Space-bounded quantum interactive proof systems

François Le Gall [1] **Yupan Liu** [3] Harumichi Nishimura [1] Qisheng Wang [2,1]

[1]Nagoya University

[2]University of Edinburgh

[3]Nagoya University → École Polytechnique Fédérale de Lausanne

Available on arXiv:2410.23958.

IQC Math & CS Seminar, University of Waterloo, August 2025

1. Space-bounded quantum computation meets interactive proofs
2. Definitions of space-bounded quantum interactive proof systems
3. Main results on $\mathsf{QIP_UL}$, QIPL, and $\mathsf{QSZK_UL}$
4. Open problems

Intermediate measurements in time-bounded quantum computation

Time-bounded quantum computation (BQP):

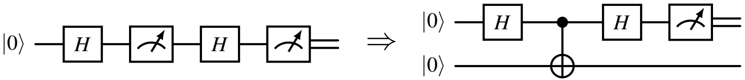
- Uses $\mathrm{poly}(n)$ elementary quantum gates, and thus requires $\mathrm{poly}(n)$ qubits.
- The goal is to find *a small corner* of an $2^{\mathrm{poly}(n)}$-dimension Hilbert space that holds the relevant information, which can only be extracted through performing measurements.

(Pinching) intermediate measurements:

- Measurements via **single-qubit pinching channels**:

$$\Phi(\rho) := \mathrm{Tr}(\rho\,|0\rangle\langle 0|)\,|0\rangle\langle 0| + \mathrm{Tr}(\rho\,|1\rangle\langle 1|)\,|1\rangle\langle 1|$$

  Removes *coherence*, leaving only diagonal terms in the post-measurement states.
  - Implicitly used in the proof of QCMA $\subseteq$ QMA [Aharonov-Naveh'02].
- Intermediate measurements are useless (principle of deferred measurements):



Eliminate intermediate measurements by introducing ancillary qubits!

What is **space-bounded** quantum computation?

Space-bounded quantum computation (BQL) is introduced in [Watrous'98, Watrous'99]:

- Limits computation to $O(\log n)$ qubits, but allows $\mathrm{poly}(n)$ quantum gates.
- A quantum logspace computation operates on a $2^{O(\log n)}$-dimension Hilbert space, making this model appear weak and contained in NC.

However, BQL has shown *notable* power and gained recent increased attention:

- ◇ INVERTING WELL-CONDITIONED MATRICES [Ta-Shma'13, Fefferman-Lin'16] is BQL-complete, fully saturating the *quadratic* space advantage over classical suggested by BQL $\subseteq$ DSPACE$[\log^2(n)]$ [Watrous'99].
- ◇ Intermediate measurements appear to make BQL stronger than $\mathrm{BQ_U L}$:
  - $O(\log n)$ intermediate measurements can be eliminated by introducing ancillary qubits.
  - Allowing both $\mathrm{poly}(n)$ *pinching* intermediate measurements and even *reset operations* provides **no advantage** for promise problems [Fefferman-Remscrim'21, Girish-Raz-Zhan'21].
  - These new techniques *don't* extend to *state-synthesizing* tasks!
- ◇ Quantum singular value transformation, a unifying quantum algorithm framework, has a logspace version [Gilyén-Su-Low-Weibe'18, Metger-Yuen'23, Le Gall-**L.**-Wang'23].
  - Another example ($\textsc{GapQSD}_{\log}$) that exhibits a space advantage over classical!
  - $\textsc{GapQSD}_{\log}$ is BQL-complete [L**L**W23], previously only in NC [Watrous'02].

What is **interactive proofs**?

Classical interactive proof systems

Given a promise problem $(\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$, there is an interactive proof system $P \rightleftharpoons V$ that involves at most $\text{poly}(n)$ messages exchanged between the prover P and the verifier V:

- P is typically all-powerful but untrusted;
- V is computationally bounded, and use *random bits*;

For any $x \in \mathcal{L}_{\text{yes}} \cup \mathcal{L}_{\text{no}}$, this proof system $P \rightleftharpoons V$ guarantees:

- For *yes* instances, $(P \rightleftharpoons V)(x)$ accepts w.p. at least $2/3$;
- For *no* instances, $(P \rightleftharpoons V)(x)$ accepts w.p. at most $1/3$.

