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

Tsinghua University, Aug 2023

1. Quantum state testing: ℓ_1 norm vs. ℓ_2 norm
2. Main result: Space-bounded quantum state testing and certification
3. Implications on space-bounded quantum computation
4. Proof technique: Space-efficient quantum singular value transformation
5. Proof overview: $\textsc{GapQSD}_{\mathsf{log}} \in \mathsf{BQL}$ and $\overline{\textsc{CertQSD}}_{\mathsf{log}} \in \mathsf{coRQ_UL}$
6. 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 (mixed) quantum 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 $\mathrm{dist}(\rho_0, \rho_1) \le \epsilon_1$ or $\mathrm{dist}(\rho_0, \rho_1) \ge \epsilon_2$.

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

- **Quantum state certification** [Bădescu-O'Donnell-Wright'19]:
  Given "sample access" to ρ_0 and ρ_1, decide whether $\rho_0 = \rho_1$ or $\mathrm{dist}(\rho_0, \rho_1) \ge \epsilon$.
- **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 $\mathrm{dist}(D_0, D_1) \le \epsilon_1$ or $\mathrm{dist}(D_0, D_1) \ge \epsilon_2$.

Goal. Minimize the number of required copies (*sample complexity*) of ρ_0 and ρ_1.

Quantum state testing: sample complexity perspective

Classical and quantum distances that are considered:

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

Sample complexity for distribution testing and quantum state testing:

	ℓ_1 norm	ℓ_2 norm	Entropy
Classical sample complexity	$\mathrm{poly}(N, 1/\epsilon)$ [CDVV14]	$\mathrm{poly}(1/\epsilon)$ [CDVV14]	$\mathrm{poly}(N, 1/\epsilon)$ [JVHW15, WY16]
Quantum sample complexity	$\mathrm{poly}(N, 1/\epsilon)$ [BOW19]	$\mathrm{poly}(1/\epsilon)$ [BOW19]	$\mathrm{poly}(N, 1/\epsilon)$ [AISW20, OW21]

Time-bounded quantum state testing: ℓ_1 norm scenario

Task 1.1 (Time-bounded quantum state testing). Given two *polynomial-size* quantum circuits Q_0 and Q_1 that prepare $\mathrm{poly}(n)$-qubit (mixed) states ρ_0 and ρ_1, respectively, with access to their "source codes".
Decide whether $\mathrm{dist}(\rho_0, \rho_1) \leq \beta$ or $\mathrm{dist}(\rho_0, \rho_1) \geq \alpha$.

Time-bounded distribution testing: Given two *efficiently samplable* distributions D_0 and D_1, decide whether $\mathrm{dist}(D_0, \mathrm{D}_1) \leq \beta$ or $\mathrm{dist}(D_0, D_1) \geq \alpha$.

Computational hardness of these tasks w.r.t. ℓ_1 norm:

- Statistical Difference Problem (SDP) is SZK-complete when *constant* $\alpha^2 - \beta > 0$. [Sahai-Vadhan'03, Goldreich-Sahai-Vadhan'98]
- Quantum State Distinguishability Problem (QSDP) is QSZK-complete when *constant* $\alpha^2 - \beta > 0$. [Watrous'02, Watrous'09]
- Open problem: (α, β)-QSDP is in QSZK when $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$.

Structural complexity-theoretic results regarding QSZK:

- BQP $\subseteq$ QSZK $\subseteq$ QIP(2) $\subseteq$ PSPACE. [Watrous'02, Watrous'09]
- $\exists \mathcal{O}$ s.t. $\mathrm{QSZK}^{\mathcal{O}} \not\subseteq \mathrm{PP}^{\mathcal{O}}$. [Bouland-Chen-Holden-Thaler-Vasudevan'19]

Time-bounded quantum state testing: ℓ_2 norm scenario

Proposition 1.2 [BCWdW01, ARSW21]. Quantum Hilbert-Schmidt distance problem, namely time-bounded quantum state testing w.r.t. ℓ_2 norm, is BQP-complete.

BQP **containment**. As all three terms in $\mathrm{HS}^2(\rho_0,\rho_1) = \frac{1}{2}\mathrm{Tr}(\rho_0^2) + \frac{1}{2}\mathrm{Tr}(\rho_1^2) - \mathrm{Tr}(\rho_0\rho_1)$ can be estimated by the SWAP test [Buhrman-Cleve-Watrous-de Wolf'01], we have a hybrid algorithm successes w.p. $\frac{1}{2} + \frac{1}{2}\mathrm{HS}^2(\rho_0,\rho_1)$:

1. Toss two random coins $r_0, r_1 \in \{0,1\}$;
2. Perform the SWAP test on quantum states according to r_0 and r_1.

BQP **hardness** [Agarwal-Rethinasamy-Sharma-Wilde'21]. Consider a BQP circuit C_x, we can construct $C'_x := C_x^\dagger X_\mathsf{O}^\dagger \mathrm{CNOT}_{\mathsf{O}\to\mathsf{F}} X_\mathsf{O} C_x$ with an ancillary qubit on F such that $\Pr[C'_x \text{ accepts}] = \|(|\bar{0}\rangle\langle\bar{0}| \otimes |0\rangle\langle 0|_\mathsf{F}) C'_x (|\bar{0}\rangle \otimes |0\rangle_\mathsf{F})\|_2^2 = \Pr^2[C_x \text{ accepts}]$.
By defining two pure states $\rho_0 := |\bar{0}\rangle\langle\bar{0}| \otimes |0\rangle\langle 0|_\mathsf{F}$ and $\rho_1 := C'_x(|\bar{0}\rangle\langle\bar{0}| \otimes |0\rangle\langle 0|_\mathsf{F})$, we have $\Pr[C'_x \text{ accepts}] = \mathrm{Tr}(\rho_0\rho_1) = 1 - \mathrm{HS}^2(\rho_0,\rho_1)$. □

Takeaways: Computational hardness of Task 1.1 **depends on distance**

- Time-bounded quantum state testing w.r.t. ℓ_1 norm (QSZK-complete) is seemingly *much harder* than only preparing these states (in BQP).
- Time-bounded quantum state testing w.r.t. ℓ_2 norm (BQP-complete) is *as easy as* only preparing these states (in BQP).

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

Task 2.1 (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 (mixed) states ρ_0 and ρ_1, respectively, with access to their "source codes".
Decide whether $\mathrm{dist}(\rho_0, \rho_1) \leq \beta$ or $\mathrm{dist}(\rho_0, \rho_1) \geq \alpha$.

Theorem 2.2 (Space-bounded quantum state testing is BQL-complete). The following (log)space-bounded quantum state testing problems are BQL-complete. For any α, β s.t. $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$ or any $g(n) \geq 1/\mathrm{poly}(n)$, decide whether

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

Here, quantum Jensen-Shannon divergence QJS is defined as
$\mathrm{QJS}_2(\rho_0, \rho_1) := S_2\left(\frac{\rho_0 + \rho_1}{2}\right) - \frac{1}{2}(S_2(\rho_0) + S_2(\rho_1))$ where $S_2(\rho) := -\mathrm{Tr}(\rho \log_2 \rho)$.

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

Computational hardness of Time-bounded and space-bounded quantum 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, ARSW21]	QSZK-complete [BASTS10]
Classical Space-bounded	BPL-hard†	BPL-complete† Folklore	BPL-complete† [ABIS19]
Quantum Space-bounded	BQL-complete This work	BQL-complete [BCWdW01] and this work	BQL-complete This work

Remark†. Space-bounded distribution testing can be viewed as a "white-box" version of *streaming distribution testing* with i.i.d. samples.

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

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

Task 2.3 (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 (mixed) states ρ_0 and ρ_1, respectively, with access to their "source codes".
Decide whether $\rho_0 = \rho_1$ or $\mathrm{dist}(\rho_0, \rho_1) \geq \alpha$.

Theorem 2.4 (Space-bounded quantum state certification is $\mathsf{coRQ_UL}$-complete).
The following space-bounded quantum state certification problems are $\mathsf{coRQ_UL}$-complete. For any $\alpha(n) \geq 1/\mathrm{poly}(n)$, decide whether

1. $\overline{\textsc{CertQSD}}_{\mathsf{log}}$: $\rho_0 = \rho_1$ or $\mathrm{td}(\rho_0, \rho_1) \geq \alpha(n)$;
2. $\overline{\textsc{CertQHS}}_{\mathsf{log}}$: $\rho_0 = \rho_1$ or $\mathrm{HS}^2(\rho_0, \rho_1) \geq \alpha(n)$.

Remark. $\mathsf{coRQ_UL}$ is a complexity class with *perfect completeness*, namely the acceptance probability $p_{\mathrm{acc}} = 1$ for *yes* instances whereas $p_{\mathrm{acc}} \leq 1/2$ for *no* instances.

BQL and $\mathsf{BQ_UL}$: Two-sided error space-bounded quantum computation

BQL (and $\mathsf{BQ_UL}$ if only allow *unitary* gates), defined in [Watrous'99, Watrous'03], captures quantum computation that performs by a *logspace-uniform* $O(\log n)$*-qubit* quantum circuit. This class admits the following properties:

- Quadratic advantage in space (?): $\mathsf{BQL} \subseteq \mathsf{DSPACE}[\log^2(n)]$ [Wat99, Wat03].
- Gateset-indep.: Space-efficient Solovay-Kitaev theorem [van Melkebeek-Watson'12].
- Error reduction for $\mathsf{BQ_UL}$ [Fefferman-Kobayashi-Lin-Morimae-Nishimura'16].
- Intermediate measurements are useless: $\mathsf{BQL} = \mathsf{BQ_UL}$ [Fefferman-Remscrim'21].

