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

Available on arXiv:2410.13559

SODA 2025, New Orleans

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

What is quantum state testing

An n-qubit quantum state ρ is a $N \times N$ positive semi-definite matrix satisfying $\mathrm{Tr}(\rho) = 1$.

Task: Quantum state testing

Given two quantum devices Q_0 and Q_1 that prepare n-qubit quantum states ρ_0 and ρ_1, respectively. Decide whether $\mathrm{dist}(\rho_0, \rho_1) \leq \varepsilon_1$ or $\mathrm{dist}(\rho_0, \rho_1) \geq \varepsilon_2$.

Consider query access to quantum devices Q_b for $b \in \{0,1\}$, where each device 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
Query access (black-box)	Query complexity (the number of queries)
Query access (white-box)	Complexity class

In this talk: We focus on the white-box model (i.e., a promise problem), while addressing three types of access (including *sample 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): $\mathrm{S}(\rho_0) - \mathrm{S}(\rho_1)$ is $\geq 1/2$ or $\leq -1/2$.
  - [Ben Aroya-Schwartz-Ta-Shma'08] QED is QSZK-complete.
  - [Bun-Kothari-Thaler'18] Query complexity lower bound for QED is $\widetilde{\Omega}(\sqrt{N})$.

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 $q > 1$.

Purity is closely related to the *quantum linear entropy* $\mathrm{S}_L(\rho) = 1 - \mathrm{Tr}(\rho^2)$.

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 Neumman entropy is recovered: $\mathrm{S}_{q=1}(\rho) = \mathrm{S}(\rho)$ and $\ln_{q=1}(x) = \ln(x)$.
When $q = 2$, the quantum linear entropy is recovered: $\mathrm{S}_{q=2}(\rho) = \mathrm{S}_L(\rho) = 1 - \mathrm{Tr}(\rho^2)$.

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 $\mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1) \leq -0.001$.

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:
   - Examples in fluid dynamics: modeling velocity changes in turbulent flows [Beck'02].

Main results (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 $O(1/\varepsilon^{1+\frac{1}{q-1}}) = \mathrm{poly}(1/\varepsilon)$.

- As a corollary, for any $q \geq 1 + \Omega(1)$, TSALLISQED$_q$ is in BQP.

Prior works have complexity (at least linearly) 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].

Our work provides an *exponential* improvement over the prior best results!

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

Let ConstRankTsallisQED$_q$ be a restricted variant of TsallisQED$_q$, where the rank of the states is at most $O(1)$.

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

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

1. **Easy regimes**. For $q \in [1,2]$, ConstRankTsallisQED$_q$ is BQP-hard. The following corollaries holds:
   - For $1+\Omega(1) \leq q \leq 2$, TsallisQED$_q$ is 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.

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

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

Summary: "A dichotomy theorem on approximating von Neumann entropy"

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

	$q=1$	$1<q\le 1+\frac{1}{n-1}$	$1+\Omega(1)\le q\le 2$	$q>2$
TSALLISQED$_q$	QSZK-complete [BASTS08]	QSZK-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 $q\ge 1+\Omega(1)$ 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 $\mathrm{Tr}(\widehat{\rho}^2)=\sum_k \lambda_k^2\le 1/n$. 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 $q\ge 2$, SWAP test-like techniques [BCWdW01,EAO+02] provide a solution.
- For non-integer $q\ge 1+\Omega(1)$, our result (Theorem 1) solves the problem.

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

We begin by implementing a two-outcome measurement $\{\Pi_0, \Pi_1\}$, where

$$\Pi_b := \frac{1}{2}\Big(I + (-1)^b U_{f(\rho)}\Big) \text{ for } b \in \{0,1\},$$

using 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 $f(x) = x^{q-1}$.
- $\{\Pi_0, \Pi_1\}$ is efficiently implementable if $U_{f(\rho)}$ can be efficiently implemented!

Efficiently implementation of the measurement. 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]:

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

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$_q$	$1 \le q \le 2$	PUREQSD is BQP-hard [RASW23]	$\mathrm{H}_q\big(\frac{1}{2}\big)-\mathrm{H}_q\big(\frac{1-\mathrm{T}}{2}\big) \le \mathsf{QJT}_q \le \mathrm{H}_q\big(\frac{1}{2}\big)\mathrm{T}^q$
TSALLISQED$_q$	$1 \le q \le 1+\frac{1}{n-1}$	QSD is QSZK-hard [Wat02, Wat09]	$\mathrm{H}_q\big(\frac{1}{2}\big)-\mathrm{H}_q\big(\frac{1-\mathrm{T}}{2}\big) \le \mathsf{QJT}_q$
TSALLISQEA$_q$	$q = 1+\frac{1}{n-1}$	QSCMM is NIQSZK-hard [Kob03, BASTS10, CCKV08]	$\big(1-\mathrm{T}-\frac{1}{2^n}\big)\ln_q(2^n) \le \mathrm{S}_q \le \ln_q(2^n(1-\mathrm{T}))$

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

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

Conclusions and open problems

Take-home messages on our work

1. For the regime $q \geq 1 + \Omega(1)$, estimating the quantum Tsallis entropy $S_q(\rho)$, equivalently the trace of quantum state powers, is computationally *easy* and has quantitative bounds that are *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 $S_q(\rho)$ is computationally *hard*:
   - The white-box problems cannot be solved efficiently unless BQP $=$ QSZK;
   - The rank dependence in quantitative bounds 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 $S_q(\rho)$ in the regime $1 < q < 2$, which has previously been challenging to compute?
2. Can we improve these quantitative bounds for the regime $q \geq 1 + \Omega(1)$?
3. What are the computational complexity and hardness for estimating the quantum Rényi entropy?

Thanks!