Complexity-theoretic perspectives on quantum state testing

by

Yupan Liu

Submitted in fulfillment of the requirements for the degree of
Doctor of Philosophy

Graduate School of Mathematics
Nagoya University

January 2025

Abstract

Recent advancements in quantum devices have posed an intriguing challenge of verifying their intended functionality. These devices, typically *time-bounded*, are often designed to prepare specific n-qubit states, denoted as ρ_0 and ρ_1. The problem of (tolerant) quantum state testing aims to design algorithms that can efficiently decide whether ρ_0 is either ϵ_1-close to or ϵ_2-far from ρ_1 with respect to a chosen distance-like measure.

This problem generalizes classical (tolerant) distribution testing [Can20] to the quantum domain and forms a part of quantum property testing [MdW16], an emerging field dedicated to developing efficient quantum testers for properties of quantum objects. The computational complexity of time-bounded quantum state testing varies significantly with the choice of closeness measure, exhibiting a *dichotomy-like behavior*:

- For both the trace distance (ℓ_1 norm) and the quantum (von Neumann) entropy difference, the problems correspond to the complexity class QSZK [Wat02, Wat09b, BASTS10], which is widely believed to be strictly more powerful than BQP.
- For the Hilbert-Schmidt distance (ℓ_2 norm) or the quantity $\mathrm{Tr}(\rho_0\rho_1)$, the problems correspond to the complexity class BQP [BCWdW01], capturing the computational power of efficient quantum computation.

This dissertation aims to deepen our understanding of the aforementioned dichotomy-like behavior by addressing time-bounded and space-bounded closeness testing problems of quantum states from complexity-theoretic perspectives. Specifically, we investigate the following problems:

(i) *What is the computational hardness of* approximating *the von Neumann entropy?* We study the time-bounded state testing with respect to quantum q-Tsallis entropy $\mathrm{S}_q(\rho) := \frac{1-\mathrm{Tr}(\rho^q)}{q-1}$, which naturally lower bounds the von Neumann entropy $\mathrm{S}(\rho) := -\mathrm{Tr}(\rho \ln \rho)$ and converges to it as q approaches to 1. Our results are as follows:

  - ◇ For the regime $1+\Omega(1) \leq q \leq 2$, which includes the purity $\mathrm{Tr}(\rho^2)$, the problem is BQP-complete. Moreover, the BQP containment holds when $q \geq 1 + \Omega(1)$.
  - ◇ For the regime $1 < q < 1+\frac{1}{n-1}$, the problem is QSZK-hard, leading to hardness of approximating von Neumann entropy as long as $\mathsf{BQP} \subsetneq \mathsf{QSZK}$.

  The hardness results are derived from reductions based on new inequalities for the quantum q-Jensen-(Shannon-)Tsallis divergence with $1 \leq q \leq 2$.

(ii) *Does this dichotomy-like behavior also arise in quantum state testing under* other *resource constraints?* We introduce *space-bounded* variants of quantum state test-

ing, focusing on state-preparation circuits acting on $O(\log n)$ qubits. We establish the following novel complete characterizations of quantum logspace:

- ◇ In one-sided error scenarios, space-bounded state testing with respect to both the trace distance and the Hilbert-Schmidt distance is $\mathsf{coRQ_UL}$-complete, making it the first family of natural complete problems for this class.
- ◇ In two-sided error scenarios, space-bounded state testing with respect to common distance-like measures is BQL-complete.

Our main technical contribution is a *space-efficient* variant of quantum singular value transformation [GSLW19], offering a unified framework for designing quantum logspace algorithms and enabling simultaneous time-space upper bounds. Our results have broader implications beyond quantum logspace:

- ◇ We prove that QSZK is in $\mathsf{QIP}(2)$ with a quantum linear-space honest prover, slightly improving from the best known upper bound $\mathsf{QIP}(2)$ [Wat02, JUW09].
- ◇ In the context of quantum interactive proofs, we introduce a space-bounded variant of quantum statistical zero-knowledge ($\mathsf{QSZK_UL}$), where the verifier uses unitary quantum logspace, and show that this model is as weak as BQL.

(iii) *How can the* QSZK *containment regime for the time-bounded state testing problem with respect to the trace distance* (QSD) *be improved?* The current QSZK containment of QSD is limited to the constant polarizing regime, owing to the limitations of the polarization lemma [SV03, Wat02]. Inspired by recent advancements in the classical setting [BDRV19], we extend the QSZK containment regime of QSD by introducing *proper* quantum analogs of the problems defined with respect to the triangular discrimination and the Jensen-Shannon divergence. We study whether the quantum analogs behave similarly to their classical counterparts and examine the limitations of existing approaches to polarization regarding quantum distances.

Furthermore, we prove that QSD with some exponentially small errors is in PP, suggesting that dimension-preserving polarization is unlikely to be achievable unless $\mathsf{QSZK} \subseteq \mathsf{PP}$. Additionally, the same problem without error is in NQP.

List of publications

Publications included in this thesis

[LW25] Yupan Liu and Qisheng Wang. On estimating the trace of quantum state powers. *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2025).*

Submitted manuscripts included in this thesis

[LLW23] François Le Gall, Yupan Liu, and Qisheng Wang. Space-bounded quantum state testing via space-efficient quantum singular value transformation. In submission.

[Liu23] Yupan Liu. Quantum state testing beyond the polarizing regime and quantum triangular discrimination. In submission.

[LLNW24] François Le Gall, Yupan Liu, Harumichi Nishimura, and Qisheng Wang. Space-bounded quantum interactive proof systems. In submission.

**Only Section 5 in Reference* [LLNW24] *is included in this thesis.*

It is noteworthy that both [LW25] and [LLNW24] would be also presented as contributed talks at the 28th Annual Quantum Information Processing Conference (QIP 2025).

Other publications during candidature

[DLLM23] Hugo Delavenne, François Le Gall, Yupan Liu, and Masayuki Miyamoto. Quantum Merlin-Arthur proof systems for synthesizing quantum states. To appear in *Quantum*.

Acknowledgements

First and foremost, I express my sincere gratitude to my advisor, François Le Gall, for his exceptional mentorship throughout my PhD at Nagoya University. I deeply appreciate his non-interventionist mentoring style, which encourages independence while offering support whenever needed. François is always willing to help his students in various ways, including giving insightful suggestions on prioritizing research projects with his remarkable overview of the field, offering advice on scientific writing and submission strategies, and providing financial support for academic visits and conference participation.

I am grateful to my collaborators and colleagues during my time in Nagoya. Harumichi Nishimura, who is super knowledgeable and a pioneer in quantum complexity theory, has always been patient in working through technical details and providing detailed feedback. I wrote the most papers together with Qisheng Wang, who is always ready to discuss research problems. He had many great insights about quantum property testing and is a very persistent problem solver, always keen on tackling the next problem. I am also thankful to Masayuki Miyamoto and Hugo Delavenne for the stateQMA project, as well as to Atsuya Hasegawa, Daiki Suruga, Yibin Wang, and others who are or were members of Francois' group for their support.

I would also like to thank the individuals who hosted my academic visits during my PhD, as well as for the enjoyable discussions with them and their group members. Zhengfeng Ji for hosting my short visit to Tsinghua University, as well as for virtually hosting me in his group seminar during the Spring 2021 semester. Tom Gur for inviting me to visit Cambridge, and Ashley Montanaro for hosting my short visit to Bristol during the same trip. Anurag Anshu, Henry Yuen, and Bill Fefferman for hosting my short visits.

This dissertation would not have been possible without the support of the Graduate School of Mathematics at Nagoya University, which provided the resources and facilities essential for my research. I also acknowledge the financial support of the JST SPRING grant No. JPMJSP2125, specifically the "THERS Make New Standards Program for the Next Generation Researchers", and the MEXT Q-LEAP grant No. JPMXS0120319794, which allowed me to dedicate myself fully to my studies.

Before my years at Nagoya, many people greatly influenced my academic journey. I am indebted to Itai Arad, who mentored me during my summer internship at CQT in my junior year and later became my MSc co-advisor. As an ambitious yet clueless young student, I was profoundly impacted by Itai's down-to-earth approach to research, conveyed through both his words and actions. I feel very fortunate to have completed my MSc at HUJI, where there are numerous (regular) theory seminars and high-quality courses in theoretical computer science, which helped me build a solid understanding of the field. Special thanks to Guy Kindler, from whom I formally learned the concept

of zero-knowledge proofs in his course – a fundamental concept closely related to the class QSZK, which is frequently discussed in this dissertation. I also gained practical and valuable knowledge from him on scientific writing. I am also thankful to Dorit Aharonov, who has deeply influenced my research taste at a high level, even though I am no longer a big fan of physics-motivated problems. Her short yet wise and precise advice – ranging from presentation and communication to general principles for selecting research problems – during my first two years at HUJI has been invaluable. Lastly, I extend my heartfelt thanks to Xin Wan, who supervised my final-year project and taught me how to approach new topics in a developing field.

My life has been greatly enriched by my friends, mostly from the communities of theoretical computer science and quantum information. Some of these connections date back to my undergraduate years through online interactions, while others began during my time in Hangzhou, Shenzhen, Singapore, Jerusalem, and Nagoya. Although I do not intend to name everyone individually, I deeply cherish the conversations, discussions, lunches, coffee breaks, and hikes we shared. I am sincerely grateful for their support and companionship.

Finally, I am forever grateful to my parent for their unwavering belief in me and for hosting me during my darkest times. Their love and support have been my greatest source of motivation and encouragement.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In recent years, the development of quantum devices has posed an intriguing challenge of verifying their intended functionality. This has made it increasingly important to characterize the computational power of feasible quantum computation models that operate under restricted resources, such as *time* (i.e., the number of gates in the circuit) and *space* (i.e., the number of qubits on which the circuit acts).

To be precise, every quantum algorithm, viewed as a quantum device, evolves an n-qubit *quantum state* ρ. This *mixed* state ρ is represented by a positive semidefinite square matrix of dimension 2^n that satisfies $\mathrm{Tr}(\rho) = 1$. In scenarios where the quantum device operates independently of any external environment, the resulting quantum state is a *pure* state, meaning $\mathrm{Tr}(\rho^2) = 1$. Equivalently, such a state can be expressed as $\rho = |\psi\rangle\langle\psi|$, where the pure state $|\psi\rangle$ is a vector on the unit sphere in $\mathbb{C}^{2^n}$.

A quantum algorithm often begins with the pure state $|0\rangle^{\otimes n}$ and proceeds through a sequence of local operations known as *quantum gates*. Each gate is a unitary operator that acts on a constant number of qubits while being implicitly tensored with the identity operator on the remaining qubits. To extract the information from the computation, particularly the resulting quantum state, a *measurement* is typically performed on the designated output qubit. This final measurement, conducted in the computational basis $\{|0\rangle, |1\rangle\}$, converts the final state into a probabilistic output by projecting the output qubit onto one of the eigenstates associated with the measurement outcomes.

The problem of (tolerant) *quantum state testing* aims to design algorithms that can efficiently test whether a quantum state ρ approximately has a certain property, assuming the state either nearly has the property or is somehow "far" from having it. Given the ability to produce copies of ρ, two notable examples illustrate this framework:

(1) The property Purity serves as a simple and interesting example. A quantum state ρ satisfies this property if and only if it is a pure state, equivalently $\mathrm{Tr}(\rho^2) = 1$.

(2) Closeness testing of quantum states provides another illustrative case. Here, a quantum device is designed to prepare a specific quantum state ρ_0, but a possibly malicious party could provide another device that outputs a different n-qubit state ρ_1, claiming that $\rho_0 \approx_\epsilon \rho_1$. The task is to test whether ρ_0 is ϵ_1-close to or ϵ_2-far from ρ_1 with respect to a specified distance-like measure.

Quantum state testing generalizes the concept of (tolerant) classical distribution test-

ing (see [Can20]), a specialized topic within classical property testing – a fundamental area in theoretical computer science (see [Gol17]). Moreover, quantum state testing constitutes a key instance of quantum property testing (see [MdW16]), an emerging field focused on designing quantum testers for the properties of quantum objects.

The remainder of this chapter reviews prior works on time-bounded (white-box) closeness testing of probability distributions and quantum states (Section 1.1). Subsequently, Section 1.3 outlines the contributions of this dissertation and highlights their significance. Finally, the organization of the dissertation is presented in Section 1.4.

1.1 Background: Time-bounded distribution and state testing

In this section, we review prior works on time-bounded distribution and state testing, with a particular focus on the closeness testing of distributions or states prepared by (poly)time-bounded classical or quantum circuits, given access to the "source code" of the respective devices. Our discussion emphasizes *white-box* scenarios, where "source code" refers to the description of classical or quantum preparation circuits using a polynomial number of elementary gates. For an overview of time-bounded closeness testing of probability distributions with respect to total variation distance or (Shannon) entropy difference, we also recommend a brief survey [GV11] by Goldreich and Vadhan.

As a general outline, the computational complexity of time-bounded closeness testing of probability distributions or quantum states varies significantly depending on the chosen closeness measure, exhibiting a *dichotomy-like* behavior:

- For the ℓ_1 norm and the entropy difference, time-bounded closeness testing appears to be *much harder than* preparing distributions or states, as SZK and QSZK are widely believed to be strictly more powerful than BPP and BQP, respectively.
- For the ℓ_2 norm, time-bounded closeness testing is *as easy as* preparing distributions or states, corresponding to complexity class BPP or BQP.

In broad terms, the complexity classes BPP and BQP capture the computational power of bounded-error *efficient* (i.e., polynomial-time) classical (specifically, randomized) and quantum computation, respectively. In contrast, the complexity classes SZK and QSZK consist of promise problems that possess classical and quantum statistical zero-knowledge proofs, which are specialized types of classical and quantum interactive proof systems, respectively. The computational power of these models is typically enhanced by the *interactions* between the prover and the verifier in the proof system, where the verifier is limited to efficient classical (more precisely, randomized) or quantum computation, and the prover is untrusted but computationally unbounded.

Next, we discuss prior works that further clarify this dichotomy-like behavior.

1.1.1 ℓ_1 norm scenarios and the complexity classes SZK and QSZK

The (white-box) time-bounded distribution testing problem, specifically the case with respect to the total variation distance, known as Statistical Difference (SD), was first introduced by Sahai and Vadhan [SV03]. Interestingly, their original motivation was to establish a natural complete characterization of the complexity class SZK, which

consists of promise problems that possess *statistical zero-knowledge proofs*. Statistical zero-knowledge is a foundational concept in complexity theory and cryptography, particularly in the study of interactive proofs. For further details or comprehensive surveys, please refer to [Vad99, Gol13]; for its quantum analog, see [VW16].

This promise problem $\mathrm{SD}[\alpha, \beta]$ involves two (time-)efficiently samplable probability distributions, D_0 and D_1, and asks whether D_0 is α-far from or β-close to D_1 with respect to the total variation distance $\|D_0 - D_1\|_{\mathrm{TV}}$. Here, a distribution D_b for $b \in \{0, 1\}$ is considered *efficiently samplable* if there exists an explicit polynomial-size classical circuit C_b that takes m random bits as input and outputs the n-bit distribution D_b, where m and n represent the input length and the output length, respectively, and m is a polynomial of n. While sampling from such distributions is in BPP, testing the closeness between them is seemingly much harder, as it is SZK-complete [SV03, GSV98].

Importantly, the SZK containment of $\mathrm{SD}[\alpha, \beta]$ for the *natural parameter regime* $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$, referred to as GapSD, remains an *open problem*. Specifically, the works of [SV03, GSV98] established that $\mathrm{SD}[\alpha, \beta]$ is in SZK for the constant polarizing regime, i.e., $\alpha^2 - \beta > 0$. This approach extends to the parameter regime $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$, as clarified in [Gol19]. More recently, Berman, Degwekar, Rothblum, and Vasudevan [BDRV19] improved the parameter regime to $\alpha^2(n) - \beta(n) \geq 1/\mathrm{poly}(n)$ by employing a series of tailor-made reductions between time-bounded distribution testing problems with respect to carefully chosen closeness measures.

In the quantum world, Watrous [Wat02], building on the pioneering work [SV03], introduced the time-bounded *state* testing problem with respect to the trace distance, known as Quantum State Distinguishability (QSD). This problem $\mathrm{QSD}[\alpha, \beta]$ involves two (time-)efficiently preparable quantum states, ρ_0 and ρ_1, and asks whether ρ_0 is α-far from or β-close to ρ_1 with respect to the trace distance $\mathrm{T}(\rho_0, \rho_1)$. Here, a state ρ_b for $b \in \{0, 1\}$ is considered *efficiently preparable* if there exists an explicit polynomial-size quantum circuit Q_b that, given the input state $|0\rangle^{\otimes m}$, produces the n-qubit state ρ_b after tracing out the non-output qubits, where m and n represent the input length and the output length, respectively, and m is a polynomial of n.

Analogous to its classical counterpart, QSD is QSZK-complete [Wat02, Wat09b], where QSZK refers to the class of promise problems that possess *quantum* statistical zero-knowledge proofs. However, the QSZK containment techniques in [Wat02, Wat09b] demonstrated that $\mathrm{QSD}[\alpha, \beta]$ is in QSZK only for the *polarizing regime*, i.e., $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$. This technical limitation leads to an intriguing question:

Problem 1.1. *How can the* QSZK *containment regime for the time-bounded state testing problem* QSD *be improved beyond the polarizing regime?*

We can similarly define GapQSD, corresponding to $\mathrm{QSD}[\alpha, \beta]$ under the natural parameter regime $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$. Both Problem 1.1 and its classical counterpart essentially address the respective upper bounds of GapSD and GapQSD. For GapSD, the strongest known upper bound is $\mathsf{AM} \cap \mathsf{coAM}$ [BL13], which matches the best known upper bound of the class SZK [For87, AH91]. In contrast, the best known upper bound of GapQSD is PSPACE, as implicitly shown in [Wat02, Proposition 21]. Meanwhile, the previously strongest known upper bound of the class QSZK is $\mathsf{QIP(2)}$ [Wat02, Wat09b, JUW09], where $\mathsf{QIP(2)}$ denotes the class of promise problems

that admit two-message quantum interactive proof systems and it holds that $\mathsf{QIP}(2) \subseteq \mathsf{PSPACE}$ [JUW09].

Why do parameter regimes matter? In computational complexity theory, we typically use *worst-case hardness*, where *a few* C-hard instances are sufficient to identify that a computational problem Prob is hard for the class C. However, to demonstrate a C containment of Prob, we need to show this containment holds for *all* instances of Prob with completeness c and soundness s (the acceptance probability for *yes* instances and *no* instances, respectively), such that $c(n) - s(n)$ is at least $1/\mathrm{poly}(n)$.

Otherwise, we may risk having *a somewhat "fake" complete problem*. For instance, if a promise problem Prob is proven to be QSZK-hard and contained in QSZK for certain parameter regime, then we cannot rule out the possibility that those parameter regimes not yet known to be in QSZK may be inherently $\mathsf{QIP}(2)$-hard. This possibility suggests that Prob is not QSZK-complete unless $\mathsf{QSZK} = \mathsf{QIP}(2)$.

Resolving such parameter regime issues is often *technically challenging*. A specific example is the low-rank variant of GapQSD, where the rank of states ρ_0 and ρ_1 is at most polynomial in n. By leveraging rank-dependent inequalities between the trace distance and the Hilbert-Schmidt distance, such as [AS17, Equation (1.31)] or [CCC19, Equation 6], we can show that this low-rank variant of GapQSD is in BQP for certain parameter regime (with polynomial precision). This is achieved through a clever use of the SWAP test [BCWdW01]. However, a BQP containment of this problem under the natural regime, as established in [WZ24a], requires more sophisticated techniques.

1.1.2 Entropy difference scenarios

Beyond the ℓ_1 norm, the (quantum) entropy difference is another widely studied closeness measure in time-bounded distribution and state testing. The time-bounded distribution testing problem with respect to the *Shannon entropy difference*, known as Entropy Difference (ED), was introduced by Goldreich and Vadhan [GV99]. This problem ED$[g]$ considers two (time-)efficiently samplable distributions D_0 and D_1 and asks whether their Shannon entropies satisfy $\mathrm{H}(D_0) - \mathrm{H}(D_1) \geq g$ or $\mathrm{H}(D_1) - \mathrm{H}(D_0) \geq g$ for $g = 1$. The problem ED also serves as a complete characterization of the class SZK, and the SZK containment naturally extends to any $g(n) \geq 1/\mathrm{poly}(n)$.

In the quantum realm, Ben-Aroya, Schwartz, and Ta-Shma [BASTS10] investigated the time-bounded state testing problem with respect to the *von Neumann entropy difference*, referred to as Quantum Entropy Difference (QED). This problem QED$[g]$ involves two (time-)efficiently preparable quantum states, ρ_0 and ρ_1, and asks whether their von Neumann entropies satisfy $\mathrm{S}(\rho_0) - \mathrm{S}(\rho_1) \geq g$ or $\mathrm{S}(\rho_1) - \mathrm{S}(\rho_0) \geq g$ for $g = 1/2$. Like its classical counterpart, the problem QED is QSZK-complete, and the QSZK containment automatically holds for any $g(n) \geq 1/\mathrm{poly}(n)$.

In addition to the Shannon entropy difference, the work of [BDRV19] explored the time-bounded distribution testing problem with respect to its distance version, known as Jensen-Shannon Divergence Problem (JSP). This problem JSP$[\alpha, \beta]$ considers two (time-)efficiently samplable distributions, D_0 and D_1, and asks whether D_0 is α-far from or β-close to D_1 with respect to the Jensen-Shannon divergence $\mathrm{JS}(D_0, D_1)$. The problem JSP is SZK-complete, and the SZK containment holds in the natural regime

where $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$.

In the quantum domain, the quantum counterparts of the Jensen-Shannon divergence implicitly appear in the Holevo bound [Hol73a],[1] the quantum counterpart of JSP has not been investigated in previous work, prompting the following open question:

Problem 1.2. *How hard is the time-bounded state testing problem with respect to the quantum counterparts of the Jensen-Shannon divergence?*

1.1.3 ℓ_2 norm scenarios and the purity

The time-bounded distribution testing problem with respect to the (squared) Euclidean distance appears to be folklore as BPP-complete. The BPP containment follows from, for example, the approach in [BCH+19, Theorem 7.1], while the BPP hardness is also straightforward.[2]

In contrast, time-bounded state testing problems with respect to closeness measures related to the ℓ_2 norm have garnered more attention. For instance, the time-bounded state testing problem with respect to the quantity $\mathrm{Tr}(\rho_0\rho_1)$ is BQP-complete. The BQP containment follows directly from the SWAP test [BCWdW01] or a similar technique [EAO+02], while the BQP hardness is observed in [Kob03, Theorem 9].[3] Moreover, since the squared Hilbert-Schmidt distance $\mathrm{HS}^2(\rho_0, \rho_1)$ can be written as a linear combination of quantities $\mathrm{Tr}(\rho_0^2)$, $\mathrm{Tr}(\rho_1^2)$, and $\mathrm{Tr}(\rho_0\rho_1)$, the corresponding state testing problem is BQP-complete, with the BQP hardness observed in [RASW23].

However, for state testing problems with respect to the purity $\mathrm{Tr}(\rho^2)$ or the trace of *integer* quantum state powers $\mathrm{Tr}(\rho^q)$, only the BQP containment is known [BCWdW01, EAO+02], leaving an open question:

Problem 1.3. *Can estimating the trace of quantum state powers, such as* $\mathrm{Tr}(\rho^2)$*, fully capture the computational power of quantum computing, i.e., is it* BQP*-complete?*

An additional intriguing observation is that the quantum linear entropy, $\mathrm{S}_L(\rho) \coloneqq 1 - \mathrm{Tr}(\rho^2)$, naturally serves as a lower bound of the von Neumann entropy $\mathrm{S}(\rho)$. Similar to the dichotomy-like behavior discussed earlier, time-bounded state testing is computationally easy for $\mathrm{S}_L(\rho)$ but appears challenging for $\mathrm{S}(\rho)$, raising another interesting question:

Problem 1.4. *What is the computational hardness of* approximating *the von Neumann entropy* $\mathrm{S}(\rho)$*? More specifically, how hard are time-bounded state testing problems with respect to quantities that lie between* $\mathrm{S}_L(\rho)$ *and* $\mathrm{S}(\rho)$*?*

1.2 Background: Space-bounded quantum computation

In models of quantum computation, another key resource often considered alongside time is *space*, specifically the number of qubits used by the quantum circuit. The study of

[1] The quantum Jensen-Shannon divergence, as defined in [MLP05], matches the Holevo χ quantity for size-2 ensembles with a uniform distribution, as seen in the Holevo bound (e.g., [NC10, Theorem 12.1]).

[2] The BPP hardness owes to the fact that the squared Euclidean distance between the distribution $(p_{\mathrm{acc}}, 1 - p_{\mathrm{acc}})$ from the output bit of any BPP algorithm and the distribution $(1, 0)$ is $(1 - p_{\mathrm{acc}})^2$.

[3] For any BQP circuit C_x, the acceptance probability $\| |1\rangle\langle 1|_{\mathrm{out}} C_x |\bar{0}\rangle \|_2^2 = \mathrm{Tr}\big(|1\rangle\langle 1|_{\mathrm{out}} C_x |\bar{0}\rangle\langle\bar{0}| C_x^\dagger\big) = \mathrm{Tr}(\rho_0\rho_1)$, where $\rho_0 \coloneqq |1\rangle\langle 1|_{\mathrm{out}}$ and $\rho_1 \coloneqq \mathrm{Tr}_{\overline{\mathrm{out}}}\big(C_x |\bar{0}\rangle\langle\bar{0}| C_x^\dagger\big)$.

space-bounded quantum computation began with Watrous [Wat99, Wat03], who established fundamental properties of the complexity class $\mathsf{BQSPACE}[s(n)]$ for $s(n) \geq \Omega(\log n)$, including closure under complement. Here, $s(n)$ denotes the number of qubits in the circuit, and the circuit size (i.e., the number of elementary gates) is at most $2^{O(s(n))}$. The specific case of space-bounded quantum computation with $s(n) = \Theta(\log(n))$, referred to as *quantum logspace*, is known as BQL, or $\mathsf{BQ_UL}$ if only *unitary* gates are permitted.

How powerful are the quantum logspace models BQL and $\mathsf{BQ_UL}$? Watrous [Wat03] investigated classical simulations of space-bounded quantum computation, presenting deterministic simulations in $O(s^2(n))$ space and unbounded-error randomized simulations in $O(s(n))$ space. A decade later, van Melkebeek and Watson [vMW12] established a time-space *simultaneous* unbounded-error randomized simulation, achieving $\tilde{O}(t(n))$ time and $O(s(n) + \log t(n))$ space for bounded-error quantum algorithms running in $t(n)$ time and $s(n)$ space. Over the past two decades, significant developments have shown that BQP is well-defined, summarized chronologically as follows:

- **The choice of gateset**. The Solovey-Kitaev theorem [Kit97] establishes that most quantum classes are gateset-independent, given that the gateset is closed under adjoint and all entries in gates have reasonable precision. The work of [vMW12] presented a space-efficient counterpart of the Solovay-Kitaev theorem, implying that BQL is also *gateset-independent*.
- **Error reduction**. Error reduction for $\mathsf{BQ_UL}$ poses challenges because sequential repetition of a $\mathsf{BQ_UL}$ circuit necessitates reusing the workspace, and intermediate measurements are not allowed in this model. To overcome this, the approach in [FKL+16] adapted the witness-preserving error reduction for QMA [MW05], incorporating additional ideas to suit the space-efficient setting.
- **Intermediate measurements**. In the space-bounded scenario, the principle of deferred measurement is not applicable, as it would lead to an exponential increase in space complexity. Initially, BQL seems more powerful than $\mathsf{BQ_UL}$ since we cannot even directly prove that $\mathsf{BPL} \subseteq \mathsf{BQ_UL}$. However, recent work by Fefferman and Remscrim [FR21] (also see [GRZ21]) established the equivalence between BQL and $\mathsf{BQ_UL}$, indicating a space-efficient approach to eliminating (non-oblivious) intermediate measurements. For oblivious intermediate measurements, a simultaneous time-space efficient approach to eliminate them has been proposed [GR22], though this improvement does not appear to extend to the non-oblivious setting [Zha24].

1.2.1 Complete characterizations of quantum logspace

We now review prior (natural) complete characterizations of quantum logspace with *two-sided* errors (BQL and $\mathsf{BQ_UL}$). Ta-Shma [TS13] proposed the first candidate BQL-complete problem, building upon the earlier work of [HHL09], which established a BQP-complete problem for inverting a well-conditioned matrix. Specifically, Ta-Shma showed that inverting a (polynomial-size) well-conditioned matrix with polynomial precision is in BQL. Similarly, computing eigenvalues of an Hermitian matrix is also in BQL. These algorithms offer a *quadratic* space advantage over the best-known classical algorithms that saturate the classical simulation bound [Wat99, Wat03, vMW12]. Moreover, an *exponential* quantum advantage emerges when the workspace is restricted to logarithmic size. Later, Fefferman and Lin [FL18] advanced this line of work by establishing the

first natural $\mathsf{BQ_UL}$-complete problem. Their approach ingeniously leveraged amplitude estimation [BBHT98] to avoid the need for (non-oblivious) intermediate measurements.

More recently, Fefferman and Remscrim [FR21] further extended this natural $\mathsf{BQ_UL}$-complete problem (or BQL-complete, equivalently) to a *family* of natural BQL-complete problems. They showed that a well-conditioned version of standard DET^*-complete problems is BQL-complete, where DET^* denotes the class of problems that are NC^1 (Turing) reducible to intDET, including well-conditioned integer determinant (DET), well-conditioned matrix powering (MATPOW), and well-conditioned iterative matrix product (ITMATPROD), among others.

Notably, all previously identified BQL (or $\mathsf{BQ_UL}$)-complete problems are rooted in linear algebra, prompting the following intriguing question:

Problem 1.5. *Are there* BQL*-complete problems outside the linear-algebraic domain that are even more natural within the context of quantum computing?*

Furthermore, prior techniques for demonstrating BQL or $\mathsf{BQ_UL}$ containments have all followed the approach introduced in [TS13], leading to another compelling question:

Problem 1.6. *Are there alternative, possibly systematic, approaches for establishing* BQL *containment? More ambitiously, can* all *techniques used for designing time-bounded quantum algorithms be adapted to space-bounded quantum computation?*

1.2.2 Quantum logspace with one-sided errors

Watrous [Wat01] introduced the one-sided error counterpart of unitary quantum logspace ($\mathsf{BQ_UL}$), namely the classes $\mathsf{RQ_UL}$ and $\mathsf{coRQ_UL}$. While error reduction for $\mathsf{BQ_UL}$ was only resolved fifteen years after the model was introduced, error reduction for $\mathsf{RQ_UL}$ and $\mathsf{coRQ_UL}$ was achieved in the same work that defined these classes. Notably, the question of whether intermediate measurements offer computational advantages in one-sided error scenarios, specifically $\mathsf{RQ_UL}$ vs. RQL and $\mathsf{coRQ_UL}$ vs. coRQL, remains unsolved.

In addition to exploring the fundamental properties of these classes, Watrous demonstrated that the undirected graph connectivity problem (USTCON) is in $\mathsf{RQ_UL} \cap \mathsf{coRQ_UL}$, highlighting a quantum advantage. However, several years later, Reingold [Rei08] proved that USTCON is in L. More recently, Fefferman and Remscrim [FR21] proposed a "verification" version of the well-conditioned iterative matrix product problem (vITMATPROD) as a *candidate* coRQL-complete problem. While this problem is known to be coRQL-hard, its containment in coRQL remains *unresolved*. Specifically, vITMATPROD requires to decide whether a single entry in the product of a polynomial number of well-conditioned matrices is equal to zero. These developments raise the following intriguing question:

Problem 1.7. *Do the classes* $\mathsf{RQ_UL}$ *and* $\mathsf{coRQ_UL}$ *have natural complete problems?*

1.3 Our contributions

This section demonstrates how our contributions (partially) resolve the problems outlined in Problems 1.1 to 1.7, which were proposed in the background sections.

1.3.1 A dichotomy theorem on approximating von Neumann entropy

We begin by addressing Problem 1.4. A natural point is the *power* quantum entropy of order q, which is closely related to the trace of quantum state powers $\mathrm{Tr}(\rho^q)$. In particular, the quantum q-Tsallis entropy $\mathrm{S}_q(\rho)$, which is a non-additive (but still concave) generalization of the von Neumann entropy $\mathrm{S}(\rho)$, with the von Neumann entropy being the limiting case of the quantum q-Tsallis entropy as q approaches 1:

$$\mathrm{S}_q(\rho) = \frac{1 - \mathrm{Tr}(\rho^q)}{q-1} \quad \text{and} \quad \lim_{q\to 1} \mathrm{S}_q(\rho) = \mathrm{S}(\rho) = -\mathrm{Tr}(\rho \log \rho).$$

This connection suggests that $\mathrm{S}_q(\rho)$ can provide a natural lower bound for $\mathrm{S}(\rho)$ when considering $\mathrm{S}_q(\rho)$ with $q = 1 + \epsilon$, where ϵ can be a small constant, such as $q = 1.0001$. Furthermore, for $1 \le q \le 2$, the inequality $\mathrm{S}_L(\rho) = \mathrm{S}_2(\rho) \le \mathrm{S}_q(\rho) \le \mathrm{S}(\rho)$ holds, indicating that $\mathrm{S}_q(\rho)$ serves as a promising candidate quantity for tackling Problem 1.4.

The study of power entropy dates back to Havrda and Charvát [HC67]. Since then, it has been rediscovered independently by Daróczy [Dar70], and finally popularized by Tsallis [Tsa88]. Raggio [Rag95] further expanded on this study by introducing the quantum Tsallis entropy. Tsallis entropy has been proven particularly useful in physics, where it describes systems with non-extensive properties, such as long-range interactions, in statistical mechanics (see [Tsa01] for further details).

A notable example is the Tsallis entropy $\mathrm{H}_q(p)$ with $q = 3/2$, which is useful for modeling systems where both frequent and rare events matter.[4] For instance, in fluid dynamics, the distribution that maximizes $\mathrm{H}_{3/2}$ helps model velocity changes in turbulent flows [Bec02]. Existing efficient quantum algorithms [BCWdW01, EAO+02] are designed particularly for integer $q \ge 2$. Therefore, estimating $\mathrm{S}_q(\rho)$ for non-integer q between 1 and 2 appears to be computationally challenging, which in turn motivates Problem 1.4.

Next, we focus on estimating the trace of quantum state powers $\mathrm{Tr}(\rho^q)$, which leads to the Quantum q-Tsallis Entropy Difference Problem ($\mathrm{TsallisQED}_q$). The definition of $\mathrm{TsallisQED}_q$ is similar to that of QED, with the key difference being the use of the quantum Tsallis entropy instead of the von Neumann entropy.

Our first main result is a sharp phase transition between the case of $q = 1$ and constant $q > 1$ in the computational complexity of $\mathrm{TsallisQED}_q$, identifying the easy and hard regimes for approximating the von Neumann entropy (Problem 1.4):

(i) For the regime $1 + \Omega(1) \le q \le 2$, which includes the purity $\mathrm{Tr}(\rho^2)$, the problem is BQP-complete. Moreover, the BQP containment holds when $q \ge 1 + \Omega(1)$.

(ii) For the regime $1 < q < 1 + \frac{1}{n-1}$, the problem is QSZK-hard, leading to hardness of approximating von Neumann entropy as long as $\mathsf{BQP} \subsetneq \mathsf{QSZK}$.

Remarkably, the BQP containment in Item (i) serves as a *time-efficient* quantum estimator for q-Tsallis entropy, *exponentially* improving the prior best results. Specifically, several quantum algorithms for estimating the q-Tsallis entropy of an n-qubit quantum state ρ, where $q > 1$ is a non-integer constant, have been proposed in [AISW20, WGL+24, WZL24, WZ24b]. All of these algorithms turn out to have time complexity $\exp(n)$ in the

[4] In contrast, the Tsallis entropy with $q = 2$ (Gini impurity) is very sensitive to rare events.

setting that ρ is given by its state-preparation circuit of size $\mathrm{poly}(n)$. Additionally, the BQP hardness in Item (i) implies that Purity Estimation is BQP-hard, which provides a positive resolution to Problem 1.3.

In terms of techniques, our BQP containments (upper bounds) are achieved by constructing (time-)efficiently computable *uniform* polynomial approximations of positive power functions, inspired by Serge Bernstein's works from nearly a century ago [Ber14, Ber38], and applying them within the quantum singular value transformation framework [GSLW19]. In addition, our hardness results (lower bounds) in Items (i) and (ii) are derived from reductions based on new inequalities for the quantum q-Jensen-Tsallis divergence [BH09] with $1 \leq q \leq 2$. Notably, when $q = 1$, this divergence coincides with the quantum Jensen-Shannon divergence [MLP05], which is related to Problem 1.2. The corresponding time-bounded state testing problem will be addressed later.

1.3.2 Space-bounded quantum state testing via space-efficient quantum singular value transformation

Does the dichotomy-like behavior also arise in quantum state testing under *other* resource constraints? A natural way to explore this question, as previously discussed, is to consider quantum computation models with limited memory, particularly space-bounded quantum computation (or quantum logspace).

To address this, we introduce *space-bounded* variants of quantum state testing problems (with two-sided errors), focusing on state-preparation circuits that act on $O(\log n)$ qubits, with the number of elementary gates being at most $\mathrm{poly}(n)$. We also consider the quantum state testing problems with *one-sided* errors, often referred to as *quantum state certification* [BOW19], in space-bounded scenarios. Our investigation leads to the following novel complete characterization of quantum logspace:

(iii) In the two-sided error setting, space-bounded state testing with respect to common distance-like measures – including the trace distance, the quantum entropy difference (and its distance version, the quantum Jensen-Shannon divergence), and the (squared) Hilbert-Schmidt distance – is BQL-complete.

(iv) In the one-sided error setting, space-bounded state certification with respect to the trace distance and the (squared) Hilbert-Schmidt distance is $\mathsf{coRQ_UL}$-complete.

