Quantum state certification

Costin Bădescu [1]   Ryan O'Donnell [1]   John Wright [2]

[1]Carnegie Mellon University

[2]Massachusetts Institute of Technology

January 19, 2018

Introduction

Let $p = (p_1, \ldots, p_d)$ and $q = (q_1, \ldots, q_d)$ be discrete distributions on $\{1, \ldots, d\}$.

Introduction

Let $p = (p_1, \ldots, p_d)$ and $q = (q_1, \ldots, q_d)$ be discrete distributions on $\{1, \ldots, d\}$.

Problem

Suppose p is not known. How many i.i.d. samples $X_1, \ldots, X_n \sim p$ are needed to decide w.h.p. whether $p = q$ or $d_{\mathrm{TV}}(p, q) \geq \epsilon$?

Introduction

Let $p = (p_1, \ldots, p_d)$ and $q = (q_1, \ldots, q_d)$ be discrete distributions on $\{1, \ldots, d\}$.

Problem

Suppose p is not known. How many i.i.d. samples $X_1, \ldots, X_n \sim p$ are needed to decide w.h.p. whether $p = q$ or $d_{\mathrm{TV}}(p, q) \geq \epsilon$?

Theorem (Paninski, 2008)

If $q = (\frac{1}{d}, \frac{1}{d}, \ldots, \frac{1}{d})$, then $n = O(\sqrt{d}/\epsilon^2)$ samples are sufficient.

Introduction

Let $p = (p_1, \ldots, p_d)$ and $q = (q_1, \ldots, q_d)$ be discrete distributions on $\{1, \ldots, d\}$.

Problem

Suppose p is not known. How many i.i.d. samples $X_1, \ldots, X_n \sim p$ are needed to decide w.h.p. whether $p = q$ or $d_{\mathrm{TV}}(p, q) \geq \epsilon$?

Theorem (Paninski, 2008)

If $q = (\frac{1}{d}, \frac{1}{d}, \ldots, \frac{1}{d})$, then $n = O(\sqrt{d}/\epsilon^2)$ samples are sufficient.

Theorem (Valiant–Valiant, 2014)

For any $q = (q_1, \ldots, q_d)$, $n = O(\sqrt{d}/\epsilon^2)$ samples are sufficient.

Introduction

Let $\rho \in \mathbb{C}^{d \times d}$ and $\sigma \in \mathbb{C}^{d \times d}$ be mixed quantum states.

Introduction

Let $\rho \in \mathbb{C}^{d \times d}$ and $\sigma \in \mathbb{C}^{d \times d}$ be mixed quantum states.

Problem

Suppose ρ is not known. How many copies $\rho^{\otimes n}$ of ρ are needed to decide w.h.p. whether $\rho = \sigma$ or $d_{\mathrm{tr}}(\rho, \sigma) \geq \epsilon$?

Introduction

Let $\rho \in \mathbb{C}^{d \times d}$ and $\sigma \in \mathbb{C}^{d \times d}$ be mixed quantum states.

Problem

Suppose ρ is not known. How many copies $\rho^{\otimes n}$ of ρ are needed to decide w.h.p. whether $\rho = \sigma$ or $d_{\mathrm{tr}}(\rho, \sigma) \geq \epsilon$?

Theorem (O'Donnell–Wright, 2015)

If $\sigma = \frac{\mathbb{1}}{d}$, then $n = O(d/\epsilon^2)$ copies are sufficient.

Introduction

Let $\rho \in \mathbb{C}^{d \times d}$ and $\sigma \in \mathbb{C}^{d \times d}$ be mixed quantum states.

Problem

Suppose ρ is not known. How many copies $\rho^{\otimes n}$ of ρ are needed to decide w.h.p. whether $\rho = \sigma$ or $d_{\mathrm{tr}}(\rho, \sigma) \geq \epsilon$?

Theorem (O'Donnell–Wright, 2015)

If $\sigma = \frac{\mathbb{1}}{d}$, then $n = O(d/\epsilon^2)$ copies are sufficient.

Theorem

For any $\sigma \in \mathbb{C}^{d \times d}$, $n = O(d/\epsilon^2)$ copies are sufficient.

Preliminaries

Representation theory

$\mathfrak{S}_n$ is the ***symmetric group*** of permutations on n letters.

[1] 1s omitted from notation; e.g. $(3, 2)$ denotes $(3, 2, 1^{n-5})$.

Preliminaries

Representation theory

$\mathfrak{S}_n$ is the ***symmetric group*** of permutations on n letters.

$\mathrm{cyc}(\pi)$ denotes the ***cycle type*** of a permutation $\pi \in \mathfrak{S}_n$.

$\mathrm{cyc}(\pi) = \mathrm{cyc}(\pi^{-1})$ and $\mathrm{cyc}(\pi\tau) = \mathrm{cyc}(\tau\pi)$ for all $\pi, \tau \in \mathfrak{S}_n$.

[1] 1s omitted from notation; e.g. $(3, 2)$ denotes $(3, 2, 1^{n-5})$.

