

Space-bounded quantum interactive proof systems

François Le Gall ¹ **Yupan Liu** ¹ Harumichi Nishimura ¹ Qisheng Wang ^{2,1}

¹Nagoya University

²University of Edinburgh

Available on arXiv:2410.23958.

CS Theory Seminar, Penn State University, January 2025

- 1 Space-bounded quantum computation meets interactive proofs
- 2 Definitions of space-bounded quantum interactive proof systems
- 3 Main results on QIP_{UL} , QIPL , and QSZK_{UL}
- 4 Open problems

What is time-bounded quantum computation?

Ingredients in quantum computation:

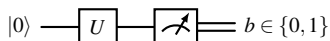
► **Qubit.** $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

► **Quantum state.** An n -qubit state is a vector $|\Psi\rangle \in \mathbb{C}^{2^n}$ satisfying $\langle\Psi|\Psi\rangle = 1$.

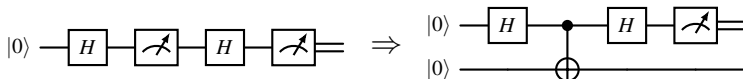
► **Quantum gate.** Elementary quantum gates G_i (from some universal gateset) are unitary matrices act on one or two qubits, e.g., $G_i \in \{\text{CNOT}, \text{Had}, \text{T}\}$:

$$|0\rangle^{\otimes n} \xrightarrow{G_1} G_1|0\rangle^{\otimes n} \xrightarrow{G_2} G_2G_1|0\rangle^{\otimes n} \rightarrow \dots$$

► **Measurement.** Projective measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ in computational basis:



► **Intermediate measurements** are useless (principle of deferred measurements):



📌 **Eliminate intermediate measurements by introducing ancillary qubits!**

Time-bounded quantum computation (BQP):

► Uses $\text{poly}(n)$ elementary quantum gates, and thus requires $\text{poly}(n)$ qubits.

► The goal is to find a *small corner* of a $2^{\text{poly}(n)}$ -dimension Hilbert space that holds the relevant information, which can only be extracted through measurements.

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 $\text{poly}(n)$ 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.

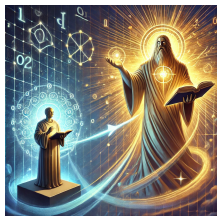
However, BQL has shown *notable* power and gained recent increased attention:

- ◇ INVERTING WELL-CONDITIONED MATRICES [Ta-Shma'13, Fefferman-Lin'16] is BQL-complete, fully saturating the *quadratic* space advantage over classical suggested by $\text{BQL} \subseteq \text{DSPACE}[\log^2(n)]$ [Watrous'99].
- ◇ Intermediate measurements appear to make BQL stronger than BQ_{UL} :
 - ▶ $O(\log n)$ intermediate measurements can be eliminated by introducing ancillary qubits.
 - ▶ Allowing $\text{poly}(n)$ *oblivious* intermediate measurements provide *no advantage* for promise problems [Girish-Raz-Zhan'21, Girish-Raz'22].
 - ▶ Even when both $\text{poly}(n)$ oblivious intermediate measurements and **reset operations** are allowed, there is *no advantage* for promise problems [Fefferman-Remscrem'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 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.

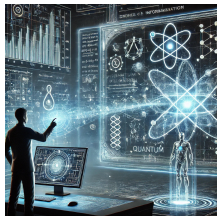
Classical interactive proofs were introduced in [Babai'85, Goldwasser-Micali-Rackoff'85]:

- 1 Public-coin ($\text{AM}[k+2]$) matches the power of private-coin ($\text{IP}[k]$) [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: $\text{IP}[O(1)] \subseteq \text{IP}[2] \subseteq \text{PH}$ [Babai'85, Goldwasser-Sipser'86].
- 3 *Polynomially* many messages: $\text{IP} = \text{PSPACE}$ [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 **share entanglement 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”: $\text{PSPACE} \subseteq \text{QIP} \subseteq \text{QIP}[3]$ [Watrous'99, Kitaev-Watrous'00].
- 2 $\text{QIP}[3] \subseteq \text{QMAM} \subseteq \text{PSPACE}$ [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 $O(\log n)$ private (random) coins (“IPL”) exactly characterizes NP [Condon-Ladner'92].
- ▶ The model of *public-coin* space-bounded classical interactive proofs is weaker:
 - ◊ With $\text{poly}(n)$ 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 $\text{poly}(\log n)$ public coins, it contains NC [Fortnow-Lund'91].
 - ◊ With $\text{poly}(n)$ 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):

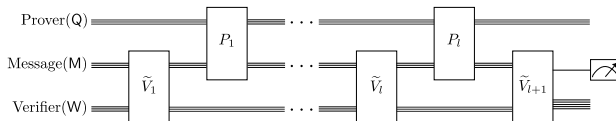
- ▶ **Direct access:** A QMAL verifier has *direct access* to an $O(\log n)$ -qubit message, processing it directly in the verifier's workspace qubit, similar to QMA.
- ▶ QMAL = BQL [Fefferman-Kobayashi-Lin-Morimae-Nishimura'16, Fefferman-Remscrem'21].