History of the only family of (natural) BQL-complete problem:

- Inverting a well-conditioned matrix is in BQL [Ta-Shma'13], whereas it only has $\mathsf{DSPACE}[\log^2(n)]$ containment without the help of quantum.
- Inverting a well-conditioned matrix is $\mathsf{BQ_UL}$-complete [Fefferman-Lin'18].
- A well-conditioned version of DET^*-complete problems are BQL-complete [Fefferman-Remscrim'21], such as well-conditioned integer determinant, well-conditioned matrix powering, well-conditioned iterative matrix product.

Takeaway. This work (Theorem 2.2) presents *a new family* of natural BQL-complete problems that emerge from quantum property testing.

$\mathsf{RQ_UL}$ and $\mathsf{coRQ_UL}$: One-sided error space-bounded quantum computation

$\mathsf{RQ_UL}$ and $\mathsf{coRQ_UL}$, defined in [Watrous'01], capture *one-sided error* quantum computation that performs by a *logspace-uniform* $O(\log n)$-*qubit* quantum circuits. These classes admit the following properties:

- Error reduction for $\mathsf{RQ_UL}$ and $\mathsf{coRQ_UL}$ [Watrous'01].
- Gateset-dependence which is because of perfect completeness or soundness.
- Undirected graph connectivity (USTCON) is in $\mathsf{RQ_UL} \cap \mathsf{coRQ_UL}$ [Watrous'01], although USTCON is actually in L [Reingold'08] .

Open problems on $\mathsf{RQ_UL}$ and $\mathsf{coRQ_UL}$:

- A (natural) complete problem for the class $\mathsf{RQ_UL}$ or $\mathsf{coRQ_UL}$ remains *unknown*. A "verification" version of well-conditioned iterative matrix product problem is coRQL-hard [Fefferman-Remscrim'21] while there is no containment (*hard direction*).
- $\mathsf{RQ_UL} \stackrel{?}{=} \mathsf{RQL}$ and $\mathsf{coRQ_UL} \stackrel{?}{=} \mathsf{coRQL}$.

Takeaway. This work (Theorem 2.4) demonstrates *the first family* of natural $\mathsf{coRQ_UL}$-complete problems that arise from quantum property testing as well.

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 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 $\hat{P}_d$ of degree $d = O\left(\frac{1}{\delta}\log\frac{1}{\epsilon}\right)$ satisfying that

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

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

Question 4.1. Can we implement a degree-d QSVT for any $s(n)$-qubit projected unitary encoding with $d \leq 2^{O(s(n))}$, using only $O(s(n))$ space in both classical pre-processing and quantum circuit implementation?

Space-efficient quantum singular value transformation

Theorem 4.2 (Space-*bounded* QSVT) [Metger-Yuen'23]. Implement a degree-d QSVT associated with *sign function* or *square-root function* for any $O(\log n)$ qubit *block-encoding* with $d \leq \mathrm{poly}(n)$ requires $O(\mathrm{poly}\log n)$ space for classical pre-processing and $O(\log n)$ qubits in quantum circuit implementation.

Remark. Theorem 4.2 can be easily extended to continuous functions bounded on $[-1,1]$.

Theorem 4.3 (Space-*efficient* QSVT). 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 classical pre-processing and $O(\log n)$ qubits in quantum circuit implementation.
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 coeffs of *Chebyshev interpolation polynomial*.

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 $\beta \geq 1/\mathrm{poly}(n)$.

Proof Sketch.

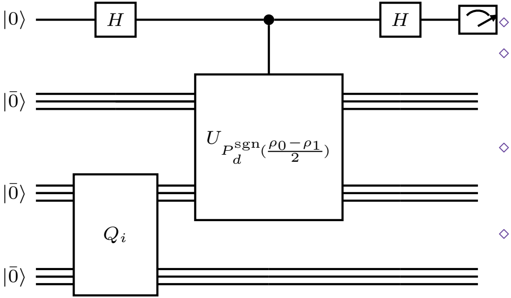
- For bounded functions, we mainly follow the construction in [MY23] with a careful analysis;
- For piecewise-smooth functions, we adapt the construction (i.e., a reduction to a linear combination of bounded functions) in [van Apeldoorn-Gilyén-Gribling-de Wolf'20].
  The main challenge can be boiled down to *stochastic matrix powering problem* which is crucial for the BPL vs. L problem [Saks-Zhou'99, Cohen-Doron-Sberlo-Ta-Shma'23, Putterman-Pyre'23]. □