* The image is generated using OpenAI's DALL·E model.

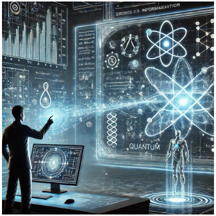
Classical interactive proofs were introduced in [Babai'85, Goldwasser-Micali-Rackoff'85]:

1. Public-coin (AM$[k+2]$) matches the power of private-coin (IP$[k]$) [Goldwasser-Sipser'86].
   - Public coins: Verifier's questions have a particular form ("random questions").
   - Private coins: Random bits used by the verifier, but hidden from the prover.
2. *Constantly* many messages: IP$[O(1)] \subseteq$ AM$[2] \subseteq$ PH [Babai'85, Goldwasser-Sipser'86].
3. *Polynomially* many messages: IP $=$ PSPACE [Lund-Fortnow-Karloff-Nisan'90, Shamir'90].

What is **quantum interactive proofs**?

Quantum interactive proof systems

Given a promise problem $(\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$, there is an interactive proof system $P \rightleftharpoons V$ that involves at most $\text{poly}(n)$ quantum messages exchanged between P and V:



- P is typically all-powerful but untrusted;
- V is bounded and capable of quantum computation;
- P and V may *become entangled* during the interaction.

For any $x \in \mathcal{L}_{\text{yes}} \cup \mathcal{L}_{\text{no}}$, this proof system $P \rightleftharpoons V$ guarantees:

- For *yes* instances, $(P \rightleftharpoons V)(x)$ accepts w.p. at least $2/3$;
- For *no* instances, $(P \rightleftharpoons V)(x)$ accepts w.p. at most $1/3$.

* The image is generated using OpenAI's DALL·E model.

Quantum interactive proofs were introduced in [Watrous'99, Kitaev-Watrous'00]:

1. "Parallelization": PSPACE $\subseteq$ QIP $\subseteq$ QIP$[3]$ [Watrous'99, Kitaev-Watrous'00].
2. QIP$[3]$ $\subseteq$ QMAM $\subseteq$ PSPACE [Marriott-Watrous'04, Jain-Ji-Upadhyay-Watrous'09].
3. Quantum analog of Babai's collapse theorem [Kobayashi-Le Gall-Nishimura'13]:
   For any $O(1)$-message (classical or quantum) "public coin" quantum interactive proofs, the corresponding class is one of PSPACE, qq-QAM, cq-QAM, or cc-QAM.

What is space-bounded (classical) interactive proofs?

Space-bounded classical interactive proofs were introduced in [Dwork-Stockmeyer'92, Condon'91], where the verifier operates in *logspace* but can run in *polynomial time*.

Public coins *weaken* the computational power of such proof systems:

- Classical interactive proofs with a logspace verifier using private (random) coins:
  - With $O(\log n)$ private coins, this model ("IPL") exactly characterizes NP [Condon-Ladner'92].
  - With $\mathrm{poly}(n)$ private coins, this model exactly characterizes PSPACE [Condon'91].
- The model of *public-coin* space-bounded classical interactive proofs is weaker:
  - With $\mathrm{poly}(n)$ public coins, this model is contained in P [Condon'89].
  - With $O(\log n)$ public coins, it contains SAC^1 [Fortnow'89], enabling *bounded* fan-in AND.
  - With $\mathrm{poly}\log(n)$ public coins, it contains NC [Fortnow-Lund'91].
  - With $\mathrm{poly}(n)$ public coins, it contains P [Goldwasser-Kalai-Rothblum'15], connecting to *doubly-efficient interactive proofs*, where the prover is also efficient in some sense.

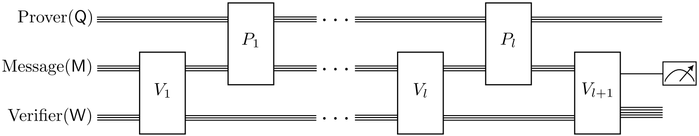
In this work, the verifier has *direct access* to messages during interaction, generalizing the space-bounded quantum Merlin-Arthur proofs (QMAL):

- **Direct access**: A QMAL verifier has *direct access* to an $O(\log n)$-qubit message, processing it directly in the verifier's workspace qubit, similar to QMA.
- QMAL $=$ BQL [Fefferman-Kobayashi-Lin-Morimae-Nishimura'16, Fefferman-Remscrim'21].

