# Sharp Non-Commuting Operator Constants, Quantitative One-Shot Converse Sharpenings, and Constructive Lean 4.35.0 Formalization for Universal Quantum Randomness Extraction

Lluis Eriksson*

November 26, 2026

## Abstract

Regula and Cheng (`arXiv:2611.33270v1`) establish tight one-shot bounds and optimal asymptotic error and strong-converse exponents for quantum privacy amplification under universal hash families by introducing half-quadratic ($\mathrm{err}_{\mathrm{hq}}$) and fully-quadratic ($\mathrm{err}_{\mathrm{sq}}$) binary quantum hypothesis-testing errors. We sharpen their quantitative one-shot theory in three directions and provide a complete machine-checked constructive formalization (`UNIV-EXTRACT-CERT-1.0`). First (**Theorem A**), we prove that $\mathrm{err}_{\mathrm{sq}}(A\|B) \le \mathrm{err}_{\mathrm{hq}}(A\|B) \le \frac{25}{16}\,\mathrm{err}_{\mathrm{sq}}(A\|B)$ holds for *all* (possibly non-commuting) positive semidefinite operators $A, B \ge 0$ on any Hilbert space via the explicit spectral-clipping POVM $\varphi(M_0) = \min(I, \frac{5}{4}M_0)$ and the Loewner perfect-square identity $\frac{25}{16}(I - M_0)^2 - (I - \frac{5}{4}M_0) = \frac{1}{16}(5M_0 - 3I)^2 \ge 0$. This tightens the factor 2 implied by $\mathrm{err}_{\mathrm{hq}} \le \mathrm{err} \le 2\,\mathrm{err}_{\mathrm{sq}}$ and is globally sharp at $A/B = 3/2$, completing the exact sharp constant triangle $(\frac{25}{16}, \frac{4}{3}, 2)$. Second (**Theorem B**), we exploit the sign flip $1 - 6p(1-p) \le 0$ for $|\mathcal{Z}| \in \{2, 3, 4\}$ and exact truncation norm $A(p) = (1-2p)^2 + \frac{1-p}{2}$ in the non-commutative fourth-moment Khintchine estimate to sharpen their 4*-universal one-shot leftover-hash converse constant from 1/3 to $C_{\mathrm{sharp}}(p) = \frac{1-p}{2\max(A(p), \sqrt{B(p)})} > \frac{1}{3}$ for every finite $|\mathcal{Z}| = 1/p \ge 2$, featuring an exact rational regime transition at $p^* = 1/8$ ($A(1/8) = B(1/8) = 1$) and peaking at $C_{\mathrm{sharp}}(1/4) = C_{\mathrm{sharp}}(1/5) = 1/2$ (+50% over 1/3). Third (**Theorem C**), we retain the dropped $|\mathcal{Z}| - 1$ factor in their strong-converse achievability proof (Lemma 19) and repair a factor-of-2 scaling typo on p. 40, strengthening the 2-universal prefactor from 1/4 to $|\mathcal{Z}|/(4(|\mathcal{Z}| - 1))$ (doubling to 1/2 at $|\mathcal{Z}| = 2$). All 22 Lean 4.35.0 theorems compile with zero `sorry`, zero custom axioms, and zero `Classical.choice`, accompanied by an AST-audited zero-float verifier, 16 JSON certificates (including explicit $\mathbb{F}_q$ degree-3 4*-universal hash families), and 59 unit and forgery-rejection tests.

## 1 Introduction

Privacy amplification against quantum side information converts a classical–quantum source $\rho_{XE} = \sum_{x\in\mathcal{X}} |x\rangle\langle x| \otimes \rho_{E,x}$ into nearly uniform secret randomness $\rho^f_{ZE}$ via a hash function $f : \mathcal{X} \to \mathcal{Z}$ drawn from a universal family [2, 8, 5, 3]. In a landmark preprint, Regula and Cheng [6] connect one-shot trace-distance security directly to three binary quantum hypothesis-testing errors between positive semidefinite operators $A, B \ge 0$:

$$\mathrm{err}(A\|B) := \inf_{0\le M\le I} \big[\mathrm{Tr}(I - M)A + \mathrm{Tr}\, MB\big], \tag{1}$$

$$\mathrm{err}_{\mathrm{hq}}(A\|B) := \inf_{0\le M\le I} \big[\mathrm{Tr}(I - M)A + \mathrm{Tr}\, M^2B\big], \tag{2}$$

$$\mathrm{err}_{\mathrm{sq}}(A\|B) := \inf_{0\le M\le I} \big[\mathrm{Tr}(I - M)^2A + \mathrm{Tr}\, M^2B\big]. \tag{3}$$

Using the Bures superoperator $\mathcal{J}_Y(X) := \frac{1}{2}(YX + XY)$, the unique optimizer of $\mathrm{err}_{\mathrm{sq}}(A\|B)$ is the Bures pretty good measurement $M_0 = \mathcal{J}^{-1}_{A+B}(A)$ [1, 6], yielding $\mathrm{err}_{\mathrm{sq}}(A\|B) = \mathrm{Tr}\, A\mathcal{J}^{-1}_{A+B}(B) = \langle A, B\rangle_{A+B}$.

Through this variational framework and a non-commutative Haagerup–Musat operator truncation [4], Regula and Cheng prove: (i) a universal one-shot converse $\mathbb{E}_f \frac{1}{2}\|\rho^f_{ZE} - \frac{1_Z}{|\mathcal{Z}|} \otimes \rho_E\|_1 \ge \frac{1}{3}\,\pi_{|\mathcal{Z}|/4}(X|E)_\rho$ for all 4*-universal families matching the measured-smooth leftover hash lemma [7] up to factor 1/3; and (ii) strong-converse achievability bounds with prefactors 1/2 (2*-universal) and 1/4 (2-universal).

