Space-Bounded Quantum Interactive Proof Systems

François Le Gall
Graduate School of Mathematics, Nagoya University, Japan

Yupan Liu
Graduate School of Mathematics, Nagoya University, Japan

Harumichi Nishimura
Graduate School of Informatics, Nagoya University, Japan

Qisheng Wang
School of Informatics, University of Edinburgh, UK
Graduate School of Mathematics, Nagoya University, Japan

Abstract

We introduce two models of space-bounded quantum interactive proof systems, QIPL and $\mathsf{QIP_U L}$. The $\mathsf{QIP_U L}$ model, a space-bounded variant of quantum interactive proofs (QIP) introduced by Watrous (CC 2003) and Kitaev and Watrous (STOC 2000), restricts verifier actions to unitary circuits. In contrast, QIPL allows logarithmically many pinching intermediate measurements per verifier action, making it the weakest model that encompasses the classical model of Condon and Ladner (JCSS 1995).

We characterize the computational power of QIPL and $\mathsf{QIP_U L}$. When the message number m is polynomially bounded, $\mathsf{QIP_U L} \subsetneq \mathsf{QIPL}$ unless $\mathsf{P} = \mathsf{NP}$:

- $\mathsf{QIPL}^{\mathrm{HC}}$, a subclass of QIPL defined by a high-concentration condition on *yes* instances, exactly characterizes NP.
- $\mathsf{QIP_U L}$ is contained in P and contains $\mathsf{SAC}^1 \cup \mathsf{BQL}$, where SAC^1 denotes problems solvable by classical logarithmic-depth, semi-unbounded fan-in circuits.

However, this distinction vanishes when m is constant. Our results further indicate that (pinching) intermediate measurements uniquely impact space-bounded quantum interactive proofs, unlike in space-bounded quantum computation, where $\mathsf{BQL} = \mathsf{BQ_U L}$.

We also introduce space-bounded unitary quantum statistical zero-knowledge ($\mathsf{QSZK_U L}$), a specific form of $\mathsf{QIP_U L}$ proof systems with statistical zero-knowledge against any verifier. This class is a space-bounded variant of quantum statistical zero-knowledge (QSZK) defined by Watrous (SICOMP 2009). We prove that $\mathsf{QSZK_U L} = \mathsf{BQL}$, implying that the statistical zero-knowledge property negates the computational advantage typically gained from the interaction.

2012 ACM Subject Classification Theory of computation → Interactive proof systems; Theory of computation → Complexity classes; Theory of computation → Quantum complexity theory

Keywords and phrases Intermediate measurements, Quantum interactive proofs, Space-bounded quantum computation

Digital Object Identifier 10.4230/LIPIcs.CCC.2025.17

Related Version *Full Version*: `https://arxiv.org/abs/2410.23958v3` [41]

Funding This work was partially supported by MEXT Q-LEAP grant No. JPMXS0120319794.
François Le Gall: Supported in part by JSPS KAKENHI grants Nos. JP20H05966, 20H00579, 24H00071, and by MEXT JST CREST grant No. JPMJCR24I4.
Yupan Liu: Supported in part by JST SPRING grant No. JPMJSP2125 and the "THERS Make New Standards Program for the Next Generation Researchers."
Harumichi Nishimura: Supported in part by JSPS KAKENHI grants Nos. JP19H04066, JP20H05966, JP21H04879, and JP22H00522.
Qisheng Wang: Supported in part by the Engineering and Physical Sciences Research Council under Grant No. EP/X026167/1.

Acknowledgements The authors appreciate Dorian Rudolph for pointing out a gap in the earlier argument that QIPL is contained in AM, specifically noting that Lemma 3.14 in the full version [41] does not directly apply to QIPL, as it does not verify the consistency of the prover strategies across different measurement outcome branches. YL is grateful to Uma Girish for a helpful discussion that inspired Question c. The authors also thank the anonymous reviewers for their helpful comments, which made the introduction more accessible to non-expert readers.

1 Background

Recent advancements in quantum computation with a limited number of qubits have been achieved from both theoretical and experimental perspectives. Theoretical work began in the late 1990s, focusing on feasible models of quantum computation operating under space restrictions, where the circuit acts on $O(\log n)$ qubits and consists of $\mathrm{poly}(n)$ elementary gates [61, 64]. These models, referred to as quantum logspace, were later shown during the 2010s to offer a quadratic space advantage for certain problems over the best known classical algorithms [57, 18], which saturates the classical simulation bound. In recent years, this area has gained increased attention, particularly in eliminating (pinching) intermediate measurements in these models [19, 26], and through further developments [25, 68]. Motivated by these achievements in quantum logspace, we are interested in exploring the power of the quantum interactive proof systems where the verifier is restricted to quantum logspace.

To put it simply, in a single-prover (quantum) interactive proof system for a promise problem $(\mathcal{I}_{\mathrm{yes}}, \mathcal{I}_{\mathrm{no}})$, a computationally weak (possibly quantum) *verifier* interacts with a computationally all-powerful but untrusted *prover*. In quantum scenarios, the prover and verifier may share entanglement during their interactions. Given an input $x \in \mathcal{I}_{\mathrm{yes}} \cup \mathcal{I}_{\mathrm{no}}$, the prover claims that $x \in \mathcal{I}_{\mathrm{yes}}$, but the verifier does not simply accept this claim. Instead, an interactive protocol is initiated, after which the verifier either "accepts" or "rejects" the claim. The protocol has completeness parameter c, meaning that if x is in $\mathcal{I}_{\mathrm{yes}}$ and the prover honestly follows the protocol, the verifier accepts with probability at least c. The protocol has soundness parameter s, meaning that if x is in $\mathcal{I}_{\mathrm{no}}$ then the verifier accepts with probability at most s, regardless of whether the prover follows the protocol. Typically, an interactive protocol for $(\mathcal{I}_{\mathrm{yes}}, \mathcal{I}_{\mathrm{no}})$ has completeness $c = 2/3$ and soundness $s = 1/3$.

1.1 Interactive proof systems with time-bounded verifier

The exploration of classical interactive proof systems (IP) was initiated in the 1980s [4, 29]. In these proof systems, the verifier is typically bounded by polynomial time, and $\mathsf{IP}[m]$ represents interactive protocols involving m messages during interactions. Particularly, when the verifier's messages are merely random bits, these *public-coin* proof systems are known as *Arthur-Merlin proof systems* [4]. Shortly thereafter, it was established that any constant-message IP protocol can be parallelized to a two-message public-coin protocol, captured by the class AM, and thus $\mathsf{IP}[O(1)]$ is contained in the second level of the polynomial-time hierarchy [4, 30]. However, IP protocols with a polynomial number of messages have been shown to be exceptionally powerful, as demonstrated by the seminal result $\mathsf{IP} = \mathsf{PSPACE}$ [46, 56]. Consequently, IP protocols with a polynomial number of messages generally cannot be parallelized to a constant number of messages unless the polynomial-time hierarchy collapses.[1]

[1] The assumption that the polynomial-time hierarchy does not collapse generalizes the conjecture that $\mathsf{P} \subsetneq \mathsf{NP}$.

About fifteen years after the introduction of interactive proof systems (and a model of quantum computation), the study of quantum interactive proof systems (QIP) began [63]. Remarkably, any QIP protocol with a polynomial number of messages can be parallelized to three messages [37]. A quantum Arthur-Merlin proof system was subsequently introduced in [47], and any three-message QIP protocol can be transformed into this form (QMAM). By the late 2000s, the computational power of QIP was fully characterized: The celebrated result QIP = PSPACE [35] established that QIP is not more powerful than IP as long as the gap $c-s$ is at least polynomially small. However, when the gap $c-s$ is double-exponentially small, this variant of QIP is precisely characterized by EXP [33]. In the late 2010s, another quantum counterpart of the Arthur-Merlin proof system was considered in [39], where the verifier's message is either random bits or halves of EPR pairs, leading to a quadrichotomy theorem that classifies the corresponding QIP protocols.

1.2 Interactive proof systems with space-bounded verifier

The investigation of (classical) interactive proof systems with space-bounded verifiers started in the late 1980s [16, 8], alongside research on time-bounded verifiers. Notably, by using the fingerprinting lemma [44], Condon and Ladner [10] showed that the class of (private-coin) classical interactive proof systems with logarithmic-space verifiers using $O(\log n)$ random bits exactly characterizes NP. In parallel, public-coin space-bounded classical interactive proofs were explored in the early 1990s [21, 20, 9]. By around 2010, it was established that such space-bounded protocols with $\mathrm{poly}(n)$ public coins precisely characterize P [28].

