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.

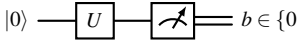
CCC 2025, Toronto

1. Space-bounded quantum computation meets interactive proofs
2. Definitions of space-bounded quantum interactive proof systems
3. Main results
4. Open problems

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

Basic ingredients in (time-bounded) quantum computation:

- **Qubit**. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
- **Quantum state**. An n-qubit (pure) state is a vector $|\Psi\rangle \in \mathbb{C}^{2^n}$ satisfying $\langle\Psi|\Psi\rangle = 1$.
  In general, an n-qubit (mixed) quantum state ρ is a positive semi-definite matrix of dimension $2^n \times 2^n$ such that $\mathrm{Tr}(\rho) = 1$.
- **Quantum gate**. Elementary quantum gates G_i (from some universal gateset) are unitary matrices act on one or two qubits, e.g., $G_i \in \{\mathsf{CNOT}, \mathsf{Had}, \mathsf{T}\}$:
$$|0\rangle^{\otimes n} \xrightarrow{G_1} G_1|0\rangle^{\otimes n} \xrightarrow{G_2} G_2 G_1 |0\rangle^{\otimes n} \to \cdots$$
- **Measurement**. Projective measurement in computational basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$:



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 *exponential*-dimension Hilbert space that holds the relevant information, which can only be extracted through performing measurements.

Intermediate measurements in (space-bounded) quantum computation

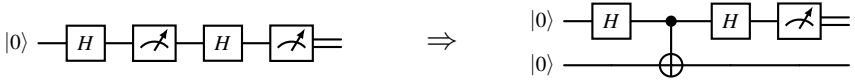
Intermediate measurements implemented by *single-qubit pinching channels*:

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

Removes *coherence*, leaving only diagonal terms in the post-measurement states.

Principle of deferred measurements

Intermediate measurements are *useless* in time-bounded quantum computation:



Eliminate intermediate measurements by introducing ancillary qubits!

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 *polynomial*-dimension Hilbert space, making this model appear weak and contained in NC.

Principle of deferred measurements *doesn't* apply to quantum logspace in general!

How powerful is **space-bounded** quantum computation?

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 $\mathsf{BQ_UL}$:
  - Using the principle of deferred measurements, $O(\log n)$ intermediate measurements can be eliminated by introducing ancillary qubits.
  - Allowing both $\mathrm{poly}(n)$ pinching intermediate measurements and even *reset operations* provide **no advantage** for promise problems [Fefferman-Remscrim'21, Girish-Raz-Zhan'21]: BQL $=$ $\mathsf{BQ_UL}$.
  - 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 ($\mathsf{GAPQSD_{log}}$) showing a space advantage over classical!
  - $\mathsf{GAPQSD_{log}}$ is BQL-complete [LLW23], previously only in NC [Watrous'02].
  - ★ **Corollary** (this work): Space-bounded *unitary* quantum statistical zero-knowledge ($\mathsf{QSZK_UL}$) is in BQL.

What is (classical) **interactive proofs**?

Classical interactive proof systems

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

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:

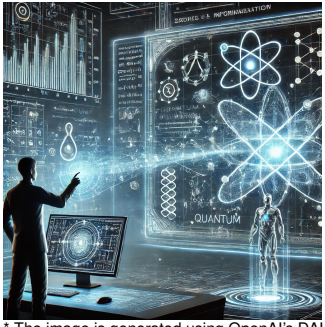
- For *yes* instances, $(P \rightleftharpoons V)(x)$ accepts w.p. at least $2/3$;
- For *no* instances, $(P \rightleftharpoons V)(x)$ accepts w.p. at most $1/3$.

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

1. Asking random questions (i.e., *public coins*) is as powerful as asking clever questions (i.e., *private coins*): $\mathsf{IP}[k] \subseteq \mathsf{AM}[k+2]$ [Goldwasser-Sipser'86].
2. *Constantly* many messages: $\mathsf{IP}[\mathrm{O}(1)] \subseteq \mathsf{AM} \subseteq \mathsf{PH}$ [Babai'85, Goldwasser-Sipser'86].
3. *Polynomially* many messages: $\mathsf{IP} = \mathsf{PSPACE}$ [Lund-Fortnow-Karloff-Nisan'90, Shamir'90].

What is **quantum interactive proofs**?

Quantum interactive proof systems



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

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 $1/3$.

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$[3] \subseteq$ PSPACE [Marriott-Watrous'04, Jain-Ji-Upadhyay-Watrous'09].

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 $\mathrm{poly}(n)$ public coins, it contains P [Goldwasser-Kalai-Rothblum'15].

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.
- $\mathrm{QMAL} = \mathrm{BQL}$ [Fefferman-Kobayashi-Lin-Morimae-Nishimura'16, Fefferman-Remscrim'21].

1 Space-bounded quantum computation meets interactive proofs

2 Definitions of space-bounded quantum interactive proof systems

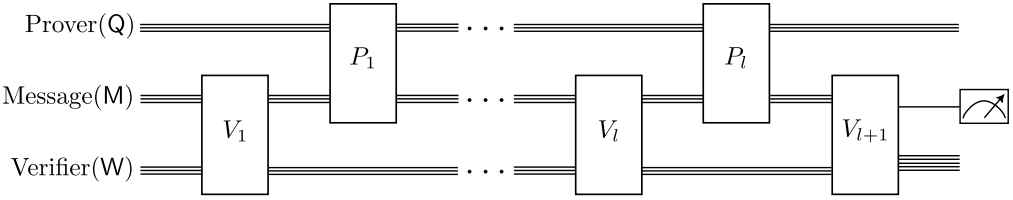
3 Main results

4 Open problems

1st attempt: Space-bounded UNITARY quantum interactive proofs

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

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*.

