

# Space-bounded quantum interactive proof systems

François Le Gall<sup>\*1</sup>, Yupan Liu<sup>†1</sup>, Harumichi Nishimura<sup>‡2</sup>, and Qisheng Wang<sup>§3,1</sup>

<sup>1</sup>Graduate School of Mathematics, Nagoya University

<sup>2</sup>Graduate School of Informatics, Nagoya University

<sup>3</sup>School of Informatics, University of Edinburgh

## Abstract

We introduce two models of space-bounded quantum interactive proof systems, QIPL and QIP<sub>UL</sub>. The QIP<sub>UL</sub> 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 QIP<sub>UL</sub>. When the message number  $m$  is polynomially bounded, QIP<sub>UL</sub>  $\not\subseteq$  QIPL unless  $P = NP$ :

- QIPL contains NP and is contained in SBP, which is a subclass of AM.
- QIP<sub>UL</sub> is contained in P and contains  $SAC^1 \cup BQL$ , 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  $BQL = BQ_{UL}$ .

We also introduce space-bounded unitary quantum statistical zero-knowledge (QSZK<sub>UL</sub>), a specific form of QIP<sub>UL</sub> 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 QSZK<sub>UL</sub> = BQL, implying that the statistical zero-knowledge property negates the computational advantage typically gained from the interaction.

---

\*Email: [legall@math.nagoya-u.ac.jp](mailto:legall@math.nagoya-u.ac.jp)

†Email: [yupan.liu.e6@math.nagoya-u.ac.jp](mailto:yupan.liu.e6@math.nagoya-u.ac.jp)

‡Email: [hnishimura@i.nagoya-u.ac.jp](mailto:hnishimura@i.nagoya-u.ac.jp)

§Email: [QishengWang1994@gmail.com](mailto:QishengWang1994@gmail.com)

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Main results . . . . .	2
1.2	Proof techniques . . . . .	5
1.2.1	Basic properties for QIPL and QIP <sub>UL</sub> . . . . .	5
1.2.2	Upper bounds for QIPL and QIP <sub>UL</sub> . . . . .	7
1.2.3	Lower bounds for QIPL and QIP <sub>UL</sub> . . . . .	8
1.2.4	The equivalence of QSZK <sub>UL</sub> and BQL . . . . .	9
1.3	Discussion and open problems . . . . .	10
1.4	Related works . . . . .	10
<b>2</b>	<b>Preliminaries</b>	<b>11</b>
2.1	Distance-like measures for quantum states . . . . .	11
2.2	Space-bounded quantum computation . . . . .	12
2.3	Space-bounded quantum state testing . . . . .	13
2.4	Classical concepts, tools, and complexity classes . . . . .	14
<b>3</b>	<b>Space-bounded (unitary) quantum interactive proofs</b>	<b>15</b>
3.1	Definitions of space-bounded quantum interactive proof systems . . . . .	17
3.2	Basic properties: Error reduction and perfect completeness . . . . .	19
3.2.1	Achieving perfect completeness for QIPL and QIP <sub>UL</sub> . . . . .	20
3.2.2	Error reduction for QIPL and QIP <sub>UL</sub> . . . . .	21
3.3	A upper bound for QIPL . . . . .	22
3.3.1	Semi-definite program formulations for QIPL proof systems . . . . .	23
3.3.2	QIPL is in SBP . . . . .	27
3.4	Lower bounds for QIPL and QIP <sub>UL</sub> . . . . .	28
3.4.1	NP is in QIPL . . . . .	28
3.4.2	SAC <sup>1</sup> ∪ BQL is in QIP <sub>UL</sub> . . . . .	30
<b>4</b>	<b>Constant-message space-bounded quantum interactive proofs</b>	<b>31</b>
4.1	Error reduction for QIPL <sub>O(1)</sub> via parallel repetition . . . . .	32
4.2	Parallelization via the turn-halving lemma . . . . .	33
4.2.1	Proof of the turn-halving lemma . . . . .	34
4.3	Weakness of QIPL <sub>O(1)</sub> with weak error bounds . . . . .	36
4.4	Weakness of QIPL <sub>O(1)</sub> : QMAML and NC containment . . . . .	37
<b>5</b>	<b>Space-bounded unitary quantum statistical zero-knowledge</b>	<b>38</b>
5.1	Definition of space-bounded unitary quantum statistical zero-knowledge . . . . .	39
5.2	$\overline{\text{INDIVPRODQSD}}$ is QSZK <sub>ULHV</sub> -hard . . . . .	40
5.3	QSZK <sub>ULHV</sub> is in BQL . . . . .	42

# 1 Introduction

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  $\text{poly}(n)$  elementary gates [Wat99, Wat03b]. 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 [TS13, FL18], which saturates the classical simulation bound. In recent years, this area has gained increased attention, particularly in eliminating (pinching) intermediate measurements in these models [FR21, GRZ21], and through further developments [GR22, Zha24]. 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  $(\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$ , 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  $x \in \mathcal{I}_{\text{yes}} \cup \mathcal{I}_{\text{no}}$ , the prover claims that  $x \in \mathcal{I}_{\text{yes}}$ , 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  $\mathcal{I}_{\text{yes}}$  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  $\mathcal{I}_{\text{no}}$  then the verifier accepts with probability at most  $s$ , regardless of whether the prover follows the protocol. Typically, an interactive protocol for  $(\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$  has completeness  $c = 2/3$  and soundness  $s = 1/3$ .

**Interactive proof systems with time-bounded verifier.** The exploration of classical interactive proof systems (IP) was initiated in the 1980s [Bab85, GMR89]. In these proof systems, the verifier is typically bounded by polynomial time, and  $\text{IP}[m]$  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* [Bab85]. 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  $\text{IP}[O(1)]$  is contained in the second level of the polynomial-time hierarchy [Bab85, GS86]. However, IP protocols with a polynomial number of messages have been shown to be exceptionally powerful, as demonstrated by the seminal result  $\text{IP} = \text{PSPACE}$  [LFKN92, Sha92]. 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.<sup>1</sup>

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 [Wat03a]. Remarkably, any QIP protocol with a polynomial number of messages can be parallelized to three messages [KW00]. A quantum Arthur-Merlin proof system was subsequently introduced in [MW05], 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  $\text{QIP} = \text{PSPACE}$  [JJUW11] 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 [IKW12]. In the late 2010s, another quantum counterpart of the Arthur-Merlin proof system was considered in [KLG19], 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.

---

<sup>1</sup>The assumption that the polynomial-time hierarchy does not collapse generalizes the conjecture that  $\text{P} \subsetneq \text{NP}$ .

**Interactive proof systems with space-bounded verifier.** The investigation of (classical) interactive proof systems with space-bounded verifiers started in the late 1980s [DS92, Con91], alongside research on time-bounded verifiers. Notably, by using the fingerprinting lemma [Lip90], Condon and Ladner [CL95] 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 [For89, FL93, Con92]. By around 2010, it was established that such space-bounded protocols with  $\text{poly}(n)$  public coins precisely characterize P [GKR15].

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  $\text{poly}(n)$ -bit message, the proof system exactly characterizes NP [Lip90]. 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 [GRZ24].

Although research has been conducted on quantum interactive proofs where the verifier uses quantum finite automata [NY09, NY15, Yak13], analogous to classical work [DS92], to our knowledge no prior work has addressed space-bounded counterparts of quantum interactive proofs that align with the circuit-based model defined in [KW00, Wat03a]. 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 [FKL<sup>+</sup>16, FR21]. However, when the (unitary) verifier has online access to a  $\text{poly}(n)$ -qubit message, where each qubit in the message state is read-once, this variant is as strong as QMA [GR23].<sup>2</sup>

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.

## 1.1 Main results

**Definitions of QIPL and QIP<sub>UL</sub>.** We introduce *space-bounded quantum interactive proof systems* and their unitary variant, denoted as QIPL and QIP<sub>UL</sub>, 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.<sup>3</sup>

The verifier  $V$  maps an input  $x \in \mathcal{I}_{\text{yes}} \cup \mathcal{I}_{\text{no}}$  to a sequence  $(V_1, \dots, V_{l+1})$ , 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 QIP<sub>UL</sub> 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  $\tilde{V}_j$  that includes  $O(\log n)$  *pinching* intermediate measurements in the computational basis. Each such measurement maps a single-qubit state  $\rho$  to  $\sum_{b \in \{0,1\}} \text{Tr}(|b\rangle\langle b|\rho)|b\rangle\langle b|$ .<sup>4</sup> 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

<sup>2</sup>An exponentially up-scaled quantum counterpart of the space-bounded Merlin-Arthur-type proof system from [Lip90], with *classical* messages, was also considered in [GR23]. The variant with *unitary* quantum *polynomial*-space verifier, implicitly allowing  $\text{poly}(n)$  random bits, precisely corresponds to NEXP.

<sup>3</sup>Our definitions of QIPL and QIP<sub>UL</sub> can be straightforwardly extended to the corresponding proof systems with an odd number of messages, as shown in Figure 4.1.

<sup>4</sup>Pinching intermediate measurements naturally arise in space-bounded quantum computation, particularly in recent developments on eliminating intermediate measurements in quantum logspace [GRZ21, GR22]. In this context, the quantum channels that capture the space-bounded computation are *unital* in the case of qubits.

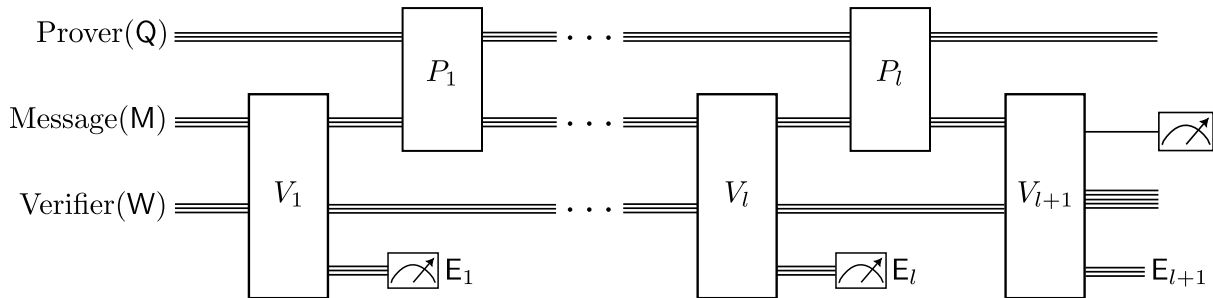


Figure 1.1: A  $2l$ -turn single-prover space-bounded quantum interactive proof system (QIPL), where each environment register  $E_j$  is introduced by applying the principle of deferred measurements to an almost-unitary quantum circuit  $\tilde{V}_j$ , resulting in the isometric quantum circuit  $V_j$ .

apply the principle of deferred measurements (e.g., [NC10, Section 4.4]), transforming the circuit  $\tilde{V}_j$  into an *isometric* quantum circuit  $V_j$  with a newly introduced environment register  $E_j$ ,<sup>5</sup> which is measured at the end of that turn, with the measurement outcome denoted by  $u_j$ , as illustrated in Figure 1.1. 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  $\text{QIP}_{\text{UL}}$  proof systems, each  $V_j$  is a unitary quantum circuit.

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  $(V_1, \dots, V_{l+1})$  must be computable by a single deterministic logspace Turing machine.<sup>6</sup>

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

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

In *constant*-turn scenarios, it is crucial to emphasize that the proof systems  $\text{QIPL}_{O(1)}[c, s]$  and  $\text{QIP}_{\text{UL}O(1)}[c, s]$  can directly simulate each other, as the environment registers  $E_1, \dots, E_{O(1)}$  collectively holds  $O(\log n)$  qubits.<sup>7</sup> Therefore, for simplicity, we define  $\text{QIPL}_{O(1)}[c, s]$  proof systems in which the verifier’s actions are implemented by *unitary* quantum circuits.

**Space-bounded (unitary) quantum interactive proofs.** Our first theorem serves as a quantum analog of the classical work by Condon and Ladner [CL95], where SBP is a subclass of AM and collapses to NP under reasonable derandomization assumptions [KvM02, MV05]:<sup>8</sup>

**Theorem 1.1** (Informal of Theorem 3.1).  $\text{NP} \subseteq \text{QIPL} \subseteq \text{SBP}$ .

<sup>5</sup>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 Definition 2.8.

<sup>6</sup>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.

<sup>7</sup>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  $\text{poly}(n)$  pinching intermediate measurements might increase the proof system’s power beyond the unitary case. This is because current techniques for proving results such as  $\text{BQL} = \text{BQ}_{\text{UL}}$  [FR21, GRZ21, GR22] do not directly apply in this context.

<sup>8</sup>For further details on the computational power of SBP and related complexity classes, see Section 2.4.

Interestingly, Theorem 1.1 suggests that the QIPL model can be viewed as the *weakest yet natural* model that encompasses space-bounded (private-coin) classical interactive proofs, as considered in [CL95]. Our definition of QIPL aims to introduce a quantum counterpart that includes 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  $\text{MIP} \subseteq \text{MIP}^*$ ) for nearly a decade [CHTW04, IV12], while in the single-prover settings (e.g., proving  $\text{IP} \subseteq \text{QIP}$ ), it is typically resolved by measuring the prover’s quantum messages and treating the outcomes as classical messages (e.g., [AN02, Claim 1]).

However, space-bounded *unitary* quantum interactive proofs ( $\text{QIP}_{\text{UL}}$ ), which denote the most natural space-bounded counterpart to quantum interactive proofs as defined in [KW00, Wat03b], do not directly achieve the stated soundness guarantee. Hence,  $\text{QIP}_{\text{UL}}$  may be computationally weaker than QIPL. Our second theorem characterizes the computational power of  $\text{QIP}_{\text{UL}}$ :

**Theorem 1.2** (Informal of Theorem 3.4 and Theorem 4.2). *The following holds:*

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

Theorems 1.1 and 1.2 suggest that  $\text{QIP}_{\text{UL}}$  is indeed *weaker* than QIPL unless  $\text{P} = \text{NP}$ . 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  $\text{SAC}^1$  is equivalent to LOGCFL [Ven91], which contains NL and is contained in  $\text{AC}^1$ .<sup>9</sup> Our third theorem, meanwhile, focuses on space-bounded quantum interactive proof systems with a constant number of messages:

**Theorem 1.3** (Informal of Theorem 4.3). *For any  $c(n) - s(n) \geq \Omega(1)$ ,  $\text{QIPL}_{O(1)}[c, s] \subseteq \text{NC}$ .*

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  $\text{QIP}_{\text{UL}}$ , 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 [Bab85, GS86], whereas the class of proof systems with  $m = \text{poly}(n)$  (the regime of the second and third rows in Table 1) exactly characterizes PSPACE [LFKN92, Sha92].
- For (time-bounded) quantum interactive proofs, all proof systems with parameters listed in Table 1 precisely capture PSPACE [Wat03a, KW00, JJUW11].

	Models	Constant gap $c(n) - s(n) \geq \Omega(1)$	Polynomial small gap $c(n) - s(n) \geq 1/\text{poly}(n)$
The number of messages: $m(n) = \text{poly}(n)$	QIPL	contains NP & in SBP Theorem 1.1	contains NP & in SBP Theorem 1.1
The number of messages: $m(n) = \text{poly}(n)$	$\text{QIP}_{\text{UL}}$	contains $\text{SAC}^1 \cup \text{BQL}$ & in P Theorem 1.2	contains $\text{SAC}^1 \cup \text{BQL}$ & in P Theorem 1.2
The number of messages: $3 \leq m(n) \leq O(1)$	QIPL & $\text{QIP}_{\text{UL}}$	in NC Theorem 1.3	contains $\text{SAC}^1 \cup \text{BQL}$ & in P Theorem 1.2

Table 1: The computational power of QIPL and  $\text{QIP}_{\text{UL}}$  with different parameters.

The central intuition underlying Table 1 is that *parallelization* [KW00, KKMV09], perhaps the most striking complexity-theoretic property of QIP proof systems, distinguishes  $\text{QIP}_{\text{UL}}$  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

<sup>9</sup>For more details on the computational power of  $\text{SAC}^1$  and related complexity classes, see Section 2.4.



in  $\mathcal{P}$ . In  $\text{QIP}_{\text{UL}}$ , the verifier’s actions are *reversible* and *dimension-preserving*, allowing direct application of parallelization techniques from [KKMV09]. In contrast,  $\text{QIPL}$  and its reversible generalization lack dimension preservation, requiring significantly more than  $O(\log n)$  space to parallelize the verifier’s actions, which prevents parallelization.

**Space-bounded unitary quantum statistical zero-knowledge.** We also introduce (*honest-verifier*) *space-bounded unitary quantum statistical zero-knowledge*, denoted as  $\text{QSZK}_{\text{ULHV}}$ . 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  $\mathcal{M}$  and  $\mathcal{W}$  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  $\text{QSZK}_{\text{ULHV}}$  serves as a space-bounded variant of honest-verifier (unitary) quantum statistical zero-knowledge, denoted by  $\text{QSZK}_{\text{HV}}$ , as introduced in [Wat02]. Our fourth theorem establishes that the statistical zero-knowledge property completely negates the computational advantage typically gained through the interaction:

**Theorem 1.4** (Informal of Theorem 5.2).  $\text{QSZK}_{\text{UL}} = \text{QSZK}_{\text{ULHV}} = \text{BQL}$ .

In addition to  $\text{QSZK}_{\text{ULHV}}$ , we can define  $\text{QSZK}_{\text{UL}}$  in line with [Wat09b], particularly considering space-bounded unitary quantum statistical zero-knowledge against *any verifier* (rather than an honest verifier). Following this definition,  $\text{BQL} \subseteq \text{QSZK}_{\text{UL}} \subseteq \text{QSZK}_{\text{ULHV}}$ . Interestingly, Theorem 1.4 serves as a direct space-bounded counterpart to  $\text{QSZK} = \text{QSZK}_{\text{HV}}$  [Wat09b].

The intuition behind Theorem 1.4 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 [MY23, Section 7]. In space-bounded scenarios, space-efficient quantum singular value transformation [LGLW23] 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 [Vad99] and [VW16, Chapter 5].

## 1.2 Proof techniques

Our proof techniques are mostly inspired by established methods for standard quantum interactive proofs, while the nature of  $\text{QIPL}$  and  $\text{QIP}_{\text{UL}}$  necessitates certain adaptations of these techniques. We will highlight the challenges that arise and briefly explain how we address them.

### 1.2.1 Basic properties for $\text{QIPL}$ and $\text{QIP}_{\text{UL}}$

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 1.5** (Properties for  $\text{QIPL}$  and  $\text{QIP}_{\text{UL}}$ , informal of Theorem 3.3 and Lemma 4.5). *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, it holds that:*

- (1) **Closure under perfect completeness.**

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

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

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

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

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

Achieving perfect completeness for QIPL and  $\text{QIP}_{\text{UL}}$  proof systems, particularly Theorem 1.5(1), can be adapted from the techniques used in QIP proof systems [VW16, Section 4.2.1] (or [KW00, Section 3]) by adding two additional turns. However, there are important subtleties to consider when establishing the other properties in Theorem 1.5.

**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  $\text{QIP}_{\text{UL}}$  when the gap  $c - s$  is polynomially small, regardless of the number of messages.<sup>10</sup> 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  $\text{QIP}_{\text{UL}}$  proof systems because the (almost-)unitary quantum logspace verifier cannot achieve this on its own.

To establish Theorem 1.5(2), 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.

**Parallelization and strict uniformity condition for the verifier’s mapping.** The original parallelization technique proposed in [KW00, Section 4] applies only to  $\text{QIP}_{\text{UL}}$  (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  $m = \omega(1)$ .

To overcome this issue, we adapt the technique from [KKMV09, 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  $\text{QIP}_{\text{UL}}$  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 1.5(3).

Next, we establish Theorem 1.2 by applying the turn-halving lemma  $O(\log n)$  times.<sup>11</sup> Specifically, any  $\text{QIP}_{\text{UL}}$  proof system with a polynomial number of messages can be parallelized to three messages,<sup>12</sup> 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  $\text{QIP}_{\text{UL}}$ . In addition, to prove Theorem 1.3, we adopt a similar approach to that used for QIP, particularly  $\text{QIP}[3] \subseteq \text{QMAM}$  [MW05], which inspired the turn-halving lemma [KKMV09, Section 4], and an exponentially down-scaling version of the work [JJUW11].

<sup>10</sup>Still, error reduction via parallel repetition works for QIPL when the gap  $c - s \geq \Omega(1)$ ; see Lemma 4.4.

<sup>11</sup>An operation based on  $r$  random bits can be simulated by a corresponding unitary controlled by the state  $|+\rangle^{\otimes r}$ , where  $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ . 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  $\text{QIP}_{\text{UL}}$ .

<sup>12</sup>Although the turn-halving lemma does not directly apply to QIPL proof systems, a similar reasoning works for its reversible generalization  $\text{QIPL}^\circ$ , reducing a constant number of messages to three.



### 1.2.2 Upper bounds for QIPL and QIP<sub>UL</sub>

$\text{QIPL}_{O(1)} \subseteq P$ . We prove this inclusion using a semi-definite program (SDP) for a given  $\text{QIPL}_{O(1)}$  proof system, adapted from the SDP formulation for QIP in [VW16, Wat16a]. Together with the turn-halving lemma, specifically Theorem 1.5(3), this inclusion implies that  $\text{QIP}_{UL} \subseteq P$ .

Consider a  $(2l)$ -turn  $\text{QIPL}_{O(1)}$  proof system  $P \rightleftharpoons V$ , where  $l \leq O(1)$ . Let  $\rho_{M_j W_j}$  and  $\rho'_{M'_j W'_j}$ , 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 Figure 3.1. The variables in this SDP correspond to these snapshot states after each prover's action, particularly  $\rho'_{M'_j W'_j}$  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  $W$ :

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

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

$$\text{Tr}_{M_j}(\rho_{M_j W_j}) = \text{Tr}_{M'_j}(\rho'_{M'_j W'_j}) \text{ for } j \in [l]. \quad (1.1)$$

Since the variables in this SDP collectively hold  $O(\log n)$  qubits, a standard SDP solver (e.g., [GM12]) provides a deterministic polynomial-time algorithm for approximately solving it.

$\text{QIPL} \subseteq \text{SBP}$ . To establish this inclusion, we approximate the maximum acceptance probability  $\omega(V)$  by reducing it to an instance of the *existential* variant of the SET SIZE ESTIMATION PROBLEM (SSE), since Existential SSE is in SBP [BGM06, Wat16b]. More precisely, using error reduction for QIPL (Theorem 1.5(2)), it suffices to construct a set  $S$  along with an efficiently verifiable membership oracle  $\mathcal{O}_S$ , which operates using a witness string  $w_S$ . This construction ensures that the set size  $|S|$  is large when  $\omega(V) = 1$  but remains small when  $\omega(V) \leq 1/4$ .

A key ingredient in our approach relies on extending the above SDP formulation to  $l$ -round QIPL proof systems, where the verifier's  $j$ -th action  $V_j$  is an *almost-unitary* quantum circuit that allows  $O(\log n)$  pinching intermediate measurements. We treat  $V_j$  as an isometric quantum circuit, introducing a new environment register  $E_j$  that is measured at the end of the turn, with the outcome denoted by  $u_j$ .

Note that  $\omega(V)|^u$  denotes the contribution of the measurement outcomes  $u = (u_1, \dots, u_l)$  to the maximum acceptance probability  $\omega(V)$ . Since  $\omega(V)$  can be expressed as a sum over all  $\omega(V)|^u$  and pinching intermediate measurements eliminate coherence between subspaces corresponding to different measurement outcomes, it suffices to focus on a specific measurement outcome  $u$  and the *unnormalized* snapshot states  $\rho_{M_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}$  after measuring  $E_j$  in this SDP formulation. Building on the SDP formulation of  $\text{QIPL}_{O(1)}$  proof systems, we obtain a family of SDP programs depending on the measurement outcomes  $\{u\}$ . Given a specific  $u$ , the SDP program includes two types of constraints:

- (i')  $\rho_{M_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j} = (I_{M_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}) V_j \rho'_{M'_{j-1} W'_{j-1}} V_j^\dagger$  for  $j \in \{2, \dots, l\}$ , and

$$\rho_{M_1 W_1} \otimes |u_1\rangle\langle u_1|_{E_1} = (I_{M_1 W_1} \otimes |u_1\rangle\langle u_1|_{E_1}) V_1 |\bar{0}\rangle\langle\bar{0}|_{MW} V_1^\dagger.$$

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

Next, we explain the SBP containment. The set  $S$  consists of tuples  $(u, \iota_1, \dots, \iota_{2\ell_{\text{tot}}})$ , where  $\ell_{\text{tot}}$  denotes the total length of the measurement outcomes and each  $\iota_j \in \{0, 1\}$  for  $1 \leq j \leq 2\ell_{\text{tot}}$ , such that the size  $|S|$  is approximately proportional to  $\omega(V)$ . The witness string  $w_S$  encodes a feasible solution  $(\rho'_{M'_1 W'_1}, \dots, \rho'_{M'_l W'_l})$  to the SDP program associated with  $u$ . This solution can be represented by  $l$  square matrices of dimension  $\text{poly}(n)$ , thus having polynomial size. The membership oracle  $\mathcal{O}_S(u, \iota_1, \dots, \iota_{2\ell_{\text{tot}}}, w_S)$  involves checking (1) whether the solution encoded in

$w_S$  satisfies these SDP constraints determined by  $u$ ; (2) whether the estimate  $\widehat{\omega}(V)|^u$  satisfies  $\widehat{\omega}(V)|^u > 0$  and  $\widehat{\omega}(V)|^u \geq \sum_{1 \leq j \leq 2\ell_{\text{tot}}} 2^{-j} \iota_j$ ,<sup>13</sup> where  $\widehat{\omega}(V)|^u$  approximates  $\omega(V)|^u$  with precision  $2^{-2\ell_{\text{tot}}}$ . All these checks can be verified using basic matrix operations in deterministic polynomial time. Finally, a direct calculation yields that the set size  $|S|$  satisfies the desired requirements.

### 1.2.3 Lower bounds for QIPL and QIP<sub>U</sub>L

$\text{NP} \subseteq \text{QIPL}$ . This inclusion draws inspiration from the interactive proof system in [CL95, Lemma 2] and presents a challenge in adapting this proof system to the QIPL setting.