Space-bounded Merlin-Arthur-type proof systems were also studied in the early 1990s. In particular, when the verifier operates in classical logspace with $O(\log n)$ random bits and has *online access* to a $\mathrm{poly}(n)$-bit message, the proof system exactly characterizes NP [44]. More recently, restricting the computational power of the honest prover to quantum logspace (BQL) has led to a counterpart *classical* proof system that exactly characterizes BQL [27].

Although research has been conducted on quantum interactive proofs where the verifier uses quantum finite automata [51, 52, 67], analogous to classical work [16], to our knowledge no prior work has addressed space-bounded counterparts of quantum interactive proofs that align with the circuit-based model defined in [37, 63]. In the case *without interaction*, space-bounded quantum Merlin-Arthur proof systems have been studied recently. When the verifier has *direct access* to an $O(\log n)$-qubit message, meaning it can process the message directly in its workspace qubits, this variant (QMAL) is as weak as BQL [17, 19]. However, when the (unitary) verifier has online access to a $\mathrm{poly}(n)$-qubit message, where each qubit in the message state is read-once, this variant is as strong as QMA [24].[2]

It is important to note that online and direct access to messages during interactions makes no difference for time-bounded interactive or Merlin-Arthur-type proof systems, whether classical or quantum. This distinction arises from the nature of space-bounded computation.

[2] An exponentially up-scaled quantum counterpart of the space-bounded Merlin-Arthur-type proof system from [44], with *classical* messages, was also considered in [24]. The variant with *unitary* quantum *polynomial*-space verifier, implicitly allowing $\mathrm{poly}(n)$ random bits, precisely corresponds to NEXP.

2 Main results

2.1 Definitions of QIPL and $\mathsf{QIP_U L}$

We introduce *space-bounded quantum interactive proof systems* and their unitary variant, denoted as QIPL and $\mathsf{QIP_U L}$, respectively. In these proof systems, the verifier V operates in quantum logspace and has direct access to messages during interaction with the prover P. Specifically, in a $2l$-turn (message) space-bounded quantum interactive proof system for a promise problem $(\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$, this proof system $P \rightleftharpoons V$ consists of the prover's private register Q, the message register M, and the verifier's private register W. Both M and W are of size $O(\log n)$, with M being accessible to both the prover and the verifier.[3]

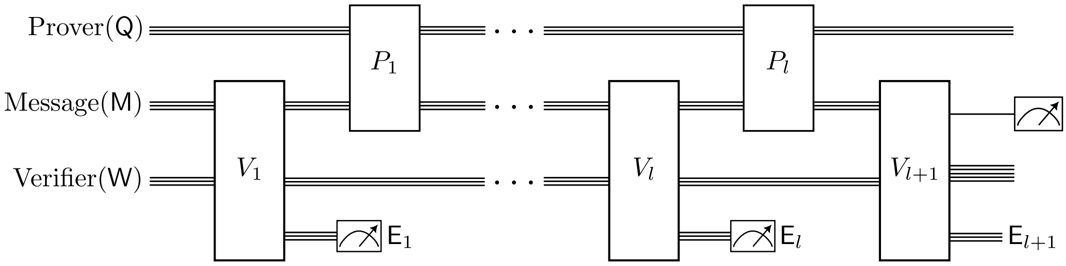

Figure 1 A $2l$-turn single-prover space-bounded quantum interactive proof system (QIPL), where each environment register E_j is introduced by applying the principle of deferred measurements to an almost-unitary quantum circuit $\widetilde{V}_j$, resulting in the isometric quantum circuit V_j.

The verifier V maps an input $x \in \mathcal{I}_{\text{yes}} \cup \mathcal{I}_{\text{no}}$ to a sequence $(V_1, \cdots, V_{l+1})$, with V_j for $j \in [l]$ representing the verifier's actions at the $(2j-1)$-th turn, and V_{l+1} representing the verifier's action just before the final measurement. The primary difference between QIPL and $\mathsf{QIP_U L}$ proof systems lies in the verifier's action V_j for $j \in [l]$:

- In QIPL proof systems, each V_j corresponds to an *almost-unitary* quantum circuit $\widetilde{V}_j$ that includes $O(\log n)$ *pinching* intermediate measurements in the computational basis.[4] Each such measurement maps a single-qubit state ρ to $\sum_{b\in\{0,1\}} \mathrm{Tr}(|b\rangle\langle b|\rho)|b\rangle\langle b|$.[5] The $O(\log n)$ bound reflects the maximum number of measurement outcomes that can be stored in logspace, aligning with the verifier's direct access to the message. For convenience, we apply the principle of deferred measurements (e.g., [50, Section 4.4]), transforming the circuit $\widetilde{V}_j$ into an *isometric* quantum circuit V_j with a newly introduced environment register E_j,[6] which is measured at the end of that turn, with the measurement outcome denoted by u_j, as illustrated in Figure 1. Furthermore, each environment register E_j remains private to the verifier and becomes inaccessible after the round that starts with the verifier's j-th action.
- In $\mathsf{QIP_U L}$ proof systems, each V_j is a unitary quantum circuit.

[3] Our definitions of QIPL and $\mathsf{QIP_U L}$ can be straightforwardly extended to the corresponding proof systems with an odd number of messages, as shown in [41, Figure 4.1].

[4] We note that restricting the number of pinching measurements in each verifier turn V_j from polynomial in n to $O(\log n)$ does not cause any loss of generality, provided that the QIPL proof system has a polynomial number of turns. See [41, Remark 3.5] for further details.

[5] Pinching intermediate measurements naturally arise in space-bounded quantum computation, particularly in recent developments on eliminating intermediate measurements in quantum logspace [26, 25]. In this context, the quantum channels that capture the space-bounded computation are *unital* in the case of qubits.

[6] An $O(\log n)$-qubit isometric quantum circuit utilizes $O(\log n)$ ancillary gates, with each ancillary gate introducing an ancillary qubit $|0\rangle$. For further details, please refer to [41, Definition 2.8].

The prover's actions can be similarly described by unitary quantum circuits. A proof system $P \rightleftharpoons V$ is said to *accept* if, after the verifier performs V_{l+1} and measures the designated output qubit in the computational basis, the outcome is 1. Additionally, we require *a strong notion of uniformity* for the verifier's mapping: the description of the sequence $(V_1, \cdots, V_{l+1})$ must be computable by a single deterministic logspace Turing machine.[7]

Lastly, for $\mathsf{QIPL}^{\mathrm{HC}}$ proof systems, we impose an additional restriction on *yes* instances: the distribution of intermediate measurement outcomes $u = (u_1, \cdots, u_l)$, conditioned on acceptance, must be *highly concentrated*. More precisely, let $\omega(V)|^u$ be the contribution of u to $\omega(V)$, where $\omega(V)$ is the maximum acceptance probability of $P \rightleftharpoons V$. Then, there must exist a u^* such that $\omega(V)|^{u^*} \geq c(n)$.

We denote m-turn space-bounded quantum interactive proof systems with completeness c and soundness s as $\mathsf{QIPL}_m[c, s]$, and their unitary variant as $\mathsf{QIP_UL}_m[c, s]$. In particular, we adopt the following notations, which naturally extend to $\mathsf{QIP_UL}$:

$$\mathsf{QIPL}_m \coloneqq \mathsf{QIPL}_m[2/3, 1/3] \text{ and } \mathsf{QIPL} \coloneqq \cup_{1 \leq m \leq \mathrm{poly}(n)} \mathsf{QIPL}_m.$$

In *constant*-turn scenarios, it is crucial to emphasize that the proof systems $\mathsf{QIPL}_{O(1)}[c, s]$ and $\mathsf{QIP_UL}_{O(1)}[c, s]$ can directly simulate each other, as the environment registers $\mathsf{E}_1, \cdots, \mathsf{E}_{O(1)}$ collectively holds $O(\log n)$ qubits.[8] Therefore, for simplicity, we define $\mathsf{QIPL}_{O(1)}[c, s]$ proof systems in which the verifier's actions are implemented by *unitary* quantum circuits.

