On estimating the trace of quantum state powers

Yupan Liu [1] Qisheng Wang [2,1]

[1] Graduate School of Mathematics, Nagoya University

[2] School of Informatics, University of Edinburgh

To appear in SODA 2025. Available on arXiv soon.

SEAS, Harvard University, October 2024

What is quantum state testing

Task: Quantum state testing

Given two quantum devices Q_0 and Q_1 that prepare n-qubit quantum states $\rho_0 \in \mathbb{C}^{N\times N}$ and $\rho_1 \in \mathbb{C}^{N\times N}$, respectively. Decide whether $\mathrm{dist}(\rho_0,\rho_1) \leq \varepsilon_1$ or $\mathrm{dist}(\rho_0,\rho_1) \geq \varepsilon_2$.

Three types of access to quantum devices Q_b for $b \in \{0,1\}$ are considered:

- **Sample access**: Receive copies of the state ρ_b from the device Q_b.
- **Query access**: Q_b denotes the state-preparation circuit of the state ρ_b:
  - **Black-box model**. Q_b is given as a black box (oracle).
  - **White-box model**. The (gate-based) description of Q_b is provided.

Typical goal. Minimize the "complexity" of ρ_b (or its corresponding Q_b) for $b \in \{0,1\}$:

Type of access	Complexity measure
Sample access	Sample complexity (the number of copies)
Query access (black-box)	Query complexity (the number of queries)
Query access (white-box)	Complexity class

In this talk: We focus on query access, primarily the white-box model (i.e., a promise problem), while addressing all three types of access in our work.

Quantum state testing: Hard and easy examples

Quantum state testing is *hard* in general, with complexity (linearly) depending on the dimension N (or rank r), through some distance-like measures make these task *easy*.

Hard examples. Quantum state testing with respect to *von Neumann entropy*:

- QUANTUM ENTROPY DIFFERENCE (QED): $S(\rho_0) - S(\rho_1)$ is $\geq 1/2$ or $\leq -1/2$.
  - [Ben Aroya-Schwartz-Ta-Shma'08] QED is QSZK-complete.
- QUANTUM ENTROPY APPROXIMATION (QEA). $S(\rho)$ is $\geq t(n) + 1/2$ or $\leq t(n) - 1/2$.
  - [BASTS08, Chailloux-Ciocan-Kerenidis-Vadhan'08] QEA is NIQSZK-complete.
  - [Bun-Kothari-Thaler'18] Query complexity lower bound for QED and QEA is $\Omega(\sqrt{N})$.

Easy example. PURITY ESTIMATION: Decide whether $\mathrm{Tr}(\rho^2)$ is $\geq 2/3$ or $\leq 1/3$.

- [Buhurman-Cleve-Watrous-de Wolf'01] Query complexity for approximating $\mathrm{Tr}(\rho^2)$ to within additive error ε is $O(1/\varepsilon)$, with BQP containment in the white-box setting.
- [Ekert-Alves-Oi-Horodecki-Horodecki-Lwek'02] The same bound and the BQP containment apply for estimating $\mathrm{Tr}(\rho^q)$ for integer $q > 1$.

These examples raise questions on estimating the trace of quantum state powers:

1. Is there an efficient quantum algorithm for estimating $\mathrm{Tr}(\rho^q)$ for *non-integer* $q > 1$?
2. Is estimating the trace of quantum state powers, e.g., $\mathrm{Tr}(\rho^2)$, BQP-*complete*?

Quantum state testing with respect to quantum q-Tsallis entropy

Quantum q-Tsallis entropy: power quantum entropy of order q

$$\mathrm{S}_q(\rho) = \frac{1-\mathrm{Tr}(\rho^q)}{q-1} = -\mathrm{Tr}(\rho^q \ln_q(\rho)), \text{ where } \ln_q(x) := \frac{1-x^{1-q}}{q-1}.$$

As $q \to 1$, the von Neumann entropy is recovered: $\mathrm{S}_q(\rho) = \mathrm{S}(\rho)$ and $\ln_q(x) = \ln(x)$.

Tsallis entropy has been independently rediscovered several times: [Havrda-Charvát'67, Daróczy'70, Tsallis'88], with the quantum version introduced in [Raggio'95].

