A Slightly Improved Upper Bound for Quantum Statistical Zero-Knowledge

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

Yupan Liu
School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne, Switzerland
Graduate School of Mathematics, Nagoya University, Japan

Qisheng Wang
School of Computer Science, Shanghai Jiao Tong University, China

Abstract

The complexity class Quantum Statistical Zero-Knowledge (QSZK), introduced by Watrous (FOCS 2002) and later refined in Watrous (SICOMP, 2009), has the best known upper bound $\mathsf{QIP}(2) \cap \text{co-}\mathsf{QIP}(2)$, which was simplified following the inclusion $\mathsf{QIP}(2) \subseteq \mathsf{PSPACE}$ established in Jain, Upadhyay, and Watrous (FOCS 2009). Here, $\mathsf{QIP}(2)$ denotes the class of promise problems that admit two-message quantum interactive proof systems in which the honest prover is typically *computationally unbounded*, and co-$\mathsf{QIP}(2)$ denotes the complement of $\mathsf{QIP}(2)$.

We slightly improve this upper bound to $\mathsf{QIP}(2) \cap \text{co-}\mathsf{QIP}(2)$ with a *quantum linear-space* honest prover. Specifically, the honest prover uses space linear in the size of the transcript of the original QSZK proof system. A similar improvement also applies to the upper bound for the non-interactive variant NIQSZK. Our main techniques are *algorithmic* versions of the Holevo–Helstrom measurement and the Uhlmann transform, both implementable in quantum *linear* space, implying polynomial-time complexity in the state dimension, using the recent *space-efficient* quantum singular value transformation of Le Gall, Liu, and Wang (CC, to appear).

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

Keywords and phrases Quantum statistical zero-knowledge, Algorithmic Holevo–Helstrom measurement, Algorithmic Uhlmann transform

Digital Object Identifier 10.4230/LIPIcs.MFCS.2026.12

Related Version *Full Version*: https://arxiv.org/abs/2512.11597v2 [36]

Funding This work was partially supported by MEXT Q-LEAP grant No. JPMXS0120319794.
François Le Gall: Supported in part by JSPS KAKENHI grant No. JP24H00071, JST ASPIRE grant No. JPMJAP2302, and JST CREST grant No. JPMJCR24I4.
Yupan Liu: Supported in part by funding from the Swiss State Secretariat for Education, Research and Innovation (SERI), and in part by JSPS KAKENHI grant No. JP24H00071.
Qisheng Wang: Supported in part by a startup funding from Shanghai Jiao Tong University and in part by the Engineering and Physical Sciences Research Council under Grant No. EP/X026167/1.

Acknowledgements A preliminary version of Section 3 (whose informal theorems are summarized in Theorems 2 and 6) appeared in Section 5 of the second arXiv version of [37] and in Section 6.3 of the second-named author's PhD thesis [38]. Part of the work of Qisheng Wang was done when the author was with the School of Informatics, University of Edinburgh, United Kingdom. The authors thank Harumichi Nishimura and Thomas Vidick for helpful feedback on a preliminary version of the manuscript. The circuit diagrams were drawn using the Quantikz package [30].

Declaration on GenAI/LLM use ChatGPT was used only for proofreading the manuscript, including identifying possible calculation errors and suggesting changes, with all corresponding changes verified and made by the authors.

1 Introduction

Quantum Statistical Zero-Knowledge (QSZK) is the complexity class of promise problems that admit (single-prover) quantum interactive proof systems with the statistical zero-knowledge property. Intuitively, this property requires that *any* verifier interacting with the honest prover (implicitly on *yes* instances) gains no information from the interaction beyond the validity of the statement. A weaker variant with *honest* verifiers, denoted by $\mathsf{QSZK}_{\mathrm{HV}}$,[1] was first investigated in [56]. The resulting class shares most of the basic properties with its classical counterpart SZK [47, 22], including that such proof systems can be parallelized to *two messages*. A few years later, it was shown in [58] that removing the honest-verifier restriction does not reduce the computational power, establishing the equivalence $\mathsf{QSZK} = \mathsf{QSZK}_{\mathrm{HV}}$.[2]

Parallel to the classical Statistical Difference Problem (SD) in [47], a complete characterization of QSZK was established in [56],[3] namely, the Quantum State Distinguishability Problem (QSD$[\alpha, \beta]$). This promise problem asks whether two quantum states ρ_0 and ρ_1, whose purifications are prepared by polynomial-size quantum circuits Q_0 and Q_1, respectively, satisfy $\mathrm{T}(\rho_0, \rho_1) \geq \alpha$ (for *yes* instances) or $\mathrm{T}(\rho_0, \rho_1) \leq \beta$ (for *no* instances), where the trace distance is defined as $\mathrm{T}(\rho_0, \rho_1) \coloneqq \frac{1}{2}\mathrm{Tr}|\rho_0 - \rho_1|$. For convenience, we refer to QSD$[\alpha(n), \beta(n)]$ with $\alpha(n) - \beta(n) \geq 1/\operatorname{poly}(n)$ as GapQSD.

Using this complete problem, the best known upper bound for QSZK was shown in [56]:

$$\mathsf{QSZK} \subseteq \mathsf{QIP}(2) \cap \mathsf{co\text{-}QIP}(2) \cap \mathsf{PSPACE}.$$

Here, QIP(2) denotes the class of problems admitting two-message quantum interactive proof systems. Notably, the PSPACE containment essentially follows from an NC(poly) algorithm for GapQSD. The development of more sophisticated NC(poly) algorithms for characterizing quantum interactive proof systems subsequently led to the celebrated result $\mathsf{QIP} = \mathsf{PSPACE}$ [27]. In particular, an intermediate step proving $\mathsf{QIP}(2) \subseteq \mathsf{PSPACE}$ in [28] immediately simplified the state-of-the-art upper bound for QSZK to

$$\mathsf{QSZK} \subseteq \mathsf{QIP}(2) \cap \mathsf{co\text{-}QIP}(2).$$

By contrast, the best known upper bound for the classical counterpart SZK is $\mathsf{AM} \cap \mathsf{coAM}$, as proven in [14, 2], where AM denotes the class of problems admitting two-message classical interactive proof systems in which the first message (from the verifier) consists *solely of (public) random coins*. This comparison naturally raises the following intriguing question:

▶ **Problem 1.** Could the current upper bound for QSZK be improved, even slightly?

1.1 Main results

In this work, we make progress on Problem 1 by restricting the computational power of the honest prover in the proof systems underlying the $\mathsf{QIP}(2) \cap \mathsf{co\text{-}QIP}(2)$ upper bound [56], from being computationally *unbounded* to quantum *linear* space (and therefore quantum single-exponential time), as stated in Theorems 2 and 3.

---

[1] For instance, in Graph Non-isomorphism [21], where the problem is to decide whether two given graphs G_0 and G_1 are non-isomorphic, an honest verifier queries only the graphs G_0 and G_1, whereas an arbitrary verifier may present some graph G' in an attempt to extract additional information.

[2] When the verifier is allowed non-unitary operations, the honest-verifier notion becomes subtle: there is a variant of $\mathsf{QSZK}_{\mathrm{HV}}$, introduced in [10], that contains PSPACE.

[3] The QSZK containment of QSD$[\alpha(n), \beta(n)]$ in [56] holds only when $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$, the so-called *polarizing regime*. Slight improvements for the SZK containment of SD beyond this regime were obtained in [4] and were later partially extended to the QSZK containment of QSD in [39].

▶ **Theorem 2** (Informal version of Theorem 17). GapQSD *is in* QIP(2) *with a quantum linear-space honest prover.*

The promise problem underlying the co-QIP(2) proof system in [56] is the Quantum State Closeness Problem (QSC), which is the complement of QSD. This problem is closely related to F^2Est (to be specified later) via the Fuchs–van de Graaf inequality [15].

▶ **Theorem 3** (Informal version of Theorem 24). GapF^2Est *is in* QIP(2) *with a quantum linear-space honest prover.*

Here, the promise problem Quantum Squared Fidelity Estimation (F^2Est$[\alpha, \beta]$) asks whether $F^2(\rho_0, \rho_1) \geq \alpha$ for *yes* instances or $F^2(\rho_0, \rho_1) \leq \beta$ for *no* instances, where the squared fidelity is defined as $F^2(\rho_0, \rho_1) := \mathrm{Tr}\left|\sqrt{\rho_0}\sqrt{\rho_1}\right|^2$. As with GapQSD, we refer to F^2Est$[\alpha(n), \beta(n)]$ with $\alpha(n) - \beta(n) \geq 1/\operatorname{poly}(n)$ as GapF^2Est.

Computational efficiency of the honest prover compared to the general case. Approximately implementing the honest prover's strategies in *general* quantum interactive proof systems has been studied in [43, Section II.C], which requires quantum *polynomial* space. In contrast, our results (Theorems 2 and 3) achieve a *polynomial* improvement in space complexity for implementing the honest prover's strategies in *specific* two-message quantum interactive proof systems for GapQSD and GapF^2Est. Moreover, the corresponding time complexity is *exponentially* improved with respect to the state dimension.[4]

This distinction appears fundamental and challenging to close: even combining the SDP-based approach of [43] with the space-efficient QSVT from [37] still requires at least quantum *quadratic* space to approximately implement the honest prover's strategy in the general case. Further discussion is deferred to Section 1.4.