2.2 Space-bounded (unitary) quantum interactive proofs

Our first theorem serves as a quantum analog of the classical work by Condon and Ladner [10]:

▶ **Theorem 1** (Informal of [41, Theorem 3.1])**.**

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

Interestingly, Theorem 1 suggests that the $\mathsf{QIPL}^{\mathrm{HC}}$ model can be viewed as the *weakest* model that encompasses space-bounded (private-coin) classical interactive proofs, as considered in [10]. Our definitions of QIPL and its subclass $\mathsf{QIPL}^{\mathrm{HC}}$ aim to introduce quantum counterparts that include these classical proof systems, ensuring that soundness against classical messages also holds for quantum messages. Similar soundness issues challenged multi-prover scenarios (e.g., proving $\mathsf{MIP} \subseteq \mathsf{MIP}^*$) for nearly a decade [7, 34], while in the single-prover settings (e.g., proving $\mathsf{IP} \subseteq \mathsf{QIP}$), it is typically resolved by measuring the prover's quantum messages and treating the outcomes as classical messages (e.g., [1, Claim 1]).

However, space-bounded *unitary* quantum interactive proofs ($\mathsf{QIP_UL}$), which denote the most natural space-bounded counterpart to quantum interactive proofs as defined in [37, 64], do not directly achieve the stated soundness guarantee. Hence, $\mathsf{QIP_UL}$ may be computationally weaker than QIPL. Our second theorem characterizes the computational power of $\mathsf{QIP_UL}$:

[7] A weaker notion of uniformity only requires that the description of each V_j can be individually computed by a deterministic logspace Turing machine. It is important to note that these distinctions do not arise in the time-bounded setting, as the composition of a polynomial number of deterministic polynomial-time Turing machines can be treated as a single deterministic polynomial-time Turing machine.

[8] This equivalence follows directly from the principle of deferred measurements. However, for constant-turn space-bounded quantum interactive proofs, allowing each verifier action to involve poly(n) pinching intermediate measurements might increase the proof system's power beyond the unitary case. This is because current techniques for proving results such as $\mathsf{BQL} = \mathsf{BQ_UL}$ [19, 26, 25] do not directly apply in this context.

▶ **Theorem 2** (Informal of [41, Theorems 3.3 and 4.2]). *The following holds*:

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

Theorems 1 and 2 suggest that $\mathsf{QIP_U L}$ is indeed *weaker* than QIPL unless $\mathsf{P} = \mathsf{NP}$. Interestingly, this distinction from the unitary case arises even when each verifier action is slightly more powerful than a unitary quantum circuit. It is also noteworthy that the class SAC^1 is equivalent to LOGCFL [59], which contains NL and is contained in AC^1.[9] Our third theorem, meanwhile, focuses on space-bounded quantum interactive proof systems with a constant number of messages:

▶ **Theorem 3** (Informal of [41, Theorem 4.3]). *For any $c(n) - s(n) \geq \Omega(1)$,*

$$\mathsf{QIPL}_{O(1)}[c,s] \subseteq \mathsf{NC}.$$

To compare with time-bounded classical or quantum interactive proofs, we summarize our three theorems in Table 1. Notably, our two models of space-bounded quantum interactive proofs, QIPL and $\mathsf{QIP_U L}$, demonstrate behavior that is distinct from both:

- For (time-bounded) classical interactive proofs, all proof systems with $m \leq O(1)$ (the regime of the last row in Table 1) are contained in the second level of the polynomial-time hierarchy [4, 30], whereas the class of proof systems with $m = \operatorname{poly}(n)$ (the regime of the second and third rows in Table 1) exactly characterizes PSPACE [46, 56].
- For (time-bounded) quantum interactive proofs, all proof systems with parameters listed in Table 1 precisely capture PSPACE [63, 37, 35].

Table 1 The computational power of QIPL and $\mathsf{QIP_U L}$ with different parameters.

	Models	Constant gap $c(n)-s(n)\geq\Omega(1)$	Polynomial small gap $c(n)-s(n)\geq 1/\operatorname{poly}(n)$
The number of messages: $m(n)=\operatorname{poly}(n)$	$\mathsf{QIPL}^{\mathrm{HC}}(\subseteq \mathsf{QIPL})$	NP Theorem 1	NP Theorem 1
The number of messages: $m(n)=\operatorname{poly}(n)$	$\mathsf{QIP_U L}$	contains $\mathsf{SAC}^1 \cup \mathsf{BQL}$ & in P Theorem 2	contains $\mathsf{SAC}^1 \cup \mathsf{BQL}$ & in P Theorem 2
The number of messages: $3 \leq m(n) \leq O(1)$	QIPL & $\mathsf{QIP_U L}$	in NC Theorem 3	contains $\mathsf{SAC}^1 \cup \mathsf{BQL}$ & in P Theorem 2

The central intuition underlying Table 1 is that *parallelization* [37, 36], perhaps the most striking complexity-theoretic property of QIP proof systems, distinguishes $\mathsf{QIP_U L}$ from QIPL. Quantum logspace operates within a polynomial-dimensional Hilbert space, remaining computationally weak even with a constant number of interactions, and is (at least) contained in P. In $\mathsf{QIP_U L}$, the verifier's actions are *reversible* and *dimension-preserving*, allowing direct application of parallelization techniques from [36]. In contrast, QIPL and its reversible generalization lack dimension preservation, requiring significantly more than $O(\log n)$ space to parallelize the verifier's actions, which prevents parallelization.

[9] For more details on the computational power of SAC^1 and related complexity classes, see [41, Section 2.4].

2.3 Space-bounded unitary quantum statistical zero-knowledge

We also introduce *(honest-verifier) space-bounded unitary quantum statistical zero-knowledge*, denoted as $\mathsf{QSZK_U L_{HV}}$. This term refers to a specific form of space-bounded quantum proofs that possess statistical zero-knowledge against an honest verifier. Specifically, a space-bounded unitary quantum interactive proof system possesses this zero-knowledge property if there exists a quantum logspace simulator that approximates the snapshot states ("the verifier's view") on the registers M and W after each turn of this proof system, where each state approximation must be very close ("indistinguishable") to the corresponding snapshot state with respect to the trace distance.

Our definition $\mathsf{QSZK_U L_{HV}}$ serves as a space-bounded variant of honest-verifier (unitary) quantum statistical zero-knowledge, denoted by $\mathsf{QSZK_{HV}}$, as introduced in [62]. Our fourth theorem establishes that the statistical zero-knowledge property completely negates the computational advantage typically gained through the interaction:

▶ **Theorem 4** (Informal of [41, Theorem 5.2])**.**

$$\mathsf{QSZK_U L} = \mathsf{QSZK_U L_{HV}} = \mathsf{BQL}.$$

In addition to $\mathsf{QSZK_U L_{HV}}$, we can define $\mathsf{QSZK_U L}$ in line with [65], particularly considering space-bounded unitary quantum statistical zero-knowledge against *any verifier* (rather than an honest verifier). Following this definition, $\mathsf{BQL} \subseteq \mathsf{QSZK_U L} \subseteq \mathsf{QSZK_U L_{HV}}$. Interestingly, Theorem 4 serves as a direct space-bounded counterpart to $\mathsf{QSZK} = \mathsf{QSZK_{HV}}$ [65].

The intuition behind Theorem 4 is that the snapshot states after each turn capture all the essential information in the proof system, such as allowing optimal prover strategies to be "recovered" from these states [48, Section 7]. In space-bounded scenarios, space-efficient quantum singular value transformation [42] enables fully utilizing this information.

Finally, we emphasize that our consideration of this zero-knowledge property is purely complexity-theoretic. A full comparison with other notions of (statistical) zero-knowledge is beyond this scope. For more on classical and quantum statistical zero-knowledge, see [58] and [60, Chapter 5].

3 Proof techniques

Standard techniques for quantum interactive proofs are typically developed under the restriction that the verifier is *unitary*. While this restriction does not limit generality in time-bounded settings (e.g., see [60, Section 4.1.4]), it presents difficulties in the context of space-bounded quantum interactive proofs, where verifiers may not be unitary. In what follows, we highlight the challenges that arise and briefly explain how we address them.

3.1 Upper bounds for $\mathsf{QIPL^{HC}}$ and $\mathsf{QIP_U L}$

3.1.1 $\mathsf{QIPL_{O(1)}} \subseteq \mathsf{P}$

We prove this inclusion using a semi-definite program (SDP) for a given $\mathsf{QIPL_{O(1)}}$ proof system, adapted from the SDP formulation for QIP in [60, 66]. Together with the turn-halving lemma, specifically Theorem 53, this inclusion implies that $\mathsf{QIP_U L} \subseteq \mathsf{P}$.