Preliminaries

Representation theory

$\mathfrak{S}_n$ is the ***symmetric group*** of permutations on n letters.

$\mathrm{cyc}(\pi)$ denotes the ***cycle type*** of a permutation $\pi \in \mathfrak{S}_n$.

$\mathrm{cyc}(\pi) = \mathrm{cyc}(\pi^{-1})$ and $\mathrm{cyc}(\pi\tau) = \mathrm{cyc}(\tau\pi)$ for all $\pi, \tau \in \mathfrak{S}_n$.

A ***partition*** $\lambda = (\lambda_1, \ldots, \lambda_k)$ of n is a nonincreasing sequence of nonnegative integers such that $\lambda_1 + \cdots + \lambda_k = n$.[1]

[1] 1s omitted from notation; e.g. $(3, 2)$ denotes $(3, 2, 1^{n-5})$.

Preliminaries

Representation theory

$\mathfrak{S}_n$ is the ***symmetric group*** of permutations on n letters.

$\mathrm{cyc}(\pi)$ denotes the ***cycle type*** of a permutation $\pi \in \mathfrak{S}_n$.

$\mathrm{cyc}(\pi) = \mathrm{cyc}(\pi^{-1})$ and $\mathrm{cyc}(\pi\tau) = \mathrm{cyc}(\tau\pi)$ for all $\pi, \tau \in \mathfrak{S}_n$.

A ***partition*** $\lambda = (\lambda_1, \ldots, \lambda_k)$ of n is a nonincreasing sequence of nonnegative integers such that $\lambda_1 + \cdots + \lambda_k = n$.[1]

The ***power sum*** symmetric polynomial p_λ is defined by

$$p_\lambda(x_1, \ldots, x_d) = (x_1^{\lambda_1} + \cdots + x_d^{\lambda_1}) \cdots (x_1^{\lambda_k} + \cdots + x_d^{\lambda_k}).$$

[1] 1s omitted from notation; e.g. $(3,2)$ denotes $(3,2,1^{n-5})$.

Preliminaries

Representation theory

$\mathfrak{S}_n$ is the ***symmetric group*** of permutations on n letters.

$\mathrm{cyc}(\pi)$ denotes the ***cycle type*** of a permutation $\pi \in \mathfrak{S}_n$.

$\mathrm{cyc}(\pi) = \mathrm{cyc}(\pi^{-1})$ and $\mathrm{cyc}(\pi\tau) = \mathrm{cyc}(\tau\pi)$ for all $\pi, \tau \in \mathfrak{S}_n$.

A ***partition*** $\lambda = (\lambda_1, \ldots, \lambda_k)$ of n is a nonincreasing sequence of nonnegative integers such that $\lambda_1 + \cdots + \lambda_k = n$.[1]

The ***power sum*** symmetric polynomial p_λ is defined by

$$p_\lambda(x_1, \ldots, x_d) = (x_1^{\lambda_1} + \cdots + x_d^{\lambda_1}) \cdots (x_1^{\lambda_k} + \cdots + x_d^{\lambda_k}).$$

If $\lambda = (7, 4, 1)$, then

$$p_\lambda(x_1, x_2) = (x_1^7 + x_2^7) \cdot (x_1^4 + x_2^4) \cdot (x_1 + x_2).$$

[1] 1s omitted from notation; e.g. $(3, 2)$ denotes $(3, 2, 1^{n-5})$.

$\mathbb{C}\mathfrak{S}_n$ is the ***symmetric group algebra*** of linear combinations

$$a_1\pi_1 + \cdots + a_k\pi_k,$$

where $a_1, \ldots, a_k \in \mathbb{C}$ and $\pi_1, \ldots, \pi_k \in \mathfrak{S}_n$.

Preliminaries

Representation theory

$\mathbb{C}\mathfrak{S}_n$ is the ***symmetric group algebra*** of linear combinations

$$a_1\pi_1 + \cdots + a_k\pi_k,$$

where $a_1, \ldots, a_k \in \mathbb{C}$ and $\pi_1, \ldots, \pi_k \in \mathfrak{S}_n$.

Let $\mathcal{P}$ map permutations $\pi \in \mathfrak{S}_n$ to operators $\mathcal{P}(\pi)$ on $(\mathbb{C}^d)^{\otimes n}$:

$$\mathcal{P}(\pi) = x_1 \otimes \cdots \otimes x_n \longmapsto x_{\pi^{-1}(1)} \otimes \cdots \otimes x_{\pi^{-1}(n)}.$$

Preliminaries

Representation theory

$\mathbb{C}\mathfrak{S}_n$ is the ***symmetric group algebra*** of linear combinations

$$a_1\pi_1 + \cdots + a_k\pi_k,$$

where $a_1, \ldots, a_k \in \mathbb{C}$ and $\pi_1, \ldots, \pi_k \in \mathfrak{S}_n$.

