Quantum state testing beyond the polarizing regime and quantum triangular discrimination

arXiv:2303.01952

Yupan Liu

Graduate School of Mathematics, Nagoya University

LA Symposium 2023, 夏の LA
July 4, 2023

1. Quantum state testing and the class QSZK
2. Main result: quantum state testing beyond the polarizing regime
3. Which parameter regime is easy for the class QSZK?
4. Open problems

Statistical Difference Problem meets statistical zero-knowledge

Definition 1.1 (Statistical zero-knowledge, informal) An interactive proof protocol admits the *(statistical) zero-knowledge* property if verifier's view ($\mathcal{P}_0$) is *(statistically) indistinguishable* from "verifier's view" ($\mathcal{P}_1$) generated by a poly-time simulator.

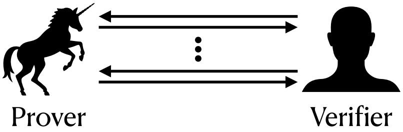

Figure: Verifier's view $\mathcal{P}_0$

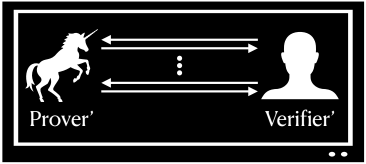

Figure: Simulated "Verifier's view" ($\mathcal{P}_1$)

- **Public-coin is sufficient.** All SZK protocols can be transformed into a form that all messages from verifier (V) to prover (P) are *public coins* [Okamoto'00].
- Intuitively, the views $\mathcal{P}_0$ and $\mathcal{P}_1$ can be treated as distributions p_0 and p_1, respectively. Then *statistical indistinguishablity* is on $\mathrm{SD}(p_0, p_1) := \frac{1}{2}\|p_0 - p_1\|_1$.

Definition 1.2 (Statistical Difference Problem, SDP) [SV03]. Given efficiently sampable (namely, using polynomial-size Boolean circuits) distributions p_0 and p_1, decide whether $\mathrm{SD}(p_0, p_1) \geq \alpha$ or $\mathrm{SD}(p_0, p_1) \leq \beta$.

Theorem 1.3 [Sahai-Vadhan'03, Goldreich-Sahai-Vadhan'98]. Statistical Difference Problem is SZK-complete. Specifically, (α, β)-SDP is in SZK if $\alpha^2 - \beta > 0$ for constant α and β.

From quantum ℓ_1 norm to Quantum State Distinguishability Problem

An n-qubit quantum state ρ is a $2^n \times 2^n$ matrix such that $\mathrm{Tr}(\rho) = 1$ and $\rho \succeq 0$.

Classical and quantum ℓ_1 norms

- Classical: statistical distance $\mathrm{SD}(p_0, p_1) = \frac{1}{2} \sum_{x \in \mathcal{S}} |p_0(x) - p_1(x)|$.
- Q (option 1): trace distance $\mathrm{td}(\rho_0, \rho_1) := \frac{1}{2} \mathrm{Tr}|\rho_0 - \rho_1|$.
- Q (option 2): "measured ℓ_1 distance" $\mathrm{td}^{\mathrm{meas}}(\rho_0, \rho_1) := \sup_{\mathcal{E}} \left\{ \mathrm{SD}\left(p_0^{(\mathcal{E})}, p_1^{(\mathcal{E})}\right) \right\}$:
  - measurement $\mathcal{E} = (E_1, \cdots, E_{2^n})$ such that $\sum_i E_i = I$ and $E_i \succeq 0 \ \forall i$;
  - induced distribution $p_k^{(\mathcal{E})} = (\mathrm{Tr}(\rho_k E_1), \cdots, \mathrm{Tr}(\rho_k E_{2^n}))$ for $k \in \{0, 1\}$.

Theorem 1.4 [Helstrom'76]. For any ρ_0 and ρ_1, $\mathrm{td}(\rho_0, \rho_1) = \mathrm{td}^{\mathrm{meas}}(\rho_0, \rho_1)$.