Quantum state testing with respect to quantum Tsallis entropy:

- QUANTUM q-TSALLIS ENTROPY DIFFERENCE (TSALLISQED$_q$): Decide whether $\mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1) \geq 0.001$ or $\mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1) \leq -0.001$.
- QUANTUM q-TSALLIS ENTROPY APPROXIMATION (TSALLISQEA$_q$): Decide whether $\mathrm{S}_q(\rho) \geq t(n) + 0.001$ or $\mathrm{S}_q(\rho) \leq t(n) - 0.001$.

Why investigate $\mathrm{S}_q(\rho)$ for non-integer q?

1. Since $\mathrm{S}_q(\rho) \leq \mathrm{S}(\rho)$, $\mathrm{S}_{q=1+\varepsilon}(\rho)$ serves as a reasonable lower bound for $\mathrm{S}(\rho)$.
   "Hardness of approximating von Neumann entropy"?
2. $\mathrm{H}_{q=3/2}(p)$ captures systems where both frequent and rare events matter. Meanwhile, estimating $\mathrm{S}_q(\rho)$ for non-integer $1 < q < 2$ seems to be challenging:
   - $H_{q=2}(p)$, also known as *Gini impurity*, is very sensitive to rare events.
   - Examples in fluid dynamics: modeling velocity changes in turbulent flows [Beck'02].

Main result (upper bounds): Quantum estimator for q-Tsallis entropy

Theorem 1 (Quantum estimator for q-Tsallis entropy).
Given quantum query access to the state-preparation circuit Q of an n-qubit state ρ, for any $q \geq 1+\Omega(1)$, there exists a quantum algorithm that estimates $\mathrm{S}_q(\rho)$ to within additive error ε with query complexity $O(1/\varepsilon^{1+\frac{1}{q-1}}) = \mathrm{poly}(1/\varepsilon)$.

- If the description of the state-preparation circuit is of size $L(n)$, the time complexity is $O(L/\varepsilon^{1+\frac{1}{q-1}}) = \mathrm{poly}(n, 1/\varepsilon)$.
  - As a corollary, for any $q \geq 1+\Omega(1)$, TSALLISQED$_q$ and TSALLISQEA$_q$ are in BQP.
- Using the samplizer [Wang-Zhang'24], allowing a quantum query-to-sample simulation, the sample complexity required to estimate $\mathrm{S}_q(\rho)$ is $\widetilde{O}(1/\varepsilon^{3+\frac{2}{q-1}})$.

Prior works have complexity depending on the dimension $N = 2^n$ or the rank r of ρ:

1. Dimension dependence: [Acharya-Issa-Shende-Wagner'19].
2. Rank dependence: [Wang-Guan-Liu-Zhang-Ying'22, Wang-Zhang-Li'22, Wang-Zhang'24].

Main results (lower bounds): Hardness for TsallisQED$_q$ and TsallisQEA$_q$

Let ConstRankTsallisQED$_q$ and ConstRankTsallisQEA$_q$ be restricted variants of TsallisQED$_q$ and TsallisQEA$_q$, respectively, where the rank of the state(s) is $\leq O(1)$.

Theorem 2 (Computational hardness for TsallisQED$_q$ and TsallisQEA$_q$).

The promise problems TsallisQED$_q$ and TsallisQEA$_q$ capture the computational power of respective complexity classes, depending on the regime of q:

1. **Easy regimes**. For $q \in [1,2]$, ConstRankTsallisQED$_q$ and ConstRankTsallisQEA$_q$ are BQP-hard. The following corollaries holds:
   - For $1+\Omega(1) \leq q \leq 2$, TsallisQED$_q$ and TsallisQEA$_q$ are BQP-complete.
   - Purity Estimation is BQP-complete.
2. **Hard regimes**. For $q \in \left(1, 1+\frac{1}{n-1}\right]$, TsallisQED$_q$ is QSZK-hard under Karp reduction, and consequently, TsallisQEA$_q$ is QSZK-hard under Turing reduction. For $q = 1+\frac{1}{n-1}$, TsallisQEA$_q$ is NIQSZK-hard under Karp reduction.