1^{st} attempt: Space-bounded UNITARY quantum interactive proofs

Space-bounded *unitary* quantum interactive proofs ($\mathsf{QIP_U L}$)

Consider a $2l$-turn space-bounded unitary quantum interactive proof system $P \rightleftharpoons V$ for $(\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$, where the verifier V operates in quantum logspace and has direct access to messages during interaction with the prover P:



- The verifier V maps $x \in \mathcal{L}_{\text{yes}} \cup \mathcal{L}_{\text{no}}$ to $(V_1, \cdots, V_{l+1})$, where each V_j is unitary.
- Both M and W are of size $O(\log n)$, with M being accessible to both P and V.
- **Strong uniformity**: The description of $(V_1, \cdots, V_{l+1})$ can be computed by a single deterministic logspace Turing machine, intuitively implying $\{V_j\}$'s *repetitiveness*.

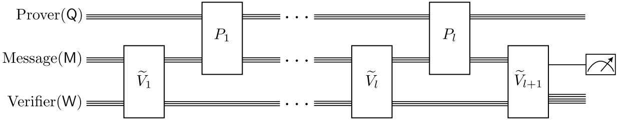
★ $\mathsf{QIP_U L}$ does not contain "IPL", particularly the model from [Condon-Ladner'92]:

- To show IP $\subseteq$ QIP, the verifier needs to *measure* the received messages at the beginning of each action, and treat the outcome as classical messages.
- Soundness against classical messages does not (directly) extend to quantum!

2^{nd} attempt: Space-bounded ISOMETRIC quantum interactive proofs

Space-bounded *isometric* quantum interactive proofs ($\mathrm{QIPL}^{\diamond}$)

Consider a $2l$-turn space-bounded isometric quantum interactive proof system $P \rightleftharpoons V$ for $(\mathcal{L}_{\mathrm{yes}}, \mathcal{L}_{\mathrm{no}})$, where V acts on $O(\log n)$ qubits and has direct access to messages:



- Each $\widetilde{V}_j$ is a unitary quantum circuit with $O(\log n)$ *pinching* intermediate measurements and reset operations.

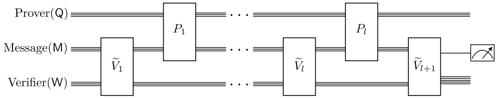
$\mathrm{QIPL}^{\diamond}$ contains the Condon-Ladner model ("IPL"), but it appears too powerful:

- For instance, the prover P can send an n-qubit state using $\lceil n/\log n \rceil$ messages, each consisting of an $O(\log n)$-qubit state, and the verifier V randomly selects only $O(\log n)$ qubits, without revealing the selection to P.
- $\mathrm{QIPL}^{\diamond}$ can verify the local Hamiltonian problem, and thus contains QMA.

Space-bounded ISOMETRIC quantum interactive proofs (Cont.)

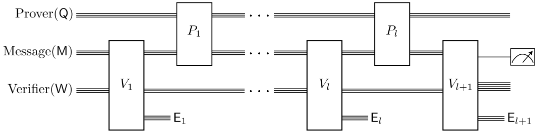
Space-bounded *isometric* quantum interactive proofs ($\mathsf{QIPL}^\diamond$)

Consider a $2l$-turn space-bounded isometric quantum interactive proof system $P \rightleftharpoons V$ for $(\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$, where V acts on $O(\log n)$ qubits and has direct access to messages:



- Each $\widetilde{V}_j$ is a unitary quantum circuit with $O(\log n)$ *pinching* intermediate measurements and reset operations.

Where is the isometry? Each $\widetilde{V}_j$ has a unitary dilation V_j, where V_j is an *isometric* quantum circuit that allows $O(\log n)$ ancillary gates:



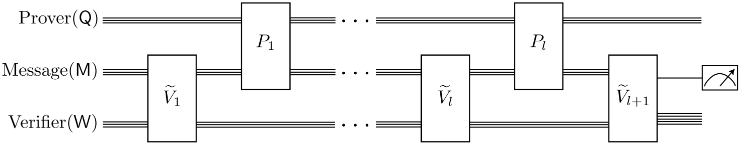
- Each ancillary gate introduces an ancillary qubit $|0\rangle$ in the environment register E_j.
- Each environment register E_j is *only accessible* in the round of V_j belongs.

