Computational hardness of estimating quantum entropies via binary entropy bounds

Yupan Liu

IC–QCC, École Polytechnique Fédérale de Lausanne

To appear in STACS 2026. Available on arXiv soon.

Zhejiang Insitute of Modern Physics, Zhejiang University, December 2025

1. Quantum state testing with respect to different entropy measures
2. Main results: Computational hardness of estimating entropies of rank-2 states
3. Proof techniques
4. Open problems

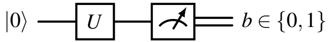
What is quantum state testing

Basic ingredients in quantum computation:

- **Quantum states.** An n-qubit quantum state $\rho \in \mathbb{C}^{N \times N}$, where $N = 2^n$, is an N-dimensional positive semi-definite (PSD) matrix such that $\mathrm{Tr}(\rho) = 1$.
- **Pure states.** An n-qubit state is *pure* if $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle \in \mathbb{C}^N$ and $\langle\psi|\psi\rangle = 1$.
  In the single-qubit case, $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ such that $|\alpha|^2 + |\beta|^2 = 1$, $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, and $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$.
- **Purification**. For any n-qubit quantum state ρ on $\mathcal{H}_\mathsf{A}$, there exists a $2n$-qubit pure state $|\psi\rangle$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ such that $\mathrm{Tr}_\mathsf{B}(|\psi\rangle\langle\psi|) = \rho$.
  For instance, let $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, then $\mathrm{Tr}_2(|\phi\rangle\langle\phi|) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = I/2$.
- **Quantum gate**. Elementary quantum gates G_i (from some universal gateset) are unitary matrices act on one or two qubits, e.g., $G_i \in \{\mathsf{CNOT}, \mathsf{Had}, \mathsf{T}\}$:

$$|0\rangle^{\otimes n} \xrightarrow{G_1} G_1\,|0\rangle^{\otimes n} \xrightarrow{G_2} G_2 G_1\,|0\rangle^{\otimes n} \rightarrow \cdots$$

- **Measurement**. Projective measurement in computational basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$:



Task: Quantum state testing via entropy approximation

Given a state-preparation circuit Q ("quantum devices") that prepares (the purification of) n-qubit quantum states $\rho \in \mathbb{C}^{N \times N}$. Decide whether $\mathrm{Ent}(\rho) \geq \tau_0(n)$ or $\mathrm{Ent}(\rho) \leq \tau_1(n)$.

What is quantum state testing (Cont.)

Task: Quantum state testing via entropy approximation

Given a state-preparation circuit Q ("quantum devices") that prepares (the purification of) n-qubit quantum states $\rho \in \mathbb{C}^{N\times N}$. Decide whether $\mathrm{Ent}(\rho) \geq \tau_0(n)$ or $\mathrm{Ent}(\rho) \leq \tau_1(n)$.

- Quantum devices Q can be given either as a query oracle (*black-box model*) or a sequence of $\mathrm{poly}(n)$ elementary quantum gates (*white-box model*).
- The most canonical choices of entropy measures are:
  - **von Neumann entropy** $\mathrm{S}(\rho) := -\mathrm{Tr}(\rho \ln \rho)$.
  - **Shannon entropy** $\mathrm{H}(D) := \sum_x -D(x) \ln D(x)$.
- Entropy *difference* problems, with respect to the quantity $\mathrm{Ent}(\rho_0) - \mathrm{Ent}(\rho_1)$, can be defined similarly and ask whether

$$\mathrm{Ent}(\rho_0) - \mathrm{Ent}(\rho_1) \geq g(n) \quad \text{or} \quad \mathrm{Ent}(\rho_0) - \mathrm{Ent}(\rho_1) \leq -g(n).$$

Typical goal. Minimize the "complexity" of ρ (or its corresponding Q):

Type of query access	Complexity measure
Black-box model	Query complexity (the number of queries to Q)
White-box model	Complexity class

Generalizations of the von Neumann entropy

<u>**Generalizations**</u>. There are two families of generalizations of the von Neumann entropy $\mathrm{S}(\rho)$, namely, the α-Rényi entropy $\mathrm{S}^{\mathtt{R}}_{\alpha}(\rho)$ and the q-Tsallis entropy $\mathrm{S}^{\mathtt{T}}_{q}(\rho)$:

$$\mathrm{S}^{\mathtt{R}}_{\alpha}(\rho) := \frac{\ln \mathrm{Tr}(\rho^{\alpha})}{1-\alpha} \quad \text{and} \quad \mathrm{S}^{\mathtt{T}}_{q}(\rho) := \frac{1-\mathrm{Tr}(\rho^{q})}{q-1}.$$

As the order approaches 1, these two generalizations converge to $\mathrm{S}(\rho)$.

