26th Asian Quantum Information Science Conference (AQIS 2026) · Daejeon, Korea · August 24-28, 2026

P3-073 · No. 279

Lean-Quantum: Toward AI-Assisted Formalization of Quantum Information

GitHub repository

Kazumi Kasaura[1,2] · Kei Tsukamoto[3] · Kento Mori[4] · Risa Mizuno[3] · Takahiro Namatame[5] · Yuta Oriike[6] · Masaya Taniguchi[2] · Sho Sonoda[2,6] · Hayata Yamasaki[3]

[1] OMRON SINIC X Corporation · [2] RIKEN · [3] The University of Tokyo · [4] MOLSIS Inc. · [5] Kyoto University · [6] CyberAgent, Inc.

Main result: sandwiched Rényi data processing for arbitrary PSD operators over the full Frank-Lieb range α ≥ 1/2, α ≠ 1.

Quantum systems

DEFINITION

A quantum system is modeled by a complex Hilbert space. The present `Qudit ℋ` carrier also assumes completeness and finite dimensionality, making traces and density representatives immediate; it stores no state, basis, or dimension field.

```
class Qudit (ℋ : Type u) extends
  NormedAddCommGroup ℋ, InnerProductSpace ℂ ℋ,
  CompleteSpace ℋ, FiniteDimensional ℂ ℋ

abbrev L (ℋ : Type u) [AddCommGroup ℋ]
    [Module ℂ ℋ] := ℋ →ₗ[ℂ] ℋ

abbrev B (ℋ : Type u) [AddCommGroup ℋ]
    [Module ℂ ℋ] [TopologicalSpace ℋ] := ℋ →L[ℂ] ℋ
```

EXAMPLE · QUANTUM.EXAMPLES.BASICCONCEPTS · IN PREPARATION

```
abbrev Qubit := EuclideanSpace ℂ (Fin 2)
example : Qudit Qubit := inferInstance
```

Quantum states

DEFINITION

In general, a state on an observable algebra $\mathcal{A}$ is a normalized positive linear functional

$$\omega : \mathcal{A} \to \mathbb{C}, \qquad \omega(A^\dagger A) \geq 0, \qquad \omega(I) = 1.$$

For the present `Qudit` instance it is represented uniquely by a density operator:

$$\omega_\rho(A) = \mathrm{Tr}(\rho A), \qquad \rho \succeq 0, \qquad \mathrm{Tr}\,\rho = 1.$$

The private API exposes algebraic `L ℋ` and continuous `B ℋ`, canonically equivalent in finite dimension. The split is an implementation/API choice: analytic instances are transported to `L`, so statement-facing interfaces (`IsDensity`, CPTP, Rényi, entropy) use `L`; `B` remains a proof-support view.

```
-- statement-facing predicate on algebraic endomorphisms
def IsDensity (ρ : L ℋ) : Prop :=
  ρ.IsPositive ∧ Tr ρ = 1
```

EXAMPLE · QUANTUM.EXAMPLES.BASICCONCEPTS · IN PREPARATION

```
noncomputable def pureState (ψ : ℋ) : L ℋ :=
  outer_product ψ ψ

lemma pureState_isDensity {ψ : ℋ} (hψ : ‖ψ‖ = 1) :
    IsDensity (pureState ψ)
```

Quantum channels

DEFINITION

A channel is a linear map $\Phi : \mathcal{L}(\mathcal{H}_1) \to \mathcal{L}(\mathcal{H}_2)$ that is completely positive on every auxiliary system and trace preserving.

```
abbrev T (ℋ₁ ℋ₂) := (L ℋ₁) →ₗ[ℂ] (L ℋ₂)

structure CPTP (ℋ₁ ℋ₂) extends
    CompletelyPositiveMap (L ℋ₁) (L ℋ₂) where
  trace_map (ρ : L ℋ₁) : Tr ρ = Tr (toFun ρ)
```

EXAMPLE · QUANTUM.EXAMPLES.BASICCONCEPTS · IN PREPARATION

```
example (Φ : CPTP ℋ 𝒦) {ρ : L ℋ}
    (hρ : IsDensity ρ) : IsDensity (Φ.toFun ρ) := by
  constructor
  · exact (LinearMap.nonneg_iff_isPositive _).mp <|
      map_nonneg Φ.toCompletelyPositiveMap <|
        (LinearMap.nonneg_iff_isPositive _).mpr hρ.1
  · exact (Φ.trace_map ρ).symm.trans hρ.2
```