The BQL-complete problems in Item (iii) are notably more natural in the context of quantum computing, resolving Problem 1.5, and are arguably simpler than previous BQL-complete problems in the linear-algebraic domain. Moreover, the $\mathsf{coRQ_UL}$-complete problems in Item (iv) serve as the *first* family of natural complete problems of quantum logspace with one-sided errors, corresponding to the classes $\mathsf{coRQ_UL}$ and $\mathsf{RQ_UL}$. This provides an answer to Problem 1.7.

The idea for establishing the containments in Items (iii) and (iv) is conceptually simple: implement the two-outcome measurement tailored to the chosen closeness measure:

$$\Pi_b = \frac{I}{2} + \frac{(-1)^b}{2} f(A), \text{ where } b \in \{0, 1\}.$$

Here, $f(A)$ represents a specific function applied to the eigenvalues of some Hermitian

matrix A, which relates to ρ_0 and ρ_1. An illustrative example is the (squared) Hilbert-Schmidt distance, where the measurement operator becomes $\Pi_b = \frac{I}{2} + \frac{(-1)^b}{2}\mathrm{SWAP}(\rho_0, \rho_1)$. The function $\mathrm{SWAP}(\rho_0, \rho_1)$ can be efficiently implemented by the SWAP test [BCWdW01], and the corresponding measurement is achievable through the one-bit precision phase estimation [Kit95], also known as the Hadamard test [AJL09].

However, for closeness measures beyond the Hilbert-Schmidt distance – widely regarded as more challenging in time-bounded state testing problems – new techniques are required. This challenge leads to the primary technical contribution of this subsection:

(v) A *space-efficient* variant of quantum singular value transformation [GSLW19]. More precisely, for any efficiently implementable unitary dilation U (a block-encoding) of an Hermitian matrix A acting on $O(\log n)$ qubits, it is possible to approximately implement the quantum singular value transform $f^{(\mathrm{SV})}(U)$ corresponding to any piecewise-smooth function $f(x)$. This quantum circuit implementation requires $O(\log n)$ qubits, and the polynomial approximation $P_d^{(f)}$ of degree $\mathrm{poly}(n)$ can also be constructed in classical (possibly randomized) logspace.

Our technique presented in Item (v) not only provides a unified framework for designing quantum logspace algorithms, offering a positive answer to Problem 1.6, but also establishes simultaneous time-space upper bounds. As a consequence, our results have broader implications beyond quantum logspace, including the following:

(vi) We prove that QSZK is in $\mathsf{QIP(2)}$ with a quantum linear-space honest prover, slightly improving from the best known upper bound $\mathsf{QIP(2)}$ [Wat02, JUW09], where the computational power of the honest prover is *unbounded*.

(vii) In the context of quantum interactive proofs, we introduce a space-bounded variant of quantum statistical zero-knowledge ($\mathsf{QSZK_UL}$), where the verifier uses *unitary* quantum logspace. We further establish that this model is as weak as BQL, implying that the statistical zero-knowledge property in the space-bounded setting negates the computational advantage typically gained from the interaction.

Interestingly, Item (vii) establishes a correspondence between the white-box state testing problem and quantum statistical zero-knowledge in the space-bounded scenario. Specifically, space-bounded state testing with respect to the trace distance ($\textsc{GapQSD}_{\log}$) is $\mathsf{QSZK_UL}$-complete. This correspondence mirrors the time-bounded setting in both classical (e.g., [GV11]) and quantum contexts, where QSD is QSZK-complete.

The main technique underlying Item (vi) is an *algorithmic* version of the Holevo-Helstrom measurement. Specifically, the celebrated Holevo-Helstrom bound [Hol73b, Hel69] states that the maximum success probability to discriminate quantum states ρ_0 and ρ_1 is given by $\frac{1}{2} + \frac{1}{2}\mathrm{T}(\rho_0, \rho_1)$. This bound is achieved by an optimal two-outcome measurement $\{\Pi_0, \Pi_1\}$, referred to as the Holevo-Helstrom measurement, satisfying $\mathrm{T}(\rho_0, \rho_1) = \mathrm{Tr}(\Pi_0\rho_0) - \mathrm{Tr}(\Pi_0\rho_1)$.

Our contribution in Item (vi) is an (approximately) explicit implementation of the Holevo-Helstrom measurement. This implementation is inspired by the BQL containment of $\textsc{GapQSD}_{\log}$ described in Item (iii). It operates within quantum single-exponential time – polynomial in the dimension of the state – and linear space, achieving an additive error of 2^{-n}. By leveraging this technique, Item (vi) is obtained by inspecting the "distance

test" in [Wat02] since GapQSD is QSZK-hard.

1.3.3 QSZK containments of QSD beyond the polarizing regime

In this subsection, we address Problem 1.1 by presenting a partial solution inspired by the classical work [BDRV19], which tackled the classical counterpart of Problem 1.1. Notably, while we establish improved QSZK containments of QSD, our results are limited to slightly *weaker* parameters. This limitation arises from fundamental differences between classical and quantum closeness measures.

More specifically, the improved SZK containment of SD, established in [BDRV19], is achieved through a series of tailor-made reductions involving time-bounded distribution testing problems with respect to the *triangular discrimination* and the *Jensen-Shannon divergence*. These two closeness measures, in particular, capture the limitation of two known approaches to polarization:

- The original polarization approach [SV03] reduces errors alternately for *yes* instances (direct product lemma) and *no* instances (XOR lemma). This approach is fully characterized by triangular discrimination, as the corresponding distribution testing problem $\mathrm{TDP}[\alpha, \beta]$ is in SZK for the regime $\alpha(n) - \beta(n) \geq 1/O(\log n)$.
- The entropy extraction approach [GSV99] relies crucially on the Jensen-Shannon divergence, which can be viewed as a distance version of entropy difference, as observed implicitly in [Vad99]. Hence, the corresponding distribution testing problem $\mathrm{JSP}[\alpha, \beta]$ is in SZK for the natural parameter regime $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$.

While classical distances (more formally, classical closeness measures) often have several quantum counterparts, the trace distance *uniquely* serves as the quantum analog of the total variation distance. Consequently, the polarization lemma applies almost directly to the trace distance, as noted in [Wat02]. However, tackling Problem 1.1 requires defining *proper* quantum analogs of the time-bounded distribution testing problems TDP and JSP. This task is challenging because quantum analogs of the corresponding closeness measures either have several choices or have not been defined yet.

To overcome this, we introduce two time-bounded state testing problems: the Measured Quantum Triangular Discrimination Problem (measQTDP) and the Quantum Jensen-Shannon Divergence Problem (QJSP). Notably, the latter corresponds exactly to Problem 1.2. We then establish that both measQTDP and QJSP are QSZK-complete, which allows us to improve the QSZK containment regime for QSD:

(viii) $\mathrm{measQTDP}[\alpha, \beta]$ is in QSZK for the regime $\alpha(n) - \beta(n) \geq 1/O(\log n)$, while $\mathrm{QJSP}[\alpha, \beta]$ is in QSZK for the regime $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$.

Additionally, the latter result improves the QSZK containment of $\mathrm{QSD}[\alpha, \beta]$, extending it to the regime $\alpha^2(n) - \sqrt{2 \ln 2}\beta(n) \geq 1/\mathrm{poly}(n)$, as opposed to the polarizing regime $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$.

The improved QSZK containment of QSD, as presented in Item (viii), is slightly weaker than the classical work [BDRV19]. This disparity arises because quantum analogs of the triangular discrimination, which are central to establish Item (viii), exhibit *distinct* behaviors from the classical equivalent.

Our definitions of measQTDP and QJSP serve as proper quantum analogs of TDP and JSP, respectively, since these time-bounded state testing problems capture the limitations of known approaches to polarize quantum distances:

- The original polarization approach [SV03, Wat02] is captured by the *measured* quantum triangular discrimination, as the corresponding state testing problem measQTDP is in QSZK for the natural parameter regime with logarithmic precision. Interestingly, another natural quantum analog, the quantum triangular discrimination *does not* achieve a similar result.
- The quantum entropy extraction approach [BASTS10] is fully characterized by the quantum Jensen-Shannon divergence. This is because not only the corresponding state testing problem QJSP is in QSZK for the natural parameter regime, but also a simple QSZK-hardness proof for QED follows from this containment.

In addition to examining the limitations of quantum polarizations, we also identify easy regimes for the class QSZK. Specifically, we prove that QSD with some exponentially small errors is in PP, suggesting that *dimension-preserving* polarization – where the number of qubits in the polarized states is as same as in the original states – is unlikely to be achievable unless $\mathsf{QSZK} \subseteq \mathsf{PP}$. Furthermore, we show that QSD without error is in NQP, a subclass of PP that serves as a precise variant of BQP with an *exact zero* acceptance probability for *no* instances [ADH97, YY99].

1.4 Organization

In Chapter 2, we introduce our notations and provide a brief review of space-bounded quantum computation, a basic mathematical background related to QSVT, and useful classical and quantum algorithmic tools.

In Chapter 3, we define closeness measures for classical probability distributions and quantum states, discuss relevant results on (time-bounded) distribution and state testing (including quantitative bounds), and briefly review space-bounded distribution testing.

In Chapter 4, we present our work on estimating the trace of quantum state powers, which can be viewed as a dichotomy theorem on approximating von Neumann entropy. This chapter is based on [LW25], a joint work with Qisheng Wang.

In Chapter 5, we develop space-efficient quantum singular value transformation and apply it to space-efficient error reduction for unitary quantum computations. This part is based on joint work with François Le Gall and Qisheng Wang [LLW23, Section 3].

In Chapter 6, we introduce space-bounded quantum state testing and explore two topics extending beyond quantum logspace: (1) implementing an algorithmic Holevo-Helstrom measurement, which leads to a slightly improved upper bound for QSZK; and (2) demonstrating the weakness of space-bounded unitary quantum statistical zero-knowledge, as an example of quantum interactive proofs. This chapter is primarily based on [LLW23, Sections 4 and 5], with Section 6.4 drawing on joint work with François Le Gall, Harumichi Nishimura, and Qisheng Wang [LLNW24, Section 5].

In Chapter 7, we establish the QSZK containment of QSD beyond the polarizing regime, based on a single-author work [Liu23].

In Chapter 8, the final chapter, we summarize the dissertation and highlight several open problems for future research.

Chapter 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 classical and quantum complexity theory, refer to [AB09, Wat09a], respectively.

Throughout this dissertation, the following conventions are adopted:

(1) The notation $[n]$ represents the set $\{1, 2, \ldots, n\}$.

(2) The notation $\widetilde{O}(f)$ is defined as $O(f \operatorname{polylog}(f))$.

(3) The notation $|\bar{0}\rangle$ is used to denote $|0\rangle^{\otimes a}$ with $a > 1$.

(4) The operator norm (i.e., the Schatten ∞-norm) of a matrix A is denoted by $\|A\|$.

Logarithm function and its generalization. Since this dissertation involves various notions of entropy-like quantities, we adopt specific conventions for the logarithm function and its generalization. Unless stated otherwise in a particular section, the terms $\log(x)$ and $\ln(x)$ are used interchangeably to denote the natural logarithm for any $x \in \mathbb{R}^+$, while the term $\log_2(x)$ specifically refers to the base-2 logarithm for any $x \in \mathbb{R}^+$.

To generalize the natural logarithm, we define the *q-logarithm* function $\ln_q \colon \mathbb{R}^+ \to \mathbb{R}$ for any real $q \neq 1$ as follows:

$$\forall x \in \mathbb{R}^+, \quad \ln_q(x) \coloneqq \frac{1 - x^{1-q}}{q - 1}.$$

It is easy to verify that $\lim_{q \to 1} \ln_q(x) = \ln(x)$ for all $x \in \mathbb{R}^+$. For $q \neq 1$, however, the q-logarithm exhibits distinct behavior; for example, it satisfies the relation

$$\ln_q(xy) = \ln_q(x) + \ln_q(y) + (1 - q) \ln_q(x) \ln_q(y).$$

Further properties of the q-logarithm can be found in [Tsa01, Appendix] and [Yam02].

Linear maps and quantum channels. We recommend [AS17, Section 2.3] as an introduction on superoperators and quantum channels. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be finite-dimensional Hilbert spaces with $\dim(\mathcal{H}_i) = N_i = 2^{n_i}$ for $i \in \{1, 2\}$. Let $\mathrm{L}(\mathcal{H}_1, \mathcal{H}_2)$ denote linear maps from $\mathcal{H}_1$ to $\mathcal{H}_2$, and specifically, let $\mathrm{L}(\mathcal{H})$ denote linear maps from $\mathcal{H}$ to $\mathcal{H}$. A map $\Phi \colon \mathrm{L}(\mathcal{H}_1) \to \mathrm{L}(\mathcal{H}_2)$ is called *self-adjointness-preserving* if $\Phi(X^\dagger) = (\Phi(X))^\dagger$ for any

$X \in \mathrm{L}(\mathcal{H}_1)$. We further say that a self-adjointness-preserving map $\Phi\colon \mathrm{L}(\mathcal{H}_1) \to \mathrm{L}(\mathcal{H}_2)$ is a *quantum channel* if Φ is a completely positive trace-preserving map. Here, a map Φ is *trace-preserving* if $\mathrm{Tr}(\Phi(X)) = \mathrm{Tr}(X)$ for any $X \in \mathrm{L}(\mathcal{H}_1)$. Let $\{|v_i\rangle\}_{i\in[N_1]}$ denote an orthonormal basis of $\mathcal{H}_1$, and a map Φ is defined as *completely positive* if $\Phi \otimes I_n$ is positive for any $n \in \mathbb{N}$, where I_n represents the identity matrix of dimension n.

Let $\mathrm{D}(\mathcal{H})$ be the set of all density matrices (often referred to as *quantum states*), which are positive semi-definite and trace-one matrices on $\mathcal{H}$. Let the trace norm of a linear map X be $\|X\|_1 \coloneqq \mathrm{Tr}\left(\sqrt{X^\dagger X}\right)$. For any quantum channels $\mathcal{E}$ and $\mathcal{F}$ that act on $\mathrm{D}(\mathcal{H})$, the *diamond norm distance* between them is defined as the following:

$$\|\mathcal{E} - \mathcal{F}\|_\diamond \coloneqq \sup_{\rho\in\mathrm{D}(\mathcal{H}\otimes\mathcal{H}')} \|(\mathcal{E}\otimes\mathcal{I}_{\mathcal{H}'})(\rho) - (\mathcal{F}\otimes\mathcal{I}_{\mathcal{H}'})(\rho)\|_1.$$

Promise problems and reductions. We say that $\mathcal{P} = (\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$ is a *promise* problem, if it satisfies the conditions $\mathcal{P}_{\text{yes}} \cap \mathcal{P}_{\text{no}} = \emptyset$ and $\mathcal{P}_{\text{yes}} \cup \mathcal{P}_{\text{no}} \subseteq \{0,1\}^*$.

We then proceed with the concept of *reductions* between promise problems. This concept serves as a fundamental tool for characterizing computational hardness, especially in the context of complexity classes. Following the definitions presented in [Gol08, Section 2.2.1], two types of reductions are considered from a promise problem $\mathcal{P} = (\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$ to another promise problem $\mathcal{P}' = (\mathcal{P}'_{\text{yes}}, \mathcal{P}'_{\text{no}})$:

- **Karp reduction**. A deterministic polynomial-time computable function f is called a *Karp reduction* from a promise problem $\mathcal{P}$ to another promise problem $\mathcal{P}'$ if, for every x, the following holds: $x \in \mathcal{P}_{\text{yes}}$ if and only if $f(x) \in \mathcal{P}'_{\text{yes}}$, and $x \in \mathcal{P}_{\text{no}}$ if and only if $f(x) \in \mathcal{P}'_{\text{no}}$.
- **Turing reduction**. A promise problem $\mathcal{P}$ is *Turing-reducible* to a promise problem $\mathcal{P}'$ if there exists a deterministic polynomial-time oracle machine $\mathcal{A}$ such that, for every function f that solves $\mathcal{P}'$ it holds that $\mathcal{A}^f$ solves $\mathcal{P}$. Here, $\mathcal{A}^f(x)$ denotes the output of machine $\mathcal{A}$ on input x when given oracle access to f.

It is noteworthy that Karp reduction is a special case of Turing reduction.

This chapter is organized as follows. Section 2.1 provides a brief overview of space-bounded quantum computation. Section 2.2 describes the basics of singular value decomposition and transformation. Section 2.3 presents techniques in polynomial approximation, including best uniform approximation of positive constant powers, Chebyshev polynomials, and Chebyshev truncated expansions. Finally, Section 2.4 outlines the classical and quantum algorithmic tools employed in this dissertation.

2.1 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 output $s(n)$ 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 output $f(n)$. Our definitions of space-bounded quantum computation are formulated in terms of *quantum circuits*, whereas many prior works focused on *quantum Turing machines* [Wat99, Wat03, vMW12]. 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 defining time-bounded and space-bounded quantum circuit families, and then proceed to the corresponding complexity class $\mathsf{BQ_USPACE}[s(n)]$. It is worth noting that we use the abbreviated notation C_x to denote that the circuit $C_{|x|}$ takes input x.

Definition 2.1 (Time- and space-bounded quantum circuit families)**.** *A (unitary) quantum circuit is a sequence of quantum gates, each of which belongs to some fixed gateset that is universal for quantum computation, such as* $\{\mathrm{H}, \mathrm{CNOT}, \mathrm{T}\}$.

For a promise problem $\mathcal{P} = (\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$*, we say that a family of quantum circuits* $\{C_x : x \in \mathcal{P}\}$ *is* $t(n)$*-time-bounded if there is a deterministic Turing machine that, on any input* $x \in \mathcal{P}$*, runs in time* $O(t(|x|))$*, and outputs a description of* C_x *such that* C_x *accepts (resp., rejects) if* $x \in \mathcal{P}_{\text{yes}}$ *(resp.,* $x \in \mathcal{P}_{\text{no}}$*).*

Similarly, we say that a family of quantum circuits $\{C_x : x \in \mathcal{P}\}$ *is* $s(n)$*-space-bounded if there is a deterministic Turing machine that, on any input* $x \in \mathcal{P}$*, runs in space* $O(s(|x|))$ *(and hence time* $2^{O(s(|x|))}$*), and outputs a description of* C_x *such that* C_x *accepts (resp., rejects) if* $x \in \mathcal{P}_{\text{yes}}$ *(resp.,* $x \in \mathcal{P}_{\text{no}}$*), as well as* C_x *is acting on* $O(s(|x|))$ *qubits and has* $2^{O(s(|x|)}$ *gates..*

Definition 2.2 ($\mathsf{BQ_USPACE}[s(n), a(n), b(n)]$, adapted from Definition 5 in [FR21])**.** *Let* $s\colon \mathbb{N} \to \mathbb{N}$ *be a space-constructible function such that* $s(n) \geq \Omega(\log n)$*. Let* $a(n)$ *and* $b(n)$ *be functions that are computable in deterministic space* $s(n)$*. A promise problem* $(\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$ *is in* $\mathsf{BQ_USPACE}[s(n), a(n), b(n)]$ *if there exists a family of* $s(n)$*-space-bounded (unitary) quantum circuits* $\{C_x\}_{x \in \mathcal{P}}$*, where* $n = |x|$*, satisfying the following:*

- *The output qubit is measured in the computational basis after applying* C_x*. We say that* C_x *accepts* x *if the measurement outcome is* 1*, whereas* C_x *rejects* x *if the outcome is* 0*.*
- $\Pr[C_x \text{ accepts } x] \geq a(|x|)$ *if* $x \in \mathcal{P}_{\text{yes}}$*, whereas* $\Pr[C_x \text{ accepts } x] \leq b(|x|)$ *if* $x \in \mathcal{P}_{no}$*.*

We remark that Definition 2.2 is *gateset-independent*, given that the gateset is closed under adjoint and all entries in chosen gates have reasonable precision. This property is due to the space-efficient Solovay-Kitaev theorem presented in [vMW12]. Moreover, we can achieve error reduction for $\mathsf{BQ_USPACE}[s(n), a(n), b(n)]$ as long as $a(n) - b(n) \geq 2^{-O(s(n))}$, which follows from [FKL+16] or our space-efficient QSVT-based construction in Section 5.4. We thereby define $\mathsf{BQ_USPACE}[s(n)] \coloneqq \mathsf{BQ_USPACE}[s(n), 2/3, 1/3]$ to represent (two-sided) bounded-error unitary quantum space, and $\mathsf{BQ_UL} \coloneqq \mathsf{BQ_USPACE}[O(\log n)]$ to denote unitary quantum logspace.

We next consider general space-bounded quantum computation, which allows (oblivious) *intermediate measurements* and *reset-to-zero operations*. As a corollary of the Stinespring dilation theorem (e.g., [AS17, Theorem 2.25], see also [AKN98, Section 4.1]), for any quantum channel Φ mapping from density matrices on k_1 qubits to density matrices on k_2 qubits, we can exactly simulate this quantum channel Φ by a unitary quantum circuit acting on $2k_1 + k_2$ qubits. Therefore, we extend Definition 2.1 to *general quantum circuits*, which allows local operations, such as intermediate measurements in the computational basis, resetting qubits to their initial states, and tracing out qubits. Now we proceed with a definition on $\mathsf{BQSPACE}[s(n)]$.

Definition 2.3 ($\mathsf{BQSPACE}[s(n), a(n), b(n)]$, adapted from Definition 7 in [FR21])**.** *Let $s\colon \mathbb{N} \to \mathbb{N}$ be a space-constructible function such that $s(n) \geq \Omega(\log n)$. Let $a(n)$ and $b(n)$ be functions that are computable in deterministic space $s(n)$. A promise problem $(\mathcal{P}_{\text{yes}}, \mathcal{P}_{\text{no}})$ is in $\mathsf{BQSPACE}[s(n), a(n), b(n)]$ if there exists a family of $s(n)$-space-bounded general quantum circuits $\{\Phi_x\}_{x\in\mathcal{P}}$, where $n = |x|$, satisfying the following holds:*

- *The output qubit is measured in the computational basis after applying Φ_x. We say that Φ_x accepts x if the measurement outcome is 1, whereas Φ_x rejects x if the outcome is 0.*
- $\Pr[\Phi_x \text{ accepts } x] \geq a(|x|)$ *if* $x \in \mathcal{P}_{\text{yes}}$, *whereas* $\Pr[\Phi_x \text{ accepts } x] \leq b(|x|)$ *if* $x \in \mathcal{P}_{no}$.

It is noteworthy that unitary quantum circuits, which correspond to unitary channels, are a specific instance of general quantum circuits that correspond to quantum channels. we thus infer that $\mathsf{BQ_USPACE}[s(n)] \subseteq \mathsf{BQSPACE}[s(n)]$ for any $s(n) \geq \Omega(\log n)$. However, the opposite direction was a long-standing open problem. Recently, Fefferman and Remscrim [FR21] demonstrated a remarkable result that

$$\mathsf{BQSPACE}[s(n)] \subseteq \mathsf{BQ_USPACE}[O(s(n))].$$

In addition, it is evident that $\mathsf{BQSPACE}[s(n)]$ can achieve error reduction since it admits sequential repetition simply by resetting working qubits. Therefore, we can define $\mathsf{BQSPACE}[s(n)] \coloneqq \mathsf{BQSPACE}[s(n), 2/3, 1/3]$ to represent (two-sided) bounded-error general quantum space, and denote general quantum logspace by $\mathsf{BQL} \coloneqq \mathsf{BQSPACE}[O(\log n)]$.

We now turn our attention to *one-sided* bounded-error unitary quantum space, particularly $\mathsf{RQ_USPACE}[s(n)]$ and $\mathsf{coRQ_USPACE}[s(n)]$ for $s(n) \geq \Omega(\log n)$. These complexity classes were first introduced by Watrous [Wat01] and have been further discussed in [FR21]. We proceed with the definitions:

$$\mathsf{RQ_USPACE}[s(n), a(n)] \coloneqq \mathsf{BQ_USPACE}[s(n), a(n), 0]$$
$$\mathsf{coRQ_USPACE}[s(n), b(n)] \coloneqq \mathsf{BQ_USPACE}[s(n), 1, b(n)]$$

It is noteworthy that $\mathsf{RQ_USPACE}[s(n), a(n)]$ and $\mathsf{coRQ_USPACE}[s(n), b(n)]$ can achieve error reduction, as shown in [Wat01] or our space-efficient QSVT-based construction in Section 5.4. We define the following

$$\mathsf{RQ_USPACE}[s(n)] \coloneqq \mathsf{BQ_USPACE}\left[s(n), \tfrac{1}{2}, 0\right]$$
$$\mathsf{coRQ_USPACE}[s(n)] \coloneqq \mathsf{BQ_USPACE}\left[s(n), 1, \tfrac{1}{2}\right]$$

to represent one-sided bounded-error unitary quantum space and logspace counterparts

$$\mathsf{RQ_UL} \coloneqq \mathsf{RQ_USPACE}[O(\log n)] \text{ and } \mathsf{coRQ_UL} \coloneqq \mathsf{coRQ_USPACE}[O(\log n)].$$

Remark 2.4 ($\mathsf{RQ_UL}$ and $\mathsf{coRQ_UL}$ are gateset-dependent). We observe that changing the gateset in space-efficient Solovay-Kitaev theorem [vMW12] can cause errors, revealing the *gateset-dependence* of unitary quantum space classes with one-sided bounded-error. To address this issue, we adopt a larger gateset $\mathcal{G}$ for $\mathsf{RQ_USPACE}[s(n)]$ and $\mathsf{coRQ_USPACE}[s(n)]$, which includes any single-qubit gates whose amplitudes can be computed in deterministic $O(s(n))$ space.

2.2 Singular value decomposition and transformation

We recommend [Bha96, HJ12, Hal87] for comprehensive textbooks on matrix analysis and linear algebra. For any $\tilde{d} \times d$ (complex) matrix A, there is a *singular value decomposition* of A such that $A = \sum_{i=1}^{\min\{d,\tilde{d}\}} \sigma_i |\tilde{\psi}_i\rangle\langle\psi_i|$, where:

- The *singular values* $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_{\min\{d,\tilde{d}\}} \geq 0$, where non-zero singular values σ_i are the square roots of non-zero the eigenvalues of $A^\dagger A$ or $AA^\dagger$.
- $|\tilde{\psi}_1\rangle, \cdots, |\tilde{\psi}_{\tilde{d}}\rangle$ form an orthonormal basis and are eigenvectors of $AA^\dagger$.
- $|\psi_1\rangle, \cdots, |\psi_d\rangle$ form an orthonormal basis and are eigenvectors of $A^\dagger A$.

Notably, the largest singular value of A coincides with the operator norm of A, specifically $\|A\| = \sigma_1(A)$. Let $\||\psi\rangle\|_2 := \sqrt{\langle\psi|\psi\rangle}$ be the Euclidean norm of a vector $|\psi\rangle$. Next, we list the families of matrices that are commonly used in this work. It is noteworthy that they all admit a singular value decomposition:

- **Hermitian matrices**. $H^\dagger = H$, if and only if $\langle\psi|H|\psi\rangle \in \mathbb{R}$ for all $|\psi\rangle$ such that $\||\psi\rangle\|_2 = 1$, if and only if the absolute values of the eigenvalues of H coincide with its singular value.
- **Unitary matrices**. $UU^\dagger = U^\dagger U = I$, if and only if $\|U|\psi\rangle\|_2 = \|U^\dagger|\psi\rangle\|_2 = 1$ for all $|\psi\rangle$ such that $\||\psi\rangle\|_2 = \||\psi\rangle\|_2 = 1$, if and only if all eigenvalues λ_i of U has modulus $|\lambda_i| = 1$, implying that all singular values of U are 1.
- **Positive semi-definite matrices**. $P = CC^\dagger$ for some matrix C, if and only if $\langle\psi|P|\psi\rangle \geq 0$ for all $|\psi\rangle$ such that $\||\psi\rangle\|_2 = 1$, if and only if all eigenvalues of P are non-negative.
- **Orthogonal projection matrices**. $\Pi^2 = \Pi = \Pi^\dagger$, if and only if $\Pi^2 = \Pi$ and $\|\Pi|\psi\rangle\|_2 \leq 1$ for all $|\psi\rangle$ such that $\||\psi\rangle\|_2 = 1$, if and only if all eigenvalues of Π are either 0 or 1 (see [Hal87, III.75] and [HJ12, Corollary 3.4.3.3] for the last characterization).
- **Partial isometries**. $GG^\dagger G = G$, if and only if $G^\dagger G G^\dagger = G^\dagger$, if and only if $\|G|\psi\rangle\|_2 = 1$ for all $|\psi\rangle \in \ker(G)^\perp$ such that $\||\psi\rangle\|_2 = 1$, if and only if $G^\dagger G$ is an orthogonal projection onto $\ker(G)^\perp$ (see [Hal87, Exercise III.76.5]). Consequently, the non-zero singular values of a partial isometry G are all 1. Moreover, an injective partial isometry is an isometry, and an invertible partial isometry is unitary.

For any matrix A satisfying $\|A\| \leq 1$, there is a unitary U with orthogonal projections $\tilde{\Pi}$ and Π such that $A = \tilde{\Pi} U \Pi$.[1] With these definitions in place, we can view the singular value decomposition as the *projected unitary encoding* (see Definition 5.3):

Definition 2.5 (Singular value decomposition of a projected unitary, adapted from Definition 7 in [GSLW19])**.** *Given a projected unitary encoding of A, denoted by U, associated with orthogonal projections Π and $\tilde{\Pi}$ on a finite-dimensional Hilbert space $\mathcal{H}_U$: $A = \tilde{\Pi} U \Pi$. Then the singular value decomposition of A ensures that orthonormal bases of Π and $\tilde{\Pi}$ such that:*

[1] As indicated in [HJ12, 2.7.P2], such a matrix U is called a *unitary dilation* of A. This unitary dilation U exists if and only if A is a contraction, namely $\|A\| \leq 1$.

- Π: $\{|\psi_i\rangle : i \in [d]\}$, *where* $d := \mathrm{rank}(\Pi)$, *of a subspace* $\mathrm{Img}(\Pi) = \mathrm{span}\{|\psi_i\rangle\}$;
- $\tilde{\Pi}$: $\left\{|\tilde{\psi}_i\rangle : i \in [\tilde{d}]\right\}$, *where* $\tilde{d} := \mathrm{rank}(\tilde{\Pi})$, *of a subspace* $\mathrm{Img}(\tilde{\Pi}) = \mathrm{span}\left\{|\tilde{\psi}_i\rangle\right\}$.

We say that a function $f\colon \mathbb{R} \to \mathbb{C}$ is *even* if $f(-x) = f(x)$ for all $x \in \mathbb{R}$, and that it is *odd* if $f(-x) = -f(x)$ for all $x \in \mathbb{R}$. Next, we define the *singular value transformation* of matrices:

Definition 2.6 (Singular value transformation by even or odd functions, adapted from Definition 9 in [GSLW19])**.** *Let $f\colon \mathbb{R} \to \mathbb{C}$ be an even or odd function. We consider a linear operator $A \in \mathbb{C}^{\tilde{d}\times d}$ satisfying the singular value decomposition $A = \sum_{i=1}^{\min\{d,\tilde{d}\}} \sigma_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$. We define the singular value transformation corresponding to f as follows:*

$$f^{(\mathrm{SV})}(A) := \begin{cases} \sum_{i=1}^{\min\{d,\tilde{d}\}} f(\sigma_i)|\tilde{\psi}_i\rangle\langle\psi_i|, & \text{for odd } f, \\ \sum_{i=1}^{d} f(\sigma_i)|\psi_i\rangle\langle\psi_i|, & \text{for even } f. \end{cases}$$

Here, $\sigma_i := 0$ for $i \in \{\min\{d,\tilde{d}\}+1, \cdots, d-1, d\}$.

Finally, for any $d \times d$ Hermitian matrix A, there is a *spectral decomposition* of A such that $A = \sum_{i=1}^{d} \lambda_i |\psi_i\rangle\langle\psi_i|$ where all eigenvalues $\{\lambda_i\}_{i=1}^{d}$ are real and $\{|\psi_i\rangle\}_{i=1}^{d}$ is an orthonormal basis. As a consequence, if f is an even or odd function,

$$f(A) = \sum_{i=1}^{d} f(\lambda_i)|\psi_i\rangle\langle\psi_i| = f^{(\mathrm{SV})}(A)$$

can be achieved by singular value transformation defined in Definition 2.6.

2.3 Polynomial approximations

This subsection introduces several useful tools for polynomial approximations.

Let $f(x)$ be a continuous function defined on the interval $[-1, 1]$ that we aim to approximate using a polynomial of degree at most d. We define P_d^* as a *best uniform (polynomial) approximation* on $[-1, 1]$ to f of degree d if, for any degree-d polynomial approximation P_d of f, the following holds:

$$\max_{x\in[-1,1]} |f(x) - P_d^*(x)| \leq \max_{x\in[-1,1]} |f(x) - P_d(x)|.$$

Let $\mathbb{R}_d[x]$ be the set of all polynomials (with real coefficients) of degree at most d. Equivalently, the best uniform approximation P_d^* to f is the polynomial that solves the minimax problem $\min_{P_d\in\mathbb{R}_d[x]} \max_{x\in[-1,1]} |f(x) - P_d(x)|$.

The best uniform polynomial approximation of positive constant powers, originally established by Bernstein [Ber14, Ber38], is particularly required:

Lemma 2.7 (Best uniform approximation of positive constant powers, adapted from Section 7.1.41 in [Tim63])**.** *For any positive integer r and order $\alpha \in (-1, 1)$, let $P_d^* \in \mathbb{R}[x]$ be the best uniform approximation for $f(x) = x^{r-1}|x|^{1+\alpha}$ of degree $d = \left\lceil (\beta_\alpha/\epsilon)^{\frac{1}{r+\alpha}} \right\rceil$, where β_α is a constant depending on α. Then, for sufficiently small ϵ, it holds that*

$$\max_{x\in[-1,1]} |P_d^*(x) - f(x)| \leq \epsilon.$$

2.3.1 Chebyshev polynomials and truncated expansions

We begin by defining Chebyshev polynomials, and then introduce Chebyshev truncation and averaged Chebyshev truncation, with the latter being known as the *de La Vallée Poussin partial sum*. We recommend [Riv90, Chapter 3] for a comprehensive review of Chebyshev series and Chebyshev expansion.

Definition 2.8 (Chebyshev polynomials)**.** *The Chebyshev polynomials (of the first kind) $T_k(x)$ are defined via the following recurrence relation:*

$$T_0(x) \coloneqq 1, T_1(x) \coloneqq x, \text{ and } T_{k+1}(x) \coloneqq 2xT_k(x) - T_{k-1}(x).$$

For $x \in [-1, 1]$, an equivalent definition is $T_k(\cos\theta) = \cos(k\theta)$.

To apply Chebyshev polynomials (of the first kind) for Chebyshev expansion, it is necessary to first define an inner product between two functions, f and g, as long as the following integral exists:

$$\langle f, g\rangle \coloneqq \frac{2}{\pi}\int_{-1}^{1} \frac{f(x)g(x)}{\sqrt{1-x^2}}\mathrm{d}x = \frac{2}{\pi}\int_{-\pi}^{0} f(\cos\theta)g(\cos\theta)\mathrm{d}\theta. \tag{2.1}$$

The Chebyshev polynomials form an orthonormal basis in the inner product space induced by $\langle\cdot,\cdot\rangle$ defined in Equation (2.1). As a result, any continuous and integrable function $f : [-1, 1] \to \mathbb{R}$ whose Chebyshev coefficients satisfy $\lim_{k\to\infty} c_k = 0$, where c_k is defined in Equation (2.2), has a Chebyshev expansion given by:

$$f(x) = \frac{1}{2}c_0T_0(x) + \sum_{k=1}^{\infty} c_kT_k(x) \text{ where } c_k \coloneqq \langle T_k, f\rangle. \tag{2.2}$$

A natural approach to approximating functions with a Chebyshev expansion is to consider the truncated version of the Chebyshev expansion $\tilde{P}_d = c_0/2+\sum_{k=1}^{d} c_kT_k$, denoted as *Chebyshev truncation*. Remarkably, $\tilde{P}_d$ provides a *nearly best* uniform (polynomial) approximation to f:

Lemma 2.9 (Nearly best uniform approximation by Chebyshev truncation, adapted from Theorem 3.3 in [Riv90])**.** *For any continuous and integrable function $f\colon [-1, 1] \to \mathbb{R}$, let $\varepsilon_d(f)$ be the truncation error that corresponds to the degree-d best uniform approximation on $[-1, 1]$ to f, then the degree-d Chebyshev truncation polynomial $\tilde{P}_d$ satisfies*

$$\varepsilon_d(f) \le \max_{x\in[-1,1]} |f(x) - \tilde{P}_d(x)| \le \left(4 + \frac{4}{\pi^2}\log d\right)\varepsilon_d(f)$$

Consequently, if there is a degree-d polynomial $P_d^* \in \mathbb{R}[x]$ such that $\max_{x\in[-1,1]} |f(x) - P_d^*(x)| \le \epsilon$, then the degree-$d$ Chebyshev truncation polynomial $\tilde{P}_d$ satisfies

$$\max_{x\in[-1,1]} |f(x) - \tilde{P}_d(x)| \le O(\epsilon \log d).$$

It is noteworthy that the proof of Lemma 2.9 in [Riv90] relies only on the linear decay of Chebyshev coefficients c_k for any Chebyshev expansion. However, for functions with a Chebyshev expansion whose Chebyshev coefficients decay almost exponentially, Chebyshev truncation is "asymptotically" as good as the best uniform approximation:

Lemma 2.10 (A sufficient condition that Chebyshev truncation is "asymptotically" best, adapted from Equation (3.44) in [Riv90])**.** *For any function f that admits a Chebyshev*

expansion, consider a degree-d Chebyshev truncation polynomial $\tilde{P}_d$, and let $\varepsilon_d(f)$ be the truncation error corresponds to the degree-d best uniform approximation on $[-1,1]$ to f. If the Chebyshev coefficients of $\tilde{P}_d$ satisfy $\sum_{k=2}^{\infty}|c_{d+j}| \le \eta|c_{d+1}|$, then

$$\varepsilon_d(f) \le \max_{x\in[-1,1]}|f(x)-\tilde{P}_d(x)| \le \frac{4}{\pi}(1+\eta)\varepsilon_d(f).$$

Although Lemma 2.10 improves the truncation error in Lemma 2.9 from $O(\epsilon \log d)$ to $O(\epsilon)$, it only applies to a fairly narrow range of functions, such as sine and cosine functions. Leveraging an average of Chebyshev truncations, known as the de La Vallée Poussin partial sum, we obtain the degree-d *averaged Chebyshev truncation* $\hat{P}_{d'}$, which is a polynomial of degree $d' = 2d-1$:

$$\hat{P}_{d'}(x) \coloneqq \frac{1}{d}\sum_{l=d}^{d'}\tilde{P}_l(x) = \frac{\hat{c}_0}{2} + \sum_{k=1}^{d'}\hat{c}_k T_k(x) \text{ where } \hat{c}_k = \begin{cases} c_k, & 0 \le k \le d' \\ \frac{2d-k}{d}c_k, & k > d \end{cases}. \tag{2.3}$$

As a consequence, we can achieve the truncation error 4ϵ for any function that admits Chebyshev expansion:

Lemma 2.11 (Asymptotically best approximation by averaged Chebyshev truncation, adapted from Exercise 3.4.6 and 3.4.7 in [Riv90])**.** *For any function f that has a Chebyshev expansion, consider the degree-d averaged Chebyshev truncation $\hat{P}_{d'}$ defined in Equation (2.3). Let $\varepsilon_d(f)$ be the truncation error corresponds to the degree-d best uniform approximation on $[-1,1]$ to f. If there is a degree-d polynomial $P_d^* \in \mathbb{R}[x]$ such that $\max_{x\in[-1,1]}|f(x)-P_d^*(x)| \le \epsilon$, then*

$$\max_{x\in[-1,1]}\left|f(x)-\hat{P}_{d'}(x)\right| \le 4\varepsilon_d(f) \le 4\max_{x\in[-1,1]}|f(x)-P_d^*(x)| \le 4\epsilon.$$

Lastly, we provide upper bounds for the ℓ_1 norm of the coefficient vector $\hat{\mathbf{c}} \coloneqq (\hat{c}_0, \cdots, \hat{c}_d)$ in Lemma 2.12. Interestingly, Chebyshev coefficients c_k (and so do $\hat{c}_k$) decay a bit faster if the function f becomes a bit smoother.