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  $\alpha$  of  $\phi$  assigns each variable  $x_j$  for  $j \in [n]$  a value  $\alpha_j$  of either  $\top$  (true) or  $\perp$  (false). To verify whether  $\phi$  is satisfied by the assignment  $\alpha$ , we encode  $\phi(\alpha)$  as  $\text{Enc}(\phi(\alpha))$ , 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  $\text{Enc}(\phi(\alpha))$ , ordered by the variable  $\text{var}(l)$  corresponding to the literal  $l$ ;
- (ii) **SATISFIABILITY CHECK** (for clauses). For each  $i \in \{1, \dots, k\}$ , the prover sends the three triples  $(l_1, i, v_1)$ ,  $(l_2, i, v_2)$ , and  $(l_3, i, v_3)$  in  $\text{Enc}(\phi(\alpha))$ .

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*.

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,<sup>14</sup> triple by triple, and compares the fingerprints from both phases at the end. The verifier accepts if all checks succeed.

Using the fingerprinting lemma [Lip90], we prove the correctness of this proof system, showing that  $3\text{-SAT} \in \text{QIPL}_{8k}[1, 1/3]$ . Interestingly, when combined with the inclusion  $\text{QIPL} \subseteq \text{NP}$ , this protocol suggests an alternative approach to (indirect) error reduction for QIPL.

$\text{SAC}^1 \subseteq \text{QIP}_{\text{U}}\text{L}$ . This inclusion is inspired by the interactive proof system in [For89, Section 3.4]. By using error reduction for QIP<sub>U</sub>L, specifically Theorem 1.5(2), it remains to demonstrate that  $\text{SAC}^1 \subseteq \text{QIP}_{\text{U}}\text{L}[1, 1 - 1/\text{poly}(n)]$ . A Boolean circuit is defined as a (uniform)  $\text{SAC}^1$  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 [For89, Section 3.4], to quantum messages

<sup>13</sup>The condition  $\widehat{\omega}(V)|^u > 0$  is necessary because, for any  $u$ ,  $(u, \iota_1, \dots, \iota_{2\ell_{\text{tot}}}) \notin S$  when  $\iota_1 = \dots = \iota_{2\ell_{\text{tot}}} = 0$ .

<sup>14</sup>See 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.

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.

#### 1.2.4 The equivalence of $\text{QSZK}_{\text{UL}}$ and BQL

We demonstrate Theorem 1.4 by introducing a  $\text{QSZK}_{\text{ULHV}}$ -complete problem:

**Theorem 1.6** (Informal of Theorem 5.3). *INDIVPRODQSD is  $\text{QSZK}_{\text{ULHV}}$ -complete.*

We begin by informally defining the promise problem INDIVIDUAL PRODUCT STATE DISTINGUISHABILITY, denoted by  $\text{INDIVPRODQSD}[k(n), \alpha(n), \delta(n)]$ , where the parameters satisfy  $\alpha(n) - k(n) \cdot \delta(n) \geq 1/\text{poly}(n)$  and  $1 \leq k(n) \leq \text{poly}(n)$ . This problem considers two  $k$ -tuples of  $O(\log n)$ -qubit quantum states, denoted by  $\sigma_1, \dots, \sigma_k$  and  $\sigma'_1, \dots, \sigma'_k$ , 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

$$\text{T}(\sigma_1 \otimes \dots \otimes \sigma_k, \sigma'_1 \otimes \dots \otimes \sigma'_k) \geq \alpha. \quad (1.2)$$

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

$$\forall j \in [k], \quad \text{T}(\sigma_j, \sigma'_j) \leq \delta. \quad (1.3)$$

Then we show that (1) the complement of  $\text{INDIVPRODQSD}$ ,  $\overline{\text{INDIVPRODQSD}}$ , is  $\text{QSZK}_{\text{ULHV}}$ -hard; and (2)  $\text{INDIVPRODQSD}$  is in BQL, which is contained in  $\text{QSZK}_{\text{ULHV}}$  by definition.

**$\overline{\text{INDIVPRODQSD}}$  is  $\text{QSZK}_{\text{ULHV}}$ -hard.** The hardness proof draws inspiration from [Wat02, Section 5]. Consider a  $\text{QSZK}_{\text{ULHV}}[2k, c, s]$  proof system, denoted by  $\mathcal{B}$ . The logspace-bounded simulator  $S_{\mathcal{B}}$  produces good state approximations  $\xi_j$  and  $\xi'_j$  of the snapshot states  $\rho_{M_j W_j}$  and  $\rho_{M'_j W_j}$  after the  $(2j-1)$ -st turn and the  $(2j)$ -th turn in  $\mathcal{B}$ , respectively, satisfying  $\xi_j \approx_{\delta} \rho_{M_j W_j}$  and  $\xi'_j \approx_{\delta} \rho_{M'_j W_j}$ , 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 (1.1) in the SDP formulation for QIPL proof systems. For convenience, let  $\sigma_j := \text{Tr}_{M_j}(\xi_j)$  and  $\sigma'_j := \text{Tr}_{M'_j}(\xi'_j)$  for  $j \in [k]$ . We then establish  $\text{QSZK}_{\text{LHV}}$  hardness as follows:

- For *yes* instances, the message-wise closeness condition of the simulator  $S_{\mathcal{B}}$  implies Equation (1.3) 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 (1.2) with  $\alpha(n) := (\sqrt{c} - \sqrt{s})^2/4(k-1)$ .

$\text{INDIVPRODQSD} \in \text{BQL}$ . Since it holds that  $\text{BQL} = \text{QMAL}$  [FKL<sup>+</sup>16, FR21], it suffices to establish that  $\text{INDIVPRODQSD} \in \text{QMAL}$ . By applying an averaging argument in combination with Equation (1.2), we derive the following:

$$\sum_{j \in [k]} \text{T}(\sigma_j, \sigma'_j) \geq \text{T}(\sigma_1 \otimes \dots \otimes \sigma_k, \sigma'_1 \otimes \dots \otimes \sigma'_k) \geq \alpha \quad \Rightarrow \quad \exists j \in [k] \text{ s.t. } \text{T}(\sigma_j, \sigma'_j) \geq \frac{\alpha}{k}. \quad (1.4)$$

The QMAL protocol works as follows: (1) The prover sends an index  $i \in [k]$  to the verifier; and (2) The verifier accepts if  $\text{Tr}(\sigma_i, \sigma'_i) \geq \alpha/k$  and rejects if  $\text{Tr}(\sigma_i, \sigma'_i) \leq \delta$ , in accordance with Equation (1.4) and Equation (1.3). The resulting promise problem to be verified is precisely an instance of  $\text{GAPQSD}_{\log}$ , which is known to be BQL-complete [LGLW23].

### 1.3 Discussion and open problems

We introduce two models of space-bounded quantum interactive proof systems: QIPL and QIP<sub>UL</sub>. Unlike BQL = BQ<sub>UL</sub>, we show that QIP<sub>UL</sub>  $\subsetneq$  QIPL unless P = 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 QIPL, specifically when allowing a general quantum logspace verifier?

A motivating example is a reversible generalization of QIPL, particularly space-bounded *isometric* quantum interactive proof systems (QIPL<sup>◊</sup>, see Remark 3.8), where all verifier actions are  $O(\log n)$ -qubit *isometric* quantum circuits. Remarkably, QIPL<sup>◊</sup> at least contains QMA: Given a local Hamiltonian  $H = \sum_{i=1}^m H_i$ , we can construct a QIPL<sup>◊</sup> proof system as follows:<sup>15</sup>

- (i) The verifier chooses a local term  $H_i$  uniformly at random from the set  $\{H_1, \dots, H_m\}$ .
- (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  $I = H_i + (I - H_i)$ .<sup>16</sup>

Further analysis indicates that the verifier accepts with probability  $1 - m^{-1}\langle\Omega|H|\Omega\rangle$ , and direct sequential repetition yields a QIPL<sup>◊</sup> 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 (QIP<sub>UL</sub>) can simulate the classical counterparts with  $O(\log n)$  public coins [For89] (see Theorem 1.2), raising the question:

- (b) Can we achieve a tighter characterization of QIP<sub>UL</sub>? For example, does QIP<sub>UL</sub> contain space-bounded classical interactive proofs with  $\omega(\log n)$  public coins?

In addition to QIPL<sup>◊</sup> and QIP<sub>UL</sub>, the class QIPL lie between NP and SBP, a subclass of AM. Under reasonable derandomization assumptions [KvM02, MV05], QIP<sub>UL</sub> exactly characterizes NP, following from the collapse of AM to NP. This raises an interesting question:

- (c) Can we obtain a tighter characterization of QIPL without derandomizing AM?

A natural approach to Question (c) is to strengthen the lower bound from NP to either MA or StoqMA by designing a QIPL proof systems for problems such as SETCSP [AG21, Liu21], where the honest prover strategy requires *coherence* rather than only classical messages.

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 7), leading to the following question:

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

### 1.4 Related works

Variants of time-bounded quantum interactive proofs with short messages were explored in [BSW11, Per12]. 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 [RY22]. Follow-up research established the equivalence  $\text{stateQIP} = \text{statePSPACE}$  [MY23]

<sup>15</sup>A similar approach is used in a streaming version of QMAL (with online access to the message) in [GR23].

<sup>16</sup>See the proof of [KSV02, Proposition 14.2] for an explicit construction of such POVMs.

and developed a parallelization technique for stateQIP [INN<sup>+</sup>22, Ros24]. A Merlin-Arthur-type variant was also explored in [DLGLM23, DLG24]. More recently, quantum interactive proofs for unitary synthesis and related problems have been studied in [BEM<sup>+</sup>23, LMW24]. Another interesting but less related variant is the exploration of interactive proof systems in distributed computing [KOS18, NPY20], and more recently, quantum distributed interactive proof systems have been investigated [FPLGN21, LGMN23, HKN24].

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 [DGRV11, AHT23, AGM<sup>+</sup>23]. More recently, a variant where the verifier has *online* (i.e., one-way) access to messages has also been explored [CDGH24].

## 2 Preliminaries

We assume that the reader is familiar with quantum computation and the theory of quantum information. For an introduction, the textbooks by [NC10] and [dW19] provide a good starting point, while for a more comprehensive survey on quantum complexity theory, refer to [Wat09a].

We introduce several conventions throughout the paper: (1) we denote  $[n] := \{1, 2, \dots, n\}$ ; (2) we use the logarithmic function  $\log(x)$  with base 2; and (3) we utilize the notation  $|\bar{0}\rangle$  to represent  $|0\rangle^{\otimes a}$  with  $a > 1$ . In addition to these conventions, we provide two useful definitions. We say that  $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$  is a *promise problem*, if it satisfies that  $\mathcal{I}_{\text{yes}} \cap \mathcal{I}_{\text{no}} = \emptyset$  and  $\mathcal{I}_{\text{yes}} \cup \mathcal{I}_{\text{no}} \subseteq \{0, 1\}^*$ . For simplicity, we use the abbreviation  $x \in \mathcal{I}$  to denote  $x \in \mathcal{I}_{\text{yes}} \cup \mathcal{I}_{\text{no}}$ . A function  $\mu(n)$  is said to be *negligible*, if for every integer  $c \geq 1$ , there is an integer  $n_c > 0$  such that for all  $n \geq n_c$ ,  $\mu(n) < n^{-c}$ .

### 2.1 Distance-like measures for quantum states

We will provide an overview of relevant quantum distances and divergences, along with useful inequalities among different quantum distance-like measures. We say that a square matrix  $\rho$  is a *quantum state* if  $\rho$  is positive semi-definite and  $\text{Tr}(\rho) = 1$ .

**Definition 2.1** (Trace distance and fidelity). *For any quantum states  $\rho_0$  and  $\rho_1$ , we define two distance-like measures:*

- **Trace distance.**  $T(\rho_0, \rho_1) := \frac{1}{2} \text{Tr}|\rho_0 - \rho_1| = \frac{1}{2} \text{Tr}((\rho_0 - \rho_1)^\dagger (\rho_0 - \rho_1))^{1/2}$ .
- **(Uhlmann) Fidelity.**  $F(\rho_0, \rho_1) := \text{Tr}|\sqrt{\rho_0} \sqrt{\rho_1}|$ .

We begin by listing two useful bounds on tensor-product quantum states with respect to the trace distance:

**Lemma 2.2** (Trace distance on tensor-product states, adapted from Exercise 9.1.2 and Corollary 9.1.10 in [Wil13]). *For any quantum states  $\rho_1 \otimes \dots \otimes \rho_k$  and  $\rho'_1 \otimes \dots \otimes \rho'_k$ , where  $\rho_i$  and  $\rho'_i$  use the same number of qubits for all  $i \in [k]$ , it holds that*

- (1)  $\forall i \in [k], T(\rho_i, \rho'_i) \leq T(\rho_1 \otimes \dots \otimes \rho_k, \rho'_1 \otimes \dots \otimes \rho'_k)$ .
- (2)  $T(\rho_1 \otimes \dots \otimes \rho_k, \rho'_1 \otimes \dots \otimes \rho'_k) \leq \sum_{i \in [k]} T(\rho_i, \rho'_i)$ .

We then provide two fundamental properties of the trace distance.

**Lemma 2.3** (Data-processing inequality for the trace distance, adapted from [NC10, Theorem 9.2]). *Let  $\rho_0$  and  $\rho_1$  be quantum states. For any quantum channel  $\mathcal{E}$ , it holds that*

$$T(\mathcal{E}(\rho_0), \mathcal{E}(\rho_1)) \leq T(\rho_0, \rho_1).$$



**Lemma 2.4** (Unitary invariance for the trace distance, adapted from [NC10, Equation (9.21)]). Let  $\rho_0$  and  $\rho_1$  be quantum states. For any unitary transformation  $U$ , it holds that

$$\mathbb{T}(U\rho_0U^\dagger, U\rho_1U^\dagger) = \mathbb{T}(\rho_0, \rho_1).$$

Next, we present two basic properties for the fidelity.

**Lemma 2.5** (Data-processing inequality for the fidelity, adapted from Theorem 9.6 in [NC10]). Let  $\rho_0$  and  $\rho_1$  be quantum states. For any quantum channel  $\mathcal{E}$ , it holds that

$$\mathbb{F}(\mathcal{E}(\rho_0), \mathcal{E}(\rho_1)) \geq \mathbb{F}(\rho_0, \rho_1).$$

**Lemma 2.6** ([SR01, Lemma 2] & [NS03, Lemma 3.3]). Let  $\rho_0$  and  $\rho_1$  be  $m$ -qubit quantum states. Then, for any  $m$ -qubit quantum state  $\xi$ , it holds that

$$\mathbb{F}(\rho_0, \xi)^2 + \mathbb{F}(\xi, \rho_1)^2 \leq 1 + \mathbb{F}(\rho_0, \rho_1).$$

Lastly, we present a lemma concerning the freedom in purifications of quantum states:

**Lemma 2.7** (Unitary equivalence of purifying the same state, adapted from [NC10, Exercise 2.81]). Let  $|\psi\rangle_{\text{AB}}$  and  $|\phi\rangle_{\text{AB}}$  be pure states on the registers **A** and **B** such that

$$\text{Tr}_{\text{B}}(|\psi\rangle\langle\psi|_{\text{AB}}) = \rho_{\text{A}} = \text{Tr}_{\text{B}}(|\phi\rangle\langle\phi|_{\text{AB}}),$$

where  $\rho_{\text{A}}$  is a mixed state on the register **A**. Then, there exists a unitary transformation  $U_{\text{B}}$  acting on the register **B** such that  $|\psi\rangle_{\text{AB}} = (I_{\text{A}} \otimes U_{\text{B}})|\phi\rangle_{\text{AB}}$ .

## 2.2 Space-bounded quantum computation

We say that a function  $s(n)$  is *space-constructible* if there exists a deterministic space  $s(n)$  Turing machine that takes  $1^n$  as an input and outputs  $s(n)$  in the unary encoding. Moreover, we say that a function  $f(n)$  is  *$s(n)$ -space computable* if there exists a deterministic space  $s(n)$  Turing machine that takes  $1^n$  as an input and outputs  $f(n)$ . Our definitions of space-bounded quantum computation are formulated in terms of *quantum circuits*. For a discussion on the equivalence between space-bounded quantum computation using *quantum circuits* and *quantum Turing machines*, we refer readers to [FL18, Appendix A] and [FR21, Section 2.2].

We begin by introducing three types of space-bounded quantum circuit families, as formalized in Definition 2.8. Our definitions align with [VW16, Section 2.3]. Throughout this work, we adopt the shorthand notation  $C_x$  to indicate that the circuit  $C_{|x|}$  takes input  $x$ .

**Definition 2.8** (Space-bounded quantum circuit families: unitary, almost-unitary, and isometric). Let us define three types of quantum circuits:

- **Unitary quantum circuit.** A unitary quantum circuit consists of a sequence of unitary quantum gates, each of which belongs to some fixed gate set that is universal for quantum computation, such as  $\{\text{H}, \text{CNOT}, \text{T}\}$ .
- **Almost-unitary quantum circuit.** An almost-unitary quantum circuit generalizes a unitary quantum circuit acting on  $O(s(n))$  qubits by allowing  $O(s(n))$  single-qubit measurement gates  $\text{M}$  in the computational basis, which are defined by a pinching channel:<sup>17</sup>

$$\Phi^{\text{M}}(\rho) := |0\rangle\langle 0| \text{Tr}(M_0\rho) + |1\rangle\langle 1| \text{Tr}(M_1\rho), \text{ where } M_b := |b\rangle\langle b| \text{ for } b \in \{0, 1\}.$$

- **Isometric quantum circuit.** An isometric quantum circuit extends a unitary quantum circuit acting on  $O(s(n))$  qubits by allowing  $O(s(n))$  ancillary gates. An ancillary gate is a non-unitary gate that takes no input and produces a single qubit in the state  $|0\rangle$  as output.

<sup>17</sup>See Section 4.1.1 (particularly Definition 4.4) in [Wat18] for further details. This type of channel, also referred to as a completely phase-damping channel, is discussed in [VW16, Equation (2.24)].



For convenience, we treat almost-unitary quantum circuits as a special case of isometric quantum circuits.<sup>18</sup> For a promise problem  $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$ , a family of unitary, almost-unitary, or isometric quantum circuits  $\{C_x : x \in \mathcal{I}\}$  is called  $s(n)$ -space-bounded if there is a deterministic Turing machine that, given any input  $x \in \mathcal{I}$  with input length  $n := |x|$ , runs in space  $O(s(n))$  (and hence time  $2^{O(s(n))}$ ) and outputs a description of  $C_x$ , where  $C_x$  accepts if  $x \in \mathcal{I}_{\text{yes}}$ , rejects if  $x \in \mathcal{I}_{\text{no}}$ , acts on  $O(s(n))$  qubits, and consists of  $2^{O(s(n))}$  gates.

*Remark 2.9* (Subtleties on space-bounded quantum circuit families). In the context of space-bounded quantum circuits, as defined in Definition 2.8, there are important subtleties:

- (1) Unlike a full projective measurement that collapses a state into a specific outcome, a pinching measurement preserves a mixed-state structure while imposing *decoherence* between subspaces. As a result, almost-unitary quantum circuits are *oblivious* to intermediate measurement outcomes, meaning their description remains independent of these outcomes despite having access to them. This subtlety prevents qubits in such circuits from being directly reset to zero, differentiating them from isometric quantum circuits.
- (2) Space-bounded unitary and almost-unitary quantum circuits are equivalent for promise problems via the principle of deferred measurements. However, such equivalences are unknown in more general settings, analogous to the scenario in Footnote 20.

In this work, we focus on (log)space-bounded quantum circuits with  $s(n) = O(\log n)$ . The complexity classes corresponding to space-bounded unitary and general quantum circuits with  $s(n) = \Theta(\log(n))$  are known as BQ<sub>U</sub>L and BQL, respectively. As described in [VW16, Section 2.3], a *general quantum circuit* extends a unitary quantum circuit by including ancillary gates and *erasure gates*.<sup>19</sup> It has been established that BQ<sub>U</sub>L = BQL for promise problems [FR21] (see also [GRZ21, GR22]), whereas such equivalences remain unproven in more general forms.<sup>20</sup> For detailed definitions and known properties of these classes, we refer to [LGLW23, Section 2.3] as a brief introduction.

Lastly, we define *logspace (many-to-one) reductions*. We begin by slightly abusing notation and considering parameterized promise problems of the form  $\mathcal{I} = \{\mathcal{I}_{n,t_1,\dots,t_r}\}_{n \in \mathbb{N}}$  for functions  $t_1, \dots, t_r : \mathbb{N} \rightarrow \mathbb{R}$ , where  $\mathcal{I}_{n,t_1,\dots,t_r}$  consists of instances of size  $n$  which satisfy conditions expressed in terms of  $t_1(n), \dots, t_r(n)$ . We say that  $\mathcal{I} = \{\mathcal{I}_{n,t_1,\dots,t_r}\}_{n \in \mathbb{N}}$  is (many-to-one) reducible to  $\mathcal{I}' = \{\mathcal{I}'_{m,t'_1,\dots,t'_r}\}_{m \in \mathbb{N}}$  if there exist  $(r+1)$ -variable real polynomials  $p_0, \dots, p_{r'}$  such that for all  $n \in \mathbb{N}$ , there exists a function  $g_n : \mathcal{I}_{n,t_1,\dots,t_r} \rightarrow \mathcal{I}'_{m,t'_1,\dots,t'_r}$  satisfying the following conditions: (1)  $m = p_0(n, t_1(n), \dots, t_r(n))$ ; (2)  $t'_j(m) = p_j(n, t_1(n), \dots, t_r(n))$  for all  $j \in [r']$ ; (3)  $g_n(x) \in \mathcal{I}'_{m,t'_1,\dots,t'_r}$  for all  $x \in \mathcal{I}_{n,t_1,\dots,t_r}$ . If the family of functions  $\{g_n\}_{n \in \mathbb{N}}$  is computable in deterministic logspace, we say that  $\mathcal{I}$  is logspace-reducible to  $\mathcal{I}'$ , denoted by  $\mathcal{I} \leq_{\text{L}}^m \mathcal{I}'$ .

## 2.3 Space-bounded quantum state testing

We begin by defining the space-bounded quantum state testing problem with respect to the trace distance, denoted as GAPQSD<sub>log</sub>:

<sup>18</sup>More specifically, by applying the principle of deferred measurements (e.g., [NC10, Section 4.4]) to an almost-unitary quantum circuit, we obtain an isometric quantum circuit in which each measurement gate is simulated by an ancillary gate, and all ancillary qubits are measured at the end.

<sup>19</sup>An erasure gate is a non-unitary gate that takes a single qubit as input and produces no output. Alternatively, a general quantum circuit can also be defined by extending a unitary quantum circuit with measurement gates and reset-to-zero gates, as in [FR21, GR22]. Notably, a reset-to-zero gate can be simulated by first applying an erasure gate to remove the original qubit and then using an ancillary gate to introduce a new qubit.

<sup>20</sup>Specifically, this refers to the transformation of a unitary quantum logspace circuit  $C'$  from a general quantum logspace circuit  $C$  (with all-zero states as input) such that the final state of  $C$  and  $C'$  are identical. This is a stronger requirement than merely ensuring that the output qubits of these circuits are the same. This general form only can be simulated in NC<sup>2</sup> [Wat99, Wat03b].

**Definition 2.10** (Space-bounded Quantum State Distinguishability Problem, adapted from Definition 4.1 and 4.2 [LGLW23]). *Let  $\alpha(n)$ ,  $\beta(n)$ ,  $r(n)$  be logspace computable functions such that  $0 \leq \beta(n) < \alpha(n) \leq 1$ ,  $\alpha(n) - \beta(n) \geq 1/\text{poly}(n)$  and  $1 \leq r(n) \leq O(\log n)$ . Let  $Q_0$  and  $Q_1$  be polynomial-size unitary quantum circuits acting on  $O(\log n)$  qubits, with  $r(n)$  specified output qubits. Here,  $n$  represents the total number of gates in  $Q_0$  and  $Q_1$ . For  $b \in \{0, 1\}$ , let  $\rho_b$  denote the quantum states obtained by running  $Q_b$  on the all-zero state  $|\bar{0}\rangle$  and tracing out the non-output qubits, then the promise is that one of the following holds:*

- *Yes instances: A pair of quantum circuits  $(Q_0, Q_1)$  such that  $T(\rho_0, \rho_1) \geq \alpha(n)$ ;*
- *No instances: A pair of quantum circuits  $(Q_0, Q_1)$  such that  $T(\rho_0, \rho_1) \leq \beta(n)$ .*

Moreover, we use the notation  $\overline{\text{GAPQSD}}_{\log}$  to denote the complement of  $\text{GAPQSD}_{\log}$  with respect to the chosen parameters  $\alpha(n)$  and  $\beta(n)$ . As established in [LGLW23],  $\text{GAPQSD}_{\log}$  is BQL-complete, and we are particularly interested in the BQL containment:

**Theorem 2.11** ( $\text{GAPQSD}_{\log}$  is in BQL, adapted from [LGLW23, Theorem 4.10]). *Let  $\alpha(n)$  and  $\beta(n)$  be logspace computable functions such that  $\alpha(n) - \beta(n) \geq 1/\text{poly}(n)$ . It holds that*

$$\text{GAPQSD}_{\log}[\alpha(n), \beta(n)] \in \text{BQL}.$$

Lastly, it is worth noting that by removing the space constraints on the quantum circuits  $Q_0$  and  $Q_1$  and allowing  $r(n) \leq n$ , where  $n$  denotes the input length of these state-preparation circuits, we obtain a variant of Definition 2.10 that aligns with the definition of  $\text{GAPQSD}[\alpha(n), \beta(n)]$ . This promise problem was considered in [Wat02] with the condition  $\alpha^2 > \beta$ , referred to as  $\text{QSD}[\alpha(n), \beta(n)]$ .

## 2.4 Classical concepts, tools, and complexity classes

**3-SAT.** The 3-SAT problem is one of the simplest examples of NP-complete problems. We provide only a brief introduction to 3-SAT here. For further details, see [AB09, Section 2.3].

A 3-SAT formula can be written as  $\phi = C_1 \wedge \cdots \wedge C_k$ , where each clause  $C_i$  for  $i \in [k]$  is of the form  $(l_1^{(i)} \vee l_2^{(i)} \vee l_3^{(i)})$ , with each literal  $l_j^{(i)}$  being either one of the variables  $x_1, \dots, x_n$  or its negation. For instance,  $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_4 \vee \neg x_2 \vee x_3) \wedge (x_4 \vee \neg x_1 \vee \neg x_3)$  illustrates the structure. An assignment of a 3-SAT formula assigns each variable  $x_j$  for  $j \in [n]$  a value of either  $\top$  (true) or  $\perp$  (false). The 3-SAT problem aims to decide whether a given formula  $\phi$  is satisfiable. We say that  $\phi$  is satisfiable if there exists an assignment  $\alpha$  such that  $\Phi(\alpha) = \top$ .