<u>**von Neumann entropy (order 1)**</u>. The entropy approximation problem in this case is *hard*, with complexity depending (polynomially) on the rank r of the state:

- The query complexity for estimating $\mathrm{S}(\rho)$ to within additive error ε is $\widetilde{O}(r/\varepsilon^2)$ [Wang–Guan–Liu–Zhang–Ying'22] and $\Omega\big(\frac{\sqrt{r}}{\sqrt{\varepsilon}} + \frac{\ln r}{\varepsilon}\big)$ [Chen–Wang–Zhang'25].
- The promise problem QUANTUM ENTROPY APPROXIMATION (QEA), with respect to $\mathrm{S}(\rho)$, is NIQSZK-complete [Kobayashi'02, Chailloux–Ciocan–Kerenidis–Vadhan'07].
  - It is widely believed that BQP $\subsetneq$ NIQSZK.
- The *poly(n)-rank* variant LOWRANKQEA is BQP-complete: containment in [Wang–Guan–Liu–Zhang–Ying'22] and hardness in [**L.**–Wang'24].
  - <u>Containment</u>: a polynomial-time ("efficient") quantum algorithm that solves the problem.
  - <u>Hardness</u>: the problem requires *at least* the full power of a quantum computer to solve efficiently; namely, if you can solve this problem, you can solve all problems in BQP.

Generalizations of the von Neumann entropy (Cont.)

Prior quantum query complexity upper bounds are summarized as follows:

Order (α or q)	Quantum α-Rényi entropy	Quantum q-Tsallis entropy
$(0,1)$	$\mathrm{poly}(r, 1/\varepsilon)$ [WZL24]	$\mathrm{poly}(r, 1/\varepsilon)$ [WGLZY22]
1	$\mathrm{poly}(r, 1/\varepsilon)$ [WGLZY22]	
$(1,\infty)$	$\mathrm{poly}(r, 1/\varepsilon)$ [WZL24]	$\mathrm{poly}(1/\varepsilon)$ [**L.**–Wang'24]

We also summarize the prior work in terms of complexity classes:

- ⋆ For all $\alpha > 0$, LowRankRényiQEA$_\alpha$ is in BQP [Wang–Zhang–Li'22].
- ⋆ For all $q \in (0,1)$, LowRankTsallisQEA$_q$ is in BQP [WGLZY22].
- ⋆ For the order-1 case (von Neumann entropy), LowRankQEA is BQP-complete; containment follows from [WGLZY22], and hardness from [**L.**–Wang'24].
- ⋆ For all $q \in (1,2]$, TsallisQEA$_q$ is BQP-complete [**L.**–Wang'24].
- ⋆ For all $q > 2$, TsallisQEA$_q$ is in BQP [**L.**–Wang'24].

These results lead to the following questions:

1. How hard is the task of estimating α-Rényi or q-Tsallis entropy of quantum states for *all* positive order α or q?
2. Could LowRankRényiQEA$_\alpha$ $(\alpha > 0)$ and LowRankTsallisQEA$_q$ $(q > 0)$ both be BQP-hard, thus capturing the full power of quantum computation?

Main results

Let $\textsc{Rank2RényiQEA}_\alpha$ and $\textsc{Rank2TsallisQEA}_q$ denote the restricted versions of $\textsc{RényiQEA}_\alpha$ and $\textsc{TsallisQEA}_q$, where the state ρ has rank 2.

Theorem 1 (Hardness of estimating quantum entropies with positive orders).

1. For all real-valued $\alpha > 0$ and $\alpha = \infty$, $\textsc{Rank2RényiQEA}_\alpha$ is BQP-hard.
2. For all real-valued $q > 0$, $\textsc{Rank2TsallisQEA}_q$ is BQP-hard.

Combining Theorem 1 with prior quantum query complexity upper bounds implies:

Corollary 2. For all real-valued $\alpha > 0$, $\textsc{LowRankRényiQEA}_\alpha$ is BQP-complete.

Corollary 3. The following holds:

1. For all real-valued $q \in (0, 1]$, $\textsc{LowRankTsallisQEA}_q$ is BQP-complete.
2. For all real-valued $q > 1$, $\textsc{TsallisQEA}_q$ is BQP-complete.

Theorem 4. $\textsc{Rank2RényiQEA}_0$ and $\textsc{Rank2TsallisQEA}_0$ are NQP-complete.