Let $\mathcal{P}$ map permutations $\pi \in \mathfrak{S}_n$ to operators $\mathcal{P}(\pi)$ on $(\mathbb{C}^d)^{\otimes n}$:

$$\mathcal{P}(\pi) = x_1 \otimes \cdots \otimes x_n \longmapsto x_{\pi^{-1}(1)} \otimes \cdots \otimes x_{\pi^{-1}(n)}.$$

$\mathcal{P}$ is a ***representation*** of $\mathfrak{S}_n$:

$$\mathcal{P}(\pi\tau) = \mathcal{P}(\pi)\mathcal{P}(\tau), \quad \mathcal{P}(\mathrm{id}) = \mathbb{1}, \quad \mathcal{P}(\pi^{-1}) = \mathcal{P}(\pi)^\dagger.$$

Preliminaries

Quantum physics

Let $\mathscr{H}$ be finite-dimensional vector space over $\mathbb{C}$.

A ***quantum state*** ρ is a pos. operator on $\mathscr{H}$ with $\mathrm{tr}(\rho) = 1$.

Preliminaries

Quantum physics

Let $\mathscr{H}$ be finite-dimensional vector space over $\mathbb{C}$.

A ***quantum state*** ρ is a pos. operator on $\mathscr{H}$ with $\mathrm{tr}(\rho) = 1$.

An ***observable*** $\mathscr{O}$ is a self-adjoint operator on $\mathscr{H}$.

Preliminaries

Quantum physics

Let $\mathscr{H}$ be finite-dimensional vector space over $\mathbb{C}$.

A ***quantum state*** ρ is a pos. operator on $\mathscr{H}$ with $\mathrm{tr}(\rho) = 1$.

An ***observable*** $\mathscr{O}$ is a self-adjoint operator on $\mathscr{H}$.

By the spectral theorem,

$$\mathscr{O} = \alpha_1 \Pi_1 + \cdots + \alpha_d \Pi_d .$$

$\mathscr{M} = \{\Pi_1, \ldots, \Pi_d\}$ defines a measurement.

Let $\mathscr{H}$ be finite-dimensional vector space over $\mathbb{C}$.

A ***quantum state*** ρ is a pos. operator on $\mathscr{H}$ with $\mathrm{tr}(\rho) = 1$.

An ***observable*** $\mathscr{O}$ is a self-adjoint operator on $\mathscr{H}$.

By the spectral theorem,

$$\mathscr{O} = \alpha_1 \Pi_1 + \cdots + \alpha_d \Pi_d .$$

$\mathscr{M} = \{\Pi_1, \ldots, \Pi_d\}$ defines a measurement.

$\mathscr{O}$ has a natural operational interpretation:

> Apply $\mathscr{M}$ to ρ and output α_i if the outcome of the measurement is $i \in [d]$.

The ***expectation*** of $\mathcal{O}$ w.r.t. ρ is

$$\mathop{\mathbf{E}}_{\rho}[\mathcal{O}] := \mathrm{tr}(\rho\mathcal{O}).$$

Preliminaries

Quantum probability

The ***expectation*** of $\mathcal{O}$ w.r.t. ρ is

$$\mathop{\mathbf{E}}_{\rho}[\mathcal{O}] := \operatorname{tr}(\rho\mathcal{O}).$$

The ***variance*** of $\mathcal{O}$ w.r.t. ρ is

$$\mathop{\mathbf{Var}}_{\rho}[\mathcal{O}] := \mathop{\mathbf{E}}_{\rho}[\mathcal{O}^2] - \mathop{\mathbf{E}}_{\rho}[\mathcal{O}]^2.$$

Preliminaries

Quantum probability

The ***expectation*** of $\mathcal{O}$ w.r.t. ρ is

$$\mathop{\mathbf{E}}_{\rho}[\mathcal{O}] := \operatorname{tr}(\rho\mathcal{O}).$$

The ***variance*** of $\mathcal{O}$ w.r.t. ρ is

$$\mathop{\mathbf{Var}}_{\rho}[\mathcal{O}] := \mathop{\mathbf{E}}_{\rho}[\mathcal{O}^2] - \mathop{\mathbf{E}}_{\rho}[\mathcal{O}]^2.$$

Lemma

$\mathbf{E}_{\rho}[\cdot]$ *is monotone w.r.t. the order on self-adjoint operators, viz.*

$$A \leq B \implies \mathop{\mathbf{E}}_{\rho}[A] \leq \mathop{\mathbf{E}}_{\rho}[B].$$

Preliminaries

Quantum probability

Let Φ be a linear map that maps observables to observables such that $\mathbf{E}_\rho[\Phi(\mathcal{O})] = \mathbf{E}_\rho[\mathcal{O}]$.

[2] Φ is ***positive*** if $\Phi(A) \geq 0$ for all $A \geq 0$; Φ is ***unital*** if $\Phi(\mathbb{1}) = \mathbb{1}$.

Preliminaries

Quantum probability

Let Φ be a linear map that maps observables to observables such that $\mathbf{E}_\rho[\Phi(\mathcal{O})] = \mathbf{E}_\rho[\mathcal{O}]$.

