Space-bounded quantum interactive proof systems

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

[1] Nagoya University

[2] University of Edinburgh

Available on arXiv:2410.23958.

QIP 2025, Raleigh

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

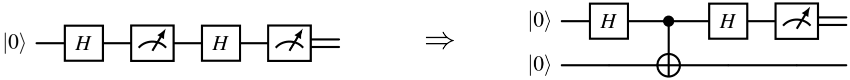
(Pinching) intermediate measurements:

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

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

  Only *coherence* is removed.

- 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 *polynomial*-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 $\mathrm{BQ_UL}$:
  - $O(\log n)$ intermediate measurements can be eliminated by introducing ancillary qubits.
  - Allowing both $\mathrm{poly}(n)$ pinching intermediate measurements and **reset operations** provide *no advantage* for promise problems [Girish-Raz-Zhan'21, Fefferman-Remscrim'21].
- 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].

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

Classical interactive proof systems

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

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

For any $x \in \mathcal{L}_{\mathrm{yes}} \cup \mathcal{L}_{\mathrm{no}}$, 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 $1/3$.

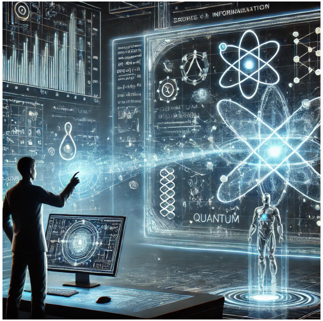
* The image is generated using OpenAI's DALL·E model.

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

1. 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: $\mathsf{IP}[O(1)] \subseteq \mathsf{IP}[2] \subseteq \mathsf{PH}$ [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



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

- The prover P is typically all-powerful but untrusted;
- The verifier V is bounded and capable of quantum computation;
- P and V may share *entanglement* during the interaction.

For any $x \in \mathcal{L}_{\mathrm{yes}} \cup \mathcal{L}_{\mathrm{no}}$, 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$[3]$ $\subseteq$ 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 $O(\log n)$ private (random) coins ("IPL") exactly characterizes NP [Condon-Ladner'92].
- 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].

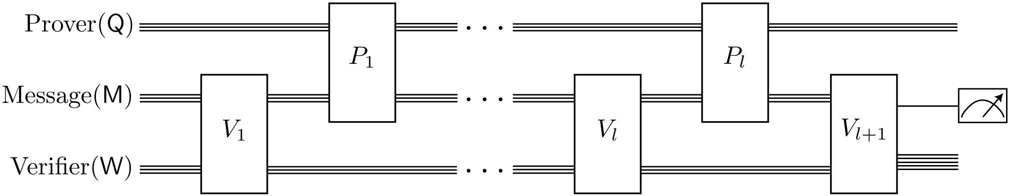
In this work, the verifier has *direct access* to messages during interaction, generalizing the space-bounded quantum Merlin-Arthur proofs (QMAL):

- **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.
- 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 ($\mathsf{QIP_UL}$)

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



- The verifier V maps $x \in \mathcal{L}_{\rm yes} \cup \mathcal{L}_{\rm no}$ 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]:

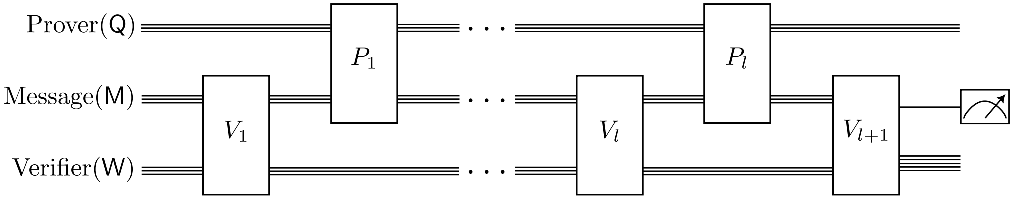
- To show IP $\subseteq$ QIP, the verifier needs to *measure* the received messages at the beginning of each action, and treat the outcome as classical messages.

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

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

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 V_j is a unitary quantum circuit with $O(\log n)$ *pinching* intermediate measurements and reset operations.