**Lemma 2.12** ([AB09, Exercise 4.6]). *3-SAT is NP-complete under logspace reductions.*

**Fingerprinting of multisets.** A fingerprint of a multiset  $\{x_1, \dots, x_k\}$ , where all elements are non-negative integers and duplicates are allowed, is defined as  $\prod_{i=1}^k (x_i + r) \bmod p$ , with  $p$  being a prime and  $r \in [p-1]$ . The fingerprinting lemma [Lip90] aims to compare whether two multisets are equal by using short fingerprints:

**Lemma 2.13** (Fingerprinting lemma, adapted from [Lip90, Theorem 3.1]). *Let  $A := \{x_1, \dots, x_{\ell_1}\}$  and  $B := \{y_1, \dots, y_{\ell_2}\}$  be two multisets in which all elements are  $b$ -bit non-negative integers, with  $\ell := \max\{\ell_1, \ell_2\}$ . If the prime  $p$  is chosen uniformly at random from the interval  $[(b\ell)^2, 2(b\ell)^2]$  and the integer  $r$  is chosen uniformly at random from the interval  $[1, p-1]$ , the probability that the distinct multisets  $A$  and  $B$  produce the same fingerprint is at most  $O\left(\frac{\log b + \log \ell}{b\ell} + \frac{1}{b^2\ell}\right)$ .*

**(Uniform) SAC<sup>1</sup>.** The complexity class (uniform) SAC<sup>1</sup> is a restricted subclass of (uniform) AC<sup>1</sup>. Throughout this paper, SAC<sup>1</sup> circuits will refer to (logspace-)uniform SAC<sup>1</sup> circuits. We define SAC<sup>1</sup> circuits and their corresponding circuit evaluation problem as follows:

**Definition 2.14** (UNIFORM SAC<sup>1</sup> CIRCUIT EVALUATION, adapted from [BCD<sup>+</sup>89]). A Boolean circuit  $C: \{0, 1\}^n \rightarrow \{0, 1\}$  is defined as an SAC<sup>1</sup> circuit if it has depth  $O(\log n)$ , includes unbounded fan-in OR ( $\vee$ ) gates, bounded fan-in AND ( $\wedge$ ) gates (e.g., with fan-in 2), and has negation ( $\neg$ ) gate restricted to the input level. The problem is to decide whether a given (logspace-)uniform SAC<sup>1</sup> circuit  $C$ , whose description can be computed by a deterministic logspace Turing machine, evaluates to 1.

Venkateswaran [Ven91] established that SAC<sup>1</sup> is equivalent to LOGCFL, the complexity class consists of languages that are logspace-reducible to context-free languages [Sud78]. To compare with other classes of logspace-uniform bounded-depth Boolean circuits, it is known that:

$$\text{NL} \subseteq \text{SAC}^1 = \text{LOGCFL} \subseteq \text{AC}^1 \subseteq \text{NC}^2$$

Here, NL is a logspace version of NP with polynomial-length witness, AC<sup>1</sup> captures the power of  $O(\log n)$ -depth Boolean circuits using *unbounded* fan-in gates, and NC<sup>2</sup> characterizes the power of  $O(\log^2 n)$ -depth Boolean circuits with *bounded* fan-in gates.

Similar to NL, LOGCFL (equivalently, SAC<sup>1</sup>) is closed under complementation [BCD<sup>+</sup>89]. However, whether SAC<sup>1</sup> is contained in BPL or BQL remains an open problem.

**Set size estimation and SBP.** Let  $S \subseteq \{0, 1\}^k$  be a set with efficiently verifiable membership. Formally, there is a membership oracle  $\mathcal{O}_S: \{0, 1\}^k \rightarrow \{0, 1\}$  satisfying  $\mathcal{O}_S(x) = 1$  if and only if  $x \in S$ . The SET SIZE ESTIMATION PROBLEM (SSE) is defined as follows:

**Definition 2.15** (Set Size Estimation Problem, SSE, adapted from [Vol20, Definition 2.10]). Let  $S \subseteq \{0, 1\}^k$ , where  $k$  is polynomial in the input size  $n$ , and assume that membership in  $S$  can be determined by an efficiently implementable oracle  $\mathcal{O}_S: \{0, 1\}^k \rightarrow \{0, 1\}$ . Given an efficiently computable positive integer function  $t$ , the problem is to distinguish between the following cases:

- Yes instances: The set size  $|S|$  is at least  $t(n)$ ;
- No instances: The set size  $|S|$  is at most  $t(n)/2$ .

The promise problem SSE is known to be SBP-complete, as stated in Lemma 2.16. The class SBP, which stands for *small bounded-error probability*, is a generalization of BPP with a constant multiplicative error and lies between MA and AM [BGM06]:

**Lemma 2.16** (Implicit in [BGM06]). SSE is SBP-complete.

Two variants of SSE arise when the membership oracle  $\mathcal{O}_S$  requires a witness string  $w$ :

- Witnessed SSE:  $x \in S$  if and only if there exists a witness  $w_x$  such that  $\mathcal{O}_S(x, w_x) = 1$ .
- Existential SSE: There exists a witness  $w_S$  such that  $x \in S$  if and only if  $\mathcal{O}_S(x, w_S) = 1$ .

Witnessed SSE is AM-complete [GS86, Vol20], as it captures the full power of the set lower bound protocol [GS86]. In contrast, Existential SSE is NSBP-complete by definition, where NSBP is the nondeterministic version of SBP. Notably, SBP is closed under nondeterminism:

**Lemma 2.17** (Theorem 4.2 in [Wat16b]). SBP = NSBP.

Furthermore, under reasonable derandomization assumptions [KvM02, MV05], AM collapses to NP, implying the equivalence  $\text{NP} = \text{MA} = \text{SBP} = \text{AM}$ .

### 3 Space-bounded (unitary) quantum interactive proofs

In this section, we introduce space-bounded quantum interactive proofs (QIPL), where the verifier's actions are implemented using space-bounded *almost-unitary* quantum circuits (see Definition 2.8 and Remark 2.9(1)); along with the variant QIP<sub>U</sub>L, in which the verifier's actions

are restricted to *unitary* circuits. Both QIPL and QIP<sub>U</sub>L are variants of single-prover quantum interactive proofs (QIP) [Wat03a, KW00] that have a space constraint. We establish three theorems concerning the classes QIPL and QIP<sub>U</sub>L, focusing on space-bounded (unitary) quantum interactive proofs with a *polynomial* number of messages.

The first theorem shows that QIPL lies between NP and SBP, as stated in Theorem 3.1. This result can be seen as a quantum analog of classical works [Lip90, CL95].

**Theorem 3.1** (Almost-tight characterization of QIPL). *The following holds:*

- (1) For any logspace-computable function  $m(n)$  such that  $1 \leq m(n) \leq \text{poly}(n)$ ,

$$\cup_{c(n)-s(n) \geq 1/\text{poly}(n)} \text{QIPL}_m[c, s] \subseteq \text{SBP}.$$

- (2)  $\text{NP} \subseteq \text{QIPL}_m$ , where  $m(n)$  is some polynomial in  $n$ .

*Remark 3.2* (A high-concentration condition yields an exact characterization of NP). Let QIPL<sub>HC</sub> be a subclass of QIPL in which *yes* instances satisfy an additional restriction: the distribution of intermediate measurement outcomes  $u = (u_1, \dots, u_l)$ , conditioned on acceptance, must be *highly concentrated*.<sup>21</sup> Using our second SDP formulation for QIPL proof systems (Lemma 3.14), one can prove that QIPL<sub>HC</sub> is contained in NP. As the honest prover strategy (classical messages) described in Protocol 3.4 corresponds to a unique measurement outcome  $u^*$ , Theorem 3.15 extends directly to QIPL<sub>HC</sub>, thereby establishing the equivalence QIPL<sub>HC</sub> = NP.

The second theorem addresses two fundamental but crucial properties of QIPL and QIP<sub>U</sub>L. Specifically, closure under perfect completeness (Lemma 3.9) and error reduction through sequential repetition (Lemma 3.10):

**Theorem 3.3** (Basic properties for QIPL and QIP<sub>U</sub>L). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable 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 the following properties hold:*

- (1) **Closure under perfect completeness.**

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

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

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

Here,  $m'$  is some polynomial in  $n$ .

The third theorem provides a lower bound for QIP<sub>U</sub>L, which serves as a quantum analog of the space-bounded public-coin classical interactive proof for SAC<sup>1</sup> established in [For89]:

**Theorem 3.4.**  $\text{SAC}^1 \cup \text{BQL} \subseteq \text{QIP}_{U,m}$ , where  $m(n)$  is some polynomial in  $n$ .

In the remainder of this section, we provide the definitions of space-bounded (unitary) quantum interactive proofs, specifically the classes QIPL and QIP<sub>U</sub>L, in Section 3.1. Next, the proof of the two basic properties in Theorem 3.3 is presented in Section 3.2. We then formulate QIPL proof systems as semi-definite programs in Section 3.3, leading to the inclusion QIPL  $\subseteq$  SBP (Theorem 3.11). Lastly, the lower bounds for QIPL and QIP<sub>U</sub>L, particularly the inclusions NP  $\subseteq$  QIPL (Theorem 3.15) and SAC<sup>1</sup>  $\subseteq$  QIP<sub>U</sub>L (Theorem 3.4), are established in Section 3.4.

<sup>21</sup>In technical terms, let  $\omega(V)|^u$  denote the contribution of  $u$  to  $\omega(V)$ , where  $\omega(V)$  is the maximum acceptance probability of  $P \equiv V$ . The high-concentration condition for *yes* instances requires the existence of some  $u^*$  such that  $\omega(V)|^{u^*} \geq c(n)$ .

### 3.1 Definitions of space-bounded quantum interactive proof systems

Our definitions of space-bounded quantum interactive proofs follow that of [KW00, Section 2.3] and [Wat02, Section 2.3]. In this framework, a (log)space-bounded quantum interactive proof system consists of two parties: an untrusted prover with unbounded computational power, and a verifier constrained to using only  $O(\log n)$  qubits, enabling at most polynomial-time quantum computation. The primary distinction between standard single-prover quantum interactive proofs and their space-bounded variants lies in this additional space constraint on the verifier, which prompts a subtle question:

**Problem 3.5.** *Is it necessary to allow  $O(\log n)$  pinching intermediate measurements in the computational basis during each verifier’s action in space-bounded quantum interactive proofs?*

Interestingly, the answer to Problem 3.5 does not affect one-message proof systems, specifically (unitary) QMAL [FKL<sup>+</sup>16, FR21], where the unitary verification circuit acts on  $O(\log n)$  qubits and inherently allows not only  $O(\log n)$  pinching intermediate measurements but also  $O(\log n)$  ancillary gates (see also Remark 2.9).

To address Problem 3.5, we introduce two types of space-bounded quantum interactive proof systems, denoted by QIPL and QIP<sub>UL</sub>. In both proof systems, the verifier has *direct access* to the messages exchanged during interactions, which limits each message size to  $O(\log n)$ . The key distinction between these proof systems lies in their differing responses to Problem 3.5: In QIPL, the verifier’s actions correspond to space-bounded *almost-unitary* quantum circuits (see Definition 2.8), allowing  $O(\log n)$  pinching intermediate measurements in each verifier’s action. However, in QIP<sub>UL</sub>, the verifier’s actions are implemented using space-bounded *unitary* quantum circuits. Consequently, the former model encompasses space-bounded (private-coin) classical interactive proof systems, particularly the model described in [CL95].<sup>22</sup>

**Formal definitions of QIPL and QIP<sub>UL</sub>.** Given a promise problem  $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$ , a quantum verifier is *logspace-computable* mapping  $V$ , where for each input string  $x \in \mathcal{I} \subseteq \{0, 1\}^*$ ,  $V(x)$  is interpreted as an encoding of a  $k(|x|)$ -tuple  $(V(x)_1, \dots, V(x)_k)$  of quantum circuits. These circuits represent the verifier’s actions at each round of the proof system, with specific constraints depending on the proof system, QIPL or QIP<sub>UL</sub>:

- In a QIPL proof system, each  $V(x)_j$  corresponds to a space-bounded *almost-unitary* quantum circuit  $\tilde{V}(x)_j$ . By applying the principle of deferred measurements,  $\tilde{V}(x)_j$  can be transformed into an isometry  $V(x)_j$  (see Definition 2.8) that takes qubits in registers  $(M, W)$  as input and outputs qubits in registers  $(M, W, E_j)$ , where  $E_j$  holds  $q_{E_j}(|x|)$  qubits. At the end of the verifier’s  $j$ -th action  $V(x)_j$ , the (newly introduced) environment register  $E_j$  is measured in the computational basis, with the measurement outcome denoted as  $u_j$ . The total number of qubits satisfies  $q_M(|x|) + q_W(|x|) + q_{E_j}(|x|) \leq O(\log n)$ , with both  $W$  and  $E_j$  private to the verifier.
- In a QIP<sub>UL</sub> proof system, each  $V(x)_j$  is a space-bounded *unitary* quantum circuit acting on two registers  $M$  and  $W$ , which hold  $q_M(|x|)$  and  $q_W(|x|)$  qubits, respectively. The total number of qubits satisfies  $q_M(|x|) + q_W(|x|) \leq O(\log n)$ , with  $W$  private to the verifier.

Furthermore, the logspace-computability of  $V(x)$  requires a *strong notion of uniformity*: there must exist a logspace deterministic Turing machine  $\mathcal{M}$  that, for each input  $x$ , outputs the classical description of  $(V(x)_1, \dots, V(x)_k)$ .<sup>23</sup> Lastly, the verifier  $V$  is called  $m(|x|)$ -message if  $k(|x|) = \lfloor m(|x|)/2 + 1 \rfloor$  for all integer  $|x|$ , depending on whether  $m$  is even or odd.

<sup>22</sup>For any proof system that ensures soundness against classical messages, we can construct a corresponding proof system that guarantees soundness against quantum messages by measuring the message in the computational basis at the beginning of each verifier’s action.

<sup>23</sup>This uniformity requirement is slightly stronger and less general than merely requiring all quantum circuits  $V(x)_1, \dots, V(x)_k$  to be logspace-bounded (referred to as a *weaker notion of uniformity*), as the classical descriptions of these quantum circuits may not be generated by a single logspace deterministic Turing machine (although



Similar to standard quantum interactive proofs, the prover and the verifier in the same space-bounded quantum interactive proof system must be *compatible*. This means that they must agree on the maximum length  $q_M(|x|)$  of each message exchanged in the proof system and the total number  $m(|x|)$  of these messages. Hence, a quantum prover  $P$  is a function that maps each input  $x \in \mathcal{I}$  to an  $l(|x|)$ -tuple  $(P(x)_1, \dots, P(x)_l)$  of quantum circuits, where  $l(|x|) = \lfloor (m(|x|) + 1)/2 \rfloor$ . Each circuit  $P(x)_j$  acts on two registers  $Q$  and  $M$  with  $q_Q(|x|)$  and  $q_M(|x|)$  qubits, respectively, satisfying that  $Q$  is private to the prover. Since there are no restrictions on the prover  $P$ , each  $P(x)_j$  can be viewed as an arbitrary unitary transformation in general.

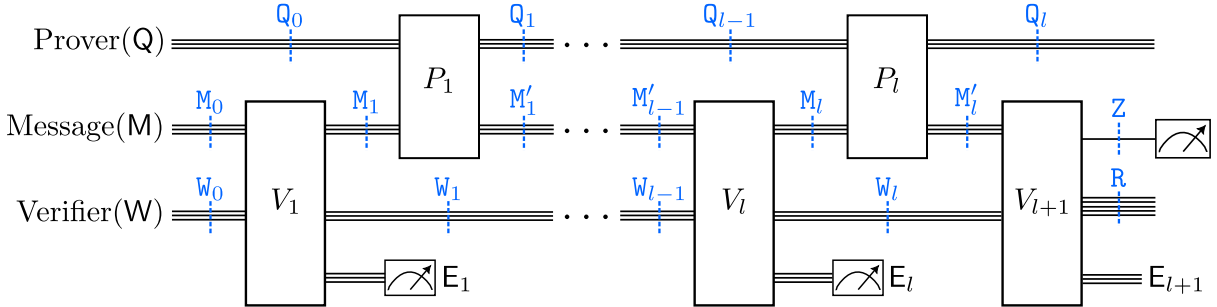


Figure 3.1: A  $2l$ -turn space-bounded quantum interactive proof system (with snapshots).

Given an input  $x \in \mathcal{I}$ , and a prover  $P$  and a verifier  $V$  that exchange  $m(|x|)$  messages, we define an  $m(|x|)$ -turn space-bounded quantum interactive proof system  $(P \rightleftharpoons V)(x)$ , namely a QIPL proof system, as a quantum circuit acting on the registers  $Q$ ,  $M$ ,  $W$ , and additional environment registers  $\{E_j\}$  as follows:

- If  $m(|x|) = 2l(|x|)$  is even, circuits  $V(x)_1, P(x)_1, \dots, V(x)_l, P(x)_l, V(x)_{l+1}$  are applied in sequence to the registers  $M$ ,  $W$ , and  $E_j$ , or to the registers  $Q$  and  $M$  accordingly. It is important to note that the register  $E_j$  is inaccessible after the  $j$ -th round.
- If  $m(|x|) = 2l(|x|) + 1$  is odd, the situation is similar, except that the prover starts the protocol, so the circuits  $P(x)_1, V(x)_1, \dots, P(x)_{l+1}, V(x)_{l+1}$  are applied in sequence.

Analogously, for an  $m(|x|)$ -turn space-bounded *unitary* quantum interactive proof system, namely a QIP<sub>U</sub>L proof system, the definition remains the same except that environment registers  $\{E_j\}$  are no longer involved. Without the loss of generality, we assume that the prover always sends the last message. See also Figure 3.1 for an illumination of the case when  $m(|x|)$  is even. For convenience, we sometimes omit the dependence on  $x$  and  $|x|$  when describing  $P$  and  $V$ , e.g., using  $P_j$  and  $V_j$  to denote  $P(x)_j$  and  $V(x)_j$ , respectively, and  $m$  to denote  $m(|x|)$ .

Assuming the mapping  $V(x) = (V(x)_1, \dots, V(x)_k)$  in a QIPL proof system is a collection of the isometries corresponding to the respective almost-unitary quantum circuits,<sup>24</sup> the state of the qubits in the circuit  $P \rightleftharpoons V$  is an (unnormalized) *pure state* on the registers  $(Q, M, V, E_j)$  after the verifier's  $j$ -th action.<sup>25</sup> A similar observation holds for QIP<sub>U</sub>L proof systems. Thus, for a given input  $x$ , the probability that  $P \rightleftharpoons V$  accepts  $x$  is defined as the probability that measuring the designated output qubit – typically the first qubit of  $(M, W)$  – of  $(P \rightleftharpoons V)(x)|\bar{0}\rangle_Q|\bar{0}\rangle_M|\bar{0}\rangle_W$  in the computational basis yields the outcome 1. We are now ready to formally define space-bounded quantum interactive proof systems:

a polynomial-time deterministic Turing machine would suffice).

<sup>24</sup>This assumption about the verifier's actions is crucial for adapting several techniques from standard quantum interactive proofs. For more on general verifiers in the standard scenario, see [VW16, Section 4.1.4].

<sup>25</sup>Specifically, a pure state occupies the registers  $(Q, M, V, E_1)$  before the measurements at the end of the verifier's first action. To align with the proof of Lemma 3.14 (the upper bound for QIPL), which considers only a specific measurement outcome, this post-measurement pure state will be unnormalized.



**Definition 3.6** (Space-bounded quantum interactive proofs, QIPL). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable functions of the input length  $n := |x|$  such that  $0 \leq s(n) < c(n) \leq 1$  and  $1 \leq m(n) \leq \text{poly}(n)$ . A promise problem  $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$  is in  $\text{QIPL}_m[c, s]$ , if there exists an  $m(n)$ -turn logspace-computable almost-unitary quantum verifier  $V$  such that:*

- **Completeness.** *For any  $x \in \mathcal{I}_{\text{yes}}$ , there exists an  $m(n)$ -message prover  $P$  such that*

$$\Pr[(P \rightleftharpoons V)(x) \text{ accepts}] \geq c(n).$$

- **Soundness.** *For any  $x \in \mathcal{I}_{\text{no}}$  and any  $m(n)$ -message prover  $P$ ,*

$$\Pr[(P \rightleftharpoons V)(x) \text{ accepts}] \leq s(n).$$

Furthermore, we define  $\text{QIPL}_m := \text{QIPL}_m[2/3, 1/3]$  and  $\text{QIPL} := \cup_{m \leq \text{poly}(n)} \text{QIPL}_m$ .

Analogously, we can define space-bounded unitary quantum interactive proof systems:

**Definition 3.7** (Space-bounded unitary quantum interactive proofs, QIP<sub>UL</sub>). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable functions of the input length  $n := |x|$  such that  $0 \leq s(n) < c(n) \leq 1$  and  $1 \leq m(n) \leq \text{poly}(n)$ . A promise problem  $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$  is in  $\text{QIP}_{\text{UL}m}[c, s]$ , if there exists an  $m(n)$ -turn logspace-computable unitary quantum verifier  $V$  such that:*

- **Completeness.** *For any  $x \in \mathcal{I}_{\text{yes}}$ , there exists an  $m(n)$ -message prover  $P$  such that*

$$\Pr[(P \rightleftharpoons V)(x) \text{ accepts}] \geq c(n).$$

- **Soundness.** *For any  $x \in \mathcal{I}_{\text{no}}$  and any  $m(n)$ -message prover  $P$ ,*

$$\Pr[(P \rightleftharpoons V)(x) \text{ accepts}] \leq s(n).$$

Furthermore, we define  $\text{QIP}_{\text{UL}m} := \text{QIP}_{\text{UL}m}[2/3, 1/3]$  and  $\text{QIP}_{\text{UL}} := \cup_{m \leq \text{poly}(n)} \text{QIP}_{\text{UL}m}$ .

*Remark 3.8* (A reversible generalization of QIPL). We introduce the class  $\text{QIPL}^\diamond$  as a reversible generalization of QIPL, primarily for convenience. A  $\text{QIPL}^\diamond$  proof system is defined similarly to a QIPL proof system, but with two crucial differences:

- (1) All of the verifier's actions are *isometric* quantum circuits, without restrictions. In particular, any unitary elementary gate can act on the ancillary qubits  $|\bar{0}\rangle$ , which are introduced by  $O(\log n)$  ancillary gates, and qubits in the message register  $\mathbf{M}$ .
- (2) The environment register  $\mathbf{E}_k$ , introduced during the verifier's  $k$ -th action, remains private to the verifier and is *accessible only during that turn*. Importantly, the qubits in  $\mathbf{E}_k$  are not measured at the end of the turn. Consequently, the qubits in  $\mathbf{E}_k$  remain unchanged after that turn, although the entanglement shared among  $\mathbf{E}_1, \dots, \mathbf{E}_k$ , and  $\mathbf{M}$  may change.

### 3.2 Basic properties: Error reduction and perfect completeness

The verifier's space constraint for the class QIPL presents several challenges when adapting techniques from standard quantum interactive proofs. For instance, techniques such as error reduction through parallel repetition [KW00, Section 5] and the parallelization approach described in [KW00, Section 4] are applicable to QIPL only under certain conditions. Nevertheless, two basic properties can still be established without additional assumptions:

- (1) Achieving perfect completeness in QIPL or QIP<sub>UL</sub> proof systems by adapting the technique in [VW16, Section 4.2.1], as detailed in Lemma 3.9.
- (2) Error reduction for QIPL and QIP<sub>UL</sub> via sequential repetition, as stated in Lemma 3.10;

We will provide detailed proofs of these properties in the remainder of this subsection.

### 3.2.1 Achieving perfect completeness for QIPL and QIP<sub>UL</sub>

Our construction and analysis in Lemma 3.9 are inspired by [VW16, Section 4.2.1].

**Lemma 3.9** (QIPL and QIP<sub>UL</sub> are closed under perfect completeness). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable 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, it follows that*

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

*Proof.* Since QIP<sub>UL</sub> proof systems are a special subclass of QIPL proof systems, it suffices to establish the inclusion for the latter. For any  $m$ -turn QIPL proof system  $P \rightleftharpoons V$  with completeness  $c$  and soundness  $s$ , which corresponds to a promise problem  $\mathcal{I}$  in  $\text{QIPL}_m[c, s]$ ,  $P \rightleftharpoons V$  acts on registers  $\mathbf{Q}$ ,  $\mathbf{M}$ , and  $\mathbf{W} = (\mathbf{Z}, \mathbf{R})$ , where  $\mathbf{Z}$  represents the output qubit just before the final measurement. To achieve perfect completeness, we propose a new proof system  $P' \rightleftharpoons V'$  based on  $P \rightleftharpoons V$ , as detailed in Protocol 3.1. In this proof system, we also introduce a new single-qubit register  $\mathbf{Z}'$ , which is initialized to be  $|0\rangle$  and is accessible only to  $V'$ .

It is noteworthy that the environment register introduced by the verifier's  $j$ -th action for  $j \in \lfloor (m+1)/2 \rfloor + 1$  in  $P \rightleftharpoons V$  has no effect on the new proof system  $P' \rightleftharpoons V'$ . This is because  $E_j$  is measured at the end of the turn in which it is introduced, it collapses to a quantum state that contains only a binary string and becomes inaccessible afterward.