Lemma 2.12 (ℓ_1-norm bounds on the averaged truncated Chebyshev coefficient vector)**.** *For any function f that admits a Chebyshev expansion and is bounded with $\max_{x\in[-1,1]}|f(x)| \le B$ for some constant $B > 0$, we have the following ℓ_1-norm bounds for the coefficient vector $\hat{\mathbf{c}}$ corresponds to the degree-d averaged Chebyshev truncation $\hat{P}_{d'}$ with $d' = 2d-1$:*

- *For any function f satisfying our conditions, we have $\|\mathbf{c}\|_1 \le O(B\log d)$;*
- *If the function f is additionally (at least) twice continuously differentiable, $\|\mathbf{c}\|_1 \le O(B)$.*

Proof. By substituting $\cos\theta$ for x and calculating a direct integral, we obtain:

$$\begin{aligned} c_k &= \frac{2}{\pi}\int_{-\pi}^{0}\cos(k\theta)f(\cos\theta)\mathrm{d}\theta \\ &\le \frac{2}{\pi}\int_{-\pi}^{0}\cos(k\theta)\Big(\max_{x\in\{-1,1\}}|f(x)|\Big)\mathrm{d}\theta \\ &\le \frac{2B}{\pi}\int_{-\pi}^{0}\cos(k\theta)\mathrm{d}\theta \\ &= \frac{2B}{\pi}\cdot\frac{\sin(k\pi)}{k}. \end{aligned} \tag{2.4}$$

Here, the third line follows from the fact that f is bounded with $\max_{x\in[-1,1]} |f(x)| \leq B$ for some constant $B > 0$. Hence, by combining Equation (2.4) and the Euler-Maclaurin formula, we know that the coefficient vector $\hat{\mathbf{c}}$ satisfies

$$\|\hat{\mathbf{c}}\|_1 = \sum_{k=0}^{d} |c_k| + \sum_{k=d+1}^{2d-1} \frac{2d-k}{d}|c_k| \leq \frac{2B}{\pi} \sum_{k=0}^{2d-1} \frac{1}{k} \leq O(B \log d).$$

For any function f that exhibits better smoothness, we can derive a sharper bound by considering $c_k = \frac{2}{\pi}\int_{-\pi}^{0} \cos(k\theta) f(\cos\theta) \mathrm{d}\theta$ as Fourier coefficients of the function $f(\cos\theta)$. For any function f that is (at least) twice continuously differentiable, the decay properties of its Fourier coefficients (e.g., [SS03, Exercise 3.18(a)]) imply that $|c_k| \leq O(B/k^2)$. Hence, we obtain an improved norm bound $\|\hat{\mathbf{c}}\|_1 \leq \sum_{k=0}^{2d-1} O(B/k^2) \leq O(B)$ as per the Euler-Maclaurin formula. □

2.4 Classical and quantum algorithmic toolkit

Our convention assumes that for any algorithm $\mathcal{A}$ in bounded-error randomized time $t(n)$ and space $s(n)$, $\mathcal{A}$ outputs the correct value with probability at least 2/3 (viewed as "success probability").

2.4.1 Tools for space-bounded randomized algorithms

We first proceed with space-efficient success probability estimation:

Lemma 2.13 (Space-efficient success probability estimation by sequential repetitions)**.** *Let $\mathcal{A}$ be a randomized (resp., quantum) algorithm that outputs the correct value with probability p, has time complexity $t(n)$, and space complexity $s(n)$. We can obtain an additive-error estimation $\hat{p}$ such that $|p - \hat{p}| \leq \epsilon$, where $\epsilon \geq 2^{-O(s(n))}$. Moreover, this estimation can be computed in bounded-error randomized (resp., quantum) time $O(\epsilon^{-2}t(n))$ and space $O(s(n))$.*

Proof. Consider a m-time sequential repetition of the algorithm $\mathcal{A}$, and let X_i be a random variable indicating whether the i-th repetition succeeds, then we obtain a random variable $X = \frac{1}{m}\sum_{i=1}^{m} X_i$ such that $\mathbb{E}[X] = p$. Now let $\hat{X} = \frac{1}{m}\sum_{i=1}^{m} \hat{X}_i$ be the additive-error estimation, where $\hat{X}_i$ is the outcome of $\mathcal{A}$ in the i-th repetition. By the Chernoff-Hoeffding bound (e.g., Theorem 4.12 in [MU17]), it holds that

$$\Pr\left[|\hat{X} - p| \geq \epsilon\right] \leq 2\exp(-2m\epsilon^2).$$

By choosing $m = 2\epsilon^{-2}$, this choice of m ensures that this procedure based on $\mathcal{A}$ succeeds with probability at least 2/3.

Furthermore, the space complexity of our algorithm is $O(s(n))$ since we can simply reuse the workspace. Also, the time complexity is $m \cdot t(n) = O(\epsilon^{-2}t(n))$ as desired. □

Notably, when applying Lemma 2.13 to a quantum algorithm, we introduce intermediate measurements to retain space complexity through reusing working qubits. While space-efficient success probability estimation without intermediate measurements is possible,[2] we will use Lemma 2.13 for convenience, given that $\mathsf{BQL} = \mathsf{BQ_UL}$ [FR21].

[2]More specifically, Fefferman and Lin [FL18] noticed that one can achieve space-efficient success prob-

Next, we move on to sub-stochastic matrix powering via space-bounded random walks. In particular, a matrix B is said to be *sub-stochastic* if all its entries are non-negative and the sum of entries in each row (resp., column) is strictly less than 1. Furthermore, a matrix B is *row-stochastic* if all its entries are non-negative and the sum of entries in each row is equal to 1.

Lemma 2.14 (Sub-stochastic matrix powering in bounded space)**.** *Let B be an $l \times l$ upper-triangular sub-stochastic matrix, where each entry of B requires at most ℓ-bit precision. Then, there exists an explicit randomized algorithm that computes the matrix power $B^k[s,t]$ in $\log_2(l+1)$ space and $O(\ell k)$ time. Specifically, the algorithm accepts with probability $B^k[s,t]$.*

Proof. Our randomized algorithm uses the equivalence between space-bounded randomized computation and Markov chains, see [Sak96, Section 2.4] for a detailed introduction.

First, we construct a row-stochastic matrix $\hat{B}$ from B by adding an additional column and row. Let $\hat{B}[i,j]$ denote the entry at the i-th column and the j-th row of $\hat{B}$, i.e.,

$$\hat{B}[i,j] \coloneqq \begin{cases} B[i,j], & \text{if } 1 \le i,j \le l; \\ 1 - \sum_{s=j}^{l} B[s,j], & \text{if } i = l+1 \text{ and } 1 \le j \le l+1; \\ 0, & \text{if } 1 \le i \le l \text{ and } j = l+1. \end{cases}$$

Next, we view $\hat{B}$ as a transition matrix of a Markov chain since $\hat{B}$ is row-stochastic. We consequently have a random walk on the directed graph $G = (V, E)$ where $V = \{1, 2, \cdots, l\} \cup \{\perp\}$ and $(u,v) \in E$ iff $\hat{B}(u,v) > 0$. In particular, the probability that a k-step random walk starting at node s and ending at node t is exactly $\hat{B}^k[s,t] = B^k[s,t]$. This is because the walker who visits the dummy node $\perp$ will not reach other nodes.

Finally, as $\hat{B}$ is a $(l+1) \times (l+1)$ matrix, the matrix powering of $\hat{B}^k$ can be computed in $\log_2(l)$ space. In addition, the overall time complexity is $O(\ell k)$ since we simulate the dyadic rationals (with ℓ-bit precision) of a single transition exactly by ℓ coin flips. □

2.4.2 Quantum subroutines for time- and space-bounded settings

We now provide present quantum subroutines that apply to both time-bounded and space-bounded settings. Specifically, we set $s(n) = n$ when using these subroutines in time-bounded scenarios, while $s(n) = O(\log n)$ is often used for space-bounded settings.

The first subroutine is the SWAP test, initially proposed for pure states in [BCWdW01]. Later, in [KMY09], it was shown that the SWAP test can also be applied to mixed states.

Lemma 2.15 (SWAP test for mixed states, adapted from [KMY09, Proposition 9])**.** *Suppose ρ_0 and ρ_1 are two $s(n)$-qubit mixed quantum states. There is a $(2s+1)$-qubit quantum circuit that outputs 0 with probability $\frac{1+\mathrm{Tr}(\rho_0\rho_1)}{2}$, using 1 sample of each ρ_0 and ρ_1 and $O(n)$ one- and two-qubit quantum gates.*

The second subroutine is the quantum amplitude estimation:

ability estimation for quantum algorithms without intermediate measurements via quantum amplitude estimation [BHMT02].

Lemma 2.16 (Quantum amplitude estimation, [BHMT02, Theorem 12]). *Suppose that U is a unitary operator such that*

$$U|0\rangle|0\rangle = \sqrt{p}|0\rangle|\phi_0\rangle + \sqrt{1-p}|1\rangle|\phi_1\rangle,$$

where $|\phi_0\rangle$ and $|\phi_1\rangle$ are normalized pure quantum states and $p \in [0,1]$. Then, there is a quantum query algorithm using $O(M)$ queries to U that outputs $\tilde{p}$ such that

$$\Pr\left[|\tilde{p}-p| \leq \frac{2\pi\sqrt{p(1-p)}}{M} + \frac{\pi^2}{M^2}\right] \geq \frac{8}{\pi^2}.$$

Moreover, if U acts on $s(n)$ qubits, then the quantum query algorithm can be implemented by using $O(Ms)$ one- and two-qubit quantum gates.

Furthermore, a subroutine of quantum amplitude estimation (Lemma 2.16) can also be employed in the *one-sided* error setting. Specifically, this technique, also known as the exact amplitude amplification [BHMT02], is adapted from the Grover search when the number of solutions is one quarter [BBHT98]:

Lemma 2.17 (Exact amplitude amplification, adapted from [BHMT02, Equation 8]). *Suppose U is a unitary of interest such that $U|\bar{0}\rangle = \sin(\theta)|\psi_0\rangle + \cos(\theta)|\psi_1\rangle$, where $|\psi_0\rangle$ and $|\psi_1\rangle$ are normalized pure states and $\langle\psi_0|\psi_1\rangle = 0$. Let $G = -U(I-2|\bar{0}\rangle\langle\bar{0}|)U^\dagger(I-2|\psi_0\rangle\langle\psi_0|)$ be the Grover operator. Then, for every integer $j \geq 0$, it holds that*

$$G^jU|\bar{0}\rangle = \sin((2j+1)\theta)|\psi_0\rangle + \cos((2j+1)\theta)|\psi_1\rangle.$$

In particular, with a single application of G, we obtain $GU|\bar{0}\rangle = \sin(3\theta)|\psi_0\rangle + \cos(3\theta)|\psi_1\rangle$, signifying that $GU|\bar{0}\rangle = |\psi_0\rangle$ when $\sin(\theta) = 1/2$.

The third subroutine prepares a purified density matrix, originally stated in [LC19]:

Lemma 2.18 (Block-encoding of density matrix, [GSLW19, Lemma 25]). *Suppose ρ is an $s(n)$-qubit density matrix and U is an $(a+s)$-qubit unitary operator such that $U|0\rangle^{\otimes a}|0\rangle^{\otimes s} = |\rho\rangle$ and $\rho = \mathrm{Tr}_a(|\rho\rangle\langle\rho|)$. Then, we can construct an $O(a+s)$-qubit quantum circuit $\widetilde{U}$ that is a $(1, O(a+s), 0)$-block-encoding of ρ, using $O(1)$ queries to U and $O(a+s)$ one- and two-qubit quantum gates.*

The fourth subroutine is a specific version of one-bit precision phase estimation [Kit95], often referred to as the Hadamard test [AJL09], as stated in [GP22]:

Lemma 2.19 (Hadamard test for block-encodings, adapted from [GP22, Lemma 9]). *Suppose U is an $(a+s)$-qubit unitary operator that is a block-encoding of $s(n)$-qubit operator A. Then, we can implement an $O(a+s)$-qubit quantum circuit that, on input $s(n)$-qubit quantum state ρ, outputs 0 with probability $\frac{1+\mathrm{Re}(\mathrm{Tr}(A\rho))}{2}$, by using 1 query to controlled-U and $O(1)$ one- and two-qubit quantum gates.*

Moreover, if an $(s+a)$-qubit unitary operator $\mathcal{O}$ prepares a purification of ρ, then, by combining Lemma 2.16, we can estimate $\mathrm{Tr}(A\rho)$ to within additive error ϵ by using $O(1/\epsilon)$ queries to each of U and $\mathcal{O}$ and $O((s+a)/\epsilon)$ one- and two-qubit quantum gates.

2.4.3 Quantum algorithmic toolkit for time-bounded settings

We begin by presenting the quantum singular value transformation [GSLW19], starting with the introduction of the notion of block-encoding:

Definition 2.20 (Block-encoding). *A linear operator A on an $(n+a)$-qubit Hilbert space is said to be an (α, a, ϵ)-block-encoding of an n-qubit linear operator B, if*

$$\|\alpha(\langle 0|^{\otimes a} \otimes I_n)A(|0\rangle^{\otimes a} \otimes I_n) - B\| \leq \epsilon,$$

where I_n is the n-qubit identity operator and $\|\cdot\|$ is the operator norm.

Then, we state the quantum singular value transformation:

Lemma 2.21 (Quantum singular value transformation, [GSLW19, Theorem 31]). *Suppose that unitary operator U is an (α, a, ϵ)-block-encoding of Hermitian operator A, and $P \in \mathbb{R}[x]$ is a polynomial of degree d with $|P(x)| \leq \frac{1}{2}$ for $x \in [-1, 1]$. Then, we can implement a quantum circuit $\tilde{U}$ that is a $(1, a+2, 4d\sqrt{\epsilon/\alpha}+\delta)$-block-encoding of $P(A/\alpha)$, by using $O(d)$ queries to U and $O((a+1)d)$ one- and two-qubit quantum gates. Moreover, the classical description of $\tilde{U}$ can be computed in deterministic time* $\mathrm{poly}(d, \log(1/\delta))$.

Next, we provide the quantum samplizer, which helps us establish the sample complexity upper bound from the query complexity upper bound (i.e., a quantum query-to-sample simulation). We begin by introducing the notion of samplizer in [WZ24b]:

Definition 2.22 (Samplizer). *A samplizer $\mathsf{Samplize}_*\langle * \rangle$ is a mapping that converts quantum query algorithms (quantum circuit families with query access to quantum unitary oracles) to quantum sample algorithms (quantum channel families with sample access to quantum states) such that: For any $\delta > 0$, quantum query algorithm $\mathcal{A}^U$, and quantum state ρ, there exists a unitary operator U_ρ that is a $(2, a, 0)$-block-encoding of ρ for some $a > 0$, satisfying*

$$\left\|\mathsf{Samplize}_\delta\langle \mathcal{A}^U \rangle[\rho] - \mathcal{A}^{U_\rho}\right\|_\diamond \leq \delta,$$

where $\mathcal{E}[\rho](\cdot)$ is a quantum channel $\mathcal{E}$ with sample access to ρ.

We then include an efficient implementation of the samplizer in [WZ24b], which is based on quantum principal component analysis [LMR14, KLL+17] and generalizes [GP22, Corollary 21] and [WZ23, Theorem 1.1].

Lemma 2.23 (Optimal samplizer, [WZ24b, Theorem 4]). *There is a samplizer $\mathsf{Samplize}_*\langle * \rangle$ such that for $\delta > 0$ and quantum query algorithm $\mathcal{A}^U$ with query complexity Q, the implementation of $\mathsf{Samplize}_\delta\langle \mathcal{A}^U \rangle[\rho]$ uses $\widetilde{O}(Q^2/\delta)$ samples of ρ.*

Chapter 3

Closeness testing of distributions and states

This chapter will begin with a review of commonly used classical closeness measures in Section 3.1, followed by their quantum counterparts in Section 3.2. Next, Section 3.3 discusses useful hardness and containment results, including quantitative bounds, on time-bounded quantum state testing. Finally, prior works closely related to space-bounded distribution testing are reviewed in Section 3.4.

For convenience, we adopt the convention $D_1 \leq D_2$ to denote an inequality between two distances or divergences, whether classical or quantum. In particular, this notation – commonly reflected in *the titles of technical lemmas* (e.g., Lemma 3.10) – indicates that D_1 is bounded above by a function f of D_2, i.e., $D_1 \leq f(D_2)$, or that D_2 is bounded below by a function g of D_1, i.e., $g(D_1) \leq D_2$.

3.1 Closeness measures for classical probability distributions

We now review several commonly used classical distances and divergences.

Total variation distance and Hellinger distance. We begin by defining the total variation distance as the following:

Definition 3.1 (Total variation distance)**.** *Let p_0 and p_1 be two probability distributions over $[N]$. The total variation distance between two p_0 and p_1 is defined by*

$$\mathrm{TV}(p_0, p_1) \coloneqq \frac{1}{2}\|p_0 - p_1\|_1 = \frac{1}{2}\sum_{x\in[N]} |p_0(x) - p_1(x)|.$$

Next, we define the (squared) Hellinger distance and the inner product $\langle P|Q\rangle$ between normalized non-negative vectors, where the latter is commonly referred to as the *Hellinger affinity* or *Bhattacharyya coefficient*:

Definition 3.2 (Hellinger distance)**.** *Let p_0 and p_1 be two probability distributions over $[N]$. The (square) Hellinger distance between two distributions p_0 and p_1 is defined by*

$$\mathrm{H}^2(p_0, p_1) \coloneqq \frac{1}{2}\sum_{x\in[N]} (\sqrt{p_0(x)} - \sqrt{p_1(x)})^2 = 1 - \langle P_0|P_1\rangle.$$

Here, $|P_0\rangle \coloneqq \sum_x \sqrt{p_0(x)}|x\rangle$ *and* $|P_1\rangle \coloneqq \sum_x \sqrt{p_1(x)}|x\rangle$.

The inequalities between the total variation distance and the (squared) Hellinger distance are established in [Kai67] as follows:

$$\mathrm{H}^2(p_0, p_1) \leq \mathrm{TV}(p_0, p_1) \leq \sqrt{2}\mathrm{H}(p_0, p_1).$$

Triangular discrimination. We then define the triangular discrimination:

Definition 3.3 (Triangular discrimination)**.** *Let* p_0 *and* p_1 *be two probability distributions over* $[N]$*. The triangular discrimination (also known as Le Cam divergence) between* p_0 *and* p_1 *is defined by*

$$\mathrm{TD}(p_0, p_1) \coloneqq \frac{1}{2} \sum_{x \in \mathcal{X}} \frac{(p_0(x) - p_1(x))^2}{p_0(x) + p_1(x)}.$$

The triangular discrimination is a symmetrized variant of the χ^2 divergence, given by

$$\forall b \in \{0, 1\}, \quad \mathrm{TD}(p_0, p_1) = \chi^2\left(p_b \middle\| \frac{p_0 + p_1}{2}\right).$$

Inequalities relating the triangular discrimination to aforementioned closeness measures have been established in [Top00] and [LC86, Page 48], respectively:

$$\mathrm{TV}^2(p_0, p_1) \leq \mathrm{TD}(p_0, p_1) \leq \mathrm{TV}(p_0, p_1),$$
$$\mathrm{H}^2(p_0, p_1) \leq \mathrm{TD}(p_0, p_1) \leq 2\mathrm{H}^2(p_0, p_1).$$

Jensen-Shannon divergence. We start by defining the Shannon entropy:

Definition 3.4 (Shannon entropy)**.** *Let* p *be a probability distribution over* $[N]$*. The Shannon entropy of* p *is defined by*

$$\mathrm{H}(p) = -\sum_{x \in [N]} p(x) \ln(p(x)).$$

For $N = 2$*, the notation is slightly abused to denote the (Shannon) binary entropy as*

$$\mathrm{H}(p_0) = \mathrm{H}(1 - p_0) = \mathrm{H}(p).$$

For convenience, the Shannon entropy and the binary Shannon entropy, both expressed using the base-2 logarithm, are denoted by $\mathrm{H}_{\mathrm{bit}}(p)$ *and* $\mathrm{H}_{\mathrm{bit}}(p_0)$*, respectively.*

Next, we proceed by defining the Jensen-Shannon divergence:

Definition 3.5 (Jensen-Shannon divergence)**.** *Let* p_0 *and* p_1 *be two probability distributions over* $[N]$*. The Jensen-Shannon divergence between* p_0 *and* p_1 *is defined by*

$$\mathrm{JS}(p_0, p_1) \coloneqq \mathrm{H}\left(\frac{p_0 + p_1}{2}\right) - \frac{1}{2}(\mathrm{H}(p_0) + \mathrm{H}(p_1)).$$

For convenience, the Jensen-Shannon divergence expressed in terms of the base-2 logarithm is denoted by $\mathrm{JS}_{\mathrm{bit}}(p_0, p_1)$*, and is given by* $\mathrm{JS}(p_0, p_1)/\ln 2$.

The Jensen-Shannon divergence, a symmetrized variant of the Kullback–Leibler divergence (also known as relative entropy), can be expressed as:

$$\mathrm{JS}(p_0, p_1) = \frac{1}{2}\mathrm{KL}\left(p_0 \middle\| \frac{p_0 + p_1}{2}\right) + \frac{1}{2}\mathrm{KL}\left(p_1 \middle\| \frac{p_0 + p_1}{2}\right).$$

Furthermore, the Jensen-Shannon divergence and the total variation distance are related through the following inequalities:

Lemma 3.6 (JS vs. TV, adapted from [Top00, Theorem 5] and [FvdG99])**.** *Let p_0 and p_1 be two probability distributions over $[N]$, the following inequalities hold*

$$\sum_{v=1}^{\infty} \frac{\mathrm{TV}(p_0,p_1)^{2v}}{2v(2v-1)} = \ln(2) - \mathrm{H}\left(\frac{1-\mathrm{TV}(p_0,p_1)}{2}\right) \le \mathrm{JS}(p_0,p_1) \le \ln(2)\cdot \mathrm{TV}(p_0,p_1).$$

Jansen-Tsallis divergence. We begin by defining the Tsallis entropy:

Definition 3.7 (q-Tsallis entropy)**.** *Let p be a probability distribution over $[N]$. The q-Tsallis entropy of p is defined by*[1]

$$\mathrm{H}_q(p) \coloneqq \frac{1-\sum_{x\in[N]} p(x)^q}{q-1} = -\sum_{x\in[N]} p(x)^q \ln_q(p(x)).$$

The Shannon entropy is the limiting case of the q-Tsallis entropy as $q \to 1$, specifically

$$\mathrm{H}_1(p) \coloneqq \lim_{q\to 1} \mathrm{H}_q(p) = \mathrm{H}(p).$$

For $N = 2$, the notation is slightly abused to denote the q-Tsallis binary entropy as

$$\mathrm{H}_q(p_0) = \mathrm{H}_q(1-p_0) = \mathrm{H}_q(p).$$

It is noteworthy that the properties in Lemma 3.8 were also provided in [Tsa88] without proofs. In addition, by considering the eigenvalues of any quantum state, Lemma 3.8 straightforwardly extends to quantum q-Tsallis entropy (see Definition 3.27).

Lemma 3.8 (Basic properties of Tsallis entropy, partially adapted from [Dar70])**.** *Let p and p' be two probability distributions over $[N]$ with $N \ge 2$, and let ν be the uniform distribution over $[N]$. For the Tsallis entropy $\mathrm{H}_q(p)$ with $q > 0$, the following holds:*

- **Concavity**: *For any $\lambda \in [0,1]$, $\mathrm{H}_q((1-\lambda)p + \lambda p') \ge (1-\lambda)\mathrm{H}_q(p) + \lambda \mathrm{H}_q(p')$. Equivalently, $F(q;x) \coloneqq \frac{x-x^q}{q-1}$ is concave in $x \in [0,1]$ for any fixed $q > 0$, and $\mathrm{H}_q(p) = \sum_{i\in[N]} F(q;p(i))$.*
- **Extremes**: $0 \le \mathrm{H}_q(p) \le \mathrm{H}_q(\nu) = \frac{1-n^{1-q}}{q-1}$. *Specifically, $\mathrm{H}_q(p) = \mathrm{H}_q(\nu)$ occurs when $p = \nu$, and $\mathrm{H}_q(p) = 0$ occurs when $p(i) = \begin{cases} 1, & i = k \\ 0, & i \ne 1 \end{cases}$ for any $k \in [N]$.*
- **Monotonicity**: *For any q and q' satisfying $0 < q \le q'$, $\mathrm{H}_q(p) \ge \mathrm{H}_{q'}(p)$.*

Proof. For the first item, by inspecting the proof of [Dar70, Theorem 6], we know that $\frac{x-x^q}{1-2^{1-q}} \cdot \frac{1-2^{1-q}}{q-1} = F(q;x)$ is concave in $x \in [0,1]$ for any fixed $q \ne 1$. It is easy to verify that $\mathrm{H}_q(p) = \sum_{i\in[N]} F(q;p(i))$, we have that $\mathrm{H}_q(p)$ is concave.

For the second item, note that $\frac{q-1}{1-2^{1-q}} \ge 0$ for $q \ne 1$ and $\lim_{q\to 1} \frac{q-1}{1-2^{1-q}} = \frac{1}{\ln 2}$. Hence, by [Dar70, Theorem 6], we deduce $0 \le \mathrm{H}_q(p) \le \mathrm{H}_q(\nu)$. Moreover, because $F(q;x)$ is non-negative and $F(q;x) = 0$ occurs when $x = 1$, we conclude that $\mathrm{H}_q(p) = 0$ occurs when p satisfies the desired condition.

[1] The definition of the q-logarithm function $\ln_q(x)$ is provided in the paragraph *Logarithm function and its generalization* in Chapter 2.

For the third item, since $\lim_{q\to 1} \mathrm{H}_q(x) = \mathrm{H}(x)$, it is enough to show that $\frac{\partial}{\partial q}\mathrm{H}_q(x) \le 0$ for any $q \neq 1$ and $x \in [0,1]$. Given that $\mathrm{H}_q(p) = \sum_{i\in[n]} F(q; p(i))$, it remains to prove that $\frac{\partial}{\partial q}F(q;x) \le 0$, specifically:

$$\frac{\partial}{\partial q}F(q;x) = -\frac{x - x^q}{(q-1)^2} - \frac{x^q \log(x)}{q-1} \le 0 \Leftrightarrow G(q;x) \coloneqq x^q - x - (q-1)x^q \log(x) \le 0. \quad (3.1)$$

A direct calculation implies that $\frac{\partial}{\partial q}G(q;x) = -(q-1)x^q \ln^2(x)$ for any $x \in [0,1]$. This inequality shows that for any fixed $x \in [0,1]$, $G(q;x)$ is monotonically increasing for $0 < q \le 1$ and monotonically decreasing for $q > 1$. Hence, by noticing

$$\forall x \in [0,1], \quad \max_{q\ge 0} G(q;x) \le G(1;x) = 0,$$

we establish Equation (3.1) and the monotonicity. □

Next, a generalization of the Jensen-Shannon divergence, based on the q-Tsallis entropy, is defined as the following:

Definition 3.9 (q-Jensen-(Shannon-)Tsallis divergence, adapted from [BR82])**.** *Let p_0 and p_1 be two probability distributions over $[N]$. The q-Jensen-(Shannon-)Tsallis divergence between p_0 and p_1 is defined as*

$$\mathrm{JT}_q(p_0,p_1) \coloneqq \begin{cases} \mathrm{H}_q\left(\frac{p_0+p_1}{2}\right) - \frac{1}{2}\left(\mathrm{H}_q(p_0) + \mathrm{H}_q(p_1)\right), & q \neq 1 \\ \mathrm{H}\left(\frac{p_0+p_1}{2}\right) - \frac{1}{2}\left(\mathrm{H}(p_0) + \mathrm{H}(p_1)\right), & q = 1 \end{cases}.$$

Specifically, the Jensen-Shannon divergence $\mathrm{JS}(p_0,p_1) = \mathrm{JT}_1(p_0,p_1)$.

We then provide a lower bound of the Jensen-Tsallis divergence in terms of the total variation distance, generalizing the lower bound in Lemma 3.6 for the case $q = 1$:

Lemma 3.10 ($\mathrm{TV} \le \mathrm{JT}_q$, adapted from [BH09, Theorem 9])**.** *Let p_0 and p_1 be two probability distributions over $[N]$. For any $1 \le q \le 2$, it holds that:*[2]

$$\mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q\left(\frac{1}{2} - \frac{\mathrm{TV}(p_0,p_1)}{2}\right) \le \mathrm{JT}_q(p_0,p_1).$$

It is important to note, the joint convexity of JT_q [BR82, Corollary 1] plays a key role in proving Lemma 3.10. And additionally, for $N \ge 3$, the joint convexity of JT_q holds if and only if $q \in [1,2]$, as stated in [BR82, Corollary 2].

3.2 Closeness measures for quantum states

We now review previous results on quantum analogs of the aforementioned classical closeness (or, distance-like) measures. Classical distances and divergences often have quantum counterparts, sometimes even with *multiple* formulations. On one side, quantum measures typically reduce to their classical versions when the quantum states $\rho_0 = \mathrm{diag}(p_0)$ and $\rho_1 = \mathrm{diag}(p_1)$ are diagonal. On the other side, for any classical f-divergence d_f, a quantum analog can be defined in two main ways:

[2] It is evident that $\mathrm{H}_q\left(\frac{1-x}{2}\right) = \mathrm{H}_q\left(\frac{1+x}{2}\right)$ for any $x \in [0,1]$. Moreover, the proof of the lower bound in [BH09, Theorem 9] uses the notation $V(p_0,p_1) \coloneqq \sum_{i=1}^n |p_0(i) - p_1(i)| = \|p_0 - p_1\|_1 = 2\mathrm{TV}(p_0,p_1)$ defined in [Top00], where p_0 and p_1 are probability distributions over $[N]$.

- By replacing arithmetic operations in the classical divergence with their matrix-theoretic counterparts, which, due to the non-commutative nature of matrices, allows for several options and results in (at least) one quantum f divergence D_f;
- By considering the probability distributions induced by applying the same POVM $\mathcal{M}$ to both states, which leads to the *measured* quantum f-divergence $\mathrm{D}_f^{\mathrm{meas}}$.

For a comprehensive overview of other quantum analogs of f-divergence and their relationships, please refer to [Hia21].

More precisely, let $\mathrm{d}_f(\cdot,\cdot)$ be a classical f-divergence. For two N-dimensional quantum (mixed) states ρ_0 and ρ_1, the measured quantum f-divergence $\mathrm{D}_f^{\mathrm{meas}}(\cdot,\cdot)$ is defined based on the "farthest" probability distributions induced by a POVM $\mathcal{M}$:

$$\begin{aligned} \mathrm{D}_f^{\mathrm{meas}}(\rho_0,\rho_1) &\coloneqq \sup_{\mathrm{POVM}\ \mathcal{M}} \left\{ \mathrm{d}_f\left(p_0^{(\mathcal{M})}, p_1^{(\mathcal{M})}\right)\right\}, \\ \text{where } p_b^{(\mathcal{M})} &\coloneqq (\mathrm{Tr}(\rho_b M_1), \cdots, \mathrm{Tr}(\rho_b M_N)) \ \text{ for } b \in \{0,1\}. \end{aligned} \tag{3.2}$$

Quantum analogs of total variation distance and Hellinger distance. We start by defining the trace distance, which is a distance metric (e.g., [Wil13, Lemma 9.1.8]):

Definition 3.11 (Trace distance)**.** *Let ρ_0 and ρ_1 be two quantum states. The trace distance between ρ_0 and ρ_1 is defined by*

$$\mathrm{T}(\rho_0,\rho_1) \coloneqq \frac{1}{2}\mathrm{Tr}(|\rho_0-\rho_1|) = \frac{1}{2}\mathrm{Tr}\Big(\big((\rho_0-\rho_1)^\dagger(\rho_0-\rho_1)\big)^{1/2}\Big).$$

The trace distance satisfies the following basic properties:

- The trace distance is 1, the maximum value, if ρ_0 and ρ_1 have orthogonal supports.
- As explained in, e.g., [NC10, Theorem 9.1], the trace distance corresponds to a measured version of the total variation distance in terms of Equation (3.2).
- For pure states $|\psi_0\rangle$ and $|\psi_1\rangle$, it holds that $\mathrm{T}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) = \sqrt{1-|\langle\psi_0|\psi_1\rangle|^2}$, as indicated in [Wil13, Equation (9.134)].

We then present four additional properties of the trace distance.

Theorem 3.12 (Holevo-Helstrom bound, [Hol73b, Hel69])**.** *Given a quantum (mixed) state ρ, either ρ_0 or ρ_1, that is chosen uniformly at random, the maximum success probability to discriminate between ρ_0 and ρ_1 by performing a POVM is given by $\frac{1}{2}+\frac{1}{2}\mathrm{T}(\rho_0,\rho_1)$.*

Lemma 3.13 (Trace distance on tensor-product states, adapted from Exercise 9.1.2 and Corollary 9.1.10 in [Wil13])**.** *For any quantum states $\rho_1\otimes\cdots\otimes\rho_k$ and $\rho_1'\otimes\cdots\otimes\rho_k'$, where ρ_i and ρ_i' use the same number of qubits for all $i\in[k]$, it holds that*

(1) $\forall i\in[k],\ \mathrm{T}(\rho_i,\rho_i') \le \mathrm{T}(\rho_1\otimes\cdots\otimes\rho_k, \rho_1'\otimes\cdots\otimes\rho_k')$.

(2) $\mathrm{T}(\rho_1\otimes\cdots\otimes\rho_k, \rho_1'\otimes\cdots\otimes\rho_k') \le \sum_{i\in[k]}\mathrm{T}(\rho_i,\rho_i')$.

Lemma 3.14 (Data-processing inequality of T, adapted from [NC10, Theorem 9.2])**.** *Let ρ_0 and ρ_1 be quantum states. For any quantum channel $\mathcal{E}$, it holds that*

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

Lemma 3.15 (Unitary invariance of T, adapted from [NC10, Equation (9.21)])**.** *Let ρ_0 and ρ_1 be quantum states. For any unitary transformation U, it holds that*

$$\mathrm{T}\big(U\rho_0 U^\dagger, U\rho_1 U^\dagger\big) = \mathrm{T}(\rho_0, \rho_1).$$

Next, we turn to the quantum analog of the Hellinger distance. Although the (squared) Hellinger distance is closely related to the inner product, several quantum analogs exist due to the non-commuting nature of matrices. We begin by defining the (squared) Bures distance, which is based on the (Uhlmann) fidelity:

Definition 3.16 (Squared Bures distance and Uhlmann fidelity)**.** *Let ρ_0 and ρ_1 be two quantum states. The squared Bures distance $\mathrm{B}^2(\cdot,\cdot)$ and the Uhlmann fidelity $\mathrm{F}(\cdot,\cdot)$ between ρ_0 and ρ_1 are defined by*

$$\mathrm{B}^2(\rho_0, \rho_1) \coloneqq 2(1 - \mathrm{F}(\rho_0, \rho_1)) \text{ and } \mathrm{F}(\rho_0, \rho_1) \coloneqq \mathrm{Tr}|\sqrt{\rho_0}\sqrt{\rho_1}|.$$

The Bures distance is the first quantum analog of the Hellinger distance, as it precisely correspond to the *measured* Hellinger distance [FC94]. We now provide the inequalities between the trace distance and the Bures distance (or the Uhlmann fidelity):

Lemma 3.17 (Trace distance vs. Bures distance, adapted from [FvdG99])**.** *Let ρ_0 and ρ_1 be two quantum states. The following inequalities hold*:

$$\frac{1}{2}\mathrm{B}^2(\rho_0, \rho_1) \le \mathrm{T}(\rho_0, \rho_1) \le \mathrm{B}(\rho_0, \rho_1) \text{ and } 1 - \mathrm{F}(\rho_0, \rho_1) \le \mathrm{T}(\rho_0, \rho_1) \le \sqrt{1 - \mathrm{F}^2(\rho_0, \rho_1)}.$$

The (Uhlmann) fidelity attains its maximum value of 1 when ρ_0 and ρ_1 are equal. For a pure state $|\psi\rangle\langle\psi|$ and a mixed state ρ, it holds that $\mathrm{F}^2(|\psi\rangle\langle\psi|, \rho) = \mathrm{Tr}(|\psi\rangle\langle\psi|\rho)$.