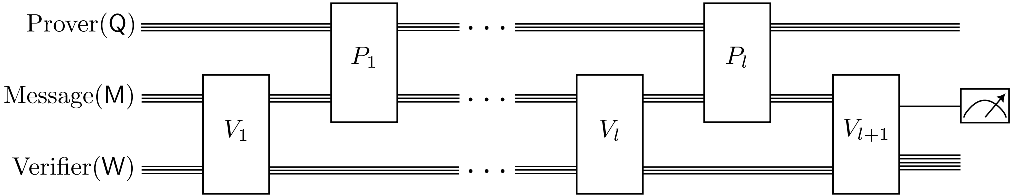
$\mathsf{QIPL}^\diamond$ contains the Condon-Ladner model ("IPL"), but it appears too powerful:

- For instance, the prover P can send an n-qubit state using $\lceil n/\log n \rceil$ messages of $(\log n)$-qubit states, while the verifier V takes only $O(\log n)$ qubits without P detecting the choices.
- $\mathsf{QIPL}^\diamond$ can verify the local Hamiltonian problem, and thus contains QMA.

3rd attempt: Space-bounded quantum interactive proofs

Space-bounded quantum interactive proofs (QIPL)

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 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.
- QIPL also contains the Condon-Ladner model ("IPL")!

Main results on $\mathsf{QIP_U L}$ and QIPL

Theorem 1. $\mathsf{NP} \subseteq \mathsf{QIPL} \subseteq \mathsf{SBP}$.

- The complexity class SBP generalizes BPP by considering a constant multiplicative error and is positioned between MA and AM [Böhler-Glaßer-Meister'03].
- Under reasonable derandomization assumptions, AM collapses to NP [Klivans-van Melkebeek'99, Miltersen-Vinodchandran'99], which implies $\mathsf{QIPL} = \mathsf{NP}$.

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

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

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!

Main results on $\mathsf{QIP_UL}$ and QIPL: Proof intuitions

Theorem 1. NP $\subseteq$ QIPL $\subseteq$ SBP.

- The lower bound is inspired by space-bounded (private-coin) classical interactive proof systems for NP, particularly 3-SAT, in [Condon-Ladner'95].

★ (Hard!) The upper bound follows from:

1. Approximating the size of an exponential-size set S with efficiently verifiable membership (using the *same* witness) within a *constant multiplicative error* is in NSBP [Böhler-Glaßer-Meister'03] , and hence in SBP [Watson'12]].
2. **Efficient verifiability** is ensured by a *family* of SDP formulations of QIPL proof systems:
   - Each *intermediate measurement outcome* corresponds to a distinct SDP formulation;
   - The *size* of this set S corresponds to the *acceptance probability* of the proof system.
3. A **constant** multiplicative error is guaranteed by **sequential** error reduction for QIPL.
   - The challenge is to *enforce the prover* to "clean" the workspace.

Main results on $\mathsf{QIP_U L}$ and QIPL: Proof intuitions (Cont.)

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

- The lower bound is inspired by space-bounded classical interactive proof systems with $O(\log n)$ public coins for evaluating SAC^1 circuits [Fortnow'89].

- The upper bound follows from:

1. **Parallelization** for $\mathsf{QIP_U L}$ 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* of the verifier's actions.
2. Adapting the SDP formulation for QIP [Vidick-Watrous'16] to $\mathsf{QIP_U L}$ proof systems:
   - All SDP constraints are matrices of *polynomial size*, ensuring P containment via standard SDP solvers.

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

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

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: $\mathsf{QIP_U L} \subsetneq \mathsf{QIPL}$ unless $\mathsf{P} = \mathsf{NP}$ (this work), while $\mathsf{BQ_U L} = \mathsf{BQL}$ [FR21, GRZ21].
2. We define three models of space-bounded quantum interactive proofs:

	$\mathsf{QIP_U L}$	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	NP "IPL" with $O(\log n)$ *private* coins	QMA
Upper bounds	P	SBP	PSPACE

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

Open problems

1. Can $\mathsf{QIP_U L}$ be more tightly characterized with a stronger lower bound?
2. Can the lower bound of QIPL be improved to MA or StoqMA?
3. What is the computational power of space-bounded quantum interactive proofs with a *general* quantum logspace verifier?

Thanks!