Quantum property testing

Myeongjin Shin

QISCA Summer School 2025
Quantum Learning and Complexity Theory – **Lecture 3**

Aug 2, 2025

Property testing

Definition 1 (Property)

Let $\mathcal{X}$ be a set of objects and $d : \mathcal{X} \times \mathcal{X} \to [0, 1]$ be a distance measure on $\mathcal{X}$. A subset $\mathcal{P} \subseteq \mathcal{X}$ is called a **property**. An object $x \in \mathcal{X}$ is ϵ-far from $\mathcal{P}$ if $d(x, y) \geq \epsilon$ for all $y \in \mathcal{P}$; x is ϵ-close to $\mathcal{P}$ if there is a $y \in \mathcal{P}$ such that $d(x, y) \leq \epsilon$.

Definition 2 (Property tester)

ϵ-**property tester** for $\mathcal{P}$ is an algorithm that receives as input either an $x \in \mathcal{P}$ or an x that is ϵ-far from P. In the former case, the algorithm accepts with probability at least $\frac{2}{3}$; in the latter case, the algorithm rejects with probability at least $\frac{2}{3}$.

Property estimation

Definition 3 (Property estimator)

ϵ-property estimator for $\mathcal{P}$ is an algorithm that receives $x, y \in \mathcal{P}$ as input and outputs $d'(x, y)$ with probability at least $\frac{2}{3}$. Which $d'(x, y)$ satisfies

$$|d(x, y) - d'(x, y)| \leq \epsilon. \tag{1}$$

The examples of classical distance measures

- Fidelity $F(x, y) = \sum_i \sqrt{x_i y_i}$.
- Trace distance $T(x, y) = \frac{1}{2} \sum_i |x_i - y_i|$.
- Shannon entropy $H(x) = -\sum_i x_i \log x_i$.
- Rényi entropy $H_\alpha(x) = -\frac{1}{1-\alpha} \log \sum_i x_i^\alpha$.

$d(x, y) = H(x) - H(y)$

Quantum property testing

If $\mathcal{X}$ are represented as quantum density matrices, the quantum analog of $\mathcal{P}$ is called as **quantum property** and d as **quantum distance measure**.
The examples of quantum distance measures (which we will look at later)

- Fidelity $F(\rho, \sigma) = \mathbf{Tr}\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}$.
- Trace distance $T(\rho, \sigma) = \frac{1}{2}\mathbf{Tr}|\rho - \sigma|$.
- von Neumann entropy $S(\rho) = -\mathbf{Tr}(\rho \log \rho)$.
- Quantum rényi entropy $S_\alpha(\rho) = \frac{1}{1-\alpha} \log \mathbf{Tr}(\rho^\alpha)$.

But, we will look at it later.

Peculiar property testing

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

$$(p_1, p_2, \cdots, p_n)$$

- Learn the multiset $\{p_1, p_2, \cdots, p_d\}$.
- Determine if $\{p_1, p_2, \cdots, p_d\}$ satisfies a certain property. (eg. $\{\frac{1}{d}, \frac{1}{d}, \cdots, \frac{1}{d}\}$)
- Learn the k largest p_i's.

Peculiar property testing: Quantum version

- Learn the multiset $\{p_1, p_2, \cdots, p_d\}$.
- Determine if $\{p_1, p_2, \cdots, p_d\}$ satisfies a certain property. (eg. $\{\frac{1}{d}, \frac{1}{d}, \cdots, \frac{1}{d}\}$)
- Learn the k largest p_i's and the associated $|\psi_i\rangle$.

Classical distribution: Young diagram (Histogram)

sampling

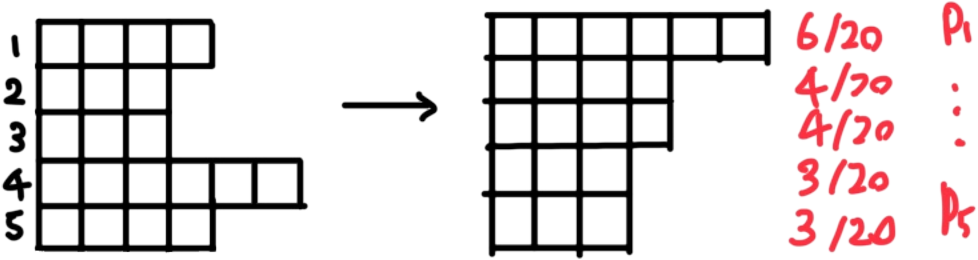
$i \sim d$

$n = \Theta(\frac{1}{\varepsilon^2})$

Say we care about a property of $\{p_1, p_2, \cdots, p_d\}$.