In addition, since the matrices $(ABA)^{1/2}$ and $A^{1/2}B^{1/2}A^{1/2}$ are not equal in general, the Uhlmann fidelity differs from the quantum Hellinger affinity

$$\mathrm{Q}_{1/2}(\rho_0, \rho_1) \coloneqq \mathrm{Tr}(\sqrt{\rho_0}\sqrt{\rho_1}).$$

This difference gives rise to the second quantum analog of the Hellinger distance:

Definition 3.18 (Quantum squared Hellinger distance)**.** *Let ρ_0 and ρ_1 be two quantum states. The quantum squared Hellinger distance between ρ_0 and ρ_1 is defined by*

$$\mathrm{QH}^2(\rho_0, \rho_1) \coloneqq \frac{1}{2}\mathrm{Tr}(\sqrt{\rho_0} - \sqrt{\rho_1})^2 = 1 - \mathrm{Q}_{1/2}(\rho_0, \rho_1).$$

It is noteworthy that $\mathrm{F}(\rho_0, \rho_1) \ge \mathrm{Q}_{1/2}(\rho_0, \rho_1)$. For a more detailed overview of different variants of the fidelity, we recommend two comprehensive reviews [CS20, BGJ19].

(Squared) Hilbert-Schmidt distance. We now define the (squared) Hilbert-Schmidt distance, which serves as a quantum analog of the (squared) Euclidean distance:

Definition 3.19 (Squared Hilbert-Schmidt distance)**.** *Let ρ_0 and ρ_1 be two quantum states. The (squared) Hilbert-Schmidt distance between ρ_0 and ρ_1 is defined by*

$$\mathrm{HS}^2(\rho_0, \rho_1) \coloneqq \frac{1}{2}\mathrm{Tr}(\rho_0 - \rho_1)^2 = \frac{1}{2}(\mathrm{Tr}(\rho_0^2) + \mathrm{Tr}(\rho_1^2)) - \mathrm{Tr}(\rho_0\rho_1).$$

Since a quantum state ρ is a pure state if and only if $\mathrm{Tr}(\rho^2) = 1$, the following equality holds for two pure states $|\psi_0\rangle\langle\psi_0|$ and $|\psi_1\rangle\langle\psi_1|$:

$$\mathrm{Tr}(|\psi_0\rangle\langle\psi_0||\psi_1\rangle\langle\psi_1|) = 1 - \mathrm{HS}^2(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|).$$

We then relate the Hilbert-Schmidt distance to the trace distance as follows:

Lemma 3.20 (Trace distance vs. Hilbert-Schmidt distance, adapted from [CCC19, Equation 6])**.** *Let ρ_0 and ρ_1 be two quantum states. The following inequalities hold*:

$$\mathrm{HS}(\rho_0, \rho_1) \leq \mathrm{T}(\rho_0, \rho_1) \leq \sqrt{\frac{2\mathrm{rank}(\rho_0)\mathrm{rank}(\rho_1)}{\mathrm{rank}(\rho_0) + \mathrm{rank}(\rho_1)}}\mathrm{HS}(\rho_0, \rho_1).$$

Notably, Lemma 3.20 serves as a special instance of the rank-dependent bounds for the Schatten p-norms, as described in [AS17, Equation (1.31)].

Quantum analogs of Jensen-Shannon Divergence. We begin by defining the von Neumann entropy, a quantum analog of the Shannon entropy:

Definition 3.21 (von Neumann entropy)**.** *Let ρ be a quantum (mixed) state. The von Neumann entropy of ρ is defined by*

$$\mathrm{S}(\rho) = -\mathrm{Tr}(\rho \ln(\rho)).$$

For convenience, the von Neumann entropy is denoted by $\mathrm{S}_{\mathrm{bit}}(\rho)$ when the base-2 matrix logarithm is used, and is given by $\mathrm{S}(\rho)/\ln 2$.

For classical-quantum states, the following decomposition theorem holds:

Lemma 3.22 (Joint entropy theorem, adapted from Theorem 11.8(5) in [NC10])**.** *Suppose p_i are probabilities corresponding to a distribution D, $|i\rangle$ are orthogonal states of a system A, and $\{\rho_i\}_i$ is any set of density operators for another system B. Then*

$$\mathrm{S}\left(\sum_i p_i |i\rangle\langle i| \otimes \rho_i\right) = \mathrm{H}(D) + \sum_i p_i \mathrm{S}(\rho_i).$$

We now consider quantum analogs of the Jensen-Shannon divergence, which trace back to the renown Holevo bound [Hol73a]. The definition of the quantum Jensen-Shannon divergence, as presented in [MLP05], is stated below:

Definition 3.23 (Quantum Jensen-Shannon divergence, adapted from [MLP05])**.** *Let ρ_0 and ρ_1 be two quantum (mixed) states. The quantum Jensen-Shannon divergence between ρ_0 and ρ_1 is defined by*

$$\mathrm{QJS}(\rho_0, \rho_1) \coloneqq \mathrm{S}\left(\frac{\rho_0 + \rho_1}{2}\right) - \frac{1}{2}(\mathrm{S}(\rho_0) + \mathrm{S}(\rho_1)).$$

For convenience, the quantum Jensen-Shannon divergence is denoted by $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1)$ when the base-2 matrix logarithm is used, and is given by $\mathrm{QJS}(\rho_0, \rho_1)/\ln 2$.

The quantum Jensen-Shannon divergence satisfies several basic properties:

- This quantity can be interpreted as a symmetrized version of the quantum relative entropy, defined as $\mathrm{D}(\rho_0\|\rho_1) \coloneqq \mathrm{Tr}(\rho_0(\ln(\rho_0) - \ln(\rho_1)))$. Specifically:

$$\mathrm{QJS}(\rho_0, \rho_1) = \frac{1}{2}\left(\mathrm{D}\left(\rho_0 \middle\| \frac{\rho_0 + \rho_1}{2}\right) + \mathrm{D}\left(\rho_1 \middle\| \frac{\rho_0 + \rho_1}{2}\right)\right). \tag{3.3}$$

- Unlike the quantum relative entropy. which is unbounded, the (base-2) quantum Jensen-Shannon divergence $\mathrm{QJS}_{\mathrm{bit}}(\cdot,\cdot)$ is bounded above by 1. The maximum is attached if and only if ρ_0 and ρ_1 have support on orthogonal subspaces.[3]
- The square root of the quantum Jensen-Shannon divergence is a distance metric, as proven in [Vir21, Sra21], and thus satisfies the triangle inequality.

Another quantum analog of the Jensen-Shannon divergence is the *measured* quantum Jensen-Shannon divergence, denoted by $\mathrm{QJS}^{\mathrm{meas}}(\rho_0,\rho_1)$. This quantity, also referred to as the *quantum Shannon distinguishability*, is defined in terms of Equation (3.2). In contrast to $\mathrm{QJS}(\cdot,\cdot)$, the quantum analog $\mathrm{QJS}^{\mathrm{meas}}(\cdot,\cdot)$ lacks an explicit formula, as it coincides with a solution of some transcendental equation [FC94]. For convenience, when the base-2 matrix logarithm is used, the measured quantum Jensen-Shannon divergence is denoted by $\mathrm{QJS}^{\mathrm{meas}}_{\mathrm{bit}}(\rho_0,\rho_1)$ and is given by $\mathrm{QJS}^{\mathrm{meas}}_{\mathrm{bit}}(\rho_0,\rho_1) = \mathrm{QJS}^{\mathrm{meas}}(\rho_0,\rho_1)/\ln 2$.

Interestingly, using the notation in [NC10, Theorem 12.1], the quantum Jensen-Shannon divergence coincides with the Holevo χ quantity on size-2 ensembles with a uniform distribution. Consequently, the Holevo bound [Hol73a] implies the following:

Lemma 3.24 ($\mathrm{QJS}^{\mathrm{meas}} \leq \mathrm{QJS}$)**.** *For any quantum states ρ_0 and ρ_1, it holds that*

$$\mathrm{QJS}^{\mathrm{meas}}(\rho_0,\rho_1) \leq \mathrm{QJS}(\rho_0,\rho_1).$$

Proof. We begin with an equivalent characterization of the Jensen-Shannon divergence, building upon its basic property (e.g., [BDRV19, Proposition 4.1]):

Proposition 3.24.1 (Mutual information characterization of Jensen-Shannon divergence)**.** *For any distributions p_0 and p_1, let T be a binary indicator variable that chooses the value of x according to p_0 if $T = i$ where $i \in \{0,1\}$, and let X be a random variable associated with a uniform mixture distribution between p_0 and p_1. Then, it holds that*

$$\mathrm{JS}(p_0,p_1) = I(T;X) = \mathrm{H}(T) - \mathrm{H}(T|X) = 1 - \mathrm{H}(T|X).$$

We then observe that $\mathrm{QJS}(\rho_0,\rho_1)$ corresponds exactly to the Holevo χ quantity [NC10, Section 12.1.1] for the ensemble $\{1/2,\rho_0;1/2,\rho_1\}$, while $\mathrm{QJS}^{\mathrm{meas}}(\rho_0,\rho_1)$ is equivalent to the accessible information of the same ensemble. This equivalence allows the proof to follow directly from the Holevo bound. □

Next, we provide the inequalities between the quantum Jensen-Shannon divergence and the trace distance in Lemma 3.25 and Lemma 3.26.

Lemma 3.25 ($\mathrm{T} \leq \mathrm{QJS}$, adapted from [Hol73a, FvdG99])**.** *Let ρ_0 and ρ_1 be two quantum states. Then, the following inequalities hold*:

$$\mathrm{QJS}_{\mathrm{bit}}(\rho_0,\rho_1) \geq \mathrm{QJS}^{\mathrm{meas}}_{\mathrm{bit}}(\rho_0,\rho_1) \geq 1 - \mathrm{H}_{\mathrm{bit}}\left(\frac{1+\mathrm{T}(\rho_0,\rho_1)}{2}\right) = \sum_{v=1}^{\infty} \frac{\mathrm{T}(\rho_0,\rho_1)^{2v}}{\ln(2)\cdot 2v(2v-1)}.$$

Proof. We first fix some POVM measurement $\mathcal{E} = \{E_x\}_{x\in\mathcal{U}}$, where $\mathcal{U} = \mathrm{supp}\,(\rho_0) \cup \mathrm{supp}\,(\rho_1)$. And let $p_z^{(\mathcal{E})}$ be the induced distribution with respect to the POVM $\mathcal{E}$ of ρ_z for

[3] This follows from the properties of von Neumann entropy, such as [NC10, Theorem 11.8], which imply $\mathrm{QJS}_{\mathrm{bit}}(\rho_0,\rho_1) \leq \mathrm{H}_{\mathrm{bit}}(1/2) = 1$.

$z \in \{0,1\}$. By utilizing the left-hand side inequality in Lemma 3.6, we have

$$\mathrm{QJS}^{\mathrm{meas}}_{\mathcal{E}^*}(\rho_0,\rho_1) \geq \mathrm{QJS}^{\mathrm{meas}}_{\mathcal{E}}(\rho_0,\rho_1) = \mathrm{JS}(p_0^{(\mathcal{E})}, p_1^{(\mathcal{E})}) \geq \sum_{v=1}^{\infty} \frac{\mathrm{SD}\left(p_0^{(\mathcal{E})}, p_1^{(\mathcal{E})}\right)^{2v}}{2v(2v-1)}. \tag{3.4}$$

Here, $\mathcal{E}^*$ is an optimal measurement of $\mathrm{QJS}^{\mathrm{meas}}(\rho_0,\rho_1)$. Let $g(x) \coloneqq \sum_{v=1}^{\infty} \frac{x^{2v}}{2v(2v-1)}$, then $g(x)$ is monotonically increasing on $0 \leq x \leq 1$. Since Equation (3.4) holds for arbitrary POVM $\mathcal{E}$, as well as the trace distance is the measured version of the statistical distance, we complete the proof by choosing the one that maximizes $\mathrm{T}(\rho_0,\rho_1)$. □

Lemma 3.26 (QJS $\leq$ T, adapted from [BH09, Theorem 14])**.** *Let ρ_0 and ρ_1 be two quantum states. Then, the following inequalities hold*:

$$\mathrm{QJS}(\rho_0,\rho_1) \leq \ln 2 \cdot \mathrm{T}(\rho_0,\rho_1).$$

It is noteworthy that the proof of Lemma 3.26 primarily adapts the argument used to establish a similar result for classical distances (e.g., [Vad99, Claim 4.4.2]).

Proof of Lemma 3.26. We begin with the construction in [BH09, Theorem 14]. Consider a single qutrit register B with basis vectors $|0\rangle, |1\rangle, |2\rangle$. Define $\tilde{\rho}_0$ and $\tilde{\rho}_1$ on $\mathcal{H} \otimes \mathcal{B}$ as below, where $\mathcal{B} = \mathbb{C}^3$ is the Hilbert space corresponding to the register B:

$$\begin{aligned}
\tilde{\rho}_0 &\coloneqq \frac{\rho_0+\rho_1-|\rho_0-\rho_1|}{2} \otimes |2\rangle\langle 2| + \frac{\rho_0-\rho_1+|\rho_0-\rho_1|}{2} \otimes |0\rangle\langle 0| \coloneqq \sigma_2 \otimes |2\rangle\langle 2| + \sigma_0 \otimes |0\rangle\langle 0|, \\
\tilde{\rho}_1 &\coloneqq \frac{\rho_0+\rho_1-|\rho_0-\rho_1|}{2} \otimes |2\rangle\langle 2| + \frac{\rho_1-\rho_0+|\rho_0-\rho_1|}{2} \otimes |1\rangle\langle 1| \coloneqq \sigma_2 \otimes |2\rangle\langle 2| + \sigma_1 \otimes |1\rangle\langle 1|.
\end{aligned}$$

Here, σ_0 corresponds to the regime that ρ_0 is "larger than" ρ_1 (where ρ_0 and ρ_1 are "distinguishable") and so does σ_1, whereas σ_2 corresponds to the regime that ρ_0 is "indistinguishable" from ρ_1. One can see this construction generalizes the proof of the classical counterparts, such as [Vad99, Claim 4.4.2], to quantum distances.

Then it is left to show $\mathrm{QJS}(\rho_0,\rho_1) \leq \mathrm{QJS}(\tilde{\rho}_0,\tilde{\rho}_1) = \mathrm{T}(\rho_0,\rho_1)$. By the data-processing inequality of the quantum relative entropy (e.g., [Pet07, Theorem 3.9]), we obtain

$$\begin{aligned}
\mathrm{QJS}(\rho_0,\rho_1) &= \mathrm{QJS}(\mathrm{Tr}_B(\tilde{\rho}_0), \mathrm{Tr}_B(\tilde{\rho}_1)) \\
&\leq \mathrm{QJS}(\tilde{\rho}_0,\tilde{\rho}_1) \\
&= -\mathrm{Tr}\left(\frac{\tilde{\rho}_0+\tilde{\rho}_1}{2} \ln \frac{\tilde{\rho}_0+\tilde{\rho}_1}{2}\right) + \frac{1}{2}\left(\mathrm{Tr}\left(\tilde{\rho}_0 \ln \tilde{\rho}_0\right) + \mathrm{Tr}\left(\tilde{\rho}_1 \ln \tilde{\rho}_1\right)\right).
\end{aligned} \tag{3.5}$$

Here, the first line is because of $\mathrm{Tr}_B(\tilde{\rho}_k) = \rho_k$ for $k \in \{0,1\}$, and the third line owes to $\mathrm{QJS}(\rho_0,\rho_1) = S(\frac{\rho_0+\rho_1}{2}) - \frac{1}{2}(S(\rho_0)+S(\rho_1))$ for any states ρ_0 and ρ_1. Notice that $\sigma_0 \otimes |0\rangle\langle 0|$, $\sigma_1 \otimes |1\rangle\langle 1|$, and $\sigma_2 \otimes |2\rangle\langle 2|$ are orthogonal to each other, and $\ln(A+B) = \ln(A) + \ln(B)$ when A and B are orthogonal (i.e., $AB = BA = 0$), we have derived that

$$\begin{aligned}
\mathrm{Tr}\left(\frac{\tilde{\rho}_0+\tilde{\rho}_1}{2} \ln \frac{\tilde{\rho}_0+\tilde{\rho}_1}{2}\right) &= \mathrm{Tr}(\sigma_2 \ln \sigma_2) + \sum_{k\in\{0,1\}} \mathrm{Tr}\left(\frac{\sigma_0}{2} \ln \frac{\sigma_0}{2}\right), \\
\forall k \in \{0,1\},\ \mathrm{Tr}\left(\tilde{\rho}_k \ln \tilde{\rho}_k\right) &= \mathrm{Tr}(\sigma_2 \ln \sigma_2) + \mathrm{Tr}(\sigma_k \ln \sigma_k).
\end{aligned} \tag{3.6}$$

Plugging Equation (3.6) into Equation (3.5), we finish the proof:

$$\mathrm{QJS}(\rho_0,\rho_1) \leq \mathrm{Tr}\left[\frac{\sigma_0}{2}\left(\ln \sigma_0 - \ln \frac{\sigma_0}{2}\right)\right] + \mathrm{Tr}\left[\frac{\sigma_1}{2}\left(\ln \sigma_1 - \ln \frac{\sigma_1}{2}\right)\right]$$

$$= \frac{\ln 2}{2} \cdot \mathrm{Tr}(\sigma_0 + \sigma_1)$$
$$= \ln 2 \cdot \mathrm{T}(\rho_0, \rho_1),$$

where the third line is due to $\sigma_0 + \sigma_1 = |\rho_0 - \rho_1|$. □

Quantum analogs of Jansen-Tsallis divergence. We start by defining the quantum q-Tsallis entropy, generalizing the von Neumann entropy:

Definition 3.27 (Quantum q-Tsallis entropy and von Neumann entropy)**.** *Let ρ be a (mixed) quantum state. The quantum q-Tsallis entropy of ρ is defined by*

$$\mathrm{S}_q(\rho) \coloneqq \frac{1 - \mathrm{Tr}(\rho^q)}{q-1} = -\mathrm{Tr}(\rho^q \ln_q(\rho)).$$

As $q \to 1$, the quantum q-Tsallis entropy converges to the von Neumann entropy.

The quantum Tsallis entropy serves as a non-additive generalization of the von Neumann entropy:

Lemma 3.28 (Pseudo-additivity of S_q, adapted from [Rag95, Lemma 3])**.** *For any quantum states ρ_0 and ρ_1, and any $q \geq 1$, we have*:

$$\mathrm{S}_q(\rho_0 \otimes \rho_1) = \mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1) - (q-1)\mathrm{S}_q(\rho_0)\mathrm{S}_q(\rho_1).$$

Specifically, the equality $\mathrm{S}_q(\rho_0 \otimes \rho_1) = \mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)$ holds if and only if (a) *$q = 1$, or* (b) *for $q > 1$, either of the states ρ_0 or ρ_1 is pure.*

Next, a generalization of the quantum Jensen-Shannon divergence [MLP05], based on the quantum q-Tsallis entropy, is defined as follows:

Definition 3.29 (Quantum q-Jensen-Tsallis Divergence, adapted from [BH09])**.** *Let ρ_0 and ρ_1 be two quantum states. The quantum q-Jensen-(Shannon-)Tsallis divergence between ρ_0 and ρ_1 is defined by*

$$\mathrm{QJT}_q(\rho_0, \rho_1) \coloneqq \begin{cases} \mathrm{S}_q\left(\frac{\rho_0+\rho_1}{2}\right) - \frac{1}{2}\left(\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)\right), & q \neq 1 \\ \mathrm{S}\left(\frac{\rho_0+\rho_1}{2}\right) - \frac{1}{2}\left(\mathrm{S}(\rho_0) + \mathrm{S}(\rho_1)\right), & q = 1 \end{cases}.$$

Specifically, for pure states $|\psi_0\rangle\langle\psi_0|$ and $|\psi_1\rangle\langle\psi_1|$, it holds that

$$\mathrm{QJT}_q(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) = \mathrm{S}_q\Big(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\Big).$$

Similar to the quantum Jensen-Shannon divergence, the square root of QJT_q is a distance metric when $0 \leq q \leq 2$, as established in [Sra21]. However, QJT_q does not satisfy an equality similar to Equation (3.3) with respect to the quantum Tsallis relative entropy, defined as $\mathrm{D}_q(\rho_0 \| \rho_1) \coloneqq \frac{1-\mathrm{Tr}(\rho_0^q \rho_1^{1-q})}{1-q}$ (see, e.g., [FYK04]). Moreover, a symmetrized version of $\mathrm{D}_q(\cdot\|\cdot)$ results in a different quantity (see [JMDA21]).

Lastly, we provide more useful properties of QJT_q. By combining [FYK07, Theorem 1.5] and [Fur05, Remark V.3], we can immediately derive Lemma 3.30 and Lemma 3.31. In particular, the equality in Lemma 3.31 holds even in a stronger form:

$$\mathrm{S}_q\left(\sum_{i\in[k]} \mu_i^q \rho_i\right) = \mathrm{H}_q(\mu) + \sum_{i\in[k]} \mu_i \mathrm{S}_q(\rho_i)$$

for orthogonal quantum states $\rho_1, \cdots, \rho_k$. Additionally, it is noteworthy that Lemma 3.31 admits a simple proof in [Kim16, Lemma 1].

Lemma 3.30 (Unitary invariance of QJT_q, adapted from [FYK07, Theorem 1.5])**.** *For any quantum states ρ_0 and ρ_1, and any unitary transformation U acting on ρ_0 or ρ_1, the following equality holds*:

$$\mathrm{QJT}_q(U^\dagger \rho_0 U, U^\dagger \rho_1 U) = \mathrm{QJT}_q(\rho_0, \rho_1).$$

Lemma 3.31 (Joint q-Tsallis entropy theorem, adapted from [FYK07, Theorem 1.5])**.** *Let k be an integer, and let $\{\rho_i\}_{i\in[k]}$ be a set of (mixed) quantum states. Let k-tuple $\mu \coloneqq (\mu_1, \cdots, \mu_k)$ be a probability distribution. Then, for any $q \geq 0$, it holds that*:

$$\mathrm{S}_q\left(\sum_{i\in[k]} \mu_i |i\rangle\langle i| \otimes \rho_i\right) = \mathrm{H}_q(\mu) + \sum_{i\in[k]} \mu_i^q \mathrm{S}_q(\rho_i).$$

Following the discussion in [Ras11, Section 3], Fannes' inequality for QJT_q, where $0 \leq q \leq 2$, was established in [FYK07, Theorem 2.4]. Notably, for QJT_q with $q > 1$, a sharper Fannes-type inequality was provided in [Zha07, Theorem 2]:

Lemma 3.32 (Fannes' inequality for QJT_q, adapted from Theorem 2 and Corollary 2 in [Zha07])**.** *For any quantum states ρ_0 and ρ_1 of dimension N, we have:*

$$\forall q > 1,\ |\mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1)| \leq \mathrm{T}(\rho_0, \rho_1)^q \cdot \ln_q(N-1) + \mathrm{H}_q(\mathrm{T}(\rho_0, \rho_1)).$$

Moreover, for the case of $q = 1$ (von Neumann entropy), we have:

$$|\mathrm{S}(\rho_0) - \mathrm{S}(\rho_1)| \leq \mathrm{T}(\rho_0, \rho_1) \cdot \ln(N-1) + \mathrm{H}(\mathrm{T}(\rho_0, \rho_1)).$$

3.3 Time-bounded quantum state testing

In this section, we focus on the problem of closeness testing for quantum states. We begin by defining the time-bounded state testing problem with respect to the trace distance, denoted as $\mathrm{QSD}[\alpha, \beta]$, along with a variant of this promise problem:

Definition 3.33 (Quantum State Distinguishability, QSD, adapted from [Wat02, Section 3.3])**.** *Let Q_0 and Q_1 be quantum circuits acting on m qubits ("input length") and having n specified output qubits ("output length"), where $m(n)$ is polynomial in n. Let ρ_i denote the quantum state obtained by running Q_i on the state $|0\rangle^{\otimes m}$ and tracing out the non-output qubits. Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions. 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 $\mathrm{T}(\rho_0, \rho_1) \leq \beta(n)$.*

Furthermore, the version of this problem restricted to pure states, where ρ_0 and ρ_1 are pure states, is referred to as PureQSD.

While Definition 3.33 aligns with the classical counterpart of QSD defined in [SV03, Section 2.2], it is slightly more restrictive than the definition in [Wat02, Section 3.3]. In particular, Definition 3.33 assumes that the input length m and the output length n are *polynomially equivalent*, whereas [Wat02, Section 3.3] allows for cases where the output length (e.g., a single qubit) is *much smaller* than the input length.

We next consider a restricted variant of the complement of QSD, which involves testing the closeness of a quantum state to the *maximally mixed state* with respect to the trace distance. This problem can be similarly defined and denoted as QSCMM$[\beta, \alpha]$:

Definition 3.34 (Quantum State Closeness to Maximally Mixed State, QSCMM, adapt from [Kob03, Section 3])**.** *Let Q be a quantum circuit acting on m qubits and having n specified output qubits, where $m(n)$ is polynomial in n. Let ρ denote the quantum state obtained by running Q on the state $|0\rangle^{\otimes m}$ and training out the non-output qubits. Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions. Decide whether*:

- Yes: *A quantum circuit Q such that* $\mathrm{T}(\rho, (I/2)^{\otimes n}) \leq \beta(n)$*;*
- No: *A quantum circuit Q such that* $\mathrm{T}(\rho, (I/2)^{\otimes n}) \geq \alpha(n)$*.*

In addition to QSD, PureQSD, and QSCMM, we also consider the time-bounded state testing problem with respect to the quantum entropy difference, denoted as QED$[g]$:

Definition 3.35 (Quantum Entropy Difference Problem, QED. adapted from [BASTS10])**.** *Let Q_0 and Q_1 be quantum circuits acting on m qubits and having n specified output qubits, where $m(n)$ is polynomial in n. Let ρ_i denote the quantum state obtained by running Q_i on the state $|0\rangle^{\otimes m}$ and tracing out the non-output qubits. Let $g(n)$ be an efficiently computable function. Decide whether*:

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

As implicitly shown in [BASTS10], the QSZK containment of QED$[g(n)]$ holds even when $g(n)$ is polynomially small:

Theorem 3.36 (Implicitly in [BASTS10])**.** *For any efficiently computable function $g(n)$ satisfying $g(n) \geq 1/\mathrm{poly}(n)$, the following holds*:

$$\mathrm{QED}[g(n)] \text{ is in } \mathsf{QSZK}.$$

Proof. To establish the QSZK containment, it suffices to show a promise gap amplification that reduces QED$[g(n)]$ to QED$[1/2]$, as QED$[1/2]$ is QSZK-hard [BASTS10, Wat02].

We begin by considering two new states $\tilde{\rho}_0$ and $\tilde{\rho}_1$, defined as $\tilde{\rho}_b = \rho_b^{\otimes p(n)}$ for $b \in \{0, 1\}$, where $p(n)$ is a polynomial function satisfying $p(n)g(n) \geq 1/2$. By the additivity of von Neumann entropy for independent quantum systems, the following holds for *yes* instances:

$$\mathrm{S}(\tilde{\rho}_0) - \mathrm{S}(\tilde{\rho}_1) = p(n) \cdot (\mathrm{S}(\rho_0) - \mathrm{S}(\rho_1)) \geq p(n)g(n) \geq 1/2.$$

Similarly, for *no* instances, we deduce that $\mathrm{S}(\tilde{\rho}_1) - \mathrm{S}(\tilde{\rho}_0) \geq 1/2$ as desired. □

3.3.1 Computational hardness of QSD and QSCMM

Inspired by the polarization lemma for the total variation distance [SV03], a corresponding polarization lemma for the trace distance was established in [Wat02]. This result follows from the trace distance exhibiting *similar* behavior to the total variation distance in this context, as both satisfy *analogous inequalities* for the relevant closeness measures.

Since the polarization lemma for the total variation distance enables an improved SZK-hardness of SD, as stated in [BDRV19, Theorem 3.14], an analogous improvement in QSZK-hardness of QSD can be deduced under the same parameters:[4]

Lemma 3.37 (QSD is QSZK-hard)**.** *Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions satisfying $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$. For any constant $\tau \in (0, 1/2)$,*

$$\mathrm{QSD}[\alpha, \beta] \text{ is } \mathsf{QSZK}\text{-hard under Karp reduction,}$$

when $\alpha(n) \leq 1 - 2^{-n^\tau}$ and $\beta(n) \geq 2^{-n^\tau}$ for every $n \in \mathbb{N}$.

Let $\overline{\mathrm{QSD}}$ denote the complement of QSD. Noting that QSZK is closed under the complement [Wat02, Wat09b], $\overline{\mathrm{QSD}}$ is also QSZK-hard.

In terms of the pure-state restriction of QSD, following the construction in [RASW23, Theorem 12] (see also [LLW23, Lemma 17] and [WZ24a, Theorem IV.1]), we can establish that PureQSD is BQP-hard under Karp reduction:

Lemma 3.38 (PureQSD is BQP-hard)**.** *Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions such that $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$. For any polynomial $l(n)$, let $n' := n + 1$, $\mathrm{PureQSD}[\alpha(n'), \beta(n')]$ is BQP-hard when $\alpha(n') \leq \sqrt{1 - 2^{-2l(n'-1)}}$ and $\beta(n') \geq 2^{-(l(n'-1)+1)/2}$ for every integer $n' \geq 2$.*

Specifically, by choosing $l(n'-1) = n'$, it holds that: For every integer $n' \geq 2$,

$$\mathrm{PureQSD}\left[\sqrt{1 - 2^{-2n'}}, 2^{-(n'+1)/2}\right] \text{ is } \mathsf{BQP}\text{-hard under Karp reduction.}$$

Proof. As BQP is closed under complement, it suffices to show that PureQSD is coBQP-hard under Karp reduction. For any promise problem $(\mathcal{P}_{yes}, \mathcal{P}_{no}) \in \mathsf{coBQP}[b(n), a(n)]$ with $a(n) - b(n) \geq 1/\mathrm{poly}(n)$, we assume without loss of generality that the coBQP circuit $\hat{C}_x$ has an output length of n. Using error reduction for coBQP via a sequential repetition, for any polynomial $l(n)$, we can achieve that the acceptance probability $\Pr[C_x \text{ accepts}] \leq 2^{-l(n)}$ for *yes* instances, whereas $\Pr[C_x \text{ accepts}] \geq 1 - 2^{-l(n)}$ for *no* instances.

Next, we construct a new quantum circuit C'_x with an additional single-qubit register F initialized to zero. The circuit C'_x is defined as $C'_x := C_x^\dagger X_{\mathsf{O}}^\dagger \mathrm{CNOT}_{\mathsf{O}\to\mathsf{F}} X_{\mathsf{O}} C_x$, where the single-qubit register O corresponds to the output qubit. It is evident that the output length n' of C'_x satisfies $n' = n + 1$. We say that C'_x accepts if the measurement outcomes of all qubits are all zero. Then, we have:

$$\begin{aligned} \Pr[C'_x \text{ accepts}] &= \left\| (|\bar{0}\rangle\langle\bar{0}| \otimes |0\rangle\langle 0|_{\mathsf{F}}) C'_x (|\bar{0}\rangle \otimes |0\rangle_{\mathsf{F}}) \right\|_2^2 \\ &= \left| \langle\bar{0}| C_x^\dagger |1\rangle\langle 1|_{\mathsf{O}} C_x |\bar{0}\rangle \right|^2 \\ &= \Pr[C_x \text{ accepts}]^2. \end{aligned} \tag{3.7}$$

Here, the second line owes to $\mathrm{CNOT}_{\mathsf{O}\to\mathsf{F}} = |0\rangle\langle 0|_{\mathsf{O}} \otimes I_{\mathsf{F}} + |1\rangle\langle 1|_{\mathsf{O}} \otimes X_{\mathsf{F}}$. By defining two pure states $|\psi_0\rangle := |\bar{0}\rangle \otimes |0\rangle_{\mathsf{F}}$ and $|\psi_1\rangle := C'_x(|\bar{0}\rangle \otimes |0\rangle_{\mathsf{F}})$ corresponding to $Q_0 = I$ and $Q_1 = C'_x$, respectively, we can derive the following:

$$\Pr[C'_x \text{ accepts}] = |\langle\psi_0|\psi_1\rangle|^2 = 1 - \mathrm{T}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|). \tag{3.8}$$

Combining Equation (3.7) and Equation (3.8), we conclude that:

[4] This work does not distinguish QSZK from its honest-verifier variant $\mathsf{QSZK}_{\mathrm{HV}}$, as these two classes are equivalent [Wat09b].

- For *yes* instances, $\Pr[C_x \text{ accepts}] = |\langle\psi_0|\psi_1\rangle| \leq 2^{-l(n)}$ implies that
$$\mathrm{T}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \geq \sqrt{1-2^{-2l(n)}} \geq \sqrt{1-2^{-2l(n'-1)}}.$$
- For *no* instances, $\Pr[C_x \text{ accepts}] = |\langle\psi_0|\psi_1\rangle| \geq 1-2^{-l(n)}$ yields that
$$\begin{aligned}\mathrm{T}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) &\leq \sqrt{1-(1-2^{-l(n)})^2} \\ &= \sqrt{2^{-l(n)+1}-2^{-2l(n)}} \\ &\leq 2^{-\frac{l(n)+1}{2}} \\ &\leq 2^{-\frac{l(n'-1)+1)}{2}}.\end{aligned}$$
□

Next, combining the proof strategy outlined in [Kob03, Section 3] and the reduction from QEA to QSCMM in [BASTS10, Section 5.3], the NIQSZK hardness of QSCMM was established in [CCKV08, Section 8.1] with an appropriate parameter trade-off:

Lemma 3.39 (QSCMM is NIQSZK-hard, adapted from [CCKV08, Section 8.1])**.**

For any $n \geq 3$, $\mathrm{QSCMM}[1/n, 1-1/n]$ is NIQSZK-hard under Karp reduction.

Here, NIQSZK is the class of promise problems possessing non-interactive quantum statistical zero-knowledge, as introduced in [Kob03].

3.3.2 Quantitative lower bounds beyond the white-box model

Quantitative lower bounds for closeness testing problems, particularly those concerning query and sample complexities for states and distributions, are established in the context of the *quantum purified access input model*, which was implicitly introduced in [Wat02]. The previously defined notions of QSD, QSCMM, and QED correspond to white-box scenarios. However, query and sample complexity bounds are typically demonstrated in black-box scenarios, defined as follows:

- **White-box input model**: The input of the problem QSD consists of descriptions of polynomial-size quantum circuits Q_0 and Q_1. Specifically, for $b \in \{0,1\}$, the description of Q_b includes a sequence of polynomially many 1- and 2-qubit gates.
- **Black-box input model**: In this model, instead of providing the descriptions of the quantum circuits Q_0 and Q_1, only query access to Q_b is allowed, denoted as O_b for $b \in \{0,1\}$. For convenience, we also allow query access to $Q_b^\dagger$ and controlled-Q_b, denoted by $O_b^\dagger$ and controlled-O_b, respectively.

We now proceed with a query complexity lower bound for QSD. Note that an n-qubit maximally mixed state $(I/2)^{\otimes n}$ is commutative with any n-qubit quantum states ρ. Consider the spectral decomposition $\rho = \sum_{i\in[2^n]} \mu_i |v_i\rangle\langle v_i|$, where $\{|v_i\rangle\}_{i\in[2^n]}$ is an orthonormal basis, then the following holds:

$$\mathrm{T}\Big(\rho, (I/2)^{\otimes n}\Big) = \mathrm{TV}(\mu, U_{2^n}).$$

Here, U_{2^n} is a uniform distribution over $[2^n]$. Leveraging a similar argument for $\rho_{\mathtt{U}}$, as in Lemmas 3.40 and 3.42, where the eigenvalues of $\rho_{\mathtt{U}}$ form a uniform distribution on the support of ρ, we can obtain:

Lemma 3.40 (Query complexity lower bound for QSD, adapted from [CFMdW10, Theorem 2]). *For any $\epsilon \in (0, 1/2]$, there exists an n-qubit quantum state ρ of rank r and the corresponding an n-qubit state $\rho_{\mathfrak{U}}$. Then, the quantum query complexity required to decide whether $\mathrm{T}(\rho, \rho_{\mathfrak{U}})$ is at least ϵ or exactly 0, under the purified quantum query access model, is given by $\Omega(r^{1/3})$.*

It is noteworthy that the quantum query model used in [CFMdW10] differs from the purified quantum query access model. Nevertheless, this lower bound also applies to our query model, as the discussion after Definition 3 in [GL20].

Next, we present a query complexity lower bound for distinguishing two probability distributions, as provided in [Bel19]:

Lemma 3.41 (Query complexity for distinguishing probability distributions, adapted from [Bel19, Theorem 4]). *Let U_p and U_q be two unitary operators satisfying:*

$$U_p|0\rangle = \sum_{j\in[N]} \sqrt{p(j)}|j\rangle|\varphi_j\rangle \text{ and } U_q|0\rangle = \sum_{j\in[N]} \sqrt{q(j)}|j\rangle|\psi_j\rangle.$$

Here, p and q are probability distributions on $[N]$, and $\{|\varphi_j\rangle\}$ and $\{|\psi_j\rangle\}$ are orthonormal bases. Then, for any quantum query algorithm that distinguishes U_p and U_q, the required query complexity is lower-bounded by $\Omega(1/\mathrm{H}(p, q))$.

It is noteworthy that Lemma 3.41 was ever used as a tool to prove the quantum query complexity lower bounds for the closeness testing of probability distributions [LWL24] and the estimations of trace distance and fidelity [Wan24].