Consider a $(2l)$-turn $\mathsf{QIPL_{O(1)}}$ proof system $P \rightleftharpoons V$, where $l \leq O(1)$. Let $\rho_{\mathtt{M}_j\mathtt{W}_j}$ and $\rho_{\mathtt{M}'_j\mathtt{W}_j}$, for $j \in [l]$, denote snapshot states in the register M and W after the $(2j-1)$-st turn and the $(2j)$-th turn in $P \rightleftharpoons V$, respectively, as illustrated in [41, Figure 3.1]. The variables in this SDP correspond to these snapshot states after each prover's action, particularly $\rho_{\mathtt{M}'_j\mathtt{W}_j}$ for

$j \in [l]$, while the objective function is the maximum acceptance probability $\omega(V)$ of $P \rightleftharpoons V$. Since the verifier's actions are *unitary* circuits, these variables can be treated independently. Hence, the SDP program mainly consists of two types of constraints, assuming that all variables are valid quantum states:

(i) Verifier's actions only operate on the registers M and W:

$$\rho_{\mathtt{M}_j\mathtt{W}_j} = V_j \rho_{\mathtt{M}'_{j-1}\mathtt{W}_{j-1}} V_j^\dagger \text{ for } j \in \{2, \cdots, l\}, \text{ and } \rho_{\mathtt{M}_1\mathtt{W}_1} = V_1 |\bar{0}\rangle\langle\bar{0}|_{\mathsf{MW}} V_1^\dagger.$$

(ii) Prover's actions do not change the verifier's private register:

$$\mathrm{Tr}_{\mathtt{M}_j}(\rho_{\mathtt{M}_j\mathtt{W}_j}) = \mathrm{Tr}_{\mathtt{M}'_j}(\rho_{\mathtt{M}'_j\mathtt{W}_j}) \text{ for } j \in [l]. \tag{1}$$

Since the variables in this SDP collectively hold $O(\log n)$ qubits, a standard SDP solver (e.g., [23]) provides a deterministic polynomial-time algorithm for approximately solving it.

3.1.2 $\mathsf{QIPL}^{\mathrm{HC}} \subseteq \mathsf{NP}$

We now extend the above SDP formulation to l-round QIPL proof systems, in which the verifier's j-th action $\widetilde{V_j}$ is an *almost-unitary* quantum circuit that allows $O(\log n)$ pinching intermediate measurements. For simplicity, we instead consider the corresponding isometric quantum circuit V_j, which introduces a new environment register E_j measured at the end of the turn, with the outcome denoted by u_j.

Recall that $\omega(V)|^u$ represents the contribution of the measurement outcome branch $u = (u_1, \cdots, u_l)$ to the maximum acceptance probability $\omega(V)$. Owing to the high-concentration condition, it suffices to consider an *approximation* $\widehat{\omega}(V)|^u$ of $\omega(V)|^u$ for some specific branch u, satisfying

$$\omega(V)|^u \leq \widehat{\omega}(V)|^u \leq \omega(V).$$

These bounds follow from two facts: (1) pinching measurements eliminate coherence between subspaces corresponding to different branches, which enables $\omega(V)|^u$ to be approximately optimized in isolation; and (2) the acceptance probability of any associated global prover strategy across all branches cannot exceed $\omega(V)$.

By extending the SDP formulation of $\mathsf{QIPL}_{\mathrm{O}(1)}$ proof systems, we construct a family of SDP programs depending on the measurement outcome branches $\{u\}$. Let $\rho_{\mathtt{M}_j\mathtt{W}_j} \otimes |u_j\rangle\langle u_j|_{\mathsf{E}_j}$ denote the *unnormalized* snapshot states after measuring E_j. For a fixed branch u, the associated SDP program includes the following three types of constraints:

(i') $\rho_{\mathtt{M}_j\mathtt{W}_j} \otimes |u_j\rangle\langle u_j|_{\mathsf{E}_j} = \big(I_{\mathtt{M}_j\mathtt{W}_j} \otimes |u_j\rangle\langle u_j|_{\mathsf{E}_j}\big) V_j \rho_{\mathtt{M}'_{j-1}\mathtt{W}_{j-1}} V_j^\dagger$ for $j \in \{2, \cdots, l\}$, and $\rho_{\mathtt{M}_1\mathtt{W}_1} \otimes |u_1\rangle\langle u_1|_{\mathsf{E}_1} = \big(I_{\mathtt{M}_1\mathtt{W}_1} \otimes |u_1\rangle\langle u_1|_{\mathsf{E}_1}\big) V_1 |\bar{0}\rangle\langle\bar{0}|_{\mathsf{MW}} V_1^\dagger$.

(ii') $\mathrm{Tr}_{\mathtt{M}_j}(\rho_{\mathtt{M}_j\mathtt{W}_j} \otimes |u_j\rangle\langle u_j|_{\mathsf{E}_j}) = \mathrm{Tr}_{\mathtt{M}'_j}(\rho_{\mathtt{M}'_j\mathtt{W}_j} \otimes |u_j\rangle\langle u_j|_{\mathsf{E}_j})$ for $j \in [l]$.

(iii') $\mathrm{Tr}(\rho_{\mathtt{M}_j\mathtt{W}_j} \otimes |u_j\rangle\langle u_j|_{\mathsf{E}_j}) = \mathrm{Tr}(\rho_{\mathtt{M}'_j\mathtt{W}_j} \otimes |u_j\rangle\langle u_j|_{\mathsf{E}_j})$ for $j \in [l]$.

Notably, for the third type of constraints, both sides evaluate to exactly 1 when the verifier is unitary, as in the cases of QIP and $\mathsf{QIP}_{\mathrm{U}}\mathsf{L}$. In contrast, for QIPL proof systems, the value varies across different measurement outcome branches and remains bounded above by 1. Crucially, this value is entirely determined by the verifier's actions and cannot be altered by the prover.

Next, we explain the NP containment. The classical witness w consists of an l-tuple u, indicating a specific SDP program, and a feasible solution $(\rho_{\mathtt{M}'_1\mathtt{W}_1}, \cdots, \rho_{\mathtt{M}'_l\mathtt{W}_l})$ to this SDP program. This solution can be represented by l square matrices of dimension $\mathrm{poly}(n)$, thus having polynomial size. The verification procedure involves checking (1) whether the solution encoded in w satisfies these SDP constraints based on u; and (2) whether $\widehat{\omega}(V)|^u \geq c(n)$. All these checks can be verified using basic matrix operations in deterministic polynomial time.

3.2 Basic properties for QIPL and $\mathsf{QIP_U L}$

We begin by outlining three basic properties of space-bounded (unitary) quantum interactive proof systems, which are dependent on the parameters $c(n)$, $s(n)$, and $m(n)$:

▶ **Theorem 5** (Properties for QIPL and $\mathsf{QIP_U L}$, informal of [41, Theorem 3.2 and Lemma 4.5])**.** *Let $c(n)$, $s(n)$, and $m(n)$ be functions such that $0 \le s(n) < c(n) \le 1$, $c(n) - s(n) \ge 1/\operatorname{poly}(n)$, and $1 \le m(n) \le \operatorname{poly}(n)$. Then, it holds that:*

(1) Closure under perfect completeness*.*

$$\mathsf{QIPL}_m[c,s] \subseteq \mathsf{QIPL}_{m+2}[1, 1-(c-s)^2/2] \text{ and } \mathsf{QIP_U L}_m[c,s] \subseteq \mathsf{QIP_U L}_{m+2}[1, 1-(c-s)^2/2].$$

(2) Error reduction*. For any polynomial $k(n)$,*

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

Here, $m' := O\big(km/\log\frac{1}{1-(c-s)^2/2}\big)$.

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

Achieving perfect completeness for QIPL and $\mathsf{QIP_U L}$ proof systems, particularly Theorem 51, can be adapted from the techniques used in QIP proof systems [60, Section 4.2.1] (or [37, Section 3]) by adding two additional turns. However, there are important subtleties to consider when establishing the other properties in Theorem 5.

3.2.1 Error reduction via sequential repetition

Since each message is of size $O(\log n)$, error reduction via *parallel repetition* does not apply to QIPL and $\mathsf{QIP_U L}$ when the gap $c - s$ is polynomially small, regardless of the number of messages.[10] Alternatively, error reduction via *sequential repetition* requires that the registers M and W (the "workspace") must be in the all-zero state ("cleaned") before each execution of the original proof systems. While this is trivial for QIP proof systems, it poses a challenge for QIPL and $\mathsf{QIP_U L}$ proof systems because the (almost-)unitary quantum logspace verifier cannot achieve this on its own.