Typical sample when $n = 20$, $d = 5$ (eg. 54423131423144554251)

Represented as Histogram.



Classically learning properties of $\{p_1, p_2, \cdots, p_d\}$

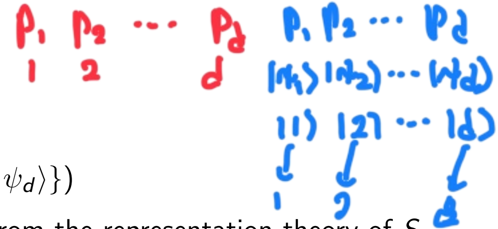
The problem has two commuting symmetries:
S_n-invariance (permuting the n outcomes)
S_d-invariance (permuting d outcome names)

“Factoring these out”, WLOG learner just gets a random Young diagram λ (with n boxes, d rows)

$$\Pr(\lambda) = \boxed{\binom{n}{\lambda}} \underline{m_\lambda(p_1, p_2, \cdots, p_d)} \tag{2}$$

some certain symmetric polynomial m_λ.

Quantumly learning properties of $\{p_1, p_2, \cdots, p_d\}$


p_1 p_2 $\cdots$ p_d
1 2 d
p_1 p_2 $\cdots$ p_d
$|\psi_1\rangle$ $|\psi_2\rangle$ $\cdots$ $|\psi_d\rangle$
$|1\rangle$ $|2\rangle$ $\cdots$ $|d\rangle$
1 2 d

The problem has two commuting symmetries:
S_n-invariance (permuting the n outcomes)
$U(d)$-invariance (rotating unknown $\{|\psi_1\rangle, |\psi_2\rangle, \cdots, |\psi_d\rangle\}$)

"Factoring these out", involves **Schur-Weyl** duality from the representation theory of S_n and $U(d)$.

$$\rho \xrightarrow{U} U\rho U^\dagger$$

$$\Pr(\lambda) = f^\lambda s_\lambda(p_1, p_2, \cdots, p_d) \tag{3}$$

some certain symmetric polynomial s_λ.

Schur-Weyl duality

Theorem 4 (Schur-Weyl duality)

The k-th order commutant of the unitary group is the span of the permutation operators associated to S_k:

$[U^{\otimes k}, A] = 0$

$$\underline{\mathrm{Comm}(\mathrm{U}(d), k)} = \mathrm{span}\left(\boxed{V_d(\pi)} : \pi \in S_k\right). \tag{4}$$

So S_n-invariance and $U(d)$-invariance can coexist.

Quantum distribution: Young diagram (RSK algorithm)

Say we care about a property of $\{p_1, p_2, \cdots, p_d\}$. $\overset{w}{\shortparallel}$ $\rightarrow \boxed{\lambda} = \underline{RSK(w)}$

Typical sample when $n = 20, d = 5$ (eg. $\underline{54423131423144554251}$)

Represented as Young diagram, using $\underline{\text{RSK algorithm.}}$

- λ_1: longest increasing subsequence (LIS)
- $\lambda_1 + \lambda_2$: longest union of 2 increasing subsequence

Tight bound on shape of RSK(w)

λ_1 1 1 1 1 4 4 4 5 5

λ_2 2 2 2 3 5

$\vdots$ 3 3 4

4 4

5

$$\rho^{\otimes n} \xrightarrow{EYD} \lambda = RSK(w)$$

$$\left| \frac{\lambda_i}{n} - p_i \right| < \varepsilon \text{ when}$$

$$n = O\left(\frac{d}{\varepsilon^2}\right)$$

$$\rho = p_1 |\psi_1\rangle\langle\psi_1| + p_2 |\psi_2\rangle\langle\psi_2| + \cdots + p_d |\psi_d\rangle\langle\psi_d|$$

$$(|1\rangle, |2\rangle, \cdots, |d\rangle) \nearrow \text{measure}$$

$$1 \rightarrow p_1 |\langle\psi_1|1\rangle|^2 + p_2 |\langle\psi_2|1\rangle|^2 + \cdots + p_d |\langle\psi_d|1\rangle|^2$$

Questions?

$$2 \rightarrow p_1 |\langle\psi_1|2\rangle|^2 + \cdots + p_d |\langle\psi_d|2\rangle|^2$$

Different input models

Distributional property testing in a quantum world [GT19]

- Classical sampling
- Quantum state sampling
- Quantum state with purification
- Classical with quantum query access

Classical and Quantum state sampling

Definition 5

A classical distribution $(p_i)_{i=1}^{n}$ is accessible via classical sampling if we can request samples from the distribution, i.e., get a random $i \in [n]$ with probability p_i.