1.1.1 Implications on QSZK and NIQSZK

The main result of this work follows directly from combining Theorems 2 and 3:

▶ **Corollary 4.** QSZK *is in* QIP(2) ∩ co-QIP(2) *with a quantum linear-space (and thus single-exponential-time) honest prover. More precisely, the space complexity of the honest prover in the resulting* QIP(2) ∩ co-QIP(2) *proof system is linear in the size of the transcript in the original* QSZK *proof system.*

In addition to QSZK, a non-interactive variant called NIQSZK was studied in [34]. In this model, the prover and verifier share prior entanglement (EPR pairs), and only the prover sends a message. As noted in [35], a direct upper bound for NIQSZK is qq-QAM, a subclass of QIP(2) in which the verifier's message consists of half of the shared EPR pairs ("quantum public coins"). A natural complete problem for NIQSZK is the Quantum State Closeness to Maximally Mixed Problem (QSCMM) [34, 3, 9], obtained by fixing the state ρ_0 in QSC to be the maximally mixed state.

Noting that QSCMM$[1/3, 2/3]$ is NIQSZK-hard,[5] Theorem 3 also yields the following:

▶ **Corollary 5.** NIQSZK *is in* qq-QAM *with a quantum linear-space (and thus single-exponential-time) honest prover. More precisely, the space complexity of the honest prover in the resulting* qq-QAM *proof system is linear in the size of the transcript in the original* NIQSZK *proof system.*

[4] For a detailed algorithmic comparison, see the discussion in the first paragraph of Section 1.5.

[5] If n denotes the number of qubits that the state-preparation circuits act on and $r(n)$ is the number of qubits in the resulting states, then QSCMM$[1/r, 1 - 1/r]$ is NIQSZK-hard [9, Section 8.1].

To justify that our notion of linearity in Corollaries 4 and 5 captures the *nature* of quantum interactive proof systems, we view the inclusions $\mathsf{QSZK} \subseteq \mathsf{QIP}(2) \cap \mathsf{co\text{-}QIP}(2)$ and $\mathsf{NIQSZK} \subseteq \mathsf{qq\text{-}QAM}$ primarily as transformations from one class of quantum interactive proof systems (e.g., proof systems with the statistical zero-knowledge property) to another class with distinct structural features (e.g., being parallelizable to two messages, which is stronger than the usual three-message parallelization in [32, 31]). From this perspective, the notion of linearity should be defined in terms of the underlying proof system, which motivates our choice to measure it by the *transcript* of the original proof system, whose size has the same order as the verifier's message length in the resulting two-message proof systems.

1.2 Revisiting the upper bound QIP(2) ∩ co-QIP(2)

Before explaining the proofs of Theorems 2 and 3, we first revisit the $\mathsf{QIP}(2) \cap \mathsf{co\text{-}QIP}(2)$ upper bound established in [56].

GapQSD ∈ QIP(2). The QIP(2) part follows directly from the QIP(2) proof system of GapQSD [56, Section 4.2]. This proof system can be seen as a computational version of quantum hypothesis testing (see Problem 13). In particular, the verifier $\mathcal{V}$ proceeds as follows:

(i) $\mathcal{V}$ sends a quantum state ρ, promised to be either ρ_0 or ρ_1.

(ii) $\mathcal{V}$ receives a guess $b \in \{0,1\}$,[6] and accepts if ρ_b exactly matches the state ρ.

Notably, this proof system has classical counterparts, such as the zero-knowledge protocol for Graph Non-isomorphism [21]. The prover aims to maximize the acceptance probability but can only perform *a two-outcome measurement* on the received state. By the Holevo–Helstrom bound [26, 25], the optimal success probability is $\frac{1}{2}+\frac{1}{2}\mathrm{T}(\rho_0,\rho_1)$, which directly yields an upper bound on the acceptance probability for *no* instances. The optimal measurement $\{\Pi_0,\Pi_1\}$, known as the *Holevo–Helstrom measurement*, has been used to achieve the acceptance probability lower bound for *yes* instances.

GapF²Est ∈ QIP(2). The co-QIP(2) part boils down to the QIP(2) proof system of GapF²Est, as presented in [56, Section 4.3]. This proof system can be interpreted as a computational version of the Uhlmann fidelity test (see Problem 18) and does not have a direct classical counterpart. A natural starting point is testing the closeness between a quantum state ρ and a pure state $|\phi\rangle$, as in [59, Exercise 9.2.2]. The test measures ρ using a two-outcome measurement $\{|\phi\rangle\langle\phi|, I-|\phi\rangle\langle\phi|\}$. The test succeeds if the first outcome is obtained, and the success probability $\mathrm{Tr}(|\phi\rangle\langle\phi|\rho)$ coincides exactly with the squared (Uhlmann) fidelity $\mathrm{F}^2(|\phi\rangle\langle\phi|,\rho)$. In the general case, the verifier $\mathcal{V}$ proceeds as follows:

(i) $\mathcal{V}$ prepares a purification $|\psi_0\rangle$ of ρ_0 by the circuit Q_0 and sends the non-output qubits.

(ii) $\mathcal{V}$ receives these qubits back, expected to be transformed by the prover. The modified "purification" of ρ_0, including the output and received qubits, is denoted by ρ_{ψ_0}.

(iii) $\mathcal{V}$ measures ρ_{ψ_0} using $\{|\psi_1\rangle\langle\psi_1|, I-|\psi_1\rangle\langle\psi_1|\}$ and accepts if the first outcome occurs.

As in the QIP(2) part, the prover aims to maximize the acceptance probability but is restricted to applying *a dimension-preserving quantum channel* $\Phi(\cdot)$ to the received qubits. By a corollary of Uhlmann's theorem [50] (Corollary 20), proven in [56, Section 4.3],

[6] Although the prover may send an arbitrary quantum state σ, the verifier can obtain the classical bit $b \in \{0,1\}$ by measuring the first qubit of σ in the computational basis, ignoring all remaining qubits, and denoting the outcome by b.

the maximum acceptance probability is $\mathrm{F}^2(\rho_0, \rho_1)$, which implies an upper bound on the acceptance probability for *no* instances. The optimal channel $\Phi_\star(\cdot) = U_\star(\cdot)U_\star^\dagger$, known as the *Uhlmann transform*, is determined by the chosen purifications of ρ_0 and ρ_1, and has been used to obtain the acceptance probability lower bound for *yes* instances.

1.3 Proof techniques

We now provide approximate implementations of the honest prover strategies described in Section 1.2, thereby establishing Theorems 2 and 3. A central ingredient in our constructions is a *space-efficient* polynomial approximation of the sign function [37].

The importance of space-efficient polynomial approximations. The quantum singular value transformation (QSVT) framework [18] reduces the design of quantum algorithms to finding good polynomial approximations P_d^{f} of a target function $f(x)$ in an appropriate form ("pre-processing"), such as rotation-angle representations [18] or coefficients in Chebyshev-type truncations [43, 37]. Moreover, the efficiency of the resulting quantum algorithms is largely determined by the degree d.[7] Importantly, d must be *exponential* in n for QSVT-based approaches to estimating the trace distance [53, 54] or the fidelity [55, 17, 43, 51] between quantum states whose purifications are on n qubits, even to within *constant* precision. This requirement arises from the *square-root*-rank dependence in quantum query complexity lower bounds [11, 8, 12].

Therefore, to establish Theorems 2 and 3, we rely on space-efficient polynomial approximations $P_{d'}$ from [37], which can be computed *simultaneously* in $\mathrm{poly}(d)$ time and $O(\log d)$ space, yielding $2^{O(n)}$ time and $O(n)$ space. Here, the original degree d comes from the time-efficiently computable polynomials [18], and the new degree $d' = O(d)$ is kept explicit to distinguish the space-efficient version.[8]

1.3.1 Algorithmic Holevo–Helstrom measurement

As discussed in Section 1.2, the honest prover's strategy underlying $\textsc{GapQSD} \in \mathsf{QIP}(2)$ is the Holevo–Helstrom measurement $\{\Pi_0, \Pi_1\}$, where $\Pi_1 \coloneqq I - \Pi_0$. The decomposition of the trace distance in [54, Equation (8)] yields an explicit form of Π_0 (see Proposition 15):

$$\mathrm{T}(\rho_0, \rho_1) = \mathrm{Tr}(\Pi_0\rho_0) - \mathrm{Tr}(\Pi_0\rho_1), \quad \text{where } \Pi_0 \coloneqq \frac{I}{2} + \frac{1}{2}\mathrm{sgn}^{(\mathrm{SV})}\Big(\frac{\rho_0 - \rho_1}{2}\Big).$$

Our first technical contribution is an explicit implementation of $\tilde{\Pi}_0$, which approximately realizes the honest prover's strategy in Theorem 2 and ensures that, for *yes* instances, the maximum acceptance probability remains at least $\frac{1}{2} + \frac{1}{2}\mathrm{T}(\rho_0, \rho_1) - 2^{-n}$:

▶ **Theorem 6** (Informal version of Theorem 16). *For quantum states ρ_0 and ρ_1 specified in* GapQSD*, whose purifications can be prepared by n-qubit polynomial-size quantum circuits Q_0 and Q_1, the Holevo–Helstrom measurement $\{\Pi_0, \Pi_1\}$ can be approximately implemented in quantum single-exponential time and linear space with additive error 2^{-n}.*

[7] The (classical) pre-processing in the time-efficient QSVT [18] uses $\mathrm{poly}(d)$ time, so the corresponding space complexity is trivially bounded above by $\mathrm{poly}(d)$.