---

**Protocol 3.1:** Achieving perfect completeness for QIPL (or QIP<sub>UL</sub>).

---

**Parameters:**  $\alpha$  is a dyadic rational number such that  $\frac{3c+s}{4} \leq \alpha \leq c$ .

1. The verifier  $V'$  executes the original proof system  $P \rightleftharpoons V$  (with the prover  $P'$ ), except for the verifier's final measurement on the register  $\mathbf{Z}$ ;
  2. The verifier  $V'$  creates a pseudo-copy of the output qubit of  $V$  by applying a  $\text{CNOT}_{\mathbf{Z} \rightarrow \mathbf{Z}'}$  gate, and then sends the register  $\mathbf{W} = (\mathbf{Z}, \mathbf{R})$  to the prover;
  3. The verifier  $V'$  receives a single-qubit state from the prover, places it in the register  $\mathbf{Z}$ , and measures registers  $\mathbf{Z}$  and  $\mathbf{Z}'$  in the binary-valued measurement  $\{|\gamma\rangle\langle\gamma|, I - |\gamma\rangle\langle\gamma|\}$ , where  $|\gamma\rangle := \sqrt{1-\alpha}|00\rangle + \sqrt{\alpha}|11\rangle$ . The verifier  $V'$  accepts if the measurement outcome is consistent with  $|\gamma\rangle$ ; otherwise, it rejects.
- 

Next, we establish the correctness of Protocol 3.1:

- For *yes* instances, the state of the total system after step 2 can be adjusted with the help of an honest prover to

$$|\Phi\rangle = \sqrt{1-\alpha}|00\rangle_{\mathbf{Z}'\mathbf{Z}}|\phi_0\rangle + \sqrt{\alpha}|11\rangle_{\mathbf{Z}'\mathbf{Z}}|\phi_1\rangle,$$

where  $|\phi_0\rangle$  and  $|\phi_1\rangle$  are normalized states that may not be orthogonal. This adjustment can be done because  $c \geq \alpha$ . The prover then applies a unitary  $U$  on all the qubits except  $\mathbf{Z}'$  (which are owned by the prover) to “disentangle”  $|\Phi\rangle$ :

$$(I_{\mathbf{Z}'} \otimes U)|\Phi\rangle = (\sqrt{1-\alpha}|00\rangle_{\mathbf{Z}'\mathbf{Z}} + \sqrt{\alpha}|11\rangle_{\mathbf{Z}'\mathbf{Z}}) \otimes |\phi\rangle, \text{ where } |\phi\rangle \text{ is a normalized state.}$$

Consequently in Step 3, the verifier  $V'$  holds the state  $(\sqrt{1-\alpha}|00\rangle + \sqrt{\alpha}|11\rangle) = |\gamma\rangle$  in registers  $\mathbf{Z}$  and  $\mathbf{Z}'$ , ensuring that  $V'$  accepts with certainty.

- For *no* instances, the original proof system  $P \rightleftharpoons V$  accepts with probability at most  $s = \alpha - \varepsilon$  where  $\varepsilon \geq \frac{3c+s}{4} - s = \frac{3}{4}(c - s)$ . The reduced density matrix in the register  $\mathbf{Z}'$  after Step 2 is

$$\rho_{\mathbf{Z}'} = \begin{pmatrix} 1 - \alpha + \varepsilon & 0 \\ 0 & \alpha - \varepsilon \end{pmatrix}.$$

Let  $\sigma_{\mathbf{ZZ}'}$  denote a two-qubit quantum state in registers  $(\mathbf{Z}, \mathbf{Z}')$  after the verifier  $V'$  receives the single-qubit state from the prover  $P'$  in Step 3. Regardless of the prover's actions,  $V'$

accepts with probability

$$\begin{aligned}
\text{Tr}(|\gamma\rangle\langle\gamma|\sigma_{ZZ'}) &= \text{F}(|\gamma\rangle\langle\gamma|, \sigma_{ZZ'})^2 \\
&\leq \text{F}(\text{Tr}_Z(|\gamma\rangle\langle\gamma|), \rho_{Z'})^2 \\
&= \text{F}\left(\begin{pmatrix} 1-\alpha & 0 \\ 0 & \alpha \end{pmatrix}, \begin{pmatrix} 1-\alpha+\varepsilon & 0 \\ 0 & \alpha-\varepsilon \end{pmatrix}\right)^2 \\
&\leq 1 - \varepsilon^2 \\
&\leq 1 - \frac{1}{2}(c-s)^2.
\end{aligned}$$

Here, the second line owes to the data-processing inequality for the fidelity (Lemma 2.5), the fourth line follows from [VW16, Equation (4.25)], and the last line is because of

$$1 - \varepsilon^2 \leq 1 - \left(\frac{3(c-s)}{4}\right)^2 \leq 1 - \frac{1}{2}(c-s)^2. \quad \square$$

### 3.2.2 Error reduction for QIPL and QIP<sub>UL</sub>

The main challenge in performing sequential repetition of a given QIPL or QIP<sub>UL</sub> proof system  $P \rightleftharpoons V$  lies in resetting the qubits in the verifier's private register  $W$  to the all-zero state after each execution of  $P \rightleftharpoons V$ . In non-interactive proof systems with a unitary logspace verifier, the reset-to-zero operation can be achieved by running the inverse of the verification circuit, as shown in [MW05, FKL<sup>+</sup>16]. However, in interactive proof systems with a restricted logspace verifier – whether unitary or almost-unitary – the reset-to-zero operation requires assistance from the prover,<sup>26</sup> who may not be honest. We now proceed to the formal statement:

**Lemma 3.10** (Error reduction for QIPL and QIP<sub>UL</sub>). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable functions such that  $0 \leq s(n) < c(n) \leq 1$ ,  $c(n) - s(n) \geq 1/\text{poly}(n)$ , and  $1 \leq m(n) \leq \text{poly}(n)$ . For any polynomial  $k(n)$ , it holds that*

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

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

*Proof.* Since QIP<sub>UL</sub> proof systems are a special subclass of QIPL proof systems, it suffices to establish the inclusion for the latter. For any  $m$ -turn proof system  $P' \rightleftharpoons V'$  with completeness  $c$  and soundness  $s$ , corresponding to a promise problem  $\mathcal{I}$  in  $\text{QIPL}_m[c, s]$ , applying Lemma 3.9 yields a new  $(m+2)$ -turn proof system  $P \rightleftharpoons V$  with completeness 1 and soundness  $1 - (c-s)^2/2$ . This proof system  $P \rightleftharpoons V$ , viewed as an isometric quantum circuit, acts on registers  $Q$ ,  $M$ , and  $W = (Z, R)$ , where  $Z$  denotes the output qubit just before the final measurement. Without loss of generality, we can assume that registers  $M$  and  $V$  are of equal size.

Error reduction for the given proof system  $P \rightleftharpoons V$  is achieved using  $r$ -fold AND-type sequential repetition of  $P \rightleftharpoons V$ , as detailed in Protocol 3.2. In this resulting proof system  $\widehat{P} \rightleftharpoons \widehat{V}$ , we introduce two new  $\lceil \log r \rceil$ -qubit registers,  $\widehat{S}$  and  $\widehat{T}$ , which are initialized to be the all-zero state and are private to  $\widehat{V}$ . The procedure from Step 3.a to Step 3.c aims to reset the verifier's original private register  $W$  with the help of the prover. Moreover, the multiple-controlled adder in Step 3.b can be implemented by  $O(q_W^2)$  uses of elementary quantum gates and the adder  $U_{\text{add}}$ , following from [BBC<sup>+</sup>95, Lemma 7.5 and Corollary 7.6].

A subtle but important point concerns the effect of the environment register  $E_j$  introduced by the verifier's  $j$ -th action for  $j \in [(m+1)/2] + 1$  in  $P \rightleftharpoons V$ . Since  $E_j$  is measured at the end

<sup>26</sup>In the case of QIPL<sup>o</sup> proof systems, where the verifier's actions are isometric quantum circuits, implementing the reset-to-zero operation becomes straightforward. However, for QIPL proof systems, the  $O(\log n)$  pinching intermediate measurements conducted during each verifier action are insufficient for re-using the workspace qubits. This limitation arises because the measurement outcome yields merely a binary string encoded in a state.

of the turn in which it is introduced, it collapses to a state that contains only a binary string and becomes inaccessible afterward. Therefore, this newly introduced register  $E_j$  has no impact on our sequential repetition protocol.

---

**Protocol 3.2:** Error reduction for QIPL (or QIP<sub>UL</sub>) via sequential repetition.

---

**Parameters:**  $r := O(k/(c-s)^2)$ .

**For**  $i \leftarrow 1$  **to**  $r$  :

1. The verifier  $\widehat{V}$  executes the original proof system  $P \rightleftharpoons V$  (with the prover  $\widehat{P}$ ), except for the verifier's final measurement on the register  $Z$ ;
2. The verifier  $\widehat{V}$  performs a controlled adder, where the single-qubit control register is  $\widehat{Z}$ , and the  $\lceil \log r \rceil$ -qubit target register is  $\widehat{S}$ ;

**If**  $i < r$  :

- 3.a The prover  $\widehat{P}$  sends a  $q_W$ -qubit state  $|O\rangle$  to the verifier  $\widehat{V}$ , where  $|O\rangle = |0\rangle^{\otimes q_W}$  for an honest prover;
- 3.b The verifier  $\widehat{V}$  performs a multiple-controlled adder, where the  $q_W$ -qubit control register is  $\widehat{M}$  (containing  $|O\rangle$ ), the  $\lceil \log r \rceil$ -qubit target register is  $\widehat{T}$ , and the adder is activated if  $|O\rangle = |0\rangle^{\otimes q_W}$ ;
- 3.c The verifier  $\widehat{V}$  performs a SWAP gate between registers  $\widehat{M}$  and  $\widehat{W}$ ;

4. The verifier  $\widehat{V}$  measures the registers  $\widehat{S}$  and  $\widehat{T}$  in the computational basis, with the outcomes denoted as  $\text{Cnt}_{\text{acc}}$  and  $\text{Cnt}_{\text{clean}}$ , respectively;
  5. The verifier  $\widehat{V}$  accepts if both  $\text{Cnt}_{\text{clean}} = r - 1$  and  $\text{Cnt}_{\text{acc}} = r$  are satisfied.
- 

It remains to establish the correctness of  $\widehat{P} \rightleftharpoons \widehat{V}$ . Let  $X_i$  be a random variable indicating whether the  $i$ -th execution of  $P \rightleftharpoons V$  is accepted, with  $\Pr[X_i = 1]$  denoting the verifier  $V$ 's maximum acceptance probability of the  $i$ -th execution. By a direct calculation, it holds that

$$\Pr[\text{Cnt}_{\text{acc}} = r] = \Pr[X_1 = 1 \wedge \dots \wedge X_r = 1] = \Pr[P \rightleftharpoons V \text{ accepts}]^r. \quad (3.1)$$

As a consequence, we conclude the following:

- For *yes* instances, an honest prover always sends  $|O\rangle = |0\rangle^{\otimes q_W}$ , and runs each of the executions independently, ensuring that the condition  $\text{Cnt}_{\text{clean}} = r - 1$  is satisfied. By combining Equation (3.1) with the completeness condition of  $P \rightleftharpoons V$ , it follows that Protocol 3.2 accepts with certainty.
- For *no* instances, it is enough to analyze the acceptance probability when the prover always sends  $|0\rangle^{\otimes q_W}$  at Step 3.a, as the verifier will otherwise reject. Although the random variables  $X_i$  may not be independent, the probability of  $X_i = 1$  is at most  $1 - (c-s)^2/2$  for any prover. Therefore, we can upper bound the acceptance probability using independent binary random variables  $X'_i$ , where the probability of  $X'_i = 1$  is  $1 - (c-s)^2/2$ . Consequently, applying Equation (3.1) (by substituting  $X_i$  with  $X'_i$ ), we can obtain that Protocol 3.2 accepts with probability at most  $2^{-k}$  by choosing  $r = O\left(k/\log \frac{1}{1-(c-s)^2/2}\right)$ . This choice results in  $m' = r(m+2) = O\left(km/\log \frac{1}{1-(c-s)^2/2}\right)$ .  $\square$

### 3.3 A upper bound for QIPL

We begin with the upper bound for the class QIPL:<sup>27</sup>

---

<sup>27</sup>It is noteworthy that this upper bound also applies to a variant of QIPL in which the verifier's mapping satisfies a weaker notion of uniformity (see Footnote 23 for details).

**Theorem 3.11** (QIPL is in SBP). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable functions such that  $0 \leq s(n) < c(n) \leq 1$ ,  $c(n) - s(n) \geq 1/\text{poly}(n)$ , and  $1 \leq m(n) \leq \text{poly}(n)$ , it holds that*

$$\text{QIPL}_m[c, s] \subseteq \text{SBP}.$$

Before presenting the proof, we introduce the term *snapshot registers* to refer to the registers  $Q$ ,  $M$ , and  $W$  after each turn in a QIPL proof system. We also refer to the quantum state within these snapshot registers as *snapshot states*. For example, the snapshot registers corresponding to  $W$  at distinct time points are  $W_0, \dots, W_l$ , as illustrated in Figure 3.1. More precisely, for an  $l$ -round (i.e.,  $2l$ -turn) QIPL proof system, we define the following:

- (1)  $Q_0$ ,  $M_0$ , and  $W_0$ , which contain the all-zero state, are the snapshot registers of registers  $Q$ ,  $M$ , and  $W$ , respectively, before the protocol begins;
- (2)  $M_j$  and  $W_j$  ( $1 \leq j \leq l$ ) are the snapshot registers of the registers  $M$  and  $W$ , respectively, after the verifier sends the message in the  $j$ -th round;
- (3)  $M'_j$  and  $W_j$  ( $1 \leq j \leq l$ ) are the snapshot registers of the registers  $M$  and  $W$ , respectively, after the verifier receives the message from the prover in the  $j$ -th round;
- (4)  $Q_j$  ( $1 \leq j \leq l$ ) is the snapshot registers of the register  $Q$  immediately after applying the prover's  $j$ -th action  $P_j$ , i.e., after the prover sends the message in the  $j$ -th round;
- (5)  $(Z, R)$  represents the snapshot registers of registers  $M$  and  $W$ , respectively, just before the verifier performs the final measurement, where  $Z$  corresponds to the designated output qubit of the verifier and  $R$  contains the remained qubits.

In the remainder of this subsection, we first present semi-definite programming (SDP) formulations for QIPL proof systems in Section 3.3.1, and then establish an upper bound for QIPL (Theorem 3.11) in Section 3.3.2.

### 3.3.1 Semi-definite program formulations for QIPL proof systems

To establish upper bounds for space-bounded (unitary) quantum interactive proofs, a commonplace approach involves solving the optimization problem of approximating the maximum acceptance probability of a QIPL and QIP<sub>UL</sub> proof system over all prover strategies. For clarity, we first present an SDP for characterizing QIPL proof systems (Lemma 3.12), directly extended from [VW16, Section 4.3] and [Wat16a, Section 4]. Next, we introduce another SDP characterization (Lemma 3.14) that fully incorporates all restrictions of QIPL proof systems.

**First SDP formulation for QIPL proof systems.** For an  $m$ -turn QIPL proof system with even  $m$ ,<sup>28</sup> we formulate this optimization problem as a semi-definite program (SDP) from the verifier's perspective, following the approach described in [VW16, Section 4.3]:

**Lemma 3.12** (First SDP formulation for QIPL proof systems). *For any  $l(n)$ -round space-bounded quantum interactive proof system  $P \rightleftharpoons V$  with completeness  $c(n)$ , soundness  $s(n)$ , which corresponds to a promise problem  $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$  in  $\text{QIPL}_{2l}[c, s]$ , there is an SDP program to*

---

<sup>28</sup>Adapting the proof to the case of odd  $m$  is straightforward, so we omit the details.

compute the maximum acceptance probability  $\omega(V)$  of the proof system  $P \rightleftharpoons V$ :

$$\begin{aligned}
& \text{maximize} && \omega(V) = \text{Tr}\left(\tilde{V}_{l+1}^\dagger |1\rangle\langle 1|_{\text{out}} \tilde{V}_{l+1} \rho_{M'_l W_l E_1 \dots E_l}\right) \\
& \text{subject to} && \text{Tr}_{M'_1}(\rho_{M'_1 W_1 E_1}) = \text{Tr}_{M_1}\left(V_1 |\bar{0}\rangle\langle \bar{0}|_{M_0 W_0} V_1^\dagger\right), \\
& && \text{Tr}_{M'_j}(\rho_{M'_j W_j E_1 \dots E_j}) = \text{Tr}_{M_j}\left(\tilde{V}_j \rho_{M'_{j-1} W_{j-1} E_1 \dots E_{j-1}} \tilde{V}_j^\dagger\right), \quad j \in [l] \setminus [1], \\
& && \text{Tr}(\rho_{M'_j W_j E_1 \dots E_j}) = 1, \quad j \in [l], \\
& && \rho_{M'_j W_j E_1 \dots E_j} \succeq 0, \quad j \in [l]
\end{aligned} \tag{3.2}$$

Here, the verifier's actions  $V_1, \dots, V_{l+1}$  are considered space-bounded isometric quantum circuits, with the notation  $\tilde{V}_j := V_j \otimes I_{E_1 \dots E_{j-1}}$  for each  $j \in [l+1] \setminus [1]$ . The variables in this SDP are  $\rho_{M'_1 W_1 E_1}, \dots, \rho_{M'_l W_l E_1 \dots E_l}$ , collectively holding  $O(l^2(n) \cdot \log n)$  qubits.

*Remark 3.13* (The applicability of the first SDP formulation for QIPL). The SDP program in Equation (3.2) essentially characterizes QIPL $^\diamond$  proof systems, which are informally defined in Remark 3.8 as a *reversible* generalization of QIPL, where the verifier's actions are *isometric* quantum circuits. Additionally, by disregarding all environment registers  $\{E_j\}$  in Equation (3.2), we immediately obtain an SDP formulation for QIPL $_{\text{U}}$  proof systems, where the variables are  $\rho_{M'_1 W_1}, \dots, \rho_{M'_l W_l}$ , collectively holding  $O(l(n) \cdot \log n)$  qubits.

Our SDP program in Equation (3.2) consists of two types of constraints, both of which can be described by simple equations: (1) the verifier remains honest, and (2) the prover's actions do not interfere with the verifier's private qubits. Importantly, every feasible solution to Equation (3.2) corresponds to a valid strategy for the prover. We now proceed with the detailed proof:

*Proof of Lemma 3.12.* For any  $m(n)$ -turn proof system  $P \rightleftharpoons V$ , with completeness  $c$ , soundness  $s$ , and  $m$  being even, which corresponds to a promise problem  $\mathcal{I}$  in QIPL $_m[c, s]$ , we consider the verifier's maximum acceptance probability  $\omega(V)$  as the objective function to be maximized. In our SDP formulation for the QIPL proof system  $P \rightleftharpoons V$ , we focus on the verifier's actions (e.g.,  $V_j$ ), specifically isometric quantum circuits that do not measure the new environment register (e.g.,  $E_j$ ) at the end. As defined in Section 3.1, the verifier  $V$  is described by an  $(l+1)$ -tuple  $(V_1, \dots, V_{l+1})$  of space-bounded unitary quantum circuits  $\{V_j\}_{j \in [l+1]}$ , where  $l = m/2$ .

To represent the variables in our SDP program, which are the states in the snapshot registers corresponding to the message register  $M$ , the verifier's private register  $W$ , and the environment registers  $E_1 \dots, E_j$  after the verifier's  $j$ -th action in  $P \rightleftharpoons V$ , we use the notations defined in Figure 3.1. Specifically, let  $\rho_{M'_j W_j E_1 \dots E_j}$  denote the state in the snapshot registers  $(M'_j, W_j, E_1, \dots, E_j)$ . Similarly, we can define snapshot states  $\rho_{M'_j W_j E_1 \dots E_j}$  for  $j \in [l]$  and  $\rho_{ZRE_1 \dots E_{l+1}}$  accordingly.

Assuming that  $P \rightleftharpoons V$  begins with the verifier, it follows that the objective function

$$\begin{aligned}
\omega(V) &= \|\lvert 1 \rangle \langle 1 \rvert_{\text{out}} V_{l+1} P_l V_l \dots P_1 V_1 \lvert \bar{0} \rangle_{Q_0, M_0, W_0}\|_2^2 \\
&= \text{Tr}\left(\text{Tr}_Q\left((V_{l+1} P_l V_l \dots P_1 V_1)^\dagger \lvert 1 \rangle \langle 1 \rvert_{\text{out}} (V_{l+1} P_l V_l \dots P_1 V_1) \lvert \bar{0} \rangle \langle \bar{0} \rvert_{Q_0, M_0, W_0}\right)\right) \\
&= \text{Tr}\left((V_{l+1}^\dagger \otimes I_{E_1 \dots E_l}) \lvert 1 \rangle \langle 1 \rvert_{\text{out}} (V_{l+1}^\dagger \otimes I_{E_1 \dots E_l}) \rho_{M'_l W_l E_1 \dots E_l}\right)
\end{aligned} \tag{3.3}$$

Noting that the verifier  $V$  remains honest and the verifier's  $j$ -th action does not act on the environment registers  $E_1, \dots, E_{j-1}$ , we obtain the first type of constraints:

$$\begin{aligned}
\rho_{M_1 W_1 E_1} &= V_1 \rho_{M_0 W_0} V_1^\dagger = V_1 \lvert \bar{0} \rangle \langle \bar{0} \rvert_{M_0 W_0} V_1^\dagger; \\
\forall j \in \{2, \dots, l\}, \rho_{M'_j W_j E_1 \dots E_j} &= (V_j \otimes I_{E_1 \dots E_{j-1}}) \rho_{M'_{j-1} W_{j-1} E_1 \dots E_{j-1}} (V_j^\dagger \otimes I_{E_1 \dots E_{j-1}}); \\
\rho_{ZRE_1 \dots E_{l+1}} &= (V_{l+1} \otimes I_{E_1 \dots E_l}) \rho_{M'_l W_l E_1 \dots E_l} (V_{l+1}^\dagger \otimes I_{E_1 \dots E_l}).
\end{aligned} \tag{3.4}$$

Since the prover's actions are described by unitary quantum circuits and the verifier's actions



by isometric quantum circuits, all intermediate states in  $(Q, M, W, E_1, \dots, E_j)$  after the verifier's  $j$ -th action in  $P \rightleftharpoons V$  are pure states. These states, denoted by  $|\psi\rangle_{Q_{j-1}M_jW_jE_1\dots E_j}$  and  $|\phi\rangle_{Q_jM'_jW_jE_1\dots E_j}$  for  $j \in [l]$ , satisfy the relation  $|\phi\rangle_{Q_jM'_jW_jE_1\dots E_j} = P_j|\psi\rangle_{Q_{j-1}M_jW_jE_1\dots E_j}$ . By the unitary freedom in purifications (Lemma 2.7), we have:

$$\forall j \in [l], \text{Tr}_{Q_{j-1}M_j}(|\psi\rangle\langle\psi|_{Q_{j-1}M_jW_jE_1\dots E_j}) = \rho_{W_jE_1\dots E_j} = \text{Tr}_{Q_jM'_j}(|\phi\rangle\langle\phi|_{Q_jM'_jW_jE_1\dots E_j}).$$

Here, the underlying unitary transformation corresponds to the prover's action  $P_j$  in the  $j$ -th round. As a consequence, the prover's actions do not interfere with the verifier's private register  $W$  or the environment registers  $E_1, \dots, E_j$  (after the verifier's  $j$ -th action) during the execution of  $P \rightleftharpoons V$ . This property leads to the second type of constraints:

$$\forall j \in [l], \text{Tr}_{M_j}(\rho_{M_jW_jE_1\dots E_j}) = \text{Tr}_{M'_j}(\rho_{M'_jW_jE_1\dots E_j}). \quad (3.5)$$

Putting Equation (3.3), Equation (3.4), and Equation (3.5) all together, we conclude our SDP formulation for the given QIPL proof system  $P \rightleftharpoons V$ , as detailed in Equation (3.2).  $\square$

**Second SDP formulation for QIPL proof systems.** The main challenge in fully utilizing all restrictions of QIPL proof systems in an SDP program is effectively using the measurement outcomes from the newly introduced environment register  $E_j$  after the verifier's  $j$ -th action. Specifically, when applying the principle of deferred measurements to the verifier's  $j$ -th action (almost-unitary quantum circuit), an environment register  $E_j$  is introduced. Thus, the variables in Equation (3.2) correspond to  $\rho_{M'_1W_1E_1}, \rho_{M'_1W_1E_1E_2}, \dots, \rho_{M'_lW_lE_1\dots E_l}$ . In general, when the verifier's actions are isometric quantum circuits, the environment registers  $E_1, \dots, E_l$  may be *entangled*.<sup>29</sup>

However, an almost-unitary quantum circuit (the verifier's  $j$ -th action) corresponds to a specific type of isometric quantum circuit, followed by measuring the environment register  $E_j$  in the computational basis at the end of the circuit. Since pinching measurements destroy coherence between subspaces associated with different measurement outcomes (see Remark 2.9(1)), the environment registers  $E_1, \dots, E_l$  remain *independent* in this restricted setting. Formally, let  $\omega(V)$  denote the maximum acceptance probability of the verifier  $V$  in the proof system  $P \rightleftharpoons V$ . We define  $\omega(V)|^u$  as the contribution of the measurement outcome  $u$  to  $\omega(V)$ , where all post-measurement states remain *unnormalized*. A direct calculation then implies that

$$\omega(V) = \sum_{u \in \{0,1\}^{q_{E_1} + \dots + q_{E_l}}} \omega(V)|^u. \quad (3.6)$$

Now we are ready to present the following SDP program:

**Lemma 3.14** (Second SDP formulation for QIPL proof systems). *For any  $l(n)$ -round space-bounded quantum interactive proof system  $P \rightleftharpoons V$  with completeness  $c(n)$  and soundness  $s(n)$ , corresponding to a promise problem  $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$  in  $\text{QIPL}_{2l}[c, s]$ , there is a family of SDP programs for computing the contribution  $\omega(V)|^u$  of the measurement outcome  $u = (u_1, \dots, u_l)$  to the maximum acceptance probability  $\omega(V)$  of the proof system  $P \rightleftharpoons V$ . Here, each  $u_j$  for  $j \in [l]$  is a measurement outcome from the environment register  $E_j$  following the verifier's  $j$ -th action.*

<sup>29</sup>For instance, the prover may send a highly-entangled  $n$ -qubit state  $\rho$  in  $n/\log n$  batches, each containing  $\log n$  qubits. In this case, the verifier keeps only  $O(\log n)$  qubits, which are not necessarily adjacent, and swaps the remaining qubits with fresh qubits in the environment registers.

Specifically, an SDP program for computing  $\omega(V)^u$  can be formulated as follows:

$$\begin{aligned}
& \text{maximize} && \omega(V)^u = \text{Tr}\left(V_{l+1}^\dagger |1\rangle\langle 1|_{\text{out}} V_{l+1} \rho_{M'_l W_l}\right) \\
& \text{subject to} && \text{Tr}_{M'_1}(\rho_{M'_1 W_1} \otimes |u_1\rangle\langle u_1|_{E_1}) = \text{Tr}_{M_1}\left((I_{M_1 W_1} \otimes |u_1\rangle\langle u_1|_{E_1}) V_1 |\bar{0}\rangle\langle \bar{0}|_{M_0 W_0} V_1^\dagger\right), \\
& && \text{Tr}_{M'_j}(\rho_{M'_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}) = \text{Tr}_{M_j}\left((I_{M_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}) V_j \rho_{M'_{j-1} W_{j-1}} V_j^\dagger\right), \quad j \in [l] \setminus [1], \\
& && \text{Tr}(\rho_{M'_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}) \leq 1, \quad j \in [l], \\
& && \rho_{M'_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j} \succeq 0, \quad j \in [l]
\end{aligned} \tag{3.7}$$

Here, the verifier's actions  $V_1, \dots, V_{l+1}$  correspond to space-bounded almost-unitary quantum circuits, which we interpret as a special class of isometric quantum circuits. The variables in this SDP are unnormalized states  $\rho_{M'_1 W_1}, \dots, \rho_{M'_l W_l}$ , collectively holding  $O(l(n) \cdot \log n)$  qubits.