Definition 6

A quantum distribution $\rho \in \mathbb{C}^{n \times n}$ accessible via quantum sampling if we can request copies of the state ρ, which is represented as:

$$\rho = \sum_{i=1}^{n} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| . \tag{5}$$

Quantum state with purification

Definition 7

A density operator ρ has purified quantum query access if we have access to a unitary oracle U_ρ (and its inverse) acting as

$$\overset{U_\rho^\dagger}{\boxed{U_\rho}} |0\rangle_A |0\rangle_B = |\psi_\rho\rangle_{AB} = \underline{\sum_{i=1}^{n} \sqrt{p_i}\, |\phi_i\rangle_A \overset{\checkmark}{|\psi_i\rangle_B}} \tag{6}$$

such that $\boxed{\mathbf{Tr}_A}(|\psi_\rho\rangle \langle\psi_\rho|) = \rho$.

Classical with quantum query access

Definition 8

A density operator ρ has purified quantum query access if we have access to a unitary oracle U_ρ (and its inverse) acting as

$$U_\rho \left|0\right\rangle_A \left|0\right\rangle_B = \left|\psi_\rho\right\rangle_{AB} = \sum_{i=1}^{n} \sqrt{p_i} \left|\phi_i\right\rangle_A \overset{\checkmark}{\left|i\right\rangle}_B \tag{7}$$

such that $\mathbf{Tr}_A(\left|\psi_\rho\right\rangle \left\langle\psi_\rho\right|) = \rho$.

Different input models: Recap

How do we test or estimate quantum properties with any of those input models?

- Quantum state sampling: $\rho = \sum_{i=1}^{\cancel{n}\,r} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$
- Quantum state with purification: $U_\rho \left|0\right\rangle_A \left|0\right\rangle_B = \sum_{i=1}^{n} \sqrt{p_i} \left|\phi_i\right\rangle_A \left|\psi_i\right\rangle_B$
- Classical with quantum query access: $U_\rho \left|0\right\rangle_A \left|0\right\rangle_B = \sum_{i=1}^{n} \sqrt{p_i} \left|\phi_i\right\rangle_A \left|i\right\rangle_B$

$O\left(\frac{d}{\varepsilon^2}\right)$

n-qubit

$d = 2^n$

For example $\boxed{\mathbf{Tr}(\rho^2)}$? → swap test.

Then, how about $\mathbf{Tr}(\sqrt{\rho})$?, $S(\rho) = -\mathbf{Tr}(\rho \log \rho)$, $F(\rho, \sigma) = \mathbf{Tr}(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})$ etc.

$$\sqrt{\rho} = \sum_i \sqrt{p_i} \left|\ \right\rangle \left\langle\ \right|$$

$$f(\rho) = \sum_i f(p_i) \left|\ \right\rangle \left\langle\ \right|$$

Polynomial approximation: Not enough

Since we can calculate $\mathbf{Tr}(\rho^k)$ for arbitrary k, let's use polynomial approximation.

$$\mathbf{Tr}(\sqrt{\rho}) = \sum_{i=1}^{K} a_i \mathbf{Tr}(\rho^i) \quad < \varepsilon \quad \rightarrow \quad \sum_{i=1}^{K} |a_i| \, \varepsilon \tag{8}$$

With the best K-degree polynomial, error is $O(\frac{1}{K})$. To reduce the error to ϵ, we set $K = O(\frac{1}{\epsilon})$. Then, the required complexity is proportional to

$$\frac{1}{\sum_{i=1}^{K} |a_i|}, \tag{9}$$

which often explodes to exponential rate (not only for $\mathbf{Tr}(\sqrt{\rho})$, almost every property functions).

Quantum singular value transformation(QSVT)

Definition 9

If we can prepare a purification of a quantum distribution / density operator ρ, then we can construct a unitary U, which has this density operator in the top-left corner, using only two queries to U_ρ. This observation is originally due to Low and Chuang (2016). We call such a unitary a block-encoding of ρ:

$$U = |0\rangle\langle 0| \otimes \rho + \cdots$$

$$U = \begin{bmatrix} \rho & \cdot \\ \cdot & \cdot \end{bmatrix} \longleftrightarrow \rho = (\langle 0|^{\otimes a} \otimes I)U(|0\rangle^{\otimes a} \otimes I) \tag{10}$$

We encode the information of ρ in a unitary. Therefore we can use unitary operations to obtain additional information of ρ.

