Space-bounded quantum state testing
via space-efficient quantum singular value transformation

François Le Gall, **Yupan Liu**, Qisheng Wang

Nagoya University

Available at arXiv:2308.05079

Shenzhen-Nagoya Workshop on Quantum Science, September 2024

1. Main results: Complete characterizations of quantum logspace from state testing
2. Implication: Algorithmic Holevo-Helstrom measurement
3. Proof technique: Space-efficient quantum singular value transformation
4. Open problems

What is quantum state testing

Task: Quantum state testing (with two-sided error).

Given two quantum devices Q_0 and Q_1 that prepare $\mathrm{poly}(n)$-qubit quantum (mixed) states $\rho_0 \in \mathbb{C}^{N\times N}$ and $\rho_1 \in \mathbb{C}^{N\times N}$, respectively, which may be viewed as "sample access" to ρ_0 and ρ_1. Decide whether $\mathrm{dist}(\rho_0, \rho_1) \leq \varepsilon_1$ or $\mathrm{dist}(\rho_0, \rho_1) \geq \varepsilon_2$.

The classical counterpart and the one-sided error variant are as follows:

- **Distribution testing** (a.k.a. closeness testing of distributions, see [Canonne'20]): Given sample accesses to probability distributions D_0 and D_1, decide whether $\mathrm{dist}(D_0, D_1) \leq \varepsilon_1$ or $\mathrm{dist}(D_0, D_1) \geq \varepsilon_2$.
- **Quantum state certification** [Bădescu-O'Donnell-Wright'19]: Given "sample access" to ρ_0 and ρ_1, decide whether $\rho_0 = \rho_1$ or $\mathrm{dist}(\rho_0, \rho_1) \geq \varepsilon$.

Typical goal: Minimize the number of copies (*sample complexity*) of ρ_0 and ρ_1.

In this work: Viewing quantum state testing as a computational (promise) problem.

Main result: Space-bounded state certification (one-sided error scenario)

Task 1.1 (Space-bounded quantum state certification). Given two *polynomial-size* $O(\log n)$-*qubit* quantum circuits Q_0 and Q_1 that prepare $O(\log n)$-qubit quantum (mixed) states ρ_0 and ρ_1, respectively. Decide whether $\rho_0 = \rho_1$ or $\mathrm{dist}(\rho_0, \rho_1) \geq \alpha$.

Classical and quantum distance-like measures that are considered:

	Quantum	Classical
ℓ_1 norm	trace distance $\mathrm{td}(\rho_0,\rho_1) := \frac{1}{2}\mathrm{Tr}\lvert\rho_0-\rho_1\rvert$	total variation distance (a.k.a. statistical distance)
ℓ_2 norm	Hilbert-Schmidt distance $\mathrm{HS}^2(\rho_0,\rho_1) := \frac{1}{2}\mathrm{Tr}(\rho_0-\rho_1)^2$	Euclidean distance

Theorem 1.2 (Space-bounded quantum state certification is coRQ$_\mathsf{U}$L-complete). The following space-bounded quantum state certification problems are coRQ$_\mathsf{U}$L-complete. For any $\alpha(n) \geq 1/\mathrm{poly}(n)$, decide whether

1. $\overline{\text{CERTQSD}}_{\log}$: $\rho_0 = \rho_1$ or $\mathrm{td}(\rho_0,\rho_1) \geq \alpha(n)$;
2. $\overline{\text{CERTQHS}}_{\log}$: $\rho_0 = \rho_1$ or $\mathrm{HS}^2(\rho_0,\rho_1) \geq \alpha(n)$.

Remark. coRQ$_\mathsf{U}$L captures the power of *unitary* quantum logspace that *always* accepts *yes* instances, while accepting *no* instances with probability at most $1/2$.