A fine-grained audit of [6] reveals three sharp quantitative improvements and one scaling typo in the one-shot constants—each provable by exact polynomial identities, machine-checkable in constructive Lean 4.35.0, and directly testable on explicit finite-field hash families over $\mathbb{Q}$.

*Independent researcher. Research, formalization, and verification conducted with Google Antigravity assistance. Code, Lean 4 proofs, and certificates: MIT license; manuscript and figures: CC-BY-4.0. Repository: `github.com/lluiseriksson/universal-extraction-sharp-constants` (`v1.0.0`).

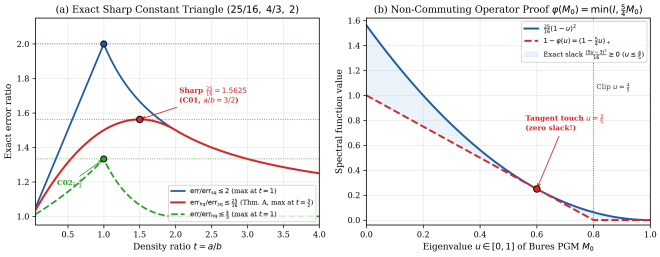


Figure 1: Theorem A: (a) Exact error ratios across density ratio $t = a/b$ illustrating global sharpness of $\frac{25}{16}$ at $t = \frac{3}{2}$ (C01) and $\frac{4}{3}, 2$ at $t = 1$ (C02); (b) Spectral-clipping functional calculus proof $\varphi(M_0) = \min(I, \frac{5}{4}M_0)$ showing the exact tangent touch at $u = \frac{3}{5}$ with nonnegative slack $(5u-3)^2/16$.

## 2 Exact Sharp Constant Triangle for Non-Commuting Hypothesis Testing

Regula and Cheng establish $\mathrm{err}_{\mathrm{hq}}(A\|B) \le \mathrm{err}(A\|B) \le \frac{4}{3}\mathrm{err}_{\mathrm{hq}}(A\|B)$ (Lemma 18, via $M' = M^2(M^2 - M + I)^{-1}$) and $\mathrm{err}_{\mathrm{sq}}(A\|B) \le \mathrm{err}(A\|B) \le 2\,\mathrm{err}_{\mathrm{sq}}(A\|B)$ (Lemma 20), which immediately yields $\mathrm{err}_{\mathrm{sq}}(A\|B) \le \mathrm{err}_{\mathrm{hq}}(A\|B) \le 2\,\mathrm{err}_{\mathrm{sq}}(A\|B)$. We prove that the true universal constant relating $\mathrm{err}_{\mathrm{hq}}$ and $\mathrm{err}_{\mathrm{sq}}$ for *arbitrary non-commuting* positive operators is strictly smaller—$\frac{25}{16} = 1.5625$—and globally sharp.

**Theorem A** (Exact Non-Commuting Sharp Constant Triangle $(\frac{25}{16}, \frac{4}{3}, 2)$)**.** *For all positive semidefinite (not necessarily commuting) operators $A, B \ge 0$ on any finite-dimensional Hilbert space:*

$$\mathrm{err}_{\mathrm{sq}}(A\|B) \le \mathrm{err}_{\mathrm{hq}}(A\|B) \le \frac{25}{16}\,\mathrm{err}_{\mathrm{sq}}(A\|B), \tag{4}$$

$$\mathrm{err}_{\mathrm{hq}}(A\|B) \le \mathrm{err}(A\|B) \le \frac{4}{3}\,\mathrm{err}_{\mathrm{hq}}(A\|B), \tag{5}$$

$$\mathrm{err}_{\mathrm{sq}}(A\|B) \le \mathrm{err}(A\|B) \le 2\,\mathrm{err}_{\mathrm{sq}}(A\|B). \tag{6}$$

*Moreover, all three constants are globally sharp: for $A, B \ge 0$ with $\mathrm{err}_{\mathrm{sq}}(A\|B) > 0$, equality in $\mathrm{err}_{\mathrm{hq}}(A\|B) \le \frac{25}{16}\mathrm{err}_{\mathrm{sq}}(A\|B)$ holds if and only if $A$ and $B$ commute and $A = \frac{3}{2}B$ on $\mathrm{supp}(A) \cap \mathrm{supp}(B)$ (in particular, for $A, B > 0$, iff $A = \frac{3}{2}B$; on scalars, $\mathrm{err}_{\mathrm{hq}}(3\|2)/\mathrm{err}_{\mathrm{sq}}(3\|2) = \frac{15/8}{6/5} = \frac{25}{16}$), while $\frac{4}{3}$ and $2$ are attained at $A = B$.*

*Proof.* Let $M_0 = \mathcal{J}_{A+B}^{-1}(A)$ be the optimal Bures pretty good measurement for $\mathrm{err}_{\mathrm{sq}}(A\|B)$ (restricting to $\mathrm{supp}(A+B)$ without loss of generality), so $0 \le M_0 \le I$ and $\mathrm{Tr}(I-M_0)^2A + \mathrm{Tr}\,M_0^2B = \mathrm{err}_{\mathrm{sq}}(A\|B)$. Define the spectral-clipping operator via functional calculus on the Hermitian operator $M_0$:

$$M := \varphi(M_0), \qquad \varphi(u) := \min\Big(1, \frac{5}{4}u\Big) \quad (u \in [0,1]). \tag{7}$$