[8] To make a polynomial approximation space-efficiently computable, as in [37, Section 3.1], this increase in degree from d to d' maintains the polynomial approximation error at $O(\epsilon)$, compared with the original approximation error ϵ associated with P_d.

Our approach is inspired by [54, Section III.A] (see also [37, Section 4.2]). We start with the one-bit precision phase estimation [33], commonly referred to as the Hadamard test [1], which has previously been used in space-bounded quantum computation [49, 13]. This procedure enables an explicit implementation of a two-outcome measurement $\{\Pi, I-\Pi\}$, where $\Pi = (I+U)/2$, such that the acceptance probability is $\mathrm{Tr}(\Pi\rho)$, provided that the unitary U can be *approximately* implemented via a block-encoding.[9]

To achieve this, we adopt the *space-efficient* quantum singular value transformation [37], specifically employing a polynomial approximation $P^{\mathrm{sgn}}_{d'}$ of the sign function. Our explicit implementation of $\tilde{\Pi}_0$ is then accomplished as follows:

(1) Using the linear-combinations-of-unitaries technique in [5, 18] (see also the space complexity analysis in [37, Lemma 3.22]), one can implement an exact block-encoding of $(\rho_0-\rho_1)/2$, namely $\langle\bar{0}|U_{(\rho_0-\rho_1)/2}|\bar{0}\rangle = (\rho_0-\rho_1)/2$, in quantum $O(n)$ space.

(2) Using the space-efficient QSVT for the sign function [37, Corollary 3.25], one can approximately implement a block-encoding of $\mathrm{sgn}^{(\mathrm{SV})}\left(\frac{\rho_0-\rho_1}{2}\right)$ in quantum $O(n)$ space.

The proof of Theorem 6 is then completed by analyzing the errors introduced by the polynomial approximation $P^{\mathrm{sgn}}_{d'}$ and the associated space-efficient QSVT implementation, which together accumulate to the desired bound of 2^{-n}, as detailed in Section 3.1.

1.3.2 Algorithmic Uhlmann transform

As discussed in Section 1.2, the honest prover's strategy for $\textsc{GapF}^2\textsc{Est} \in \mathsf{QIP}(2)$ is given by the Uhlmann transform $\Phi_\star(\cdot) = U_\star(\cdot)U_\star^\dagger$. Let $|\psi_0\rangle$ and $|\psi_1\rangle$ be purifications of the quantum states ρ_0 and ρ_1 on register A, defined on two registers (A,R), where R serves as the reference register. An explicit form of $U_\star$ is provided implicitly in [29, Lemma 6] (see Lemma 21), yielding an alternative expression of the squared Uhlmann fidelity:

$$\mathrm{F}^2(\rho_0,\rho_1) = \left|\langle\psi_0|\left(I^{\mathsf{A}}\otimes U_\star^{\mathsf{R}}\right)|\psi_1\rangle\right|^2, \quad \text{where } U_\star \coloneqq \mathrm{sgn}^{(\mathrm{SV})}(\mathrm{Tr}_{\mathsf{A}}(|\psi_0\rangle\langle\psi_1|)).$$

Our second technical contribution is an explicit implementation of $\Phi_\star(\cdot)$, which approximately realizes the honest prover's strategy in Theorem 3. This implementation guarantees that, for *yes* instances, the maximum acceptance probability remains at least $\mathrm{F}^2(\rho_0,\rho_1)-2^{-n}$:

▶ **Theorem 7** (Informal version of Theorem 22)**.** *For quantum states ρ_0 and ρ_1 specified in* $\textsc{GapF}^2\textsc{Est}$*, whose purifications can be prepared by n-qubit polynomial-size quantum circuits Q_0 and Q_1, the Uhlmann transform $\Phi_\star(\cdot)$ can be approximately implemented in quantum single-exponential time and linear space with additive error 2^{-n}.*

Our approach is inspired by [51, Section 5.1]. Analogous to Section 1.3.1, we aim to use the space-efficient QSVT associated with the sign function, as established in [37, Section 3], corresponding to the space-efficient polynomial approximation $P^{\mathrm{sgn}}_{d'}$. A technical challenge is to obtain an *exact* block-encoding of $X_{\mathrm{Uhl}} \coloneqq \mathrm{Tr}_{\mathsf{A}}(|\psi_0\rangle\langle\psi_1|)$. A straightforward approach for realizing the partial trace is to contract $|\mathsf{A}| = \log\dim(\mathcal{H}_{\mathsf{A}})$ EPR pairs, yielding only an exact encoding of $X_{\mathrm{Uhl}}/\dim(\mathcal{H}_{\mathsf{A}})$, as shown in [43, Section II.D]. Handling this normalization factor $\dim(\mathcal{H}_{\mathsf{A}})$ requires additional effort and leads to an implementation that is both less efficient and conceptually more involved. Notably, an exact block-encoding W of X_{Uhl} was recently proposed in [51, Section 5.1]. Leveraging this key ingredient, our explicit implementation of $\Phi_\star(\cdot)$ proceeds as follows:

[9] Following [17, Lemma 9], given a block-encoding of a linear operator, the Hadamard test naturally extends to implement $\Pi = (I+A)/2$ with acceptance probability $\mathrm{Re}(\mathrm{Tr}(\Pi\rho))$.

(1) Following [51, Section 5.1] (see Lemma 25), one can implement an exact block-encoding W of $\mathrm{Tr}_{\mathsf{A}}(|\psi_0\rangle\langle\psi_1|)$, namely $\langle\bar{0}|W|\bar{0}\rangle = \mathrm{Tr}_{\mathsf{A}}(|\psi_0\rangle\langle\psi_1|)$, using quantum $O(n)$ space.
(2) Using the space-efficient QSVT associated with the sign function [37, Corollary 3.25], a block-encoding of $\mathrm{sgn}^{(\mathrm{SV})}(\mathrm{Tr}_{\mathsf{A}}(|\psi_0\rangle\langle\psi_1|))$ can be approximately implemented in quantum $O(n)$ space.

Similar to Section 1.3.1, the proof of Theorem 7 is completed by analyzing the errors introduced by the polynomial approximation $P_{d'}^{\mathrm{sgn}}$ and the associated space-efficient QSVT implementation. These errors combine to the desired bound of 2^{-n}, as stated in Section 4.1.

1.4 Discussion: Improving upper bounds for QSZK

1.4.1 Improving upper bounds for QSZK

The main open problem is to further improve the upper bounds for QSZK and NIQSZK beyond our results (Corollaries 4 and 5). Since the best known upper bound for the classical counterpart SZK is AM ∩ coAM, as established in [14, 2], this inclusion naturally motivates the following question:

(a) Could the quantum upper bound for QSZK be improved to a subclass of QIP(2) defined in terms of "public coins" quantum interactive proof systems [42, 35], such as qq-QAM ∩ co-qq-QAM?

An intriguing question concerns the *classical* upper bound for QSZK, whose best known bound is PSPACE and is believed "almost certainly can be improved" in [56, Section 7]:

(b) Could the classical upper bounds for QSZK and NIQSZK be improved to any subclass of PSPACE?

As noted at the beginning of this section, the classical upper bound PSPACE for complexity classes ranging from QSZK to QIP [56, 28, 27] is obtained via NC(poly) algorithms for the corresponding problems. Consequently, making progress on Question b likely requires techniques that go beyond this paradigm.

1.4.2 Improving the computational efficiency of the honest prover

As noted in Section 1.1, a naïve approach consists of combining the method underlying [43, Theorem II.4] with the space-efficient QSVT from [37]. Let $\omega(\mathcal{V})$ denote the maximum acceptance probability of the quantum interactive proof system $\mathcal{P} \rightleftharpoons \mathcal{V}$. Informally, this combination yields a quantum algorithm that computes $\omega(\mathcal{V})$ to within constant precision and simultaneously produces an SDP solution specifying the associated quantum states. This algorithm requires $O(n)$ iterations on a block-encoding that initially acts on $O(n)$ qubits. The honest prover's strategy is then approximately implemented via the algorithmic Uhlmann transform constructed from these states. Since the number of required ancillary qubits in this algorithm eventually grows to $O(n^2)$, the resulting algorithm still requires at least *quadratic* quantum space.[10]

Noting that the notion of honest-prover efficiency in our results (Theorems 2 and 3) appears specifically tailored for *two-message* quantum interactive proof systems, the distinction between our results and the general case suggests the following question:

[10] See also the discussion in [37, Section 1.6].

(c) Could the honest prover's strategy in any two-message quantum interactive proof system be approximately implemented in quantum *linear* space, meaning that the space complexity of the algorithmic implementation scales *linearly* with the number of qubits on which the verifier's message-preparing circuit acts?

A natural starting point for Question c is to revisit the qq-QAM containment of the Close Image to Totally Mixed Problem (CITM) [35].[11] Here, as a qq-QAM-hard problem, CITM generalizes QSCMM, defined via $\min_\sigma \mathrm{T}(\Phi(\sigma), (I/2)^{\otimes r})$, where the quantum channel $\Phi(\cdot)$ can be implemented by a polynomial-size mixed-state quantum circuit.