The qubits in E_j cannot be altered after V_j, but entanglement with W can change!

3^{rd} attempt: Space-bounded quantum interactive proofs

Space-bounded quantum interactive proofs (QIPL & QIPL^{HC})

Consider a $2l$-turn space-bounded quantum interactive proof system $P \rightleftharpoons V$ for $(\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$, where V acts on $O(\log n)$ qubits and has direct access to messages:

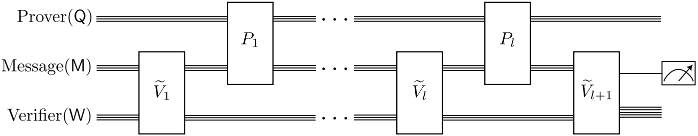


- Each $\widetilde{V}_j$ is an *almost-unitary* quantum circuit, meaning that a unitary quantum circuit with $O(\log n)$ *pinching* intermediate measurements.
  - The $O(\log n)$ bound on pinching intermediate measurements corresponds to the maximum number of measurement outcomes that can be *stored* in logspace.
- $\underline{\text{QIPL}^{\text{HC}}}$: For *yes* instances, the distribution of intermediate measurement outcomes $u = (u_1, \cdots, u_l)$, condition on acceptance, must be *highly concentrated*.
  - ★ This requirement leads to the NP containment for any QIPL^{HC} proof system.
  - Specifically, let $\omega(V)|^u$ be the contribution of u to $\omega(V)$, where $\omega(V)$ is the maximum acceptance probability of $P \rightleftharpoons V$. There must exists a u^* such that $\omega(V)|^{u^*} \geq c(n)$.
- Both QIPL^{HC} and QIPL also contain the Condon-Ladner model ("IPL")!

3rd attempt: Space-bounded quantum interactive proofs (Cont.)

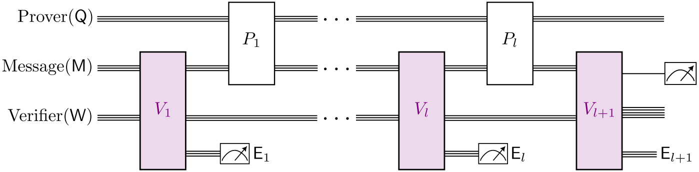
Space-bounded quantum interactive proofs (QIPL & $\mathrm{QIPL}^{\mathrm{HC}}$)

Consider a $2l$-turn space-bounded quantum interactive proof system $P \rightleftharpoons V$ for $(\mathcal{L}_{\mathrm{yes}}, \mathcal{L}_{\mathrm{no}})$, where V acts on $O(\log n)$ qubits and has direct access to messages:



- Each $\widetilde{V}_j$ is an *almost-unitary* quantum circuit, meaning that a unitary quantum circuit with $O(\log n)$ *pinching* intermediate measurements.

Applying the *principle of deferred measurements* to the almost-unitary quantum circuit $\widetilde{V}_j$ transforms it into **a special class** of isometric quantum circuits V_j, followed by *measuring* the register E_j with outcome u_j:



Main results on $\mathsf{QIP_UL}$ and QIPL

Theorem 1. $\mathsf{NP} = \mathsf{QIPL}^{\mathsf{HC}} \subseteq \mathsf{QIPL}$.

- $\mathsf{QIPL}^{\mathsf{HC}}$ is the *weakest* model that includes space-bounded classical interactive proof systems, particularly the Condon-Ladner model ("IPL").
- **New technique**: *Directly* upper-bounding quantum interactive proof systems with *non-unitary* verifier, whereas existing techniques only handle *unitary* verifier.
  - To ensure that soundness against classical messages also holds against quantum messages, the verifier needs to perform $\mathrm{poly}(n)$ pinching measurement in total.

Theorem 2. $\mathsf{SAC}^1 \cup \mathsf{BQL} \subseteq \mathsf{QIP_UL} \subseteq \cup_{c(n)-s(n)\geq 1/\mathrm{poly}(n)} \mathsf{QIPL}_{O(1)}[c,s] \subseteq \mathsf{P}$.