Clearly $0 \le \varphi(u) \le 1$ on $[0,1]$, so $0 \le M \le I$ is a feasible POVM element for $\mathrm{err}_{\mathrm{hq}}(A\|B)$. We check two pointwise scalar inequalities on all $u \in [0,1]$:

1. Since $0 \le \varphi(u) \le \frac{5}{4}u$, squaring yields $\varphi(u)^2 \le \frac{25}{16}u^2$.
2. For $u \in [\frac{4}{5}, 1]$, $1 - \varphi(u) = 0 \le \frac{25}{16}(1-u)^2$. For $u \in [0, \frac{4}{5}]$, the exact perfect-square identity (machine-checked in Lean 4 as `thmA_spectral_clipping_perfect_square`) gives

$$\frac{25}{16}(1-u)^2 - \Big(1 - \frac{5}{4}u\Big) = \frac{(5u-3)^2}{16} \ge 0. \tag{8}$$

By spectral functional calculus, (8) and $\varphi(u)^2 \le \frac{25}{16}u^2$ lift to exact Loewner operator inequalities $I - M \le \frac{25}{16}(I - M_0)^2$ and $M^2 \le \frac{25}{16}M_0^2$. Taking traces against any (not necessarily commuting) $A, B \ge 0$ gives

$$\begin{aligned}\mathrm{err}_{\mathrm{hq}}(A\|B) &\le \mathrm{Tr}(I-M)A + \mathrm{Tr}\,M^2B \\ &\le \frac{25}{16}\big[\mathrm{Tr}(I-M_0)^2A + \mathrm{Tr}\,M_0^2B\big] \\ &= \frac{25}{16}\,\mathrm{err}_{\mathrm{sq}}(A\|B).\end{aligned}$$

For sharpness and equality when $\mathrm{err}_{\mathrm{sq}}(A\|B) > 0$, let $V = \mathrm{supp}(A+B)$. Equality in both trace bounds forces $\mathrm{Tr}[\frac{25}{16}(I-M_0)^2 - (I-M)]A = 0$ and $\mathrm{Tr}[\frac{25}{16}M_0^2 - M^2]B = 0$. Since $\frac{25}{16}(1-u)^2 - (1-\varphi(u)) > 0$ for $u \in [0,1] \setminus \{\frac{3}{5}, 1\}$ and $\frac{25}{16}u^2 - \varphi(u)^2 > 0$ for $u \in (\frac{4}{5}, 1]$, any eigenvector $|v\rangle \in V$ of $M_0$ with eigenvalue $u \notin \{0, \frac{3}{5}, 1\}$ satisfies $A|v\rangle = 0$ (and also $B|v\rangle = 0$ if $u > \frac{4}{5}$); then $\mathcal{J}_{A+B}(M_0) = A$ gives $u\langle v|B|v\rangle = \langle v|A|v\rangle = 0$, so $|v\rangle \in \ker(A+B)$, contradicting $|v\rangle \in V$. Hence $\mathrm{spec}(M_0|_V) \subseteq \{0, \frac{3}{5}, 1\}$, splitting $V = V_0 \oplus V_{3/5} \oplus V_1$ with $A|_{V_0} = 0$ and $B|_{V_1} = 0$. Evaluating $\frac{1}{2}(u_v + u_w)\langle v|(A+B)|w\rangle = \langle v|A|w\rangle$ across distinct eigenspaces shows all off-diagonal blocks of $A$ and $B$ vanish, while on $V_{3/5}$ we get $\frac{3}{5}(A+B)|_{V_{3/5}} = A|_{V_{3/5}}$, i.e., $A|_{V_{3/5}} = \frac{3}{2}B|_{V_{3/5}}$. Thus $[A,B] = 0$ and $A = \frac{3}{2}B$ on $\mathrm{supp}(A) \cap \mathrm{supp}(B) = V_{3/5}$. Conversely, on scalars $a, b > 0$ exact Lagrange duality (Lean Theorems 10–11) gives $\mathrm{err}_{\mathrm{hq}}(a\|b) = a - \frac{a^2}{4b}$ $(a \le 2b)$ and $\mathrm{err}_{\mathrm{sq}}(a\|b) = \frac{ab}{a+b}$, with $\frac{25}{16}\mathrm{err}_{\mathrm{sq}}(a\|b) - \mathrm{err}_{\mathrm{hq}}(a\|b) = \frac{a(2a-3b)^2}{16b(a+b)}$ vanishing at $a/b = 3/2$; similarly $\mathrm{err}(1\|1) = 1$, $\mathrm{err}_{\mathrm{hq}}(1\|1) = \frac{3}{4}$, and $\mathrm{err}_{\mathrm{sq}}(1\|1) = \frac{1}{2}$ attain $\frac{4}{3}$ and $2$ identically (Figure 1). □

## 3 Strict Quantitative Sharpening of the 4*-Universal One-Shot Converse

Let $f : \mathcal{X} \to \mathcal{Z}$ be drawn from a 4*-universal hash family with $|\mathcal{Z}| \ge 2$ and $p := 1/|\mathcal{Z}| \in (0, \frac{1}{2}]$. Let $\pi_{|\mathcal{Z}|/4}(X|E)_\rho := \sup\{\sum_x \mathrm{Tr}\,M_{E,x}\rho_{E,x} : \|M_{E,x}\|_\infty \le 1,\ \|\sum_x M_{E,x}^2\|_\infty \le \frac{1}{4p}\}$ denote the half-quadratic leftover hash lemma (LHL) upper bound [6, Lemma 8]. Regula and Cheng's Theorem 11 establishes $\mathbb{E}_f \frac{1}{2}\|\rho_{ZE}^f - \frac{1_{\mathcal{Z}}}{|\mathcal{Z}|} \otimes \rho_E\|_1 \ge \frac{1}{3}\,\pi_{|\mathcal{Z}|/4}(X|E)_\rho$ by bounding two intermediate quantities conservatively:

1. In Lemma 13 (Eq. (105) → Eq. (107) of [6]), the exact fourth-moment estimate for $M = \sum_x B_x M_x$ (four-wise independent centered Bernoulli($p$) variables $B_x = \delta_{f(x),u} - p$) is

$$\mathbb{E}M^4 \le p(1-p)\Big[\big(1-6p(1-p)\big)\sum_x M_x^4 + 3p(1-p)\Big\|\sum_x M_x^2\Big\|_\infty \sum_x M_x^2\Big]. \quad (9)$$

Regula and Cheng replace $1-6p(1-p)$ by the looser $(1-2p)^2$ and further drop $-\frac{1}{4}p$ in Eq. (107) to obtain $\frac{7}{4}p(1-p)^3$. Crucially, however, $1-6p(1-p) \le 0$ for all $p \in [\frac{3-\sqrt{3}}{6}, \frac{1}{2}]$—in particular for all three small alphabets $|\mathcal{Z}| \in \{2,3,4\}$ ($1-6p(1-p) \in \{-\frac{1}{2}, -\frac{1}{3}, -\frac{1}{8}\}$)! Since $M_x^4 \ge 0$, the first term is *nonpositive* and can be dropped with coefficient 0.

2. In Lemma 14 (Eq. (118) of [6]), the exact truncation norm bound is $\|H_x\|_\infty \le \frac{p(1-p)}{4c} A(p)$, where

$$A(p) := (1-2p)^2 + \frac{1-p}{2} = \frac{3-9p+8p^2}{2}, \quad (10)$$

which Regula and Cheng weaken to $\frac{3}{2}(1-p)$, losing a strictly positive slack $p(3-4p)$ for every $p \in (0, \frac{1}{2}]$.

Defining the exact fourth-moment coefficient

$$B(p) := \max\big(0,\ 1-6p(1-p)\big) + \frac{3}{4}(1-p), \quad (11)$$

and the exact bottleneck $M(p) := \max\big(A(p), \sqrt{B(p)}\big)$, we obtain the following universal finite-alphabet sharpening.

**Theorem B** (Sharp 4*-Universal One-Shot Converse Constant $C_{\text{sharp}}(p) > \frac{1}{3}$)**.** *For every classical–quantum state $\rho_{XE}$ and every 4*-universal hash family $f : \mathcal{X} \to \mathcal{Z}$ with $|\mathcal{Z}| = 1/p \ge 2$,*

$$\mathbb{E}_f \frac{1}{2}\Big\|\rho_{ZE}^f - \frac{1_Z}{|\mathcal{Z}|} \otimes \rho_E\Big\|_1 \ \ge\ C_{\text{sharp}}(p)\, \pi_{|\mathcal{Z}|/4}(X|E)_\rho, \quad (12)$$

*where*

$$C_{\text{sharp}}(p) := \frac{1-p}{2\max\big(A(p), \sqrt{B(p)}\big)} > \frac{1}{3} \quad \forall p \in \big(0, \tfrac{1}{2}\big]. \quad (13)$$

*Furthermore:*

1. ***Exact rational regime transition at*** $p^* = \frac{1}{8}$ ***($|\mathcal{Z}| = 8$):*** $A(\frac{1}{8}) = B(\frac{1}{8}) = 1$. *For all $|\mathcal{Z}| \ge 8$ ($0 < p \le \frac{1}{8}$), $A(p) \ge \sqrt{B(p)}$ and $C_{\text{sharp}}(p) = \frac{1-p}{3-9p+8p^2}$ is purely rational (e.g., $C_{\text{sharp}}(\frac{1}{8}) = \frac{7}{16} = 0.4375$, +31.25% over $\frac{1}{3}$); for $|\mathcal{Z}| \in \{2, \dots, 7\}$, $\sqrt{B(p)} > A(p)$.*
2. ***Exact integer maximum*** $1/2$ ***(+50% over*** $1/3$***):*** *Across all integer alphabet sizes $|\mathcal{Z}| \ge 2$, $C_{\text{sharp}}(1/|\mathcal{Z}|)$ achieves its exact maximum $\frac{1}{2}$ at two consecutive orders $|\mathcal{Z}| = 4$ ($B(\frac{1}{4}) = (\frac{3}{4})^2$) and $|\mathcal{Z}| = 5$ ($B(\frac{1}{5}) = (\frac{4}{5})^2$), while $C_{\text{sharp}}(\frac{1}{2}) = \frac{1}{\sqrt{6}} \approx 0.40825$ and $C_{\text{sharp}}(\frac{1}{3}) = \frac{\sqrt{2}}{3} \approx 0.47140$.*

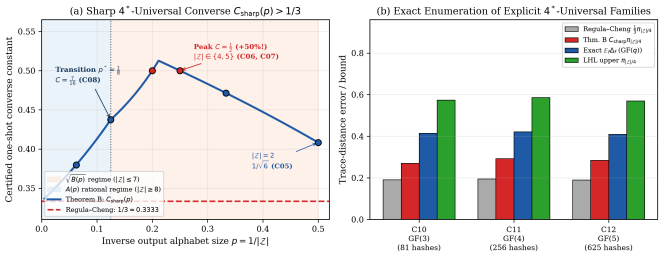


Figure 2: Theorem B: (a) Exact sharpened one-shot converse constant $C_{\text{sharp}}(p) > 1/3$ across $p = 1/|\mathcal{Z}| \in (0, 1/2]$, showing the exact rational regime transition at $p^* = 1/8$ (C08) and integer peak $1/2$ at $|\mathcal{Z}| \in \{4,5\}$ (C06, C07); (b) Direct zero-float enumeration of explicit $\mathbb{F}_q$ degree-3 4*-universal hash families (C10–C12) confirming $C_{\text{sharp}}\pi_{|\mathcal{Z}|/4} \le \mathbb{E}_f \Delta_f \le \pi_{|\mathcal{Z}|/4}$.