Main result: Space-bounded quantum state testing (two-sided error scenario)

Task 1.3 (Space-bounded quantum state testing). Given two *polynomial-size* $O(\log n)$*-qubit* quantum circuits Q_0 and Q_1 that prepare $O(\log n)$-qubit quantum (mixed) states ρ_0 and ρ_1, respectively. Decide whether $\mathrm{dist}(\rho_0, \rho_1) \leq \beta$ or $\mathrm{dist}(\rho_0, \rho_1) \geq \alpha$.

Theorem 1.4 (Space-bounded quantum state testing is BQL-complete). The following space-bounded quantum state testing problems are BQL-complete. For any α, β such that $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$ or any $g(n) \geq 1/\mathrm{poly}(n)$, decide whether

1. GapQSD$_{\text{log}}$: $\mathrm{td}(\rho_0, \rho_1) \geq \alpha$ or $\mathrm{td}(\rho_0, \rho_1) \leq \beta$;
2. GapQHS$_{\text{log}}$: $\mathrm{HS}^2(\rho_0, \rho_1) \geq \alpha$ or $\mathrm{HS}^2(\rho_0, \rho_1) \leq \beta$;
3. GapQED$_{\text{log}}$: $S(\rho_0) - S(\rho_1) \geq g$ or $S(\rho_1) - S(\rho_0) \geq g$;
4. GapQJS$_{\text{log}}$: $\mathrm{QJS}_2(\rho_0, \rho_1) \geq \alpha$ or $\mathrm{QJS}_2(\rho_0, \rho_1) \leq \beta$.

Remark. BQL captures the power of quantum computation with $O(\log n)$ qubits.

Summary: Time- and space-bounded distribution and state testing

Task 1.5 (Time-bounded quantum state testing). Given two *polynomial-size* quantum circuits Q_0 and Q_1 that prepare $\mathrm{poly}(n)$-qubit quantum (mixed) states ρ_0 and ρ_1, respectively. Decide whether $\mathrm{dist}(\rho_0, \rho_1) \leq \beta$ or $\mathrm{dist}(\rho_0, \rho_1) \geq \alpha$.

Computational hardness of time- and space-bounded distribution and state testing:

	ℓ_1 norm	ℓ_2 norm	Entropy
Classical Time-bounded	SZK-complete* [SV03,GSV98]	BPP-complete Folklore	SZK-complete [GV99,GSV98]
Quantum Time-bounded	QSZK-complete* [Wat02,Wat09]	BQP-complete [BCWdW01, RASW23]	QSZK-complete [BASTS10]
Quantum Space-bounded	BQL-complete This work	BQL-complete [BCWdW01] and this work	BQL-complete This work

Takeaways. For space-bounded state testing and certification problems, the computational hardness of these problems is *as easy as* just preparing quantum states, which is *independent of the choice* of aforementioned distance-like measures.

Distinguishing quantum states and Holevo-Helstrom bound

Problem 2.1 (Computational Quantum Hypothesis Testing). Given polynomial-size quantum circuits Q_0 and Q_1 acting on n qubits and having r output qubits. Let ρ_b be the state obtained by performing Q_b on $|0^n\rangle$ and tracing out the non-output qubits for $b \in \{0,1\}$. Now, consider the following computational task:

- **Input:** A quantum state ρ, either ρ_0 or ρ_1, is chosen uniformly at random.
- **Output:** A bit b indicates that $\rho = \rho_b$.

Holevo-Helstrom bound

Theorem 2.2 [Holevo'73, Helstrom'69] Given a quantum state ρ, either ρ_0 or ρ_1, that is chosen uniformly at random, the maximum success probability to discriminate between quantum states ρ_0 and ρ_1 is given by $\frac{1}{2} + \frac{1}{2}\mathrm{td}(\rho_0,\rho_1)$.