Furthermore, we also need a sample complexity lower bound for QSD, which follows from [OW21, Theorem 4.2] and is specified in Lemma 3.42. Here, *sample complexity* denotes the number of copies of ρ required to accomplish a specific closeness testing task.

Lemma 3.42 (Sample complexity lower bound for QSD, adapted from [OW21, Corollary 4.3]). *For any $\epsilon \in (0, 1/2]$, there exists an n-qubit quantum state ρ of rank r and the corresponding an n-qubit state $\rho_{\mathfrak{U}}$. Then, the quantum sample complexity required to decide whether $\mathrm{T}(\rho, \rho_{\mathfrak{U}})$ is at least ϵ or exactly 0 is given by $\Omega(r/\epsilon^2)$.*

3.4 Space-bounded distribution testing and related works

To the best of our knowledge, no prior work has specifically focused on space-bounded distribution (or quantum state) testing from a complexity-theoretic perspective. Instead, we review prior works that are closely related to this computational problem.

More precisely, we focus on a computational problem involving two $\mathrm{poly}(n)$-size classical circuits, C_0 and C_1, which generate samples from the distributions D_0 and D_1, respectively. Each circuit is equipped with a read-once polynomial-length random-coins tape, setting it apart from time-bounded scenarios such as SD and ED, where random coins are provided as *input* to classical circuits C_0 and C_1 for generating samples from the corresponding distributions.

The input length and output length of the circuits are $O(\log n)$. The task is to decide whether D_0 is α-far from or β-close to D_1 with respect to some distance-like measure.

Furthermore, it is straightforward to observe that space-bounded distribution testing with respect to the squared Euclidean distance (ℓ_2 norm) is BPL-complete, similar to its time-bounded counterpart.

Several models related to space-bounded distribution testing have been investigated previously. Earlier streaming-algorithmic works [FKSV02, GMV06] utilize *entries* of the distribution as the data stream, with entries given in different orders for different models. On the other hand, a later work [CLM10] considered a data stream consisting of a sequence of i.i.d. samples drawn from distributions and studied low-space streaming algorithms for distribution testing.

For the task of (Shannon) entropy estimation, previous streaming algorithms have the setting under the assumption of worst-case ordered samples drawn from N-dimensional distributions. Their algorithm requires $\mathrm{polylog}(N/\epsilon)$ space, where ϵ is the additive error. Recently, Acharya, Bhadane, Indyk, and Sun [ABIS19] addressed the entropy estimation problem with i.i.d. samples drawn from distributions as the data stream and demonstrated the first $O(\log(N/\epsilon))$ space streaming algorithm. The sample complexity, viewed as the time complexity, was subsequently improved in [AMNW22].

However, for the total variation distance (ℓ_1 norm), previous works focused on the trade-off between the sample complexity and the space complexity (memory constraints), achieving only a nearly-log-squared space streaming algorithm [DGKR19].

It is noteworthy that the primary distinction between the computational and streaming settings lie in how the sampling devices are accessed. Of course, not all distributions can be described as a polynomial-size circuit (i.e., a succinct description). The distinction can be summarized as follows:

- In the computational problem, we have access to the "source code" of the devices and can potentially use them for purposes like "reverse engineering".
- In contrast, the streaming setting utilizes the sampling devices in a "black-box" manner, and then obtains independent and identically distributed (i.i.d.) samples.

As a consequence, a logspace streaming algorithm can imply containment in BPL. Particularly, in the space-bounded distribution testing testing, the sample-generating circuits C_0 and C_1 can produce the i.i.d. samples, which are typically provided through the data stream in the streaming distribution testing setting.

Chapter 4

On estimating the trace of quantum state powers

4.1 Introduction

The time-bounded (tolerant) state testing problems are generally associated with the class QSZK [Wat02, Wat09b, BASTS10], as discussed in Section 1.1. These problems are unlikely to be efficiently solvable by a quantum computer unless BQP = QSZK. In contrast, when considering some specific closeness measure such as $\mathrm{Tr}(\rho_0\rho_1)$, the corresponding time-bounded state testing problem is captured by the class BQP[BCWdW01, Kob03], making them computationally as easy as preparing the states. A similar contrast appears in terms of quantitative bounds, particularly the query and sample complexities. While the general upper bound for (tolerant) quantum state testing depends (at least) linearly on the dimension (e.g., [MdW16, Section 4.2]), certain properties of quantum states can be tested far more efficiently than the general case.

A simple and interesting example is the property Purity, where ρ satisfies the property if and only if it is a pure state. This example is essentially an instance of estimating the trace of quantum state powers, specifically $\mathrm{Tr}(\rho^2)$. A natural approach to test Purity is to apply the SWAP test [BCWdW01] to two copies of ρ, and this algorithm accepts with probability $(1+\mathrm{Tr}(\rho^2))/2$, which is equal to 1 if and only if ρ is pure. Further analysis deduces that Purity can be tolerantly tested with $O(1/\epsilon^2)$ copies of ρ.[1] Meanwhile, Ekert et al. [EAO+02] presented an efficient quantum algorithm for estimating $\mathrm{Tr}(\rho^q)$ where $q > 1$ is an integer. These fundamental works raise two interesting questions:

(i) Is there an efficient quantum algorithm for estimating the trace of quantum state powers $\mathrm{Tr}(\rho^q)$ for any non-integer $q > 1$?

(ii) Can estimating the trace of quantum state powers, e.g., $\mathrm{Tr}(\rho^2)$, fully capture the computational power of quantum computing, namely BQP-complete?

In this chapter, we focus on estimating the trace of quantum state powers, or equivalently, the Quantum q-Tsallis Entropy Difference Problem ($\mathrm{TsallisQED}_q$)

[1] The sample (or query) complexity for Purity varies depending on whether the scenario involves one-sided or two-sided error. Our upper bound applies to the two-sided error case, whereas the sample complexity for the one-sided error case is $O(1/\epsilon)$, as detailed in [MdW16, Section 4.2].

and the Quantum q-Tsallis Entropy Approximation Problem (TsallisQEA_q). These two problems constitute the (white-box) quantum state testing problem with respect to the quantum q-Tsallis entropy. For TsallisQED_q, we consider two polynomial-size quantum circuits (devices), denoted as Q_0 and Q_1, which prepare n-qubit quantum states ρ_0 and ρ_1, respectively, with access to the descriptions of these circuits. Our goal is to decide whether the difference $\mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1)$ is at least 0.001 or at most -0.001.[2] The setting of TsallisQEA_q is similar to TsallisQED_q, except that we only consider a single n-qubit quantum state ρ, and the task is to decide whether the difference $\mathrm{S}_q(\rho) - t(n)$ is at least 0.001 or at most -0.001, where $t(n)$ is a known threshold.

Next, we will state our main results and provide justifications for their significance.

4.1.1 Main results

We begin by presenting our first main result, which provides a positive answer to Question (i) for the regime $q \geq 1 + \Omega(1)$:[3]

Theorem 4.1 (Quantum estimator for q-Tsallis entropy)**.** *Given quantum query access to the state-preparation circuit of an n-qubit quantum state ρ, for any $q \geq 1 + \Omega(1)$, there is a quantum algorithm for estimating $\mathrm{S}_q(\rho)$ to additive error 0.001 with query complexity $O(1)$. Moreover, if the description of the state-preparation circuit is of size $\mathrm{poly}(n)$, then the time complexity of the quantum algorithm is $\mathrm{poly}(n)$. Consequently, for any $q \geq 1 + \Omega(1)$, TsallisQED_q and TsallisQEA_q are in BQP.*

More specifically, when the desired additive error is set to ϵ, the explicit query complexity of Theorem 4.1 becomes $O(1/\epsilon^{1+\frac{1}{q-1}})$, or expressed as $\mathrm{poly}(1/\epsilon)$ (see Theorem 4.5). Moreover, if the state-preparation circuit of ρ is of size $L(n) = \mathrm{poly}(n)$, Theorem 4.1 provides a quantum algorithm with time complexity $O(L/\epsilon^{1+\frac{1}{q-1}})$, or equivalently, $\mathrm{poly}(n, 1/\epsilon)$. Using the same idea, we can also derive an upper bound $\widetilde{O}(1/\epsilon^{3+\frac{2}{q-1}})$, or expressed as $\mathrm{poly}(1/\epsilon)$, for the sample complexity needed to estimate $\mathrm{S}_q(\rho)$ (see Theorem 4.6). This is achieved by applying the *samplizer* from [WZ24b], which allows a quantum query-to-sample simulation.

There are several quantum algorithms for estimating the q-Tsallis entropy of an n-qubit mixed quantum state ρ for non-integer constant $q > 1$ proposed in [AISW20, WGL+24, WZL24, WZ24b], all of which turn out to have time complexity $\exp(n)$ in the setting that ρ is given by its state-preparation circuit of size $\mathrm{poly}(n)$.

- In [AISW20, Theorem 3] and [WZ24b, Theorem 1.2], for non-integer constant $q > 1$, they proposed quantum algorithms for estimating the q-Rényi entropy of an n-qubit quantum state ρ by using $\mathsf{S} = \mathrm{poly}(1/\epsilon) \cdot \exp(n)$ samples of ρ and $\mathsf{T} = \mathrm{poly}(1/\epsilon) \cdot \exp(n)$ quantum gates.[4] Their result implies an estimator for $\mathrm{S}_q(\rho)$ with the same complexity, because any estimator for q-Rényi entropy implies an

[2] It is noteworthy that 0.001 is just an arbitrary constant for the precision parameter, which can be replaced by any inverse polynomial function in general. See Definition 4.17 and Definition 4.18 for formal definitions.

[3] We implicitly assume that q satisfies $1 + \Omega(1) \leq q \leq O(1)$. Since $\mathrm{S}_q(\rho) \leq o(1)$ when $q = \omega(1)$, it is reasonable to consider constantly large q.

[4] The explicit sample complexities of the approaches of [AISW20, Theorem 3] and [WZ24b, Theorem 2]

estimator for q-Tsallis entropy with the same parameter for $q > 1$ (as noted in [AOST17, Appendix A]). By preparing each sample of ρ using its state-preparation circuit of size $\mathrm{poly}(n)$, one can estimate $\mathrm{S}_q(\rho)$ by using their estimators with overall time complexity $\mathsf{S} \cdot \mathrm{poly}(n) + \mathsf{T} = \mathrm{poly}(1/\epsilon) \cdot \exp(n)$.

- In [WGL+24, Theorem III.9], for non-integer constant $q > 1$, they proposed a quantum algorithm for estimating $\mathrm{S}_q(\rho)$ with query complexity $\widetilde{O}(r^{1/\{\frac{q-1}{2}\}}/\epsilon^{1+1/\{\frac{q-1}{2}\}}) = \mathrm{poly}(r, 1/\epsilon)$, where r is (an upper bound on) the rank of ρ and $\{x\} \coloneqq x - \lfloor x \rfloor$ denotes the fractional part of x. In [WZL24, Corollary 5], for non-integer constant $q > 1$, they proposed a quantum algorithm for estimating the q-Rényi entropy of a quantum state with query complexity $\widetilde{O}(r/\epsilon^{1+\frac{1}{q}}) = \mathrm{poly}(r, 1/\epsilon)$, which also implies a quantum algorithm for estimating $\mathrm{S}_q(\rho)$ with query complexity $\mathrm{poly}(r, 1/\epsilon)$ (the reason has been discussed in the last item). For n-qubit quantum state ρ without prior knowledge, by taking $r = 2^n$, their query compelxity is then $\mathrm{poly}(2^n, 1/\epsilon) = \mathrm{poly}(1/\epsilon) \cdot \exp(n)$, which is exponentially larger than our $\mathrm{poly}(n, 1/\epsilon)$.

Our efficient quantum estimator for $\mathrm{S}_q(\rho)$ where $q \geq 1+\Omega(1)$ (Theorem 4.1), combined with our hardness results for $\textsc{TsallisQED}_q$ and $\textsc{TsallisQEA}_q$ (Theorem 4.2), indicates a sharp phase transition between the case of $q = 1$ and constant $q > 1$ and answers to Question (i) and (ii). For clarity, we summarize our main results in Table 4.1.

	$q = 1$	$1 < q \leq 1+\frac{1}{n-1}$	$1+\Omega(1) \leq q \leq 2$	$q > 2$
$\textsc{TsallisQED}_q$	QSZK-complete [BASTS10]	QSZK-hard Theorem 4.2(2)	BQP-complete Theorem 4.1 and Theorem 4.2(1)	in BQP Theorem 4.1
$\textsc{TsallisQEA}_q$	NIQSZK-complete [BASTS10, CCKV08]	NIQSZK-hard[5] Theorem 4.2(2)	BQP-complete Theorem 4.1 and Theorem 4.2(1)	in BQP Theorem 4.1

Table 4.1: Computational hardness of $\textsc{TsallisQED}_q$ and $\textsc{TsallisQEA}_q$.

For the case of $q = 1$, $\textsc{TsallisQED}_q$ and $\textsc{TsallisQEA}_q$ coincide with the Quantum Entropy Difference Problem (QED) and the Quantum Entropy Approximation Problem (QEA) introduced in [BASTS10], respectively. Moreover, QED is complete for the class QSZK [BASTS10], whereas QEA is complete for the class NIQSZK [BASTS10, CCKV08]. These two classes contain BQP and are seemingly much harder than BQP.[6] Meanwhile, the best known upper bound for QSZK is QIP(2) with a quantum linear-space honest prover [LLW23], and the best known upper bound for NIQSZK is qq-QAM [KLN19], both of which are contained in QIP(2) $\subseteq$ PSPACE [JUW09].

In terms of *quantitative* bounds on quantum query and sample complexities, QSZK-hard or NIQSZK-hard in the white-box setting correspond to rank-dependent complexities

are $O(2^{2n}/\epsilon^2)$ and $O(2^{(\frac{4}{q}-2)n}/\epsilon^{1+\frac{4}{q}} \cdot \mathrm{poly}(n, \log(1/\epsilon)))$, respectively, both of which are $\mathrm{poly}(1/\epsilon) \cdot \exp(n)$. The number of quantum states in the approach of [AISW20, Theorem 3] was mentioned in [WZ24b] to be $O((2^{2n}/\epsilon^2)^3 \cdot \mathrm{polylog}(2^n, 1/\epsilon)) = \mathrm{poly}(1/\epsilon) \cdot \exp(n)$ by using the weak Schur sampling in [MdW16, Section 4.2.2] and the quantum Fourier transform over symmetric groups [KS16]. Another possible implementation noted in [Hay24] is to use the Schur transform in [Ngu23], resulting in $O(2^{2n}/\epsilon^2 \cdot 2^{4n} \cdot \mathrm{polylog}(2^n, 1/\epsilon)) = \mathrm{poly}(1/\epsilon) \cdot \exp(n)$.

[5] $\textsc{TsallisQEA}_q$ is NIQSZK-hard only for $q(n) = 1 + \frac{1}{n-1}$, as detailed in Theorem 4.2(2).

[6] Following the oracle separation between NISZK and PP [BCH+19], it holds that $\mathsf{NIQSZK}^{\mathcal{O}} \not\subseteq \mathsf{PP}^{\mathcal{O}}$ and likewise $\mathsf{QSZK}^{\mathcal{O}} \not\subseteq \mathsf{PP}^{\mathcal{O}}$ for some classical oracle $\mathcal{O}$.

in black-box settings. Specifically, we establish lower bounds for both the easy regime $q \geq 1 + \Omega(1)$ and the hard regime $1 < q \leq 1 + \frac{1}{n-1}$, with the upper bounds for the hard regime derived from those for estimating quantum Rényi entropy, as detailed in Table 4.2.

Regime of q	Query Complexity		Sample Complexity	
	Upper Bound	Lower Bound	Upper Bound	Lower Bound
$q \geq 1 + \Omega(1)$	$O(1/\epsilon^{1+\frac{1}{q-1}})$ Theorem 4.5	$\Omega(1/\sqrt{\epsilon})$ Theorem 4.28	$\widetilde{O}(1/\epsilon^{3+\frac{2}{q-1}})$ Theorem 4.6	$\Omega(1/\epsilon)$ Theorem 4.31
$1 < q \leq 1 + \frac{1}{n-1}$	$\widetilde{O}(r/\epsilon^2)$ [WZL24]	$\Omega(r^{0.17-c})$[7] Theorem 4.29	$\widetilde{O}(r^2/\epsilon^5)$[8] [WZ24b]	$\Omega(r^{0.51-c'})$[7] Theorem 4.32
$q = 1$	$\widetilde{O}(r/\epsilon^2)$[9] [WGL+24]	$\widetilde{\Omega}(\sqrt{r})$ [BKT20]	$\widetilde{O}(r^2/\epsilon^5)$[8] [WZ24b]	$\Omega(r/\epsilon)$ [WZ24b]

Table 4.2: (Rank-dependent) bounds on query and sample complexities for estimating $\mathrm{S}_q(\rho)$.

On the other hand, understanding why the regime $q \geq 1 + \Omega(1)$ is computationally easy can be illustrated by the case of $q = 2$ (Purity Estimation), particularly deciding whether $\mathrm{Tr}(\rho^2)$ is at least $2/3$ or at most $1/3$. Let $\{\lambda_k\}_{k\in[2^n]}$ be the eigenvalues of an n-qubit quantum state ρ. For any quantum state $\hat{\rho}$ having eigenvalues at most $1/n$, it follows that $\mathrm{Tr}(\hat{\rho}^2) = \sum_{k\in[2^n]} \lambda_k^2 \leq n \cdot n^{-2} = 1/n$, hence 0 provides a good estimate of $\mathrm{Tr}(\hat{\rho}^2)$ to within additive error $1/3$. This intuition implies that only sufficiently large eigenvalues contribute to estimating the value of $\mathrm{Tr}(\rho^2)$. Consequently, the computational complexity of Purity Estimation is supposed to be independent of the rank r.

However, this argument is just the first step towards establishing an efficient quantum estimator for $\mathrm{S}_q(\rho)$.[10] We also need to estimate $\sum_{k\in\mathcal{I}_{\mathrm{large}}} \lambda_k^q$, where $\mathcal{I}_{\mathrm{large}}$ is the index set for sufficiently large eigenvalue λ_k. For the case of integer $q > 1$, the approach of [BCWdW01, EAO+02] equipped with quantum amplitude estimation [BHMT02] provides a solution, whereas the case of non-integer $q \geq 1 + \Omega(1)$ is more challenging and requires more sophisticated techniques. Notably, the task is finally resolved by our first main result, as presented in Theorem 4.1.

Lastly, we provide our second main result, i.e., the computational hardness of TsallisQED$_q$ and TsallisQEA$_q$, as stated in Theorem 4.2. Let ConstRankTsallisQED$_q$ and ConstRankTsallisQEA$_q$ denote restricted variants of TsallisQED$_q$ and TsallisQEA$_q$, respectively, such that the ranks of the states of interest are at most $O(1)$.

Theorem 4.2 (Computational hardness of TsallisQED$_q$ and TsallisQEA$_q$, informal)**.** *The promise problems* TsallisQED$_q$ *and* TsallisQEA$_q$ *capture the computa-*

[7] In these bounds, $c > 0$ is a constant that can be made arbitrarily small, and we set $c' = 3c$.

[8] In the regime $1 \leq q \leq 1 + \frac{1}{n-1}$, as the rank r approaches 2^n, a sample complexity upper bound of $O(4^n/\epsilon^2)$ with better dependence on ϵ was given in [AISW20].

[9] As the rank r approaches 2^n, a better query complexity upper bound of $\widetilde{O}(2^n/\epsilon^{1.5})$ was shown in [GL20].

[10] A similar argument also applies to the classical Tsallis entropy, see [AOST17, Section III.C]. However, this type of argument does not extend to von Neumann entropy ($q = 1$), see [QKW24, Section 7].

tional power of their respective complexity classes in the corresponding regimes of q:[11]

(1) **Easy regimes:** *For any $q \in [1,2]$,* $\textsc{ConstRankTsallisQED}_q$ *is* BQP*-hard under Karp reduction, and consequently,* $\textsc{ConstRankTsallisQEA}_q$ *is* BQP*-hard under Turing reduction. As a corollary,* $\textsc{TsallisQED}_q$ *and* $\textsc{TsallisQEA}_q$ *are* BQP*-complete for $1 + \Omega(1) \leq q \leq 2$.*

(2) **Hard regimes:** *For any $q \in \left(1, 1 + \frac{1}{n-1}\right]$,* $\textsc{TsallisQED}_q$ *is* QSZK*-hard under Karp reduction, and consequently,* $\textsc{TsallisQEA}_q$ *is* QSZK*-hard under Turing reduction. Furthermore, for $q = 1 + \frac{1}{n-1}$,* $\textsc{TsallisQEA}_q$ *is* NIQSZK*-hard under Karp reduction.*

It is noteworthy that BQP-hardness under Turing reduction is as strong as BQP-hardness under Karp reduction, due to the BQP subroutine theorem [BBBV97].[12] Moreover, Theorem 4.2 implies a direct corollary, offering a positive answer to Question (ii):

Corollary 4.3. Purity Estimation *is* BQP*-hard.*

Interestingly, the BQP-hardness of a similar problem, specifically deciding whether $\mathrm{Tr}(\rho_0\rho_1)$ is at least $2/3$ or at most $1/3$, turns out to be not difficult to show.[13] However, this result does not imply Corollary 4.3.

4.1.2 Proof techniques: BQP containment for q constantly larger than 1

The proof of Theorem 4.1 consists of an efficient quantum (query) algorithm for estimating the value of $\mathrm{Tr}(\rho^q)$ for $q > 1$, given quantum query access to the state-preparation circuit Q of the mixed quantum state ρ. Our approach to estimating $\mathrm{Tr}(\rho^q)$ is via one-bit precision phase estimation [Kit95], also known as the Hadamard test [AJL09], equipped with the quantum singular value transformation (QSVT) [GSLW19]. Our algorithm is sketched in the following four steps (see Section 4.2 for more details):

1. Find a good polynomial approximation of x^{q-1}.
2. Implement a unitary block-encoding U of ρ^{q-1} using QSVT, with the state-preparation circuit Q.
3. Perform the Hadamard test on U and ρ with outcome $b \in \{0,1\}$.
4. One can learn the value of $\mathrm{Tr}(\rho^q)$ from a good estimate of b via quantum amplitude estimation.

The idea is simple. Similar ideas were ever used to estimate the fidelity [GP22], trace distance [WZ24a, LLW23], and von Neumann entropy [LLW23, WZ24b]. However, all of the aforementioned quantum algorithms have query or time complexity polynomials in the rank r of quantum states. Additionally, all these prior works rely on the quantum

[11] For detailed definitions of Karp reduction and Turing reduction, please refer to Chapter 2.

[12] Once we have an efficient quantum algorithm $\mathcal{A}$ for $\textsc{TsallisQEA}_q$, any problem in BQP can be solved using $\mathcal{A}$ as a subroutine. The BQP subroutine theorem, as stated in [BBBV97, Section 4], implies that $\mathsf{BQP}^{\mathcal{A}} \subseteq \mathsf{BQP}$.

[13] For any BQP circuit C_x, the acceptance probability $\||1\rangle\langle 1|_{\mathrm{out}} C_x|\bar{0}\rangle\|_2^2 = \mathrm{Tr}(\rho_0\rho_1)$, where $\rho_0 \coloneqq |1\rangle\langle 1|_{\mathrm{out}}$ and $\rho_1 \coloneqq \mathrm{Tr}_{\overline{\mathrm{out}}}(C_x|\bar{0}\rangle\langle\bar{0}|C_x^\dagger)$. Similar observations appeared in [Kob03, Theorem 9].

singular value transformation [GSLW19], which is a technique for designing quantum algorithms by approximating the target functions.[14] The main technical reason is that the functions to be approximated in their key steps are not smooth in the whole range of $[0,1]$, so they have to use the polynomial approximations of piece-wise smooth functions in [GSLW19, Corollary 23] to avoid the bad part (which is actually the regime of tiny eigenvalues);[15] this results in an estimation error dependent on r because, technically, the error for each bad eigenvalue has to be bounded individually (there are at most r bad eigenvalues), thereby introducing an (at least) linear r-dependence. Specifically, in their approaches, a target function $f(x)$ is specified and the goal is to estimate the value of $\mathrm{Tr}(\rho f(\rho))$. For example, $f(x) = -\log(x)$ for estimating the von Neumann entropy. The target function $f(x)$ is usually only approximated well in the range $x \in [\delta, 1]$ for some parameter δ, while leaving the rest range of x unspecified; more precisely, $f(x)$ is approximated by a polynomial $P(x)$ by, e.g., [GSLW19, Corollary 23], such that

$$\max_{x\in[\delta,1]} |P(x) - f(x)| \leq \epsilon, \ \max_{x\in[-1,1]} |P(x)| \leq 1, \text{ and } \deg(P) = O\Big(\frac{1}{\delta}\log\frac{1}{\epsilon}\Big). \tag{4.1}$$

Then, they instead estimate the value of $\mathrm{Tr}(\rho P(\rho))$. The intrinsic error turns out to be

$$\begin{aligned} |\mathrm{Tr}(\rho f(\rho)) - \mathrm{Tr}(\rho P(\rho))| &\leq \sum_{\lambda_j<\delta} |\lambda_j f(\lambda_j) - \lambda_j P(\lambda_j)| + \sum_{\lambda_j\geq\delta} |\lambda_j f(\lambda_j) - \lambda_j P(\lambda_j)| \\ &\leq r \cdot \mathrm{poly}(\delta) + O(\epsilon). \end{aligned}$$

Here, $\{\lambda_j\}_{1\leq j\leq 2^n}$ are the eigenvalues of the state ρ, with each λ_j satisfying $0 \leq \lambda_j \leq 1$. To make the intrinsic error bounded, δ must be sufficiently small, e.g., $\delta = 1/\mathrm{poly}(r)$.

The above standard method has drawbacks: the intrinsic error is $r \cdot \mathrm{poly}(\delta)$ for the small-eigenvalue part and $O(\epsilon)$ for the large-eigenvalue part. While the ϵ-dependence in the approximation degree is logarithmic (and thus not the dominating term), the δ-dependence is significant. This suggests the need for the following trade-off: Can we reduce the error caused by the small-eigenvalue part, at the cost of a possibly worse error caused by the large-eigenvalue part?

To make this trade-off possible for our purpose, we turn to find polynomials that uniformly approximate the positive power functions. This is inspired by the Stone-Weierstrass theorem, stating that any continuous function (e.g., x^q) on a closed interval (e.g., $[0,1]$) can be uniformly approximated by polynomials. The study of the *best uniform approximation* (by polynomials)[16] of positive power functions was initiated by Bernstein [Ber14, Ber38] almost a century ago in an abstract manner.[17] The best uniform approximation polynomial of x^q was shown with a non-constructive proof in [Tim63, Section 7.1.41], stating that there is a family of polynomials $P_d(x)$ of degree d such that

$$\max_{x\in[0,1]} |P_d(x) - x^q| \to \frac{1}{d^q}, \text{ as } d \to \infty, \tag{4.2}$$

whose approximation range is in sharp contrast to that in Equation (4.1). However, the

[14] For example, estimating the fidelity and trace distance requires to approximate the sign function; and estimating the von Neumann entropy requires to approximate the logarithmic function.

[15] These eigenvalues correspond to the inputs of the target function.

[16] The best uniform approximation polynomial of a continuous function $f(x)$ on $[-1,1]$ is a degree-d polynomial that minimizes $\max_{x\in[-1,1]} |f(x) - P_d(x)|$ over all degree-d polynomials P_d. For a formal definition, see Section 2.3.

[17] Actually, the function $|x|^q$ for $x \in [-1,1]$ is commonly considered in the literature. Nevertheless, we are only interested in the non-negative part, i.e., the range $[0,1]$.

coefficients of the leading error terms and the explicit construction of these polynomial approximations seem still not fully understood (e.g., [Gan02]). Consequently, it is somewhat challenging to directly use such polynomial approximations (e.g., [Tim63, Section 7.1.41]) in a time-efficient manner.

Inspired by the result of the best uniform approximation of positive power functions in [Tim63], we, instead, aim to find a good enough uniform approximation that is also efficiently computable. This is achieved by employing the construction of asymptotically best uniform approximation via combining Chebyshev truncations and the de La Vallée Poussin partial sum (cf. [Riv90, Chapter 3]). Finally, we obtain a family of efficiently computable uniform approximation polynomials of (scaled) x^q that are suitable for QSVT:

$$\max_{x\in[0,1]}\left|P(x)-\frac{1}{2}x^q\right|\leq\epsilon,\ \max_{x\in[-1,1]}|P(x)|\leq 1,\ \text{and}\ \deg(P)=O\left(\frac{1}{\epsilon^{1/q}}\right). \tag{4.3}$$

Using these efficiently computable uniform approximation polynomials, we are able to give a quantum algorithm for estimating $\mathrm{Tr}(\rho^q)$. First, we approximate the function x^{q-1} in the range $[0,1]$ to error ϵ by a polynomial of degree $O(1/\epsilon^{\frac{1}{q-1}})$. Then, we can apply the algorithm sketched at the very beginning of this subsection. With further analysis, we can estimate the value of $\mathrm{Tr}(\rho^q)$ to additive error ϵ with quantum query complexity $O(1/\epsilon^{1+\frac{1}{q-1}})$, as stated in Theorem 4.5. Using the same idea, we can also estimate $\mathrm{Tr}(\rho^q)$ to additive error ϵ by using $\widetilde{O}(1/\epsilon^{3+\frac{2}{q-1}})$ copies of ρ through the samplizer [WZ24b], as presented in Theorem 4.6.

To conclude this subsection, it can be seen that our quantum algorithm for estimating $\mathrm{Tr}(\rho^q)$ is naturally applicable to solving $\textsc{TsallisQED}_q$ and $\textsc{TsallisQEA}_q$. Particularly for the precision in the regime $1/\mathrm{poly}(n)\leq\epsilon\leq 1$, the efficiently-computability of the uniform approximation polynomials in Equation (4.3) ensures that the description of the quantum circuit of our algorithm can be computed by a classical deterministic Turing machine in $\mathrm{poly}(n)$ time, which is a significant step to show the BQP-completeness of $\textsc{TsallisQED}_q$ and $\textsc{TsallisQEA}_q$ for $1+\Omega(1)\leq q\leq 2$ and precision $1/\mathrm{poly}(n)\leq\epsilon\leq 1$.

4.1.3 Proof techniques: Hardness via QJT_q-based reductions

Before we proceed with the proof of Theorem 4.2, we start by reviewing the definition of the (white-box) quantum state testing problem with respect to the trace distance (QSD). For simplicity, we adopt a slightly restrictive definition, particularly $\mathrm{QSD}[1-\epsilon(n),\epsilon(n)]$, which corresponds to Definition 3.33 with $\alpha(n)=1-\epsilon(n)$ and $\beta(n)=\epsilon(n)$. Additionally, the two variants of QSD, specifically PureQSD and QSCMM, as defined in Section 3.3, are also involved.

The proof of Theorem 4.2, particularly the hardness results under Karp reduction, uses reductions from the aforementioned variants of QSD to $\textsc{TsallisQED}_q$ or $\textsc{TsallisQEA}_q$ for the respective ranges of q. Next, we will specify two main technical challenges related to the corresponding inequalities necessary for establishing Theorem 4.2:

(1) For $\textsc{ConstRankTsallisQED}_q$ and $\textsc{TsallisQED}_q$, the key ingredient of these reductions is the quantum q-Jensen-(Shannon-)Tsallis divergence (QJT_q, see Definition 3.29), first introduced in [BH09]. We notice that QJT_q can be viewed as

a *distance version* of the quantum q-Tsallis entropy difference for $1 \leq q \leq 2$,[18] and consequently, these reductions heavily rely on the inequalities between QJT_q and the trace distance. However, such inequalities are only known for the case of $q = 1$ [FvdG99, Hol73a, BH09], presenting the first technical challenge.

(2) For $\textsc{TsallisQEA}_q$, the reduction essentially relies on the lower and upper bounds on the quantum q-Tsallis entropy of a quantum state ρ in terms of the trace distance between the state and the maximally mixed state, when the trace distance is promised to be a fixed value. These bounds are also only known for the case of $q = 1$ [Vaj70, CCKV08, KLN19], leading to the second technical challenge.

For clarity, we summarize the correspondence between our reductions for establishing Theorem 4.2 and the new inequalities in Table 4.3. The definition and properties of the q-logarithm, $\ln_q(x)$, are provided at the beginning of Chapter 2.

Problem	Regime of q	Reduction from	New inequalities
$\textsc{ConstRank}$ $\textsc{TsallisQED}_q$ Theorem 4.2(1)	$1 \leq q \leq 2$	$\textsc{PureQSD}$ is BQP-hard adapted from [RASW23]	$\mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q\left(\frac{1-\mathrm{T}}{2}\right) \leq \mathrm{QJT}_q \leq \mathrm{H}_q\left(\frac{1}{2}\right)\mathrm{T}^q$ Theorem 4.7
$\textsc{TsallisQED}_q$ Theorem 4.2(2)	$1 \leq q \leq 1+\frac{1}{n-1}$	QSD is QSZK-hard [Wat02, Wat09b]	$\mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q\left(\frac{1-\mathrm{T}}{2}\right) \leq \mathrm{QJT}_q$ Theorem 4.7
$\textsc{TsallisQEA}_q$ Theorem 4.2(2)	$q = 1+\frac{1}{n-1}$	QSCMM is NIQSZK-hard [Kob03, BASTS10, CCKV08]	$\left(1-\mathrm{T}-\frac{1}{2^n}\right)\ln_q(2^n) \leq \mathrm{S}_q \leq \ln_q(2^n(1-\mathrm{T}))$ Lemma 4.16

Table 4.3: Reductions for $\textsc{TsallisQED}_q$ and $\textsc{TsallisQEA}_q$, and the related inequalities.

Once we have established these new inequalities, together with our new bounds for the Tsallis binary entropy $\mathrm{H}_q(x) \leq \mathrm{H}_q\left(\frac{1}{2}\right)\sqrt{4x(1-x)}$ (see Theorem 4.8, where previously only the case of $q = 1$ was known [Lin91, Top01]), we can establish our three hardness results under Karp reduction in Theorem 4.2 through relatively complicated and detailed analyses. The additional two hardness results for $\textsc{ConstRankTsallisQEA}_q$ and $\textsc{TsallisQEA}_q$ under Turing reduction in Theorem 4.2 follow straightforwardly from a binary search for promise problems.

In the remainder of this subsection, we provide insights into proving the new inequalities in Table 4.3. The first technical challenge involves establishing the inequalities between QJT_q and the trace distance. The main barrier is to provide the data-processing inequality $\mathrm{QJT}_q(\Phi(\rho_0), \Phi(\rho_1)) \leq \mathrm{QJT}_q(\rho_0, \rho_1)$ for $1 < q \leq 2$.[19] This implies that applying any quantum channel Φ on states ρ_0 and ρ_1 does not increase the divergence between

[18] For the case of $q = 1$, similar observations are implicitly used to show that QED is QSZK-hard [BASTS10], and recently explicitly emphasized in [Liu23] (see Chapter 7), leading to a simple proof for the QSZK hardness of QED.

[19] We generalize the approach in [BH09] for $q = 1$. Using the data-processing inequality with a measurement channel, we can establish the lower bound via the measured version of QJT_q (see Equation (3.2)) and the classical counterpart inequality for JT_q in [BH09]. For the upper bound, we construct new states $\hat{\rho}_0$ and $\hat{\rho}_1$ with an ancillary qubit, making $\mathrm{QJT}_q(\hat{\rho}_0, \hat{\rho}_1)$ related to the trace distance for $1 < q \leq 2$ (and coincide with the trace distance for $q = 1$). Applying the data-processing inequality with the partial trace, we obtain $\mathrm{QJT}_q(\rho_0, \rho_1) \leq \mathrm{QJT}_q(\hat{\rho}_0, \hat{\rho}_1)$.

them. For $q = 1$, the quantum Jensen-Shannon divergence (QJS), defined in [MLP05], can be decomposed into a sum of quantum relative entropy $\mathrm{D}(\rho_0\|\rho_1)$:

$$\mathrm{QJS}(\rho_0, \rho_1) \coloneqq \mathrm{S}\left(\frac{\rho_0+\rho_1}{2}\right) - \frac{\mathrm{S}(\rho_0)+\mathrm{S}(\rho_1)}{2} = \frac{1}{2}\left(\mathrm{D}\left(\rho_0\middle\|\frac{\rho_0+\rho_1}{2}\right) + \mathrm{D}\left(\rho_1\middle\|\frac{\rho_0+\rho_1}{2}\right)\right). \tag{4.4}$$

Since the data-processing inequality (essentially, the joint convexity) for the quantum relative entropy was established decades ago [Lie73, Uhl77], and given the equality in Equation (4.4), it directly follows that the data-processing inequality also holds for QJS. However, a similar decomposition does not apply to the quantum q-Tsallis entropy when $q \neq 1$. Fortunately, the joint convexity of QJT_q for $1 \leq q \leq 2$, specifically,

$$\mathrm{QJT}_q((1-\lambda)\rho_0 + \lambda\rho_0', (1-\lambda)\rho_1 + \lambda\rho_1') \leq (1-\lambda)\mathrm{QJT}_q(\rho_0, \rho_1) + \lambda\mathrm{QJT}_q(\rho_0', \rho_1'),$$

was established few years ago [CT14, Vir19], where $0 < \lambda < 1$. As a consequence, once we establish the data-processing inequality for QJT_q, we can then generalize the inequalities between QJS and the trace distance to QJT_q for $1 \leq q \leq 2$, using the same approach applied to QJS.

For the second technical challenge, i.e., the bounds for $\mathrm{S}_q(\rho)$ when $\mathrm{T}(\mathrm{S}_q(\rho), (I/2)^{\otimes n}) = \gamma$ is fixed, it suffices to focus on the classical counterpart,[20] as the maximally mixed state commutes with any state ρ. The lower bound can be established by following the approach in [KLN19] for $q = 1$. On the other hand, the upper bound for $q = 1$ can be derived using Vajda's inequality [Vaj70], but similar results for $q \neq 1$ are unknown. However, by assuming an appropriate condition between q and the fixed distance γ, we can deduce an upper bound analogous to the $q = 1$ case.