- Intermediate measurements enhance the model: $\mathsf{QIP_UL} \subsetneq \mathsf{QIPL}$ unless $\mathsf{P} = \mathsf{NP}$.
- $\mathsf{QIP_UL}$ proof systems, regarded as the most natural space-bounded analog to QIP, do not achieve the aforementioned soundness guarantee.

Main results on $\mathsf{QIP_UL}$ and QIPL (Cont.)

Theorem 3. For any $c(n) - s(n) \geq \Omega(1)$, $\mathsf{QIPL}_{O(1)}[c,s] \subseteq \mathsf{NC}$.

- For constant-turn space-bounded quantum proofs, all three models are equivalent!

Theorem 4 (Properties for QIPL and $\mathsf{QIP_UL}$). Let $c(n)$, $s(n)$, and $m(n)$ be functions such that $0 \leq s(n) < c(n) \leq 1$, $c(n) - s(n) \geq 1/\mathrm{poly}(n)$, and $1 \leq m(n) \leq \mathrm{poly}(n)$. Then, we have:

1. ***Closure under perfect completeness***. $\mathsf{QIPL}_m[c,s] \subseteq \mathsf{QIPL}_{m+2}\left[1, 1-\frac{1}{2}(c-s)^2\right]$ and $\mathsf{QIP_UL}_m[c,s] \subseteq \mathsf{QIP_UL}_{m+2}\left[1, 1-\frac{1}{2}(c-s)^2\right]$.
2. ***Error reduction***. For any polynomial $k(n)$, there is a polynomial $m'(n)$ such that: $$\mathsf{QIPL}_m[c,s] \subseteq \mathsf{QIPL}_{m'}\left[1, 2^{-k}\right] \text{ and } \mathsf{QIP_UL}_m[c,s] \subseteq \mathsf{QIP_UL}_{m'}\left[1, 2^{-k}\right].$$
3. ***Parallelization***. $\mathsf{QIP_UL}_{4m+1}[1,s] \subseteq \mathsf{QIP_UL}_{2m+1}[1,(1+\sqrt{s})/2]$.

◇ To establish Theorem 4 ❷, we use *sequential repetition* due to the space constraint, with the key being to force the prover to "clean" the workspace.

Main results: Proof intuitions for *upper* bounds (*unitary* verifier)

Theorem 2. $\mathsf{SAC}^1 \cup \mathsf{BQL} \subseteq \mathsf{QIP_UL} \overset{ⓐ}{\subseteq} \cup_{c(n)-s(n)\geq 1/\mathrm{poly}(n)} \mathsf{QIPL}_{O(1)}[c,s] \overset{ⓑ}{\subseteq} \mathsf{P}$.

ⓐ **Parallelization** (Theorem 4 ❸) for $\mathsf{QIP_UL}$ proof systems:

- ◇ The original approach in [Kitaev-Watrous'00] fails, since it requires sending all snapshot states in a single message, which *exceeds* logarithmic size.
- ◇ The turn-halving approach in [Kempe-Kobayashi-Matsumoto-Vidick'07] works, a "dequantized" version of the above approach, which leverages the *reversibility* and *dimension preservation* of the verifier's actions.

ⓑ Adapting the SDP formulation for QIP [Vidick-Watrous'16] to $\mathsf{QIP_UL}$ proof systems:

- ◇ For any *constant*-round $\mathsf{QIP_UL}$ proof system, the corresponding SDP admits *polynomial-size* solutions, ensuring P containment via standard SDP solvers.
- 🔔 Parallelization (Theorem 4 ❸) makes $\mathsf{QIP_UL}$ easy!

Theorem 3. For any $c(n) - s(n) \geq \Omega(1)$, $\mathsf{QIPL}_{O(1)}[c,s] \subseteq \mathsf{NC}$.

- ◇ An exponentially down-scaling version of $\mathsf{QIP} = \mathsf{PSPACE}$ [Jain-Ji-Upadhyay-Watrous'09].

Main results: Proof intuitions for *upper* bounds (*non-unitary* verifier)

Theorem 1. $\mathsf{NP} = \mathsf{QIPL}^{\mathsf{HC}} \subseteq \mathsf{QIPL}$.