Noting that the proof system in [35, Figure 2] is structurally similar to the QIP(2) containment of GapF^{2}Est, one might expect that Theorems 3 and 7 extend naturally to this more general setting. However, the honest prover now also needs to construct a nearly optimal $\tilde{\sigma}_\star$ satisfying $\mathrm{T}(\Phi(\tilde{\sigma}_\star), (I/2)^{\otimes r}) \approx_\epsilon \min_\sigma \mathrm{T}(\Phi(\sigma), (I/2)^{\otimes r})$. It remains unclear how to achieve such a construction in quantum linear space, and this difficulty constitutes a technical barrier to resolving Question c. Notably, an affirmative answer to that question would yield a tighter characterization of QIP(2).

1.5 Related works

An approximate implementation of the Uhlmann transform was previously studied in [43, Section II.D] under the name "Algorithmic Uhlmann's Theorem", in the context of unitary-synthesis complexity classes (e.g., unitaryPSPACE; see also [6]). The central distinction between the prior construction in [43, Theorem II.5][12] and Theorem 22 (whose informal version is Theorem 7) is that our construction achieves an *exponentially* improved time complexity when measured in the state dimension $N \coloneqq 2^n$. This improvement arises because our construction requires only quantum *linear* space, whereas theirs requires quantum *polynomial* space. As a consequence, our resulting time complexity is $2^{O(n)} = \mathrm{poly}(N)$, while theirs is $2^{p(n)} = N^{q(n)}$ for some functions $p(n)$ and $q(n) \coloneqq p(n)/n$ that are both polynomial in n.

Beyond the algorithmic perspective, it is worth noting that a *stability* result of the Uhlmann transform, referred to as "robust rigidity", has been recently investigated in [7].

Other notions of the honest-prover efficiency

A natural, though folklore, notion of honest-prover efficiency is that of *in-class* interactive proofs, formalized in [24, Definition 1]. This notion means that for any promise problem in a complexity class C, there exists a proof system $P \rightleftharpoons V$ such that the verifier decides the problem and the honest prover's strategy can be (approximately) implemented in C. This notion applies to complexity classes such as $\mathsf{P}^{\#\mathsf{P}}$ and PSPACE [41, 48] via the sum-check protocol, as well as to an intermediate class PreciseQCMA [24].[13] The same notion naturally extends to other settings, including in-class space-bounded classical interactive proofs for P [23], in-class quantum interactive proofs for BQPSPACE [43], and in-class streaming proofs for BQL [19].

[11] It is worth noting that the qq-QAM containment of CITM$[a, b]$, as stated in [35, Lemma 4.1], holds only for the constant parameter regime $(1-a)^2 > 1-b^2$. This is because the underlying proof system in [35, Figure 2] is essentially designed for the closeness testing problem associated with $\max_\sigma \mathrm{F}^2(\Phi(\sigma), (I/2)^{\otimes r})$.

[12] For the formal statement, please refer to Theorem 7.4 in the arXiv version of [43].

[13] The equivalence of PreciseQCMA and $\mathsf{NP}^{\mathsf{PP}}$ is established in [44, 16].

A more quantitative, practically motivated notion is that of *doubly-efficient* interactive proofs (see the survey [20]), in which a polynomial-time (honest) prover ideally delegates the computation to an almost-linear-time verifier via interactions, with [23] serving as a canonical example and subsequent improvements in [46].

2 Preliminaries

We assume that the reader has a basic familiarity with quantum computation and quantum information theory. For an introduction, the textbooks by [45, 60] offer accessible starting points. For a more comprehensive overview of quantum complexity theory, see [57]; for a survey specifically focused on quantum interactive proof systems, refer to [52].

For convenience, we adopt the following notations throughout this work: (i) the symbol $|\bar{0}\rangle$ denotes an a-qubit state $|0\rangle^{\otimes a}$ for $a > 1$. (ii) the logarithmic function log is taken to be base-2 by default, i.e., $\log(x) \coloneqq \log_2(x)$ for all positive real numbers x. (iii) hidden log factors are suppressed using the notation $\widetilde{O}(f) \coloneqq O(f \operatorname{polylog}(f))$.

2.1 Closeness measures for quantum states and the testing problems

We begin by defining quantum states. A square matrix ρ is called a *quantum state* if ρ is positive semi-definite and has unit trace, that is, $\mathrm{Tr}(\rho) = 1$.

2.1.1 Closeness measures for quantum states

We then introduce two closeness measures:

▶ **Definition 8** (Trace distance). *Let ρ_0 and ρ_1 be two (possibly mixed) quantum states. The trace distance between ρ_0 and ρ_1 is defined by* $\mathrm{T}(\rho_0, \rho_1) \coloneqq \frac{1}{2}\mathrm{Tr}|\rho_0 - \rho_1| = \frac{1}{2}\|\rho_0 - \rho_1\|_1$.

▶ **Definition 9** (Uhlmann fidelity). *Let ρ_0 and ρ_1 be two (possibly mixed) quantum states. The (Uhlmann) fidelity between ρ_0 and ρ_1 and its square are defined by*

$$\mathrm{F}(\rho_0, \rho_1) \coloneqq \mathrm{Tr}|\sqrt{\rho_0}\sqrt{\rho_1}| = \|\sqrt{\rho_0}\sqrt{\rho_1}\|_1 \quad \text{and} \quad \mathrm{F}^2(\rho_0, \rho_1) \coloneqq \|\sqrt{\rho_0}\sqrt{\rho_1}\|_1^2.$$

The trace distance reaches its minimum value of 0 when ρ_0 equals ρ_1, while the (squared) fidelity attains its maximum of 1. Conversely, the trace distance reaches its maximum value of 1 when the supports of ρ_0 and ρ_1 are orthogonal, and the squared fidelity attains its minimum of 0. Importantly, the trace distance and the (squared) fidelity are related by the well-known Fuchs–van de Graaf inequalities:

▶ **Lemma 10** (Trace distance vs. fidelity, adapted from [15]). *Let ρ_0 and ρ_1 be two (possibly mixed) quantum states. Then, it holds that*

$$1 - \mathrm{F}(\rho_0, \rho_1) \leq \mathrm{T}(\rho_0, \rho_1) \leq \sqrt{1 - \mathrm{F}^2(\rho_0, \rho_1)}.$$

Furthermore, the operational interpretations of the trace distance and the (squared) fidelity, namely the Holevo–Helstrom bound [26, 25] and Uhlmann's theorem [50, 29], together with the corresponding *optimal* operations that achieve these maxima, play a central role in this work. To keep the technical sections self-contained, we defer the formal statements of these results to Sections 3 and 4, respectively.

2.1.2 Closeness testing of quantum states via state-preparation circuits

Next, we introduce two promise problems defined with respect to the trace distance:

▶ **Definition 11** (Quantum State Distinguishability, QSD$[\alpha, \beta]$, adapted from [56, Section 3.3])**.** *Let Q_0 and Q_1 be polynomial-size quantum circuits acting on n qubits, each with r designated output qubits. For $b \in \{0,1\}$, let ρ_b denote the quantum state obtained by applying Q_b to the initial state $|0\rangle^{\otimes n}$ and tracing out the non-output qubits. Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions. The problem is to decide whether:*

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

▶ **Definition 12** (Quantum State Closeness, QSC$[\beta, \alpha]$, adapted from [34, Section 3])**.** *Let Q_0 and Q_1 be quantum circuits defined as in Definition 11, and let ρ_0 and ρ_1 denote the corresponding quantum states obtained from these circuits. Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions. The problem is to decide whether:*

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

It is evident that QSC is the complement of QSD. Beyond Definitions 11 and 12, this work also focuses on two additional closeness testing problems:

(1) An important special case of Definition 12 is the Quantum State Closeness to Maximally Mixed State (QSCMM). This problem arises when ρ_0 is fixed to be the $r(n)$-qubit maximally mixed state $(I/2)^{\otimes r}$, and Q_0 is the circuit that prepares $r(n)$ EPR pairs acting on $n = 2r$ qubits.

(2) A closeness testing problem defined via the squared fidelity, in particular, the promise problem Quantum Squared Fidelity Estimation (F^2Est$[\alpha, \beta]$). This problem asks whether $\mathrm{F}^2(\rho_0, \rho_1) \geq \alpha(n)$ for *yes* instances or $\mathrm{F}^2(\rho_0, \rho_1) \leq \beta(n)$ for *no* instances.

3 Algorithmic Holevo–Helstrom measurement and its implication

In this section, we introduce an *algorithmic* version of the Holevo–Helstrom measurement that nearly achieves the optimal probability for discriminating between states ρ_0 and ρ_1. We start by defining the Computational Quantum Hypothesis Testing Problem, which assumes access to the descriptions of the corresponding state-preparation circuits:

▶ **Problem 13** (Computational Quantum Hypothesis Testing Problem)**.** Let Q_0 and Q_1 be two polynomial-size quantum circuits acting on n qubits and having r designated output qubits. Let ρ_b be the quantum state obtained by performing Q_b on the initial state $|0\rangle^{\otimes n}$ and tracing out the non-output qubits for $b \in \{0,1\}$. Now, consider the following computational task:

- **Input:** A quantum state ρ, either ρ_0 or ρ_1, is chosen uniformly at random.
- **Output:** A bit b indicates that $\rho = \rho_b$.