4.2 Efficient quantum algorithms for estimating q-quantum Tsallis entropy

In this section, we propose efficient quantum algorithms for estimating the quantum Tsallis entropy $\mathrm{S}_q(\rho)$ when $q \geq 1 + \Omega(1)$, using either queries to the state-preparation circuit or samples of the state ρ. The key ingredient underlying our algorithms is an *efficient* uniform approximation to positive constant power functions. Specifically, our polynomial approximation (Lemma 4.4) is "full-range", meaning it maintains a uniform error bound across the entire interval $[-1, 1]$. This differs from the polynomial approximations commonly used in QSVT, which typically provide separate error bounds for the intervals $[-\delta, \delta]$ and $[-1, -\delta) \cup (\delta, 1]$.

Utilizing our "full-range" polynomial approximation, we construct a query-efficient quantum algorithm for estimating $\mathrm{Tr}(\rho^q)$, as established in Theorem 4.5. Consequently, our quantum query algorithm (Theorem 4.5) directly leads to BQP containments of the promise problems $\textsc{TsallisQEA}_q$ and $\textsc{TsallisQED}_q$, defined in Section 4.4. Furthermore, by employing the samplizer in [WZ24b], we develop a sample-efficient quantum algorithm for estimating $\mathrm{Tr}(\rho^q)$, as presented in Theorem 4.6.

[20] Let p denote the distribution of the eigenvalues of ρ, and let ν be the uniform distribution over 2^n items. This task is exactly equivalent to proving the bounds for $\mathrm{H}_q(p)$ when $\mathrm{TV}(p, \nu) = \gamma$ is fixed.

4.2.1 Efficient uniform approximations to positive constant power functions

We start by establishing an efficiently computable uniform approximation to positive constant powers:

Lemma 4.4 (Efficient uniform polynomial approximation to positive constant powers)**.** *Let r be a positive integer and let α be a real number in $(-1,1)$. For any $\epsilon \in (0,1/2)$, there is a degree-d polynomial $P_d \in \mathbb{R}[x]$, where $d = \left\lceil (\beta'_\alpha/\epsilon)^{\frac{1}{r+\alpha}} \right\rceil$ and β'_α is a constant depending on α, that can be deterministically computed in $\widetilde{O}(d)$ time. For sufficiently small ϵ, it holds that*:

$$\max_{x\in[-1,1]} \left| \frac{1}{2} x^{r-1}|x|^{1+\alpha} - P_d(x) \right| \le \epsilon \text{ and } \max_{x\in[-1,1]} |P_d(x)| \le 1.$$

Furthermore, P_d has the same parity as the integer $r-1$.

Proof. Let $f(x) \coloneqq \frac{1}{2}x^{r-1}|x|^{1+\alpha}$. For any $\tilde{\epsilon} \in (0,1/8)$, using Lemma 2.7, we obtain the degree-$\tilde{d}$ best polynomial approximation $P^*_{\tilde{d}}(x)$, where $\tilde{d} = \left\lceil (\beta_\alpha/\tilde{\epsilon})^{\frac{1}{r+\alpha}} \right\rceil$ and β_α is a constant depending on α, such that

$$\max_{x\in[-1,1]} \left| \frac{1}{2} x^{r-1}|x|^{1+\alpha} - P^*_{\tilde{d}}(x) \right| \le \tilde{\epsilon} \text{ and } \max_{x\in[-1,1]} \left| P^*_{\tilde{d}}(x) \right| \le \frac{1}{2} + \tilde{\epsilon}. \tag{4.5}$$

Next, we consider the degree-$\tilde{d}$ averaged Chebyshev truncation (Equation (2.3)) of $f(x)$. In particular, let $d \coloneqq 2\tilde{d}-1 = \left\lceil (\beta'_\alpha/\epsilon)^{\frac{1}{r+\alpha}} \right\rceil$, where β'_α is another constant depending on α and ϵ will be specified later. We obtain the following degree-d polynomial:

$$P_d(x) = \frac{\hat{c}_0}{2} + \sum_{k=1}^{d} \hat{c}_k T_k(x), \text{ where } \hat{c}_k \coloneqq \begin{cases} c_k, & 0 \le k \le \tilde{d} \\ \frac{2\tilde{d}-k}{\tilde{d}} c_k, & k > \tilde{d} \end{cases} \text{ and } c_k \coloneqq \langle T_k, f \rangle. \tag{4.6}$$

By leveraging the asymptotically best approximation by averaged Chebyshev truncation (Lemma 2.11) and Equation (4.5), we can derive that $P_d(x)$ satisfies the following:

$$\max_{x\in[-1,1]} \left| \frac{1}{2} x^{r-1}|x|^{1+\alpha} - P_d(x) \right| \le 4\tilde{\epsilon} \coloneqq \epsilon \text{ and } \max_{x\in[-1,1]} |P_d(x)| \le \frac{1}{2} + 4\tilde{\epsilon} = \frac{1}{2} + \epsilon < 1.$$

It remains to show that $P_d(x)$ can be computed in deterministic time $\widetilde{O}(d)$. A straightforward calculation implies that the Chebyshev coefficient $\{c_k\}_{0\le k\le d}$ in Equation (4.6) satisfy the following:

$$\begin{aligned} c_{2l+1} &= c_{2l-1} \cdot \frac{r+\alpha-2l+1}{r+\alpha+2l+1}, \quad c_{2l} = c_{2l-2} \cdot \frac{r+\alpha-2l+2}{r+\alpha+2l}, \\ c_0 &= \frac{2}{\pi} \int_{-1}^{1} \frac{\frac{1}{2}x^{r-1}|x|^{1+\alpha} \cdot T_0(x)}{\sqrt{1-x^2}} \mathrm{d}x = -\frac{-1+(-1)^r}{2\sqrt{\pi}} \cdot \frac{\Gamma\left(\frac{1}{2}(r+\alpha+1)\right)}{\Gamma\left(\frac{1}{2}(r+\alpha+2)\right)}, \\ c_1 &= \frac{2}{\pi} \int_{-1}^{1} \frac{\frac{1}{2}x^{r-1}|x|^{1+\alpha} \cdot T_1(x)}{\sqrt{1-x^2}} \mathrm{d}x = \frac{1+(-1)^r}{2\sqrt{\pi}} \cdot \frac{\Gamma\left(\frac{1}{2}(r+\alpha+2)\right)}{\Gamma\left(\frac{1}{2}(r+\alpha+3)\right)}. \end{aligned}$$

Here, the Gamma function $\Gamma(x) \coloneqq \int_0^\infty t^{x-1}e^{-x}\mathrm{d}t$ for any $x > 0$.

Consequently, we can recursively compute the averaged Chebyshev coefficient $\{\hat{c}_k\}_{0\le k\le d}$ in deterministic time $\widetilde{O}(d)$. We complete the proof by noting that the Chebyshev poly-

nomials $\{T_k(x)\}_{0\le k\le d}$ also can be recursively computed in deterministic time $\widetilde{O}(d)$. □

4.2.2 Quantum q-Tsallis entropy approximation for q constantly larger than 1

Query-efficient quantum algorithm for estimating $\mathrm{Tr}(\rho^q)$. We now present efficient quantum query algorithms for estimating the q-Tsallis entropy of a mixed quantum state. For readability, their framework is given in Algorithm 4.2.1.

Algorithm 4.2.1: A framework for estimating q-Tsallis entropy for $q \ge 1+\Omega(1)$ (query access).

Input : A quantum circuit Q that prepares a purification of an n-qubit mixed quantum state ρ, and a precision parameter $\epsilon \in (0,1)$.
Output: A single bit $b \in \{0,1\}$ such that $\Pr[b=0] \approx \frac{1}{2} + \frac{1}{8}\mathrm{Tr}(\rho^q)$.
1. Implement a unitary operator U_ρ that is a block-encoding of ρ by Lemma 2.18, using $O(1)$ queries to Q.
2. Let $P(x)$ be a polynomial that approximates $\frac{1}{4}x^{q-1}$ in the range $[0,1]$, where $P(x)$ is determined according to ϵ, n, and q. More precisely, for constant $q>1$, $P(x)$ is chosen by Lemma 4.4.
3. Implement a unitary operator $U_{P(\rho)}$ that is a block-encoding of $P(\rho)$ by quantum singular value transformation (Lemma 2.21), using $O(\deg(P))$ queries to U_ρ.
4. Perform the Hadamard test on ρ and $U_{P(\rho)}$ by Lemma 2.19, and return the measurement outcome.

Theorem 4.5 (Trace estimation of quantum state constant powers via queries)**.** *Suppose that Q is a unitary operator that prepares a purification of mixed quantum state ρ. For every $q \ge 1+\Omega(1)$, there is a quantum query algorithm that estimates $\mathrm{Tr}(\rho^q)$ to within additive error ϵ by using $O(1/\epsilon^{1+\frac{1}{q-1}})$ queries to Q.*

Proof. Let Q be an $(n+a)$-qubit unitary operator that prepares a purification of the n-qubit mixed quantum state ρ. Then, by Lemma 2.18, we can implement a unitary operator U_ρ that is a $(1,n+a,0)$-block-encoding of ρ, by using $O(1)$ queries to Q.

Let $\epsilon_p \in (0,1)$ be a parameter to be determined later. By Lemma 4.4 with $r := \max\{\lfloor q-1 \rfloor, 1\}$, $\alpha := q-1-r$, and $\epsilon := \epsilon_p$, there exists a polynomial $P \in \mathbb{R}[x]$ of degree $d = O(1/\epsilon_p^{\frac{1}{q-1}})$ such that

$$\max_{x\in[0,1]} \left| P(x) - \frac{1}{2}x^{q-1} \right| \le \epsilon_p, \quad \text{and} \max_{x\in[-1,1]} |P(x)| \le 1.$$

By Lemma 2.21 with $P := \frac{1}{2}P$, $\alpha := 1$, $a := n+a$, $\epsilon := 0$ and $d := O(1/\epsilon_p^{\frac{1}{q-1}})$, we can implement a quantum circuit $U_{P(\rho)}$ that is a $(1,n+a+2,\delta)$-block-encoding of $\frac{1}{2}P(\rho)$, by using $O(1/\epsilon_p^{\frac{1}{q-1}})$ queries to U_ρ. Moreover, the classical description of $U_{P(\rho)}$ can be computed in deterministic time $\mathrm{poly}(1/\epsilon_p, \log(1/\delta))$.

Suppose that $U_{P(\rho)}$ is a $(1,n+a+2,0)$-block-encoding of A, i.e., $\|A - \frac{1}{2}P(\rho)\| \le \delta$. Then, by Lemma 2.19, we can obtain an estimate $\tilde{x}$ of $\mathrm{Tr}(A\rho)$ to within additive error

ϵ_H by using $O(1/\epsilon_H)$ queries to each of $U_{P(\rho)}$ and Q such that

$$\Pr\Big[|\tilde{x} - \mathrm{Tr}(A\rho)| \leq \epsilon_H\Big] \geq \frac{2}{3}. \tag{4.7}$$

In the overall quantum circuit to obtain $\tilde{x}$, the number of queries to Q is

$$O\Big(\frac{1}{\epsilon_H}\Big) \cdot O\Big(\frac{1}{\epsilon_p^{1/(q-1)}}\Big) = O\Big(\frac{1}{\epsilon_H \epsilon_p^{1/(q-1)}}\Big),$$

and the number of one- and two-qubit quantum gates is

$$O\Big(\frac{n+a}{\epsilon_H \epsilon_p^{1/(q-1)}}\Big).$$

Moreover, the classical description of the overall quantum circuit can be computed in deterministic time $\mathrm{poly}(1/\epsilon_p, 1/\epsilon_H, \log(1/\delta))$.

On the other hand, we have

$$\Big|\mathrm{Tr}(A\rho) - \mathrm{Tr}\Big(\frac{1}{2}P(\rho)\rho\Big)\Big| \leq \Big\|A - \frac{1}{2}P(\rho)\Big\| \leq \delta, \tag{4.8}$$

where we use the inequality $|\mathrm{Tr}(AB)| \leq \|A\|\mathrm{Tr}(|B|)$ (which is a special case of the matrix Hölder inequality, e.g., [Bau11, Theorem 2]). We also have

$$\Big|\mathrm{Tr}\Big(\frac{1}{2}P(\rho)\rho\Big) - \mathrm{Tr}\Big(\frac{1}{4}\rho^q\Big)\Big| \leq \frac{1}{2}\epsilon_p. \tag{4.9}$$

To see Equation (4.9), suppose that $\rho = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$ is the spectrum decomposition of ρ with $\lambda_j \geq 0$ for all j and $\sum_j \lambda_j = 1$. Then,

$$\begin{aligned}
\Big|\mathrm{Tr}\Big(\frac{1}{2}P(\rho)\rho\Big) - \mathrm{Tr}\Big(\frac{1}{4}\rho^q\Big)\Big| &= \Big|\sum_j \Big(\frac{1}{2}P(\lambda_j)\lambda_j - \frac{1}{4}\lambda_j^q\Big)\Big| \\
&\leq \sum_j \frac{1}{2}\lambda_j \Big|P(\lambda_j) - \frac{1}{2}\lambda_j^{q-1}\Big| \\
&\leq \frac{1}{2}\sum_j \lambda_j \epsilon_p = \frac{1}{2}\epsilon_p.
\end{aligned}$$

Finally, by combining Equations (4.7) to (4.9), we obtain

$$\Pr\Big[|4\tilde{x} - \mathrm{Tr}(\rho^q)| \leq 2\epsilon_p + 4\epsilon_H + 4\delta\Big] \geq \frac{2}{3}.$$

To make $4\tilde{x}$ an ϵ-estimate of $\mathrm{Tr}(\rho^q)$ with high probability, it is sufficient to take $\epsilon_p = \epsilon_H = \delta = \epsilon/10$, thereby the required number of queries to Q is

$$O\Big(\frac{1}{\epsilon^{1+1/(q-1)}}\Big).$$

□

Sample-efficient quantum algorithm for estimating $\mathrm{Tr}(\rho^q)$**.** We also study the sample complexity for the trace estimation of quantum state powers, which is obtained by extending the quantum query algorithm in Theorem 4.5 via the samplizer in Lemma 2.23. An illustrative framework is given in Algorithm 4.2.2.

Theorem 4.6 (Trace estimation of quantum state constant powers via samples)**.** *For every $q \geq 1 + \Omega(1)$, there is a quantum sample algorithm that estimates $\mathrm{Tr}(\rho^q)$ to within additive error ϵ by using $\widetilde{O}(1/\epsilon^{3+\frac{2}{q-1}})$ samples of ρ.*

Algorithm 4.2.2: A framework for estimating q-Tsallis entropy for $q \geq 1+\Omega(1)$ (sample access).

Input : Independent and identical samples of an n-qubit mixed quantum state ρ, and parameters $q > 1$ and $\delta, \epsilon_p, \delta_p \in (0,1)$.

Output: A single bit $b \in \{0,1\}$ such that $\Pr[b=0] \approx \frac{1}{2} + \frac{1}{2^{q+3}}\mathrm{Tr}(\rho^q)$.

Function $\texttt{ApproxPower}(q, \epsilon_p, \delta_p)^U$

- **Input :** A unitary $(1, a, 0)$-block-encoding U of A, and parameters $q > 1, \epsilon_p, \delta_p \in (0,1)$.
- **Output:** A unitary operator $\widetilde{U}$.
- **a.** Let $P(x)$ be a polynomial of degree $d = O(1/\epsilon_p^{\frac{1}{q-1}})$ such that $\max_{x\in[0,1]}|P(x) - \frac{1}{2}x^{q-1}| \leq \epsilon_p$ and $\max_{x\in[-1,1]}|P(x)| \leq 1$ (by Lemma 4.4).
- **b.** Construct a unitary $(1, a+2, \delta_p)$-block-encoding $\widetilde{U}$ of $\frac{1}{2}P(A)$ (by Lemma 2.21).
- **c.** Return $\widetilde{U}$.

1. Let b' be the outcome of the Hadamard test (by Lemma 2.19) performing on the quantum state ρ and $\mathsf{Samplize}_\delta\langle\texttt{ApproxPower}(q, \epsilon_p, \delta_p)^U\rangle[\rho]$ (as if it were unitary).

2. Return b'.

Proof. Let unitary operator U be a $(1, a, 0)$-block-encoding of A for some $a > 0$. Let $\epsilon_p, \delta_p \in (0,1)$ be parameters to be determined. Using Lemma 4.4 with the parameters $r := \max\{\lfloor q-1 \rfloor, 1\}$, $\alpha := q-1-r$, and $\epsilon := \epsilon_p$, there is a polynomial $P \in \mathbb{R}[x]$ of degree $d = O(1/\epsilon_p^{\frac{1}{q-1}})$ such that

$$\max_{x\in[0,1]}\left|P(x) - \frac{1}{2}x^{q-1}\right| \leq \epsilon_p \text{ and } \max_{x\in[-1,1]}|P(x)| \leq 1.$$

By Lemma 2.21 with $P := \frac{1}{2}P$, $\alpha := 1$, $a := n + a$, $\epsilon := 0$, $\delta := \delta_p$ and $d := O(1/\epsilon_p^{\frac{1}{q-1}})$, we can implement a quantum circuit $U_{P(A)}$ that is a $(1, n+a+2, \delta_p)$-block-encoding of $\frac{1}{2}P(A)$, by using $O(1/\epsilon_p^{\frac{1}{q-1}})$ queries to U. Moreover, the classical description of $U_{P(A)}$ can be computed in deterministic time $\mathrm{poly}(1/\epsilon_p, \log(1/\delta_p))$. Let $\texttt{ApproxPower}(q, \epsilon_p, \delta_p)^U$ denote the procedure of implementing $U_{P(A)}$ by using queries to U.

For our purpose, we take $A := \rho/2$. Suppose that $U_{P(\frac{\rho}{2})}$ is a $(1, n+a+2, 0)$-block-encoding of B, then $\|B - \frac{1}{2}P(\frac{\rho}{2})\| \leq \delta_p$. Let $b \in \{0,1\}$ be the outcome of the Hadamard test (by Lemma 2.19) on ρ and $U_{P(\frac{\rho}{2})}$, then

$$\Pr[b=0] = \frac{1}{2} + \frac{1}{2}\,\mathrm{Re}[\mathrm{Tr}(B\rho)]. \tag{4.10}$$

Let $\delta \in (0,1)$ be a parameter to be determined, and let $b' \in \{0,1\}$ be the outcome of the Hadamard test (by Lemma 2.19) on ρ and $\mathsf{Samplize}_\delta\langle\texttt{ApproxPower}(q, \epsilon_p, \delta_p)^U\rangle[\rho]$ (as if it were $U_{P(\frac{\rho}{2})}$). Then,

$$\left|\Pr[b=0] - \Pr[b'=0]\right| \leq \delta. \tag{4.11}$$

Now we repeat the Hadamard test k times, obtaining outcomes $b'_1, b'_2, \ldots, b'_k \in \{0,1\}$, where k is an integer to be determined. Let $X = \frac{1}{k}\sum_{j=1}^k b'_j$. Then, by the Hoeffding

bound (e.g., [MU17, Theorem 4.12]), we have

$$\Pr[|X - \mathbb{E}[b']| \leq \epsilon_H] \geq 1 - 2\exp\left(-2k\epsilon_H^2\right). \tag{4.12}$$

On the other hand, similar to the proof of Theorem 4.5, we have

$$\begin{aligned}\left|\mathrm{Re}[\mathrm{Tr}(B\rho)] - \mathrm{Tr}\left(\frac{1}{2}P\left(\frac{\rho}{2}\right)\rho\right)\right| &\leq \left|\mathrm{Tr}(B\rho) - \mathrm{Tr}\left(\frac{1}{2}P\left(\frac{\rho}{2}\right)\rho\right)\right| \\ &\leq \left\|B - \frac{1}{2}P\left(\frac{\rho}{2}\right)\right\| \\ &\leq \delta_p.\end{aligned} \tag{4.13}$$

We also have

$$\left|\mathrm{Tr}\left(\frac{1}{2}P\left(\frac{\rho}{2}\right)\rho\right) - \mathrm{Tr}\left(\frac{1}{2^{q+2}}\rho^q\right)\right| \leq \frac{1}{2}\epsilon_p. \tag{4.14}$$

To see Equation (4.9), suppose that $\rho = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$ is the spectrum decomposition of ρ with $\lambda_j \geq 0$ for all j and $\sum_j \lambda_j = 1$. Then,

$$\begin{aligned}\left|\mathrm{Tr}\left(\frac{1}{2}P\left(\frac{\rho}{2}\right)\rho\right) - \mathrm{Tr}\left(\frac{1}{2^{q+2}}\rho^q\right)\right| &= \left|\sum_j \left(\frac{1}{2}P\left(\frac{\lambda_j}{2}\right)\lambda_j - \frac{1}{2^{q+2}}\lambda_j^q\right)\right| \\ &\leq \sum_j \frac{1}{2}\lambda_j \left|P\left(\frac{\lambda_j}{2}\right) - \frac{1}{2}\left(\frac{\lambda_j}{2}\right)^{q-1}\right| \\ &\leq \frac{1}{2}\sum_j \lambda_j \epsilon_p = \frac{1}{2}\epsilon_p.\end{aligned}$$

Finally, by combining Equations (4.10) to (4.14), we obtain

$$\Pr\left[\left|2^{q+2}(1-2X) - \mathrm{Tr}(\rho^q)\right| \leq 2^{q+1}(4\delta + 4\epsilon_H + 2\delta_p + \epsilon_p)\right] \geq 1 - 2\exp(-2k\epsilon_H^2).$$

By taking $\delta = \epsilon_H = \delta_p = \epsilon_p := 2^{-q-5}\epsilon$ and $k := \left\lceil \frac{\ln(6)}{2\epsilon_H^2} \right\rceil$, we have

$$\Pr\left[\left|2^{q+2}(1-2X) - \mathrm{Tr}(\rho^q)\right| \leq \epsilon\right] \geq \frac{2}{3},$$

which means that $2^{q+2}(1-2X)$ is an ϵ-estimate of $\mathrm{Tr}(\rho^q)$ with high probability.

To complete the proof, we analyze the sample complexity of our algorithm. The algorithm consists of k repetitions of the Hadamard test, where each repetition requires one sample of ρ and one call to $\mathsf{Samplize}_\delta\langle\mathtt{ApproxPower}(q, \epsilon_p, \delta_p)^U\rangle[\rho]$. Here, $\mathtt{ApproxPower}(q, \epsilon_p, \delta_p)^U$ uses $O(1/\epsilon_p^{\frac{1}{q-1}})$ queries to U. Hence, by applying Lemma 2.23, we can implement $\mathsf{Samplize}_\delta\langle\mathtt{ApproxPower}(q, \epsilon_p, \delta_p)^U\rangle[\rho]$ by using $\widetilde{O}(1/(\delta\epsilon_p^{\frac{2}{q-1}}))$ samples of ρ. Therefore, the total number of samples of ρ is

$$k \cdot \widetilde{O}\left(\frac{1}{\delta\epsilon_p^{2/(q-1)}}\right) = \widetilde{O}\left(\frac{1}{\epsilon^{3+2/(q-1)}}\right). \qquad \square$$

4.3 Properties of quantum Jensen-Tsallis divergence and Tsallis entropy

In this section, we present inequalities between the quantum q-Jensen-Tsallis divergence ($1 \leq q \leq 2$) and the trace distance. Our results extend the previous results for the quantum Jensen-Shannon divergence ($q = 1$, see [BH09, Theorem 14]):

Theorem 4.7 (QJT_q vs. T)**.** *For any quantum states ρ_0 and ρ_1, and $1 \le q \le 2$, we have*:

$$\mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q\left(\frac{1-\mathrm{T}(\rho_0,\rho_1)}{2}\right) \le \mathrm{QJT}_q(\rho_0,\rho_1) \le \mathrm{H}_q\left(\frac{1}{2}\right)\cdot \mathrm{T}(\rho_0,\rho_1)^q.$$

To prove Theorem 4.7, we first need to prove the data-processing inequality for QJT_q (Lemma 4.11), which crucially relies on the relatively recent results on the *joint convexity* of QJT_q [CT14, Vir19]. Consequently, we can establish Theorem 4.7 by proving the inequalities in Section 4.3.2. In particular, the lower bound on QJT_q in terms of T (Lemma 4.12) holds for $q \in [1,2]$, and the upper bound on QJT_q in terms of T (Lemma 4.13) for the same range of q.

Next, to utilize Lemma 4.12, we provide bounds of the Tsallis binary entropy in Section 4.3.3:

Theorem 4.8 (Tsallis binary entropy bounds)**.** *For any $p = (x, 1-x)$, let $\mathrm{H}_q(x)$ denote the Tsallis binary entropy with $1 \le q \le 2$, we have*:

$$\mathrm{H}_q(1/2)\cdot 4x(1-x) \le \mathrm{H}_q(x) \le \mathrm{H}_q(1/2)\cdot (4x(1-x))^{1/2}.$$

It is noteworthy that the best known bounds for the Shannon binary entropy ($q = 1$) are $\mathrm{H}(1/2)\cdot 4x(1-x) \le \mathrm{H}(q) \le \mathrm{H}(1/2)\cdot (4x(1-x))^{\frac{1}{2\mathrm{H}(1/2)}}$, as shown in [Top01, Theorem 1.2]. Our lower bound on the Tsallis binary entropy (Lemma 4.14) matches the case of $q = 1$, whereas our upper bound (Lemma 4.15) only aligns with a weaker bound $\mathrm{H}(q) \le \mathrm{H}(1/2)\cdot(4x(1-x))^{1/2}$ in [Lin91, Theorem 8] and the proof of Lemma 4.15 is more complicated than in the case of $q = 1$.

Lastly, we provide the inequalities between the Tsallis entropy of a distribution p and the total variation distance between p and the uniform distribution ν of the same dimension, as stated in Lemma 4.16. By adding an additional assumption regarding q and $\mathrm{TV}(p,\nu)$, this lemma partially generalizes the previous result for the case of $q = 1$ (cf. [CCKV08, Fact 8.4] and [KLN19, Lemma 16]) to the case of $q > 1$.

4.3.1 Data-processing inequality for QJT_q from the joint convexity

With the correspondence between QJS and the quantum relative entropy (Equation (3.3)), the joint convexity of QJS directly follows from the joint convexity of the quantum relative entropy [Lie73, Uhl77] (see also [Rus22] for a simple proof). However, since QJT_q does not correspond to a Tsallis variant of quantum relative entropy (e.g., quasi-entropy [Pet07, Equation (3.23)]) in this sense, the joint convexity of QJT_q can only be established by the recent results of [CT14, Vir19]:

Lemma 4.9 (Joint convexity of QJT_q, adapted from [CT14, Vir19])**.** *Let k be an integer. For any $i \in [k]$, let $\rho_0^{(i)}$ and $\rho_1^{(i)}$ be two quantum states. Let k-tuple $\mu := (\mu_1, \cdots, \mu_k)$ be a probability distribution. Then, for any $q \in [1,2]$ and $t \in (0,1)$, the joint convexity of QJT_q holds*:

$$\mathrm{QJT}_q\left(\sum_{i\in[k]}\mu_i\rho_0^{(i)}, \sum_{i\in[k]}\mu_i\rho_1^{(i)}\right) \le \sum_{i\in[k]}\mu_i \mathrm{QJT}_q\left(\rho_0^{(i)},\rho_1^{(i)}\right).$$

Proof. Following [CT14, Theorem 2.3(2)], we know that the quantum q-Tsallis entropy $\mathrm{S}_q(\rho)$ for $1 \leq q \leq 2$ is in the Matrix Entropy Class [CT14, Definition 2.2] (or [Vir19, Definition 2]). Therefore, as a corollary of [Vir19, Theorem 1], we can obtain: for any $1 \leq q \leq 2$ and $0 < \lambda < 1$,

$$\mathrm{QJT}_q((1-\lambda)\rho_0 + \lambda\rho_0', (1-\lambda)\rho_1 + \lambda\rho_1') \leq (1-\lambda)\mathrm{QJT}_q(\rho_0, \rho_1) + \lambda\mathrm{QJT}_q(\rho_0', \rho_1'). \quad (4.15)$$

Hence, we can complete the proof by applying Equation (4.15) inductively. □

Remark 4.10 (Data-processing inequality for $\mathrm{QJT}_{q,t}$). It is noteworthy that Lemma 4.9 applies to a generalized version of QJT_q, denoted as $\mathrm{QJT}_{q,t}$, such that $\mathrm{QJT}_{q,1/2} = \mathrm{QJT}_q$:

$$\forall t \in (0,1),\ \mathrm{QJT}_{q,t} \coloneqq \mathrm{S}_q\left((1-t)\rho_0 + t\rho_1\right) - (1-t)\mathrm{S}_q(\rho_0) - t\mathrm{S}_q(\rho_1).$$

Lemma 3.30 also directly extends to $\mathrm{QJT}_{q,t}$, and consequently, Lemma 4.11 holds for $\mathrm{QJT}_{q,t}$ with $1 \leq q \leq 2$. However, the inequalities between QJT_q and the trace distance provided in this work, particularly Lemma 4.12 and Lemma 4.13, do not extend to $\mathrm{QJT}_{q,t}$ for $1 \leq q \leq 2$.

Lemma 4.11 (Data-processing inequality for QJT_q)**.** *For any quantum state ρ_0 and ρ_1, any quantum channel Φ, and $1 \leq q \leq 2$, we have*

$$\mathrm{QJT}_q(\Phi(\rho_0), \Phi(\rho_1)) \leq \mathrm{QJT}_q(\rho_0, \rho_1).$$

Interestingly, the inequality in Lemma 4.11 *cannot* hold for $0 \leq q < 1$. We can see this by considering pure states $|\psi\rangle\langle\psi|$ and $|\phi\rangle\langle\phi|$, and their average $\hat{\rho}_{\psi,\phi} \coloneqq \frac{1}{2}\left(|\psi\rangle\langle\psi| + |\phi\rangle\langle\phi|\right)$, then $\mathrm{QJT}_q(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = \mathrm{S}_q\left(\hat{\rho}_{\psi,\phi}\right)$. Following Lemma 4.11, we have $\mathrm{S}_q\left(\Phi\left(\hat{\rho}_{\psi,\phi}\right)\right) \leq \mathrm{S}_q\left(\hat{\rho}_{\psi,\phi}\right)$ for $q \in [1,2]$. However, using [FYK04, Corollary 2.6], we have $\mathrm{S}_q\left(\Phi\left(\hat{\rho}_{\psi,\phi}\right)\right) \geq \mathrm{S}_q\left(\hat{\rho}_{\psi,\phi}\right)$ for $q \in [0,1)$.

Proof of Lemma 4.11. The case of $q = 1$ coincides with the quantum Jensen-Shannon divergence: Using Equation (3.3), $\mathrm{QJS}(\Phi(\rho_0), \Phi(\rho_1)) \leq \mathrm{QJS}(\rho_0, \rho_1)$ follows from the data-processing inequality of the quantum relative entropy [Lin75, Uhl77] (see also [Pet07, Theorem 3.9]).

It remains to prove the case for $1 < q \leq 2$. We use the standard proof strategy to derive the data-processing inequality from joint convexity, as in [FYK04, Theorem 2.5].

First, we consider the case of the partial trace Tr_{B} on the quantum registers A and B, where $\rho_0, \rho_1 \in \mathrm{L}\left(\mathcal{H}_{\mathsf{AB}}\right)$ and $\dim(\mathcal{H}_{\mathsf{B}}) = N_{\mathsf{B}}$. Since $\mathrm{QJT}_q(\rho_0 \otimes \tilde{I}_{\mathsf{B}}, \rho_1 \otimes \tilde{I}_{\mathsf{B}}) = \mathrm{QJT}_q(\rho_0, \rho_1)$ where $\tilde{I}_{\mathsf{B}}$ is the maximally mixed state in B, it suffices to consider a quantum channel on registers A and B that is completely depolarizing on B and identity on A, denoted as $\Phi_{\mathrm{Tr}_{\mathsf{B}}}$. Noting that $\Phi_{\mathrm{Tr}_{\mathsf{B}}}$ can be expressed as a convex combination of unitary channels (e.g., [Wil13, Exercise 4.4.9] or [Rus22, Equation (9)]), for any quantum state ρ_{AB} on registers A and B, we can obtain:

$$\Phi_{\mathrm{Tr}_{\mathsf{B}}}(\rho_{\mathsf{AB}}) \coloneqq \mathrm{Tr}_{\mathsf{B}}(\rho_{\mathsf{AB}}) \otimes \mathrm{Tr}(\rho_{\mathsf{AB}})\tilde{I}_{\mathsf{B}} = \sum_{l \in [N_{\mathsf{B}}^2]} \frac{1}{N_{\mathsf{B}}^2}(I_{\mathsf{A}} \otimes U_l)\rho_{\mathsf{AB}}(I_{\mathsf{A}} \otimes U_l)^\dagger,$$

where U_l is a unitary operator on B for each $l \in [N_{\mathsf{B}}^2]$.

Using the joint convexity (Lemma 4.9) and the unitary invariance (Lemma 3.30) of

QJS_q, we derive the data-processing inequality concerning the quantum channel $\Phi_{\mathrm{Tr}_\mathsf{B}}$:

$$\begin{aligned}
&\mathrm{QJT}_q\left(\mathrm{Tr}_\mathsf{B}(\rho_0), \mathrm{Tr}_\mathsf{B}(\rho_1)\right) \\
&= \mathrm{QJT}_q(\Phi_{\mathrm{Tr}_\mathsf{B}}(\rho_0), \Phi_{\mathrm{Tr}_\mathsf{B}}(\rho_1)) \\
&\leq \sum_{l\in[N_\mathsf{B}^2]} \frac{1}{N_\mathsf{B}^2} \mathrm{QJT}_q\left((I_\mathsf{A}\otimes U_l)\rho_0(I_\mathsf{A}\otimes U_l)^\dagger, (I_\mathsf{A}\otimes U_l)\rho_1(I_\mathsf{A}\otimes U_l)^\dagger\right) \\
&= \sum_{l\in[N_\mathsf{B}^2]} \frac{1}{N_\mathsf{B}^2} \mathrm{QJT}_q\left(\rho_0, \rho_1\right) \\
&= \mathrm{QJT}_q(\rho_0, \rho_1).
\end{aligned} \tag{4.16}$$

Next, we move to the general case. By leveraging the Stinespring dilation theorem (e.g., [AS17, Theorem 2.25]), for any quantum channel Φ on the registers (A, B), we have the following representation with some unitary U_Φ on the registers $(\mathsf{A}, \mathsf{B}, \mathsf{E})$ where $\dim(\mathcal{H}_\mathsf{E}) \leq \dim(\mathcal{H}_{\mathsf{AB}})^2$:

$$\Phi(\rho_{\mathsf{AB}}) = \mathrm{Tr}_\mathsf{E}\left(U_\Phi(\rho_{\mathsf{AB}}\otimes|\bar{0}\rangle\langle\bar{0}|_\mathsf{E})U_\Phi^\dagger\right).$$

Consequently, we can obtain the following for any quantum channel Φ:

$$\begin{aligned}
\mathrm{QJT}_q(\Phi(\rho_0), \Phi(\rho_1)) &\leq \mathrm{QJT}_q\left(U_\Phi(\rho_0\otimes|\bar{0}\rangle\langle\bar{0}|_\mathsf{E})U_\Phi^\dagger, U_\Phi(\rho_1\otimes|\bar{0}\rangle\langle\bar{0}|_\mathsf{E})U_\Phi^\dagger\right) \\
&= \mathrm{QJT}_q\left(\rho_0\otimes|\bar{0}\rangle\langle\bar{0}|_\mathsf{E}, \rho_1\otimes|\bar{0}\rangle\langle\bar{0}|_\mathsf{E}\right) \\
&= \mathrm{QJT}_q(\rho_0, \rho_1).
\end{aligned}$$

Here, the first line owes to Equation (4.16), the second line is due to the unitary invariance of QJT_q (Lemma 3.30), and the last line is because $\mathrm{Tr}\left((\rho_b\otimes|\phi\rangle\langle\phi|_\mathsf{E})^q\right) = \mathrm{Tr}(\rho_b^q)$ for any $b\in\{0,1\}$ and $q\in[1,2]$. We now complete the proof. □

4.3.2 Inequalities between the trace distance and QJT_q

We begin by establishing the lower bound on QJT_q in terms of the trace distance, as stated in Lemma 4.12. The measured variant of the q-Jensen-Tsallis divergence (JT_q), denoted by $\mathrm{QJT}_q^{\mathrm{meas}}$, is derived from the definition provided in Equation (3.2).

Lemma 4.12 ($\mathrm{T}\leq\mathrm{QJT}_q$)**.** *For any quantum states ρ_0 and ρ_1, we have*:

$$\forall q\in[1,2],\ \mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q\left(\frac{1}{2} - \frac{\mathrm{T}(\rho_0,\rho_1)}{2}\right) \leq \mathrm{QJT}_q^{\mathrm{meas}}(\rho_0,\rho_1) \leq \mathrm{QJT}_q(\rho_0,\rho_1).$$

Proof. The case of $q=1$ follows from [BH09, Theorem 14]. An alternative proof can be derived by combining [FvdG99, Theorem 1] with the Holevo bound, see Lemma 3.24 and Lemma 3.25 in Section 3.2 for details.