- 1 Space-bounded quantum computation meets interactive proofs
- 2 Definitions of space-bounded quantum interactive proof systems
- 3 Main results on QIP_{UL} , QIPL , and QSZK_{UL}
- 4 Open problems

2nd attempt: Space-bounded ISOMETRIC quantum interactive proofs

Space-bounded *isometric* quantum interactive proofs (QIPL[◇])

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

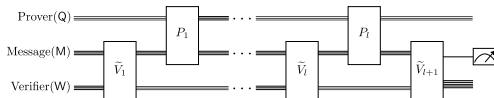
📌 QIPL[◇] contains the Condon-Ladner model (“IPL”), but it appears too powerful:

- ▶ For instance, P can send an n -qubit state using $\lceil n/\log n \rceil$ messages of $(\log n)$ -qubit states, while V takes only $O(\log n)$ qubits without P detecting the choices.
- ▶ QIPL[◇] can verify the local Hamiltonian problem, and thus contains QMA.

Space-bounded ISOMETRIC quantum interactive proofs (Cont.)

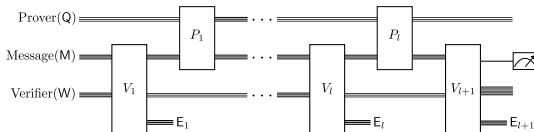
Space-bounded *isometric* quantum interactive proofs (QIPL $^\diamond$)

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

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



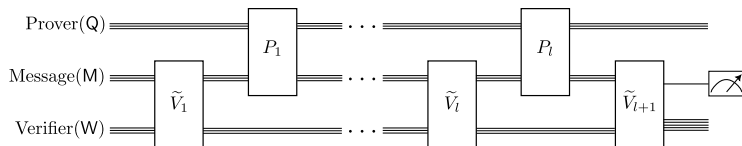
- ▶ Each ancillary gate introduces an ancillary qubit $|0\rangle$ in the environment register E_j .
- ▶ Each environment register E_j is *only accessible* in the round of V_j belongs.

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

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 $(\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$, where V acts on $O(\log n)$ qubits and has direct access to messages:

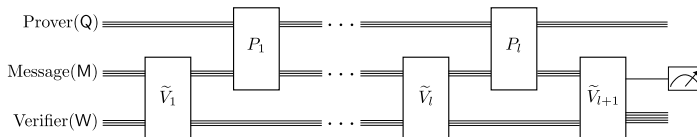


- ▶ Each \tilde{V}_j is an *almost-unitary* quantum circuit, meaning that a unitary quantum circuit with $O(\log n)$ *oblivious* intermediate measurements.
 - ◊ QIPL also contains the Condon-Ladner model ("IPL").
- ▶ For *yes* instances, the distribution of intermediate measurement outcomes $u = (u_1, \dots, u_l)$, condition on acceptance, must be *highly concentrated*.
 - ◊ This requirement leads to the NP containment for any QIPL 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 exist a u^* such that $\omega(V)|^{u^*} \geq c(n)$.

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

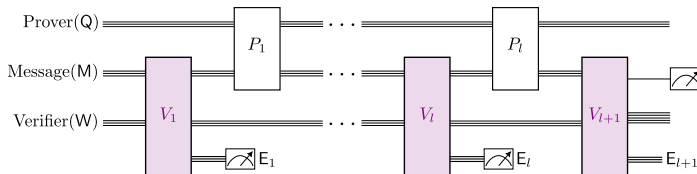
Space-bounded quantum interactive proofs (QIPL)

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



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

Applying the *principle of deferred measurements* to the almost-unitary quantum circuit \tilde{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 :



- 1 Space-bounded quantum computation meets interactive proofs
- 2 Definitions of space-bounded quantum interactive proof systems
- 3 Main results on QIP_{UL} , QIPL , and QSZK_{UL}**
- 4 Open problems

Main results on QIP_{UL} and QIPL

Theorem 1. QIPL = NP.

- QIPL is the *weakest* model that includes space-bounded classical interactive proofs, ensuring that soundness against classical messages extends to quantum.