The goal is to maximize the probability that the test in Problem 13 succeeds, which can be achieved by performing an appropriate measurement on the given state ρ.

Information-theoretic background. For the Quantum Hypothesis Testing Problem analogous to Problem 13, where ρ_0 and ρ_1 are not necessarily efficiently preparable, the maximum success probability to discriminate between quantum states ρ_0 and ρ_1 is given by the celebrated Holevo–Helstrom bound:

▶ **Theorem 14** (Holevo–Helstrom bound, [26, 25]). *Given a quantum state ρ, either ρ_0 or ρ_1, that is chosen uniformly at random, the maximum success probability to discriminate between quantum states ρ_0 and ρ_1 is given by $\frac{1}{2} + \frac{1}{2}\mathrm{T}(\rho_0, \rho_1)$.*

Noting that the trace distance can be written as[14]

$$\mathrm{T}(\rho_0, \rho_1) \coloneqq \frac{1}{2}\mathrm{Tr}|\rho_0 - \rho_1| = \frac{1}{2}\left(\mathrm{Tr}\left(\rho_0 \ \mathrm{sgn}^{(\mathrm{SV})}\left(\frac{\rho_0 - \rho_1}{2}\right)\right) - \mathrm{Tr}\left(\rho_1 \ \mathrm{sgn}^{(\mathrm{SV})}\left(\frac{\rho_0 - \rho_1}{2}\right)\right)\right), \quad (1)$$

one can directly obtain an explicit form of the optimal two-outcome measurement $\{\Pi_0, \Pi_1\}$ that achieves Theorem 14 and satisfies $\mathrm{T}(\rho_0, \rho_1) = \mathrm{Tr}(\Pi_0\rho_0) - \mathrm{Tr}(\Pi_0\rho_1)$:

▶ **Proposition 15** (Explicit form of the Holevo–Helstrom measurement). *An optimal two-outcome measurement $\{\Pi_0, \Pi_1\}$ that maximizes the discrimination probability in quantum hypothesis testing and achieves the Holevo–Helstrom bound (Theorem 14) is given by*

$$\Pi_0 = \frac{I}{2} + \frac{1}{2}\mathrm{sgn}^{(\mathrm{SV})}\left(\frac{\rho_0 - \rho_1}{2}\right) \quad \text{and} \quad \Pi_1 = \frac{I}{2} - \frac{1}{2}\mathrm{sgn}^{(\mathrm{SV})}\left(\frac{\rho_0 - \rho_1}{2}\right).$$

Algorithmic implementation. Using the space-efficient quantum singular value transformation in [37, Section 3], the Holevo–Helstrom measurement specified in Proposition 15 can be approximately implemented in quantum *single-exponential* time and *linear* space. We refer to this explicit implementation as the *algorithmic Holevo–Helstrom measurement*:

▶ **Theorem 16** (Algorithmic Holevo–Helstrom measurement). *Let ρ_0 and ρ_1 be quantum states prepared by n-qubit quantum circuits Q_0 and Q_1, respectively, as defined in Problem 13. An approximate version of the Holevo–Helstrom measurement Π_0 specified in Proposition 15, denoted as $\tilde{\Pi}_0$, can be implemented so that*

$$\mathrm{T}(\rho_0, \rho_1) - 2^{-n} \leq \mathrm{Tr}(\tilde{\Pi}_0\rho_0) - \mathrm{Tr}(\tilde{\Pi}_0\rho_1) \leq \mathrm{T}(\rho_0, \rho_1). \quad (2)$$

The quantum circuit implementation of $\tilde{\Pi}_0$, acting on $O(n)$ qubits, requires $2^{O(n)}$ queries to the quantum circuits Q_0 and Q_1, as well as $2^{O(n)}$ one- and two-qubit gates. Moreover, the circuit description can be computed in deterministic time $2^{O(n)}$ and space $O(n)$.

Additionally, we demonstrate an implication of our algorithmic Holevo–Helstrom measurement in Theorem 16. By inspecting the (honest-verifier) quantum statistical zero-knowledge protocol ("distance test") for $\mathrm{QSD}[\alpha, \beta]$ with constants $\alpha^2 > \beta$ in [56, Section 4.2], we obtain the QIP(2) part in Corollary 4, since GapQSD is QSZK-hard:

▶ **Theorem 17** (GapQSD is in QIP(2) with a quantum linear-space honest prover). *There exists a two-message quantum interactive proof system for $\mathrm{QSD}[\alpha(n), \beta(n)]$ with completeness $c(n) = \big(1 + \alpha(n) - 2^{-n}\big)/2$ and soundness $s(n) = (1 + \beta(n))/2$. Moreover, a near-optimal prover strategy for this proof system can be implemented in quantum single-exponential time and linear space. Consequently, for any $\alpha(n)$ and $\beta(n)$ satisfying $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$,*

$$\mathrm{QSD}[\alpha(n), \beta(n)] \text{ is in QIP(2) with a quantum } O(n') \text{ space honest prover,}$$

where n' is the total input length of the quantum circuits that prepare the corresponding tuple of quantum states.[15]

[14] Notably, Equation (1) is fundamental in quantum algorithms for estimating the trace distance [54]. An extension of this identity also underlies quantum algorithms for estimating the (powered) quantum ℓ_α distance [40], which generalizes the trace distance via the (powered) Schatten (α-)norm.

[15] This tuple of quantum states arises from a standard parallel repetition of the QIP(2) proof system for $\mathrm{GapQSD}[\alpha(n), \beta(n)]$ with $c(n) - s(n) \geq 1/\mathrm{poly}(n)$. See Section 2.4 in the full version [36] for details.

In the rest of this section, we sketch the proof of Theorem 16 and the proof of Theorem 17 in Section 3.1 and Section 3.2, respectively.

3.1 Algorithmic Holevo–Helstrom measurement

To implement our algorithmic Holevo–Helstrom measurement, we adopt the one-bit precision phase estimation (often referred to as the Hadamard test, e.g., Lemma 2.13 in the full version [36]) which reduces the task to implementing the corresponding unitary. The starting point is the space-efficient polynomial approximation $P_{d'}^{\mathrm{sgn}}$ of the sign function (Lemma 2.9 in the full version [36]), which yields the two-outcome measurement $\{\hat{\Pi}_0, \hat{\Pi}_1\}$ defined by:

$$\hat{\Pi}_b = \frac{I}{2} + (-1)^b \cdot \frac{1}{2} P_{d'}^{\mathrm{sgn}}\left(\frac{\rho_0 - \rho_1}{2}\right) \text{ for } b \in \{0,1\}.$$

By applying the space-efficient QSVT associated with the polynomial $P_{d'}^{\mathrm{sgn}}$ to the block-encoding of $(\rho_0 - \rho_1)/2$ (Lemma 2.10 in the full version [36]), we obtain the unitary U_{HH} which is a block-encoding of $A_{\mathrm{HH}} \coloneqq\approx P_{d'}^{\mathrm{sgn}}\left(\frac{\rho_0-\rho_1}{2}\right)$. We thus implement two-outcome measurement $\{\tilde{\Pi}_0, \tilde{\Pi}_1\}$ where $\tilde{\Pi}_0 = (I + A_{\mathrm{HH}})/2$, and the difference between $\{\hat{\Pi}_0, \hat{\Pi}_1\}$ and $\{\tilde{\Pi}_0, \tilde{\Pi}_1\}$ is caused by the implementation error of our space-efficient QSVT. The proof of Theorem 16 can be found in the full version [36, Section 3.1].

3.2 A slightly improved upper bound for GapQSD

We start by presenting the quantum interactive proof system used in Theorem 17, as shown in Protocol 1. This proof system aligns with [56, Figure 2], with the new component being the honest prover's behavior. In particular, the honest prover now employs the algorithmic Holevo–Helstrom measurement $\{\tilde{\Pi}_0, \tilde{\Pi}_1\}$ from Theorem 16, rather than the optimal measurement $\{\Pi_0, \Pi_1\}$ in Proposition 15 as per Theorem 14. The proof of Theorem 17 and the analysis of Protocol 1 can be found in the full version [36, Section 3.2].

Protocol 1 Two-message proof system for GapQSD (quantum linear-space prover).

1. The verifier $\mathcal{V}$ first chooses $b \in \{0,1\}$ uniformly at random. Subsequently, $\mathcal{V}$ applies Q_b to $|0\rangle^{\otimes n}$, traces out all non-output qubits, and sends the resulting state ρ_b.
2. The verifier $\mathcal{V}$ receives a single-qubit state $\hat{\sigma}$, measures the state in the computational basis, and denotes the outcome by $\hat{b} \in \{0,1\}$.

   The *honest* prover $\mathcal{P}$ measures the received state ρ by the algorithmic Holevo–Helstrom measurement $\{\tilde{\Pi}_0, \tilde{\Pi}_1\}$ (Theorem 16), and sends the outcome $\hat{b}$. In particular, the outcome equals $\hat{b}$ if the measurement indicates ρ is $\rho_{\hat{b}}$.