Lemma

If Φ is positive and unital[2]*, then*

$$\mathop{\mathbf{Var}}_{\rho}[\Phi(\mathcal{O})] \leq \mathop{\mathbf{Var}}_{\rho}[\mathcal{O}].$$

[2] Φ is ***positive*** if $\Phi(A) \geq 0$ for all $A \geq 0$; Φ is ***unital*** if $\Phi(\mathbb{1}) = \mathbb{1}$.

Preliminaries

Quantum probability

Let Φ be a linear map that maps observables to observables such that $\mathbf{E}_\rho[\Phi(\mathcal{O})] = \mathbf{E}_\rho[\mathcal{O}]$.

Lemma

If Φ is positive and unital[2]*, then*

$$\underset{\rho}{\mathbf{Var}}[\Phi(\mathcal{O})] \leq \underset{\rho}{\mathbf{Var}}[\mathcal{O}].$$

Proof.

By Kadison's inequality, $\Phi(\mathcal{O})^2 \leq \Phi(\mathcal{O}^2)$. Hence, by monotonicity of $\mathbf{E}_\rho$,

$$\underset{\rho}{\mathbf{E}}[\Phi(\mathcal{O})^2] \leq \underset{\rho}{\mathbf{E}}[\Phi(\mathcal{O}^2)] = \underset{\rho}{\mathbf{E}}[\mathcal{O}^2]. \qquad \blacksquare$$

[2] Φ is ***positive*** if $\Phi(A) \geq 0$ for all $A \geq 0$; Φ is ***unital*** if $\Phi(\mathbb{1}) = \mathbb{1}$.

Preliminaries

Measures of distance between quantum states

The ***trace distance*** between ρ and σ is

$$d_{\mathrm{tr}}(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_1 = \frac{1}{2}\,\mathrm{tr}(|\rho-\sigma|).$$

The ***Hilbert–Schmidt distance*** between ρ and σ is

$$d_{\mathrm{HS}}(\rho,\sigma) = \|\rho-\sigma\|_2 = \sqrt{\mathrm{tr}((\rho-\sigma)^2)}.$$

The ***squared Hilbert–Schmidt distance*** between ρ and σ is

$$\begin{aligned} d_{\mathrm{HS}}^2(\rho,\sigma) &= \|\rho-\sigma\|_2^2 = \mathrm{tr}((\rho-\sigma)^2) \\ &= \mathrm{tr}(\rho^2) + \mathrm{tr}(\sigma^2) - 2\,\mathrm{tr}(\rho\sigma). \end{aligned}$$

Preliminaries

Measures of distance between quantum states

If ρ and σ are d-dimensional quantum states, then

$$\frac{1}{2} d_{\mathrm{HS}}(\rho, \sigma) \leq d_{\mathrm{tr}}(\rho, \sigma) \leq \frac{\sqrt{d}}{2} d_{\mathrm{HS}}(\rho, \sigma).$$

Preliminaries

Measures of distance between quantum states

If ρ and σ are d-dimensional quantum states, then

$$\frac{1}{2} d_{\mathrm{HS}}(\rho, \sigma) \leq d_{\mathrm{tr}}(\rho, \sigma) \leq \frac{\sqrt{d}}{2} d_{\mathrm{HS}}(\rho, \sigma).$$

We will show that:

Theorem

For any $\sigma \in \mathbb{C}^{d \times d}$, $n = O(1/\epsilon)$ copies are sufficient to decide w.h.p. whether $\rho = \sigma$ or $d_{\mathrm{HS}}^2(\rho, \sigma) \geq \epsilon$.

Quantum state certification

Problem

Given measurement access to $\varrho := \rho^{\otimes n}$*, decide w.h.p. whether* $\rho = \sigma$ *or* $d_{\mathrm{HS}}^2(\rho, \sigma) \geq \epsilon$*.*

Quantum state certification

Problem

Given measurement access to $\varrho := \rho^{\otimes n}$, decide w.h.p. whether $\rho = \sigma$ or $d_{\mathrm{HS}}^2(\rho, \sigma) \geq \epsilon$.

Solution

Find an observable $\mathcal{O}$ such that:

1. $\mathbf{E}_{\varrho}[\mathcal{O}] = d_{\mathrm{HS}}^2(\rho, \sigma)$;
2. *the distribution defined by $\mathcal{O}$ and ϱ is sufficiently concentrated around its mean.*

Quantum state certification

Problem

Given measurement access to $\varrho := \rho^{\otimes n}$, *decide w.h.p. whether* $\rho = \sigma$ *or* $d_{\mathrm{HS}}^2(\rho, \sigma) \geq \epsilon$.

Solution

Find an observable $\mathcal{O}$ *such that:*

1. $\mathbf{E}_\varrho[\mathcal{O}] = d_{\mathrm{HS}}^2(\rho, \sigma)$;
2. *the distribution defined by* $\mathcal{O}$ *and* ϱ *is sufficiently concentrated around its mean.*

By Chebyshev's inequality,

$$\mathop{\mathbf{Var}}_{\varrho}[\mathcal{O}] = O\left(\frac{1}{n^2} + \frac{d_{\mathrm{HS}}^2(\rho, \sigma)}{n}\right)$$

suffices.