Our reductions for the hard regimes also leads to query and sample complexity lower bounds for estimating $S_q(\rho)$ to within additive error ε :

The regime of q	Query complexity	Sample complexity
$q \geq 1+\Omega(1)$	$\Omega(1/\sqrt{\varepsilon})$	$\Omega(1/\varepsilon)$
$1 < q \leq 1+\frac{1}{n-1}$	$\Omega(r^{1/3})$	$\Omega(r^{2/3})$

Summary: "Hardness of approximating von Neumann entropy"

Quick summary for estimating $S_q(\rho)$ for $q=1$ (von Neumann entropy) and $q>1$:

	$q=1$	$1<q\leq 1+\frac{1}{n-1}$	$1+\Omega(1)\leq q\leq 2$	$q>2$
TSALLISQED$_q$	QSZK-complete [BASTS08]	QSZK-hard Theorem 2(2)	BQP-complete Theorem 1 & Theorem 2(1)	in BQP Theorem 1
TSALLISQEA$_q$	NIQSZK-complete [BASTS08,CCKV08]	NIQSZK-hard* Theorem 2(2)	BQP-complete Theorem 1 & Theorem 2(1)	in BQP Theorem 1

A sharp phase transition occurs between the case of $q=1$ and constant $q>1$.

Why is the regime $q\geq 1+\Omega(1)$ computationally easy?

Let's focus on PURITY ESTIMATION ($q=2$). Let $\{\lambda_k\}_{k\in[2^n]}$ be eigenvalues of an n-qubit state ρ. For any state $\widehat{\rho}$ having eigenvalues at most $1/n$, we have $\mathrm{Tr}(\widehat{\rho}^2)=\sum_k \lambda_k^2\leq 1/n$. Hence, *zero* serves as a good estimate of $\mathrm{Tr}(\widehat{\rho}^2)$ to within additive error $1/3$.

Only (sufficiently) large eigenvalues contribute to the estimate of $\mathrm{Tr}(\rho^2)$!

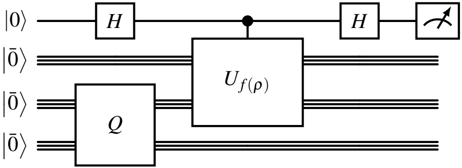
Q: How to estimate $\sum_{k\in\mathcal{I}_{\mathrm{large}}}\lambda^2$, where $\mathcal{I}_{\mathrm{large}}$ is the index set of large eigenvalues λ_k?

- For integer $q\geq 2$, SWAP test-like techniques [BCWdW01,EAO+02] provide a solution.
- For non-integer $q\geq 1+\Omega(1)$, our result (Theorem 1) solves the problem.

1. Quantum state testing with respect to the trace of quantum state powers
2. Main results: Upper and lower bounds
3. Proof techniques: Uniform polynomial approximation and QJT_q-based reductions
4. Open problems

BQP containment for the regime $q \geq 1 + \Omega(1)$

We begin with a procedure that accepts with probability $\frac{1}{2}\left(1 + \mathrm{Tr}(\rho U_{f(\rho)})\right)$, utilizing the Hadamard test [Kitaev'95, Aharonov-Jones-Landau'06]:



- $U_{f(\rho)}$ is an *approximate* unitary block-encoding of $f(\rho) = \rho^{q-1}$, constructed from the state-preparation circuit Q and implemented using quantum singular value transformation [Gilyén-Su-Low-Wiebe'19], with an appropriate polynomial approximation $P_d(x)$ of $f(x) = x^{q-1}$.
- This approach has been applied to estimate fidelity [Gilyén-Poremba'22], trace distance [Wang-Zhang'23, Le Gall-**L.**-Wang'23], and von Neumann entropy [Le Gall-**L.**-Wang'23, Wang-Zhang'24].
- The acceptance probability of this procedure can be further *boosted*, to say at least $2/3$ for *yes* instances, through quantum amplitude estimation.