3. The verifier $\mathcal{V}$ accepts if $b = \hat{b}$; otherwise $\mathcal{V}$ rejects.

4 Algorithmic Uhlmann transform and its implications

In this section, we introduce an *algorithmic* version of the Uhlmann transform that approximately attains the maximum overlap between purifications of the quantum states ρ_0 and ρ_1. We begin by defining the Computational Uhlmann Fidelity Test Problem, which assumes access to the descriptions of the corresponding state-preparation circuits:

▶ **Problem 18** (Computational Uhlmann Fidelity Test Problem)**.** Let Q_0 and Q_1 be two known polynomial-size quantum circuits acting on n qubits in registers (A, R), each with r designated output qubits in register A. Let $|\psi_b\rangle$ be the pure state produced by applying Q_b to the initial state $|0\rangle^{\otimes n}$ for $b \in \{0,1\}$, and let ρ_b be the quantum state obtained by tracing out all non-output qubits in register R.

- **Input:** The qubits of the purification $|\psi_1\rangle$ in the reference register R, while all qubits in the output register A are fixed and cannot be modified.
- **Output:** A bit z obtained from the two-outcome measurement $\{\Pi, I - \Pi\}$, where $\Pi := |\psi_0\rangle\langle\psi_0|$.

The goal is to maximize the probability that the test in Problem 18 succeeds (i.e., obtaining the first outcome), which can be accomplished by applying an appropriate dimension-preserving quantum channel to register R.

Information-theoretic background. Problem 18 naturally generalizes the (information-theoretic) Uhlmann fidelity test between a quantum state ρ and a pure state $|\phi\rangle\langle\phi|$, as stated in [59, Exercise 9.2.2]. In that setting, the reference register R does not appear, and the two-outcome measurement is $\{|\phi\rangle\langle\phi|, I - |\phi\rangle\langle\phi|\}$. The success probability of the test is $\mathrm{Tr}(|\phi\rangle\langle\phi|\rho)$, which coincides exactly with the squared fidelity $\mathrm{F}^2(|\phi\rangle\langle\phi|, \rho)$.

For two quantum states that may be mixed, the probability of obtaining the first outcome in the Uhlmann fidelity test (i.e., the information-theoretic counterpart of Problem 18) is characterized by the squared fidelity [50], as will be seen later in Corollary 20. A refined formulation with an elementary proof appears in [29] and is stated below:

▶ **Theorem 19** (Uhlmann's theorem, adapted from [29, Theorem 2])**.** *Let ρ_0 and ρ_1 be quantum states on register A. For any fixed purification $|\psi_0\rangle$ of ρ_0 on registers (A, R), the maximum squared overlap between $|\psi_0\rangle$ and any purification $|\psi_1\rangle$ of ρ_1 on the same registers is given by the squared (Uhlmann) fidelity:*[16]

$$\mathrm{F}^2(\rho_0, \rho_1) := \mathrm{Tr}(|\sqrt{\rho_0}\sqrt{\rho_1}|)^2 = \max_{|\psi_1\rangle} |\langle\psi_0|\psi_1\rangle|^2 = \max_{U} \left|\langle\psi_0|\left(I^{\mathsf{A}} \otimes U^{\mathsf{R}}\right)|\psi_1'\rangle\right|^2. \tag{3}$$

Here, the last identity transfers the freedom in choosing $|\psi_1\rangle$ to the freedom in choosing a unitary U^{R} while keeping the purification $|\psi_1'\rangle$ fixed.

By inspecting the soundness analysis in the proof of [56, Theorem 11], which uses the monotonicity $\mathrm{F}^2(\rho_0, \rho_1) \leq \mathrm{F}^2(\mathcal{E}(\rho_0), \mathcal{E}(\rho_1))$ for every quantum channel $\mathcal{E}$, see e.g., [45, Theorem 9.6], one obtains a stronger form of Theorem 19:[17]

▶ **Corollary 20** (A stronger form of Uhlmann's theorem, implicit in [56, Theorem 11])**.** *Let ρ_0 and ρ_1 be quantum states on register A. For any fixed purifications $|\psi_0\rangle$ and $|\psi_1\rangle$ of ρ_0 and ρ_1, respectively, on registers (A, R), the squared (Uhlmann) fidelity satisfies*

$$\mathrm{F}^2(\rho_0, \rho_1) = \max_{\Phi} \langle\psi_0|\left(I^{\mathsf{A}} \otimes \Phi^{\mathsf{R}}\right)(|\psi_1\rangle\langle\psi_1|)|\psi_0\rangle,$$

where the maximization ranges over all quantum channels Φ acting on the register R and preserving its dimension.

[16] The last equality in Equation (3) follows from the freedom in purifications (see, e.g., [45, Exercise 2.81]).

[17] Noting that although an arbitrary quantum channel $\Phi(\cdot)$ may act on register R, the reduced density matrix on register A remains ρ_1. Let $\sigma := \left(I^{\mathsf{A}} \otimes \Phi^{\mathsf{R}}\right)(|\psi_1\rangle\langle\psi_1|)$ be the resulting state on registers (A, R) such that $\mathrm{Tr}_{\mathsf{R}}(\sigma) = \rho_1$, then $\langle\psi_0|\sigma|\psi_0\rangle = \mathrm{F}^2(|\psi_0\rangle\langle\psi_0|, \sigma) \leq \mathrm{F}^2(\mathrm{Tr}_{\mathsf{R}}(|\psi_0\rangle\langle\psi_0|), \mathrm{Tr}_{\mathsf{R}}(\sigma)) = \mathrm{F}^2(\rho_0, \rho_1)$. The same argument applies when the roles of ρ_0 and ρ_1 are exchanged.

By examining the proof of [29, Theorem 2] together with [29, Lemma 6], one can extract an explicit expression for the optimal unitary, later referred to as the *Uhlmann transform*, that achieves the maximum in Equation (3), as stated in Lemma 21.[18]

▶ **Lemma 21** (Explicit form of the Uhlmann transform, implicit in [29, Lemma 6]). *Let $|\psi_0\rangle$ and $|\psi_1\rangle$ be purifications of quantum states ρ_0 and ρ_1 on register A, defined on registers (A,R), where R is the reference register. A unitary $U_\star$ on register R that attains the maximum in Uhlmann's theorem (Theorem 19) is given by*

$$U_\star = \mathrm{sgn}^{(\mathrm{SV})}\big(\mathrm{Tr}_{\mathsf{A}}\big(|\psi_0\rangle\langle\psi_1|^{\mathsf{AR}}\big)\big).$$

Algorithmic implementation. Unlike the Holevo–Helstrom measurement in Proposition 15, for which one can directly obtain an *exact* block-encoding of $X_{\mathrm{HH}} \coloneqq (\rho_0-\rho_1)/2$, constructing a block-encoding of $X_{\mathrm{Uhl}} \coloneqq \mathrm{Tr}_{\mathsf{A}}\big(|\psi_0\rangle\langle\psi_1|^{\mathsf{AR}}\big)$ is more involved. A straightforward approach introduces a normalization factor of $\dim(\mathcal{H}_{\mathsf{A}})$ and results only in an exact encoding of $X_{\mathrm{Uhl}}/\dim(\mathcal{H}_{\mathsf{A}})$ [43].[19] Instead, an exact block-encoding of X_{Uhl} was recently proposed in [51, Section 5.1]. By combining this key ingredient with the space-efficient quantum singular value transformation in [37, Section 3], one can implement the unitary in Lemma 21 in a natural manner using quantum *single-exponential* time and *linear* space. We refer to this explicit implementation as the *algorithmic Uhlmann transform*:

▶ **Theorem 22** (Algorithmic Uhlmann transform). *Let ρ_0 and ρ_1 be quantum states prepared by n-qubit quantum circuits Q_0 and Q_1, and let $|\psi_0\rangle$ and $|\psi_1\rangle$ denote their purifications before tracing out the non-output qubits, as in Problem 18. An approximate version of the Uhlmann transform $U_\star$ specified in Lemma 21, denoted by $\tilde{U}_\star$, can be implemented so that*

$$\mathrm{F}^2(\rho_0,\rho_1) - 2^{-n} \le \big|\langle\psi_0|^{\mathsf{AR}}\big(I^{\mathsf{A}}\otimes\tilde{U}_\star^{\mathsf{R}}\big)|\psi_1\rangle^{\mathsf{AR}}\big|^2 \le \mathrm{F}^2(\rho_0,\rho_1). \tag{4}$$

The quantum circuit implementation of $\tilde{U}_\star$, acting on $O(n)$ qubits, requires $2^{O(n)}$ queries to the quantum circuits Q_0 and Q_1, as well as $2^{O(n)}$ one- and two-qubit gates. Moreover, the circuit description can be computed in deterministic time $2^{O(n)}$ and space $O(n)$.

▶ Remark 23 ($\mathrm{GapF}^2\mathrm{Est}_{\log}$ is BQL-complete). In analogy with the connection between the algorithmic Holevo–Helstrom measurement (Theorem 16) and the BQL containment of $\mathrm{GapQSD}_{\log}$ proven in [37, Section 4.2], one can establish that $\mathrm{GapF}^2\mathrm{Est}_{\log}$ is in BQL by adapting the space-efficient QSVT-based approach in Theorem 22.[20]

By inspecting the (honest-verifier) quantum statistical zero-knowledge protocol ("closeness test") for $\mathrm{QSC}[\beta,\alpha]$, serving as the complement of QSD, with constant satisfying $\alpha^2 > \beta$ in [56, Section 4.3], we establish a slightly improved upper bound for $\mathrm{GapF}^2\mathrm{Est}$:

▶ **Theorem 24** ($\mathrm{GapF}^2\mathrm{Est}$ is in QIP(2) with a quantum linear-space honest prover). *There exists a two-message quantum interactive proof system for $\mathrm{F}^2\mathrm{Est}[\alpha(n),\beta(n)]$ with completeness $c(n) = \alpha(n) - 2^{-n}$ and soundness $s(n) = \beta(n)$. Moreover, a near-optimal prover strategy for this proof system can be implemented in quantum single-exponential time and linear space. Consequently, for any $\alpha(n)$ and $\beta(n)$ satisfying $\alpha(n) - \beta(n) \ge 1/\mathrm{poly}(n)$,*

$$\mathrm{F}^2\mathrm{Est}[\alpha(n),\beta(n)] \text{ is in } \mathsf{QIP}(2) \text{ with a quantum } O(n') \text{ space honest prover,}$$

where n' is the total input length of the quantum circuits that prepare the corresponding tuple of quantum states.