U $\quad U^2 \quad\quad \rho \quad \frac{\rho+\sigma}{2} \quad \rho^2$

QSVT with polynomial approximation

Definition 10 (Singular value transformation)

Let $f : \mathbb{R} \to \mathbb{C}$ be an even or odd function. Let $A \in C^{\tilde{d} \times d}$ have the following singular value decomposition

$$A = \sum_{i=1}^{d_{\min}} \varsigma_i |\tilde{\psi}_i\rangle \langle \psi_i|$$

$U = \begin{bmatrix} \rho & \\ & \end{bmatrix}$ $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

$V = \begin{bmatrix} f(\rho) & \\ & \end{bmatrix}$ $f(\rho) = \sum_i f(p_i)|\psi_i\rangle\langle\psi_i|$

where $d_{\min} := \min(d, \tilde{d})$. For the function f we define the *singular value transformation* on A as

$|f| \leq 1$, d-degree

$\rightarrow O(d)$

$$f^{(SV)}(A) := \begin{cases} \sum_{i=1}^{d_{\min}} f(\varsigma_i) |\tilde{\psi}_i\rangle \langle \psi_i| & \text{if } f \text{ is odd, and} \\ \sum_{i=1}^{d} f(\varsigma_i) |\psi_i\rangle \langle \psi_i| & \text{if } f \text{ is even, where for } i \in [d] \setminus [d_{\min}], \varsigma_i := 0. \end{cases}$$

$f = \frac{\theta}{|\theta|} \quad \times |\theta|$

QSVT with polynomial approximation

Theorem 11

Let H_U be a finite-dimensional Hilbert space and let $U, \Pi, \widetilde{\Pi} \in H_U$ be linear operators on H_U such that U is a unitary, and $\Pi, \widetilde{\Pi}$ are orthogonal projectors. Suppose that $P = \sum_{k=0}^{n} a_k x^k \in \mathrm{R}[x]$ is a degree-n polynomial such that

- $a_k \neq 0$ *only if* $k \equiv n \mod 2$, *and*
- *for all* $x \in [-1,1]$: $|P(x)| \leq 1$.

$[f(p)\quad]$

Then there exist $\Phi \in \mathrm{R}^n$, such that

$f \to \phi_i$

$$P^{(SV)}\left(\widetilde{\Pi} U \Pi\right) = \begin{cases} \left(\langle+| \otimes \widetilde{\Pi}\right)\left(|0\rangle\langle 0| \otimes U_\Phi + |1\rangle\langle 1| \otimes U_{-\Phi}\right)\left(|+\rangle \otimes \Pi\right) & \text{if } n \text{ is odd, and} \\ \left(\langle+| \otimes \Pi\right)\left(|0\rangle\langle 0| \otimes U_\Phi + |1\rangle\langle 1| \otimes U_{-\Phi}\right)\left(|+\rangle \otimes \Pi\right) & \text{if } n \text{ is even,} \end{cases} \tag{11}$$

where $U_\Phi = e^{i\phi_1(2\widetilde{\Pi}-I)} \prod_{j=1}^{(n-1)/2} \left(e^{i\phi_{2j}(2\Pi-I)} U^\dagger e^{i\phi_{2j+1}(2\widetilde{\Pi}-I)} U\right).$ [a] $[? \, :]$

[a] This is the mathematical form for odd n; even n is defined similarly.

QSVT

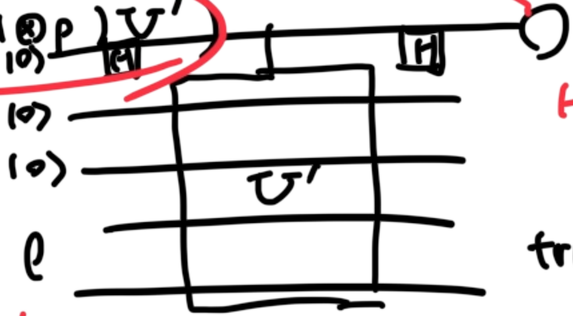
Thus for an even or odd polynomial P of degree n, we can apply singular value transformation of the matrix $\widetilde{\Pi} U \Pi$ with n uses of U, $U^\dagger$ and the same number of controlled reflections $I - 2\Pi, I - 2\widetilde{\Pi}$.

QSVT explanation

$\mathrm{tr}(\rho^3)$ $\quad U = \begin{bmatrix} \rho & \cdot \\ \cdot & \cdot \end{bmatrix} \rightarrow$ QSVT $\quad U' = \begin{bmatrix} \rho^2 & \cdot \\ \cdot & \cdot \end{bmatrix}$

$\shortparallel$

$\mathrm{tr}\left[(|0\rangle\langle 0| \otimes \rho)\, U'\right]$



Hadamard test

U_ρ

$\mathrm{tr}(\rho f(\rho))$

$$(I \otimes U_\rho^\dagger)\,\underline{(\mathrm{CNOT} \otimes \mathrm{SWAP})}\,(I \otimes U_\rho) \rightarrow \begin{bmatrix} \rho & \cdot \\ \cdot & \cdot \end{bmatrix}$$

Applying QSVT to property estimation

Suppose that we want to estimate $\mathbf{Tr}(f(\rho))$.