In $P \rightleftharpoons V$, let $\omega(V)|^u$ denote the contribution of the branch $u = (u_1, \cdots, u_l)$ to the maximum acceptance probability $\omega(V) = \sum_u \omega(V)|^u$, where u_k denotes the intermediate measurement outcome in the verifier's k-th turn ($1 \leq k \leq l$).

- Pinching measurements eliminate coherence between subspaces corresponding to different branches, allowing $\omega(V)|^u$ to be approximately optimized *in isolation*.
- Therefore, for any QIPL proof system $P \rightleftharpoons V$ *with a **fixed** branch* u, one can write a SDP formulation, which computes an approximation $\widehat{\omega}(V)|^u$ of $\omega(V)|^u$ satisfying
$$\omega(V)|^u \leq \widehat{\omega}(V)|^u \leq \omega(V).$$
- **"Efficient verifiability"**: Noting that a solution to this SDP formulation can be written as a *Cartesian* product of a polynomial number of $O(\log n)$-qubit states (i.e., *snapshot states* in $P \rightleftharpoons V$), we can verify the SDP feasibility of this solution in NP.

★ "Efficient verifiability" does not imply QIPL $\subseteq$ AM: The set lower bound protocol [Goldwasser-Sipser'86] and similar techniques are not directly applicable to QIPL.

Main results: Proof intuitions for *lower* bounds

Theorem 2. $\mathsf{SAC}^1 \cup \mathsf{BQL} \subseteq \mathsf{QIP_U L} \subseteq \cup_{c(n)-s(n)\geq 1/\mathrm{poly}(n)} \mathsf{QIPL}_{O(1)}[c,s] \subseteq \mathsf{P}$.

- **Key idea**: Simulating $O(\log n)$ *public* coins in space-bounded classical interactive proof systems by performing $O(\log n)$ pinching measurements.
- The lower bound ($\mathsf{SAC}^1 \subseteq \mathsf{QIP_U L}$) is inspired by space-bounded classical interactive proof systems *with* $O(\log n)$ *public coins* for evaluating (uniform) SAC^1 circuits [Fortnow'89].
  - It is known that $\mathsf{NL} \subseteq \mathsf{SAC}^1 = \mathsf{LOGCFL} \subseteq \mathsf{AC}^1 \subseteq \mathsf{NC}^2$ [Venkateswaran'91].

Theorem 1. $\mathsf{NP} = \mathsf{QIPL}^{\mathsf{HC}} \subseteq \mathsf{QIPL}$.

- **Key idea**: Simulating $O(\log n)$ *private* coins in space-bounded classical interactive proof systems by
  1. Measuring each $O(\log n)$-qubit message received from the prover in the proof system;
  2. Performing $O(\log n)$ pinching measurement to generate $O(\log n)$ random coins.
- The lower bound ($\mathsf{NP} \subseteq \mathsf{QIPL}^{\mathsf{HC}}$) is inspired by space-bounded classical interactive proof systems *with* $O(\log n)$ *private coins* for NP (i.e., 3-SAT) in [Condon-Ladner'95].

Statistical zero-knowledge: General cases and in $\mathsf{QIP_UL}$

Definition 5 (Statistical zero-knowledge, informal). An interactive proof system 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 an *efficient* simulator.

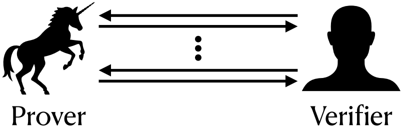


Figure: Verifier's view ($\mathcal{P}_0$)

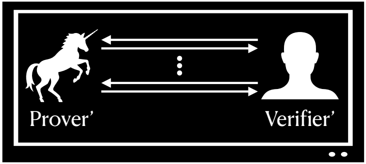


Figure: Simulated "Verifier's view" ($\mathcal{P}_1$)

- A common misusage (*unrelated to science*!): zero-knowledge vs. zero-entropy.
- Intuitively, the classical views $\mathcal{P}_0$ and $\mathcal{P}_1$ can be treated as distributions p_0 and p_1, respectively. The notion of *statistical indistinguishablity* is then characterized by the ℓ_1 norm distance $\mathrm{TV}(p_0, p_1) := \frac{1}{2}\|p_0 - p_1\|_1$.