To establish Theorem 52, our solution is to have *the prover "clean" the workspace* while ensuring that the prover behaves honestly. This is achieved through the following proof system: The verifier applies a multiple-controlled adder before each proof system execution, with the adder being activated only when the control qubits are all zero. The verifier then measures the register that the adder acts on and accepts if (1) the workspace is "cleaned" for each execution and (2) *all* outcomes of the original proof system executions are acceptance.

3.2.2 Parallelization and strict uniformity condition for the verifier's mapping

The original parallelization technique proposed in [37, Section 4] applies only to $\mathsf{QIP_U L}$ (also QIPL) proof systems with a constant number of messages. This limitation stems from the requirement that the prover sends the snapshot states for all m turns in a single message. As m increases, the size of this message grows to $O(m \log n)$, which becomes $\omega(\log n)$ when $m = \omega(1)$.

[10] Still, error reduction via parallel repetition works for QIPL when the gap $c - s \ge \Omega(1)$; see [41, Lemma 4.4].

To overcome this issue, we adapt the technique from [36, Section 4], a "dequantized" version of the original approach that fully utilizes the *reversibility* of the verifier's actions. Instead of sending all snapshot states in one message, the new verifier performs the original verifier's action or its reverse at any turn in a single action. Specifically, when applying this method to a $(4m+1)$-turn $\mathsf{QIP_U L}$ proof system $P \rightleftharpoons V$, the prover starts by sending only the snapshot state after the $(2m+1)$-st turn. The verifier then chooses $b \in \{0,1\}$ uniformly at random: if $b=0$, the verifier continues to interact with the prover according to $P \rightleftharpoons V$, keeping the acceptance condition unchanged; while if $b=1$, the verifier executes $P \rightleftharpoons V$ in reverse, and finally accepts if its private qubits are all zero. This proof system, which halves the number of turns, is referred to as the *turn-halving lemma*, as detailed in Theorem 53.

Next, we establish Theorem 2 by applying the turn-halving lemma $O(\log n)$ times.[11] Specifically, any $\mathsf{QIP_U L}$ proof system with a polynomial number of messages can be parallelized to three messages,[12] while the gap $c-s$ of the resulting proof system becomes polynomially small. However, this reasoning poses a challenge: the resulting verifier must know all original verifier actions, necessitating a strong notion of uniformity for the verifier's mapping in our definition of $\mathsf{QIP_U L}$. In addition, to prove Theorem 3, we adopt a similar approach to that used for QIP, particularly $\mathsf{QIP}[3] \subseteq \mathsf{QMAM}$ [47], which inspired the turn-halving lemma [36, Section 4], and an exponentially down-scaling version of the work [35].

3.3 Lower bounds for QIPL and $\mathsf{QIP_U L}$

3.3.1 $\mathsf{NP} \subseteq \mathsf{QIPL}$

This inclusion draws inspiration from the interactive proof system in [10, Lemma 2] and presents a challenge in adapting this proof system to the QIPL setting. Notably, our construction essentially provides a $\mathsf{QIPL^{HC}}$ proof system, since the pinching measurement outcomes are *unique* (even stronger than the high-concentration condition) for *yes* instances.

We start by outlining this QIPL proof system for 3-SAT. Consider a 3-SAT formula

$$\phi = C_1 \vee C_2 \vee C_3 = (x_1 \vee x_2 \vee x_3) \wedge (\neg x_4 \vee \neg x_2 \vee x_3) \wedge (x_4 \vee \neg x_1 \vee \neg x_3)$$

with $k=3$ clauses and $n=4$ variables. An assignment α of ϕ assigns each variable x_j for $j \in [n]$ a value α_j of either $\top$ (true) or $\perp$ (false). To verify whether ϕ is satisfied by the assignment α, we encode $\phi(\alpha)$ as $\mathrm{Enc}(\phi(\alpha))$, consisting of $3k$ triples (l,i,v), where l denotes the literal (either x_j or $\neg x_j$), i represents the i-th clause, and v denotes the value assigned to l. The prover's actions are divided into two phases:

(i) Consistency Check (for variables). The prover sends one by one all the triples (l,i,v) in $\mathrm{Enc}(\phi(\alpha))$, ordered by the variable $\mathrm{var}(l)$ corresponding to the literal l;

(ii) Satisfiability Check (for clauses). For each $i \in \{1,\ldots,k\}$, the prover sends the three triples (l_1,i,v_1), (l_2,i,v_2), and (l_3,i,v_3) in $\mathrm{Enc}(\phi(\alpha))$.

The verifier's actions are as follows. To prevent the prover from entangling with the verifier and revealing the private coins, the verifier measures the received messages in the computational basis at the beginning of each action, interpreting the measurement outcomes as the prover's messages. Therefore, it suffices to establish soundness *against classical messages.*

[11] An operation based on r random bits can be simulated by a corresponding unitary controlled by the state $|+\rangle^{\otimes r}$, where $|+\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Thus, simulating $O(\log n)$ random bits across all turns of the proof system requires $O(\log n)$ ancillary qubits in total, which is feasible for the unitary quantum logspace verifier in $\mathsf{QIP_U L}$.

[12] Although the turn-halving lemma does not directly apply to QIPL proof systems, a similar reasoning works for its reversible generalization $\mathsf{QIPL^{\diamond}}$, reducing a constant number of messages to three.

We now focus on this specific proof system. In Phase (i), the verifier checks whether the assigned values to the same variable are consistent. Since the verifier's actions are almost-unitary circuits and *cannot discard information*, this seems challenging. Our solution is that the verifier keeps only the current and the previous triples, returning the previous triple to the prover in the next turn. In Phase (ii), the verifier checks whether each batch of three triples is satisfied and returns them immediately. Lastly, to ensure that the multisets of triples from Phase (i) and (ii) are identical, the verifier computes the "fingerprint" of these multisets,[13] triple by triple, and compares the fingerprints from both phases at the end. The verifier accepts if all checks succeed.

Using the fingerprinting lemma [44], we prove the correctness of this proof system, showing that 3-SAT $\in \mathsf{QIPL}_{8k}[1,1/3]$. Interestingly, when combined with the inclusion $\mathsf{QIPL}^{\mathrm{HC}} \subseteq \mathsf{NP}$, this proof system implies (indirect) error reduction for $\mathsf{QIPL}^{\mathrm{HC}}$ (see [41, Remark 3.15]).

3.3.2 $\mathsf{SAC}^1 \subseteq \mathsf{QIP}_{\mathrm{U}}\mathsf{L}$

This inclusion is inspired by the interactive proof system in [21, Section 3.4]. By using error reduction for $\mathsf{QIP}_{\mathrm{U}}\mathsf{L}$, specifically Theorem 52, it remains to demonstrate that $\mathsf{SAC}^1 \subseteq \mathsf{QIP}_{\mathrm{U}}\mathsf{L}[1, 1-1/\mathrm{poly}(n)]$. A Boolean circuit is defined as a (uniform) SAC^1 circuit C if it is an $O(\log n)$-depth Boolean circuit that employs unbounded fan-in OR gates, bounded fan-in AND gates, and negation gates at the input level.

The interactive proof system for evaluating the circuit C starts at its top gate. If the gate is an OR, the prover selects a child gate; if it's an AND, the verifier flips a coin to select one. This process repeats until reaching an input x_i or its negation, with the verifier accepting if $x_i = 1$ or $x_i = 0$, respectively. Since the computational paths in C do not interfere, extending soundness against classical messages, following directly from [21, Section 3.4], to quantum messages can be done by measuring the registers M and W in the computational basis at the end of the verifier's last turn. Finally, given that C has $O(\log n)$ depth, implementing the verifier's actions requires only $O(\log n)$ ancillary qubits, which is indeed achievable by a unitary verifier.