*Proof.* Our proof strategy follows a similar approach to that of Lemma 3.12, so we will only highlight the key differences. As defined in Section 3.1, the verifier  $V$  is described by an  $(l+1)$ -tuple  $(V_1, \dots, V_{l+1})$  of space-bounded almost-unitary quantum circuits  $\{V_j\}_{j \in [l+1]}$ , which are a special class of isometric quantum circuits, where  $l = m/2$ .

To represent the variables in this SDP program, which are the *unnormalized* states in the snapshot registers corresponding to the message register  $M$  and the verifier's private register  $W$ , we use the notations from Figure 3.1. Assume that it suffices to consider the measurement outcome  $u_j$  obtained from measuring  $E_j$  in the computational basis at the end of the verifier's  $j$ -th action. Consequently, the state  $|u_j\rangle\langle u_j|$  in the environment register  $E_j$  is treated as part of the SDP constraints, not as the variables. In particular, we slightly abuse the notation by letting  $\rho_{M'_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}$  denote the unnormalized snapshot state in the registers  $(M, W, E_j)$  after the  $j$ -th verifier's action. Similarly, we define unnormalized snapshot states  $\rho_{M'_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}$  for  $1 \leq j \leq l$  and  $\rho_{ZRE_{l+1}}$  for the corresponding registers.

**Objective function and dependence on measurement outcomes.** Assuming that  $P \rightleftharpoons V$  begins with the verifier, it follows that the objective function is defined as

$$\omega(V)^u = \||1\rangle\langle 1|_{\text{out}} V_{l+1} P_l V_l \dots P_1 V_1 |\bar{0}\rangle_{Q_0 M_0 W_0}\|_2^2 = \text{Tr}\left(V_{l+1}^\dagger |1\rangle\langle 1|_{\text{out}} V_{l+1} \rho_{M'_l W_l}\right). \tag{3.8}$$

Noting that pinching measurements eliminate coherence between subspaces corresponding to different measurement outcomes  $\{u\}$ , it suffices to consider each outcome  $u_j$  independently. Here, each  $u_j$  arises from measuring  $E_j$  for  $j \in [l]$ , along with the unnormalized resulting state in the registers  $(Q, M, W)$  after these pinching intermediate measurements.

**Constraints.** Note that the verifier  $V$  remains honest, with the initial state given by  $\rho_{M_0 W_0} = |\bar{0}\rangle\langle \bar{0}|_{M_0 W_0}$ . The first type of constraints arises from applying the verifier's action  $V_j$ :

$$\begin{aligned}
& \rho_{M_1 W_1} \otimes |u_1\rangle\langle u_1|_{E_1} = (I_{M_1 W_1} \otimes |u_1\rangle\langle u_1|_{E_1}) V_1 |\bar{0}\rangle\langle \bar{0}|_{M_0 W_0} V_1^\dagger; \\
& \forall j \in \{2, \dots, l\}, \rho_{M'_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j} = (I_{M'_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}) V_j \rho_{M'_{j-1} W_{j-1}} V_j^\dagger; \\
& \rho_{ZRE_{l+1}} = V_{l+1} \rho_{M'_l W_l} V_{l+1}^\dagger.
\end{aligned} \tag{3.9}$$

Since the prover's actions are described by unitary quantum circuits, and the verifier's  $j$ -th action is an isometric quantum circuit, followed by measuring the (newly introduced) environment register  $E_j$  at the end of this turn, all intermediate states in  $(Q, M, W, E_j)$  after the verifier's  $j$ -th action in  $P \rightleftharpoons V$  are pure states. These unnormalized states, denoted by  $|\psi\rangle_{Q_{j-1} M_j W_j} \otimes |u_j\rangle_{E_j}$  and  $|\phi\rangle_{Q_j M'_j W_j} \otimes |u_j\rangle_{E_j}$  for  $j \in [l]$ , satisfy the relation  $|\phi\rangle_{Q_j M'_j W_j} \otimes |u_j\rangle_{E_j} = P_j |\psi\rangle_{Q_{j-1} M_j W_j} \otimes |u_j\rangle_{E_j}$ . By the unitary freedom in purifications (Lemma 2.7), it follows that:

$$\forall j \in [l], \text{Tr}_{Q_{j-1} M_j}(|\psi\rangle\langle \psi|_{Q_{j-1} M_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}) = \rho_{W_j} \otimes |u_j\rangle\langle u_j|_{E_j} = \text{Tr}_{Q_j M'_j}(|\phi\rangle\langle \phi|_{Q_j M'_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}).$$

Here, the underlying unitary transformation corresponds to the prover's action  $P_j$  in the  $j$ -th round. Consequently, the prover's actions do not interfere with the verifier's private register  $W$  or the environment register  $E_j$  (introduced by the verifier's  $j$ -th action) during the execution of  $P \rightleftharpoons V$ . This property gives rise to the second type of constraints:

$$\forall j \in [l], \operatorname{Tr}_{M_j}(\rho_{M_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}) = \operatorname{Tr}_{M'_j}(\rho_{M'_j W_j} \otimes |u_j\rangle\langle u_j|_{E_j}). \quad (3.10)$$

Replacing the constraints in Equation (3.2) by Equation (3.9) and Equation (3.10), we conclude the second SDP formulation for the given QIPL protocol, as specified in Equation (3.7).  $\square$

### 3.3.2 QIPL is in SBP

To establish that  $\text{QIPL} \subseteq \text{SBP}$  (Theorem 3.11), we approximate the maximum acceptance probability  $\omega(V)$  by relating it to an instance of the *existential* variant of the SET SIZE ESTIMATION PROBLEM (SSE). A key ingredient in this approach is the feasibility of our second SDP formulation for QIPL proof systems (Lemma 3.14). As Existential SSE is in SBP [BGM06, Wat16b], this achieves the desired containment. We now proceed with the proof.

*Proof of Theorem 3.11.* Without loss of generality, we assume that the number of turns  $m'(n)$  is even, and particularly  $m'(n) = 2l'(n)$ . For any  $l'$ -round proof system  $P' \rightleftharpoons V'$  with completeness  $c$  and soundness  $s$ , corresponding to a promise problem  $\mathcal{I}$  in  $\text{QIPL}_{2l'}[c, s]$ , we obtain an  $l$ -round proof system  $P \rightleftharpoons V$  with completeness 1 and soundness  $1/4$  via error reduction for QIPL (Lemma 3.10), where  $l = O(l' / \log \frac{1}{1-(c-s)^2/2})$ .

Our goal is to approximate the maximum acceptance probability  $\omega(V)$  of the proof system  $P \rightleftharpoons V$ . Since the promise problem SSE is in SBP (Lemma 2.16) and SBP is closed under nondeterminism (Lemma 2.17), it suffices to construct a set  $S$  along with an efficiently verifiable membership oracle  $\mathcal{O}_S$  that operates using a witness string  $w_S$ . There exists an efficiently computable positive integer function  $t(n)$  such that

$$\begin{aligned} \omega(V) = 1 &\Rightarrow |S| \geq t(n), \\ \omega(V) \leq 1/4 &\Rightarrow |S| \leq t(n)/2. \end{aligned}$$

**Construing the membership oracle  $\mathcal{O}_S$ .** For any  $1 \leq j \leq l$ , let  $u_j$  denote the intermediate measurement outcome obtained during the verifier's  $j$ -th action. The total number of bits required to describe all intermediate measurement outcomes  $u_1, \dots, u_l$  during the execution of  $P \rightleftharpoons V$  is given by  $\ell_{\text{tot}} = \sum_{1 \leq j \leq l} |u_j|$ . Recall that  $u := (u_1, \dots, u_l)$ , the set  $S$  consists of elements of the form  $(u, \iota_1, \dots, \iota_{2\ell_{\text{tot}}})$  such that the size  $|S|$  is approximately proportional to  $\omega(V)$ . Equivalently, for any given  $u$ , it holds that:

$$\frac{1}{2^{2\ell_{\text{tot}}}} \sum_{\iota_1, \dots, \iota_{2\ell_{\text{tot}}} \in \{0,1\}} \mathcal{O}_S((u, \iota_1, \dots, \iota_{2\ell_{\text{tot}}}), w_S) \in \left[ \omega(V)^{|u|} - \frac{1}{2^{2\ell_{\text{tot}}}}, \omega(V)^{|u|} + \frac{1}{2^{2\ell_{\text{tot}}}} \right]. \quad (3.11)$$

Here, the witness string  $w_S$  represents the classical description of the unnormalized states  $\rho_{M'_1 W_1}, \dots, \rho_{M'_l W_l}$ . The size of  $w_S$  remains polynomial in  $n$  for the following reasons: (i) the dimension of each unnormalized state  $\rho_{M'_j W_j}$ , for  $1 \leq j \leq l$ , is at most  $2^{O(\log n)}$ , which is polynomial in  $n$ ; (ii) the length of each binary string  $u_j$  is bounded by  $O(\log n)$ ; and (iii) the number of rounds  $l(n)$  is at most  $\text{poly}(n)$ . We next describe the membership oracle  $\mathcal{O}_S$  using our second SDP formulation for QIPL proof systems (Lemma 3.14), as detailed in Algorithm 3.3.

It is evident that all steps in Algorithm 3.3 can be accomplished in deterministic polynomial time. Using the guarantee in Equation (3.11) provided by Algorithm 3.3, we proceed with the following analysis concerning the set size  $|S|$ :

---

**Algorithm 3.3:** Implementation of the membership oracle  $\mathcal{O}_S(u, \iota_1, \dots, \iota_{2\ell_{\text{tot}}}, w_S)$ .

---

**Parameters:** the witness string  $w_S$ , the intermediate measurement outcomes

$$u \in \{0, 1\}^{\ell_{\text{tot}}}, \text{ and } \iota_1, \dots, \iota_{2\ell_{\text{tot}}} \in \{0, 1\}.$$

1. Check whether  $w_S$  represents a feasible solution to the SDP program for computing  $\omega(V)^u$ , as specified in Equation (3.7), which results from applying Lemma 3.14 to the proof system  $P \rightleftharpoons V$ . Return 0 if  $w_S$  is not a feasible solution.
  2. Compute the value of  $\omega(V)^u$  using  $u$  and  $w_S$  to with precision  $2^{-2\ell_{\text{tot}}}$ , denoted as  $\widehat{\omega}(V)^u$ , by performing a polynomial number of matrix multiplications and partial traces of matrices with polynomial dimensions.
  3. Return 1 if  $\widehat{\omega}(V)^u > 0$  and  $\widehat{\omega}(V)^u \geq \sum_{1 \leq j \leq 2\ell_{\text{tot}}} 2^{-j} \iota_j$ , otherwise return 0.
- 

- For *yes* instances, where  $\omega(V) = 1$ , it holds that

$$\frac{|S|}{2^{2\ell_{\text{tot}}}} = \sum_u \widehat{\omega}(V)^u \geq \sum_u \left( \omega(V)^u - \frac{1}{2^{2\ell_{\text{tot}}}} \right) = \omega(V) - \frac{1}{2^{2\ell_{\text{tot}}}} = 1 - \frac{1}{2^{2\ell_{\text{tot}}}} := t_{\text{yes}}(\ell_{\text{tot}}). \quad (3.12)$$

- For *no* instances, where  $\omega(V) \leq 1/4$ , it follows that

$$\frac{|S|}{2^{2\ell_{\text{tot}}}} = \sum_u \widehat{\omega}(V)^u \leq \sum_u \left( \omega(V)^u + \frac{1}{2^{2\ell_{\text{tot}}}} \right) = \omega(V) + \frac{1}{2^{2\ell_{\text{tot}}}} \leq \frac{1}{4} + \frac{1}{2^{2\ell_{\text{tot}}}} := t_{\text{no}}(\ell_{\text{tot}}). \quad (3.13)$$

Combining Equations (3.12) and (3.13), a straightforward calculation implies that the function  $f(\ell_{\text{tot}}) := t_{\text{yes}}(\ell_{\text{tot}})/t_{\text{no}}(\ell_{\text{tot}})$  is monotonically increasing for any  $\ell_{\text{tot}} \geq 0$ . Therefore, we conclude the proof by noting that  $f(\ell_{\text{tot}}) \geq f(3) = 7/3 > 2$  for  $\ell_{\text{tot}} \geq 3$ , and consequently, the efficiently computable positive integer function  $t(n)$  exists as desired.  $\square$

### 3.4 Lower bounds for QIPL and QIP<sub>UL</sub>

Our lower bounds for QIPL and QIP<sub>UL</sub> are motivated by the prior works on space-bounded classical interactive proofs, particularly those involving either private coins [CL95] or public coins [For89, FL93, Con92, GKR15, CR23]:<sup>30</sup>

- **Private-coin proof systems vs. QIPL:** Soundness against classical messages may not extend to quantum messages for private-coin proof systems. This is because the prover could generate shared entanglement with the verifier, potentially leaking information about the private coins. Consequently, space-bounded private-coin classical interactive proofs are simulatable only by QIPL proof systems (Theorem 3.15).
- **Public-coin proof systems vs. QIP<sub>UL</sub>:** Public coins can be simulated by halves of EPR pairs sent from the verifier in QIP<sub>UL</sub> proof systems, thus avoiding the soundness issue. However, the verifier is limited to sending only  $O(\log n)$  halves of EPR pairs, leading to a limitation on completeness. Therefore, only the work of [For89] can be simulated by QIP<sub>UL</sub> proof systems (Lemma 3.16 and thus Theorem 3.4).

In the remainder of this subsection, we first establish that  $\text{NP} \subseteq \text{QIPL}$  in Section 3.4.1, and then demonstrate that  $\text{SAC}^1 \cup \text{BQL} \subseteq \text{QIP}_{\text{UL}}$  in Section 3.4.2.

#### 3.4.1 NP is in QIPL

Our approach in Theorem 3.15 draws inspiration from [CL95, Lemma 2]. Soundness against classical messages is guaranteed by *the fingerprinting lemma* [Lip90], which is used for comparing multisets through short fingerprints (see Section 2.4). To ensure soundness against quantum

---

<sup>30</sup>Space-bounded classical interactive proofs with  $\text{poly}(n)$  public coins are in  $\text{P}$ , see [Con92, Theorem 6].

messages in private-coin proof systems, the verifier must measure the received quantum message in the computational basis at the beginning of each action.

**Theorem 3.15.**  $\text{NP} \subseteq \text{QIPL}_m$ , where  $m(n)$  is some polynomial in  $n$ .

*Proof.* We begin by noting that 3-SAT is NP-hard under logspace reductions (Lemma 2.12), and QIPL is closed under logspace reductions.<sup>31</sup> It suffices to establish that 3-SAT is in QIPL.

To verify whether a 3-SAT instance  $\phi = C_1 \wedge \cdots \wedge C_k$  is satisfied by an assignment  $\alpha$ , we encode  $\phi(\alpha)$  as a collection of  $3k$  tuples  $(l, i, v)$ , denoted as  $\text{Enc}(\phi(\alpha))$ . In this encoding, each  $(l, i, v)$  represents the literal  $l \in \{x_j\}_{j \in [n]} \cup \{\neg x_j\}_{j \in [n]}$  in the clause  $C_i$  is assigned the value  $v \in \{\top, \perp\}$ . Hence,  $\text{Enc}(\phi(\alpha))$  forms a multiset of  $\ell = 3k$  elements, with each element representable by  $b = 2\lceil \log n \rceil + \lceil \log k \rceil + 1 = O(\log(kn))$  bits. For convenience, let  $a_{(l,i,v)}$  denote the non-negative integer that encodes the triple  $(l, i, v)$ , and let  $\text{var}(l)$  be the variable in the literal  $l$ . Next, we proceed with the detailed QIPL protocol, as outlined in Protocol 3.4.

---

**Protocol 3.4:** A QIPL proof system for 3-SAT.

---

**Parameters:**  $\phi(\alpha)$  is a 3-SAT formula  $\phi$  with an assignment  $\alpha$ ;  $n$  and  $k$  are the number of variables and clauses in  $\phi$ , respectively.

1. The verifier  $V$  chooses a prime  $p$  and an integer  $r$  uniformly at random from the intervals  $[(b\ell)^2, 2(b\ell)^2]$  and  $[1, p-1]$ , respectively. The verifier then initializes the (partial) fingerprints  $F_{\text{var}} = 1$  and  $F_{\text{cl}} = 1$ .
  2. CONSISTENCY CHECK (for each variable) :
    - The prover  $P$  sends the triples  $(l, i, v)$  in  $\text{Enc}(\phi(\alpha))$ , represented as quantum states  $|\psi_{\text{var}(l), C_i}\rangle$ , to the verifier  $V$ , ordered by the variable  $\text{var}(l)$  in the literal  $l$  and then by the clause index  $i$ ;
    - For each state  $|\psi_{\text{var}(l), C_i}\rangle$  received :
      - 2.a  $V$  measures the state  $|\psi_{\text{var}(l), C_i}\rangle$  in the computational basis, with the measurement outcome denoted by the triple  $(l, i, v)$ ;
      - 2.b  $V$  rejects if the following conditions hold: (i)  $(l, i, v)$  is not the first triple in  $\text{Enc}(\phi(\alpha))$ , (ii)  $\text{var}(l) = \text{var}(l')$ , and (iii) the value  $v$  and  $v'$  are inconsistent;
      - 2.c  $V$  updates the fingerprint  $F_{\text{var}} = F_{\text{var}} \cdot (a_{(l,i,v)} + r) \pmod p$ ;
      - 2.d  $V$  sends the previous triple  $(l', i', v')$  back to  $P$ , if applicable.  $V$  then retains the current triple  $(l, i, v)$  in its private memory, unless  $(l, i, v)$  is the last triple in  $\text{Enc}(\phi(\alpha))$ .
  3. SATISFIABILITY CHECK (for each clause) :
    - The prover  $P$  sends the triples  $(l_1, i, v_1)$ ,  $(l_2, i, v_2)$ , and  $(l_3, i, v_3)$  in  $\text{Enc}(\phi(\alpha))$ , represented as states  $|\psi_{C_i}\rangle$ , to the verifier  $V$ , ordered by the clause index  $i$ ;
    - For each clause  $C_i$ , with the state  $|\psi_{C_i}\rangle$  received :
      - 3.a  $V$  measures the state  $|\psi_{C_i}\rangle$  in the computational basis, where this state is expected to be  $|\psi_{\text{var}(l_1), C_i}\rangle \otimes |\psi_{\text{var}(l_2), C_i}\rangle \otimes |\psi_{\text{var}(l_3), C_i}\rangle$ . The measurement outcomes are denoted by the triples  $(l_1, i, v_1)$ ,  $(l_2, i, v_2)$ , and  $(l_3, i, v_3)$ ;
      - 3.b If  $v_1 \vee v_2 \vee v_3 = \perp$ ,  $V$  rejects;
      - 3.c  $V$  updates the fingerprints  $F_{\text{cl}} = F_{\text{cl}} \cdot \prod_{j \in [3]} (a_{(l_j, i, v_j)} + r) \pmod p$ ;
      - 3.d  $V$  returns the triples  $(l_1, i, v_1)$ ,  $(l_2, i, v_2)$ , and  $(l_3, i, v_3)$  to  $P$ .
  4. The verifier  $V$  accepts if the fingerprints  $F_{\text{var}} = F_{\text{cl}}$ ; otherwise, it rejects.
- 

<sup>31</sup>QIPL is closed under logspace reductions if, for any logspace reduction  $R$  such that  $\mathcal{I} \leq_{\text{L}}^m \mathcal{I}'$ , it holds that  $\mathcal{I} \in \text{QIPL}$  if  $\mathcal{I}' \in \text{QIPL}$ . Let  $\mathcal{M}_{\mathcal{I}'}$  and  $\mathcal{M}_R$  be the deterministic logspace Turing machines that compute (the description of) the verifier's mapping associated with  $\mathcal{I}'$  and the reduction  $R$ , respectively. The closure under logspace reductions for QIPL is then achieved by considering the concatenation  $\mathcal{M}_{\mathcal{I}} := \mathcal{M}_R \circ \mathcal{M}_{\mathcal{I}'}$ . A similar argument applies to a weaker notion of the uniformity of the verifier's mapping discussed in Footnote 23.

To establish the correctness of Protocol 3.4, we first observe that since  $k$  is a polynomial in  $n$ , the integer  $2(bl)^2$  can be represented using  $O(\log n)$  bits. Following the argument in the proof [CL95, Lemma 2],<sup>32</sup> a classical logspace verifier can find the prime  $p$  and the integer  $r$  in Step 1 of Protocol 3.4 with probability at least  $3/4$ , using  $O(\log n)$  random bits. Since a classical operation depending on  $r$  random bits can be simulated by a corresponding unitary controlled by the state  $|+\rangle^{\otimes r}$ , Step 1 can be implemented using  $O(\log n)$  ancillary qubits, which remain untouched throughout the rest of the proof system. Additionally, because the state  $|\psi_{\text{varl}, C_i}\rangle$ , which encodes the triple  $(l, i, v)$ , requires at most  $O(\log n)$  qubits, space-bounded almost-unitary quantum circuits suffice to implement the verifier's actions in Protocol 3.4.

Although there are  $3k + k = 4k$  rounds in Protocol 3.4, the verifier's actions are of only constantly many kinds. Therefore, the verifier's mapping is logspace computable. We now turn to the analysis required to finish the proof:

- For *yes* instances, where the 3-SAT formula  $\phi$  is satisfiable, there is a prover strategy such that the verifier in Protocol 3.4 accepts with certainty.
- For *no* instances, we first bound the probability that the verifier in Protocol 3.4 accepts an unsatisfiable  $\phi$ , assuming the prover sends only classical messages. This event may happen if: (1) the verifier fails to successfully choose the random prime  $p$  and the random integer  $r$ ; or (2) the two multisets sent by the prover – specifically in Step 2 and Step 3 of Protocol 3.4 – are unequal but still yield the same fingerprint. According to the proof of [CL95, Lemma 2], the former occurs with probability at most  $1/4$ . And the fingerprinting lemma (Lemma 2.13) ensures that the latter occurs with probability at most

$$O\left(\frac{\log b + \log \ell}{b\ell} + \frac{1}{b^2\ell}\right) = O\left(\frac{\log \log(kn) + \log(3k)}{\log(kn) \cdot 3k} + \frac{1}{\log(kn)^2 \cdot 3k}\right) = O\left(\frac{1}{k}\right).$$

Therefore, the acceptance probability is at most  $1/4 + O(1/k) \leq 1/3$ .

Next, let  $\omega(V)|_u$  be the verifier  $V$ 's maximum acceptance probability conditioned on the intermediate measurement outcome  $u$ . A direct calculation shows that  $\omega(V)$  is a convex combination of  $\omega(V)|_u$  over all obtainable measurement outcomes  $u$ . Since each verifier action begins with a measurement that forces the prover's message to be classical, we have:

$$\omega(V) = \sum_{u \in \mathcal{J}_{\text{obt}}} p_u \cdot \omega(V)|_u \leq \sum_{u \in \mathcal{J}_{\text{obt}}} p_u \cdot \frac{1}{3} = \frac{1}{3}.$$

Here,  $p_u$  denotes the probability of obtaining the measurement outcome  $u$ ,  $\mathcal{J}_{\text{obt}}$  represents the index set of all obtainable intermediate measurement outcomes, and the inequality follows from the established soundness against classical messages.

In conclusion, we complete the proof by establishing that  $3\text{-SAT} \in \text{QIPL}_{8k}[1, 1/3]$ . □

### 3.4.2 $\text{SAC}^1 \cup \text{BQL}$ is in $\text{QIP}_{\text{UL}}$

Our approach follows [For89, Section 3.4]. To establish Theorem 3.4, along with error reduction for  $\text{QIP}_{\text{UL}}$  (Lemma 3.10) and  $\text{BQL} \subseteq \text{QIP}_{\text{UL}}$ , we need to prove the following:

**Lemma 3.16.**  $\text{SAC}^1 \subseteq \text{QIP}_{\text{UL}_{O(\log n)}}[1, 1 - 1/p(n)]$ , where  $p(n)$  is some polynomial in  $n$ .

*Proof.* For any promise problem  $\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$  in  $\text{SAC}^1$  where  $\mathcal{I}_{\text{yes}} \cup \mathcal{I}_{\text{no}} = \{0, 1\}^*$ , it suffices to consider the corresponding (uniform)  $\text{SAC}^1$  circuit evaluation problem, as defined in Definition 2.14. Let  $C$  be the (uniform)  $\text{SAC}^1$  circuit associated with  $\mathcal{I}$ , taking  $x \in \mathcal{I}$  as input, such that  $C(x) = 1$  if and only if  $x \in \mathcal{I}_{\text{yes}}$ .

We now present the  $\text{QIP}_{\text{UL}}$  proof system for  $\text{SAC}^1$ , as detailed in Protocol 3.5.

<sup>32</sup>See the first paragraph on Page 515 in [CL95] for the details.