Zero-knowledge property in $\mathsf{QIP_UL}$. A $\mathsf{QIP_UL}$ proof system has *the zero-knowledge property* if there is a *space-bounded* simulator that well approximates the snapshot states ("the verifier's view") in (M, W) after each turn, with respect to the trace distance.

Main results on space-bounded *unitary* quantum statistical zero-knowledge

$\mathsf{QSZK_UL_{HV}}$ and $\mathsf{QSZK_UL}$ are space-bounded variants of quantum statistical zero-knowledge against an honest and arbitrary verifier, $\mathsf{QSZK_{HV}}$ and QSZK, respectively, introduced in [Watrous'02] and [Watrous'09].

Theorem 6. $\mathsf{QSZK_UL} = \mathsf{QSZK_UL_{HV}} = \mathsf{BQL}$.

The $\textsc{IndivProdQSD}[k,\alpha,\delta]$ **problem** ($\textsc{Individual Product State Distinguishability}$) involves two k-tuples of $O(\log n)$-qubit states, $\sigma_1, \cdots, \sigma_k$ and $\sigma'_1, \cdots, \sigma'_k$, whose purifications can be prepared by unitary quantum logspace circuits, satisfying $\alpha(n) - k(n) \cdot \delta(n) \geq 1/\mathrm{poly}(n)$ and $1 \leq k(n) \leq \mathrm{poly}(n)$, with the following conditions:

- ◇ For *yes* instances, the k-tuples are *globally far*, i.e., $\mathrm{T}(\sigma_1 \otimes \cdots \otimes \sigma_k, \sigma'_1 \otimes \cdots \otimes \sigma'_k) \geq \alpha$.
- ◇ For *no* instances, the k-tuples are *pairwise close*, i.e., $\forall j \in [k]$, $\mathrm{T}(\sigma_j, \sigma'_j) \leq \delta$.

$\mathsf{QSZK_UL_{HV}} \subseteq \mathsf{BQL}$ follows since $\textsc{IndivProdQSD}$ is $\mathsf{QSZK_UL_{HV}}$-complete:

- ▶ Since $\textsc{IndivProdQSD}$ implies an "existential" version of $\textsc{GapQSD}_{\log}$, which is BQL-complete [Le Gall-**L.**-Wang'23], it follows that $\textsc{IndivProdQSD} \in \mathsf{QMAL} \subseteq \mathsf{BQL}$.
- ▶ The complement of $\textsc{IndivProdQSD}$ is $\mathsf{QSZK_UL_{HV}}$-hard, similar to [Watrous'02].

Conclusions and open problems

Take-home messages on our work

1. Intermediate measurements play a *distinct* role in space-bounded quantum interactive proofs compared to space-bounded quantum computation: $\mathsf{QIP_UL} \subsetneq \mathsf{QIPL}$ unless $\mathsf{P} = \mathsf{NP}$ (this work), while $\mathsf{BQ_UL} = \mathsf{BQL}$ [FR21, GRZ21].
2. We define three models of space-bounded quantum interactive proofs:

	$\mathsf{QIP_UL}$	QIPL	$\mathsf{QIPL}^{\diamond}$
Verifier's actions	unitary	almost-unitary	isometry
Lower bounds	$\mathsf{SAC}^1 \cup \mathsf{BQL}$ "IPL" with $O(\log n)$ *public* coins	$\mathsf{NP}(= \mathsf{QIPL}^{\mathsf{HC}})$ "IPL" with $O(\log n)$ *private* coins	QMA
Upper bounds	P	PSPACE	PSPACE

3. Introducing the *zero-knowledge* property for $\mathsf{QIP_UL}$ proof systems, i.e., $\mathsf{QSZK_UL}$, eliminates the usual advantage gained from interaction ($\mathsf{QSZK_UL} = \mathsf{BQL}$).

Open problems

1. Is it possible to obtain a tighter characterization of $\mathsf{QIP_UL}$? Thus may require to simulate $\omega(\log n)$ public coins using only $O(\log n)$ pinching measurements.
2. What is the computational power of the classes QIPL and $\mathsf{QIPL}^{\diamond}$?

Thanks!