3.4 The equivalence of $\mathsf{QSZK}_{\mathrm{U}}\mathsf{L}$ and BQL

We demonstrate Theorem 4 by introducing a $\mathsf{QSZK}_{\mathrm{U}}\mathsf{L}_{\mathrm{HV}}$-complete problem:

▶ **Theorem 6** (Informal of [41, Theorem 5.3])**.** IndivProdQSD *is* $\mathsf{QSZK}_{\mathrm{U}}\mathsf{L}_{\mathrm{HV}}$*-complete.*

We begin by informally defining the promise problem Individual Product State Distinguishability, denoted by IndivProdQSD$[k(n), \alpha(n), \delta(n)]$, where the parameters satisfy $\alpha(n) - k(n) \cdot \delta(n) \geq 1/\mathrm{poly}(n)$ and $1 \leq k(n) \leq \mathrm{poly}(n)$. This problem considers two k-tuples of $O(\log n)$-qubit quantum states, denoted by $\sigma_1, \cdots, \sigma_k$ and $\sigma'_1, \cdots, \sigma'_k$, where the purifications of these states can be prepared by corresponding polynomial-size unitary quantum circuits acting on $O(\log n)$ qubits. For *yes* instances, these two k-tuples are "globally" far, satisfying

$$\mathrm{T}(\sigma_1 \otimes \cdots \otimes \sigma_k, \sigma'_1 \otimes \cdots \otimes \sigma'_k) \geq \alpha. \tag{2}$$

[13] See [41, Section 2.4] for the definition of the fingerprint of a multiset. The computation of each fingerprint requires $O(\log n)$ random bits, which can be simulated in a QIPL proof system; see Footnote 11 for details.

While for *no* instances, each pair of corresponding states in these k-tuples are close, satisfying

$$\forall j \in [k], \quad \mathrm{T}\big(\sigma_j, \sigma'_j\big) \le \delta. \tag{3}$$

Then we show that (1) the complement of IndivProdQSD, $\overline{\text{IndivProdQSD}}$, is $\mathsf{QSZK_UL_{HV}}$-hard; and (2) IndivProdQSD is in BQL, which is contained in $\mathsf{QSZK_UL_{HV}}$ by definition.

3.4.1 $\overline{\text{IndivProdQSD}}$ is $\mathsf{QSZK_UL_{HV}}$-hard

The hardness proof draws inspiration from [62, Section 5]. Consider a $\mathsf{QSZK_UL_{HV}}[2k, c, s]$ proof system, denoted by $\mathcal{B}$. The logspace-bounded simulator $S_{\mathcal{B}}$ produces good state approximations ξ_j and ξ'_j of the snapshot states $\rho_{\mathtt{M}_j\mathtt{W}_j}$ and $\rho_{\mathtt{M}'_j\mathtt{W}_j}$ after the $(2j-1)$-st turn and the $(2j)$-th turn in $\mathcal{B}$, respectively, satisfying $\xi_j \approx_\delta \rho_{\mathtt{M}_j\mathtt{W}_j}$ and $\xi'_j \approx_\delta \rho_{\mathtt{M}'_j\mathtt{W}_j}$, where $\delta_{\mathcal{B}}(n)$ is a negligible function.

Since the verifier's actions are unitary and the verifier is honest, it suffices to check that the prover's actions do not change the verifier's private register, corresponding to the type (ii) constraints Equation (1) in the SDP formulation for QIPL proof systems. For convenience, let $\sigma_j := \mathrm{Tr}_{\mathtt{M}_j}(\xi_j)$ and $\sigma'_j := \mathrm{Tr}_{\mathtt{M}'_j}(\xi'_j)$ for $j \in [k]$. We then establish $\mathsf{QSZKL_{HV}}$ hardness as follows:

- For *yes* instances, the message-wise closeness condition of the simulator $S_{\mathcal{B}}$ implies Equation (3) with $\delta(n) := 2\delta_{\mathcal{B}}(n)$.
- For *no* instances, the simulator $S_{\mathcal{B}}$ produces the snapshot state before the final measurement, which accepts with probability $c(n)$ for all instances, while the proof system accepts with probability at most $s(n)$. The inconsistency between the simulator's state approximations and the snapshot states yields Equation (2) with $\alpha(n) := (\sqrt{c} - \sqrt{s})^2/4(l-1)$.

3.4.2 IndivProdQSD $\in \mathsf{BQL}$

Since it holds that $\mathsf{BQL} = \mathsf{QMAL}$ [17, 19], it suffices to establish that IndivProdQSD $\in \mathsf{QMAL}$. By applying an averaging argument in combination with Equation (2), we derive the following:

$$\sum_{j\in[k]} \mathrm{T}\big(\sigma_j, \sigma'_j\big) \ge \mathrm{T}\big(\sigma_1 \otimes \cdots \otimes \sigma_k, \sigma'_1 \otimes \cdots \otimes \sigma'_k\big) \ge \alpha \quad \Rightarrow \quad \exists j \in [k] \text{ s.t. } \mathrm{T}\big(\sigma_j, \sigma'_j\big) \ge \frac{\alpha}{k}. \tag{4}$$

The QMAL protocol works as follows: (1) The prover sends an index $i \in [k]$ to the verifier; and (2) The verifier accepts if $\mathrm{Tr}(\sigma_i, \sigma'_i) \ge \alpha/k$ and rejects if $\mathrm{Tr}(\sigma_i, \sigma'_i) \le \delta$, in accordance with Equations (3) and (4). The resulting promise problem to be verified is precisely an instance of $\text{GapQSD}_{\text{log}}$, which is known to be BQL-complete [42].

4 Discussion and open problems

We introduce two models of space-bounded quantum interactive proof systems: QIPL and $\mathsf{QIP_UL}$. Unlike $\mathsf{BQL} = \mathsf{BQ_UL}$, we show that $\mathsf{QIP_UL} \subsetneq \mathsf{QIPL}$ unless $\mathsf{P} = \mathsf{NP}$. Our results highlight the distinctive role of (pinching) intermediate measurements in space-bounded quantum interactive proofs, setting them apart from space-bounded quantum computation. This prompts an intriguing question:

(a) What is the computational power of space-bounded quantum interactive proofs beyond $\mathsf{QIPL^{HC}}$, particularly when the high-concentration requirement for *yes* instances (the completeness condition) is removed, as in the class QIPL, or when the verifier is allowed to perform general quantum logspace computations?

A motivating example is a reversible generalization of QIPL, particularly space-bounded *isometric* quantum interactive proof systems ($\mathsf{QIPL}^{\diamond}$, see [41, Remark 3.8]), where all verifier actions are $O(\log n)$-qubit *isometric* quantum circuits. Remarkably, $\mathsf{QIPL}^{\diamond}$ at least contains QMA: Given a local Hamiltonian $H = \sum_{i=1}^{m} H_i$, we can construct a $\mathsf{QIPL}^{\diamond}$ proof system as follows:[14]

(i) The verifier chooses a local term H_i uniformly at random from the set $\{H_1, \cdots, H_m\}$.
(ii) The prover sends a ground state $|\Omega\rangle$ qubit by qubit, while the verifier sends a state $|0\rangle$ in each round and retains only the qubits associated with H_i in its private registers.
(iii) The verifier performs the POVM corresponding to the decomposition $I = H_i + (I - H_i)$.[15]

Further analysis indicates that the verifier accepts with probability $1 - m^{-1}\langle\Omega|H|\Omega\rangle$, and direct sequential repetition yields a $\mathsf{QIPL}^{\diamond}$ proof system. Additionally, it is evident that all candidate models of Question a are contained in QIP, and thus in PSPACE.

Furthermore, space-bounded *unitary* quantum interactive proofs ($\mathsf{QIP_UL}$) can simulate the classical counterparts with $O(\log n)$ public coins [21] (see Theorem 2), raising the question:

(b) Can we achieve a tighter characterization of $\mathsf{QIP_UL}$? For example, does $\mathsf{QIP_UL}$ contain space-bounded classical interactive proofs with $\omega(\log n)$ public coins, as studied in [20, 28, 11]?

Finally, for *constant*-turn space-bounded quantum interactive proofs, the three models discussed here become equivalent due to the principle of deferred measurements, contrasting with the aforementioned polynomial-turn settings. However, this equivalence does not directly extend to more general verifiers (see Footnote 8), leading to the following question:

(c) What is the computational power of constant-turn space-bounded quantum interactive proofs with a general quantum logspace verifier?

5 Related works

Variants of time-bounded quantum interactive proofs with short messages were explored in [5, 53]. Depending on the settings, these variants are as powerful as QMA or BQP.

The concept of interactive proof systems has been extended to other computational models. Quantum interactive proofs for synthesizing quantum states, known as stateQIP, were introduced in [55]. Follow-up research established the equivalence stateQIP = statePSPACE [48] and developed a parallelization technique for stateQIP [32, 54]. A Merlin-Arthur-type variant was also explored in [14, 13]. More recently, quantum interactive proofs for unitary synthesis and related problems have been studied in [6, 45]. Another interesting but less related variant is the exploration of interactive proof systems in distributed computing [40, 49], and more recently, quantum distributed interactive proof systems have been investigated [22, 43, 31].