Theorem 2. $\text{SAC}^1 \cup \text{BQL} \subseteq \text{QIP}_{\text{UL}} \subseteq \bigcup_{c(n)-s(n) \geq 1/\text{poly}(n)} \text{QIPL}_{O(1)}[c, s] \subseteq \text{P}.$

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

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

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

Main results on QIP_{UL} and QIPL (Cont.): Proof intuitions

Theorem 1. QIPL = NP.

- ▶ 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 a SDP formulation of QIPL proof systems.

Theorem 2. $\text{SAC}^1 \cup \text{BQL} \subseteq \text{QIP}_{\text{UL}} \subseteq \bigcup_{c(n)-s(n) \geq 1/\text{poly}(n)} \text{QIPL}_{O(1)}[c, s] \subseteq \text{P}$.

- ▶ 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].
 - ◊ It is known that $\text{NL} \subseteq \text{SAC}^1 = \text{LOGCFL} \subseteq \text{AC}^1 \subseteq \text{NC}^2$ [Venkateswaran'91].
- ▶ The upper bound is inspired by the SDP formulation for QIP [Vidick-Watrous'16].

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

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

Basic properties for QIPL and QIP_UL

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

① **Closure under perfect completeness.**

$$\text{QIPL}_m[c, s] \subseteq \text{QIPL}_{m+2}\left[1, 1 - \frac{1}{2}(c-s)^2\right] \text{ and } \text{QIP}_{\text{U}L}_m[c, s] \subseteq \text{QIP}_{\text{U}L}_{m+2}\left[1, 1 - \frac{1}{2}(c-s)^2\right].$$

② **Error reduction.** For any polynomial $k(n)$, there is a polynomial $m'(n)$ such that:

$$\text{QIPL}_m[c, s] \subseteq \text{QIPL}_{m'}[1, 2^{-k}] \text{ and } \text{QIP}_{\text{U}L}_m[c, s] \subseteq \text{QIP}_{\text{U}L}_{m'}[1, 2^{-k}].$$

③ **Parallelization.** $\text{QIP}_{\text{U}L}_{4m+1}[1, s] \subseteq \text{QIP}_{\text{U}L}_{2m+1}[1, (1 + \sqrt{s})/2]$.

Proof Intuition.

- ▶ Theorem 4 ① is directly adapted from [Vidick-Watrous'16].
- ▶ Theorem 4 ② uses *sequential repetition* due to the space constraint, with the key being to **force the prover to “clean” the workspace**.
- ▶ For establishing Theorem 4 ③:
 - ◇ 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.

Statistical zero-knowledge in general

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.

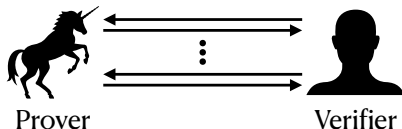


Figure: Verifier's view (\mathcal{P}_0)

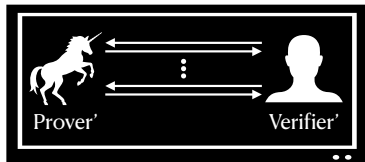


Figure: Simulated "Verifier's view" (\mathcal{P}_1)

- ▶ A common misuse (*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 indistinguishability* is then characterized by the ℓ_1 norm distance $\text{TV}(p_0, p_1) := \frac{1}{2} \|p_0 - p_1\|_1$.

Zero-knowledge property in QIP_{UL}. A 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

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

Theorem 6. QSZK_{UL} = QSZK_{ULHV} = BQL.

The INDIVPRODQSD $[k, \alpha, \delta]$ **problem** (INDIVIDUAL PRODUCT STATE DISTINGUISHABILITY)

involves two k -tuples of $O(\log n)$ -qubit states, $\sigma_1, \dots, \sigma_k$ and $\sigma'_1, \dots, \sigma'_k$, whose purifications can be prepared by unitary quantum logspace circuits, satisfying $\alpha(n) - k(n) \cdot \delta(n) \geq 1/\text{poly}(n)$ and $1 \leq k(n) \leq \text{poly}(n)$, with the following conditions:

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

QSZK_{ULHV} \subseteq BQL follows since INDIVPRODQSD is QSZK_{ULHV}-complete:

- ▶ Since INDIVPRODQSD implies an “existential” version of GAPQSD_{log}, which is BQL-complete [Le Gall-L.-Wang'23], it follows that INDIVPRODQSD \in QMAL \subseteq BQL.
- ▶ The complement of INDIVPRODQSD is QSZK_{ULHV}-hard, similar to [Watrous'02].

- 1 Space-bounded quantum computation meets interactive proofs
- 2 Definitions of space-bounded quantum interactive proof systems
- 3 Main results on QIP_{UL} , QIPL , and QSZK_{UL}
- 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:

$\text{QIP}_{\text{UL}} \subsetneq \text{QIPL}$ unless $P = NP$ (this work), while $\text{BQ}_{\text{UL}} = \text{BQL}$ [FR21, GRZ21].