Quantum state certification

Henceforth, assume $\sigma = \frac{\mathbb{1}}{d}$.

The following proof technique extends easily to arbitrary σ.

Quantum estimators

Let $\varrho := \rho^{\otimes n}$ and let $f : \mathbb{C}^{d \times d} \to \mathbb{R}$ be a statistic.

Quantum estimators

Let $\varrho := \rho^{\otimes n}$ and let $f : \mathbb{C}^{d \times d} \to \mathbb{R}$ be a statistic.

A ***quantum estimator*** for f is an observable $\mathcal{O}$ such that $\mathbf{E}_{\varrho}[\mathcal{O}] = f(\rho)$.

Quantum estimators

Let $\varrho := \rho^{\otimes n}$ and let $f : \mathbb{C}^{d \times d} \to \mathbb{R}$ be a statistic.

A ***quantum estimator*** for f is an observable $\mathcal{O}$ such that $\mathbf{E}_{\varrho}[\mathcal{O}] = f(\rho)$.

$\mathcal{O}$ is ***efficient*** if $\mathbf{Var}_{\varrho}[\mathcal{O}]$ is minimum.

Quantum estimators

Let $\varrho := \rho^{\otimes n}$ and let $f : \mathbb{C}^{d \times d} \to \mathbb{R}$ be a statistic.

A ***quantum estimator*** for f is an observable $\mathcal{O}$ such that $\mathbf{E}_\varrho[\mathcal{O}] = f(\rho)$.

$\mathcal{O}$ is ***efficient*** if $\mathbf{Var}_\varrho[\mathcal{O}]$ is minimum.

Since $d_{\mathrm{HS}}^2(\rho, \frac{\mathbb{1}}{d}) = \mathrm{tr}(\rho^2) - \frac{1}{d}$, it suffices to estimate the ***purity*** $f(\rho) := \mathrm{tr}(\rho^2)$.

Quantum estimators

Let $\varrho := \rho^{\otimes n}$ and let $f : \mathbb{C}^{d \times d} \to \mathbb{R}$ be a statistic.

A ***quantum estimator*** for f is an observable $\mathcal{O}$ such that $\mathbf{E}_\varrho[\mathcal{O}] = f(\rho)$.

$\mathcal{O}$ is ***efficient*** if $\mathbf{Var}_\varrho[\mathcal{O}]$ is minimum.

Since $d_{\mathrm{HS}}^2(\rho, \frac{\mathbb{1}}{d}) = \operatorname{tr}(\rho^2) - \frac{1}{d}$, it suffices to estimate the ***purity*** $f(\rho) := \operatorname{tr}(\rho^2)$.

Since f is ***unitarily invariant***, i.e. $f(\rho) = f(U\rho U^\dagger)$ for all $U \in \mathrm{U}(d)$,

$$
\begin{aligned}
\mathop{\mathbf{E}}_{\varrho}[(U^\dagger)^{\otimes n} \mathcal{O} U^{\otimes n}] &= \operatorname{tr}((U\rho U^\dagger)^{\otimes n} \mathcal{O}) \\
&= f(U\rho U^\dagger) \\
&= f(\rho).
\end{aligned}
$$

Quantum estimators

Let Φ denote the averaging map

$$\Phi(\mathcal{O}) = \int_{\mathrm{U}(d)} (U^\dagger)^{\otimes n} \mathcal{O} U^{\otimes n} dU.$$

If $\mathcal{O}$ is an estimator for f, then $\Phi(\mathcal{O})$ is an estimator for f.

Quantum estimators

Let Φ denote the averaging map

$$\Phi(\mathcal{O}) = \int\limits_{\mathrm{U}(d)} (U^\dagger)^{\otimes n} \mathcal{O} U^{\otimes n} \, dU.$$

If $\mathcal{O}$ is an estimator for f, then $\Phi(\mathcal{O})$ is an estimator for f.

Since Φ is mean-preserving, positive, and unital,

$$\operatorname*{\mathbf{Var}}_{\varrho}[\Phi(\mathcal{O})] \leq \operatorname*{\mathbf{Var}}_{\varrho}[\mathcal{O}].$$

Quantum estimators

Let Φ denote the averaging map

$$\Phi(\mathcal{O}) = \int_{\mathrm{U}(d)} (U^\dagger)^{\otimes n} \mathcal{O} U^{\otimes n} dU.$$

If $\mathcal{O}$ is an estimator for f, then $\Phi(\mathcal{O})$ is an estimator for f.

Since Φ is mean-preserving, positive, and unital,

$$\mathbf{\underset{\varrho}{Var}}[\Phi(\mathcal{O})] \leq \mathbf{\underset{\varrho}{Var}}[\mathcal{O}].$$

Proposition

The map Φ is a projection into $\mathcal{P}(\mathbb{C}\mathfrak{S}_n)$.

Proof.