Finally, space-bounded (classical) statistical zero-knowledge, where the verifier has *read-only (i.e., two-way) access* to (polynomial-length) messages during interactions, was studied in [15, 3, 2]. More recently, a variant where the verifier has *online (i.e., one-way) access* to messages has also been explored [12].

[14] A similar approach is used in a streaming version of QMAL (with online access to the message) in [24].
[15] See the proof of [38, Proposition 14.2] for an explicit construction of such POVMs.

References

1 Dorit Aharonov and Tomer Naveh. Quantum NP – a survey. *arXiv preprint quant-ph/0210077*, 2002. arXiv:quant-ph/0210077.

2 Eric Allender, Jacob Gray, Saachi Mutreja, Harsha Tirumala, and Pengxiang Wang. Robustness for space-bounded statistical zero knowledge. In *Proceedings of the International Workshop on Randomization and Computation*, volume 275 of *LIPIcs*, pages 56:1–56:21, 2023. ECCC:TR22-138. doi:10.4230/LIPICS.APPROX/RANDOM.2023.56.

3 Eric Allender, Shuichi Hirahara, and Harsha Tirumala. Kolmogorov complexity characterizes statistical zero knowledge. In *Proceedings of the 14th Innovations in Theoretical Computer Science Conference*, volume 251, pages 3:1–3:19, 2023. ECCC:TR22-127.

4 László Babai. Trading group theory for randomness. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985. doi:10.1145/22145.22192.

5 Salman Beigi, Peter Shor, and John Watrous. Quantum interactive proofs with short messages. *Theory of Computing*, 7(1):101–117, 2011. arXiv:1004.0411. doi:10.4086/toc.2011.v007a007.

6 John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary complexity and the Uhlmann transformation problem. *arXiv preprint*, 2023. arXiv:2306.13073.

7 Richard Cleve, Peter Høyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *19th Annual IEEE Conference on Computational Complexity (CCC 2004), 21-24 June 2004, Amherst, MA, USA*, pages 236–249. IEEE Computer Society, 2004. arXiv:quant-ph/0404076. doi:10.1109/CCC.2004.1313847.

8 Anne Condon. Space-bounded probabilistic game automata. *Journal of the ACM*, 38(2):472–494, 1991. Preliminary Version in *SCT 1988*. doi:10.1145/103516.128681.

9 Anne Condon. The complexity of space boundes interactive proof systems. In *Complexity Theory: Current Research*, pages 147–189. Cambridge University Press, 1992. URL: https://dl.acm.org/doi/10.5555/183589.183728.

10 Anne Condon and Richard Ladner. Interactive proof systems with polynomially bounded strategies. *Journal of Computer and System Sciences*, 50(3):506–518, 1995. Preliminary Version in *SCT 1992*. doi:10.1006/jcss.1995.1040.

11 Joshua Cook and Ron D. Rothblum. Efficient interactive proofs for non-deterministic bounded space. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2023)*, volume 275 of *LIPIcs*, pages 47:1–47:22. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. ECCC:TR23-097. doi:10.4230/LIPIcs.APPROX/RANDOM.2023.47.

12 Graham Cormode, Marcel de Sena Dall'Agnol, Tom Gur, and Chris Hickey. Streaming zero-knowledge proofs. In *Proceedings of the 39th Computational Complexity Conference*, volume 300 of *LIPIcs*, pages 2:1–2:66. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. arXiv:2301.02161. doi:10.4230/LIPICS.CCC.2024.2.

13 Hugo Delavenne and François Le Gall. Quantum state synthesis: Relation with decision complexity classes and impossibility of synthesis error reduction. *Quantum Information and Computation*, 24(9-10):754–765, 2024. arXiv:2407.02907. doi:10.26421/qic24.9-10-3.

14 Hugo Delavenne, François Le Gall, Yupan Liu, and Masayuki Miyamoto. Quantum Merlin-Arthur proof systems for synthesizing quantum states. *Quantum*, 9:1688, 2025. arXiv:2303.01877. doi:10.22331/q-2025-04-03-1688.

15 Zeev Dvir, Dan Gutfreund, Guy N. Rothblum, and Salil P. Vadhan. On approximating the entropy of polynomial mappings. In *Proceedings of Second Symposium on Innovations in Computer Science*, pages 460–475, 2011. URL: https://conference.iiis.tsinghua.edu.cn/ICS2011/content/papers/28.html.

16 Cynthia Dwork and Larry Stockmeyer. Finite state verifiers I: The power of interaction. *Journal of the ACM*, 39(4):800–828, 1992. Preliminary Version in *FOCS 1989*. doi:10.1145/146585.146599.

17 Bill Fefferman, Hirotada Kobayashi, Cedric Yen-Yu Lin, Tomoyuki Morimae, and Harumichi Nishimura. Space-efficient error reduction for unitary quantum computations. In *Proceedings of the 43rd International Colloquium on Automata, Languages, and Programming*, volume 55 of *LIPIcs*, page 14, 2016. arXiv:1604.08192. doi:10.4230/LIPIcs.ICALP.2016.14.

18 Bill Fefferman and Cedric Yen-Yu Lin. A complete characterization of unitary quantum space. In *Proceedings of the 9th Innovations in Theoretical Computer Science Conference*, volume 94 of *LIPIcs*, page 4, 2018. arXiv:1604.01384. doi:10.4230/LIPIcs.ITCS.2018.4.

19 Bill Fefferman and Zachary Remscrim. Eliminating intermediate measurements in space-bounded quantum computation. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1343–1356, 2021. arXiv:2006.03530. doi:10.1145/3406325.3451051.

20 Lance Fortnow and Carsten Lund. Interactive proof systems and alternating time—space complexity. *Theoretical Computer Science*, 113(1):55–73, 1993. Preliminary Version in *STACS 1991*. doi:10.1016/0304-3975(93)90210-K.

21 Lance J. Fortnow. *Complexity-Theoretic Aspects of Interactive Proof Systems*. PhD thesis, Massachusetts Institute of Technology, 1989. URL: https://lance.fortnow.com/papers/files/thesis.pdf.

22 Pierre Fraigniaud, Ami Paz, François Le Gall, and Harumichi Nishimura. Distributed quantum proofs for replicated data. In *Proceedings of the 12th Innovations in Theoretical Computer Science Conference*, volume 185 of *LIPIcs*, pages 28:1–28:20, 2021. arXiv:2002.10018. doi:10.4230/LIPIcs.ITCS.2021.28.

23 Bernd Gärtner and Jiří Matoušek. *Approximation Algorithms and Semidefinite Programming*. Springer Berlin Heidelberg, 1st edition, 2012. doi:10.1007/978-3-642-22015-9_2.

24 Sevag Gharibian and Dorian Rudolph. Quantum space, ground space traversal, and how to embed multi-prover interactive proofs into unentanglement. In *Proceedings of the 14th Innovations in Theoretical Computer Science*, volume 251 of *LIPIcs*, pages 53:1–53:23, 2023. arXiv:2206.05243. doi:10.4230/LIPICS.ITCS.2023.53.

25 Uma Girish and Ran Raz. Eliminating intermediate measurements using pseudorandom generators. In *Proceedings of the 13th Innovations in Theoretical Computer Science Conference*, volume 215 of *LIPIcs*, pages 76:1–76:18, 2022. arXiv:2106.11877. doi:10.4230/LIPIcs.ITCS.2022.76.

26 Uma Girish, Ran Raz, and Wei Zhan. Quantum logspace algorithm for powering matrices with bounded norm. In *Proceedings of the 48th International Colloquium on Automata, Languages, and Programming*, volume 198 of *LIPIcs*, pages 73:1–73:20, 2021. arXiv:2006.04880. doi:10.4230/LIPIcs.ICALP.2021.73.

27 Uma Girish, Ran Raz, and Wei Zhan. Quantum logspace computations are verifiable. In *Proceedings of the 2024 Symposium on Simplicity in Algorithms*, pages 144–150, 2024. arXiv:2307.11083. doi:10.1137/1.9781611977936.14.

28 Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. Delegating computation: interactive proofs for muggles. *Journal of the ACM (JACM)*, 62(4):1–64, 2015. Preliminary Version in *STOC 2008*. ECCC:TR17-108. doi:10.1145/2699436.

29 Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989. Preliminary Version in *STOC 1985*. doi:10.1137/0218012.