BQP containment (Cont.): Removing the rank dependence

Rank dependence in prior works. Prior works based on this approach require time (or query) complexity that depends at least *linearly* on the rank. Specifically,

$$\begin{aligned}|\mathrm{Tr}(\rho f(\rho) - \mathrm{Tr}(\rho P_d(\rho))| &\leq \sum_{0\leq\lambda_j<\delta} \left|\lambda_j f(\lambda_j) - \lambda_j P_d(\lambda_j)\right| + \sum_{\lambda_j\geq\delta} \left|\lambda_j f(\lambda_j) - \lambda_j P_d(\lambda_j)\right| \\ &\leq r\cdot\mathrm{poly}(\delta) + O(\varepsilon).\end{aligned}$$

To ensure that the last line is bounded by $O(\varepsilon)$, δ must be *sufficiently small*, e.g., $1/\mathrm{poly}(r)$, introducing rank dependence. The target function $f(x)$ is approximated by a polynomial $P_d(x)$ of degree $d = O\big(\frac{1}{\delta}\log\frac{1}{\varepsilon}\big)$ such that

$$\max_{x\in[\delta,1]} |P_d(x) - f(x)| \leq \varepsilon \quad \text{and} \quad \max_{x\in[-1,1]} |P(x)| \leq 1.$$

Removing the rank dependence. Instead, we need a polynomial that *uniformly* approximates $f(x)$. The best uniform (polynomial) approximation of x^q was investigated in [Bernstein'38], with a non-constructive proof in [Timan'63], satisfies:

$$\max_{x\in[0,1]} \left|P^*_{d'}(x) - x^q\right| \to 1/d'^q, \quad \text{as } d' \to \infty.$$

The remaining challenge is to make the coefficients of $P^*_{d'}(x)$ *efficiently computable*. This can be achieved using the asymptotically best uniform (polynomial) approximation $\widehat{P}_{\hat{d}}(x)$, particularly via Chebyshev truncation and the de La Vallée Poussin partial sum:

$$\max_{x\in[0,1]} \left|\widehat{P}_{\hat{d}}(x) - x^q/2\right| \leq \varepsilon \quad \text{and} \quad \max_{x\in[-1,1]} |P(x)| \leq 1, \quad \text{where } \hat{d} = O(1/\varepsilon^{1/q}).$$

Hardness results via QJT_q-based reductions

The key quantity underlying our proof is the quantum q-Jensen-(Shannon-)Tsallis divergence, as defined in [Briët-Harremoës'09]:

$$\mathsf{QJT}_q(\rho_0,\rho_1) := \frac{1}{2}\left(\mathrm{S}_q(\rho_0)+\mathrm{S}_q(\rho_1)\right) - \mathrm{S}_q\left(\frac{\rho_0+\rho_1}{2}\right).$$

Specifically, we focus on reductions from restricted versions of quantum state testing with respect to the trace distance (QSD), particularly decide whether $\mathrm{T}(\rho_0,\rho_1)$ is at least $1-\varepsilon(n)$ or at most $\varepsilon(n)$, to TSALLISQED$_q$ or TSALLISQEA$_q$:

Problem	Regime of q	Reduction from	New inequalities
ConstRank-TsallisQED$_q$	$1 \leq q \leq 2$	PUREQSD is BQP-hard [RASW23]	$\mathrm{H}_q\left(\frac{1}{2}\right)-\mathrm{H}_q\left(\frac{1-\mathrm{T}}{2}\right) \leq \mathsf{QJT}_q \leq \mathrm{H}_q\left(\frac{1}{2}\right)\mathrm{T}^q$
TSALLISQED$_q$	$1 \leq q \leq 1+\frac{1}{n-1}$	QSD is QSZK-hard [Wat02, Wat09]	$\mathrm{H}_q\left(\frac{1}{2}\right)-\mathrm{H}_q\left(\frac{1-\mathrm{T}}{2}\right) \leq \mathsf{QJT}_q$
TSALLISQEA$_q$	$q = 1+\frac{1}{n-1}$	QSCMM is NIQSZK-hard [Kob03, BASTS10, CCKV08]	$\left(1-\mathrm{T}-\frac{1}{2^n}\right)\ln_q(2^n) \leq \mathrm{S}_q \leq \ln_q(2^n(1-\mathrm{T}))$

Our upper bound for Tsallis binary entropy is also crucial: $\mathrm{H}_q(x) \leq \mathrm{H}_q\left(\frac{1}{2}\right)\sqrt{x(1-x)}$.

Hardness results via QJT_q-based reductions (Cont.)