---

**Protocol 3.5:** A  $\text{QIP}_{\text{UL}}$  proof system for (uniform)  $\text{SAC}^1$ .

---

1. The prover  $P$  and verifier  $V$  start at the output level of the circuit  $C$  :
    - If the top gate  $G$  is an OR gate :
      - 2.1  $P$  selects one of  $G$ 's child gates;
      - 2.2  $P$  sends the selection to  $V$  by sending a quantum state  $|\psi\rangle$ ;
    - If the top gate  $G$  is an AND gate :
      - 2.a  $V$  selects one of the two child gate of  $G$  uniformly at random;
      - 2.b  $V$  send the selection to  $P$  using half of an EPR pair;
  2. At each intermediate level of the circuit  $C$ , the prover  $P$  and verifier  $V$  repeat this process on the selected child gate, as outlined in Step 1.
  3. At the input level of the circuit  $C$  :
    - 3.1 The verifier  $V$  measures the register containing the currently selected child gate in the computational basis. Here, the measurement outcomes corresponds to either  $x_j$  or  $\neg x_j$  for some  $j \in [n]$ ;
    - 3.2 The verifier  $V$  checks the following :
      - For an **input**  $x_i$ :  $V$  accepts if  $x_i = 1$ ; otherwise,  $V$  rejects;
      - For a **negation of an input**  $x_i$ :  $V$  accepts if  $x_i = 0$ ; otherwise,  $V$  rejects.
- 

To establish the correctness of Protocol 3.5, we first observe that the depth of the circuit  $C$  is  $O(\log n)$ , implying that the size is polynomial in  $n$ . Consequently, each prover's selection can be represented by an  $O(\log n)$ -bit string. This observation also implies that Protocol 3.5 has  $O(\log n)$  rounds, but the verifier's actions are of only three kinds. Therefore, the verifier's mapping is logspace computable. We now turn to the analysis required to complete the proof:

- For *yes* instances, for any choices made by the verifier  $V$  at the AND gates, there exist corresponding choices at the OR gates that lead to the circuit  $C$  to accept. Therefore, the prover  $P$  has a winning strategy for all verifier choices, ensuring that the verifier  $V$  accepts with certainty.
- For *no* instances, since the computational paths in the circuit  $C$  do not interfere with each other, it suffices to establish soundness against classical messages. Note that certain verifier choices will cause  $V$  to reject. Given the  $O(\log n)$  depth of the circuit  $C$ ,  $V$  makes one choice out of two at each AND gate, resulting in a rejection probability of at least  $2^{-O(\log n)} = 1/p(n)$  for some polynomial  $p(n)$ . Therefore, the verifier accepts with probability at most  $1 - 1/p(n)$ .  $\square$

## 4 Constant-message space-bounded quantum interactive proofs

In this section, we investigate space-bounded quantum interactive proof systems with a *constant* number of messages. Building on the definitions in Section 3.1, we define the classes  $\text{QIPL}_{O(1)}$  and  $\text{QMAML}$  with *constant* promise gap as follows:

$$\text{QIPL}_{O(1)} := \cup_{m \leq O(1)} \text{QIP}_{\text{UL}_m}[2/3, 1/3] \text{ and } \text{QMAML} := \text{QMAML}[1, 1/3]. \quad (4.1)$$

Here, the class  $\text{QMAML}$  possesses *public-coin* three-message space-bounded *unitary* quantum interactive proofs, which is the space-bounded variant of the class  $\text{QMAM}$  introduced in [MW05].

Importantly, the definitions in Equation (4.1) align with those in Section 3.1 without loss of generality. Specifically, the two notions of space-bounded quantum interactive proof systems,  $\text{QIPL}$  and  $\text{QIP}_{\text{UL}}$ , coincide when the number of messages is constant:

*Remark 4.1* (The equivalence of  $\text{QIPL}_{O(1)}$  and  $\text{QIP}_{\text{UL}_{O(1)}}$ ). In a  $\text{QIPL}_{O(1)}$  proof system (or its reversible generalization,  $\text{QIPL}_{O(1)}^\diamond$ , see Remark 3.8), the number of turns (i.e., messages) is a constant. Consequently, the verifier’s actions during the execution of the proof system introduce only a constant number of additional environment registers, each containing  $O(\log n)$  qubits. Therefore, a  $\text{QIPL}_{O(1)}$  proof system (even its reversible generalization) can be straightforwardly simulated by a  $\text{QIP}_{\text{UL}_{O(1)}}$  proof system with the same parameters  $m(n)$ ,  $c(n)$ , and  $s(n)$ .

We establish the following upper bounds for  $\text{QIP}_{\text{UL}}$  and  $\text{QIPL}_{O(1)}$ . The first theorem, as detailed in Theorem 4.2, is obtained by combining Corollary 4.8 and Lemma 4.9, where the former is a direct corollary of the parallelization.<sup>33</sup> It is noteworthy that the second inclusion in Theorem 4.2 applies to the case where  $m(n) \leq O(1)$  and  $c(n) - s(n) \geq 1/\text{poly}(n)$ .

**Theorem 4.2** ( $\text{QIP}_{\text{UL}} \subseteq \text{P}$ ). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable 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, it holds that*

$$\text{QIP}_{\text{UL}_m}[c, s] \subseteq \text{QIPL}_3 \left[ 1, 1 - \frac{1}{q(n)} \right] \subseteq \text{P}, \text{ where } q(n) := \frac{2(m(n) + 1)^2}{(c(n) - s(n))^2}.$$

The second theorem, as stated in Theorem 4.3, is derived by combining Corollary 4.7 and Lemma 4.10. The class  $\text{NC}$  captures the power of (logspace-uniform) classical poly-logarithmic depth computation using bounded fan-in gates. Specifically, Corollary 4.7 is a direct consequence of the parallelization, while the  $\text{NC}$  containment (Lemma 4.10) follows directly from the celebrated  $\text{QIP} = \text{PSPACE}$  result [JJUW11].

**Theorem 4.3** ( $\text{QIPL}_{O(1)} \subseteq \text{NC}$ ). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable functions such that  $0 \leq s(n) < c(n) \leq 1$ ,  $c(n) - s(n) \geq \Omega(1)$ , and  $1 \leq m(n) \leq O(1)$ . Then, it holds that*

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

Unlike standard quantum interactive proofs, constant-message space-bounded quantum interactive proofs with constant promise gap ( $\text{QIPL}_{O(1)}$ ) are unlikely to be as computationally powerful as their polynomial-message counterparts ( $\text{QIPL}$ ). Furthermore, space-bounded quantum interactive proofs ( $\text{QIPL}$ ) appears to be more powerful than their unitary counterparts ( $\text{QIP}_{\text{UL}}$ ). These distinctions align with the widely believed conjectured separations  $\text{NC} \subsetneq \text{P} \subsetneq \text{NP}$ .

In the remainder of this section, we first demonstrate error reduction for  $\text{QIPL}_{O(1)}$  via parallel repetition in Section 4.1. Then, Section 4.2 provides the parallelization technique for  $\text{QIP}_{\text{UL}}$  and  $\text{QIPL}_{O(1)}$ , drawing inspiration from [KKMV09], with a focus on the turn-halving lemma (Lemma 4.5) and its corollaries. Next, we proceed to establish an upper bound for  $\text{QIPL}_{O(1)}$  with weak error bounds in Section 4.3. Finally, Section 4.4 presents the equivalence of  $\text{QIPL}_{O(1)}$  and  $\text{QMAML}$  (Corollary 4.11) and the  $\text{NC}$  containment (Lemma 4.10), using a simplified version of the turn-halving lemma.

## 4.1 Error reduction for $\text{QIPL}_{O(1)}$ via parallel repetition

Beyond the sequential repetition approach presented in the proof of Lemma 3.10, another common method for error reduction is the parallel repetition of the original proof system  $P \rightleftharpoons V$ . In this approach,  $k$  pairs of provers and verifiers execute  $P \rightleftharpoons V$  in parallel, where all  $k$  provers are independent only when they are honest. However, when adapting this approach for  $\text{QIPL}$  (or  $\text{QIP}_{\text{UL}}$ ), the message size in the parallelized protocol  $P' \rightleftharpoons V'$  becomes  $O(k \log n)$ , meaning  $P' \rightleftharpoons V'$  remains a  $\text{QIPL}$  (or  $\text{QIP}_{\text{UL}}$ ) proof system only when  $k$  is constant.

Next, we provide the formal statement and its proof inspired by [VW16, Section 4.3]:

<sup>33</sup>Importantly, Theorem 4.2 holds only when we define the class  $\text{QIP}_{\text{UL}}$  with the strong notion of uniformity for the verifier’s mapping, as detailed in Section 3.1. If the verifier’s mapping satisfies only a weaker notion of uniformity, as specified in Footnote 23, then the verifier’s action in the resulting proof system may not be space-bounded. This is because its description might not be produced by a logspace deterministic Turing machine.

**Lemma 4.4** (Error reduction for  $\text{QIPL}_{O(1)}$  via parallel repetition). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable functions such that  $0 \leq s(n) < c(n) \leq 1$ ,  $c(n) - s(n) \geq 1/\text{poly}(n)$ , and  $1 \leq m(n) \leq O(1)$ . For any constant  $k(n)$ , it holds that*

$$\text{QIPL}_m[c, s] \subseteq \text{QIPL}_m[c^k, s^k].$$

*Proof.* For convenience, we prove the inclusion for  $\text{QIPL}_{O(1)}^\diamond$  proof systems, which serves as a reversible generalization of  $\text{QIPL}_{O(1)}$  (see Remark 3.8) and is equivalent to it (see Remark 4.1).

For any  $l$ -round proof system  $P \rightleftharpoons V$  with completeness  $c$  and soundness  $s$ , corresponding to a promise problem  $\mathcal{I}$  in  $\text{QIPL}_m^\diamond[c, s]$ , the maximum acceptance probability of the verifier, denoted by  $\omega(V)$ , serves as the objective function in the SDP formulation provided in Lemma 3.12. See also Remark 3.13 for the applicability of the SDP to  $\text{QIPL}^\diamond$  proof systems.

Now, consider a  $k$ -fold parallel repetition of  $P \rightleftharpoons V$ , involving  $k$  verifiers  $V^{(i)} := (V_1^{(i)}, \dots, V_{l+1}^{(i)})$  for  $i \in [k]$ . Let  $V^{(1)} \otimes \dots \otimes V^{(k)}$  be the combined verifier, obtained by executing  $V^{(1)}, \dots, V^{(k)}$  in parallel, with the output bit being the AND of the output bits of  $V^{(1)}, \dots, V^{(k)}$ . It follows that

$$\omega(V^{(1)} \otimes \dots \otimes V^{(k)}) \geq \omega(V^{(1)}) \dots \omega(V^{(k)}),$$

since dishonest provers  $P^{(1)}, \dots, P^{(k)}$  may apply entangled actions. However, due to the strong duality of the SDP program for computing  $\omega(V^{(i)})$  for each  $i \in [k]$ , the equality also holds:

$$\omega(V^{(1)} \otimes \dots \otimes V^{(k)}) = \omega(V^{(1)}) \dots \omega(V^{(k)}). \quad (4.2)$$

In particular, the SDP formulation specified in Lemma 3.12 serves as the primal form of an SDP program for computing  $\omega(V^{(i)})$ , with the corresponding dual form obtainable similarly to [VW16, Figure 4.7]. Following an argument analogous to Equation (4.49) through (4.53) in [VW16, Section 4.3], we arrive at Equation (4.2), with details omitted here.  $\square$

## 4.2 Parallelization via the turn-halving lemma

Our approach to do parallelization for  $\text{QIPL}_{O(1)}$  is inspired by [KKMV09, Section 4]. We begin with the key lemma that halves the number of turns (i.e., messages) in the proof system:

**Lemma 4.5** (Turn-halving lemma). *Let  $s(n)$  and  $m(n)$  be logspace-computable functions such that  $0 \leq s(n) \leq 1$  and  $1 \leq m(n) \leq \text{poly}(n)$ . Then, it holds that*

$$\text{QIP}_{\cup L_{4m+1}}[1, s] \subseteq \text{QIP}_{\cup L_{2m+1}}[1, (1 + \sqrt{s})/2].$$

*Remark 4.6* (Limitations on the turn-halving lemma). The parallelization technique described in [KKMV09, Section 4] requires the verifier's actions to be *reversible*. This requirement implies that these actions must be implemented using either unitary or isometric quantum circuits. Therefore, it is straightforward to extend Lemma 4.5 to  $\text{QIPL}^\diamond$ , a reversible generalization of  $\text{QIPL}$ . However, this extended version can be applied recursively at most a *constant* number of times; otherwise, the new verifier in the resulting proof system would no longer be space-bounded. Specifically, if the extended version is applied  $\omega(1)$  times, it will introduce  $2^{\omega(1)}$  environment registers, each containing  $O(\log n)$  qubits, during a single verifier action.

Before presenting the proof, we provide two corollaries of the turn-halving lemma (Lemma 4.5) with their proofs to illuminate its applications, as stated in Corollary 4.7 and Corollary 4.8.

**Corollary 4.7** ( $\text{QIPL}_{O(1)} \subseteq \text{QIPL}_3$ ). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable functions with  $0 \leq s(n) < c(n) \leq 1$ ,  $c(n) - s(n) \geq \Omega(1)$ , and  $3 \leq m(n) \leq O(1)$ . Then, it holds that*

$$\text{QIPL}_m[c, s] \subseteq \text{QIPL}_3[1, 1/16].$$

*Proof.* It suffices to prove the following inclusions:

$$\text{QIPL}_m[c, s] \subseteq \text{QIPL}_{m+2} \left[ 1, 1 - \frac{(c-s)^2}{2} \right] \subseteq \text{QIPL}_3 \left[ 1, 1 - \frac{(c-s)^2}{2(m+1)^2} \right] \subseteq \text{QIPL}_3 \left[ 1, \frac{1}{16} \right]. \quad (4.3)$$

The first inclusion in Equation (4.3) follows directly from Lemma 3.9. To show the last inclusion in Equation (4.3), we consider an  $r$ -fold (AND-type) parallel repetition of this three-message QIPL proof system. By applying Lemma 4.4 with  $r = O\left(k / \log \frac{1}{1-(c-s)^2/(2(m+1)^2)}\right)$ , we derive the following inclusions:

$$\text{QIPL}_3 \left[ 1, 1 - \frac{(c-s)^2}{2(m+1)^2} \right] \subseteq \text{QIPL}_3 \left[ 1, \left( 1 - \frac{(c-s)^2}{2(m+1)^2} \right)^r \right] \subseteq \text{QIPL}_3 \left[ 1, \frac{1}{16} \right].$$

It remains to show the second inclusion in Equation (4.3). By repeatedly applying the turn-halving lemma (Lemma 4.5)  $l$  times, where  $l$  satisfies  $2^l + 1 \leq m + 2 \leq 2^{l+1} + 1$ , we obtain:

$$\text{QIPL}_{m+2} \left[ 1, 1 - \frac{(c-s)^2}{2} \right] \subseteq \text{QIPL}_{2^{l+1}+1} \left[ 1, 1 - \frac{(c-s)^2}{2} \right] \subseteq \text{QIPL}_3 \left[ 1, 1 - \frac{(c-s)^2}{2(m+1)^2} \right]. \quad (4.4)$$

Here, in the last inclusion, the reasoning behind the parameters – particularly  $m(n)$ ,  $c(n)$ , and  $s(n)$  – follows directly from the proof of [KKMV09, Lemma 4.2], so we omit the details.

Let  $P \rightleftharpoons V$  be the original proof system. For the resulting proof system  $P' \rightleftharpoons V'$ , we now need to establish that the verifier's actions are space-bounded unitary circuits, and that the verifier's mapping is logspace computable. This follows because (1) an operation depending on  $r$  random coins can be simulated by applying a corresponding unitary controlled by  $|+\rangle^{\otimes r}$ , meaning that simulating  $l$  random coins in all of the verifier's actions requires  $l$  ancillary qubits; and (2) since a logspace deterministic Turing machine (DTM) can produce the description of all verifier's actions in  $P \rightleftharpoons V$ , there is another logspace DTM which can produce the description of each verifier's action in  $P' \rightleftharpoons V'$ .  $\square$

**Corollary 4.8** (QIP<sub>U</sub>L is parallelized to three messages with weaker error bounds). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable functions with  $0 \leq s(n) < c(n) \leq 1$ ,  $c(n) - s(n) \geq 1/\text{poly}(n)$ , and  $3 \leq m(n) \leq \text{poly}(n)$ . Then, it holds that*

$$\text{QIP}_{\text{U}L}_m[c, s] \subseteq \text{QIP}_{\text{U}L}_3 \left[ 1, 1 - \frac{1}{q(n)} \right] \text{ where } q(n) := \frac{2(m(n)+1)^2}{(c(n)-s(n))^2}.$$

*Proof.* It suffices to prove the following inclusions:

$$\text{QIP}_{\text{U}L}_m[c, s] \subseteq \text{QIP}_{\text{U}L}_{m+2} \left[ 1, 1 - \frac{(c-s)^2}{2} \right] \subseteq \text{QIP}_{\text{U}L}_3 \left[ 1, 1 - \frac{(c-s)^2}{2(m+1)^2} \right]. \quad (4.5)$$

The first inclusion in Equation (4.5) follows directly from Lemma 3.9. The second inclusion in Equation (4.5) is achieved using a similar approach as that used to prove Equation (4.4) in Corollary 4.7. Finally, we need to show that the verifier's actions in the resulting proof system are space-bounded unitary circuits, and that the verifier's mapping is logspace computable. By noticing that  $l = O(\log n)$ , we can achieve this using reasoning analogous to the proof of Corollary 4.7, and we omit the details for brevity.  $\square$

#### 4.2.1 Proof of the turn-halving lemma

Next, we proceed with the detailed proof of the turn-halving lemma (Lemma 4.5):

*Proof of Lemma 4.5.* Our proof strategy is inspired by the proof of [KKMV09, Lemma 4.1]. For any  $(4m+1)$ -message QIP<sub>U</sub>L proof system  $P \rightleftharpoons V$  with completeness  $c$  and soundness  $s$ , corresponding to a promise problem  $\mathcal{I} \in \text{QIP}_{\text{U}L}$ , we can construct a new  $(2m+1)$ -message proof system  $\widehat{P} \rightleftharpoons \widehat{V}$ . We use the notations specified in Figure 4.1 to denote the snapshot states on

registers  $Q$ ,  $M$ , and  $W$  (resp.,  $\hat{Q}$ ,  $\hat{M}$ , and  $\hat{W}$ ) during the execution of  $P \rightleftharpoons V$  (resp.,  $\hat{P} \rightleftharpoons \hat{V}$ ), with slight adjustments for convenience compared to Figure 3.1 in Section 3.3.

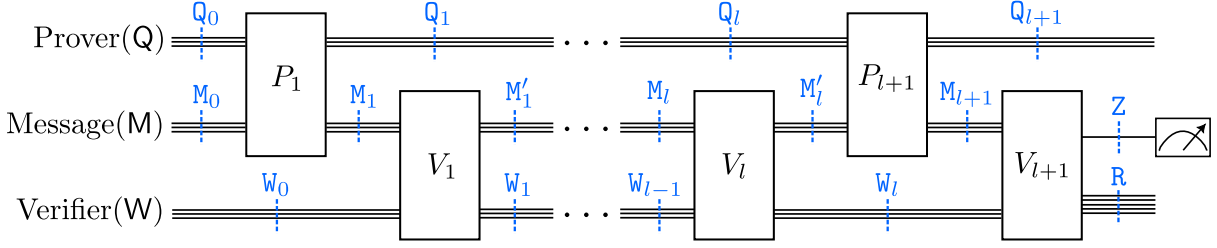


Figure 4.1: A  $(2l + 1)$ -turn space-bounded unitary quantum interactive proof system.

We now describe the new proof system  $\hat{P} \rightleftharpoons \hat{V}$  in an intuitive manner: the verifier  $\hat{V}$  first receives the snapshot state  $\rho_{\mathbf{M}_{m+1}\mathbf{W}_m}$ , which corresponds to the state after the prover  $P$  sent the  $(2m + 1)$ -st message in  $P \rightleftharpoons V$ . The verifier  $\hat{V}$  then executes  $P \rightleftharpoons V$  either forward or backward from the given snapshot, with equal probability. In the forward execution,  $\hat{V}$  accepts if  $V$  accepts; while in the backward execution,  $\hat{V}$  accepts if  $\hat{W}_0$  contains the all-zero state.<sup>34</sup> The detailed proof system  $\hat{P} \rightleftharpoons \hat{V}$  is presented in Protocol 4.1.

---

**Protocol 4.1:** A QIPL proof system for halving the number of messages in  $P \rightleftharpoons V$ .

---

1. The verifier  $\hat{V}$  receives the snapshot state  $\rho_{m+1} = \rho_{\mathbf{M}_{m+1}\mathbf{W}_m}$  from the prover  $\hat{P}$ , and then transfers the qubits corresponding to  $\mathbf{W}_m$  in  $\rho_{m+1}$  to its private register  $\hat{W}$ ;
  2. The verifier  $\hat{V}$  chooses  $b \in \{0, 1\}$  uniformly at random, and executes the original proof system  $P \rightleftharpoons V$  either forward (if  $b = 0$ ) or backward (if  $b = 1$ ):
    - FORWARD EXECUTION of  $P \rightleftharpoons V$  ( $b = 0$ ):
      - 2.1  $\hat{V}$  applies  $V_{m+1}$  to  $(\hat{M}, \hat{W})$ , and then sends  $b$  and  $\rho_{\hat{M}}$  to  $\hat{P}$ ;
      - 2.2 For  $j \leftarrow m + 2$  to  $2m$ :
        - └  $\hat{V}$  receives  $\rho_j = \rho_{\mathbf{M}_j}$  from  $\hat{P}$ , applies  $V_j$  on  $(\hat{M}, \hat{W})$ , and sends  $\rho_{\hat{M}}$  to  $\hat{V}$ ;
      - 2.3  $\hat{V}$  receives  $\rho_{2m+1} = \rho_{\mathbf{M}_{2m+1}}$  from  $\hat{P}$ , applies  $V_{2m+1}$  on  $(\hat{M}, \hat{W})$ .  $\hat{V}$  accepts if  $(\hat{M}, \hat{W})$  contains an accepting state of  $P \rightleftharpoons V$ ; otherwise, it rejects;
    - BACKWARD EXECUTION of  $P \rightleftharpoons V$  ( $b = 1$ ):
      - 2.a  $\hat{V}$  sends  $b$  and  $\rho_{\hat{M}} = \rho_{\mathbf{M}_{m+1}}$  to  $\hat{P}$ ;
      - 2.b For  $j \leftarrow m$  to  $2$ :
        - └  $\hat{V}$  receives  $\rho_j = \rho_{\mathbf{M}_j}$  from  $\hat{P}$ , applies  $V_j^\dagger$  on  $(\hat{M}, \hat{W})$ , and sends  $\rho_{\hat{M}}$  to  $\hat{V}$ ;
      - 2.c  $\hat{V}$  receives  $\rho_1 = \rho_{\mathbf{M}_1}$  from  $\hat{P}$ , applies  $V_1^\dagger$  on  $(\hat{M}, \hat{W})$ .  $\hat{V}$  accepts if  $\hat{W}$  contains the all-zero state; otherwise, it rejects;
- 

It remains to establish the correctness of the proof system  $\hat{P} \rightleftharpoons \hat{V}$ . Since the verifier  $V$ 's mapping (of  $P \rightleftharpoons V$ ) is logspace computable, and in each turn, the verifier  $\hat{V}$ 's action corresponds to one of two possible actions of  $V$  (depending on  $b$ ),<sup>35</sup> the verifier  $\hat{V}$ 's mapping is likewise logspace computable. Moreover, we need the following analyses:

- For *yes* instances, an honest prover  $\hat{P}$  can prepare the pure state  $|\psi_{\mathbf{Q}_{m+1}\mathbf{M}_{m+1}\mathbf{W}_m}\rangle$ , which corresponds to the state in  $(\mathbf{Q}, \mathbf{M}, \mathbf{W})$  after the  $(2m + 1)$ -st turn in  $P \rightleftharpoons V$ . Depending on

<sup>34</sup>Since the proof system  $\mathcal{A}$  begins with the prover  $P$ , the verifier  $\hat{V}$  does not need to measure  $\hat{M}_0$ .

<sup>35</sup>The random bit  $b$  can be simulated by a fresh qubit and a pinching intermediate measurement, following an argument similar to the proof of Theorem 3.15 concerning Step 1 in Protocol 3.4

the value of  $b$ , the prover  $\widehat{P}$  then applies the corresponding prover's actions  $P_j$  (if  $b = 0$ ) or  $P_j^\dagger$  (if  $b = 1$ ) in  $P \rightleftharpoons V$  during the execution of Step 2 in Protocol 4.1. For any  $x \in \mathcal{I}_{\text{yes}}$ , as  $(P \rightleftharpoons V)(x)$  accepts with certainty, it follows that  $(\widehat{P} \rightleftharpoons \widehat{V})(x)$  also accepts with certainty.