The statement follows from Schur–Weyl duality. ∎

Quantum estimators

If $X = a_1\pi_1 + \cdots + a_k\pi_k \in \mathbb{C}\mathfrak{S}_n$, then

$$\mathcal{P}(X) = a_1\mathcal{P}(\pi_1) + \cdots + a_k\mathcal{P}(\pi_k).$$

[3] If $\varrho = \rho_1 \otimes \rho_2 \otimes \rho_3 \otimes \rho_4 \otimes \rho_5$, $\mathbf{E}_\varrho[\mathcal{P}((1\ 2\ 3)(4\ 5))] = \mathrm{tr}(\rho_3\rho_2\rho_1)\,\mathrm{tr}(\rho_5\rho_4)$.

Quantum estimators

If $X = a_1\pi_1 + \cdots + a_k\pi_k \in \mathbb{C}\mathfrak{S}_n$, then

$$\mathcal{P}(X) = a_1\mathcal{P}(\pi_1) + \cdots + a_k\mathcal{P}(\pi_k).$$

Corollary

To find an efficient estimator for f, it suffices to consider estimators of the form $\mathcal{P}(X)$ for $X \in \mathbb{C}\mathfrak{S}_n$.

[3] If $\varrho = \rho_1 \otimes \rho_2 \otimes \rho_3 \otimes \rho_4 \otimes \rho_5$, $\mathbf{E}_\varrho[\mathcal{P}((1\ 2\ 3)(4\ 5))] = \mathrm{tr}(\rho_3\rho_2\rho_1)\,\mathrm{tr}(\rho_5\rho_4)$.

Quantum estimators

If $X = a_1\pi_1 + \cdots + a_k\pi_k \in \mathbb{C}\mathfrak{S}_n$, then

$$\mathcal{P}(X) = a_1\mathcal{P}(\pi_1) + \cdots + a_k\mathcal{P}(\pi_k).$$

Corollary

To find an efficient estimator for f, it suffices to consider estimators of the form $\mathcal{P}(X)$ for $X \in \mathbb{C}\mathfrak{S}_n$.

Lemma

If $\varrho = \rho^{\otimes n}$ and $\lambda = \mathrm{cyc}(\pi) = (\lambda_1, \ldots, \lambda_k)$, then

$$\mathop{\mathbf{E}}_{\varrho}[\mathcal{P}(\pi)] = p_\lambda(\alpha),$$

where α is the sorted spectrum of ρ.[3]

[3] If $\varrho = \rho_1 \otimes \rho_2 \otimes \rho_3 \otimes \rho_4 \otimes \rho_5$, $\mathbf{E}_\varrho[\mathcal{P}((1\ 2\ 3)(4\ 5))] = \mathrm{tr}(\rho_3\rho_2\rho_1)\,\mathrm{tr}(\rho_5\rho_4)$.

Quantum estimators

If $X = a_1\pi_1 + \cdots + a_k\pi_k \in \mathbb{C}\mathfrak{S}_n$, then

$$\mathcal{P}(X) = a_1\mathcal{P}(\pi_1) + \cdots + a_k\mathcal{P}(\pi_k).$$

Corollary

To find an efficient estimator for f, it suffices to consider estimators of the form $\mathcal{P}(X)$ for $X \in \mathbb{C}\mathfrak{S}_n$.

Lemma

If $\varrho = \rho^{\otimes n}$ and $\lambda = \mathrm{cyc}(\pi) = (\lambda_1, \ldots, \lambda_k)$, then

$$\mathop{\mathbf{E}}_{\varrho}[\mathcal{P}(\pi)] = p_\lambda(\alpha),$$

where α is the sorted spectrum of ρ.[3]

Note that $\mathbf{E}_\varrho[\mathcal{P}(\pi)]$ depends only on $\lambda = \mathrm{cyc}(\pi)$.

[3] If $\varrho = \rho_1 \otimes \rho_2 \otimes \rho_3 \otimes \rho_4 \otimes \rho_5$, $\mathbf{E}_\varrho[\mathcal{P}((1\ 2\ 3)(4\ 5))] = \mathrm{tr}(\rho_3\rho_2\rho_1)\,\mathrm{tr}(\rho_5\rho_4)$.

Quantum estimators

Since $\mathrm{cyc}(\pi_1\pi_2) = \mathrm{cyc}(\pi_2\pi_1)$, it follows that

$$\mathop{\mathbf{E}}_{\varrho}[\mathcal{P}(X)] = \mathop{\mathbf{E}}_{\varrho}[\mathcal{P}(\pi^{-1}X\pi)] \text{ for all } \pi \in \mathfrak{S}_n.$$

Quantum estimators

Since $\mathrm{cyc}(\pi_1\pi_2) = \mathrm{cyc}(\pi_2\pi_1)$, it follows that

$$\mathop{\mathbf{E}}_{\varrho}[\mathcal{P}(X)] = \mathop{\mathbf{E}}_{\varrho}[\mathcal{P}(\pi^{-1}X\pi)] \text{ for all } \pi \in \mathfrak{S}_n.$$

Hence, if $\mathcal{P}(X)$ is an estimator for f, then $\mathcal{P}(\overline{X})$ with

$$\overline{X} = \frac{1}{n!}\sum_{\pi\in\mathfrak{S}_n} \pi^{-1}X\pi$$

is an estimator for f such that $\mathbf{Var}_{\varrho}[\mathcal{P}(\overline{X})] \leq \mathbf{Var}_{\varrho}[\mathcal{P}(X)]$.