[18] A self-contained proof can be found in [51, Appendix F] (derived from Jozsa's lemma) or Lemma 7.6 in the arXiv version of [43].

[19] See Section 7 in the arXiv version of [43].

[20] Here, $\mathrm{GapF}^2\mathrm{Est}_{\log}$ denotes the space-bounded version of $\mathrm{GapF}^2\mathrm{Est}$, where the state-preparation circuits have input length $O(\log n)$. The BQL hardness follows directly from [37, Lemma 4.23].

In the remainder of this section, we first sketch the proofs of Theorem 22 and Theorem 24 in Section 4.1 and Section 4.2, respectively. The implications of Theorem 24 for promise problems defined with respect to the trace distance are provided in Section 4.3, which are closely related to the complexity classes QSZK and NIQSZK.

4.1 Algorithmic Uhlmann transform

To implement our algorithmic Uhlmann transform, we begin by stating an exact block-encoding of $\mathrm{Tr}_{\mathsf{A}'}\big(|\psi_0\rangle\langle\psi_1|^{\mathsf{A}'\mathsf{R}}\big)$, as specified in Lemma 25. The proof of Lemma 25 appears at the beginning of [51, Section 5.1], specifically from Equation (37) to Equation (42).

▶ **Lemma 25** (Exact block-encoding of $\mathrm{Tr}_{\mathsf{A}}\big(|\psi_0\rangle\langle\psi_1|^{\mathsf{A}\mathsf{R}}\big)$, adapted from [51, Section 5.1])**.** *Let $X_{\mathrm{Uhl}} \coloneqq \mathrm{Tr}_{\mathsf{A}}\big(|\psi_0\rangle\langle\psi_1|^{\mathsf{A}\mathsf{R}}\big)$ be a linear operator on register R such that the unitary $\mathrm{sgn}^{(\mathrm{SV})}(X_{\mathrm{Uhl}})$ attains the maximum in Uhlmann's theorem (Theorem 19). Recall that Q_0 and Q_1 denote the state-preparation circuits of ρ_0 and ρ_1, as specified in Problem 18. Then the unitary W on registers $(\mathsf{A}', \mathsf{R}, \mathsf{E})$, where A' is identical to A and E contains the same number of qubits as R, is a $(1, n, 0)$-block-encoding of X_{Uhl}, given by*

$$\langle\bar{0}|^{\mathsf{A}'}\langle\bar{0}|^{\mathsf{E}} W |\bar{0}\rangle^{\mathsf{A}'}|\bar{0}\rangle^{\mathsf{E}} = X_{\mathrm{Uhl}}, \quad \text{where } W \coloneqq \big(Q_1^{\mathsf{A}'\mathsf{R}}\big)^{\dagger}\Big(I^{\mathsf{A}'} \otimes \mathrm{SWAP}^{\mathsf{R},\mathsf{E}}\Big)Q_0^{\mathsf{A}'\mathsf{R}}.$$

This block-encoding can be implemented using a single query to each state-preparation circuit Q_0 and Q_1, together with $O(n)$ one- and two-qubit quantum gates.

Next, using the space-efficient polynomial approximation $P_{d'}^{\mathrm{sgn}}$ of the sign function from Lemma 2.9 in the full version [36], it suffices to implement another transform $\hat{U}_\star$ that is very close to $U_\star$:

$$\hat{U}_\star = P_{\mathrm{sgn},d'}^{(\mathrm{SV})}\big(\mathrm{Tr}_{\mathsf{A}}\big(|\psi_0\rangle\langle\psi_1|^{\mathsf{A}\mathsf{R}}\big)\big).$$

By applying the space-efficient QSVT associated with the polynomial $P_{d'}^{\mathrm{sgn}}$ to the block-encoding of $\mathrm{Tr}_{\mathsf{A}}\big(|\psi_0\rangle\langle\psi_1|^{\mathsf{A}\mathsf{R}}\big)$, we obtain a unitary $V_\star$ that is a block-encoding of $\hat{U}_\star$. In particular, $V_\star$ acts as an exact block-encoding of $\tilde{U}_\star \coloneqq \langle\bar{0}|\tilde{V}_\star|\bar{0}\rangle$, which gives an approximate implementation of the Uhlmann transform. The difference between $\tilde{U}_\star$ and $\hat{U}_\star$ comes from the implementation error of the space-efficient QSVT.[21] The proof of Theorem 22 can be found in the full version [36, Section 4.1].

4.2 A slightly improved upper bound for GapF^{2}Est

We begin by presenting the quantum interactive proof system used in Theorem 24, as shown in Protocol 2. This proof system aligns with [56, Figure 3], with the new component being the honest prover's behavior. Specifically, the honest prover now utilizes the algorithmic Uhlmann transform $\tilde{U}_\star$ from Theorem 22, instead of the Uhlmann transform in Lemma 21. The proof of Theorem 24 and the analysis of Protocol 2 can be found in the full version [36, Section 4.2].

4.3 Implications for closeness testing problems based on the trace distance

Combining the Fuchs–van de Graaf inequality (Lemma 10), which relates the squared fidelity to the trace distance, with the polarization lemma for the trace distance [56], a direct calculation yields the following corollary, whose proof can be found in the full version [36, Section 4.3]:

[21] It is worth noting that $\tilde{U}_\star$ is *not* necessarily a unitary.

Protocol 2 Two-message proof system for GapF^{2}Est (quantum linear-space prover).

1. The verifier $\mathcal{V}$ applies Q_0 to $|0\rangle^{\otimes n}$, and sends the *non-output* qubits in register R, while keeping output qubits in register A.
2. The verifier $\mathcal{V}$ receives the (possibly modified) qubits in register R.

   The *honest* prover $\mathcal{P}$ applies the algorithmic Uhlmann transform $\tilde{U}_\star$ (Theorem 22) to the received qubits, and sends the resulting qubits back.

3. The verifier $\mathcal{V}$ applies $Q_1^\dagger$ to the registers (A, R), where register A contains the output qubits of Q_0 and register R contains the received qubits. $\mathcal{V}$ then measures all qubits in (A, R) in the computational basis and accepts if the measurement outcome is the n-bit all-zero string; otherwise, $\mathcal{V}$ rejects.

▶ **Corollary 26** (A slightly improved upper bound for QSC). *For any efficiently computable functions $\alpha(n)$ and $\beta(n)$ satisfying $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$,*

$\mathrm{QSC}[\beta(n), \alpha(n)]$ *is in* QIP(2) *with a quantum $O(n')$ space honest prover.*

Here, n' denotes the total input length of the state-preparation circuits.

Since the co-QSZK-hard regime of QSC, implicitly specified in [56, Section 5], is covered by Corollary 26, applying the complement gives the co-QIP(2) part in Corollary 4. In addition, by fixing ρ_0 in QSC to be the maximally mixed state and choosing the state-preparation circuit Q_0 to create EPR pairs across the registers A and R, Corollary 26 yields a two-message quantum interactive proof system in which the verifier's message consists exactly of half of EPR pairs, leading to Corollary 5:

▶ **Corollary 27** (A slightly improved upper bound for QSCMM). *For any efficiently computable functions $\alpha(n)$ and $\beta(n)$ satisfying $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$,*

$\mathrm{QSCMM}[\beta(n), \alpha(n)]$ *is in* qq-QAM *with a quantum $O(n')$ space honest prover.*

Here, n' denotes the total input length of the state-preparation circuits.

References

1 Dorit Aharonov, Vaughan Jones, and Zeph Landau. A polynomial quantum algorithm for approximating the Jones polynomial. *Algorithmica*, 55(3):395–421, 2009. Preliminary version in *STOC 2006*. arXiv:quant-ph/0511096. doi:10.1007/s00453-008-9168-0.

2 William Aiello and Johan Håstad. Statistical zero-knowledge languages can be recognized in two rounds. *Journal of Computer and System Sciences*, 42(3):327–345, 1991. Preliminary version in *FOCS 1987*. doi:10.1016/0022-0000(91)90006-Q.

3 Avraham Ben-Aroya, Oded Schwartz, and Amnon Ta-Shma. Quantum expanders: Motivation and construction. *Theory of Computing*, 6(1):47–79, 2010. Preliminary version in *CCC 2008*. doi:10.4086/toc.2010.v006a003.

4 Itay Berman, Akshay Degwekar, Ron D Rothblum, and Prashant Nalini Vasudevan. Statistical difference beyond the polarizing regime. In *Theory of Cryptography Conference*, pages 311–332. Springer, 2019. ECCC:TR19-038. doi:10.1007/978-3-030-36033-7_12.