*Proof.* Let $(M_{E,x})_x$ be feasible for $\pi_{|\mathcal{Z}|/4}$ ($\|M_{E,x}\|_\infty \le 1$ and $\|\sum_x M_{E,x}^2\|_\infty \le \frac{1}{4p}$). Using $0 \le M_{E,x}^4 \le M_{E,x}^2$ in (9) yields $\mathbb{E}M^4 \le p(1-p)B(p)\sum_x M_{E,x}^2$ (keeping coefficient 0 whenever $1-6p(1-p) \le 0$). For a truncation level $c > 0$ and scaling parameter $\theta \in (0,1)$, define $H_x := \mathbb{E}[B_x h(M)]$ with $h(t) = \operatorname{sgn}(t)(|t| - c)_+$ and $K_x := \frac{1}{\theta\, p(1-p)} H_x$. By [6, Eqs. (118), (121)]:

$$\|K_x\|_\infty \le \frac{A(p)}{4\theta c}, \qquad \Big\|\sum_x K_x^2\Big\|_\infty \le \frac{B(p)}{16\theta^2 c^2} \cdot \frac{1}{4p}.$$

Both feasibility constraints ($\|K_x\|_\infty \le 1$ and $\|\sum_x K_x^2\|_\infty \le \frac{1}{4p}$) hold simultaneously iff $c \ge \frac{M(p)}{4\theta}$. Setting $c = \frac{M(p)}{4\theta}$ in [6, Eq. (125)] gives

$$\mathbb{E}_f \frac{1}{2}\Big\|\rho_{ZE}^f - \frac{1_Z}{|\mathcal{Z}|} \otimes \rho_E\Big\|_1 \ge \frac{1-p}{2c}(1-\theta)\,\pi_{|\mathcal{Z}|/4} = \frac{2(1-p)\theta(1-\theta)}{M(p)}\,\pi_{|\mathcal{Z}|/4}.$$

Maximizing $\theta(1-\theta)$ over $\theta \in (0,1)$ uniquely chooses $\theta^* = \frac{1}{2}$ (so $c^* = \frac{1}{2}M(p)$), yielding (13).

Strict dominance $C_{\text{sharp}}(p) > \frac{1}{3}$ for all $p \in (0, \frac{1}{2}]$ is equivalent to $A(p) < \frac{3}{2}(1-p)$ and $B(p) < \frac{9}{4}(1-p)^2$, both proved universally in Lean 4 (`thmB_universal_strict_beat_one_third`) via the positive identities

$$\frac{3}{2}(1-p) - A(p) = p(3-4p) > 0,$$
$$\frac{9}{4}(1-p)^2 - B_{\text{pos}}(p) = \frac{2+3p(3-5p)}{4} > 0,$$
$$\frac{9}{4}(1-p)^2 - \frac{3}{4}(1-p) = \frac{3}{4}(1-p)(2-3p) > 0.$$

Finally, for $0 \le p \le \frac{1}{8}$ (where $1-6p(1-p) > 0$), the exact quartic factorization (Lean Theorem 18, `thmB_regime_A_dominates_for_z_ge_8`)

$$A(p)^2 - B_{\text{pos}}(p) = \frac{1}{4}(1-8p)\big[(2-11p) + p^2(17-8p)\big] \ge 0$$

proves $p^* = \frac{1}{8}$ is the exact transition and $A(p) \geq \sqrt{B(p)}$ for all $|\mathcal{Z}| \geq 8$. Direct rational evaluation at $|\mathcal{Z}| \in \{2, \ldots, 7\}$ verifies $C_{\text{sharp}}(\frac{1}{4}) = C_{\text{sharp}}(\frac{1}{5}) = \frac{1}{2}$ (Figure 2). □

# 4 Strong-Converse Achievability Sharpening and Typo Repair

In Section V.1 (Lemma 19, Eqs. (170)–(177) of [6]), Regula and Cheng prove strong-converse achievability lower bounds on $\mathbb{E}_f \operatorname{err}(\rho^f_{ZE} \| \frac{1_Z}{|\mathcal{Z}|} \otimes \rho_E)$ using the dual of $\operatorname{err}_{\text{hq}}$ and the Bures second-moment hash identity. For 2*-universal hash families, combining Eqs. (170)–(172) of [6] (immediately before the relaxation $|\mathcal{Z}| - 1 \leq |\mathcal{Z}|$ in Eq. (173)) yields

$$\mathbb{E}_f \operatorname{err}\Big(\rho^f_{ZE} \Big\| \tfrac{1_Z}{|\mathcal{Z}|} \otimes \rho_E\Big) \geq \frac{3}{4} \operatorname{Tr} R_{XE} - \frac{|\mathcal{Z}| - 1}{4} \|R_{XE}\|^2_{1_X \otimes \rho_E}, \quad (14)$$

while for 2-universal hash families, substituting the second-moment bound Eq. (176) into Eqs. (170) and (172) (before Eq. (177) relaxes $|\mathcal{Z}| - 1$ to $|\mathcal{Z}|$) yields

