega^2 & 0 \\ 0 & \omega^2 & \omega & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The other two cuts replace the isolated unit amplitudes and the middle pair by the corresponding phases. In all three products with the conjugate transpose, using $\omega + \omega^2 = -1$ gives

$$\rho_0 = \rho_1 = \rho_2 = \frac{1}{6}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{19}$$

The middle block has eigenvectors $(1, 1)$ and $(1, -1)$ with eigenvalues 1 and 3, respectively. Thus the eigenvalues of each density matrix are $1/2, 1/6, 1/6, 1/6$, and

$$S(\rho_j) = -\tfrac{1}{2}\log(\tfrac{1}{2}) - \tfrac{1}{2}\log(\tfrac{1}{6}) = \log 2 + \tfrac{1}{2}\log 3.$$

This proves attainment in Theorem 1.1. The same spectrum gives $e_3(\rho_j) = 5/108$, proving sharpness in Theorem 3.1. No classification of all maximizing vectors is asserted here.

7 Formalization and scope

The companion formalization uses Lean 4.35.0 and a pinned mathlib revision. Its final greatest-value statements include both the upper bounds and their attainment. They use the eigenvalues of the actual reduced matrices. The reproduction package gives the exact source versions, build commands, and axiom checks.

The coefficient data can also be checked with integer arithmetic. One program reconstructs the cubics from the row formulas and expands the forty-eight determinants. A separate checker directly expands the principal minors of the reduced density matrices. Both compare the collected coefficients. This check does not require a numerical optimization solver.

The result applies to pure states of four distinguishable two-dimensional systems. It uses the equally weighted average of the three balanced cuts. Other local dimensions, mixed states, other entanglement measures, and different cut weights require separate results. The proof gives an attaining state but does not classify all maximizers.

8 Research process and AI disclosure

This work is fully autonomous agentic research. The initial research and proofs were generated autonomously by GPT 6 with Pro Reasoning in ChatGPT. GPT 6 Astra in Codex autonomously produced the formalizations and corrections. The author checked the proofs to the best of their mathematical abilities; this check is not expert validation or peer review. 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 and consolidated this disclosure. The revision does not change the mathematics. Dev D. Goyal is responsible for publication. The work has not been externally peer reviewed. The formal scope and the limits of the result are stated in Section 7, and the earlier public work in the priority note.

References

[1] A. Higuchi and A. Sudbery, *How entangled can two couples get?*, Physics Letters A **273** (2000), 213–217. doi:10.1016/S0375-9601(00)00480-1. https://arxiv.org/abs/quant-ph/0005013.

[2] S. Brierley and A. Higuchi, *On maximal entanglement between two pairs in four-qubit pure states*, Journal of Physics A: Mathematical and Theoretical **40** (2007), 8455–8465. doi:10.1088/1751-8113/40/29/018. https://arxiv.org/abs/0704.2961.

[3] G. Gour and N. R. Wallach, *All maximally entangled four-qubit states*, Journal of Mathematical Physics **51** (2010), 112201. doi:10.1063/1.3511477. https://arxiv.org/abs/1006.0036.

[4] The Omega Institute, public problem record and claimed Lean proof for the four-qubit Higuchi–Sudbery bound (problem registered 5 October 2026; proof committed 7 October 2026). https://github.com/the-omega-institute/trureturing/issues/13454.

[5] J. Pauwels and O. Gühne, *The Entanglement Content of Quantum Measurement Bases*, arXiv preprint (2026). https://arxiv.org/abs/2608.21185.

[6] B. Collins, *The Failure of Simultaneous Quantum Typicality*, arXiv preprint (2026). https://arxiv.org/abs/2609.25726.