30 Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pages 59–68, 1986. doi:10.1145/12130.12137.

31 Atsuya Hasegawa, Srijita Kundu, and Harumichi Nishimura. On the power of quantum distributed proofs. In *Proceedings of the 43rd ACM Symposium on Principles of Distributed Computing*, pages 220–230, 2024. arXiv:2403.14108. doi:10.1145/3662158.3662788.

32 Sandy Irani, Anand Natarajan, Chinmay Nirkhe, Sujit Rao, and Henry Yuen. Quantum search-to-decision reductions and the state synthesis problem. In *Proceedings of the 37th*

Computational Complexity Conference, pages 1–19, 2022. arXiv:2111.02999. doi:10.4230/LIPIcs.CCC.2022.5.

33 Tsuyoshi Ito, Hirotada Kobayashi, and John Watrous. Quantum interactive proofs with weak error bounds. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pages 266–275, 2012. arXiv:1012.4427. doi:10.1145/2090236.2090259.

34 Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for NEXP sound against entangled provers. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 243–252. IEEE Computer Society, 2012. arXiv:1207.0550. doi:10.1109/FOCS.2012.11.

35 Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. *Journal of the ACM*, 58(6):1–27, 2011. Preliminary Version in *STOC 2010*. arXiv:0907.4737. doi:10.1145/2049697.2049704.

36 Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, and Thomas Vidick. Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18:273–307, 2009. Preliminary Version in *CCC 2008*. arXiv:0711.3715. doi:10.1007/s00037-009-0275-3.

37 Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 608–617, 2000. doi:10.1145/335305.335387.

38 Alexei Y. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 1st edition, 2002. doi:10.1090/gsm/047/10.

39 Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Generalized quantum Arthur–Merlin games. *SIAM Journal on Computing*, 48(3):865–902, 2019. Preliminary Version in *CCC 2015*. arXiv:1312.4673. doi:10.1137/17M1160173.

40 Gillat Kol, Rotem Oshman, and Raghuvansh R Saxena. Interactive distributed proofs. In *Proceedings of the 37th ACM Symposium on Principles of Distributed Computing*, pages 255–264, 2018. doi:10.1145/3212734.3212771.

41 François Le Gall, Yupan Liu, Harumichi Nishimura, and Qisheng Wang. Space-bounded quantum interactive proof systems. *arXiv preprint arXiv:2410.23958v3*, 2024. arXiv:2410.23958v3. doi:10.48550/arXiv.2410.23958.

42 François Le Gall, Yupan Liu, and Qisheng Wang. Space-bounded quantum state testing via space-efficient quantum singular value transformation. *arXiv preprint arXiv:2308.05079*, 2023. arXiv:2308.05079. doi:10.48550/arXiv.2308.05079.

43 François Le Gall, Masayuki Miyamoto, and Harumichi Nishimura. Distributed quantum interactive proofs. In *Proceedings of the 40th International Symposium on Theoretical Aspects of Computer Science*, volume 254 of *LIPIcs*, pages 42:1–42:21, 2023. arXiv:2210.01390. doi:10.4230/LIPIcs.STACS.2023.42.

44 Richard J. Lipton. Efficient checking of computations. In *Proceedings of the 7th Annual Symposium on Theoretical Aspects of Computer Science*, volume 415 of *Lecture Notes in Computer Science*, pages 207–215. Springer, 1990. doi:10.1007/3-540-52282-4_44.

45 Alex Lombardi, Fermi Ma, and John Wright. A one-query lower bound for unitary synthesis and breaking quantum cryptography. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 979–990, 2024. arXiv:2310.08870. doi:10.1145/3618260.3649650.

46 Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992. Preliminary Version in *FOCS 1990*. doi:10.1145/146585.146605.

47 Chris Marriott and John Watrous. Quantum Arthur–Merlin games. *Computational Complexity*, 14(2):122–152, 2005. Preliminary Version in *CCC 2004*. arXiv:cs/0506068. doi:10.1007/s00037-005-0194-x.

48 Tony Metger and Henry Yuen. stateQIP = statePSPACE. In *Proceedings of the 64th Annual IEEE Symposium on Foundations of Computer Science*, pages 1349–1356. IEEE, 2023. arXiv:2301.07730. doi:10.1109/FOCS57990.2023.00082.

49 Moni Naor, Merav Parter, and Eylon Yogev. The power of distributed verifiers in interactive proofs. In *Proceedings of the 31st Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1096–115. SIAM, 2020. arXiv:1812.10917. doi:10.1137/1.9781611975994.67.

50 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 10th anniversary edition, 2010. doi:10.1017/CBO9780511976667.

51 Harumichi Nishimura and Tomoyuki Yamakami. An application of quantum finite automata to interactive proof systems. *Journal of Computer and System Sciences*, 75(4):255–269, 2009. Preliminary Version in *CIAA 2004*. arXiv:quant-ph/0410040. doi:10.1016/j.jcss.2008.12.001.

52 Harumichi Nishimura and Tomoyuki Yamakami. Interactive proofs with quantum finite automata. *Theoretical Computer Science*, 568:1–18, 2015. arXiv:1401.2929. doi:10.1016/j.tcs.2014.11.030.

53 Attila Pereszlényi. On quantum interactive proofs with short messages. *Chicago Journal of Theoretical Computer Science*, 2012(9):1–10, 2012. arXiv:1109.0964. doi:10.4086/cjtcs.2012.009.

54 Gregory Rosenthal. Efficient quantum state synthesis with one query. In *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2508–2534, 2024. arXiv:2306.01723. doi:10.1137/1.9781611977912.89.

55 Gregory Rosenthal and Henry Yuen. Interactive proofs for synthesizing quantum states and unitaries. In *Proceedings of the 13th Innovations in Theoretical Computer Science Conference*, volume 215, pages 112:1–112:4, 2022. arXiv:2108.07192. doi:10.4230/LIPIcs.ITCS.2022.112.

56 Adi Shamir. $\mathsf{IP} = \mathsf{PSPACE}$. *Journal of the ACM*, 39(4):869–877, 1992. Preliminary Version in *FOCS 1990*. doi:10.1145/146585.146609.

57 Amnon Ta-Shma. Inverting well conditioned matrices in quantum logspace. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 881–890, 2013. doi:10.1145/2488608.2488720.

58 Salil P Vadhan. *A study of statistical zero-knowledge proofs*. PhD thesis, Massachusetts Institute of Technology, 1999. URL: http://hdl.handle.net/1721.1/85349.

59 Hari Venkateswaran. Properties that characterize LOGCFL. *Journal of Computer and System Sciences*, 43(2):380–404, 1991. Preliminary Version in *STOC 1987*. doi:10.1016/0022-0000(91)90020-6.

60 Thomas Vidick and John Watrous. Quantum proofs. *Foundations and Trends® in Theoretical Computer Science*, 11(1-2):1–215, 2016. arXiv:1610.01664. doi:10.1561/0400000068.

61 John Watrous. Space-bounded quantum complexity. *Journal of Computer and System Sciences*, 59(2):281–326, 1999. Preliminary Version in *CCC 1998*. doi:10.1006/jcss.1999.1655.

62 John Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 459–468, 2002. arXiv:quant-ph/0202111. doi:10.1109/SFCS.2002.1181970.

63 John Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003. Preliminary Version in *FOCS 1999*. arXiv:cs/9901015. doi:10.1016/S0304-3975(01)00375-9.

64 John Watrous. On the complexity of simulating space-bounded quantum computations. *Computational Complexity*, 12:48–84, 2003. Preliminary Version in *FOCS 1999*. arXiv:cs/9911008. doi:10.1007/s00037-003-0177-8.

65 John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009. Preliminary Version in *STOC 2006*. arXiv:quant-ph/0511020. doi:10.1137/060670997.

66 John Watrous. Semidefinite programs for interactive proofs (Tutorial at the 19th Conference on Quantum Information Processing, QIP 2016). https://qipconference.org/2016/qip-sdp-handout.pdf, 2016. Accessed: 2024-09-18.

67 Abuzer Yakaryılmaz. Public qubits versus private coins. In *Proceedings of Workshop on Quantum and Classical Complexity*, pages 45–60, 2013. ECCC:TR12-130.

68 Mark Zhandry. The space-time cost of purifying quantum computations. In *Proceedings of the 15th Innovations in Theoretical Computer Science Conference*, volume 287 of *LIPIcs*, pages 102:1–102:22, 2024. arXiv:2401.07974. doi:10.4230/LIPIcs.ITCS.2024.102.