- For *no* instances, let  $|\psi\rangle$  be the state in  $(\widehat{Q}, \widehat{M}, \widehat{W})$  just after the first turn in  $\widetilde{P} \rightleftharpoons \widehat{V}$ . Let  $\widetilde{P}_j^{(b)}$  be the prover  $\widetilde{P}$ 's action, which is an arbitrary unitary transformation on  $(\widehat{Q}, \widehat{M})$ , at the  $(2j - 1)$ -st turn for  $2 \leq j \leq m + 1$ . We can then define unitary transformations  $U^{(0)}$  and  $U^{(1)}$  corresponding to the forward and backward execution of  $P \rightleftharpoons V$ , respectively:

$$U^{(0)} := V_{2m+1} \widetilde{P}_{m+1}^{(0)} V_{2m} \cdots \widetilde{P}_2^{(0)} \quad \text{and} \quad U^{(1)} := V_1^\dagger \widetilde{P}_{m+1} \cdots V_m^\dagger \widetilde{P}_2. \quad (4.6)$$

Based on Equation (4.6), we define the snapshot state  $|\Psi^{(b)}\rangle$  at Step 2.3 for  $b = 0$  and at Step 2.c for  $b = 1$ , respectively, before the corresponding final measurement:

$$\begin{aligned} |\Psi^{(0)}\rangle &:= \frac{1}{\sqrt{p_{\text{acc}}^{(0)}}} \Pi_{\text{acc}}^{(0)} U^{(0)} |\psi\rangle, \quad \text{where } p_{\text{acc}}^{(0)} := \left\| \Pi_{\text{acc}}^{(0)} U^{(0)} |\psi\rangle \right\|_2^2 \quad \text{and} \quad \Pi_{\text{acc}}^{(0)} := |1\rangle\langle 1|_{\text{out}} = \Pi_{\text{acc}}, \\ |\Psi^{(1)}\rangle &:= \frac{1}{\sqrt{p_{\text{acc}}^{(1)}}} \Pi_{\text{acc}}^{(1)} U^{(1)} |\psi\rangle, \quad \text{where } p_{\text{acc}}^{(1)} := \left\| \Pi_{\text{acc}}^{(1)} U^{(1)} |\psi\rangle \right\|_2^2 \quad \text{and} \quad \Pi_{\text{acc}}^{(1)} := |\bar{0}\rangle\langle \bar{0}|_{\widehat{W}}. \end{aligned}$$

As a result, the acceptance probability  $p_{\text{acc}}^{(b)}$  for  $b \in \{0, 1\}$  can be expressed as:

$$\forall b \in \{0, 1\}, \quad p_{\text{acc}}^{(b)} = \frac{1}{\left\| \Pi_{\text{acc}}^{(b)} U^{(b)} |\psi\rangle \right\|_2^2} \left| \langle \psi | U^{(b)\dagger} \Pi_{\text{acc}}^{(b)} U^{(b)} |\psi\rangle \right|^2 = \left| \langle \psi | U^{(b)\dagger} |\Psi^{(b)}\rangle \right|^2. \quad (4.7)$$

Note that the acceptance probability of the proof system  $(\widetilde{P} \rightleftharpoons \widehat{V})(x)$  for  $x \in \mathcal{I}_{\text{no}}$  can be written as  $p_{\text{acc}} = \frac{1}{2}(p_{\text{acc}}^{(0)} + p_{\text{acc}}^{(1)})$ . Substituting Equation (4.7) into this equality, we obtain:

$$\begin{aligned} p_{\text{acc}} &= \frac{1}{2} \left( \mathbb{F} \left( U^{(0)\dagger} |\Psi^{(0)}\rangle \langle \Psi^{(0)} | U^{(0)}, |\psi\rangle \langle \psi| \right)^2 + \mathbb{F} \left( U^{(1)\dagger} |\Psi^{(1)}\rangle \langle \Psi^{(1)} | U^{(1)}, |\psi\rangle \langle \psi| \right)^2 \right) \\ &\leq \frac{1}{2} \left( 1 + \mathbb{F} \left( U^{(0)\dagger} |\Psi^{(0)}\rangle \langle \Psi^{(0)} | U^{(0)}, U^{(1)\dagger} |\Psi^{(1)}\rangle \langle \Psi^{(1)} | U^{(1)} \right) \right) \\ &\leq \frac{1}{2} \left( 1 + \left\| \Pi_{\text{acc}} U^{(0)} U^{(1)\dagger} |\Psi^{(1)}\rangle \right\|_2 \right) \\ &\leq \frac{1}{2} (1 + \sqrt{s}). \end{aligned}$$

Here, the second line follows from Lemma 2.6, and the last line is due to the fact that  $p_{\text{acc}} = \left\| \Pi_{\text{acc}} U^{(0)} U^{(1)\dagger} |\Psi^{(1)}\rangle \right\|_2^2 \leq s$ , as guaranteed by the soundness condition of  $P \rightleftharpoons V$ .  $\square$

### 4.3 Weakness of $\text{QIPL}_{O(1)}$ with weak error bounds

We demonstrate an upper bound for  $\text{QIPL}_{O(1)}$  with weak error bounds:

**Lemma 4.9** ( $\text{QIPL}_{O(1)}$  is in  $\text{P}$ ). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable functions such that  $0 \leq s(n) < c(n) \leq 1$ ,  $c(n) - s(n) \geq 1/\text{poly}(n)$ , and  $1 \leq m(n) \leq O(1)$ , it holds that*

$$\text{QIPL}_m[c, s] \subseteq \text{P}.$$

Our approach parallels the proof of  $\text{QIP} \subseteq \text{EXP}$ , as outlined in [Wat16a, Page 31] and originally established in [KW00, Section 6]. Specifically, the SDP program for characterizing constant-turn QIPL proof systems, as detailed in Lemma 3.12, has a dimension of  $\text{poly}(n)$ . Therefore, we conclude a deterministic polynomial-time algorithm using a standard SDP solver.

*Proof of Lemma 4.9.* For any  $m$ -turn proof system  $P \rightleftharpoons V$ , with completeness  $c$ , soundness  $s$ , and  $m$  being even, which corresponds to a promise problem  $\mathcal{I}$  in  $\text{QIPL}_m[c, s]$ , we can utilize



Lemma 3.12 to obtain an SDP program, as specified in Equation (3.2). This SDP program maximizes the verifier's maximum acceptance probability  $\omega(V)$  over all choices of quantum states (variables)  $\rho_{M'_1 W_1 E_1}, \dots, \rho_{M'_l W_l E_1 \dots E_l}$ , where the number of rounds  $l := m/2$ . Since the number of turns  $m(n) \leq O(1)$ , the variables in this SDP collectively hold  $O(\log n)$  qubits. Thus, we can compute a description of this SDP program in deterministic polynomial time.

Next, consider the Frobenius norm defined as  $\|X\|_F := \sqrt{\text{Tr}(X^\dagger X)}$ , and let  $\{\sigma_i(X)\}$  be the singular values of a square matrix  $X$ . We then have the following:

$$\begin{aligned} \|\rho_{M'_1 W_1 E_1} \otimes \dots \otimes \rho_{M'_l W_l E_1 \dots E_l}\|_F &= \sqrt{\text{Tr}\left(\rho_{M'_1 W_1 E_1}^2 \otimes \dots \otimes \rho_{M'_l W_l E_1 \dots E_l}^2\right)} \\ &= \sqrt{\sum_{i=1}^D \sigma_i^2\left(\rho_{M'_1 W_1 E_1} \otimes \dots \otimes \rho_{M'_l W_l E_1 \dots E_l}\right)} \\ &\leq \sqrt{D}. \end{aligned}$$

Here,  $D$  represents the dimension of  $\rho_{M'_1 W_1 E_1} \otimes \dots \otimes \rho_{M'_l W_l E_1 \dots E_l}$ , which is bounded by  $2^{O(\log n)}$ , indicating that it is in  $\text{poly}(n)$ . The last line follows from the fact that all singular values of the density matrix  $\rho_{M'_1 W_1 E_1} \otimes \dots \otimes \rho_{M'_l W_l E_1 \dots E_l}$  are at most 1.

As a consequence, by employing the standard SDP solver based on the ellipsoid method (e.g., [GM12, Theorem 2.6.1]; see also [GLS93, Chapter 3]), we obtain an algorithm for approximately solving the SDP program in Equation (3.2), ensuring that the condition  $\omega(V) \geq c(n)$  is satisfied. This algorithm runs in deterministic time  $\text{poly}(D) \cdot \text{polylog}(\sqrt{D}/\varepsilon)$ , or expressed as  $\text{poly}(D, \log(1/\varepsilon))$ , outputting either an  $\varepsilon$ -approximate feasible solution  $\hat{X}$  or a certificate indicating that no such solution exists. Particularly, the error parameter  $\varepsilon(n)$  ensures that  $\|\hat{X} - X\|_F \leq \varepsilon(n)$  for some feasible solution  $X$ , with  $\omega(V)|_{\hat{X}} \geq c(n) - \varepsilon(n)$ , where  $\omega(V)|_{\hat{X}}$  represents the objective function evaluated at  $\hat{X}$ . We conclude the proof by observing that  $\varepsilon(n) \leq 1/\text{poly}(n)$  holds as long as  $c(n) - s(n) \geq 1/\text{poly}(n)$ .  $\square$

#### 4.4 Weakness of $\text{QIPL}_{O(1)}$ : QMAML and NC containment

We present an upper bound of  $\text{QIPL}_{O(1)}$ :

**Lemma 4.10.**  $\text{QIPL}_3[1, 1/16] \subseteq \text{QMAML}^\circ[1, 5/8] \subseteq \text{NC}$ .

The proof of Lemma 4.10 relies crucially on the *single-coin* variant of public-coin three-message quantum interactive proofs  $\text{QMAML}^\circ$ , where the second message is a single random coin. Specifically, the first inclusion corresponds to a space-bounded variant of  $\text{QIP}(3) \subseteq \text{QMAM}$  [MW05, Section 5], and the turn-halving lemma (Lemma 4.5) naturally extends this result. The second inclusion is exactly a down-scaling version of  $\text{QMAM}^\circ \subseteq \text{NC}(\text{poly})$  [JJUW11].<sup>36</sup>

Furthermore, the first inclusion in Lemma 4.10 implies the following:<sup>37</sup>

**Corollary 4.11.**  $\text{QIPL}_3 = \text{QMAML}$ .

We now move to the proof of Lemma 4.10.

*Proof of Lemma 4.10.* We begin by proving the first inclusion using a variant of the turn-halving lemma (Lemma 4.5). Let  $P \rightleftharpoons V$  denote the original  $\text{QIPL}_3$  proof system, which acts on registers  $Q$ ,  $M$ , and  $W$ , following the notations in Figure 4.1 with  $l = 1$ . We propose a  $\text{QMAML}^\circ$

<sup>36</sup>This inclusion does not extend to the variant with  $1/\text{poly}(n)$  promise gap. Specifically, applying the parallel SDP solver in [JJUW11], the resulting algorithm runs in parallel time (i.e., circuit depth)  $\text{poly} \log(n) \cdot \text{poly}(1/\varepsilon)$ , using  $\text{poly}(n)$  processors (i.e., circuit width), as noted in the first paragraph of [JY11]. Since the parameter  $\varepsilon$  for  $\text{QMAML}^\circ[1, 1 - 1/p(n)]$  is polynomially small, this algorithm does not run in NC as the parallel running time becomes  $\text{poly}(n)$ . This issue also arises when applying width-independent parallel SDP solvers [JY11, AZLO16].

<sup>37</sup>The inclusion  $\text{QMAML}^\circ[1, 5/8] \subseteq \text{QMAML}[1, 125/512] \subseteq \text{QMAML}[1, 1/3]$  is obtained by applying three-fold parallel repetition (Lemma 4.4), where the second message in the resulting proof system is three random coins.

proof system  $\widehat{P} \rightleftharpoons \widehat{V}$ , which acts on registers  $\widehat{Q}$ ,  $\widehat{M}$ , and  $\widehat{W}$ , as described in Protocol 4.2. It is noteworthy that this proof system is a simplified version of Protocol 4.1.

---

**Protocol 4.2:** A QMAML<sup>⊙</sup> proof system for verifying a QIPL<sub>3</sub> proof system  $P \rightleftharpoons V$ .

---

1. The verifier  $\widehat{V}$  receives the qubits contained in  $W_1$  from the prover  $\widehat{P}$ , and then transfers them to  $\widehat{W}$ .
  2. The verifier  $\widehat{V}$  chooses  $b \in \{0, 1\}$  uniformly at random and sends  $b$  to the prover  $\widehat{P}$ .
  3. The verifier  $\widehat{V}$  receives the qubits written in  $\widehat{M}$  from the prover  $\widehat{P}$ :
    - If  $b = 0$ , the verifier  $\widehat{V}$  applies  $V_2$  on  $(\widehat{M}, \widehat{W})$ .  $\widehat{V}$  accepts if  $(\widehat{M}, \widehat{W})$  contains an accepting state of  $P \rightleftharpoons V$ , and rejects otherwise.
    - If  $b = 1$ , the verifier  $\widehat{V}$  applies  $V_1^\dagger$  on  $(\widehat{M}, \widehat{W})$ .  $\widehat{V}$  accepts if  $\widehat{W}$  contains the all-zero state, and rejects otherwise.
- 

It remains to establish the correctness of Protocol 4.2. This is straightforward for *yes* instances. For *no* instances, the desired bound essentially follows from the inequality in Lemma 2.6, using reasoning similar to that in the proof of Lemma 4.5. We omit the details.

Next, we address the second inclusion. We start by observing that Protocol 4.2 aligns with the definition of single-coin quantum Arthur-Merlin games as described in [JJUW11, Section 2.4], with two key differences: the message length  $m$  is  $\log(n)$  rather than  $\text{poly}(n)$ , and the verifier is space-bounded instead of polynomial-time bounded. This proof system achieves completeness 1 and soundness  $5/8$  due to the first inclusion. Consequently, we can obtain the corresponding primal-dual SDP programs of dimension  $\text{poly}(n)$ , as opposed to  $\exp(\text{poly}(n))$ , following [JJUW11, Section 2.5]. Therefore, we conclude an NC containment by applying the parallel SDP solver from [JJUW11] to the resulting SDP programs of dimension  $\text{poly}(n)$ .  $\square$

## 5 Space-bounded unitary quantum statistical zero-knowledge

We now introduce (honest-verifier) space-bounded unitary quantum statistical zero-knowledge, denoted as QSZK<sub>UL</sub> and QSZK<sub>ULHV</sub>, as specific types of space-bounded unitary quantum interactive proofs (QIP<sub>UL</sub>) that possess an additional statistical zero-knowledge property.

Before presenting our results, we start by defining the promise problem INDIVPRODQSD, which is analogous to QSD [Wat02] and GAPQSD<sub>log</sub> [LGLW23]:

**Definition 5.1** (Individual Product State Distinguishability Problem, INDIVPRODQSD $[k, \alpha, \delta]$ ). Let  $k(n)$ ,  $\alpha(n)$ ,  $\delta(n)$ , and  $r(n)$  be logspace computable functions such that  $1 \leq k(n) \leq \text{poly}(n)$ ,  $0 \leq \alpha(n), \delta(n) \leq 1$ ,  $\alpha(n) - \delta(n) \cdot k(n) \geq 1/\text{poly}(n)$ , and  $1 \leq r(n) \leq O(\log n)$ . Let  $Q_1, \dots, Q_k$  and  $Q'_1, \dots, Q'_k$  be polynomial-size unitary quantum circuits acting on  $O(\log n)$  qubits, each with  $r(n)$  specified output qubits. For  $j \in [k]$ , let  $\sigma_j$  and  $\sigma'_j$  denote the states obtained by running  $Q_j$  and  $Q'_j$  on the all-zero state  $|\bar{0}\rangle$ , respectively, and tracing out the non-output qubits, then the promise is that one of the following holds:

- *Yes instances:* Two  $k$ -tuples of quantum circuits  $(Q_1, \dots, Q_k)$  and  $(Q'_1, \dots, Q'_k)$  such that

$$\text{T}(\sigma_1 \otimes \dots \otimes \sigma_k, \sigma'_1 \otimes \dots \otimes \sigma'_k) \geq \alpha(n);$$

- *No instances:* Two  $k$ -tuples of quantum circuits  $(Q_1, \dots, Q_k)$  and  $(Q'_1, \dots, Q'_k)$  such that

$$\forall j \in [k], \quad \text{T}(\sigma_j, \sigma'_j) \leq \delta(n).$$

Additionally, we denote the *complement* of INDIVPRODQSD $[k(n), \alpha(n), \delta(n)]$ , with respect to the chosen parameters  $\alpha(n)$ ,  $\delta(n)$ , and  $k(n)$ , as  $\overline{\text{INDIVPRODQSD}}$ .

With these definitions in hand, we now provide our first theorem in this section:

**Theorem 5.2** (The equivalence of  $\text{QSZK}_{\text{UL}}$  and  $\text{BQL}$ ). *The following holds:*

- (1) For any logspace-computable function  $m(n)$  such that  $1 \leq m(n) \leq \text{poly}(n)$ ,

$$\cup_{c(n)-s(n) \geq 1/\text{poly}(n)} \text{QSZK}_{\text{ULHV}}[m, c, s] \subseteq \text{BQL}.$$

- (2)  $\text{BQL} \subseteq \text{QSZK}_{\text{UL}} \subseteq \text{QSZK}_{\text{ULHV}}$ .

The class  $\text{QSZK}_{\text{UL}}$  consists of space-bounded unitary quantum interactive proof systems that possess statistical zero-knowledge against *any* verifier, whereas  $\text{QSZKL}$  proof systems possess statistical zero-knowledge against only an *honest* verifier. Consequently, the inclusion in Theorem 5.2(2) is straightforward, following directly from these definitions. To establish the direction  $\text{QSZK}_{\text{ULHV}} \subseteq \text{BQL}$ , we proceed by proving the following:

**Theorem 5.3** ( $\text{INDIVPRODQSD}$  is  $\text{QSZK}_{\text{ULHV}}$ -complete). *The following holds:*

- (1) Let  $c(n)$  and  $s(n)$  be logspace computable functions such that  $0 \leq s(n) < c(n) \leq 1$ . For any logspace-computable function  $m(n)$  such that  $3 \leq m(n) \leq \text{poly}(n)$ ,

$$\overline{\text{INDIVPRODQSD}}[m/2, \alpha, 2\delta] \text{ is } \text{QSZK}_{\text{ULHV}}[m, c, s]\text{-hard}.$$

Here,  $\alpha := (\sqrt{c} - \sqrt{s})^2 / (2m - 4)$  and  $\delta$  is some negligible function.

- (2) Let  $k(n)$ ,  $\alpha(n)$  and  $\delta(n)$  be logspace computable functions such that  $1 \leq k(n) \leq \text{poly}(n)$ ,  $0 \leq \alpha(n), \delta(n) \leq 1$ , and  $\alpha(n) - \delta(n) \cdot k(n) \geq 1/\text{poly}(n)$ . Then, it holds that

$$\text{INDIVPRODQSD}[k, \alpha, \delta] \in \text{BQL} \subseteq \text{QSZK}_{\text{ULHV}}.$$

In the remainder of this section, we first provide the definition of honest-verifier space-bounded quantum statistical zero-knowledge proofs (the class  $\text{QSZK}_{\text{ULHV}}$ ) in Section 5.1. Next, we establish that  $\text{INDIVPRODQSD}$  is  $\text{QSZK}_{\text{ULHV}}$ -hard (Theorem 5.3(1)) in Section 5.2. Subsequently, we present the  $\text{BQL}$  upper bound for  $\text{QSZK}_{\text{ULHV}}$  (Theorem 5.3(2)) in Section 5.3.

## 5.1 Definition of space-bounded unitary quantum statistical zero-knowledge

Our definition of (honest-verifier) space-bounded quantum statistical zero-knowledge follows that of [Wat02, Section 3.1]. In this framework, an honest-verifier space-bounded unitary quantum statistical zero-knowledge proof system is a space-bounded unitary quantum interactive proof system, as defined in Section 3.1, that satisfies an additional *zero-knowledge* property. Intuitively, the zero-knowledge property in  $\text{QIP}_{\text{UL}}$  proof systems requires that, after each message is sent, the quantum states representing the verifier's view – including snapshot states in the message register  $\mathbf{M}$  and the verifier's private register  $\mathbf{W}$  – should be approximately indistinguishable by a space-bounded unitary quantum circuit on accepted inputs.

We then formalize this notion. Consider a set  $\{\rho_{x,i}\}$  of mixed states, we say that this state set is *logspace-preparable* if there exists a family of  $m$ -tuples  $S_x := (S_{x,1}, \dots, S_{x,m})$ , where each  $S_{x,i}$  for  $i \in [m]$  is a space-bounded unitary quantum circuit (see Definition 2.8) with a specified collection of output qubits, such that for each input  $x$  and index  $i$ , the state  $\rho_{x,i}$  is the mixed state obtained by running  $S_{x,i}$  on the input state  $|\bar{0}\rangle$ , and then tracing out all non-output qubits. We refer to such  $\{S_x\}_{x \in \mathcal{I}}$  as the *space-bounded simulator* for the promise problem  $\mathcal{I}$ .

Next, for any space-bounded quantum interactive proof system  $P \stackrel{?}{=} V$ , we define the verifier's view after the  $i$ -th turn, denoted by  $\text{view}_{P \stackrel{?}{=} V}(x, i)$ , as the reduced state in registers  $(\mathbf{M}, \mathbf{W})$  immediately after  $i$  messages have been exchanged, with the prover's private qubits traced out.

We are now ready for the formal definition:

**Definition 5.4** (Honest-verifier space-bounded unitary quantum statistical zero-knowledge,  $\text{QSZK}_{\text{ULHV}}$ ). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace-computable functions of the input length  $n := |x|$  such that  $0 \leq s(n) < c(n) \leq 1$  and  $1 \leq m(n) \leq \text{poly}(n)$ . A promise problem*

$\mathcal{I} = (\mathcal{I}_{\text{yes}}, \mathcal{I}_{\text{no}})$  is in  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}[m, c, s]$ , if there exists an  $m(n)$ -message space-bounded unitary quantum interactive proof system  $(P \rightleftharpoons V)(x)$  such that:

- **Completeness.** For any  $x \in \mathcal{I}_{\text{yes}}$ , there exists an  $m(n)$ -message prover  $P$  such that

$$\Pr[(P \rightleftharpoons V)(x) \text{ accepts}] \geq c(n).$$

- **Soundness.** For any  $x \in \mathcal{I}_{\text{no}}$  and any  $m(n)$ -message prover  $P$ ,

$$\Pr[(P \rightleftharpoons V)(x) \text{ accepts}] \leq s(n).$$

- **Zero-knowledge.** There exists a space-bounded simulator  $\{S_x\}_{x \in \mathcal{I}}$  and a negligible function  $\delta(n)$  such that for any  $x \in \mathcal{I}_{\text{yes}}$  and each message  $i \in [m]$ , the circuit  $S_x(i)$  produces the corresponding state  $\sigma_{x,i}$  satisfying

$$\mathbb{T}(\sigma_{x,i}, \text{view}_{P \rightleftharpoons V}(x, i)) \leq \delta(n).$$

We define  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}[m] := \text{QSZK}_{\text{U}}\text{L}_{\text{HV}}[m, \frac{2}{3}, \frac{1}{3}]$  and  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}} := \cup_{m \leq \text{poly}(n)} \text{QSZK}_{\text{U}}\text{L}_{\text{HV}}[m]$ .

Since the inequality condition in the zero-knowledge property holds independently for each message in Definition 5.4, error reduction via sequential repetition (Lemma 3.10) directly applies to an honest-verifier space-bounded quantum statistical zero-knowledge proof system, with the zero-knowledge property automatically preserved.

*Remark 5.5* (Robustness of the zero-knowledge property in  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}$ ). Let  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}^*$  denote a weaker version of  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}$ , where the threshold function  $\delta(n) := (\sqrt{c} - \sqrt{s})^2 / (2m^2)$ ,<sup>38</sup> rather than being negligible. While it is clear that  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}} \subseteq \text{QSZK}_{\text{U}}\text{L}_{\text{HV}}^*$ , the standard approach to establish the reverse direction does not apply to  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}$ .<sup>39</sup> Instead, the inclusion  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}^* \subseteq \text{QSZK}_{\text{U}}\text{L}_{\text{HV}}$  only follows from  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}^* = \text{BQL}$  (Theorem 5.2).

## 5.2 $\overline{\text{INDIVPRODQSD}}$ is $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}$ -hard

Instead of directly proving that  $\overline{\text{INDIVPRODQSD}}$  is  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}$ -hard, we establish a slightly stronger result: the promise problem  $\overline{\text{INDIVPRODQSD}}$  is hard for the class  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}^*$  that contains  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}$  (Remark 5.5), as detailed in Theorem 5.6. This result mirrors the relationship between  $\overline{\text{QSD}}$  and the class  $\text{QSZK}$ .

**Theorem 5.6** ( $\overline{\text{INDIVPRODQSD}}$  is  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}^*$ -hard). *Let  $c(n)$ ,  $s(n)$ , and  $m(n)$  be logspace computable functions such that  $0 \leq s(n) < c(n) \leq 1$ ,  $c(n) - s(n) \geq 1/\text{poly}(n)$ , and  $3 \leq m(n) \leq \text{poly}(n)$ .<sup>40</sup> Then, it holds that*

$$\overline{\text{INDIVPRODQSD}}[[m(n)/2], \alpha(n), 2\delta(n)] \text{ is } \text{QSZK}_{\text{U}}\text{L}_{\text{HV}}^*[m(n), c(n), s(n)]\text{-hard.}$$

Here,  $\delta := (\sqrt{c} - \sqrt{s})^2 / (2m^2)$  and  $\alpha := (\sqrt{c} - \sqrt{s})^2 / (2m - 4)$ .

Before presenting the proof, we will first illustrate the properties of the simulator and explain the underlying intuition behind the proof. Our proof strategy follows some ideas from [Wat02, Section 5]. Consider a space-bounded quantum interactive proof system  $P \rightleftharpoons V$  for a promise problem  $\mathcal{I} \in \text{QSZK}_{\text{U}}\text{L}_{\text{HV}}^*[m(n), c(n), s(n)]$  that is statistical zero-knowledge against an honest verifier. Without loss of generality, assume that the number of turns in  $P \rightleftharpoons V$  is even. We use the notations introduced in Figure 3.1 and Section 3.3.

Let us now focus on the space-bounded simulator  $\{S_x\}_{x \in \mathcal{I}}$ . Let  $\xi'_0, \dots, \xi'_l$  and  $\xi_1, \dots, \xi_{l+1}$  denote the simulator's approximation to the reduced snapshot states in registers (M, W) after

<sup>38</sup>This bound results from the reduction to the  $\text{QSZK}_{\text{U}}\text{L}_{\text{HV}}$ -hard problem  $\text{INDIVPRODQSD}$ , see Theorem 5.6.

<sup>39</sup>In particular, the polarization lemma for the trace distance [Wat02, Section 4.1] is not applicable in the space-bounded scenario due to message size constraints.

<sup>40</sup>Without loss of generality, we can assume that  $m \geq 3$  by adding one or two dummy messages when  $m < 3$ , as discussed in Footnote 42.

the  $(2j - 1)$ -st and the  $(2j)$ -th turn, respectively, during the execution of  $P \rightleftharpoons V$ , as specified in Figure 5.1. For *yes* instances, these states closely approximate the actual view of the verifier (the corresponding snapshot states) during the execution of  $P \rightleftharpoons V$ . However, there is no *direct* closeness guarantee for *no* instances. Consequently, we can assume that the state  $\xi_{l+1}$  satisfies  $\text{Tr}(|1\rangle\langle 1|_Z \xi_{l+1}) = c(n)$  for *all* instances.

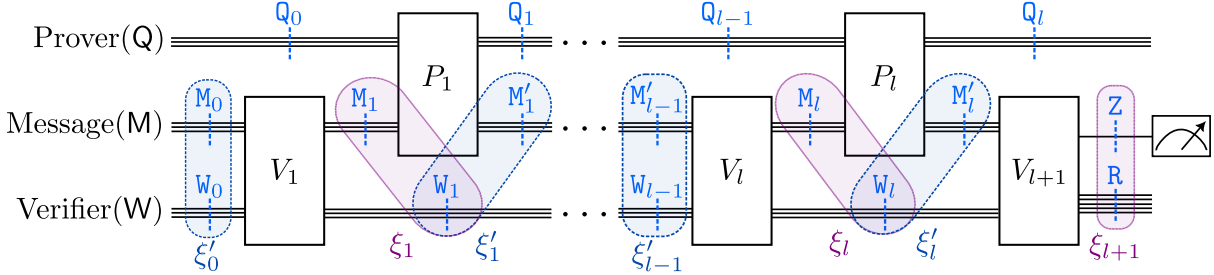


Figure 5.1: Quantum states  $\xi'_0, \dots, \xi'_l$  and  $\xi, \dots, \xi_{l+1}$  prepared by the simulator.