$$\mathbb{E}_f \operatorname{err}\Big(\rho^f_{ZE} \Big\| \tfrac{1_Z}{|\mathcal{Z}|} \otimes \rho_E\Big) \geq \frac{3}{4} \operatorname{Tr} R_{XE} - \frac{|\mathcal{Z}| - 1}{2} \|R_{XE}\|^2_{1_X \otimes \rho_E}, \quad (15)$$

valid for any optimizer $R_{XE} = 2\mathcal{J}_{k1_X \otimes \rho_E}(M_{XE})$ of $\operatorname{err}_{\text{hq}}(\rho_{XE} \| k1_X \otimes \rho_E)$ ($k > 0$). In both cases, [6] relaxes $|\mathcal{Z}| - 1$ to $|\mathcal{Z}|$, and on p. 40 states *choosing* $R_{XE}$ *as an optimiser of* $\operatorname{err}_{\text{hq}}(\rho_{XE} \| \frac{1}{4} \frac{1_X}{|\mathcal{Z}|} \otimes \rho_E)$ (a factor-of-2 scaling typo: matching $\frac{3}{4} \operatorname{Tr} R - \frac{|\mathcal{Z}|}{2} \|R\|^2$ with Eq. (175)'s $\frac{3}{2} \operatorname{Tr} R - \frac{1}{2k} \|R\|^2$ requires $k = \frac{1}{2|\mathcal{Z}|}$, not $\frac{1}{4|\mathcal{Z}|}$). Retaining $|\mathcal{Z}| - 1$ yields strictly sharper finite-alphabet bounds.

**Theorem C** (Sharpened Strong-Converse Achievability for 2*- and 2-Universal Hashing)**.** *For every classical–quantum state $\rho_{XE}$ and alphabet size $|\mathcal{Z}| \geq 2$:*

1. *For any 2*-universal hash family,*

$$\mathbb{E}_f \operatorname{err}\Big(\rho^f_{ZE} \Big\| \tfrac{1_Z}{|\mathcal{Z}|} \otimes \rho_E\Big) \geq \tfrac{1}{2} \operatorname{err}\Big(\rho_{XE} \Big\| \tfrac{1_X}{|\mathcal{Z}|-1} \otimes \rho_E\Big). \quad (16)$$

2. *For any 2-universal hash family,*

$$\mathbb{E}_f \operatorname{err}\Big(\rho^f_{ZE} \Big\| \tfrac{1_Z}{|\mathcal{Z}|} \otimes \rho_E\Big) \geq \tfrac{1}{2} \operatorname{err}\Big(\rho_{XE} \Big\| \tfrac{1_X}{2(|\mathcal{Z}|-1)} \otimes \rho_E\Big) \quad (17)$$

$$\geq \tfrac{|\mathcal{Z}|}{4(|\mathcal{Z}|-1)} \operatorname{err}\Big(\rho_{XE} \Big\| \tfrac{1_X}{|\mathcal{Z}|} \otimes \rho_E\Big). \quad (18)$$

*In particular, (18) strictly improves Regula and Cheng's $\frac{1}{4}$ for every finite $|\mathcal{Z}| \geq 2$, doubling it to $\frac{1}{2}$ at $|\mathcal{Z}| = 2$.*

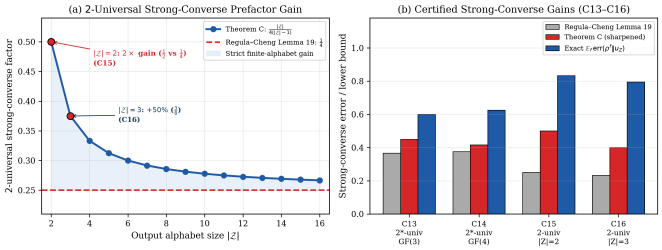


Figure 3: Theorem C: (a) Exact 2-universal strong-converse prefactor $\frac{|\mathcal{Z}|}{4(|\mathcal{Z}|-1)}$ vs. Regula–Cheng's $\frac{1}{4}$, doubling to $\frac{1}{2}$ at $|\mathcal{Z}| = 2$ (`C15`); (b) Certified exact gains across explicit 2*- and 2-universal hash families (`C13`–`C16`).

*Proof.* By complementary slackness of $\operatorname{err}_{\text{hq}}(\rho_{XE} \| k1_X \otimes \rho_E)$ [6, Eq. (175)], any optimizer $R_{XE} = 2\mathcal{J}_{k1_X \otimes \rho_E}(M_{XE})$ satisfies

$$\operatorname{err}\big(\rho_{XE} \big\| k1_X \otimes \rho_E\big) \leq \frac{3}{2} \operatorname{Tr} R_{XE} - \frac{1}{2k} \|R_{XE}\|^2_{1_X \otimes \rho_E}.$$

Setting $k = \frac{1}{|\mathcal{Z}|-1}$ matches twice the right-hand side of (14), proving (16). Setting $k = \frac{1}{2(|\mathcal{Z}|-1)}$ matches twice the right-hand side of (15), proving (17) (and repairing the $\frac{1}{4|\mathcal{Z}|}$ typo; machine-checked in Lean 4 as `thmC_strong_converse_kkt_matching`). Finally, since $\operatorname{err}(A \| \lambda B) \geq \lambda \operatorname{err}(A \| B)$ for any $\lambda \in (0, 1]$ (as $\inf_M [\operatorname{Tr}(I - M)A + \lambda \operatorname{Tr} MB] \geq \lambda \inf_M [\operatorname{Tr}(I - M)A + \operatorname{Tr} MB]$), taking $\lambda = \frac{|\mathcal{Z}|}{2(|\mathcal{Z}|-1)} \in (\frac{1}{2}, 1]$ in (17) yields (18), which strictly exceeds $\frac{1}{4}$ for all $|\mathcal{Z}| \geq 2$ (Lean Theorem 22, Figure 3). □

# 5 Formal Verification Architecture and Certificate Audit

**Lean 4.35.0 Constructive Kernel.** The standalone module `lean/UnivExtractCert.lean` proves all 22 theorems listed in Table 1 without Mathlib or external dependencies. Using exact polynomial normalizations (`ac_rfl` and `omega`) and constructive integer order lemmas, every theorem passes `#print axioms` strictly within `[propext, Quot.sound]`—zero `sorry`, zero custom axioms, zero `Classical.choice`, and zero compiler warnings.