Optimal two-outcome measurement $\{\Pi_0, \Pi_1\}$ achieving the max. discrimination prob.:

$$\Pi_0 = \frac{I}{2} + \frac{1}{2}\mathrm{sgn}^{(\mathrm{SV})}\left(\frac{\rho_0-\rho_1}{2}\right) \text{ and } \Pi_1 = \frac{I}{2} - \frac{1}{2}\mathrm{sgn}^{(\mathrm{SV})}\left(\frac{\rho_0-\rho_1}{2}\right).$$

It is straightforward to see that $\mathrm{td}(\rho_0,\rho_1) = \frac{1}{2}\mathrm{Tr}|\rho_0-\rho_1| = \mathrm{Tr}(\Pi_0\rho_0) - \mathrm{Tr}(\Pi_0\rho_1)$.

An approximately explicit implementation of the HH measurement

Theorem 2.3 (Algorithmic Holevo-Helstrom measurement, this work). Let ρ_0 and ρ_1 be states prepared by n-qubit quantum circuits Q_0 and Q_1, respectively, as defined in Problem 2.1. An approximate version of the Holevo-Helstrom measurement Π_0, denoted as $\tilde{\Pi}_0$, can be implemented such that

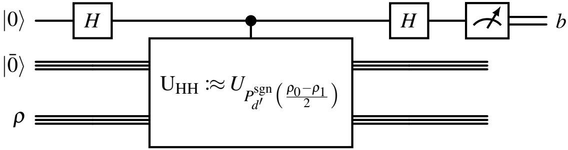
$$|\mathrm{td}(\rho_0,\rho_1) - \big(\mathrm{Tr}(\tilde{\Pi}_0\rho_0) - \mathrm{Tr}(\tilde{\Pi}_0\rho_1)\big)| \leq 2^{-n}.$$

The quantum circuit implementation of $\tilde{\Pi}_0$, acting on $O(n)$ qubits, requires $\mathrm{poly}(N)$ queries onto the circuits Q_0, Q_1, one-, and two-qubit gates, where $N = 2^n$. Moreover, the circuit description can be computed in deterministic time $\mathrm{poly}(N)$ and space $O(n)$.

Proof Sketch. Instead of implementing $\{\Pi_0, \Pi_1\}$, it suffices to approx. implement $\{\hat{\Pi}_0, \hat{\Pi}_1\}$ by the space-efficient QSVT assoc. with the sign function (Theorem 1.4 1):

$$\hat{\Pi}_0 = \frac{I}{2} + \frac{1}{2} P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0 - \rho_1}{2}\right) \text{ and } \hat{\Pi}_1 = \frac{I}{2} - \frac{1}{2} P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0 - \rho_1}{2}\right).$$

Once we have a block-encoding of $P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0-\rho_1}{2}\right)$, we can implement Π_0:



Quantum singular value transformation in a nutshell

QSVT [Gilyén-Su-Low-Wiebe'19] is a systematic approach to (time-efficiently) *manipulating singular values* $\{\sigma_i\}_i$ of an Hermitian matrix A using a corresponding projected unitary encoding $A = \tilde{\Pi} U \Pi$ for orthogonal projectors $\tilde{\Pi}$ and Π.

Quantum singular value transformation, revisited

Given a singular value decomposition $A = \sum_i \sigma_i |\tilde{\psi}_i\rangle\langle\psi_i|$ associated with an $s(n)$-qubit *projected unitary encoding*, we can *approximately* implement a QSVT $f^{(\mathrm{SV})}(A) = \sum_i f(\sigma_i)|\tilde{\psi}_i\rangle\langle\psi_i|$ by employing a polynomial P_d of degree $d = O\big(\frac{1}{\delta}\log\frac{1}{\varepsilon}\big)$ satisfying that

- P_d well-approximates f on the interval of interest $\mathcal{I}$: $\max_{x\in\mathcal{I}\setminus\mathcal{I}_\delta} |P_d(x) - f(x)| \leq \varepsilon$ where $\mathcal{I}_\delta \subseteq \mathcal{I} \subseteq [-1,1]$ and typically $\mathcal{I}_\delta := (-\delta,\delta)$.
- P_d is bounded: $\max_{x\in[-1,1]} |P_d(x)| \leq 1$.