Our focus will be on the cases where $1<q\leq 2$. We first prove the second inequality. Let $\mathcal{M}^*$ be an optimal POVM corresponding to $\mathrm{QJT}_q^{\mathrm{meas}}(\rho_0,\rho_1)$, then this POVM $\mathcal{M}^*$ corresponds to a quantum-to-classical channel $\Phi_{\mathcal{M}^*}(\rho) = \sum_{i=1}^N |i\rangle\langle i|\mathrm{Tr}(\rho M_i^*)$, e.g., [AS17, Equatin (2.41)]. Leveraging the data-processing inequality for QJT_q (Lemma 4.11), for $1<q\leq 2$, we obtain:

$$\mathrm{QJT}_q^{\mathrm{meas}}(\rho_0,\rho_1) = \mathrm{QJT}_q\left(\Phi_{\mathcal{M}^*}(\rho_0), \Phi_{\mathcal{M}^*}(\rho_1)\right) \leq \mathrm{QJT}_q(\rho_0,\rho_1).$$

Next, let us move to the first inequality. Let $p_b^{\mathcal{M}}$ be the induced distribution with respect to the POVM $\mathcal{M}$ of ρ_b for any $b \in \{0,1\}$. Utilizing Lemma 3.10, for $1 < q \leq 2$, we can derive that:

$$\begin{aligned} \mathrm{QJS}^{\mathrm{meas}}_{q,\mathcal{M}^*}(\rho_0,\rho_1) &\geq \mathrm{QJS}^{\mathrm{meas}}_{q,\mathcal{M}}(\rho_0,\rho_1) \\ &= \mathrm{JT}_q\left(p_0^{\mathcal{M}}, p_1^{\mathcal{M}}\right) \\ &\geq \mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q\left(\frac{1}{2} - \frac{\mathrm{TV}\left(p_0^{\mathcal{M}}, p_1^{\mathcal{M}}\right)}{2}\right). \end{aligned} \tag{4.17}$$

We then consider the function $g(q;x)$ and its first derivative $\frac{\partial}{\partial x} g(q;x)$:

$$\begin{aligned} g(q;x) &:= \mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q\left(\frac{1-x}{2}\right) = \frac{2^{-q}}{q-1}\left((1+x)^q + (1-x)^q - 2\right), \\ \frac{\partial}{\partial x} g(q;x) &= \frac{2^{-q} q}{q-1}\left((1+x)^{q-1} - (1-x)^{q-1}\right). \end{aligned}$$

Since it is easy to see that $\frac{\partial}{\partial x} g(q;x) \geq 0$ for $0 \leq x \leq 1$ when $1 < q \leq 2$, we know that $g(q;x)$ is monotonically increasing for $0 \leq x \leq 1$. Noting that Equation (4.17) holds for arbitrary POVM $\mathcal{M}$, and the trace distance is the measured version of the total variation distance (e.g., [NC10, Theorem 9.1]), we thus complete the proof by choosing the POVM that maximizes $\mathrm{T}(\rho_0,\rho_1)$. □

Next, we demonstrate the upper bound on QJT_q in terms of the trace distance:

Lemma 4.13 ($\mathrm{QJT}_q \leq \mathrm{T}$)**.** *For any quantum states ρ_0 and ρ_1, we have*:

$$\forall q \in [1,2], \quad \mathrm{QJT}_q(\rho_0,\rho_1) \leq \mathrm{H}_q\left(\frac{1}{2}\right) \cdot \frac{1}{2}\mathrm{Tr}(|\rho_0 - \rho_1|^q) \leq \mathrm{H}_q\left(\frac{1}{2}\right) \cdot \mathrm{T}(\rho_0,\rho_1)^q.$$

Proof. We begin with the construction for establishing $\mathrm{QJT}_q \leq \ln 2 \cdot \mathrm{T}$ for $q = 1$ as in [BH09, Theorem 14], see also the proof of Lemma 3.26. Our analysis differs since we need to address the cases of $1 \leq q \leq 2$. Consider a single qutrit register B with basis vectors $|0\rangle, |1\rangle, |2\rangle$. Define $\hat{\rho}_0$ and $\hat{\rho}_1$ on $\mathcal{H} \otimes \mathcal{B}$ as below, where $\mathcal{B} = \mathbb{C}^3$ is the Hilbert space corresponding to the register B:

$$\begin{aligned} \hat{\rho}_0 &:= \frac{\rho_0 + \rho_1 - |\rho_0 - \rho_1|}{2} \otimes |2\rangle\langle 2| + \frac{\rho_0 - \rho_1 + |\rho_0 - \rho_1|}{2} \otimes |0\rangle\langle 0| := \quad \sigma_2 \otimes |2\rangle\langle 2| + \sigma_0 \otimes |0\rangle\langle 0|, \\ \hat{\rho}_1 &:= \frac{\rho_0 + \rho_1 - |\rho_0 - \rho_1|}{2} \otimes |2\rangle\langle 2| + \frac{\rho_1 - \rho_0 + |\rho_0 - \rho_1|}{2} \otimes |1\rangle\langle 1| := \quad \sigma_2 \otimes |2\rangle\langle 2| + \sigma_1 \otimes |1\rangle\langle 1|. \end{aligned}$$

Intuitively, σ_b represents the case where ρ_b is "larger than" ρ_{1-b} for $b \in \{0,1\}$ (i.e., ρ_0 and ρ_1 are "distinguishable"), while σ_2 represents the case where ρ_0 is "indistinguishable" from ρ_1. This construction generalizes the proof of the classical analogs (e.g., [Vad99, Claim 4.4.2]).

Since QJT_q is contractive when applying a partial trace (Lemma 4.11), we obtain:

$$\begin{aligned} \mathrm{QJT}_q(\rho_0,\rho_1) &= \mathrm{QJT}_q(\mathrm{Tr}_{\mathsf{B}}(\hat{\rho}_0), \mathrm{Tr}_{\mathsf{B}}(\hat{\rho}_1)) \\ &\leq \mathrm{QJT}_q(\hat{\rho}_0, \hat{\rho}_1) \\ &= \frac{1}{q-1}\left(\mathrm{Tr}\left(\left(\frac{\hat{\rho}_0 + \hat{\rho}_1}{2}\right)^q\right) - \frac{1}{2}\mathrm{Tr}(\hat{\rho}_0^q) - \frac{1}{2}\mathrm{Tr}(\hat{\rho}_1^q)\right). \end{aligned} \tag{4.18}$$

As that $\sigma_0 \otimes |0\rangle\langle 0|$, $\sigma_1 \otimes |1\rangle\langle 1|$, and $\sigma_2 \otimes |2\rangle\langle 2|$ are orthogonal to each other, we have:

$$\mathrm{Tr}\left(\left(\frac{\hat{\rho}_0+\hat{\rho}_1}{2}\right)^q\right) = \mathrm{Tr}\left(\left(\sigma_2\otimes|2\rangle\langle 2| + \sum_{b\in\{0,1\}}\frac{\sigma_b}{2}\otimes|b\rangle\langle b|\right)^q\right) = \mathrm{Tr}\left(\sigma_2^q+\frac{\sigma_0^q}{2^q}+\frac{\sigma_1^q}{2^q}\right), \tag{4.19}$$

$$\forall b\in\{0,1\},\ \mathrm{Tr}(\hat{\rho}_b^q) = \mathrm{Tr}\left((\sigma_2\otimes|2\rangle\langle 2| + \sigma_b\otimes|b\rangle\langle b|)^q\right) = \mathrm{Tr}\left(\sigma_2^q+\sigma_b^q\right).$$

Plugging Equation (4.19) and $\mathrm{H}_q\left(\frac{1}{2}\right) = \frac{1-2^{1-q}}{q-1}$ into Equation (4.18), we obtain:

$$\begin{aligned}\mathrm{QJT}_q(\rho_0,\rho_1) &\le \mathrm{H}_q\left(\frac{1}{2}\right)\cdot\frac{1}{2}\mathrm{Tr}(\sigma_0^q+\sigma_1^q)\\ &\le \mathrm{H}_q\left(\frac{1}{2}\right)\cdot\frac{1}{2}(\mathrm{Tr}(\sigma_0)^q+\mathrm{Tr}(\sigma_1)^q)\\ &= \mathrm{H}_q\left(\frac{1}{2}\right)\cdot\mathrm{T}(\rho_0,\rho_1)^q.\end{aligned} \tag{4.20}$$

Here, the second line is due to the monotonicity of the Schatten p-norm (e.g., [AS17, Equation (1.31)]), equivalently, $\mathrm{Tr}(M^q) \le \mathrm{Tr}(M)^q$ for any positive semi-definite matrix M and $q \ge 1$. The last line owes to the fact that

$$\mathrm{Tr}(\sigma_b) = (-1)^b\mathrm{Tr}\left(\frac{\rho_0-\rho_1}{2}\right)+\frac{1}{2}\mathrm{Tr}(|\rho_0-\rho_1|) = \frac{1}{2}\mathrm{Tr}(|\rho_0-\rho_1|) \text{ for } b\in\{0,1\}.$$

Lastly, since σ_0 and σ_1 are orthogonal to each other, we complete the proof by plugging the equality $\mathrm{Tr}(\sigma_0^q+\sigma_1^q) = \mathrm{Tr}((\sigma_0+\sigma_1)^q) = \mathrm{Tr}(|\rho_0-\rho_1|^q)$ into the first line in Equation (4.20). □

4.3.3 Bounds for the Tsallis binary entropy

In this subsection, we establish lower and upper bounds (Lemma 4.14 and Lemma 4.15, respectively) for the Tsallis binary entropy, which are useful when applying the lower bound on QJT_q in terms of the trace distance (Lemma 4.12).

We begin by proving an lower bound, which extends the bound

$$\mathrm{H}(1/2)\cdot 4x(1-x) \le \mathrm{H}(x)$$

from the case of $q = 1$, as stated in [Top01, Theorem 1.2], to a broader range of q:

Lemma 4.14 (Tsallis binary entropy lower bound)**.** *For any $p = (x, 1-x)$, let $\mathrm{H}_q(x)$ denote the Tsallis binary entropy with $q \in [0,2]\cup[3,+\infty)$, we have*:

$$\mathrm{H}_q(1/2)\cdot 4x(1-x) \le \mathrm{H}_q(x).$$

Proof. We need only consider the cases where $q \in \mathcal{I} := [0,1)\cup(1,2]\cup[3,+\infty)$, as the case $q = 1$ directly follows from [Top01, Theorem 1.2]. Our proof strategy is inspired by the approach used in that theorem. We start by defining functions $F(q;x)$ and $G(q;x)$ on $0 \le x \le 1$ and $q \in \mathcal{I}$:

$$F(q;x) := \frac{\mathrm{H}_q(x)}{x(1-x)} = \frac{1-x^q-(1-x)^q}{(q-1)x(1-x)} \text{ and } G(q;x) := \frac{x^{q-1}-1}{(q-1)(x-1)}.$$

It is evident that $F(q;0) = F(q;1) = \infty$ and $F(q;1/2) = 4\mathrm{H}_q(1/2)$. We then assume

that $G(q;x)$ is convex on $x \in [0,1]$ for any fixed $q \in \mathcal{I}$: For any $x \in [0,1]$ and $q \in (1,2]$,

$$\frac{\partial^2 G(q;x)}{\partial x^2} = \frac{(q-2)x^{q-3}}{x-1} - \frac{2x^{q-2}}{(x-1)^2} + \frac{2(x^{q-1}-1)}{(x-1)^3(q-1)} \geq 0. \tag{4.21}$$

Since $F(q;x) = G(q;x) + G(q;1-x)$, Equation (4.21) implies that $F(q,x)$ is convex on $x \in [0,1]$ for any fixed $q \in \mathcal{I}$. By noticing that $F(q;x) = F(q;1-x)$ for any $x \in [0,1]$, we can obtain that: for any $q \in \mathcal{I}$, $F(q;x)$ is monotonically decreasing on $x \in (0,1/2)$ and monotonically increasing on $x \in (1/2,1)$. Consequently, we establish the lower bound by noticing that:

$$\text{For any } x \in [0,1] \text{ and } q \in \mathcal{I}, F(q;x) \geq F(q;1/2) = 4\mathrm{H}_q(1/2).$$

It remains to prove Equation (4.21). Noting that $(x-1)^3 \leq 0$ for any $0 \leq x \leq 1$, Equation (4.21) holds if and only if the following holds:

$$f(q;x) \coloneqq (q-2)(x-1)^2 x^{q-3} - 2(x-1)x^{q-2} + \frac{2(x^{q-1}-1)}{q-1} \leq 0.$$

A direct calculation implies that $\frac{\partial}{\partial x} f(q;x) = (q-3)(q-2)(x-1)^2 x^{q-4} \geq 0$ for any $q \in \mathcal{I}$ and $x \in [0,1]$ since $\mathcal{I} \cup (2,3) = \emptyset$. Hence, for any fixed $q \in \mathcal{I}$, $f(q;x)$ is monotonically increasing for any $x \in (0,1)$. Therefore, we complete the proof by concluding that

$$\max_{x \in [0,1]} f(q;x) \leq f(q,1) = 0. \qquad \square$$

Next, we will show an upper bound for the range of $1 < q \leq 2$ that is weaker than the best known upper bound for the case of $q = 1$ as shown in [Top01, Theorem 1.2]:[21]

Lemma 4.15 (Tsallis binary entropy upper bound)**.** *For any $p = (x, 1-x)$, let $\mathrm{H}_q(x)$ denote the Tsallis binary entropy with $1 \leq q \leq 2$, we have*:

$$\mathrm{H}_q(x) \leq \mathrm{H}_q(1/2) \cdot (4x(1-x))^{1/2}.$$

Proof. The case of $q = 1$ follows directly from [Lin91, Theorem 8], it remains to address the range $1 < q \leq 2$. We will establish the bound separately for $x \in \mathcal{I}_{\text{inner}}$ and $x \in \mathcal{I}_{\text{outer}}$, where $\mathcal{I}_{\text{inner}} \cup \mathcal{I}_{\text{outer}} = [0,1]$. Specifically, these intervals are defined as $\mathcal{I}_{\text{inner}} \coloneqq [0,1/8] \cup [1/8,1]$ and $\mathcal{I}_{\text{outer}} \coloneqq [1/2 - \tau(q), 1/2 + \tau(q)]$, where $\tau(q)$ will be specified latter.

The outer interval case. We start with the case of $x \in \mathcal{I}_{\text{outer}}$. Since $\mathrm{H}_q(x) = \mathrm{H}_q(1-x)$ for any $0 \leq x \leq 1$, it is sufficient to consider the case of $0 \leq x \leq 1/8$. Noting that $q - 1 \geq 0$, it suffices to show that: For any $0 \leq x \leq 1/8$ and $1 < q \leq 2$,

$$\begin{aligned} & (q-1)\left(\mathrm{H}_q\left(\frac{1}{2}\right)\sqrt{4x(1-x)} - \mathrm{H}_q(x)\right) \\ = \; & \left(2 - 2^{2-q}\right)\sqrt{x(1-x)} - (1 - x^q - (1-x)^q) \\ \geq \; & 0. \end{aligned} \tag{4.22}$$

[21] Numerical evidence suggests that Lemma 4.15 can be improved to $\mathrm{H}_q(x) \leq \mathrm{H}_q\left(\frac{1}{2}\right) \cdot (4x(1-x))^{\frac{1}{2\mathrm{H}_q(1/2)}}$ for any $0 \leq x \leq 1$ and $1 \leq q \leq 2$, which matches the bound $\mathrm{H}(q) \leq \mathrm{H}(1/2)(4x(1-x))^{\frac{1}{2\mathrm{H}_q(1/2)}}$ in [Top01].

Leveraging the Taylor expansion of $1-(1-x)^q$ at $x=0$, we obtain that:

$$1-(1-x)^q = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k!} \prod_{r=0}^{k-1}(q-r)x^k \coloneqq \sum_{k=1}^{\infty} \alpha_k x^k \leq qx. \tag{4.23}$$

Here, notice that $1 < q \leq 2$, the last inequality owes to the fact that $\alpha_1 = q > 0$ and $\alpha_k \leq 0$ for all integer $k \geq 2$. Plugging Equation (4.23) into Equation (4.22), it remains to prove that:

$$F_1(q;x) \coloneqq \frac{-x^q + qx}{\sqrt{x(1-x)}} \leq 2 - 2^{2-q}.$$

A direct calculation implies that $F_1(q;1/8) = (q - 2^{3-3q})/\sqrt{7}$ satisfies $2 - 2^{2-q} - F_1(q;1/8) > 0$ for $1 < q \leq 2$.[22] As a consequence, it is enough to show that $F_1(q,x)$ is monotonically non-decreasing on $x \in [0, 1/8]$ for any fixed $q \in (1,2]$, specifically:

$$\frac{\partial}{\partial x} F_1(q;x) = \frac{1}{2}(x(1-x))^{-3/2}\left(qx + (1 + 2q(x-1) - 2x)x^q\right) \geq 0. \tag{4.24}$$

Since $\frac{1}{2}(x(1-x))^{-3/2} \geq 0$, Equation (4.24) holds if and only if the following holds:

$$F_2(q;x) \coloneqq \left(2(1-q)x + 2q - 1\right)x^{q-1} \leq q.$$

A straightforward calculation implies that $F_2(q;1/8) = 2^{1-3q}(7q-3)$ satisfies that $q - F_2(q;1/8) > 0$ for $1 < q \leq 2$. Consequently, it suffices to show that $F_2(q;x)$ is monotonically non-decreasing on $x \in [0, 1/8]$ for any fixed $q \in (1,2]$, particularly:

$$\frac{\partial}{\partial x} F_2(q;x) = x^{q-2}(q-1)(2q(1-x) - 1) \geq 0. \tag{4.25}$$

Since $x^{q-2}(q-1) > 0$ for any $q \in (1,2]$ and $x \in [0, 1/8]$, Equation (4.25) holds if and only if $F_3(q;x) \coloneqq 2q(1-x) - 1 \geq 0$. It is evident that $F_3(q;x) \geq 0$ is equivalent to $x \leq 1 - 1/2q < 1/2$ for $1 < q \leq 2$. And consequently, we complete the proof of the outer interval case.

The inner interval case. Next, we move to the case of $x \in \mathcal{I}_{\text{inner}}$. Let $x = (1+t)/2$, then it suffices to consider the case of $0 \leq t \leq 1$ since $\mathrm{H}_q(x) = \mathrm{H}_q(1-x)$ for any $0 \leq x \leq 1$. Noting that $2^q/(q-1) > 0$ for $1 < q \leq 2$, it is sufficient to show that: For any $0 \leq t \leq 2\tau(q)$ and $1 < q \leq 2$,

$$\begin{aligned} &\frac{2^q}{q-1}\left(\mathrm{H}_q\left(\frac{1}{2}\right)\sqrt{4x(1-x)} - \mathrm{H}_q(x)\right) \\ &= (1-t)^q + (1+t)^q - \left(2^q + (2-2^q)\sqrt{1-t^2}\right) \\ &\geq 0. \end{aligned} \tag{4.26}$$

Utilizing the Taylor expansion of $(1-t)^q + (1+t)^q$ at $t=0$, we obtain that:

$$(1-t)^q + (1+t)^q = \sum_{k=0}^{\infty} \frac{2}{(2k)!} \prod_{r=0}^{2k-1}(q-r)t^{2k} \coloneqq \sum_{k=0}^{\infty} \beta_k t^{2k} \geq \beta_0 + \beta_1^2 = 2 + q(q-1)t^2. \tag{4.27}$$

Here, the last inequality is because $\beta_k \geq 0$ for all integer $k \geq 0$. Substituting Equa-

[22] It is noteworthy that $2 - 2^{2-q} - F_1(q;1/2) = 2 - 2^{1-q} - q < 0$ for $1 < q \leq 2$, and consequently, the outer interval case is not enough to establish our Tsallis binary entropy upper bound for any $0 \leq x \leq 1$.

tion (4.27) into Equation (4.26), it remains to show that:

$$2 + q(q-1)t^2 \geq 2^q + (2-2^q)\sqrt{1-t^2}. \tag{4.28}$$

A direct calculation implies that Equation (4.28) holds for the following range of t:

$$|t| \leq \frac{\sqrt{(2q^2-2q+2-2^q)(2^q-2)}}{q(q-1)} = 2\tau(q),$$
$$\text{where } \tau(q) \coloneqq \frac{\sqrt{(q^2-q+1-2^{q-1})(2^{q-1}-1)}}{q(q-1)}.$$

It is easy to see that $\lim_{q\to 1^+}\tau(q) = \sqrt{\ln 2(1-\ln 2)} \approx 0.4612$ and $\tau(2) = 1$. Assume that $\tau(q)$ is monotonically non-decreasing for $q \in (1,2]$, we obtain that $[1/2 - \sqrt{\ln 2(1-\ln 2)}, 1/2 + \sqrt{\ln 2(1-\ln 2)}] \subseteq \mathcal{I}_{\text{inner}}$, and consequently, $\mathcal{I}_{\text{inner}} \cup \mathcal{I}_{\text{outer}} = [0,1]$.

It is left to show that $\tau(q)$ is monotonically non-decreasing for $q \in (1,2]$, specifically:

$$\frac{\mathrm{d}}{\mathrm{d}q}\tau(q) = \frac{2}{q^3(q-1)^3}\underbrace{\left(2^q - q^2 + q - 2\right)}_{g_1(q)}\underbrace{\left(2 - 2^q - 2^q q^2 \ln 2 + q\left(2^{1+q} + 2q\ln 2 - 4\right)\right)}_{g_2(q)} \geq 0. \tag{4.29}$$

Note that $g_1(q) = 0$ corresponds to an intersection between a quadratic function and an exponential function, indicating that $g_1(q)$ has at most three zeros. It is evident that $g_1(1) = g_1(2) = g_1(3) = 0$ and $g(3/2) = 2\sqrt{2} - 11/4 \approx 0.078$, and thus $g_1(q) \geq 0$ for $1 \leq q \leq 2$. For $g_2(q)$, notice that $g_2(1) = 0$. Assuming that $g_2(q)$ is monotonically non-decreasing on $1 \leq q \leq 2$, we obtain $g_2(q) \geq g_2(1) = 0$ for $1 \leq q \leq 2$. In particular, it remains to prove that:

$$\text{For any } q \in [1,2],\ g_3(q) \coloneqq \frac{\mathrm{d}}{\mathrm{d}q}g_2(q) = 2^q(-(\ln 2)^2 q^2 + (\ln 2)^2 q + 2) - 4 \geq 0. \tag{4.30}$$

Since $g_3(q)+4$ is the product of a quadratic function and an exponential function, $g_3(q)$ has at most two zeros. Therefore, we establish Equation (4.30), and thus Equation (4.29), by noticing that $g_3(1) = 0$, $g_3(2) = 4 - 8(\ln 2)^2 > 0$, and $g_3(3) = 12 - 48(\ln 2)^2 < 0$. □

4.3.4 Useful bounds on Tsallis entropy

In this subsection, we present a useful bound on Tsallis entropy. Lemma 4.16 establishes inequalities between the Tsallis entropy of a distribution p and the total variation distance between p and the uniform distribution of the same dimension.

Lemma 4.16 (Tsallis entropy bounds by closeness to uniform distribution)**.** *Let p be a probability distribution over $[N]$ with $N \geq 2$, and let ν be the uniform distribution over $[N]$. Then, for any $q > 1$ and $0 \leq \mathrm{TV}(p,\nu) \leq 1 - 1/N$, it holds that:*

$$(1 - \mathrm{TV}(p,\nu) - 1/N)\ln_q(N) \leq \mathrm{H}_q(p).$$

Moreover, for any $q > 1$ and N satisfying $1/q \leq \mathrm{TV}(p,\nu) \leq 1 - 1/N$, it holds that:

$$\mathrm{H}_q(p) \leq \ln_q\Big(N(1 - \mathrm{TV}(p,\nu))\Big).$$

Proof. Let $\gamma \coloneqq \mathrm{TV}(p,\nu)$, and let Δ_N be the set of probability distributions of dimension

N. It is evident that $0 \le \mathrm{TV}(p,\nu) \le 1 - 1/N$. To establish the lower bound, it suffices to minimize the Tsallis entropy $\mathrm{H}_q(p)$ subject to the constraint $\mathrm{TV}(p,\nu) = \gamma$, which is equivalent to solve the convex optimization problem in Equation (4.31).[23]

$$\begin{aligned} &\text{minimize} && \mathrm{H}_q(p') \\ &\text{subject to} && p' \in \Delta_n, \\ &&& \mathrm{TV}(p',\nu) \le \gamma \end{aligned} \tag{4.31}$$

$$\begin{aligned} p_{\min}(i) &= \begin{cases} \frac{1}{N}, & \text{if } i \in [k_{\min}] \\ \frac{1}{N} + \gamma, & \text{if } i = k_{\min}+1 \\ \frac{\varepsilon}{N}, & \text{if } i = k_{\min}+2 \\ 0, & \text{otherwise} \end{cases}, \\ \text{where} \quad & k_{\min} \coloneqq \lfloor N(1-\gamma) \rfloor - 1, \\ & \varepsilon \coloneqq N(1-\gamma) - \lfloor N(1-\gamma) \rfloor. \end{aligned} \tag{4.32}$$

Note that $\mathrm{H}_q(p)$ is concave (Lemma 3.8) for any fixed $q > 1$, and the constraints in Equation (4.31) form a closed convex set. Since the minimum of a concave function is attained at some extreme point (e.g., [Roc70, Corollary 32.3.1]) and the Tsallis entropy is permutation-invariant, we deduce an optimal solution $p_{\min}$ to Equation (4.31), as stated in Equation (4.32).

Next, we can deduce the lower bound of the Tsallis entropy by evaluating $\mathrm{H}_q(p_{\min})$:

$$\begin{aligned} \mathrm{H}_q(p_{\min}) &= \frac{1}{q-1}\left(1 - k_{\min}\left(\frac{1}{N}\right)^q - \left(\frac{1}{N}+\gamma\right)^q - \left(\frac{\varepsilon}{N}\right)^q\right) \\ &\ge \frac{1}{q-1}\left(\frac{(\lfloor N(1-\gamma)\rfloor - 1)}{N} + \frac{\varepsilon}{N} - (\lfloor N(1-\gamma)\rfloor - 1 + \varepsilon^q)\left(\frac{1}{N}\right)^q\right) \\ &\ge \frac{1}{q-1}\left(1 - \gamma - \frac{1}{N} - \left(1-\gamma-\frac{1}{N}\right)\left(\frac{1}{N}\right)^{q-1}\right) \\ &= \left(1 - \gamma - \frac{1}{N}\right)\ln_q(N). \end{aligned}$$

Here, the second line excludes terms corresponding to $p_{\min}(k_{\min}+1)$, and the third line follows from the fact that $\varepsilon^q \le \varepsilon$ for $q \ge 1$ and $0 \le \varepsilon \le 1$.

To demonstrate the upper bound, it remains to maximize the Tsallis entropy $\mathrm{H}_q(p)$ subject to the constraint $\mathrm{TV}(p,\nu) = \gamma$, which is equivalent to solve a *non-convex* optimization problem analogous to Equation (4.31). This task is challenging in general, but we consider only the regime $\mathrm{TV}(p,\nu) \ge 1/q$.[24]. Particularly, we focus on the following optimization problem:

$$\begin{aligned} &\text{maximize} && \mathrm{H}_q(p') \\ &\text{subject to} && p' \in \Delta_n, \\ &&& \mathrm{TV}(p',\nu) \ge \gamma \ge 1/q \end{aligned} \tag{4.33}$$

It is not too hard to obtain an optimal solution $p_{\max}$ to Equation (4.33), where ε is defined as in Equation (4.32), as stated in Proposition 4.16.1. The proof is deferred to the end of this subsection.

[23] A similar formulation also appeared in the proof of [KLN19, Lemma 16].

[24] For the regime $0 \le \mathrm{TV}(p,\nu) \le 1/q$, the optimal solution to Equation (4.33) depends on the choice of q.

Proposition 4.16.1. *For the optimization problem presented in Equation (4.33), an optimal solution is the distribution provided in Equation (4.34), where* $\varepsilon = N(1-\gamma) - \lfloor N(1-\gamma) \rfloor$:

$$p_{\max}(i) = \begin{cases} \frac{1}{N} + \frac{\gamma}{k_{\max}}, & \text{if } i \in [k_{\max}] \\ \frac{\varepsilon}{N(N-k_{\max})}, & \text{otherwise} \end{cases}, \text{ where } k_{\max} \coloneqq \lfloor N(1-\gamma) \rfloor. \tag{4.34}$$

Then, we can derive the upper bound of the Tsallis entropy by evaluating $\mathrm{H}_q(p_{\max})$:

$$\begin{aligned} \mathrm{H}_q(p_{\max}) &= \frac{1}{q-1}\left(1 - k_{\max}\left(\frac{1}{N} + \frac{\gamma}{k_{\max}}\right)^q - (N-k_{\max})\left(\frac{\varepsilon}{N(N-k_{\max})}\right)^q\right) \\ &= \frac{1}{q-1}\left(1 - \left(1-\frac{\varepsilon}{N}\right)^q \left(\frac{1}{(N(1-\gamma)-\varepsilon}\right)^{q-1} - \left(\frac{\varepsilon}{N}\right)^q \left(\frac{1}{N\gamma+\varepsilon}\right)^{q-1}\right) \\ &\le \frac{1}{q-1}\left(1 - \left(\frac{1}{(N(1-\gamma)}\right)^{q-1}\right) \\ &= \ln_q\Big(N(1-\gamma)\Big). \end{aligned}$$

Let $F(q; N, \varepsilon, \gamma) \coloneqq \left(1-\frac{\varepsilon}{N}\right)^q (N(1-\gamma)-\varepsilon)^{1-q} + \left(\frac{\varepsilon}{N}\right)^q (N\gamma+\varepsilon)^{1-q}$, then the third line holds by assuming that $F(q; N, \varepsilon, \gamma)$ is monotonically non-decreasing on $0 \le \varepsilon \le 1$ for any fixed γ, q, and N satisfying $q\gamma \ge 1$ and $N \ge q/(q-1)$.

It remains to prove $\frac{\partial}{\partial \varepsilon} F(q; N, \varepsilon, \gamma) \ge 0$ the aforementioned range of x, γ, q, and N. By a direct calculation, we complete the proof by noticing all terms in the following are non-negative:

$$\frac{\partial}{\partial \varepsilon} F(q; N, \varepsilon, \gamma) = \left(1-\frac{\epsilon}{N}\right)^q \frac{(N(\gamma q - 1) + \epsilon)}{(N-\epsilon)(N(1-\gamma)-\epsilon)^q} + \left(\frac{\epsilon}{N}\right)^q \frac{(\gamma N q + \epsilon)}{\epsilon(\gamma N + \epsilon)^q} \ge 0. \qquad \square$$

Proof of Proposition 4.16.1. We begin by noting that $\mathrm{H}_q(p) = \frac{1}{q-1}\left(1 - \sum_{i\in[N]} p(i)^q\right)$ is concave (Lemma 3.8) for any fixed $q > 1$. Consequently, an optimal solution $p_{\max}$ to the optimization problem specified in Equation (4.33) has a particular form. Specifically, $p_{\max}$ is one of probability distributions $p^{(k)}$ for integer $k \in [\lfloor N(1-\gamma) \rfloor]$ defined in Equation (4.35) with a maximum Tsallis entropy:[25]

$$\mathrm{H}_q(p_{\max}) = \max_{k \in [\lfloor N(1-\gamma) \rfloor]} \mathrm{H}_q\left(p^{(k)}\right), \text{ where } p^{(k)}(i) \coloneqq \begin{cases} \frac{1}{N} + \frac{\gamma}{k}, & \text{if } i \in [k] \\ \frac{1}{N} - \frac{\gamma}{N-k}, & \text{otherwise} \end{cases}. \tag{4.35}$$

Plugging Equation (4.35) into Equation (4.33), it suffices to solve the following optimization problem with $q > 1$:

$$\begin{aligned} \text{minimize} \quad & F_q(N, k, \gamma) \coloneqq \sum_{i\in[N]} p(i)^q = k \cdot \left(\frac{1}{N} + \frac{\gamma}{k}\right)^q + (N-k) \cdot \left(\frac{1}{N} - \frac{\gamma}{N-k}\right)^q \\ \text{subject to} \quad & 1/q \le \gamma \le 1 - 1/N, \\ & 1 \le k \le \lfloor N(1-\gamma) \rfloor, \\ & k, N \in \mathbb{Z}_+ \end{aligned} \tag{4.36}$$

To establish that Equation (4.34) is an optimal solution to Equation (4.36), it remains

[25] It is easy to verify that $\frac{1}{N} - \frac{\gamma}{N-k} \ge 0$ holds if and only if $k \le N(1-\gamma)$ holds.

to show that the objective function $F_q(N,k,\gamma)$ is monotonically non-increasing in k for N, γ, and $q > 1$ satisfying the constraints in Equation (4.36). Equivalently, it requires to be shown that $\frac{\partial}{\partial k}F_q(N,k,\gamma) \leq 0$ for $1/q \leq \gamma \leq 1 - 1/N$ and $1 \leq k \leq \lfloor N(1-\gamma) \rfloor$, specifically:

$$\begin{aligned}
&\frac{\partial}{\partial k}F_q(N,k,\gamma) \\
&= \frac{(k-\gamma N(q-1))\left(\frac{\gamma}{k}+\frac{1}{N}\right)^q}{k+\gamma N} + \frac{\left(\frac{1}{N}-\frac{\gamma}{N-k}\right)^q(\gamma N(q-1)+N-k)}{\gamma N-(N-k)} \\
&\leq 0.
\end{aligned} \tag{4.37}$$

Since it is evident that $\frac{\gamma}{k}+\frac{1}{N} \geq 0$, $k+\gamma N \geq 0$, and $k \leq \lfloor N(1-\gamma) \rfloor \leq N(1-\gamma)$, we can deduce Equation (4.37) by combining the following inequalities:

$$\begin{aligned}
k-\gamma N(q-1) &\leq N(1-\gamma)-\gamma N(q-1) = N(1-q\gamma) \leq 0, \\
\frac{1}{N}-\frac{\gamma}{N-k} &\geq \frac{1}{N}-\frac{\gamma}{N-N(1-\gamma)} = 0, \\
\gamma N(q-1)+N-k &\geq N(q-1)+N-N(1-\gamma) = Nq\gamma \geq N > 0, \\
\gamma N-(N-k) &\leq N-(N-N(1-\gamma)) = 0.
\end{aligned}$$

Here, the first and the third line hold also due to $\gamma \geq 1/q$. This completes the proof. □

4.4 Hardness and lower bounds via QJT_q-based reductions

In this section, we will establish reductions from the closeness testing of quantum states via the trace distance to testing via the quantum q-Tsallis entropy difference. Our proof crucially depends on the properties of the quantum Jensen-Tsallis divergence (QJT_q) demonstrated in Section 4.3. Using these reductions, we will prove computational hardness results and query complexity lower bounds for several problems related to the quantum q-Tsallis entropy difference under various circumstances.

We begin by defining the Quantum q-Tsallis Entropy Difference and the Quantum q-Tsallis Entropy Approximation, denoted by $\mathrm{TsallisQED}_q[g(n)]$ and $\mathrm{TsallisQEA}_q[t(n),g(n)]$, respectively. These definitions generalize the counterpart definitions in [BASTS10] from the von Neumann entropy (i.e., QJT_q with $q=1$) to the quantum q-Tsallis entropy for $1 \leq q \leq 2$.

Definition 4.17 (Quantum q-Tsallis Entropy Difference, $\mathrm{TsallisQED}_q$)**.** *Let Q_0 and Q_1 be quantum circuits acting on m qubits and having n specified output qubits, where $m(n)$ is a polynomial in n. Let ρ_i be the quantum state obtained by running Q_i on $|0\rangle^{\otimes m}$ and tracing out the non-output qubits. Let $g(n)$ be a positive efficiently computable function. Decide whether*:

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

Definition 4.18 (Quantum q-Tsallis Entropy Approximation, $\mathrm{TsallisQEA}_q$)**.** *Let Q be a quantum circuit acting on m qubits and having n specified output qubits, where $m(n)$ is a polynomial in n. Let ρ be the quantum state obtained by running Q on $|0\rangle^{\otimes m}$ and*

tracing out the non-output qubits. Let $g(n)$ and $t(n)$ be positive efficiently computable functions. Decide whether:

- Yes: *A quantum circuit Q such that $\mathrm{S}_q(\rho) \geq t(n) + g(n)$;*
- No: *A quantum circuit Q such that $\mathrm{S}_q(\rho) \leq t(n) - g(n)$.*

Notably, the quantum q-Tsallis entropy of any pure state is zero. Hence, similar to Section 3.3, it is reasonable to define *constant-rank* variants of $\textsc{TsallisQED}_q$ and $\textsc{TsallisQEA}_q$:

(1) $\textsc{ConstRankTsallisQED}_q$: the ranks of ρ_0 and ρ_1 are at most $O(1)$.

(2) $\textsc{ConstRankTsallisQEA}_q$: the rank of ρ is at most $O(1)$.

Next, we present the main theorem in this section:

Theorem 4.19 (Computational hardness of $\textsc{TsallisQED}_q$ and $\textsc{TsallisQEA}_q$)**.** *The promise problems $\textsc{TsallisQED}_q$ and $\textsc{TsallisQEA}_q$ capture the computational power of their respective complexity classes in the corresponding regimes of q*:

(1) *For any $q \in [1,2]$ and $n \geq 3$, the following holds: For any $1/\mathrm{poly}(n) \leq g_q(n) \leq 2^q \mathrm{H}_q(1/2)\left(1 - 2^{-\frac{qn}{2}+1}\right)$, $\textsc{ConstRankTsallisQED}_q[g_q(n)]$ is BQP-hard under Karp reduction. Consequently, $\textsc{ConstRankTsallisQEA}_q$ with $g(n) = \Theta(1)$ is BQP-hard under Turing reduction.*

(2) *For any $q \in \left(1, 1 + \frac{1}{n-1}\right]$ and $n \geq 90$, it holds that: For any $1/\mathrm{poly}(n) \leq g(n) \leq 1/400$, $\textsc{TsallisQED}_q[g(n)]$ is QSZK-hard under Karp reduction. Consequently, $\textsc{TsallisQEA}_q$ with $g(n) = \Theta(1)$ is QSZK-hard under Turing reduction.*

(3) *For any $n \geq 5$, it holds that: For $1/\mathrm{poly}(n) \leq g(n) \leq 1/150$, $\textsc{TsallisQEA}_{1+\frac{1}{n-1}}$ with $g(n)$ is NIQSZK-hard.*

In particular, Theorem 4.19(1) is derived from the pure-state reduction (Lemma 4.20), and the detailed statements are Theorem 4.23 and Theorem 4.24. Moreover, Theorem 4.19(2) is obtained through a mixed-state reduction (Lemma 4.21), and the detailed statements are Theorem 4.25 and Theorem 4.26. Furthermore, Theorem 4.19(3) follows from a tailor-made mixed state reduction for QSCMM (Lemma 4.22), and the detailed statement is Theorem 4.27.