Definition 1.5 (Quantum State Distinguishability Problem, QSDP) [Wat02]. Given efficiently preparable (namely, using polynomial-size quantum circuits) quantum states ρ_0 and ρ_1, decide whether $\mathrm{td}(\rho_0, \rho_1) \geq \alpha$ or $\mathrm{td}(\rho_0, \rho_1) \leq \beta$.

Theorem 1.6 [Watrous'02, Watrous'09]. Quantum State Distinguishability Problem is QSZK-complete. Specifically, (α, β)-QSDP is in QSZK if $\alpha^2 - \beta > 0$ for const α and β.

Polarization lemma: SZK and QSZK containments

Polarization lemma [Sahai-Vadhan'03]

There is an efficient algorithm to construct p'_k for $k \in \{0,1\}$ such that

- Yes: $\mathrm{SD}(p_0, p_1) \geq \alpha$;
- No: $\mathrm{SD}(p_0, p_1) \leq \beta$;

where the dimension of p_k is 2^n.

- Yes: $\mathrm{SD}(p'_0, p'_1) \geq 1 - \epsilon$;
- No: $\mathrm{SD}(p'_0, p'_1) \leq \epsilon$;

where the dimension of p'_k is $2^n \cdot \ln(1/\epsilon)$.

The construction of (p'_0, p'_1) is based on an appropriate composition of:

- Direct product lemma (*yes* instances): $(p_0^{\otimes l}, p_1^{\otimes l})$;
- XOR lemma (*no* instances): $\left(2^{-l} \sum_{i_1 \oplus \cdots \oplus i_l = 0} p_{i_1} \otimes \cdots \otimes p_{i_l}, 2^{-l} \sum_{i_1 \oplus \cdots \oplus i_l = 1} p_{i_1} \otimes \cdots \otimes p_{i_l}\right)$.

By inspection, the proof techniques in [SV03] can achieve:

Theorem 2.1 [SV03,GSV98]. (α, β)-SDP is in SZK if $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$.

Theorem 2.2 [Wat02,Wat06]. (α, β)-QSDP is in QSZK if $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$.

- **Q1:** What about the parameter regime $\alpha^2 < \beta < \alpha$?
- **Q2:** Could we make the promise gap $\alpha^2(n) - \beta(n) \geq 1/\mathrm{poly}(n)$?

Main result on quantum state testing and QSZK

Theorem 2.3 [Berman-Degwekar-Rothblum-Vasudevan'19]. (α,β)-SDP is in SZK if $\alpha^2(n)-\beta(n)\geq 1/\mathrm{poly}(n)$. Additionally, there are two new SZK-complete problems:

- Jensen-Shannon Divergence Problem: (α,β)-JSP is in SZK if $\alpha-\beta\geq 1/\mathrm{poly}$.
- Triangular Discrimination Problem: (α,β)-TDP is in SZK if $\alpha-\beta\geq 1/\mathrm{poly}$;

- Examining *existing approaches* to polarization: TDP $\leftrightarrow$ original polarization lemma [SV03] and JSP $\leftrightarrow$ entropy extraction based polarization [GV99];
- **Proof** by reductions: Entropy Difference $\to$ JSP $\to$ TDP $\to$ $1/\mathrm{poly}$-SDP.

Theorem 2.4. (α,β)-QSDP is in QSZK if $\alpha^2-\sqrt{2\ln 2}\beta\geq 1/\mathrm{poly}$. In addition, there are two new QSZK-complete problems:

- Quantum Jensen-Shannon Divergence Problem: (α,β)-QJSP is in QSZK if $\alpha(n)-\beta(n)\geq 1/\mathrm{poly}(n)$.
- Measured Quantum Triangular Discrimination Problem: (α,β)-measQTDP is in QSZK if $\alpha(n)-\beta(n)\geq 1/O(\log n)$;

What we need: Quantum counterparts of classical distances...

Quantum analogues of the triangular discrimination

Triangular discrimination: $\mathrm{TD}(p_0, p_1) := \frac{1}{2}\sum_{x\in\mathcal{S}} \frac{(p_0(x)-p_1(x))^2}{p_0(x)+p_1(x)}$.