In addition, given that the verifier is always assumed to act honestly, we can take<sup>41</sup>

$$\xi'_0 = (|0\rangle\langle 0|)^{\otimes (q_M + q_W)} \text{ and } \xi_j = V_j \xi'_{j-1} V_j^\dagger \text{ for } j \in [l + 1]. \quad (5.1)$$

**Proof intuition.** Notably, the space-bounded simulator  $\{S_x\}_{x \in \mathcal{I}}$  essentially produces an approximation solution, in the form of snapshot states, to the SDP program Equation (3.2) for computing the maximum acceptance probability  $\omega(V)$  of the space-bounded unitary quantum interactive proof systems  $P \rightleftharpoons V$  for  $\mathcal{I} \in \text{QIP}_{\text{UL}}$ . As we stated in the proof of Lemma 3.12, there are only two types of constraints: (1) Verifier's actions are honest; and (2) Prover's actions do not affect the verifier's private qubits.

As mentioned in Equation (5.1), these states produced by the simulator exactly satisfy the first type of constraints for all instances, but satisfy the second type of constraints *only* for *yes* instances. This observation leads to our proof and the hard problem INDIVPRODQSD. Specifically, we consider two tensor product states, each consisting of a polynomial number of  $O(\log n)$ -qubit states, where all components are defined in Figure 5.1:

$$\text{Tr}_M(\xi_1) \otimes \dots \otimes \text{Tr}_M(\xi_l) \text{ and } \text{Tr}_M(\xi'_1) \otimes \dots \otimes \text{Tr}_M(\xi'_l). \quad (5.2)$$

For *yes* instances, the zero-knowledge property ensures a component-wise closeness bound  $\text{Tr}_M(\xi_j) \approx \text{Tr}_M(\xi'_j)$  for  $j \in [l]$ . For *no* instances, we need to show that the two states in Equation (5.2) are far from each other, given that  $\omega(V) \leq s(n)$ . This follows directly from [Wat02, Lemma 15]. We state the counterpart result below and omit the detailed proof:

**Proposition 5.6.1** (Adapted from [Wat02, Lemma 15]). *Let  $P \rightleftharpoons V$  be an  $m(n)$ -turn space-bounded quantum interactive proof system, with even  $m := 2l$ , such that  $\omega(V) \leq s(n)$ . Let  $\xi'_0, \dots, \xi'_l$  and  $\xi_k, \dots, \xi_{l+1}$  be the states produced by the simulators as defined in Figure 5.1. Assume that  $\text{Tr}(|\bar{0}\rangle\langle \bar{0}|_{M_0 W_0} \xi'_0) = 1$  and  $\text{Tr}(|1\rangle\langle 1|_Z \xi_{l+1}) = c$ . Then, it holds that*

$$\mathbb{T}(\text{Tr}_M(\xi_1) \otimes \dots \otimes \text{Tr}_M(\xi_l), \text{Tr}_M(\xi'_1) \otimes \dots \otimes \text{Tr}_M(\xi'_l)) \geq \frac{(\sqrt{c} - \sqrt{s})^2}{4(l-1)}.$$

Then, we proceed with the formal proof of Theorem 5.6:

*Proof of Theorem 5.6.* Let  $P \rightleftharpoons V$  be an  $m(n)$ -turn honest-verifier unitary quantum statistical zero-knowledge proof system for a promise problem  $\mathcal{I} \in \text{QSZKL}_{\text{HV}}^*[m, c, s]$ , with completeness  $c(n)$  and soundness  $s(n)$ . Without loss of generality, we assume that  $m$  is even for all  $x \in \mathcal{I}$ .<sup>42</sup> Hence, we can denote the verifier's actions by  $V_1, \dots, V_{l+1}$  for  $l = m/2$ , and the verifier

<sup>41</sup>Consequently, the simulator only needs to prepare  $\xi'_{j-1}$ , since  $\xi_j$  is obtained by applying  $V_j$  to this state.

<sup>42</sup>If  $m$  is odd, we can add an initial turn to  $P \rightleftharpoons V$  in which the verifier sends the all-zero state to the prover.

initiates the protocol. Let  $\{\sigma_{x,i}\}_{x \in \mathcal{I}, i \in [m+2]}$  represent the mixed states produced by the simulator  $\{S_x\}_{x \in \mathcal{I}}$ , with the threshold function  $\delta(n) := 1/m(n)^2$ . For any  $x \in \mathcal{I}$ , we can define states  $\xi'_0, \dots, \xi'_l$  and  $\xi_1, \dots, \xi_{l+1}$  as illustrated in Figure 5.1:

- Initial state before executing  $P \rightleftharpoons V$ :  $\xi'_0 := |\bar{0}\rangle\langle\bar{0}|_{M_0 W_0}$ .
- $(2j)$ -th message for  $j \in [l]$  in  $P \rightleftharpoons V$ :  $\xi'_j := \sigma_{x,2j}$ , where  $\sigma_{x,2j}$  satisfies:

$$\forall x \in \mathcal{I}_{\text{yes}}, \quad \mathbb{T}(\sigma_{x,2j-1}, \text{view}_{P \rightleftharpoons V}(x, 2j)) = \mathbb{T}(\sigma_{x,2j-1}, \rho_{M_j W_j}) \leq \delta(n). \quad (5.3)$$

- $(2j+1)$ -st message for  $j \in [l]$  in  $P \rightleftharpoons V$ :  $\xi_j := V_j \xi'_{j-1} V_j^\dagger$ .
- State before the final measurement in  $P \rightleftharpoons V$ :  $\xi_{l+1} := V_{l+1} \xi'_l V_{l+1}^\dagger$  satisfies

$$\text{Tr}(|1\rangle\langle 1|_{\mathcal{Z}} \xi_{l+1}) = c(n).$$

Let  $Q_1, \dots, Q_k$  and  $Q'_1, \dots, Q'_k$  be polynomial-size unitary quantum circuits acting on  $O(\log n)$  qubits which satisfy that  $Q_j = S_{x,2j-1}$  and  $Q'_j = S_{x,2j}$  for  $j \in [l]$ , and the output qubits are qubits in the verifier's private register  $W$ . It is evident that  $Q_j$  and  $Q'_j$  prepare the states  $\text{Tr}_M(\xi_j)$  and  $\text{Tr}_M(\xi'_j)$ , respectively. We claim that the  $l$ -tuples  $(Q_1, \dots, Q_l)$  and  $(Q'_1, \dots, Q'_l)$  form an instance of  $\overline{\text{INDIVPRODQSD}}[l(n), \alpha(n), \delta'(n)]$ , satisfying the following conditions:

$$\forall x \in \mathcal{I}_{\text{yes}}, \quad \mathbb{T}(\text{Tr}_M(\xi_j), \text{Tr}_M(\xi'_j)) \leq 2\delta = \frac{(\sqrt{c} - \sqrt{s})^2}{4l^2} := \delta' \text{ for } j \in [l]; \quad (5.4)$$

$$\forall x \in \mathcal{I}_{\text{no}}, \quad \mathbb{T}(\text{Tr}_M(\xi_1) \otimes \dots \otimes \text{Tr}_M(\xi_l), \text{Tr}_M(\xi'_1) \otimes \dots \otimes \text{Tr}_M(\xi'_l)) \geq \frac{(\sqrt{c} - \sqrt{s})^2}{4(l-1)} := \alpha. \quad (5.5)$$

By substituting Equation (5.4) into Lemma 2.2, it follows that:

$$\begin{aligned} \mathbb{T}(\text{Tr}_M(\xi_1) \otimes \dots \otimes \text{Tr}_M(\xi_l), \text{Tr}_M(\xi'_1) \otimes \dots \otimes \text{Tr}_M(\xi'_l)) &\leq \sum_{j \in [l]} \mathbb{T}(\text{Tr}_M(\xi_j), \text{Tr}_M(\xi'_j)) \\ &\leq \frac{(\sqrt{c} - \sqrt{s})^2}{4l}. \end{aligned} \quad (5.6)$$

Consequently, by comparing Equations (5.4) to (5.6), we can conclude the parameter requirement of  $\overline{\text{INDIVPRODQSD}}[l(n), \alpha(n), \delta'(n)]$ , specifically that  $\alpha(n) - \delta'(n) \cdot l(n) \geq 1/\text{poly}(n)$ .

It remains to establish Equation (5.4) and Equation (5.5). The latter follows directly from Proposition 5.6.1. To prove the former, note that the prover's actions do not affect the verifier's private register for *yes* instances, we thus derive the following for  $j \in \{2, \dots, l\}$ :

$$\begin{aligned} \mathbb{T}(\text{Tr}_M(\xi_j), \text{Tr}_M(\xi'_j)) &\leq \mathbb{T}(\xi_j, \xi'_j) \\ &\leq \mathbb{T}(\xi_j, \rho_{M_j W_j}) + \mathbb{T}(\rho_{M_j W_j}, \rho_{M'_j W_j}) + \mathbb{T}(\rho_{M'_j W_j}, \xi'_j) \\ &= \mathbb{T}(\xi'_{j-1}, \rho_{M'_{j-1} W_{j-1}}) + \mathbb{T}(\rho_{M_j W_j}, \rho_{M'_j W_j}) + \mathbb{T}(\rho_{M'_j W_j}, \xi'_j) \\ &\leq \delta(n) + 0 + \delta(n) \\ &= 2\delta(n). \end{aligned}$$

Here, the first line follows from the data-process inequality (Lemma 2.3), the second line is due to the triangle inequality, the third line owes to the unitary invariance (Lemma 2.4) and the fact that  $\rho_{M_j W_j} = V_j \rho_{M'_{j-1} W_{j-1}} V_j^\dagger$ , and the fourth line is because of Equation (5.3). We complete the proof by noting that similar reasoning applies to the case of  $j = 1$ , using  $\mathbb{T}(\xi_1, \rho_{M_1 W_1}) = 0$  instead of at most  $\delta(n)$ .  $\square$

### 5.3 QSZK<sub>U</sub>L<sub>HV</sub> is in BQL

We will establish the hard direction in the equivalence of QSZK<sub>U</sub>L<sub>HV</sub> and BQL. The key lemma underlying the proof involves a logspace (many-to-one) reduction  $\overline{\text{INDIVPRODQSD}}$  to



an “existential” version of  $\text{GAPQSD}_{\log}$ , where  $\text{GAPQSD}_{\log}$  is a  $\text{BQL}$ -complete problem (see Section 2.3). This reduction leads to a  $\text{BQL}$  containment for  $\text{INDIVPRODQSD}$ :

**Lemma 5.7** ( $\text{INDIVPRODQSD}$  is in  $\text{BQL}$ ). *Let  $k(n)$ ,  $\alpha(n)$  and  $\delta(n)$  be logspace computable functions such that  $1 \leq k(n) \leq \text{poly}(n)$ ,  $0 \leq \alpha(n), \delta(n) \leq 1$ , and  $\alpha(n) - \delta(n) \cdot k(n) \geq 1/\text{poly}(n)$ . Then, it holds that*

$$\text{INDIVPRODQSD}[k(n), \alpha(n), \delta(n)] \in \text{BQL}.$$

As  $\overline{\text{INDIVPRODQSD}}$  is  $\text{QSZK}_{\text{UHV}}$ -hard (Theorem 5.6), and given that  $\text{BQ}_{\text{UL}}$  is closed under complement [Wat99, Corollary 4.8] and the equivalence  $\text{BQL} = \text{BQ}_{\text{UL}}$  [FR21], we can directly conclude the following corollary:

**Corollary 5.8.**  $\text{QSZK}_{\text{UHV}} \subseteq \text{BQL}$ .

We now proceed with the formal proof of the key lemma:

*Proof of Lemma 5.7.* We first establish a logspace (many-to-one) reduction from  $\text{INDIVPRODQSD}$  to an “existential” version of  $\text{GAPQSD}_{\log}$ . Let  $(Q_1, \dots, Q_k)$  and  $(Q'_1, \dots, Q'_k)$  be an instance of  $\text{INDIVPRODQSD}[k, \alpha, \delta]$ . For each  $j \in [k]$ , let  $\sigma_j$  and  $\sigma'_j$  denote the states obtained by running  $Q_j$  and  $Q'_j$  on the all-zero state  $|\bar{0}\rangle$ , respectively, and tracing out the non-output qubits. We now need to decide which of the following cases in Equation (5.7) and Equation (5.8) holds:

$$\text{T}(\sigma_1 \otimes \dots \otimes \sigma_k, \sigma'_1 \otimes \dots \otimes \sigma'_k) \geq \alpha(n). \quad (5.7)$$

$$\forall j \in [k], \quad \text{T}(\sigma_j, \sigma'_j) \leq \delta(n). \quad (5.8)$$

By combining Lemma 2.2 with Equation (5.7), we obtain:

$$\sum_{j \in [k]} \text{T}(\sigma_j, \sigma'_j) \geq \text{T}(\sigma_1 \otimes \dots \otimes \sigma_k, \sigma'_1 \otimes \dots \otimes \sigma'_k) \geq \alpha(n). \quad (5.9)$$

Applying an averaging argument to Equation (5.9), we can conclude that

$$\exists j \in [k], \quad \text{T}(\sigma_j, \sigma'_j) \geq \alpha/k. \quad (5.10)$$

Clearly, a violation of Equation (5.10) implies a violation of Equation (5.7), without contradicting Equation (5.8). For each  $j \in [k]$ , the pair of circuits  $Q_j$  and  $Q'_j$  forms an instance of  $\text{GAPQSD}_{\log}$ . The resulting promise problem is thus an “existential” version of  $\text{GAPQSD}_{\log}$ , where *yes* instances satisfy Equation (5.10) and *no* instances satisfy Equation (5.8).

Next, we proceed by demonstrating the  $\text{BQL}$  containment. Given the equivalence of  $\text{BQL}$  and  $\text{QMAL}$  [FKL<sup>+</sup>16, FR21], it remains to establish a  $\text{QMAL}$  containment for this “existential” version of  $\text{GAPQSD}_{\log}$ . The verification protocol is outlined in Protocol 5.1.

---

**Protocol 5.1:** A  $\text{QMAL}$  proof system for  $\text{INDIVPRODQSD}$ .

---

1. The verifier receives an index  $j \in [k]$  from the prover.
  2. The verifier executes the quantum logspace algorithm  $\mathcal{A}$  for  $\text{GAPQSD}_{\log}[\alpha/k, \delta]$  underlying in Theorem 2.11, using the pair of circuits  $Q_j$  and  $Q'_j$  as the  $\text{GAPQSD}_{\log}$  instance. The verifier accepts (or rejects) if  $\mathcal{A}$  accepts (or rejects).
- 

To complete the proof, we establish the correctness of Protocol 5.1. Since the algorithm  $\mathcal{A}$  is a  $\text{BQL}$  containment for  $\text{GAPQSD}_{\log}[\alpha/k, \delta]$  (Theorem 2.11), we conclude the following:

- For *yes* instances, Equation (5.10) ensures that there exists an  $j \in [k]$  (the witness) such that  $\text{T}(\sigma_j, \sigma'_j) \geq \alpha/k$ . Consequently,  $\mathcal{A}$  accepts with probability at least  $2/3$ .
- For *no* instances, Equation (5.8) yields that for all  $j \in [k]$ ,  $\text{T}(\sigma_j, \sigma'_j) \leq \delta$ . This statement implies that  $\mathcal{A}$  accepts with probability at most  $1/3$ .  $\square$

## Acknowledgments

YL is grateful to Uma Girish for helpful discussion that inspired Question (d). This work was partially supported by MEXT Q-LEAP grant No. JPMXS0120319794. FLG was also supported by JSPS KAKENHI grants Nos. JP20H05966, 20H00579, 24H00071, and by MEXT JST CREST grant No. JPMJCR24I4. YL was further supported by JST SPRING grant No. JPMJSP2125 and acknowledges the “THERS Make New Standards Program for the Next Generation Researchers.” HN was additionally supported by JSPS KAKENHI grants Nos. JP19H04066, JP20H05966, JP21H04879, and JP22H00522. QW was supported in part by the Engineering and Physical Sciences Research Council under Grant No. EP/X026167/1.

## References

- [AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 1st edition, 2009. [14](#)
- [AG21] Dorit Aharonov and Alex B. Grilo. Two combinatorial MA-complete problems. In *12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference*, volume 185 of *LIPICs*, pages 36:1–36:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. [arXiv:2003.13065](#). [10](#)
- [AGM<sup>+</sup>23] 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](#). [11](#)
- [AHT23] 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, page 3, 2023. [ECCC:TR22-127](#). [11](#)
- [AN02] Dorit Aharonov and Tomer Naveh. Quantum NP – a survey. *arXiv preprint quant-ph/0210077*, 2002. [arXiv:quant-ph/0210077](#). [4](#)
- [AZLO16] Zeyuan Allen-Zhu, Yin Tat Lee, and Lorenzo Orecchia. Using optimization to obtain a width-independent, parallel, simpler, and faster positive SDP solver. In *Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms*, pages 1824–1831, 2016. [arXiv:1507.02259](#). [37](#)
- [Bab85] László Babai. Trading group theory for randomness. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985. [1](#), [4](#)
- [BBC<sup>+</sup>95] Adriano Barenco, Charles H Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical review A*, 52(5):3457, 1995. [arXiv:quant-ph/9503016](#). [21](#)
- [BCD<sup>+</sup>89] Allan Borodin, Stephen A. Cook, Patrick W. Dymond, Walter L. Ruzzo, and Martin Tompa. Two applications of inductive counting for complementation problems. *SIAM Journal on computing*, 18(3):559–578, 1989. Preliminary version in *SCT 1988*. [15](#)
- [BEM<sup>+</sup>23] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary complexity and the Uhlmann transformation problem, 2023. [arXiv:2306.13073](#). [11](#)

- [BGM06] Elmar Böhler, Christian Glaßer, and Daniel Meister. Error-bounded probabilistic computations between MA and AM. *Journal of Computer and System Sciences*, 72(6):1043–1076, 2006. Preliminary version in *MFCS 2003*. [ECCC:TR03-069](#). 7, 15, 27
- [BSW11] Salman Beigi, Peter Shor, and John Watrous. Quantum interactive proofs with short messages. *Theory of Computing*, 7(1):101–117, 2011. [arXiv:1004.0411](#). 10
- [CDGH24] 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](#). 11
- [CHTW04] 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](#). 4
- [CL95] 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*. 2, 3, 4, 8, 16, 17, 28, 30
- [Con91] Anne Condon. Space-bounded probabilistic game automata. *Journal of the ACM*, 38(2):472–494, 1991. Preliminary version in *SCT 1988*. 2
- [Con92] Anne Condon. The complexity of space bounded interactive proof systems. In *Complexity Theory: Current Research*, pages 147–189, 1992. 2, 28
- [CR23] 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](#). 28
- [DGRV11] 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. 11
- [DLG24] 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. 11
- [DLGLM23] Hugo Delavenne, François Le Gall, Yupan Liu, and Masayuki Miyamoto. Quantum Merlin-Arthur proof systems for synthesizing quantum states. *arXiv preprint arXiv:2303.01877*, 2023. [arXiv:2303.01877](#). 11
- [DS92] 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*. 2
- [FKL<sup>+</sup>16] 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](#). 2, 9, 17, 21, 43

- [FL93] 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*. [2](#), [28](#)
- [FL18] 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](#). [1](#), [12](#)
- [For89] Lance J. Fortnow. *Complexity-Theoretic Aspects of Interactive Proof Systems*. PhD thesis, Massachusetts Institute of Technology, 1989. [2](#), [8](#), [10](#), [16](#), [28](#), [30](#)
- [FPLGN21] 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](#). [11](#)
- [FR21] 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](#). [1](#), [2](#), [3](#), [9](#), [12](#), [13](#), [17](#), [43](#)
- [GKR15] 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](#). [2](#), [28](#)
- [GLS93] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*. Algorithms and Combinatorics. Springer Berlin Heidelberg, 2nd edition, 1993. [37](#)
- [GM12] Bernd Gärtner and Jiří Matoušek. *Approximation Algorithms and Semidefinite Programming*. Springer Berlin Heidelberg, 1st edition, 2012. [7](#), [37](#)
- [GMR89] 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*. [1](#)
- [GR22] 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](#). [1](#), [2](#), [3](#), [13](#)
- [GR23] 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](#). [2](#), [10](#)
- [GRZ21] 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](#). [1](#), [2](#), [3](#), [13](#)
- [GRZ24] 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](#). [2](#)

- [GS86] 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. [1](#), [4](#), [15](#)
- [HKN24] 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](#). [11](#)
- [IKW12] 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](#). [1](#)
- [INN<sup>+</sup>22] 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](#). [11](#)
- [IV12] 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](#). [4](#)
- [JJUW11] 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](#). [1](#), [4](#), [6](#), [32](#), [37](#), [38](#)
- [JY11] Rahul Jain and Penghui Yao. A parallel approximation algorithm for positive semidefinite programming. In *Proceedings of the 52nd Annual Symposium on Foundations of Computer Science*, pages 463–471, 2011. [arXiv:1104.2502](#). [37](#)
- [KKMV09] 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](#). [4](#), [5](#), [6](#), [32](#), [33](#), [34](#)
- [KLG19] 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](#). [1](#)
- [KOS18] Gillat Kol, Rotem Oshman, and Raghuvaran R Saxena. Interactive distributed proofs. In *Proceedings of the 37th ACM Symposium on Principles of Distributed Computing*, pages 255–264, 2018. [11](#)
- [KSV02] 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. [10](#)
- [KvM02] Adam R. Klivans and Dieter van Melkebeek. Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. *SIAM Journal on Computing*, 31(5):1501–1526, 2002. Preliminary version in *STOC 1999*. [ECCC:TR98-075](#). [3](#), [10](#), [15](#)
- [KW00] 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. [1](#), [2](#), [4](#), [6](#), [16](#), [17](#), [19](#), [36](#)



- [LFKN92] 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*. [1](#), [4](#)
- [LGLW23] 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](#). [5](#), [9](#), [13](#), [14](#), [38](#)
- [LGMN23] 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](#). [11](#)
- [Lip90] Richard J Lipton. Efficient checking of computations. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 207–215, 1990. [2](#), [8](#), [14](#), [16](#), [28](#)
- [Liu21] Yupan Liu. StoqMA meets distribution testing. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference*, volume 197 of *LIPICs*, pages 4:1–4:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. [arXiv:2011.05733](#). [10](#)
- [LMW24] 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](#). [11](#)
- [MV05] Peter Bro Miltersen and N Variyam Vinodchandran. Derandomizing Arthur–Merlin games using hitting sets. *Computational Complexity*, 14(3):256–279, 2005. Preliminary version in *FOCS 1999*. [3](#), [10](#), [15](#)
- [MW05] Chris Marriott and John Watrous. Quantum Arthur–Merlin games. *Computational Complexity*, 14(2):122–152, 2005. Preliminary version in *CCC 2004*. [arXiv:cs/0506068](#). [1](#), [6](#), [21](#), [31](#), [37](#)
- [MY23] 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](#). [5](#), [10](#)
- [NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 10th anniversary edition, 2010. [3](#), [11](#), [12](#), [13](#)
- [NPY20] 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 1096–1115. SIAM, 2020. [arXiv:1812.10917](#). [11](#)
- [NS03] Ashwin Nayak and Peter Shor. Bit-commitment-based quantum coin flipping. *Physical Review A*, 67(1):012304, 2003. [arXiv:quant-ph/0206123](#). [12](#)
- [NY09] 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](#). [2](#)
- [NY15] Harumichi Nishimura and Tomoyuki Yamakami. Interactive proofs with quantum finite automata. *Theoretical Computer Science*, 568:1–18, 2015. [arXiv:1401.2929](#). [2](#)



- [Per12] Attila Pereszlényi. On quantum interactive proofs with short messages. *Chicago Journal of Theoretical Computer Science*, 2012(9):1–10, 2012. [arXiv:1109.0964](#). 10
- [Ros24] 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](#). 11
- [RY22] 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](#). 10
- [Sha92] Adi Shamir.  $IP = PSPACE$ . *Journal of the ACM*, 39(4):869–877, 1992. Preliminary version in *FOCS 1990*. 1, 4
- [SR01] Robert W Spekkens and Terry Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65(1):012310, 2001. [arXiv:quant-ph/0106019](#). 12
- [Sud78] Ivan Hal Sudborough. On the tape complexity of deterministic context-free languages. *Journal of the ACM*, 25(3):405–414, 1978. Preliminary version in *STOC 1976*. 15
- [TS13] 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. 1
- [Vad99] Salil P Vadhan. *A study of statistical zero-knowledge proofs*. PhD thesis, Massachusetts Institute of Technology, 1999. 5
- [Ven91] Hari Venkateswaran. Properties that characterize LOGCFL. *Journal of Computer and System Sciences*, 43(2):380–404, 1991. Preliminary version in *STOC 1987*. 4, 15
- [Vol20] Ilya Volkovich. The untold story of SBP. In *International Computer Science Symposium in Russia*, pages 393–405. Springer, 2020. 15
- [VW16] Thomas Vidick and John Watrous. Quantum proofs. *Foundations and Trends® in Theoretical Computer Science*, 11(1-2):1–215, 2016. [arXiv:1610.01664](#). 5, 6, 7, 12, 13, 18, 19, 20, 21, 23, 32, 33
- [Wat99] John Watrous. Space-bounded quantum complexity. *Journal of Computer and System Sciences*, 59(2):281–326, 1999. Preliminary version in *CCC 1998*. 1, 13, 43
- [Wat02] 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](#). 5, 9, 14, 17, 38, 39, 40, 41
- [Wat03a] 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](#). 1, 2, 4, 16
- [Wat03b] 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](#). 1, 4, 13

- [Wat09a] John Watrous. Quantum computational complexity. *Encyclopedia of Complexity and Systems Science*, pages 7174–7201, 2009. [arXiv:0804.3401](#). 11
- [Wat09b] 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](#). 5
- [Wat16a] 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. 7, 23, 36
- [Wat16b] Thomas Watson. The complexity of estimating min-entropy. *Computational Complexity*, 25(1):153–175, 2016. [ECCC:TR12-070](#). 7, 15, 27
- [Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 1st edition, 2018. 12
- [Wil13] Mark M Wilde. *Quantum Information Theory*. Cambridge University Press, 1st edition, 2013. 11
- [dW19] Ronald de Wolf. Quantum computing: Lecture notes, 2019. [arXiv:1907.09415](#). 11
- [Yak13] Abuzer Yakaryılmaz. Public qubits versus private coins. In *Proceedings of Workshop on Quantum and Classical Complexity*, pages 45–60, 2013. [ECCC:TR12-130](#). 2
- [Zha24] 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](#). 1