Proof Sketch (New Inequalities between QJT_q and T). We follow the approach for proving the inequalities for QJS from [Briët-Harremoës'09]. The key step is to establish the data-processing inequality $\mathrm{QJT}_q(\Phi(\rho_0),\Phi(\rho_1)) \leq \mathrm{QJT}_q(\rho_0,\rho_1)$ for $1 \leq q \leq 2$:

- For $q=1$ (QJS), this follows from $\mathrm{QJS}(\rho_0,\rho_1) = \frac{1}{2}\big(\mathrm{D}\big(\rho_0 \| \frac{\rho_0+\rho_1}{2}\big) + \mathrm{D}\big(\rho_1 \| \frac{\rho_0+\rho_1}{2}\big)\big)$.
- For $1 < q \leq 2$, we need the joint convexity for QJT_q [Chen-Tropp'14, Virosztek'17]:

$$\mathrm{QJT}_q\big((1-\lambda)\rho_0 + \lambda\rho_0', (1-\lambda)\rho_1 + \lambda\rho_1'\big) \leq (1-\lambda)\mathrm{QJT}_q\big(\rho_0,\rho_1\big) + \lambda \mathrm{QJT}_q(\rho_0',\rho_1').$$

Proof Sketch (Reductions from variants of QSD to (ConstRank)TsallisQED$_q$).

❶ **Pure-state reductions** are inspired by [L.'23], namely QJT_q can be viewed as a *distance version* of $\mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1)$ for $1 \leq q \leq 2$. Consider the following states

$$\rho_0' := (p_0 |0\rangle\langle 0| + p_1 |1\rangle\langle 1|) \otimes \frac{1}{2}(|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|),$$
$$\rho_1' := \frac{1}{2}|0\rangle\langle 0| \otimes |\psi_0\rangle\langle\psi_0| + \frac{1}{2}|1\rangle\langle 1| \otimes |\psi_1\rangle\langle\psi_1|.$$

Using the pseudo-additivity and the joint entropy theorem for S_q, we obtain

$$\mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1') = (1-(q-1)\mathrm{H}_q(p_0)) \cdot \mathrm{QJT}_q(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) + \mathrm{H}_q(p_0) - \mathrm{H}_q\big(\tfrac{1}{2}\big).$$

By choosing a suitable $p_0 \in (0,1/2)$, the bounds for $\mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1')$ follow from the inequalities between QJT_q and the trace distance.

❷ **Mixed-state reductions**, inspired by [BASTS'08], are a bit more complicated. The upper bound for $\mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1')$ now needs the Fannes' inequality for QJT_q [Zhang'07]:

$$\forall q > 1, \quad \big|\mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1)\big| \leq \mathrm{T}(\rho_0,\rho_1)^q \cdot \ln_q(2^n - 1) + \mathrm{H}_q(\mathrm{T}(\rho_0,\rho_1)).$$

Conclusions and open problems

Take-home messages on our work

1. For the regime $q \geq 1+\Omega(1)$, estimating the quantum Tsallis entropy $\mathrm{S}_q(\rho)$, equivalently the trace of quantum state powers, is computationally *easy* and has query or sample complexity that is *independent* of the rank of the state.
   This provides an efficiently computable lower bound for the von Neumann entropy!
2. For the regime $1 < q \leq 1+\frac{1}{n-1}$, estimating the quantum Tsallis entropy $\mathrm{S}_q(\rho)$ is computationally *hard*:
   - The white-box problems cannot be solved efficiently unless BQP $=$ QSZK;
   - The rank dependence in query or sample complexity is *unavoidable* in black-box settings.

   This can be interpreted as "hardness of approximating the von Neumann entropy".

Open problems

1. Are there more applications for estimating quantum q-Tsallis entropy $\mathrm{S}_q(\rho)$ in the regime $1 < q < 2$, which has previously been challenging to compute?
2. Can we improve query and sample complexity bounds for the regime $q \geq 1+\Omega(1)$?
3. What are the computational complexity and hardness for estimating $\mathrm{S}_q(\rho)$ for the regime $0 < q < 1$? Can we show that TsallisQED$_q$ (or TsallisQEA$_q$) for the regime $1 < q < 1+\frac{1}{n-1}$ is contained in QSZK (or NIQSZK)?

Thanks!