Quantum estimators

Lemma

$\overline{X}$ commutes with all elements of $\mathbb{C}\mathfrak{S}_n$, i.e. $\overline{X}Y = Y\overline{X}$ for all $Y \in \mathbb{C}\mathfrak{S}_n$. Moreover, $\overline{X}$ can expressed uniquely as

$$\overline{X} = \sum_{\mu \vdash n} a_\mu X_\mu, \quad \textit{where} \quad X_\mu = \operatorname*{avg}_{\substack{\pi \in \mathfrak{S}_n \\ \mathrm{cyc}(\pi) = \mu}} \{\pi\}.$$

Quantum estimators

Lemma

$\overline{X}$ commutes with all elements of $\mathbb{C}\mathfrak{S}_n$, i.e. $\overline{X}Y = Y\overline{X}$ for all $Y \in \mathbb{C}\mathfrak{S}_n$. Moreover, $\overline{X}$ can expressed uniquely as

$$\overline{X} = \sum_{\mu \vdash n} a_\mu X_\mu, \quad \textit{where} \quad X_\mu = \operatorname*{avg}_{\substack{\pi \in \mathfrak{S}_n \\ \mathrm{cyc}(\pi) = \mu}} \{\pi\}.$$

Lemma

$\mathcal{P}(\overline{X})$ is the unique estimator for f that commutes with all elements of $\mathcal{P}(\mathbb{C}\mathfrak{S}_n)$.

Quantum estimators

Lemma

$\overline{X}$ commutes with all elements of $\mathbb{C}\mathfrak{S}_n$, i.e. $\overline{X}Y = Y\overline{X}$ for all $Y \in \mathbb{C}\mathfrak{S}_n$. Moreover, $\overline{X}$ can expressed uniquely as

$$\overline{X} = \sum_{\mu \vdash n} a_\mu X_\mu, \quad \textit{where} \quad X_\mu = \operatorname*{avg}_{\substack{\pi \in \mathfrak{S}_n \\ \mathrm{cyc}(\pi) = \mu}} \{\pi\}.$$

Lemma

$\mathcal{P}(\overline{X})$ is the unique estimator for f that commutes with all elements of $\mathcal{P}(\mathbb{C}\mathfrak{S}_n)$.

Corollary

$\mathcal{P}(\overline{X})$ is efficient.

Quantum state certification

Problem

Given measurement access to $\varrho := \rho^{\otimes n}$*, decide w.h.p. whether* $\rho = \sigma$ *or* $d_{\mathrm{HS}}^2(\rho, \sigma) \geq \epsilon$*.*

Quantum state certification

Problem

Given measurement access to $\varrho := \rho^{\otimes n}$*, decide w.h.p. whether* $\rho = \sigma$ *or* $d^2_{\mathrm{HS}}(\rho, \sigma) \geq \epsilon$*.*

Solution

Let $\mu := (2)$ *and* $\boxed{\mathcal{O} := \mathcal{P}(X_\mu).}$ *Thus,*

$$\mathop{\mathbf{E}}_{\varrho}[\mathcal{O}] = p_\mu(\alpha) = \alpha_1^2 + \cdots + \alpha_d^2 = \mathrm{tr}(\rho^2).$$

Quantum state certification

Problem

Given measurement access to $\varrho := \rho^{\otimes n}$*, decide w.h.p. whether* $\rho = \sigma$ *or* $d_{\mathrm{HS}}^2(\rho, \sigma) \geq \epsilon$*.*

Solution

Let $\mu := (2)$ *and* $\boxed{\mathcal{O} := \mathcal{P}(X_\mu).}$ *Thus,*

$$\mathop{\mathbf{E}}_{\varrho}[\mathcal{O}] = p_\mu(\alpha) = \alpha_1^2 + \cdots + \alpha_d^2 = \mathrm{tr}(\rho^2).$$

Since $\mathcal{O}^2 = \mathcal{P}(X_\mu) \cdot \mathcal{P}(X_\mu) = \mathcal{P}(X_\mu^2)$ and

$$X_{(2)}^2 = \frac{1}{\binom{n}{2}} \mathrm{id} + \frac{2(n-2)}{\binom{n}{2}} X_{(3)} + \frac{\binom{n-2}{2}}{\binom{n}{2}} X_{(2,2)},$$

$\mathbf{Var}_\varrho[\mathcal{O}]$ can be computed exactly.

Quantum state certification

Problem

Given measurement access to $\varrho := \rho^{\otimes n}$, decide w.h.p. whether $\rho = \sigma$ or $d_{\mathrm{HS}}^2(\rho, \sigma) \geq \epsilon$.