Moreover, all coefficients of P_d (namely, *pre-processing*) can be computed in deterministic $\mathrm{poly}(d)$ time (and thus space). Hence, the transformation $P_d^{(\mathrm{SV})}(A)$ can be implemented by a $\mathrm{poly}(d)$-size quantum circuit acts on $O(\max\{\log d, s(n)\})$ qubits.

Remark. Quantum circuit implementation in QSVT is already space-efficient!

Space-efficient quantum singular value transformation

Question 3.1 (Space-efficient QSVT). Can we implement a degree-d QSVT for any $O(\log n)$-qubit projected unitary encoding with $d \leq \mathrm{poly}(n)$, using only $O(\log n)$ space in both (classical) pre-processing and quantum circuit implementation?

Partial solutions:

- Space-efficient QSVT associated with *Chebyshev polynomials* (underlying Grover search) is implicitly established in [Gilyén-Su-Low-Wiebe'19].
- A natural approach is "projecting" the *continuous function bounded on* $[-1,1]$, e.g., the sign function, to the basis formed by Chebyshev polynomials [Metger-Yuen'23]:
  - Classical (deterministic) pre-processing requires $O(\mathrm{poly}\log n)$ space;
  - The approximation error (caused directly by the polynomial approximation) on the interval of interest increases from ε to $O(\varepsilon \log d)$ due to the Chebyshev truncation.

Theorem 3.2 (Space-*efficient* QSVT, this work). Implement a degree-d QSVT associated with *piecewise-smooth functions* for any $O(\log n)$ qubit *bitstring indexed encoding* with $d \leq \mathrm{poly}(n)$ requires (randomized) $O(\log n)$ space for pre-processing and $O(\log n)$ qubits in quantum circuit implementation. The polynomial approximation error on the interval of interest is $O(\varepsilon)$. Moreover, the implementation requires $O(d^2\|\mathbf{c}\|_1)$ uses of U, $U^\dagger$, $\mathrm{C}_\Pi\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, among with other gates, where $\mathbf{c}$ is the coefficients of *averaged* Chebyshev truncation, and $\|\mathbf{c}\|_1 \leq O(\log d)$.

E.g. Normalized log function $\ln_\beta(x) := \frac{2\ln(1/x)}{2\ln(2/\beta)}$ on the interval $\mathcal{I} = [\beta, 1]$ for any $\beta \geq 1/\mathrm{poly}(n)$.

1. Main results: Complete characterizations of quantum logspace from state testing
2. Implication: Algorithmic Holevo-Helstrom measurement
3. Proof technique: Space-efficient quantum singular value transformation
4. Open problems

Conclusions and open problems

Take-home messages on our work

1. Space-bounded quantum state certification problems w.r.t. trace distance and Hilbert-Schmidt distance are $\mathsf{coRQ_UL}$-complete (Theorem 1.2).
   This is the *first* family of natural $\mathsf{coRQ_UL}$-complete problem!
2. Space-bounded quantum state testing problems w.r.t. common distance-like measures (i.e., trace distance, squared Hilbert-Schmidt distance, quantum entropy difference, quantum Jensen-Shannon divergence) are BQL-complete (Theorem 1.4).
3. Holevo-Helstrom measurement can be approx. implemented by the space-efficient QSVT in quantum $\mathrm{poly}(N)$ time and $O(n)$ space (Theorem 2.3), where $N = 2^n$. Consequently, QSZK is in $\mathsf{QIP}(2)$ with a quantum linear space honest prover.
4. Quantum singular value transformation on bitstring indexed encoding can be done in *quantum logspace*, with a *randomized* classical pre-processing (Theorem 3.2).

Open problems

1. Are there any other applications of space-efficient QSVT?
2. (Inspired by Tom Gur) What about the computational complexity for space-bounded quantum *channel* testings with respect to different distance-like measures?

Thanks!