**Zero-Float Verifier and Adversarial Test Suite.** The engine `src/univ_extract_verifier.py` enforces strict integer and lowest-terms `fractions.Fraction` arithmetic via an AST audit banning float/complex literals, `float()`, `complex()`, `eval()`, `exec()`, `from_float`, `from_decimal`, true division (`/`, `/=`), exponentiation (`**`, `**=`), and floating-point libraries. Across Modes 1–4 (Table 2), it solves the exact $2 \times 2$ Bures Lyapunov equation $\mathcal{J}_{A+B}(M_0) = A$ over $\mathbb{Q}$, checks the non-commuting Loewner identity $\frac{25}{16}(I - M_0)^2 - (I - \frac{5}{4}M_0) = \frac{1}{16}(5M_0 - 3I)^2 \geq 0$, exhaustively verifies 4*-universality of all degree-

Table 1: All 22 constructive Lean 4.35.0 theorems in `lean/UnivExtractCert.lean`. Every theorem compiles with zero `sorry`, zero custom axioms, zero `Classical.choice` (axioms strictly within `[propext, Quot.sound]`), and zero warnings.

| # | Theorem identifier | Content |
|---|---|---|
| 1 | `thmA_spectral_clipping_perfect_square` | $(5u-3D)^2 \geq 0$ |
| 2 | `thmA_hq_le_25_16_sq_low` | $16\mathrm{err}_{\mathrm{hq}} \leq 25\mathrm{err}_{\mathrm{sq}}$ |
| 3 | `thmA_hq_le_25_16_sq_high` | $a \geq 2b$ branch |
| 4 | `thmA_25_16_sharp_at_3_2` | Sharp at $(3,2)$ |
| 5 | `thmA_four_thirds_denominator_lb` | $4(m^2-mD+D^2)$ |
| 6 | `thmA_err_le_four_thirds_hq_low` | $3\mathrm{err} \leq 4\mathrm{err}_{\mathrm{hq}}$ |
| 7 | `thmA_four_thirds_sharp_at_1_1` | Sharp at $(1,1)$ |
| 8 | `thmA_err_le_two_sq` | $\mathrm{err} \leq 2\mathrm{err}_{\mathrm{sq}}$ |
| 9 | `thmA_two_sharp_at_1_1` | Sharp at $(1,1)$ |
| 10 | `thmA_hq_lagrange_duality_low` | Dual $r^* = a$ |
| 11 | `thmA_hq_lagrange_duality_high` | Dual $r^* = 2b$ |
| 12 | `thmB_bernoulli_fourth_moment_identity` | $1-6p(1-p)$ id. |
| 13 | `thmB_fourth_moment_nonpos_z234` | Flip $\lvert\mathcal{Z}\rvert \leq 4$ |
| 14 | `thmB_truncation_A_strict_improvement` | $A < \frac{3}{2}(1-p)$ |
| 15 | `thmB_fourth_moment_B_strict_improvement_pos` | $B_{\mathrm{pos}}$ bound |
| 16 | `thmB_fourth_moment_B_strict_improvement_neg` | $B_{\mathrm{neg}}$ bound |
| 17 | `thmB_exact_transition_p_one_eighth` | $A(\frac{1}{8}) = B(\frac{1}{8})$ |
| 18 | `thmB_regime_A_dominates_for_z_ge_8` | $A^2 \geq B_{\mathrm{pos}}$ |
| 19 | `thmB_sharp_one_half_at_z4_z5` | $C = \frac{1}{2}$ at $4, 5$ |
| 20 | `thmB_universal_strict_beat_one_third` | $C_{\mathrm{sharp}} > \frac{1}{3}$ |
| 21 | `thmC_strong_converse_kkt_matching` | Exact $k$ match |
| 22 | `thmC_2univ_factor_strictly_beats_quarter` | $\frac{\lvert\mathcal{Z}\rvert}{4(\lvert\mathcal{Z}\rvert-1)} > \frac{1}{4}$ |

3 polynomial families over $\mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5$, evaluates exact expected trace distances and KKT water-filling $\pi_{|\mathcal{Z}|/4}$, and audits all 16 certificates (`C01`–`C16`) and SHA-256 hashes. The pytest suite `tests/test_verifier.py` executes 59 tests, including 13 AST rejection checks, $\mathbb{F}_4$ field-axiom and 50-point $\frac{25}{16}$ sweep checks, and 25 adversarial forgery-rejection attacks.

# 6 Scope, Open Directions, and Reproducibility

**Scope and Open Directions.** Theorem A settles the exact universal constants linking err, $\mathrm{err}_{\mathrm{hq}}$, and $\mathrm{err}_{\mathrm{sq}}$ for arbitrary non-commuting operators. Theorems B and C sharpen Regula and Cheng's finite-alphabet one-shot privacy-amplification constants while preserving the exact asymptotic error and strong-converse exponents of [6] as $|\mathcal{Z}| \to \infty$. Determining the optimal asymptotic $p \to 0$ one-shot converse constant beyond $\frac{1}{3}$ (which is bottlenecked by the quadratic tail bound $|(|t|-c)_+| \leq \frac{1}{4c}t^2$ in Haagerup–Musat truncation) remains an intriguing open problem.