Quantum analogues of the triangular discrimination

- Option 1: $\mathrm{QTD}(\rho_0,\rho_1) := \frac{1}{2}\mathrm{Tr}\Big((\rho_0-\rho_1)(\rho_0+\rho_1)^{-1/2}(\rho_0-\rho_1)(\rho_0+\rho_1)^{-1/2}\Big)$;
- Option 2: $\mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) := \sup_{\text{measurement } \mathcal{E}} \Big\{\mathrm{TD}\Big(p_0^{(\mathcal{E})}, p_1^{(\mathcal{E})}\Big)\Big\}$.

Theorem 2.5. Inequalities on quantum analogues of triangular discrimination:

	Classical	Quantum
SD vs. TD	$\mathrm{SD}^2 \leq \mathrm{TD} \leq \mathrm{SD}$ [Topsøe'00]	$\mathrm{td}^2 \leq \mathrm{QTD}^{\mathrm{meas}} \leq \mathrm{QTD} \leq \mathrm{td}$
JS vs. TD	$\frac{1}{2}\mathrm{TD} \leq \mathrm{JS} \leq \ln 2 \cdot \mathrm{TD}$ [Topsøe'00]	$\frac{1}{2}\mathrm{QTD}^2 \leq \mathrm{QJS} \leq \mathrm{QTD}$
TD vs. H^2	$\mathrm{H}^2 \leq \mathrm{TD} \leq 2\mathrm{H}^2$ [Le Cam'86]	$\frac{1}{2}\mathrm{B}^2 \leq \mathrm{QTD}^{\mathrm{meas}} \leq \mathrm{B}^2$ $\frac{1}{2}\mathrm{B}^2 \leq \mathrm{QTD} \leq \mathrm{B}$

Easy regimes for the class QSZK

Theorem 3.1 (Easy regimes for the class QSZK).

Parameter regimes	$(1-\epsilon,\epsilon)$-$\overline{\mathrm{SDP}}$	$(1-\epsilon,\epsilon)$-$\overline{\mathrm{QSDP}}$
$\epsilon = 0$	in NP Folklore	in BQP This work
$\epsilon \leq 2^{-n/2-1}$	in PP [Bouland-Chen-Holden-Thaler-Vasudevan'19]	in PP This work
$\epsilon \geq 2^{-n^{1/2-\gamma}}$ for $\gamma \in (0,1/2)$	SZK-hard Implicitly in [Sahai-Vadhan'03]	QSZK-hard Implicitly in [Watrous'02]

The proof is mainly based on different usages of the SWAP test [Buhrman-Cleve-Watrous-de Wolf'01].

Corollary 3.2. Length-preserving polarization seems impossible unless QSZK $\subseteq$ PP.

1. Quantum state testing and the class QSZK
2. Main result: quantum state testing beyond the polarizing regime
3. Which parameter regime is easy for the class QSZK?
4. Open problems

Conclusions and open problems

Take-home messages

1. A classical distance may have *several* quantum counterpart, and a *unique* counterpart will make our life much easier.
2. We define two quantum counterparts of the triangular discrimination, and demonstrate inequalities between these distances and other common distances.
3. By employing these inequalities, we improve the QSZK containment of QSDP to *non-polarizing regimes* via two new QSZK-complete problems.
4. Easy regimes for QSZK indicates that length-preserving polarization seems impossible unless QSZK $\subseteq$ PP.

Open problems

1. Is there any *other applications* of these quantum analogues of the triangular discrimination? For instance, triangular discrmination can be used to improve the communication compleixty lower bound of the point chasing problem [Yehudayoff'20].
2. Better upper bound for (α,β)-QSDP with $\alpha-\beta \geq 1/\mathrm{poly}$? The best known bound is PSPACE which is implicitly shown in [Watrous'02].
3. Quantum analogue of the set lower bound protocol and better bounds for QSZK?

Thanks!