Channel representations

THEOREM

For a linear superoperator, complete positivity has equivalent Choi, Kraus, and Stinespring representations:

$$\Phi \text{ is CP} \iff J_b(\Phi) \succeq 0 \iff \Phi(X) = \sum_a A_a X A_a^\dagger \iff \Phi(X) = \mathrm{Tr}_E(VXV^\dagger).$$

```
theorem cp_iff_choi (b : Module.Basis κ ℂ ℋ₁)
    (Φ : (L ℋ₁) →ₗ[ℂ] (L ℋ₂)) :
    IsCompletelyPositive Φ ↔ ChoiPositive b Φ

theorem cp_iff_kraus (Φ : (L ℋ₁) →ₗ[ℂ] (L ℋ₂)) :
    IsCompletelyPositive Φ ↔ HasKraus Φ

theorem cp_iff_stinespring
    (Φ : (L ℋ₁) →ₗ[ℂ] (L ℋ₂)) :
    IsCompletelyPositive Φ ↔ HasStinespring Φ
```

Lean keeps the basis-dependent Choi operator behind `ChoiPositive b Φ`, while CP, Kraus, and Stinespring are basis-independent predicates. Later proofs can therefore switch representation without changing the channel itself.

Measurements

DEFINITION · IN PREPARATION

A finite-outcome POVM consists of positive effects resolving the identity. The real part is explicit because `Tr` is complex valued.

$$M_i \succeq 0, \quad \sum_i M_i = I, \qquad p(i \mid \rho, M) = \mathrm{Re}\mathrm{Tr}(\rho M_i).$$

```
structure POVM (ι) (ℋ) where
  effect : ι → L ℋ
  effect_nonneg (i) : 0 ≤ effect i
  sum_effect : ∑ i, effect i = I ℋ

noncomputable def POVM.probability (M) (ρ) (i) : ℝ :=
  (Tr (ρ * M i)).re
```

THEOREM · IN PREPARATION

```
lemma probability_nonneg (M : POVM ι ℋ) {ρ : L ℋ}
    (hρ : ρ.IsPositive) (i : ι) :
    0 ≤ M.probability ρ i

lemma sum_probability_of_isDensity (M : POVM ι ℋ)
    {ρ : L ℋ} (hρ : IsDensity ρ) :
    ∑ i, M.probability ρ i = 1
```

EXAMPLE · QUANTUM.EXAMPLES.BASICCONCEPTS · IN PREPARATION

```
example (b : OrthonormalBasis ι ℂ ℋ) : POVM ι ℋ :=
  POVM.ofOrthonormalBasis b
```

arXiv v1 **Sandwiched Rényi DPI · theorem and proof tools**

Why sandwiched Rényi DPI?

- **Concrete downstream need.** Coauthor Hayata Yamasaki proved, with Masahito Hayashi, a stronger generalized quantum Stein's lemma under weaker assumptions [3].
- **A known gap in formalization.** In the October 2025 report [4], sandwiched Rényi DPI was still listed among the assumed standard facts.
- **A genuinely quantum stress test.** Unlike the commuting classical case, noncommuting states prevent componentwise reduction; real powers, supports, trace inequalities, dilation, and unitary averaging must work together.

Proof tools in the preprint

THEOREM

The preprint develops the reusable chain needed by the DPI proof: Löwner-Heinz and logarithm monotonicity, Jensen and generalized perspectives, operator power means, and Lieb-Ando trace inequalities. Representative conclusions are

$$0 \preceq A \preceq B \Longrightarrow A^p \preceq B^p \; (0 \leq p \leq 1), \qquad 0 < A \preceq B \Longrightarrow \log A \preceq \log B.$$

```
theorem power_Icc_zero_one_operatorMonotoneOn_Ici
    (p : ℝ) (hp : p ∈ Set.Icc (0 : ℝ) 1) :
    OperatorMonotoneOn (𝒜 := 𝒜) (Set.Ici 0)
      (fun x ↦ x ^ p)

theorem log_operatorMonotoneOn_Ioi :
    OperatorMonotoneOn (𝒜 := 𝒜) (Set.Ioi 0) Real.log

theorem liebTrace_jointlyConcaveOn_pdSet
    {s : ℝ} (hs0 : 0 < s) (hs1 : s < 1) (K : B ℋ) :
    JointlyConcaveOn (pdSet (ℋ := ℋ)) (pdSet (ℋ := ℋ))
      (liebTraceMap (ℋ := ℋ) s K)
```

The statements live above matrices where possible and are deliberately more general than DPI-specific lemmas.

In Lean, monotonicity and convexity are predicates on functions over ordered C^*-algebras. Hilbert-space operators and matrices become instances of the same results, rather than separate proofs with duplicated coordinate calculations.