- Find a polynomial g that $\underline{xg(x)}$ approximates $\underline{f(x)}$ for $x \in [0,1]$.
- Block encode ρ in U using 1 queries to U_ρ and $U_\rho^\dagger$. (If U_ρ is not given, $\frac{\mathsf{rank}(\rho)}{\epsilon^2}$ samples of ρ can construct the channel approximation of U within ϵ-additive error)
- Using QSVT, we can encode the d-degree polynomial $\underline{g(\rho)}$ in a unitary (denoted as U_g), using d queries to ✓ U_ρ and $U_\rho^\dagger$. $(\forall x \in [0,1], |g(x)| \leq 1)$ $\begin{bmatrix} g(\rho) & \cdot \\ \cdot & \cdot \end{bmatrix}$
- Calculate $\underline{\mathbf{Tr}((|0\rangle\langle 0| \otimes \rho)U_g)} = \underline{\mathbf{Tr}(\rho g(\rho))}$ by using **Hadamard test** and **Amplitude estimation** (we will look at it later). $\approx \mathrm{Tr}(f(\rho))$

Hadamard test

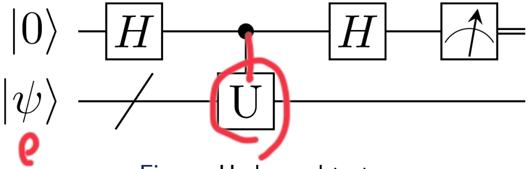


Figure: Hadamard test

$\mathrm{tr}(\rho U) \left\langle \begin{matrix} \mathrm{Re} \\ \mathrm{Im} \end{matrix} \right.$

Estimates $\mathrm{Re}(\langle\psi| U |\psi\rangle), \mathrm{Im}(\langle\psi| U |\psi\rangle)$ within additive error ϵ using $\mathcal{O}(\frac{1}{\epsilon^2})$ queries to $U, U^\dagger$. Using amplitude estimation techniques we can reduce this to $\mathcal{O}(\frac{1}{\epsilon})$.

= Grover

With little refinement, hadamard test allows us to estimate $\mathbf{Tr}((|0\rangle\langle 0| \otimes \rho)U_g) = \mathbf{Tr}(\rho g(\rho))$.

Amplitude estimation

Classically, given i.i.d. samples of a Bernoulli random variable X with $\overset{E}{\vee}[X] = p$, it takes $\Theta(1/\epsilon^2)$ samples to estimate p within ϵ with high success probability. Quantumly, if we are given a unitary U such that

$$\boxed{U} |0\rangle |0\rangle = \boxed{\sqrt{p}} |0\rangle |\phi\rangle + |0^\perp\rangle \,, \text{ where } \| |\phi\rangle \| = 1 \text{ and } (\langle 0| \otimes I) |0^\perp\rangle = 0, \qquad (12)$$

then if measure the output state, we get 0 in the first register with probability p.

$O(\frac{1}{\epsilon})$

Amplitude estimation

Given access to U we can estimate the value of p quadratically more efficiently than what is possible by sampling:

Theorem 12

Given U satisfying, the amplitude estimation algorithm outputs $\tilde{p}$ such that $\tilde{p} \in [0,1]$ and

$$|\tilde{p} - p| \leq \frac{2\pi\sqrt{p(1-p)}}{\underline{M}} + \frac{\pi^2}{M^2} < \varepsilon \qquad O\left(\frac{1}{\varepsilon}\right) \tag{13}$$

with success probability at least $8/\pi^2$, using M calls to U and $U^\dagger$

p

$U_p, U_p^\dagger$

Amplitude estimation

In particular, if we take $M = \left\lceil 2\pi \left(\frac{2\sqrt{p}}{\epsilon} + \frac{1}{\sqrt{\epsilon}} \right) \right\rceil = \Theta \left(\frac{\sqrt{p}}{\epsilon} + \frac{1}{\sqrt{\epsilon}} \right)$, we have

$$|\tilde{p} - p| \leq \frac{2\pi\sqrt{p(1-p)}}{2\pi}\epsilon + \frac{\pi^2}{4\pi^2}\epsilon^2 \leq \frac{\epsilon}{2} + \frac{\epsilon}{4} \leq \epsilon.$$

Therefore, using only $\Theta(1/\epsilon)$ implementations of U and $U^\dagger$, we could get an ϵ-additive approximation of p with success probability at least $8/\pi^2$, which is a quadratic speed-up compared to the classical sample complexity $\Theta(1/\epsilon^2)$.