- NP $\subseteq$ NQP by comparing definitions, while it is widely believed that NP $\not\subseteq$ BQP.

The BQP-hardness in Theorem 1 holds for the *smallest non-trivial* rank, as rank-1 states are pure states whose entropies are 0 for all orders.

Prior approaches via quantum entropy difference

The key quantity behind the prior approaches in [Ben-Aroya–Ta-Shma'07, **L.**'23] is the *quantum Jensen–Shannon divergence* $\mathrm{QJS}(\rho_0,\rho_1)$, introduced in [Majtey–Lamberti–Prato'05]:

$$\mathrm{QJS}(\rho_0,\rho_1) := \mathrm{S}\left(\frac{\rho_0+\rho_1}{2}\right) - \frac{\mathrm{S}(\rho_0)+\mathrm{S}(\rho_1)}{2} = \frac{1}{2}\cdot\left(\mathrm{S}\left(\frac{\rho_0+\rho_1}{2}\otimes\frac{\rho_0+\rho_1}{2}\right) - \mathrm{S}(\rho_0\otimes\rho_1)\right).$$

The BQP-hardness of LowRankQED (and LowRankQEA) follows from the facts:

1. The *pure-state variant* of the Quantum State Distinguishability Problem (PureQSD$[2/3,1/3]$), deciding whether $\mathrm{T}(|\psi_0\rangle\langle\psi_0|,|\psi_1\rangle\langle\psi_1|)$ is at least $2/3$ or at most $1/3$, is BQP-hard [Rethinasamy–Agarwal–Sharma–Wilde'21, Wang–Zhang'23].
2. The inequalities connect QJS to T [Fuchs–van de Graaf'99, Briët–Harremoës'09]:

$$\mathrm{H}\left(\frac{1}{2}\right) - \mathrm{H}\left(\frac{1-\mathrm{T}(\rho_0,\rho_1)}{2}\right) \leq \mathrm{QJS}(\rho_0,\rho_1) \leq \mathrm{H}\left(\frac{1}{2}\right)\cdot\mathrm{T}(\rho_0,\rho_1).$$

This approach can be generalized to TsallisQED$_q$ **($1\leq q\leq 2$).**

The key quantity is the *quantum Jensen–Tsallis divergence* $\mathrm{QJT}_q(\rho_0,\rho_1)$ for $1\leq q\leq 2$, introduced in [Briët–Harremoës'09], whose square root is a metric [Virosztek'19, Sra'19]:

$$\mathrm{QJT}_q(\rho_0,\rho_1) := \mathrm{S}_q^{\mathtt{T}}\left(\frac{\rho_0+\rho_1}{2}\right) - \frac{\mathrm{S}_q^{\mathtt{T}}(\rho_0)+\mathrm{S}_q^{\mathtt{T}}(\rho_1)}{2}.$$

Using the *joint convexity* of QJT_q [Chen–Tropp'13, Virosztek'19], [**L.**–Wang'24] establishes:

$$\mathrm{H}_q^{\mathtt{T}}\left(\frac{1}{2}\right) - \mathrm{H}_q^{\mathtt{T}}\left(\frac{1-\mathrm{T}(\rho_0,\rho_1)}{2}\right) \leq \mathrm{QJT}_q(\rho_0,\rho_1) \leq \mathrm{H}_q^{\mathtt{T}}\left(\frac{1}{2}\right)\cdot\mathrm{T}(\rho_0,\rho_1)^q.$$

Establishing the hardness via binary entropy bounds

We start with a new approach that establishes the BQP-hardness of RANK2QEA. This approach is based on two key observations:

1. The 2-Tsallis entropy of a rank-2 state $\frac{1}{2}(|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|)$ can be expressed as the 2-Tsallis binary entropy, and this coincidence naturally extends to all $q > 0$:
$$\mathrm{S}_2^{\mathtt{T}}\left(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\right) = \frac{1 - |\langle\psi_0|\psi_1\rangle|^2}{2} = \mathrm{H}_2^{\mathtt{T}}\left(\frac{1 - \langle\psi_0|\psi_1\rangle}{2}\right).$$
2. The following bounds on the Shannon binary entropy in [Lin'91, Topsøe'01]:
$$2\mathrm{H}\left(\frac{1}{2}\right) \cdot \mathrm{H}_2^{\mathtt{T}}(x) \leq \mathrm{H}(x) \leq \sqrt{2}\mathrm{H}\left(\frac{1}{2}\right) \cdot \sqrt{\mathrm{H}_2^{\mathtt{T}}(x)}.$$

Since PURE-STATE INFIDELITY ESTIMATION (PUREINFIDELITY$\left[\frac{2}{3}, \frac{1}{3}\right]$), deciding whether $1 - |\langle\psi_0|\psi_1\rangle|^2$ is at least $2/3$ or at most $1/3$, is BQP-hard [Rethinasamy–Agarwal–Sharma–Wilde'21], it follows that both RANK2TSALLISQEA$_2$ and RANK2RÉNYIQEA$_2$ are BQP-hard.