Rényi divergence

DEFINITION

For PSD ρ, σ with $\rho \neq 0$ and $\alpha > 0$, $\alpha \neq 1$, set $\beta_\alpha = (1-\alpha)/(2\alpha)$:

$$Q_\alpha(\rho \| \sigma) = \mathrm{Tr}\big[(\sigma^{\beta_\alpha} \rho \sigma^{\beta_\alpha})^\alpha\big], \qquad D_\alpha = \frac{1}{\alpha - 1} \log \frac{\mathrm{Re}\, Q_\alpha}{\mathrm{Re}\mathrm{Tr}\,\rho}.$$

```
noncomputable def sandwichedQuasi
    (α : ℝ) (ρ σ : L ℋ) : ℂ :=
  Tr (CFC.rpow
    (CFC.rpow σ ((1 - α) / (2 * α)) * ρ *
     CFC.rpow σ ((1 - α) / (2 * α))) α)

noncomputable def sandwichedRenyiDiv
    (α : ℝ) (ρ σ : L ℋ) : ℝ :=
  (1 / (α - 1)) *
    Real.log ((sandwichedQuasi α ρ σ).re / (Tr ρ).re)
```

The `EReal` extension is $+\infty$ when $\alpha > 1$ and support inclusion fails, or when $0 < \alpha < 1$, $\rho \neq 0$, and $\mathrm{Re}\, Q_\alpha = 0$. The zero operator is handled by the convention $D_\alpha^{\mathrm{NN}}(0 \| \sigma) = 0$.

Data processing

THEOREM

$$D_\alpha^{\mathrm{NN}}(\Phi(\rho) \| \Phi(\sigma)) \leq D_\alpha^{\mathrm{NN}}(\rho \| \sigma), \qquad \alpha \in [\tfrac{1}{2}, 1) \cup (1, \infty), \quad \Phi \text{ CPTP}.$$

```
theorem sandwichedRenyiDivNN_monotone
    (E : CPTP ℋ 𝒦) {α : ℝ}
    (hα_ge : (1 : ℝ) / 2 ≤ α) (hα_ne1 : α ≠ 1)
    {ρ σ : L ℋ} (hρ : 0 ≤ ρ) (hσ : 0 ≤ σ) :
    sandwichedRenyiDivNN α (E.toFun ρ) (E.toFun σ) ≤
      sandwichedRenyiDivNN α ρ σ
```

No trace-one assumption is needed: the Lean theorem is stated for arbitrary positive semidefinite operators. Its input class is therefore more general than the density-operator specialization.

Proof structure

PROOF ARCHITECTURE

1. Trace Young / reverse-Young inequalities give variational formulas for Q_α.
2. Generalized perspectives and Lieb-Ando give joint convexity or concavity.
3. Stinespring dilation, Haar twirling, Jensen, and tensor rules handle a CPTP map.
4. A separate regularization argument extends the positive-definite core to arbitrary PSD inputs.

After arXiv v1 **Independent extensions in private main**

Löwner theorem

THEOREM · PRIVATE MAIN · POST-PREPRINT

On the normalized interval, Löwner positivity yields an integral representation by a finite positive measure ν and operator monotonicity:

$$\left.\begin{array}{l} f(x) = f(0) + \displaystyle\int_{[-1,1]} \frac{x}{1+tx}\, d\nu(t), \quad x \in (-1,1), \\ \qquad \nu \geq 0, \quad \mathrm{supp}\,\nu \subseteq [-1,1] \end{array}\right\} \iff f \text{ is operator monotone on } (-1,1).$$

The 275-module development also covers Pick/Korányi theory, half-line and Kubo-Ando representations. Post-preprint work factors the direct and Löwner proofs through a common Hiai-Petz equivalence interface. Current `main` supplies Umegaki DPI from the sandwiched Rényi $\alpha \to 1^+$ limit; the Hiai-Petz interface provides alternative direct/Löwner routes. Downstream derivations, including SSA, depend only on the shared Umegaki-DPI statement and can be reused unchanged.

After arXiv v1 · continued **Entropy endpoints and applications**

Entropy

DEFINITION · PRIVATE MAIN · POST-PREPRINT

The private development defines von Neumann entropy by total continuous functional calculus and uses it as entropy under positivity and trace-one hypotheses.

$$S(\rho) = -\,\mathrm{Re}\mathrm{Tr}(\rho \log \rho).$$

```
noncomputable def vonNeumannEntropy (ρ : L ℋ) : ℝ :=
  -(Tr (ρ * CFC.log ρ)).re
```

The analytic instances are transported once and for all to the algebraic layer `L ℋ`; the definition and its continuous-functional-calculus logarithm are read directly on `L ℋ`, in line with every other statement-facing interface (`IsDensity`, CPTP, Rényi).