von Neumann entropy estimation (with pad)

$$S(\rho) = -\mathrm{tr}(\rho \log \rho)$$

$$f(x) = -x\log x$$

$$\rotatebox{90}{=}$$

$$x g(x) \to g(x) = -\log x = \log\frac{1}{x}$$

$$-\log x = -\log(1-(1-x)) = \sum_{k=1}^{\infty} \frac{(1-x)^k}{k}$$

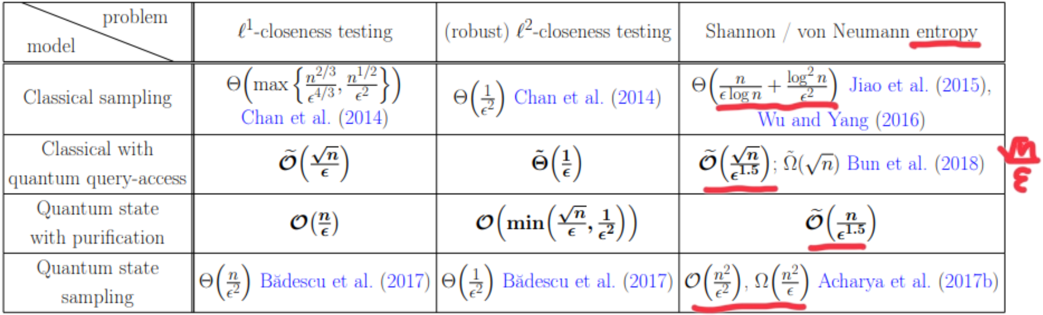
$$\begin{bmatrix} \frac{I-\rho}{2} & \\ & \end{bmatrix} \xrightarrow{\text{QSVT}} \begin{bmatrix} -\log\rho & \\ & \end{bmatrix}$$

Hadamard $\mathrm{tr}(-\rho\log\rho)$

$$\begin{bmatrix} \rho & \\ & \end{bmatrix} \begin{bmatrix} \sigma & \\ & \end{bmatrix} \to \begin{bmatrix} \frac{\rho+\sigma}{2} & \\ & \end{bmatrix}$$

$$D\left(\frac{r}{\varepsilon^2}\right)$$

Known complexity across different input models



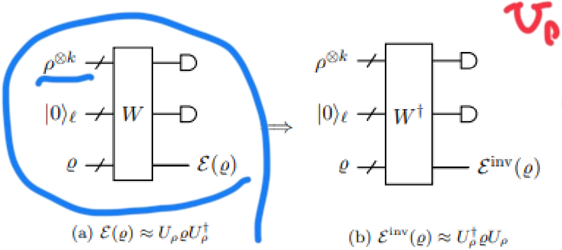
problem model	ℓ^1-closeness testing	(robust) ℓ^2-closeness testing	Shannon / von Neumann entropy
Classical sampling	$\Theta\left(\max\left\{\frac{n^{2/3}}{\epsilon^{4/3}}, \frac{n^{1/2}}{\epsilon^2}\right\}\right)$ Chan et al. (2014)	$\Theta\left(\frac{1}{\epsilon^2}\right)$ Chan et al. (2014)	$\Theta\left(\frac{n}{\epsilon \log n} + \frac{\log^2 n}{\epsilon^2}\right)$ Jiao et al. (2015), Wu and Yang (2016)
Classical with quantum query-access	$\tilde{\mathcal{O}}\left(\frac{\sqrt{n}}{\epsilon}\right)$	$\tilde{\Theta}\left(\frac{1}{\epsilon}\right)$	$\tilde{\mathcal{O}}\left(\frac{\sqrt{n}}{\epsilon^{1.5}}\right)$; $\tilde{\Omega}(\sqrt{n})$ Bun et al. (2018)
Quantum state with purification	$\mathcal{O}\left(\frac{n}{\epsilon}\right)$	$\mathcal{O}\left(\min\left(\frac{\sqrt{n}}{\epsilon}, \frac{1}{\epsilon^2}\right)\right)$	$\tilde{\mathcal{O}}\left(\frac{n}{\epsilon^{1.5}}\right)$
Quantum state sampling	$\Theta\left(\frac{n}{\epsilon^2}\right)$ Bădescu et al. (2017)	$\Theta\left(\frac{1}{\epsilon^2}\right)$ Bădescu et al. (2017)	$\mathcal{O}\left(\frac{n^2}{\epsilon^2}\right)$, $\Omega\left(\frac{n^2}{\epsilon}\right)$ Acharya et al. (2017b)

$\frac{\sqrt{n}}{\epsilon}$

Figure: Upper bound across different input models

What makes the discrepancy between different input models?