The inequalities relating the order-2 binary entropy to Shannon binary entropy (Step 2) can be extended to *all* positive orders! This is the main technical contribution of our work and explains why rank-2 quantum states suffice to capture the BQP-hardness.

Establishing the hardness via binary entropy bounds (Cont.)

The BQP-hardness of RANK2RÉNYIQEA$_\alpha$ can then be established via the following inequalities that relate $\mathrm{H}_2^{\mathrm{R}}(x)$ to $\mathrm{H}_\alpha^{\mathrm{R}}(x)$:

Range of α	Hardness	Reduction from	New inequalities
$0<\alpha<1$	BQP-hard Theorem 1(1)	RANK2RÉNYIQEA$_2$	$\mathrm{H}_2^{\mathrm{R}}(x) \leq \mathrm{H}_\alpha^{\mathrm{R}}(x)$ $\mathrm{H}_\alpha^{\mathrm{R}}(x) \leq \ln(2)^{1-\frac{\alpha}{2}} \cdot \mathrm{H}_2^{\mathrm{R}}(x)^{\frac{\alpha}{2}}$ [Beck–Schögl'93, Sec 5.3]
$1 \leq \alpha < 2$	BQP-hard Theorem 1(1)	RANK2RÉNYIQEA$_2$	
$\alpha = 2$	BQP-hard Theorem 1(1)	PUREINFIDELITY [RASW'21]	None
$\alpha \in (2,\infty]$	BQP-hard Theorem 1(1)	RANK2RÉNYIQEA$_2$	$\frac{\alpha}{2(\alpha-1)} \cdot \mathrm{H}_2^{\mathrm{R}}(x) \leq \mathrm{H}_\alpha^{\mathrm{R}}(x) \leq \mathrm{H}_2^{\mathrm{R}}(x)$ [Beck–Schögl'93, Sec 5.3]

Establishing the hardness via binary entropy bounds (Cont.^{2})

The BQP-hardness of RANK2TSALLISQEA$_q$ can then be established via the following inequalities that relate $\mathrm{H}_2^{\mathtt{T}}(x)$ to $\mathrm{H}_q^{\mathtt{T}}(x)$:

Range of q	Hardness	Reduction from	New inequalities
$0 < q < 1$	BQP-hard Theorem 1(2)	RANK2TSALLISQEA$_2$	$2\mathrm{H}_q^{\mathtt{T}}\left(\frac{1}{2}\right) \cdot \mathrm{H}_2^{\mathtt{T}}(x) \leq \mathrm{H}_q^{\mathtt{T}}(x)$ $\mathrm{H}_q^{\mathtt{T}}(x) \leq 2^{\frac{q}{2}}\mathrm{H}_q^{\mathtt{T}}\left(\frac{1}{2}\right) \cdot \left(\mathrm{H}_2^{\mathtt{T}}(x)\right)^{\frac{q}{2}}$ [L.–Wang'24]
$1 \leq q < 2$	BQP-hard Theorem 1(2)	RANK2TSALLISQEA$_2$	
$q = 2$	BQP-hard Theorem 1(2)	PUREINFIDELITY [RASW'21]	None
$2 < q \leq 3$	BQP-hard Theorem 1(2)	RANK2TSALLISQEA$_2$	$\frac{q}{2(q-1)} \cdot \mathrm{H}_2^{\mathtt{T}}(x) \leq \mathrm{H}_q^{\mathtt{T}}(x) \leq 2\mathrm{H}_q^{\mathtt{T}}\left(\frac{1}{2}\right) \cdot \mathrm{H}_2^{\mathtt{T}}(x)$
$q \in (3, \infty)$	BQP-hard Theorem 1(2)	RANK2TSALLISQEA$_2$	$2\mathrm{H}_q^{\mathtt{T}}\left(\frac{1}{2}\right) \cdot \mathrm{H}_2^{\mathtt{T}}(x) \leq \mathrm{H}_q^{\mathtt{T}}(x)$ $\mathrm{H}_q^{\mathtt{T}}(x) \leq \frac{q}{2(q-1)} \cdot \mathrm{H}_2^{\mathtt{T}}(x)$ [L.–Wang'24]

The additional row links to the *normalized* q-Tsallis entropy $\widetilde{H}_q^{\mathtt{T}}(x) := \mathrm{H}_q^{\mathtt{T}}(x)/\mathrm{H}_q^{\mathtt{T}}(1/2)$ (cf. [Daróczy'70]), whose monotonicity *changes* at some point $q^*(x) \in [2,3]$.