5 Dominic W Berry, Andrew M Childs, Richard Cleve, Robin Kothari, and Rolando D Somma. Simulating Hamiltonian dynamics with a truncated Taylor series. *Physical Review Letters*, 114(9):090502, 2015. arXiv:1412.4687. doi:10.1103/PhysRevLett.114.090502.

6 John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary complexity and the Uhlmann transformation problem. In *Proceedings of the 17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, volume 362 of *LIPIcs*, pages 24:1–24:17. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2026. arXiv:2306.13073. doi:10.4230/LIPIcs.ITCS.2026.24.

7 John Bostanci, Tony Metger, and Henry Yuen. Local transformations of bipartite entanglement are rigid. In *Proceedings of the 17th Innovations in Theoretical Computer Science Conference (ITCS 2026)*, volume 362 of *LIPIcs*, pages 26:1–26:8. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2026. arXiv:2509.05257. doi:10.4230/LIPIcs.ITCS.2026.26.

8 Mark Bun, Robin Kothari, and Justin Thaler. The polynomial method strikes back: tight quantum query bounds via dual polynomials. *Theory of Computing*, 16(10):1–71, 2020. Preliminary version in *STOC 2018*. arXiv:1710.09079. doi:10.4086/toc.2020.v016a010.

9 André Chailloux, Dragos Florin Ciocan, Iordanis Kerenidis, and Salil Vadhan. Interactive and noninteractive zero knowledge are equivalent in the help model. In *Theory of Cryptography Conference*, pages 501–534. Springer, 2008. IACR ePrint:2007/467. doi:10.1007/978-3-540-78524-8_28.

10 André Chailloux and Iordanis Kerenidis. Increasing the power of the verifier in quantum zero knowledge. In *Proceedings of the IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2008)*, LIPIcs, pages 95–106, 2008. arXiv:0711.4032. doi:10.4230/LIPIcs.FSTTCS.2008.1744.

11 Sourav Chakraborty, Eldar Fischer, Arie Matsliah, and Ronald de Wolf. New results on quantum property testing. In *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2010)*, volume 8 of *LIPIcs*, pages 145–156. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2010. arXiv:1005.0523. doi:10.4230/LIPIcs.FSTTCS.2010.145.

12 Kean Chen, Qisheng Wang, and Zhicheng Zhang. A list of complexity bounds for property testing by quantum sample-to-query lifting. *arXiv preprint*, 2025. arXiv:2512.01971.

13 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, page 4, 2018. arXiv:1604.01384. doi:10.4230/LIPIcs.ITCS.2018.4.

14 Lance Fortnow. The complexity of perfect zero-knowledge. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, page 204–209, New York, NY, USA, 1987. Association for Computing Machinery. doi:10.1145/28395.28418.

15 Christopher A Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999. arXiv:quant-ph/9712042. doi:10.1109/18.761271.

16 Sevag Gharibian, Miklos Santha, Jamie Sikora, Aarthi Sundaram, and Justin Yirka. Quantum generalizations of the polynomial hierarchy with applications to QMA(2). *computational complexity*, 31(2):1–52, 2022. Preliminary version in *MFCS 2018*. arXiv:1805.11139. doi:10.1007/s00037-022-00231-8.

17 András Gilyén and Alexander Poremba. Improved quantum algorithms for fidelity estimation. *arXiv preprint*, 2022. arXiv:2203.15993.

18 András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 193–204, 2019. arXiv:1806.01838. doi:10.1145/3313276.3316366.

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

20 Oded Goldreich. On doubly-efficient interactive proof systems. *Foundations and Trends® in Theoretical Computer Science*, 13(3):158–246, 2018. ECCC:TR17-017. doi:10.1561/0400000084.

21 Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(3):691–729, 1991. Preliminary version in *FOCS 1986*. doi:10.1145/116825.116852.

22 Oded Goldreich, Amit Sahai, and Salil Vadhan. Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 399–408, 1998. doi:10.1145/276698.276852.

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

24 Ayal Green, Guy Kindler, and Yupan Liu. Towards a quantum-inspired proof for IP = PSPACE. *Quantum Information & Computation*, 21(5&6):377–386, 2021. arXiv:1912.11611. doi:10.26421/QIC21.5-6-2.

25 Carl W Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1:231–252, 1969. doi:10.1007/BF01007479.

26 Alexander S Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, 3(4):337–394, 1973. doi:10.1016/0047-259X(73)90028-6.

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

28 Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 534–543. IEEE, 2009. arXiv:0905.1300. doi:10.1109/FOCS.2009.30.

29 Richard Jozsa. Fidelity for mixed quantum states. *Journal of modern optics*, 41(12):2315–2323, 1994. doi:10.1080/09500349414552171.

30 Alastair Kay. Tutorial on the quantikz package. *arXiv preprint*, 2018. arXiv:1809.03842.

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

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

33 Alexei Yu Kitaev. Quantum measurements and the Abelian stabilizer problem. *arXiv preprint*, 1995. arXiv:quant-ph/9511026.

34 Hirotada Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In *Proceedings of the 14th International Symposium on Algorithms and Computation*, pages 178–188. Springer, 2003. doi:10.1007/978-3-540-24587-2_20.

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

36 François Le Gall, Yupan Liu, and Qisheng Wang. A slightly improved upper bound for quantum statistical zero-knowledge. *arXiv preprint*, 2025. arXiv:2512.11597v2.

37 François Le Gall, Yupan Liu, and Qisheng Wang. Space-bounded quantum state testing via space-efficient quantum singular value transformation. To appear in *computational complexity*, 2026. arXiv:2308.05079. doi:10.1007/s00037-025-00284-5.

38 Yupan Liu. *Complexity-theoretic perspectives on quantum state testing*. PhD thesis, Nagoya University, 2025. URL: https://nagoya.repo.nii.ac.jp/records/2012662.

39 Yupan Liu. Quantum state testing beyond the polarizing regime and quantum triangular discrimination. *Computational Complexity*, 34(11):1–67, 2025. arXiv:2303.01952. doi:10.1007/s00037-025-00273-8.

40 Yupan Liu and Qisheng Wang. On estimating the quantum ℓ_α distance. In *Proceedings of the 33rd Annual European Symposium on Algorithms (ESA 2025)*, volume 351 of *LIPIcs*, pages 105:1–105:20. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025. doi:10.4230/LIPIcs.ESA.2025.105.

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

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

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

44 Tomoyuki Morimae and Harumichi Nishimura. Merlinization of complexity classes above BQP. *Quantum Information & Computation*, 17(11&12):959–972, 2017. arXiv:1704.01514. doi:10.26421/QIC17.11-12-3.

45 Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2010. doi:10.1017/CBO9780511976667.

46 Omer Reingold, Guy N. Rothblum, and Ron D. Rothblum. Constant-round interactive proofs for delegating computation. *SIAM Journal on Computing*, 50(3), 2021. Preliminary version in *STOC 2016*. ECCC:TR16-016. doi:10.1137/16M1096773.

47 Amit Sahai and Salil Vadhan. A complete problem for statistical zero knowledge. *Journal of the ACM*, 50(2):196–249, 2003. Preliminary version in *FOCS 1997*. ECCC:TR00-084. doi:10.1145/636865.636868.

48 Adi Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992. Preliminary version in *FOCS 1990*. doi:10.1145/146585.146609.

49 Amnon Ta-Shma. Inverting well conditioned matrices in quantum logspace. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, pages 881–890, 2013. doi:10.1145/2488608.2488720.

50 Armin Uhlmann. The "transition probability" in the state space of A^*-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976. doi:10.1016/0034-4877(76)90060-4.

51 Takeru Utsumi, Yoshifumi Nakata, Qisheng Wang, and Ryuji Takagi. Quantum algorithms for Uhlmann transformation. *arXiv preprint*, 2025. arXiv:2509.03619.

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

53 Qisheng Wang, Ji Guan, Junyi Liu, Zhicheng Zhang, and Mingsheng Ying. New quantum algorithms for computing quantum entropies and distances. *IEEE Transactions on Information Theory*, 70(8):5653–5680, 2024. arXiv:2203.13522. doi:10.1109/TIT.2024.3399014.

54 Qisheng Wang and Zhicheng Zhang. Fast quantum algorithms for trace distance estimation. *IEEE Transactions on Information Theory*, 70(4):2720–2733, 2024. arXiv:2301.06783. doi:10.1109/TIT.2023.3321121.

55 Qisheng Wang, Zhicheng Zhang, Kean Chen, Ji Guan, Wang Fang, Junyi Liu, and Mingsheng Ying. Quantum algorithm for fidelity estimation. *IEEE Transactions on Information Theory*, 69(1):273–282, 2023. arXiv:2103.09076. doi:10.1109/TIT.2022.3203985.

56 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. IEEE, 2002. arXiv:quant-ph/0202111. doi:10.1109/SFCS.2002.1181970.

57 John Watrous. Quantum computational complexity. *Encyclopedia of Complexity and Systems Science*, pages 7174–7201, 2009. arXiv:0804.3401. doi:10.1007/978-0-387-30440-3_428.

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

59 Mark M Wilde. *Quantum Information Theory*. Cambridge University Press, 1st edition, 2013. doi:10.1017/9781316809976.

60 Ronald de Wolf. Quantum computing: Lecture notes. *arXiv preprint*, 2019. arXiv:1907.09415.