Suppose the quantum state sampling input model, where only copies of the state ρ is given. To perform QSVT, we need to construct a quantum channel $\mathcal{E}$ that approximates the unitary block encoding of ρ. $\mathcal{E}$ is given by a quantum circuit W with k samples of ρ.



(a) $\mathcal{E}(\varrho) \approx U_\rho \varrho U_\rho^\dagger$

(b) $\mathcal{E}^{\text{inv}}(\varrho) \approx U_\rho^\dagger \varrho U_\rho$

$U_\rho, U_\rho^\dagger \rightarrow [\rho \quad]$

$\rho \quad ? \nearrow$

$U_\rho \rightarrow O(1)$

$\rho \rightarrow O(\text{poly}(r, \frac{1}{\varepsilon}))$

Figure: Quantum circuit for approximately implementing the inverse of unitary operators.

Often, the complexity of k tend to follow the polynomial of r and $\frac{1}{\epsilon}$.

What makes the discrepancy between different input models?

Suppose the classical with quantum query access model U_p

$|\phi_i\rangle_B$

$\uparrow$

$$U_\rho |0\rangle_A |0\rangle_B = |\psi_\rho\rangle_{AB} = \sum_{i=1}^{n} \sqrt{p_i}\, |\phi_i\rangle_A \underline{|i\rangle_B} \qquad \begin{bmatrix} \rho & \\ & \end{bmatrix} \rightarrow p_n \qquad (14)$$

Take for example $U := (U_p \otimes I)$, $\Pi := (\sum_{i=1}^{n} I \otimes |i\rangle\langle i| \otimes |i\rangle\langle i|)$, and $\widetilde{\Pi} := (|0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes I)$. These operators form a projected unitary encoding of

$$A = \Pi U \widetilde{\Pi} = \sum_{i=1}^{n} \sqrt{p_i}\, |\phi_i\rangle\langle 0| \otimes |i\rangle\langle 0| \otimes |i\rangle\langle i|\,. \qquad \begin{bmatrix} \sqrt{\rho} & \\ & \end{bmatrix} \rightarrow \sqrt{p_n} \qquad (15)$$

We can perform QSVT with square-root efficiency.

$$\frac{1}{p_n} \gg \frac{1}{\sqrt{p_n}}$$

Recent work!

I proved an improved upper bound for classical entropy estimation with quantum query access:

$$\mathcal{O}(\frac{\sqrt{r}}{\epsilon^{1.5}}) \to \mathcal{O}(\frac{\sqrt{r}}{\epsilon} + \frac{r}{\sqrt{\epsilon}}), \tag{16}$$

$\varepsilon \leq \frac{1}{r}$ $\quad O(\frac{\sqrt{r}}{\varepsilon})$

which is better when $\epsilon \leq \frac{1}{\sqrt{r}}$. (Actually, we can loosen it to $\epsilon \leq \frac{1}{r^{\frac{1}{3}}}$.)
This work improves Rényi entropy too!

Distance measures estimation

A more difficult subject... estimate $F(\rho,\sigma)$, $T(\rho,\sigma)$.

Block encode U_f, U_g with U_ρ, U_σ (and each inverses) and use QSVT to block encode $f(\rho)g(\sigma)$ into a unitary.

$$\rho \to \begin{bmatrix} \rho & \\ & \end{bmatrix} \xrightarrow{\text{QSVT}} \begin{bmatrix} f(\rho) & \\ & \end{bmatrix}$$

$$\sigma \to \begin{bmatrix} \sigma & \\ & \end{bmatrix} \to \begin{bmatrix} g(\sigma) & \\ & \end{bmatrix}$$

$$\begin{bmatrix} \underline{f(\rho)g(\sigma)} & \\ & \end{bmatrix}$$

Trace distance estimation (with pad)

$$T(\rho,\sigma) = \frac{1}{2}\mathrm{Tr}|\rho-\sigma|$$

$$A = \rho-\sigma = \sum_i v_i|\ \rangle\langle\ |$$

$$\mathrm{Tr}(\rho,\sigma) = \frac{1}{2}\underset{\mathrm{Tr}}{\wedge}|A| = \frac{1}{2}\sum_i|v_i|$$

$$\mathrm{Tr}(|A|) = \mathrm{Tr}(A\cdot \underset{\underset{g}{\shortparallel}}{\mathrm{Sign}}(A)) = \mathrm{Tr}(\rho\cdot g(A)) - \mathrm{Tr}(\sigma\cdot g(A))$$

$$A = \rho-\sigma \longrightarrow \underbrace{\begin{bmatrix}\rho & \\ & \end{bmatrix}\begin{bmatrix}\sigma & \\ & \end{bmatrix}}_{\downarrow}$$

$$\begin{bmatrix}\frac{\rho-\sigma}{2}=\frac{A}{2} & \\ & \end{bmatrix} \longrightarrow \begin{bmatrix}g(A) & \\ & \end{bmatrix}$$