Conclusions and open problems

Take-home messages on our work

For ***all*** **positive** orders, estimating α-Rényi or q-Tsallis entropies of **rank-**2 quantum states, *the smallest non-trivial rank*, is BQP-hard.

Discussion and open problems

Two limitations of our new approach are as follows:

- Our approach works only when quantum entropy values and the promise gap $\tau_0 - \tau_1$ are both *constant*. Otherwise, reductions based on inequalities, such as $\mathrm{S}^{\mathrm{R}}_{\infty}(\rho) \leq \mathrm{S}^{\mathrm{R}}_{\alpha}(\rho) \leq \frac{\alpha}{\alpha-1}\mathrm{S}^{\mathrm{R}}_{\infty}(\rho)$ for all $\alpha > 1$, break down for sufficiently large n.
- A complexity-theoretic barrier is that reductions between different orders do not hold in general. Noting that RÉNYIQEA$_{\infty}$ is coSBP-complete [Watson'12] and EA is NISZK-complete [Goldreich–Vadhan'99], such reductions would yield

  $$\text{coNP} \subseteq \text{coSBP} \subseteq \text{NISZK} \subseteq \text{SZK} \subseteq \text{AM} \cap \text{coAM}.$$

  These inclusions would collapse PH to its second level [Boppana–Håstad–Zachos'87].

Question: Is it possible to establish a complexity-theoretic classification theorem for estimating the quantum (α-Rényi or q-Tsallis) entropies?

Thanks!

Generalizations of the von Neumann entropy: Prior work

α-Rényi entropy ($\alpha > 0$). The corresponding entropy approximation problems are also *hard*, with complexity depending (polynomially) on the rank r of the state:

- The query complexity for estimating $\mathrm{S}^{\mathrm{R}}_{\alpha}(\rho)$ to within additive error ε is $\widetilde{O}(r^{\frac{1}{\alpha}}/\varepsilon^{1+\frac{1}{\alpha}})$ for $0 < \alpha < 1$ and $\widetilde{O}(r/\varepsilon^{1+\frac{1}{\alpha}})$ for $\alpha > 1$ [Wang–Zhang–Li'22], while the lower bounds depend polynomially on r and $1/\varepsilon$ (e.g., [Wang–Guan–Liu–Zhang–Ying'22]).
- For $\alpha \in (0,1) \cup (1,\infty)$, the *low-rank* variant of the QUANTUM α-RÉNYI ENTROPY APPROXIMATION (LOWRANKRÉNYIQEA$_\alpha$) is in BQP [Wang–Zhang–Li'22].

q-Tsallis entropy ($0 < q < 1$). The entropy approximation problems are *hard*:

- For all $q \in (0,1)$, the query complexity for estimating $\mathrm{S}^{\mathrm{T}}_{q}(\rho)$ to within additive error ε is $\mathrm{poly}(r, 1/\varepsilon)$ [Wang–Guan–Liu–Zhang–Ying'22], specifically $\widetilde{O}(r^{\frac{3-q^2}{2q}}/\varepsilon^{\frac{3+q}{2q}})$.
- For all $q \in (0,1)$, the *low-rank* variant of the QUANTUM q-TSALLIS ENTROPY APPROXIMATION (LOWRANKTSALLISQEA$_q$) is in BQP [Wang–Guan–Liu–Zhang–Ying'22].

q-Tsallis entropy ($q > 1$). The corresponding entropy approximation problems are *easy*, with *rank-independent* complexity:

- The query complexity for estimating $\mathrm{S}^{\mathrm{T}}_{q}(\rho)$ is $O(1/\varepsilon^{1+\frac{1}{q-1}})$ for $q > 1$ [**L.**–Wang'24], while it is $\Omega(1/\varepsilon^{\frac{1}{2(q-1)}})$ for $1 < q < \frac{3}{2}$ and $\Omega(1/\varepsilon)$ for $q \geq \frac{3}{2}$ [Chen–Wang–Zhang'25].
- For all $q \in (1,2]$, TSALLISQEA$_q$ and TSALLISQED$_q$ are BQP-complete, while the BQP containment also holds for $q > 2$ [**L.**–Wang'24].