Solution

Let $\mu := (2)$ and $\boxed{\mathcal{O} := \mathcal{P}(X_\mu).}$ Thus,

$$\mathop{\mathbf{E}}_{\varrho}[\mathcal{O}] = p_\mu(\alpha) = \alpha_1^2 + \cdots + \alpha_d^2 = \mathrm{tr}(\rho^2).$$

We obtain

$$\mathop{\mathbf{Var}}_{\varrho}[\mathcal{O}] = O\left(\frac{1}{n^2} + \frac{d_{\mathrm{HS}}^2(\rho, \frac{\mathbb{1}}{d})}{n}\right),$$

as needed.

Quantum state certification

For $\sigma \in \mathbb{C}^{d \times d}$ arbitrary:

Quantum state certification

For $\sigma \in \mathbb{C}^{d \times d}$ arbitrary:

- Given access to $\rho^{\otimes n}$, prepare $\varrho := \rho^{\otimes n} \otimes \sigma^{\otimes n}$.

Quantum state certification

For $\sigma \in \mathbb{C}^{d \times d}$ arbitrary:

- Given access to $\rho^{\otimes n}$, prepare $\varrho := \rho^{\otimes n} \otimes \sigma^{\otimes n}$.
- Let $f(\rho, \sigma) = d_{\mathrm{HS}}^2(\rho, \sigma)$. Thus,

$$f(U\rho U^\dagger, U\sigma U^\dagger) = f(\rho, \sigma) \text{ for all } U \in \mathrm{U}(d).$$

Quantum state certification

For $\sigma \in \mathbb{C}^{d \times d}$ arbitrary:

- Given access to $\rho^{\otimes n}$, prepare $\varrho := \rho^{\otimes n} \otimes \sigma^{\otimes n}$.
- Let $f(\rho, \sigma) = d_{\mathrm{HS}}^2(\rho, \sigma)$. Thus,

$$f(U\rho U^\dagger, U\sigma U^\dagger) = f(\rho, \sigma) \text{ for all } U \in \mathrm{U}(d).$$

- Consider observables $\mathcal{O}$ with $\mathbf{E}_\varrho[\mathcal{O}] = f(\rho, \sigma)$.

Quantum state certification

For $\sigma \in \mathbb{C}^{d \times d}$ arbitrary:

- Given access to $\rho^{\otimes n}$, prepare $\varrho := \rho^{\otimes n} \otimes \sigma^{\otimes n}$.
- Let $f(\rho, \sigma) = d_{\mathrm{HS}}^2(\rho, \sigma)$. Thus,

$$f(U\rho U^\dagger, U\sigma U^\dagger) = f(\rho, \sigma) \text{ for all } U \in \mathrm{U}(d).$$

- Consider observables $\mathcal{O}$ with $\mathbf{E}_\varrho[\mathcal{O}] = f(\rho, \sigma)$.
- Efficient estimators defined by orbits of action

$$\mathfrak{S}_n \times \mathfrak{S}_n \curvearrowright \mathfrak{S}_{2n}.$$

Conclusion

- Method to construct efficient estimators for symmetric polynomials of the spectrum.

Conclusion

- Method to construct efficient estimators for symmetric polynomials of the spectrum.
- State certification algorithm is **robust**; i.e. decides w.h.p. whether $d_{\mathrm{tr}}(\rho, \sigma) \leq 0.99\epsilon$ or $d_{\mathrm{tr}}(\rho, \sigma) \geq \epsilon$.

Conclusion

- Method to construct efficient estimators for symmetric polynomials of the spectrum.
- State certification algorithm is **robust**; i.e. decides w.h.p. whether $d_{\mathrm{tr}}(\rho, \sigma) \leq 0.99\epsilon$ or $d_{\mathrm{tr}}(\rho, \sigma) \geq \epsilon$.
- Algorithm works if both ρ and σ are unknown.

Conclusion

- Method to construct efficient estimators for symmetric polynomials of the spectrum.
- State certification algorithm is **robust**; i.e. decides w.h.p. whether $d_{\mathrm{tr}}(\rho, \sigma) \leq 0.99\epsilon$ or $d_{\mathrm{tr}}(\rho, \sigma) \geq \epsilon$.
- Algorithm works if both ρ and σ are unknown.
- If either ρ or σ is close to a state of rank k, $n = O(k/\epsilon^2)$ copies are sufficient.

Conclusion

- Method to construct efficient estimators for symmetric polynomials of the spectrum.
- State certification algorithm is **robust**; i.e. decides w.h.p. whether $d_{\mathrm{tr}}(\rho, \sigma) \leq 0.99\epsilon$ or $d_{\mathrm{tr}}(\rho, \sigma) \geq \epsilon$.
- Algorithm works if both ρ and σ are unknown.
- If either ρ or σ is close to a state of rank k, $n = O(k/\epsilon^2)$ copies are sufficient.
- Other result: for all states $\sigma \in \mathbb{C}^{d \times d}$ and $\epsilon > 0$,

Theorem

$n = O(d/\epsilon)$ copies of ρ are sufficient to decide w.h.p. whether $\rho = \sigma$ or $\mathrm{F}(\rho, \sigma) < 1 - \epsilon$.

Thank you!

`arXiv:1708.06002`