Distance measures estimation complexity

Task	Resources	Query/Sample Complexity	Approach
Tomography	Purified Access	$\widetilde{O}(Nr/\varepsilon)^*$	[37]
	Identical Copies	$\widetilde{\Theta}(Nr/\varepsilon^2)$	[35, 36]
Trace Distance	Purified Access	$\widetilde{O}(r^5/\varepsilon^6)$	[42]
		$r \cdot \widetilde{O}(1/\varepsilon^2)$	Algorithm 1
	Identical Copies	$\widetilde{O}(r^2/\varepsilon^5)$	Algorithm 2
Fidelity	Purified Access	$\widetilde{O}(r^{12.5}/\varepsilon^{13.5})$	[41]
		$\widetilde{O}(r^{6.5}/\varepsilon^{7.5})$	[42]
		$\widetilde{O}(r^{2.5}/\varepsilon^5)$	[43]
	Identical Copies	$\widetilde{O}(r^{5.5}/\varepsilon^{12})$	[43]

Figure: Here, N is the dimension of quantum states, r is the rank of quantum states.

Any lower bounds?

Task: Discriminate two distributions $\{p_i\}$ and $\{q_i\}$. Define $d_H(p,q)$ as

$$d_H(p,q) = \sqrt{\sum_i (\sqrt{p_i} - \sqrt{q_i})^2/2} \tag{17}$$

We will look at the lower bounds on purification and sample model.

Lower bound on purification model

Theorem 13

Assume the quantum state with purification input model.

$$U_\rho |0\rangle |0\rangle = \sum_i \sqrt{p_i} |\phi_i\rangle |\psi_i\rangle , \tag{18}$$

$$U_\sigma |0\rangle |0\rangle = \sum_i \sqrt{q_i} |\phi_i'\rangle |\psi_i'\rangle . \tag{19}$$

Then discriminating the two distributions have the lower bound

$$\Omega(\frac{1}{d_H(p,q)}) \tag{20}$$

Lower bound on sample model

Theorem 14

Assume the quantum state with ~~purification~~ sampling input model.

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| , \tag{21}$$

$$\sigma = \sum_i q_i \left|\phi_i\right\rangle \left\langle\phi_i\right| . \tag{22}$$

Then discriminating the two distributions have the lower bound

$$\Omega(\frac{1}{d_H(p,q)^{\boxed{2}}}) \tag{23}$$

Limitations on the current lower bound techniques

With the above theorem, for almost every property we can only deduce the lower bound $\Omega(\frac{1}{\epsilon})$ (purification), $\Omega(\frac{1}{\epsilon^2})$ (sample). Which are far from tight.

There are other techniques for sample lower bounds (explanation in future lectures?). But, query (purification) lower bounds are very rare. This could be a future research subject.

Property testing (easier? or harder? than estimation)

- Calculating $d(\rho, \sigma)$ with $\frac{\epsilon}{2}$-precision allows us to determine whether it is $d(\rho, \sigma) > \epsilon$ or $d(\rho, \sigma) = 0$.
- So,in terms of complexity, property testing is easier than estimation.
- But, since we expect lower complexity algorithm for property testing, finding suitable algorithms for property testing is harder.

Other usage of QSVT, QAE, etc

- QSVT: Quantum channel verification, Quantum principal component analysis(actually this is property testing too), Hamiltonian simulation, Gibbs state sampling, etc.
- QAE: Almost every quantum square speed-up advantage.

Recent works: Grover's algorithm is an approximation of imaginary-time evolution

P. Shor argued "quantum computers operate in a manner so different from classical computers that our techniques for designing algorithms and our intuitions for understanding the process of computation no longer work". Here, however, we show that Grover's algorithm can be viewed through the well-established lenses of Riemannian optimization and ITE. That is, Grover's algorithm is simply performing Riemannian optimization, a standard classical optimization strategy, but on the manifold of unitaries.

An interesting point to highlight is that, while the optimal query complexity for unstructured search is limited to a quadratic speed-up, ITE in general converges exponentially to the target state.

Recent works: Amplitude amplification and estimation require inverses

Prove that the generic quantum speedups for brute-force search and counting only hold when the process we apply them to can be efficiently inverted.
In other words, $U^\dagger$ is necessary for quantum advantage.

Thanks a lot!