1. Quantum state testing: ℓ_1 norm vs. ℓ_2 norm
2. Main result: Space-bounded quantum state testing and certification
3. Implications on space-bounded quantum computation
4. Proof technique: Space-efficient quantum singular value transformation
5. Proof overview: $\textsc{GapQSD}_{\mathsf{log}} \in \mathsf{BQL}$ and $\overline{\textsc{CertQSD}}_{\mathsf{log}} \in \mathsf{coRQ_UL}$
6. Open problems

Proof overview

Proof of Theorem 2.2 ①: $\textsc{GapQSD}_{\log} \in \mathsf{BQL}$

Inspired by the approach in [Gilyén-Poremba'22, Wang-Zhang'23], note that $\mathrm{sgn}(x) \approx_{\epsilon,\delta} P_d^{\mathrm{sgn}}(x)$ and $\mathrm{td}(\rho_0,\rho_1) = \frac{1}{2}\mathrm{Tr}|\rho_0-\rho_1| = \frac{1}{2}\left(\mathrm{Tr}\left(\mathrm{sgn}^{(\mathrm{SV})}(\frac{\rho_0-\rho_1}{2})\rho_0\right) - \mathrm{Tr}\left(\mathrm{sgn}^{(\mathrm{SV})}(\frac{\rho_0-\rho_1}{2})\right)\rho_1\right)$.



- $Q_i (i=0,1)$ prepares the state ρ_i.
- We implement $U_{P_d^{\mathrm{sgn}}(\frac{\rho_0-\rho_1}{2})}$ by the space-efficient QSVT associated with P_d^{sgn}(Thm 4.3).
- "Acceptance probability" of ρ_i: $\Pr[\text{outcome}=0] = \frac{1}{2}\left(1+\mathrm{Tr}\left(P_d^{\mathrm{sgn}}(\frac{\rho_0-\rho_1}{2})\right)\rho_i\right)$.
- For $i\in\{0,1\}$, estimating $\mathrm{Tr}\left(P_d^{\mathrm{sgn}}(\frac{\rho_0-\rho_1}{2})\rho_i\right) \pm \varepsilon$ using $O(1/\varepsilon^2)$ repetitions. □

Proof of Theorem 2.4 ①: $\overline{\textsc{CertQSD}}_{\log} \in \mathsf{coRQ_UL}$

- If $\rho_0=\rho_1$, $\Pr[\text{outcome}=0]=\frac{1}{2}$. Then we obtain an algorithm $\mathcal{A}$ accept with certainty via *exact amplitude amplification* [Boyer-Brassard-Høyer-Tapp'98, Brassard-Høyer-Mosca-Tapp'02].
- If $\mathrm{td}(\rho_0,\rho_1)\geq\alpha$, $|\Pr[\text{outcome}=0]-\frac{1}{2}|\geq\Omega(\alpha)$. Make sure the algorithm $\mathcal{A}$ accepts w.p. at most $1-\Omega(\alpha^2)$ by a direct calculation. □

1. Quantum state testing: ℓ_1 norm vs. ℓ_2 norm
2. Main result: Space-bounded quantum state testing and certification
3. Implications on space-bounded quantum computation
4. Proof technique: Space-efficient quantum singular value transformation
5. Proof overview: $\textsc{GapQSD}_{\mathsf{log}} \in \mathsf{BQL}$ and $\overline{\textsc{CertQSD}_{\mathsf{log}}} \in \mathsf{coRQ_UL}$
6. Open problems

Conclusions and open problems

Take-home messages on our work

1. Space-bounded quantum state testing problems w.r.t. common distances (i.e., trace distance, Hilbert-Schmidt distance, entropy difference, quantum Jensen-Shannon divergence) are BQL-complete (Theorem 2.2).
2. Space-bounded quantum state certification problems w.r.t. trace distance and Hilbert-Schmidt distance are $\mathsf{coRQ_UL}$-complete (Theorem 2.4).
   This is the *first* family of natural $\mathsf{coRQ_UL}$-complete problem!
3. Quantum singular value transformation on bitstring indexed encoding can be done in *quantum logspace*, with a *randomized* classical pre-processing (Theorem 4.3).

Open problems

1. Space-efficient QSVT with $O(d)$ queries instead of $O(d^2\|\mathbf{c}\|_1)$ in Theorem 4.3, as well as make the pre-processing *deterministic* rather than randomized.
2. Are space-bounded state testings with respect to other (proper) *quantum analogs of symmetric f-divergence* also in BQL?
3. Is space-bounded distribution testing problem w.r.t. the *total variation distance* BPL-complete? What about the streaming distribution testing counterpart?

Thanks!