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

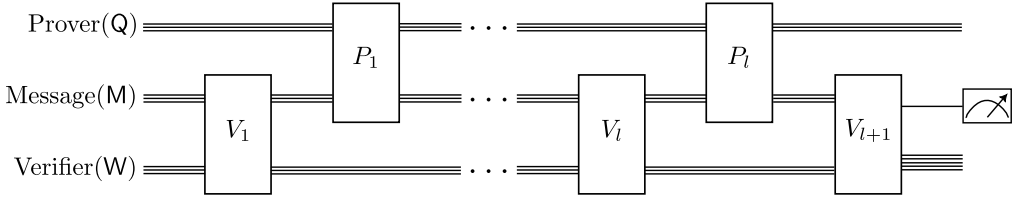
- To show IP $\subseteq$ QIP, the verifier needs to *measure* the received messages at the beginning of each action, and treat the outcome as classical messages.

🔔 Soundness against classical messages does not (directly) extend to quantum!

2nd attempt: Space-bounded ISOMETRIC quantum interactive proofs

Space-bounded *isometric* quantum interactive proofs (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 V_j is a unitary quantum circuit with $O(\log n)$ *pinching* intermediate measurements and reset operations.

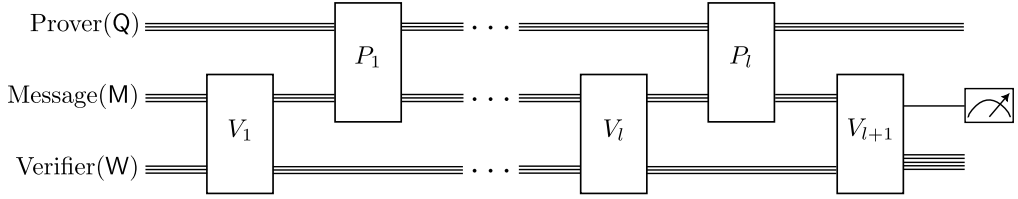
QIPL$^\diamond$ contains the Condon-Ladner model ("IPL"), but it appears too powerful:

- 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 choice to P.
- QIPL$^\diamond$ can verify the local Hamiltonian problem, and thus contains QMA.

3rd attempt: Space-bounded quantum interactive proofs

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

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 V_j is an *almost-unitary* quantum circuit, meaning that a unitary quantum circuit with $O(\log n)$ *pinching* intermediate measurements.
- QIPL$^{\mathsf{HC}}$: For *yes* instances, the distribution of intermediate measurement outcomes $u = (u_1, \cdots, u_l)$, condition on acceptance, must be *highly concentrated*.
  - Intuitively, this condition may be interpreted as the prover's messages being **almost classical** for *yes* instances.
- Both QIPL and QIPL$^{\mathsf{HC}}$ also contain the Condon-Ladner model ("IPL")!

1 Space-bounded quantum computation meets interactive proofs

2 Definitions of space-bounded quantum interactive proof systems

3 Main results

4 Open problems

Main results on $\mathsf{QIP}_{\mathsf{U}}\mathsf{L}$ 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.

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

- Intermediate measurements enhance the model: $\mathsf{QIP}_{\mathsf{U}}\mathsf{L} \subsetneq \mathsf{QIPL}$ unless $\mathsf{P} = \mathsf{NP}$.

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

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

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

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

a **Parallelization** for $\mathsf{QIP}_{\mathsf{U}}\mathsf{L}$ 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.

b Adapting the SDP formulation for QIP [Vidick-Watrous'16] to $\mathsf{QIP}_{\mathsf{U}}\mathsf{L}$ proof systems:
- For any *constant*-round $\mathsf{QIP}_{\mathsf{U}}\mathsf{L}$ proof system, the corresponding SDP admits *polynomial-size* solutions, ensuring P containment via standard SDP solvers.

Parallelization makes $\mathsf{QIP}_{\mathsf{U}}\mathsf{L}$ easy!

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

- 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
$$\omega(V)|^u \leq \widehat{\omega}(V)|^u \leq \omega(V).$$
- NP **containment**: 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.

Main results: Proof intuitions for *lower* bounds

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

- **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 ($\mathsf{SAC}^1 \subseteq \mathsf{QIP}_{\mathsf{U}}\mathsf{L}$) is inspired by space-bounded classical interactive proof systems *with* $O(\log n)$ *public coins* for evaluating (uniform) SAC^1 circuits [Fortnow'89].

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].

1. Space-bounded quantum computation meets interactive proofs
2. Definitions of space-bounded quantum interactive proof systems
3. Main results
4. Open problems

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:

$$\mathsf{QIP_UL} \subsetneq \mathsf{QIPL} \text{ unless } \mathsf{P} = \mathsf{NP} \text{ (this work), while } \mathsf{BQ_UL} = \mathsf{BQL} \text{ [FR21, GRZ21].}$$

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. Can $\mathsf{QIP_UL}$ be more tightly characterized with a stronger lower bound?
2. What is the computational power of the classes QIPL and $\mathsf{QIPL}^\diamond$?

Thanks!