THEOREM · PRIVATE MAIN · POST-PREPRINT

The limits identify the Umegaki and max-relative entropies; support-aware `EReal`-valued DPI theorems are formalized for both endpoints.

```
theorem umegakiRelEntropyNN_monotone
    (E : CPTP ℋ 𝒦) {ρ σ : L ℋ}
    (hρ : 0 ≤ ρ) (hσ : 0 ≤ σ) :
    umegakiRelEntropyNN (E.toFun ρ) (E.toFun σ) ≤
      umegakiRelEntropyNN ρ σ
```

The parallel declaration `maxRelEntropyNN_monotone` gives the $\alpha = \infty$ endpoint, both with support-aware `EReal` values.

Strong subadditivity

APPLICATION OF THE PREPRINT THEOREM

Applying Umegaki DPI to a partial-trace channel gives

$$D_{\mathrm{U}}(\rho_{AB} \| \rho_A \otimes \rho_B) \leq D_{\mathrm{U}}(\rho_{ABC} \| \rho_A \otimes \rho_{BC}).$$

Expanding both sides and cancelling $S(\rho_A)$ yields

$$S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC}).$$

THEOREM · PRIVATE MAIN · POST-PREPRINT

Faithful-marginal assumptions occur only in an intermediate lemma and are removed by full-rank regularization and continuity.

```
theorem strongSubadditivity_of_state
    (ρ : L (ℋA ⊗[ℂ] (ℋB ⊗[ℂ] ℋC)))
    (hρ : 0 ≤ ρ)
    (hTr : Tr ρ = 1) :
    vonNeumannEntropy ρ +
        vonNeumannEntropy
          (QuantumChannel.traceOutRight (QuantumChannel.traceOutLeft ρ)) ≤
      vonNeumannEntropy (QuantumChannel.traceOutThird ρ) +
        vonNeumannEntropy (QuantumChannel.traceOutLeft ρ)
```

The final theorem assumes only positivity and trace one. Named general-state corollaries then provide

$$S(AB) \leq S(A) + S(B), \qquad I(A:B) \geq 0, \qquad S(A \mid BC) \leq S(A \mid B).$$

Contributions

1. **Coordinate-free quantum-information API.** Systems, states, channels, tensor products, partial traces, and CP representations use Hilbert-space operators without fixing matrix coordinates; statement-facing declarations share the `L` carrier.
2. **Reusable trace-inequality hierarchy.** Continuous functional calculus, Jensen, generalized perspectives, operator means, Lieb-Ando, Young inequalities, tensor powers, and Haar averaging become independent Lean interfaces.
3. **A formalization-friendly DPI proof.** Young / reverse-Young replace Euler-Lagrange optimization; the positive-definite analytic core is separated from the support-sensitive PSD extension.

AI-assisted methodology: humans design stable theorem statements and dependency structure; AI assists local proof search and code; Lean's kernel checks the resulting proof terms.

Formalization payoff: general-state SSA without faithful-marginal assumptions, more general PSD-input DPI statements, unified CP representations, and machine-checkable reusable definitions such as POVMs become explicit interfaces.

Related work

- **Generalized Stein lemma.** Hayashi-Yamasaki [3] corrected a gap in the 2010 proof; our theorem independently discharges the sandwiched Rényi DPI assumption recorded in the October 2025 report [4].
- **Lean-QuantumInfo.** It proves α ≥ 1 DPI for possibly singular density operators. Ours treats arbitrary PSD inputs and α ≥ 1/2, α ≠ 1 [2,4].
- **Formal quantum science.** Physlib covers entropy inequalities, quantum computation, error correction, and optimization; this project supplies coordinate-free operator-theoretic infrastructure [1].

Development status

BEYOND ARXIV V1 · PRIVATE DEVELOPMENT

- **Private main; public release in preparation:** direct-`L` entropy, endpoint DPI, general-state SSA, Löwner/Kubo-Ando, two Hiai-Petz routes, and route-neutral downstream entropy interfaces.
- **Branch/worktree:** POVMs/examples, spectral methods, thermodynamics/OPT, and unified TP representation equivalences.

Machine-checked build

510	4156	0
private-main Lean modules	top-level build jobs	sorry / admit / custom axiom

[1] K. Kasaura et al., arXiv:2607.05492 (2026). [2] R. L. Frank and E. H. Lieb, *J. Math. Phys.* 54, 122201 (2013). [3] M. Hayashi and H. Yamasaki, *Nature Phys.* 21, 1988 (2025). [4] A. Meiburg, L. A. Lessa, and R. R. Soldati, arXiv:2510.08672 (2025); github.com/Timeroot/Lean-QuantumInfo.