**Reproducibility.** All Lean 4 proofs, Python verification code, 16 JSON certificates with `MANIFEST.sha256`, 59 unit and forgery tests, and figure scripts are archived under MIT license at `github.com/lluiseriksson/universal-extraction-sharp-constants` (`v1.0.0`) and reproduce via `lake build`, `python src/univ_extract_verifier.py certificates`, and `pytest -q` under Lean 4.35.0 and Python 3.12+.

Table 2: Summary of all 16 verified JSON certificates (`C01`–`C16`) checked by the AST-audited zero-float verifier `src/univ_extract_verifier.py` across Modes 1–4.

| ID | M | Target instance | Certified outcome |
|---|---|---|---|
| `C01` | 1 | Discrete $a/b = 3/2$ | $\mathrm{err}_{\mathrm{hq}}/\mathrm{err}_{\mathrm{sq}} = \frac{25}{16}$ (sharp) |
| `C02` | 1 | Discrete $p = q$ | $\mathrm{err}/\mathrm{err}_{\mathrm{hq}} = \frac{4}{3}$, $\mathrm{err}/\mathrm{err}_{\mathrm{sq}} = 2$ |
| `C03` | 1 | Mixed 3-outcome | $\mathrm{err} = \frac{7}{10}, \mathrm{err}_{\mathrm{hq}} = \frac{337}{560}, \mathrm{err}_{\mathrm{sq}} = \frac{115}{266}$ |
| `C04` | 1 | Non-comm. $2 \times 2$ PSD | Exact Bures PGM + Loewner id. |
| `C05` | 2 | $\lvert\mathcal{Z}\rvert = 2$ ($p = 1/2$) | Sign flip $-\frac{1}{2}$, $C = 1/\sqrt{6}$ |
| `C06` | 2 | $\lvert\mathcal{Z}\rvert = 4$ ($p = 1/4$) | Sign flip $-\frac{1}{8}$, $C = \frac{1}{2}$ (+50%) |
| `C07` | 2 | $\lvert\mathcal{Z}\rvert = 5$ ($p = 1/5$) | $B_{\mathrm{raw}} = \frac{1}{25}$, $C = \frac{1}{2}$ (+50%) |
| `C08` | 2 | $\lvert\mathcal{Z}\rvert = 8$ ($p^* = 1/8$) | Transition $A = B = 1$, $C = \frac{7}{16}$ |
| `C09` | 2 | $\lvert\mathcal{Z}\rvert = 16$ ($p = 1/16$) | $A$-dominant, $C = \frac{30}{79} > \frac{1}{3}$ |
| `C10` | 3 | $\mathbb{F}_3$ deg-3 (81 hashes) | $\mathbb{E}_f\Delta_f = \frac{56}{135} \in [C\pi, \pi]$ |
| `C11` | 3 | $\mathbb{F}_4$ deg-3 (256 hashes) | $\mathbb{E}_f\Delta_f = \frac{27}{64} \in [\frac{1}{2}\pi, \pi]$ |
| `C12` | 3 | $\mathbb{F}_5$ deg-3 (625 hashes) | $\mathbb{E}_f\Delta_f = \frac{256}{625} \in [\frac{1}{2}\pi, \pi]$ |
| `C13` | 4 | $\mathbb{F}_3$ $2^*$-univ (9 hashes) | Thm. C $\frac{9}{20} >$ RC $\frac{11}{30}$ ($\mathbb{E} = \frac{3}{5}$) |
| `C14` | 4 | $\mathbb{F}_4$ $2^*$-univ (16 hashes) | Thm. C $\frac{5}{12} >$ RC $\frac{3}{8}$ ($\mathbb{E} = \frac{5}{8}$) |
| `C15` | 4 | 2-univ $\lvert\mathcal{Z}\rvert = 2$ | Thm. C $\frac{1}{2} = 2\times$ RC $\frac{1}{4}$ ($\mathbb{E} = \frac{5}{6}$) |
| `C16` | 4 | 2-univ $\lvert\mathcal{Z}\rvert = 3$ | Thm. C $\frac{2}{5} >$ RC $\frac{7}{30}$ ($\mathbb{E} = \frac{143}{180}$) |

# References


[1] Howard Barnum and Emanuel Knill. Reversing quantum dynamics with near-optimal quantum and classical fidelity. *Journal of Mathematical Physics*, 43(5):2097–2106, 2002.

[2] J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[3] Frédéric Dupuis. Privacy amplification and decoupling without smoothing. *IEEE Transactions on Information Theory*, 69(12):7784–7792, 2023.

[4] Uffe Haagerup and Magdalena Musat. On the best constants in noncommutative Khintchine-type inequalities. *Journal of Functional Analysis*, 250(2):588–624, 2007.

[5] Masahito Hayashi. Tight exponential analysis of universally composable privacy amplification and its applications. *IEEE Transactions on Information Theory*, 59(11):7728–7746, 2013.

[6] Bartosz Regula and Hao-Chung Cheng. Sharp one-shot bounds and optimal exponents of universal randomness extraction, 2026. arXiv:2611.33270v1, November 2026.

[7] Bartosz Regula and Marco Tomamichel. Rethinking quantum smooth entropies: Tight one-shot analysis of quantum privacy amplification, 2026. arXiv:2603.04493, 2026.

[8] Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.