- 2 We define three models of space-bounded quantum interactive proofs:

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

- 3 Introducing the *zero-knowledge* property for QIP_{UL} proof systems, i.e., QSZK_{UL} , eliminates the usual advantage gained from interaction ($\text{QSZK}_{\text{UL}} = \text{BQL}$).

Open problems

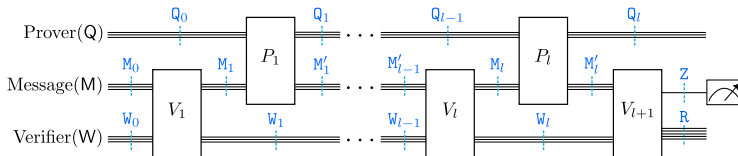
- 1 Is it possible to obtain a tighter characterization of QIP_{UL} ? For example, does QIP_{UL} contain "IPL" with $\omega(\log n)$ public coins?
- 2 What is the computational power of space-bounded quantum interactive proofs with a general quantum logspace verifier?

Thanks!

Proof techniques: Upper bounds for QIPL and QIP_{UL}

Our approach is inspired by the SDP formulation for QIP [Vidick-Watrous'16].

$\text{QIPL}_{O(1)} = \text{QIP}_{\text{UL}_{O(1)}} \subseteq \text{P}$. Consider a $2l$ -turn $\text{QIPL}_{O(1)}$ proof system $P \rightleftharpoons V$, with $l \leq O(1)$. Let $\rho_{M_j W_j}$ and $\rho_{M'_j W_j}$, for $j \in [l]$, be snapshot states in the registers (M, W) after the verifier's and prover's action in the j -th round in $P \rightleftharpoons V$, respectively.



In this SDP formulation, we consider the following:

- ◇ Variables \Leftrightarrow The snapshot states $\rho_{M'_j W_j}$ for $j \in [l]$ after each prover action;
- ◇ Objection function \Leftrightarrow Maximum acceptance probability $\omega(V)$.

These variables are **independent** due to the *unitary* verifier. The SDP constraints are:

- ① Verifier is always honest:

$$\rho_{M_j W_j} = V_j \rho_{M'_{j-1} W_{j-1}} V_j^\dagger \text{ for } j \in \{2, \dots, l\}, \text{ and } \rho_{M_1 W_1} = V_1 |\bar{0}\rangle\langle\bar{0}|_{MW} V_1^\dagger.$$

- ② Prover's actions do not change the verifier's private register:

$$\text{Tr}_{M_j}(\rho_{M_j W_j}) = \text{Tr}_{M'_j}(\rho_{M'_j W_j}) \text{ for } j \in [l].$$

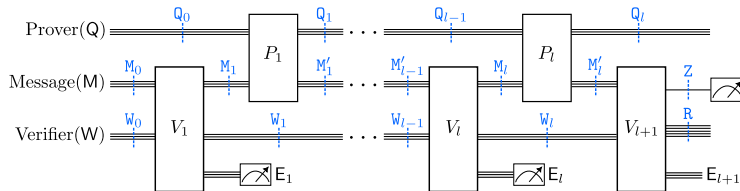
As any SDP solution holds $O(\log n)$ qubits, standard SDP solvers ensure the efficiency.

Proof techniques: Upper bounds for QIPL and QIP_{UL} (Cont.)

QIPL \subseteq NP. Now the verifier's actions are *almost-unitary* quantum circuits.

There is a family of SDP programs depending on the measurement outcome $\{u\}$:

- ◊ Variables \Leftrightarrow The *unnormalized* snapshot states $\rho_{M_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}$ for $j \in [l]$.
- ◊ Objection function $\Leftrightarrow \omega(V)|^u$, namely the contribution of u to $\omega(V)$.



For a given $u = (u_1, \dots, u_l)$, the SDP program includes two types of constraints:

- ① Verifier is always honest: Let $\rho_{M'_0 W_0} := |\bar{0}\rangle\langle\bar{0}|_{MW}$, then

$$\rho_{M_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j} = (I_{M_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}) V_j \rho_{M'_{j-1} W_{j-1}} V_j^\dagger \text{ for } j \in [1].$$
- ② Prover's actions do not change the verifier's private register:

$$\text{Tr}_{M_j}(\rho_{M_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}) = \text{Tr}_{M'_j}(\rho_{M'_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}) \text{ for } j \in [l].$$

Next, we explain the NP containment:

- ▶ The classical witness w includes an l -tuple u and a feasible poly-size solution.
- ▶ The verification procedure involves checking whether (1) the solution encoded in w satisfies the SDP constraints based on u ; and (2) $\omega(V)|^u \geq c(n)$.