Lastly, using the reductions in Lemma 4.21, we derive lower bounds on the quantum query and sample complexity for estimating $\mathrm{S}_q(\rho)$ where $1 < q \leq 1 + \frac{1}{n-1}$, as presented in Theorem 4.29 and Theorem 4.32. These theorems build on prior works in quantum query complexity [CFMdW10] and sample complexity [OW21] lower bounds for the trace distance. In addition, we provide quantum query and sample complexity lower bounds for estimating $\mathrm{S}_q(\rho)$ when $q \geq 1 + \Omega(1)$, leveraging the hard instances from [Bel19], as detailed in Theorem 4.28 and Theorem 4.31.

4.4.1 Pure-state reduction: PureQSD $\leq$ ConstRankTsallisQED$_q$ for $1 \leq q \leq 2$

The reduction in Lemma 4.20 is from the trace distance between two n-qubit pure states (PureQSD) to the quantum q-Tsallis entropy difference between two new constant-rank $(n+1)$-qubit states (ConstRankTsallisQED$_q$), for $1 \leq q \leq 2$.

Lemma 4.20 (PureQSD $\leq$ ConstRankTsallisQED$_q$)**.** *Let Q_0 and Q_1 be quantum circuits acting on n qubits and having the same number of output qubits. Let $|\psi_i\rangle$ be the quantum state obtained by running Q_i on $|0\rangle^{\otimes n}$. For any $b \in \{0,1\}$, there is a new quantum circuit Q'_b acting on $n+3$ qubits, using $O(1)$ queries to controlled-Q_0 and controlled-Q_1, as well as $O(1)$ one- and two-qubit gates. The circuit Q'_b prepares a new quantum state ρ'_b, which has constant rank and acts on $n' := n+1$ qubits, such that for any efficiently computable functions $\alpha(n)$ and $\beta(n)$, where $\beta(n) + \sqrt{1-\alpha(n)^2} < 1$, and any $q \in [1,2]$, the following holds*:

$$\begin{aligned} \mathrm{T}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \geq \alpha(n) \;&\Rightarrow\; \mathrm{S}_q(\rho'_0) - \mathrm{S}_q(\rho'_1) \geq g_q(n') = g_q(n+1), \\ \mathrm{T}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \leq \beta(n) \;&\Rightarrow\; \mathrm{S}_q(\rho'_1) - \mathrm{S}_q(\rho'_0) \geq g_q(n') = g_q(n+1), \end{aligned}$$

where $g_q(n+1) := 2^{-q} \cdot \mathrm{H}_q(1/2) \cdot \left(1 - \beta(n)^q - \sqrt{1-\alpha(n)^2}\right)$.

Proof. Our proof strategy is inspired by the proof of Corollary 7.21 and Lemma 7.22. We begin by considering the following constant-rank quantum states ρ'_0 and ρ'_1, which can be prepared by the quantum circuits Q'_0 and Q'_1, respectively:

$$\begin{aligned} \rho'_0 &:= (p_0|0\rangle\langle 0| + p_1|1\rangle\langle 1|) \otimes \frac{1}{2}\left(|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|\right) \\ \rho'_1 &:= \frac{1}{2}|0\rangle\langle 0| \otimes |\psi_0\rangle\langle\psi_0| + \frac{1}{2}|1\rangle\langle 1| \otimes |\psi_1\rangle\langle\psi_1|. \end{aligned}$$

Here, (p_0, p_1) is some two-element probability distribution that will be specified later. Furthermore, for any $b \in \{0,1\}$, the quantum circuit Q'_b uses $O(1)$ queries to controlled-Q_0 and controlled-Q_1 as well as $O(1)$ one- and two-qubit gates, as presented in Figures 7.1 and 7.2.

Using the pseudo-additivity of S_q (Lemma 3.28), we can obtain that:

$$\begin{aligned} &\mathrm{S}_q(\rho'_0) \\ &= \mathrm{H}_q(p_0) + \mathrm{S}_q\left(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\right) - (q-1) \cdot \mathrm{H}_q(p_0) \cdot \mathrm{S}_q\left(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\right) \\ &= \mathrm{H}_q(p_0) + (1 - (q-1)\mathrm{H}_q(p_0)) \cdot \mathrm{S}_q\left(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\right). \end{aligned} \tag{4.38}$$

By the joint q-Tsallis entropy theorem (Lemma 3.31), we have:

$$\mathrm{S}_q(\rho'_1) = \mathrm{H}_q(1/2) + 2^{-q}(\mathrm{S}_q(|\psi_0\rangle\langle\psi_0|) + \mathrm{S}_q(|\psi_1\rangle\langle\psi_1|)) = \mathrm{H}_q(1/2). \tag{4.39}$$

Combining Equation (4.38) and Equation (4.39), we conclude that:

$$\begin{aligned}
&\mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1') \\
&= (1-(q-1)\mathrm{H}_q(p_0)) \cdot \mathrm{S}_q\left(\frac{|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|}{2}\right) + \mathrm{H}_q(p_0) - \mathrm{H}_q\left(\frac{1}{2}\right) \\
&= (1-(q-1)\mathrm{H}_q(p_0)) \cdot \mathrm{QJT}_q(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) + \mathrm{H}_q(p_0) - \mathrm{H}_q\left(\frac{1}{2}\right).
\end{aligned} \tag{4.40}$$

Next, we choose $p_0 \in (0, 1/2)$ satisfying the following equality:

$$\mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q(p_0) = \frac{1-(q-1)\mathrm{H}_q(p_0)}{2}\left(\mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q\left(\frac{1-\alpha}{2}\right) + \mathrm{H}_q\left(\frac{1}{2}\right) \cdot \beta^q\right). \tag{4.41}$$

As a consequence, we can derive that:

- For the case where $\mathrm{T}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \geq \alpha$, plugging the lower bound on QJT_q in terms of the trace distance (Lemma 4.12) into Equation (4.40) and Equation (4.41), we obtain

$$\begin{aligned}
\mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1') &\geq (1-(q-1)\mathrm{H}_q(p_0)) \cdot \left(\mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q\left(\frac{1-\alpha}{2}\right)\right) + \mathrm{H}_q(p_0) - \mathrm{H}_q\left(\frac{1}{2}\right) \\
&= \frac{1-(q-1)\mathrm{H}_q(p_0)}{2}\left(\mathrm{H}_q\left(\frac{1}{2}\right) \cdot (1-\beta^q) - \mathrm{H}_q\left(\frac{1-\alpha}{2}\right)\right) := \tilde{g}_q.
\end{aligned}$$

- For the case where $\mathrm{T}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \leq \beta$, plugging the upper bound on QJT_q in terms of the trace distance (Lemma 4.13) into Equation (4.40) and Equation (4.41), we obtain

$$\begin{aligned}
\mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1') &\leq (1-(q-1)\mathrm{H}_q(p_0)) \cdot \beta^q \cdot \mathrm{H}_q\left(\frac{1}{2}\right) + \mathrm{H}_q(p_0) - \mathrm{H}_q\left(\frac{1}{2}\right) \\
&= -\frac{1-(q-1)\mathrm{H}_q(p_0)}{2}\left(\mathrm{H}_q\left(\frac{1}{2}\right) \cdot (1-\beta^q) - \mathrm{H}_q\left(\frac{1-\alpha}{2}\right)\right) = -\tilde{g}_q.
\end{aligned}$$

It is left to show a lower bound on $\tilde{g}(n)$. By $\mathrm{H}_q(x) \leq \mathrm{H}_q(1/2)$ in Lemma 3.8, we have

$$\frac{1-(q-1)\cdot\mathrm{H}_q(p_0)}{2} \geq \frac{1}{2} - \frac{q-1}{2} \cdot \mathrm{H}_q\left(\frac{1}{2}\right) = 2^{-q}. \tag{4.42}$$

Plugging the Tsallis binary entropy upper bound (Lemma 4.15) and Equation (4.42) into $\tilde{g}(n)$, we complete the proof by concluding the following:

$$\tilde{g}_q(n) \geq 2^{-q} \cdot \mathrm{H}_q(1/2) \cdot \left(1 - \beta(n)^q - \sqrt{1-\alpha^2(n)}\right) := g_q(n+1) = g_q(n'). \qquad \square$$

4.4.2 Mixed-state reductions

In this subsection, we present two reductions for mixed states. The first reduction is from the trace distance between two n-qubit states (QSD), to the quantum q-Tsallis entropy difference between two new $(n+1)$-qubit states ($\textsc{TsallisQED}_q$), for $1 \leq q \leq 2$, under appropriate assumptions about $\mathrm{S}_q(\rho_0)$ and $\mathrm{S}_q(\rho_1)$, as stated in Lemma 4.21. The second reduction is from the trace distance between an n-qubit quantum state (QSCMM) and the n-qubit maximally mixed state to the quantum q-Tsallis entropy of the state ($\textsc{TsallisQEA}_q$) for $q = 1 + \frac{1}{n-1}$, as state in Lemma 4.22.

QSD $\leq$ TsallisQED$_q$ for $1 \leq q \leq 2$

Lemma 4.21 (QSD $\leq$ TsallisQED$_q$). *Let Q_0 and Q_1 be quantum circuits acting on m qubit, defined in Definition 4.17, that prepares the purification of n-qubit mixed states ρ_0 and ρ_1, respectively. For any $b \in \{0,1\}$, there is a new quantum circuits Q'_b acting on $m+3$ qubits, requiring $O(1)$ queries to controlled-Q_0 and controlled-Q_1, as well as $O(1)$ one- and two- qubit gates, that prepares a new n'-qubit mixed state ρ'_b, where $n' := n+1$, such that: For any ρ_0 and ρ_0 satisfying $\max\{\mathrm{S}_q(\rho_0), \mathrm{S}_q(\rho_1)\} \leq \gamma(n)$ with $\mathrm{S}_q(I/2) \leq \gamma(n) \leq \mathrm{S}_q((I/2)^{\otimes n})$, any $\varepsilon(n) \in (0, 1/2)$, and any $q \in [1,2]$, there is a $g(n) > 0$ with appropriate ranges of γ, ε, and n such that*

$$\begin{aligned} \mathrm{T}(\rho_0,\rho_1) \geq 1-\varepsilon(n) \quad &\Rightarrow\ \mathrm{S}_q(\rho'_0) - \mathrm{S}_q(\rho'_1) \geq g_q(n') = g_q(n+1), \\ \mathrm{T}(\rho_0,\rho_1) \leq \varepsilon(n) \quad &\Rightarrow\ \mathrm{S}_q(\rho'_1) - \mathrm{S}_q(\rho'_0) \geq g_q(n') = g_q(n+1), \end{aligned}$$

where $g_q(n) := \frac{1}{2}\mathrm{H}_q\left(\frac{1}{2}\right) - \gamma(n)\left(\frac{1}{2} - \frac{1}{2^q}\right) - \left(\frac{1}{2} + \frac{1}{2^q}\right)\left(\frac{\varepsilon(n)^q}{2^q}\ln_q\left(2^n\right) + \mathrm{H}_q\left(\frac{1}{2}\right)\sqrt{\varepsilon(n)(2-\varepsilon(n))}\right)$.

Proof. Our proof strategy is somewhat inspired by [BASTS10, Section 5.4]. We start by considering the following mixed states ρ'_0 and ρ'_1:

$$\begin{aligned} \rho'_0 &:= (\vartheta|0\rangle\langle 0| + (1-\vartheta)|1\rangle\langle 1|) \otimes \rho_+, \text{ where } 2\mathrm{H}_q(\vartheta) = \mathrm{H}_q\left(\frac{1}{2}\right) \text{ and } \rho_+ := \frac{\rho_0+\rho_1}{2}, \\ \rho'_1 &:= \frac{1}{2}|0\rangle\langle 0| \otimes \rho_0 + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_1. \end{aligned}$$

These states ρ'_0 and ρ'_1 can be prepared by the quantum circuits Q'_0 and Q'_1, respectively. For instance, adapting the constructions in Figures 7.1 and 7.2, for any $b \in \{0,1\}$, the quantum circuit Q'_b uses $O(1)$ queries to controlled-Q_0 and controlled-Q_1, as well as $O(1)$ one- and two-qubit gates.

Utilizing the pseudo-additivity of S_q (Lemma 3.28), we have:

$$\begin{aligned} \mathrm{S}_q(\rho'_0) &= \mathrm{H}_q(\vartheta) + (1-(q-1)\mathrm{H}_q(\vartheta))\mathrm{S}_q(\rho_+) \\ &= \frac{1}{2}\mathrm{H}_q\left(\frac{1}{2}\right) + \left(1 - \frac{q-1}{2}\cdot \mathrm{H}_q\left(\frac{1}{2}\right)\right)\mathrm{S}_q(\rho_+). \end{aligned} \tag{4.43}$$

Using the joint q-Tsallis entropy theorem (Lemma 3.31), we obtain:

$$\mathrm{S}_q(\rho'_1) = \mathrm{H}_q\left(\frac{1}{2}\right) + \frac{1}{2^q}(\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)). \tag{4.44}$$

Combining Equation (4.44) and Equation (4.43), we obtain:

$$\mathrm{S}_q(\rho'_0) - \mathrm{S}_q(\rho'_1) = \left(1 - \frac{q-1}{2}\cdot \mathrm{H}_q\left(\frac{1}{2}\right)\right)\mathrm{S}_q(\rho_+) - \frac{1}{2}\mathrm{H}_q\left(\frac{1}{2}\right) - \frac{1}{2^q}(\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)) \tag{4.45}$$

Next, we can consider the following two cases:

- For the case where $\mathrm{T}(\rho_0,\rho_1) \geq 1-\varepsilon$, using the lower bound on QJT$_q$(Lemma 4.12), it holds that:

$$\mathrm{S}_q(\rho_+) - \frac{1}{2}(\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)) = \mathrm{QJT}_q(\rho_0,\rho_1) \geq \mathrm{H}_q\left(\frac{1}{2}\right) - \mathrm{H}_q\left(\frac{1-\mathrm{T}(\rho_0,\rho_1)}{2}\right). \tag{4.46}$$

Substituting Equation (4.46) into Equation (4.45), we obtain:

$\mathrm{S}_q(\rho'_0) - \mathrm{S}_q(\rho'_1)$

$$
\begin{aligned}
&\geq \left(1 - \tfrac{q-1}{2} \cdot \mathrm{H}_q\left(\tfrac{1}{2}\right)\right)\left(\tfrac{1}{2}(\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)) + \mathrm{H}_q\left(\tfrac{1}{2}\right) - \mathrm{H}_q\left(\tfrac{\varepsilon}{2}\right)\right) - \tfrac{1}{2}\mathrm{H}_q\left(\tfrac{1}{2}\right) - \tfrac{1}{2^q}(\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)) \\
&\geq \left(\tfrac{1}{2} - \tfrac{1}{2^q} - \tfrac{q-1}{4}\mathrm{H}_q\left(\tfrac{1}{2}\right)\right)(\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)) + \left(1 - \tfrac{q-1}{2}\mathrm{H}_q\left(\tfrac{1}{2}\right)\right)\mathrm{H}_q\left(\tfrac{1}{2}\right)\left(1 - \sqrt{\varepsilon(2-\varepsilon)}\right) - \tfrac{1}{2}\mathrm{H}_q\left(\tfrac{1}{2}\right) \\
&\geq \left(\tfrac{1}{2} + \tfrac{1}{2^q}\right)\mathrm{H}_q\left(\tfrac{1}{2}\right)\left(1 - \sqrt{\varepsilon(2-\varepsilon)}\right) - \tfrac{1}{2}\mathrm{H}_q\left(\tfrac{1}{2}\right) \\
&= \tfrac{1}{2^q}\mathrm{H}_q\left(\tfrac{1}{2}\right) - \left(\tfrac{1}{2} + \tfrac{1}{2^q}\right)\mathrm{H}_q\left(\tfrac{1}{2}\right)\sqrt{\varepsilon(2-\varepsilon)} \coloneqq \tilde{g}_q^{\mathtt{Y}}(\varepsilon).
\end{aligned}
$$

Here, the third line uses the Tsallis binary entropy upper bound (Lemma 4.15) and the fact that $1 - \frac{q-1}{2}\mathrm{H}_q\left(\frac{1}{2}\right) > 0$ for $q \in [1, 2]$. The last line relies on the following facts: (a) $\mathrm{S}_q(\rho) \geq 0$ for any state ρ; (b) $2\left(\frac{1}{2} - \frac{1}{2^q} - \frac{q-1}{4}\mathrm{H}_q\left(\frac{1}{2}\right)\right) = \frac{1}{2} - \frac{1}{2^q} \geq 0$ for $q \in [1, 2]$; and (c) $1 - \frac{q-1}{2}\mathrm{H}_q\left(\frac{1}{2}\right) = \frac{1}{2} + \frac{1}{2^q}$;

- For the case where $\mathrm{T}(\rho_0, \rho_1) \leq \varepsilon$, utilizing Fannes' inequality for QJT_q (Lemma 3.32), it holds that:

$$
\begin{aligned}
\mathrm{S}_q(\rho_+) &\leq \frac{|\mathrm{S}_q(\rho_+) - \mathrm{S}_q(\rho_0)|}{2} + \frac{|\mathrm{S}_q(\rho_+) - \mathrm{S}_q(\rho_1)|}{2} + \frac{\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)}{2} \\
&\leq \mathrm{T}(\rho_+, \rho_b)^q \cdot \ln_q(2^n - 1) + \mathrm{H}_q(\mathrm{T}(\rho_+, \rho_b)) + \frac{\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)}{2} \\
&\leq \left(\frac{\mathrm{T}(\rho_0, \rho_1)}{2}\right)^q \ln_q\left(2^n\right) + \mathrm{H}_q\left(\frac{\mathrm{T}(\rho_0, \rho_1)}{2}\right) + \frac{\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)}{2}
\end{aligned} \tag{4.47}
$$

Here, the first line is due to the triangle inequality, and the last line is because $\ln_q(x)$ is monotonically increasing on $x > 0$ for any fixed $q > 1$.

Plugging Equation (4.47) into Equation (4.45), we can derive that:

$$
\begin{aligned}
&\mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1') \\
&\leq \left(1 - \tfrac{q-1}{2}\mathrm{H}_q\left(\tfrac{1}{2}\right)\right)\left((\tfrac{\varepsilon}{2})^q \ln_q(2^n) + \mathrm{H}_q(\tfrac{\varepsilon}{2}) + \tfrac{1}{2}(\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1))\right) - \tfrac{1}{2}\mathrm{H}_q\left(\tfrac{1}{2}\right) - \tfrac{1}{2^q}(\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)) \\
&\leq \left(\tfrac{1}{2} - \tfrac{1}{2^q} - \tfrac{q-1}{4}\mathrm{H}_q\left(\tfrac{1}{2}\right)\right)(\mathrm{S}_q(\rho_0) + \mathrm{S}_q(\rho_1)) + \left(1 - \tfrac{q-1}{2}\mathrm{H}_q\left(\tfrac{1}{2}\right)\right)\left((\tfrac{\varepsilon}{2})^q \ln_q(2^n) + \mathrm{H}_q\left(\tfrac{1}{2}\right)\sqrt{\varepsilon(2-\varepsilon)}\right) - \tfrac{1}{2}\mathrm{H}_q\left(\tfrac{1}{2}\right) \\
&\leq \left(\tfrac{1}{2} - \tfrac{1}{2^q}\right) \cdot \gamma + \left(\tfrac{1}{2} + \tfrac{1}{2^q}\right)\left((\tfrac{\varepsilon}{2})^q \cdot \ln_q(2^n) + \mathrm{H}_q\left(\tfrac{1}{2}\right)\sqrt{\varepsilon(2-\varepsilon)}\right) - \tfrac{1}{2}\mathrm{H}_q\left(\tfrac{1}{2}\right) \coloneqq -\tilde{g}_q^{\mathtt{N}}(\varepsilon, n, \gamma).
\end{aligned}
$$

Here, the third line uses the Tsallis binary entropy upper bound (Lemma 4.15) and the fact that $1 - \frac{q-1}{2}\mathrm{H}_q\left(\frac{1}{2}\right) > 0$ for $q \in [1, 2]$. The last line relies on the following facts: (a) $1 - \frac{q-1}{2}\mathrm{H}_q\left(\frac{1}{2}\right) = \frac{1}{2} + \frac{1}{2^q}$; (b) $2\left(\frac{1}{2} - \frac{1}{2^q} - \frac{q-1}{4}\mathrm{H}_q\left(\frac{1}{2}\right)\right) = \frac{1}{2} - \frac{1}{2^q} \geq 0$ for $q \in [1, 2]$; and (c) $\mathrm{S}_q(\rho) \leq \gamma \leq \mathrm{S}_q((I/2)^{\otimes n})$ for any n-qubit state ρ.

It is evident that $\tilde{g}_q^{\mathtt{N}}(\varepsilon, n, \gamma)$ is monotonically decreasing on $\gamma \geq 0$ for any fixed q, ε, and n. Consequently, it remains to show that $\tilde{g}_q^{\mathtt{Y}}(\varepsilon) \geq \tilde{g}_q^{\mathtt{N}}(\varepsilon, n, \mathrm{H}_q(1/2)) \geq \tilde{g}_q^{\mathtt{N}}(\varepsilon, n, \gamma)$ for $\mathrm{H}_q(1/2) = \mathrm{S}_q(I/2) \leq \gamma \leq \mathrm{S}_q((I/2)^{\otimes n})$. In particular, by noting that $(\varepsilon/2)^q \cdot \ln_q\left(2^n\right) \geq 0$ for $q \geq 1$ and $\varepsilon \geq 0$, we obtain:

$$
\begin{aligned}
&\tilde{g}_q^{\mathtt{Y}}(\varepsilon) - \tilde{g}_q^{\mathtt{N}}\left(\varepsilon, n, \mathrm{H}_q\left(\frac{1}{2}\right)\right) \\
&= \frac{1}{2^q}\mathrm{H}_q\left(\frac{1}{2}\right) + \left(\frac{1}{2} + \frac{1}{2^q}\right)\left(\frac{\varepsilon}{2}\right)^q \ln_q\left(2^n\right) - \frac{1}{2}\mathrm{H}_q\left(\frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{2^q}\right)\mathrm{H}_q\left(\frac{1}{2}\right) \\
&= \left(\frac{1}{2} + \frac{1}{2^q}\right)\left(\frac{\varepsilon}{2}\right)^q \ln_q\left(2^n\right)
\end{aligned}
$$

≥ 0.

Therefore, we complete the proof by choosing $g_q(n) = \tilde{g}_q^{\mathtt{N}}(\varepsilon(n), n, \gamma(n))$, specifically:

$$g_q(n) \coloneqq \frac{1}{2}\mathrm{H}_q\Big(\frac{1}{2}\Big) - \gamma(n)\Big(\frac{1}{2} - \frac{1}{2^q}\Big) - \Big(\frac{1}{2} + \frac{1}{2^q}\Big)\left(\frac{\varepsilon(n)^q}{2^q}\ln_q\Big(2^n\Big) + \mathrm{H}_q\Big(\frac{1}{2}\Big)\sqrt{\varepsilon(n)(2-\varepsilon(n))}\right). \quad \square$$

QSCMM $\leq$ TsallisQEA$_q$ for $q(n) = 1 + \frac{1}{n-1}$

Lemma 4.22 (QSCMM $\leq$ TsallisQEA$_q$)**.** *Let Q be a quantum circuit acting on m qubit, defined in Definition 4.18, that prepares the purification of n-qubit mixed states ρ, respectively. For any ρ, any $n \geq 5$, and any $q(n) = 1 + 1/(n-1)$, let $t(n) \coloneqq \frac{1}{4}\Big(3n - n^{1+\frac{1}{n}} - 1\Big)$, we have:*

$$\begin{aligned} &\mathrm{T}\Big(\rho, (I/2)^{\otimes n}\Big) \leq 1/n && \Rightarrow\ \mathrm{S}_q(\rho) > t(n) + 1/150, \\ &\mathrm{T}\Big(\rho, (I/2)^{\otimes n}\Big) \geq 1 - 1/n && \Rightarrow\ \mathrm{S}_q(\rho) < t(n) - 1/150. \end{aligned}$$

Proof. Let $\rho = \sum_{i\in[2^n]} \lambda_i |v_i\rangle\langle v_i|$ be the spectral decomposition of ρ, where $\{v_i\}_{i\in[2^n]}$ is an orthonormal basis and $p \coloneqq (\lambda_1, \cdots, \lambda_{2^n})$ is a probability distribution of dimension 2^n. And let ν be the uniform distribution of dimension 2^n. Noting that ρ and $(I/2)^{\otimes n}$ commute, we have $\mathrm{T}(\rho, (I/2)^{\otimes n}) = \mathrm{TV}(p, \nu)$ and $\mathrm{S}_q(\rho) = \mathrm{H}_q(p)$.

Let $t(n) \coloneqq \frac{1}{4}\Big(3n - n^{1+\frac{1}{n}} - 1\Big)$. Next, we can consider the following two cases:

- For the case where $\mathrm{T}(\rho, (I/2)^{\otimes n}) \leq 1/n$, by the lower bound on $\mathrm{H}_q(p)$ in Lemma 4.16, it follows that

$$\begin{aligned} \mathrm{S}_q(\rho) &\geq \ln_{1+\frac{1}{n-1}}\Big(2^n\Big) \cdot \Big(1 - \mathrm{T}\Big(\rho, (I/2)^{\otimes n}\Big) - 2^{-n}\Big) \\ &\geq (n-1)\left(1 - \frac{1}{2}\cdot\Big(\frac{1}{2}\Big)^{\frac{1}{n-1}}\right)\Big(1 - \frac{1}{n} - 2^{-n}\Big) \coloneqq \tau_{\mathtt{Y}}(n). \end{aligned}$$

  By a direct calculation, we obtain:

$$\begin{aligned} &\mathrm{S}_q(\rho) - t(n) \geq \tau_{\mathtt{Y}}(n) - t(n) = g_1(n) + g_2(n) + g_3(n) - \frac{7}{4}, \\ &\text{where } g_1(n) \coloneqq 2^{-n} + \frac{1 - 2^{\frac{n}{1-n}}}{n} + 2^{\frac{n^2}{1-n}}(n-1) + \frac{n}{4}\Big(1 - 2^{\frac{1}{1-n}}\Big), \\ &\qquad g_2(n) \coloneqq 2^{\frac{1}{1-n}} - 2^{-n}n, \quad g_3(n) \coloneqq \frac{n}{4}\Big(n^{\frac{1}{n}} - 2^{\frac{1}{1-n}}\Big). \end{aligned} \tag{4.48}$$

  Through a fairly tedious calculation, we know that $g_1(n)$, $g_2(n)$, and $g_3(n)$ defined in Equation (4.48) satisfy the properties in Fact 4.22.1, and the proof is deferred to the end of this subsection.

Fact 4.22.1. *Let $g_1(n)$, $g_2(n)$, and $g_3(n)$ be functions defined in Equation (4.48). It holds that:*

(1) *For $n \geq 3$, $g_1(n) \geq 0$.*

(2) *For $n \geq 3$, $g_2(n)$ and $g_3(n)$ are monotonically increasing.*

Combining Equation (4.48) and Fact 4.22.1, we obtain that:

$$\forall n \geq 5,\ \mathrm{S}_q(\rho) - t(n) \geq \tau_{\mathtt{Y}}(n) - t(n) \geq g_2(n) + g_3(n) - \frac{7}{4} > \frac{1}{150}. \tag{4.49}$$

- For the case where $\mathrm{T}(\rho, (I/2)^{\otimes n}) \geq 1 - 1/n$, by noting $\mathrm{T}(\rho, (I/2)^{\otimes n})q \geq \left(1 - \frac{1}{n}\right)\left(1 + \frac{1}{n-1}\right) = 1$ and using the upper bound on $\mathrm{H}_q(p)$ in Lemma 4.16, it holds that

$$\begin{aligned}
\mathrm{S}_q(\rho) &\leq \ln_{1+\frac{1}{n-1}}\left(2^n\left(1 - \mathrm{T}\left(\rho, (I/2)^{\otimes n}\right)\right)\right) \\
&\leq \ln_{1+\frac{1}{n}}\left(2^n\left(1 - \mathrm{T}\left(\rho, (I/2)^{\otimes n}\right)\right)\right) \\
&\leq n\left(1 - \frac{1}{2} \cdot n^{1/n}\right) \coloneqq \tau_{\mathtt{N}}(n).
\end{aligned}$$

Here, the second line is because $\ln_q(x) < \ln_{q'}(x)$ for $q > q' > 0$ and $\frac{1}{n-1} > \frac{1}{n}$.

Similarly, a direct calculation implies that:

$$t(n) - \mathrm{S}_q(\rho) \geq t(n) - \tau_{\mathtt{N}}(n) = \frac{g_4(n) - 1}{4},\ \text{where } g_4(n) \coloneqq n\left(n^{\frac{1}{n}} - 1\right). \tag{4.50}$$

Next, we will prove that $g_4(n)$ is monotonically non-decreasing for $n \geq 2$. We proceed by expressing the first and second derivative of $g_4(n)$:

$$\frac{\mathrm{d}}{\mathrm{d}n} g_4(n) = \frac{n^{\frac{1}{n}}}{n}(n - \log(n) + 1) - 1,\ \text{and}\ \frac{\mathrm{d}^2}{\mathrm{d}n^2} g_4(n) = \frac{n^{\frac{1}{n}}}{n^3}\left((\log(n) - 1)^2 - n\right).$$

As $\sqrt{n} > \log n$, $\frac{\mathrm{d}^2}{\mathrm{d}n^2} g_4(n)$ has one zero at $n = 1$. As $\frac{\mathrm{d}^2}{\mathrm{d}n^2} g_4(n)\Big|_{n=e} = -e < 0$, we have that $\frac{\mathrm{d}}{\mathrm{d}n} g_4(n)$ is monotonically decreasing for $n \geq 2$, and thus, $\frac{\mathrm{d}}{\mathrm{d}n} g_4(n) \geq \lim_{n\to\infty} \frac{\mathrm{d}}{\mathrm{d}n} g_4(n) = 0$ for $n \geq 2$. Hence, we conclude that $g_4(n)$ is monotonically non-decreasing for $n \geq 2$. Hence, combining with Equation (4.50), we obtain:

$$\forall n \geq 3,\ t(n) - \mathrm{S}_q(\rho) \geq t(n) - \tau_{\mathtt{N}}(n) = \frac{g_4(n) - 1}{4} > \frac{1}{13}. \tag{4.51}$$

Lastly, we finish the proof by comparing Equation (4.49) with Equation (4.51). □

Proof of Fact 4.22.1. We begin by defining $f_1(n) \coloneqq 2^{-n} + \frac{1 - 2^{\frac{n}{1-n}}}{n}$, $f_2(n) \coloneqq 2^{\frac{n^2}{1-n}}(n-1)$, and $f_3(n) \coloneqq \frac{n}{4}\left(1 - 2^{\frac{1}{1-n}}\right)$ such that $g_1(n) = f_1(n) + f_2(n) + f_3(n)$. We then prove the first item separately:

- For $f_1(n)$, since $2^{\frac{n}{1-n}} = 2^{-\left(1 + \frac{1}{n-1}\right)}$, we know that $f_1(n)$ is monotonically decreasing for $n \geq 2$, and thus, $f_1(n) \geq \lim_{n\to\infty} f_1(n) = 0$ for $n \geq 2$.
- For $f_2(n)$, noting that $\frac{\mathrm{d}}{\mathrm{d}n} f_2(n) = \frac{2^{n^2/(1-n)}}{n-1}(-\log(2)n^2 + (1 + \log(2))n - 1)$, we obtain that $f_2(n)$ is monotonically decreasing for $n \geq 3 > \frac{1 + 2\log(2) + \sqrt{1 + 4\log(2)^2}}{2\log(2)} \approx 2.9544$, and consequently, $f_2(n) \geq \lim_{n\to\infty} g_2(n) = 0$ for $n \geq 3$.
- For $f_3(n)$, it suffices to show that $2^{1/(1-n)} \leq 1$ for $n \geq 3$. Since $2^{1/(1-n)}$ is monotonically increasing for $n \geq 3$, we prove the first item by noting that $2^{1/(1-n)} \leq \lim_{n\to\infty} 2^{1/(1-n)} = 1$.

For $g_2(n)$, noting that $\frac{\mathrm{d}}{\mathrm{d}n} g_3(n) = \frac{2^{\frac{1}{1-n}}\log(2)}{(n-1)^2} + 2^{-n}(n\log(2) - 1)$ and $n\log(2) \geq 1$ for $n \geq 2$, we obtain that $g_3(n)$ is monotonically increasing for $n \geq 2$.

For $g_3(n)$, since $2^{-1/x}$ is monotonically increasing for $x \geq 1$, we have $g_3(n) \geq \frac{1}{4}n(n^{1/n} - 2^{-1/n})$. It remains to show that $\tilde{g}_3(n) \coloneqq \frac{1}{4}n(n^{1/n} - 2^{-1/n})$ are monotonically increasing for $n \geq 3$, namely:

$$\frac{\mathrm{d}}{\mathrm{d}n}\tilde{g}_3(n) = \frac{1}{4n}\underbrace{\left(n^{1/n} - 2^{-1/n}\log(2)\right)}_{f_4(n)} + \underbrace{\frac{1}{4n}\left(n^{1/n}n - n^{1/n}\log(n) - n2^{-1/n}\right)}_{f_5(n)} \geq 0. \tag{4.52}$$

Noting that $\frac{\mathrm{d}}{\mathrm{d}n}f_4(n) = -\frac{1}{n^2}\left(n^{1/n}(\log(n)-1) + 2^{-1/n}\log^2(2)\right) < 0$ for $n > e$, namely $f_4(n)$ is monotonically decreasing for $n \geq 3$, we obtain that $\frac{f_4(n)}{4n} \geq \frac{1}{4n}\lim_{n\to\infty} f_4(n) = \frac{1}{4n} > 0$. Let $f_6(n) \coloneqq \left(\frac{1}{2n}\right)^{1/n}$. Notice that

$$\frac{\mathrm{d}}{\mathrm{d}n}f_6(n) = 2^{-1/n}\left(\frac{1}{n}\right)^{\frac{1}{n}+2}\left(-\log\left(\frac{1}{n}\right) - 1 + \log(2)\right) \geq 0 \text{ for } n \geq e/2.$$

It holds that $f_6(n) = \left(\frac{1}{2n}\right)^{1/n} \geq f_6(2) = 1/2$ for $n \geq 2$. Consequently, we can derive that:

$$\begin{aligned}\left(\frac{1}{n}\right)^{\frac{1}{n}}\frac{\mathrm{d}f_5(n)}{\mathrm{d}n} &= \frac{(\log(n)-1)\log(n) - \left(\frac{1}{2n}\right)^{\frac{1}{n}}n\log(2)}{4n^3} \\ &\leq \frac{1}{4n^2}\left(\frac{(\log(n)-1)\log(n)}{n} - \frac{\log(2)}{2}\right) < 0.\end{aligned}$$

Here, the last inequality follows by assuming $f_7(n) \coloneqq \frac{\log(n)(\log(n)-1)}{n} < \frac{\log(2)}{2}$. A direct calculation implies that $\frac{\mathrm{d}}{\mathrm{d}n}f_7(n) = -\frac{1}{n^2}((\log(n)-3)\log(n)+1) = 0$ have two zeros at $n = \exp(\frac{3\pm\sqrt{5}}{2})$. Therefore, we establish Equation (4.52) by noticing

$$f_7(n) \leq \max\left\{f_7\left(\frac{3-\sqrt{5}}{2}\right), f_7\left(\frac{3+\sqrt{5}}{2}\right)\right\} < \frac{\log(2)}{2}. \qquad \square$$

4.4.3 Computational hardness results

In this subsection, we present the computational hardness results for various settings of TsallisQED$_q$ and TsallisQEA$_q$ by using our reductions established in Section 4.4.1 and Section 4.4.2.

BQP hardness results

Theorem 4.23 (ConstRankTsallisQED$_q$ is BQP-hard for $1 \leq q \leq 2$)**.** *For any $q \in [1,2]$ and any $n \geq 3$, the following holds*:

$$\forall g_q(n) \in \left[\frac{1}{\mathrm{poly}(n)}, 2^{-q}\mathrm{H}_q\left(\frac{1}{2}\right)\left(1 - 2^{-\frac{qn}{2}+1}\right)\right],\ \textsc{ConstRankTsallisQED}_q[g_q(n)] \textit{ is } \mathsf{BQP}\textit{-hard.}$$

Proof. Using Lemma 3.38, we have that PureQSD$\left[\sqrt{1-2^{-2\hat{n}}}, 2^{-(\hat{n}+1)/2}\right]$ is BQP-hard for $\hat{n} \geq 2$. Let Q_0 and Q_1 be the corresponding BQP-hard instance such that these circuits are polynomial-size and prepare the pure states $|\psi_0\rangle\langle\psi_0|$ and $|\psi_1\rangle\langle\psi_1|$, respectively. Leveraging the reduction from PureQSD to ConstRankTsallisQED$_q$ (Lemma 4.20), there are two polynomial-size quantum circuits Q_0' and Q_1', which prepares the purifications of

constant-rank states ρ_0' and ρ_1', such that: For any $1 \le q \le 2$ and any $n = \hat{n} + 1 \ge 3$,

$$\begin{aligned} \mathrm{T}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \ge \sqrt{1 - 2^{-2\hat{n}}} \quad &\Rightarrow \ \mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1') \ge g_q(n) = g_q(\hat{n}+1), \\ \mathrm{T}(|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|) \le 2^{-(\hat{n}+1)/2} \quad &\Rightarrow \ \mathrm{S}_q(\rho_1') - \mathrm{S}_q(\rho_0') \le g_q(n) = g_q(\hat{n}+1). \end{aligned}$$

Hence, we complete the proof by a direct calculation:

$$\begin{aligned} g_q(n) &\coloneqq 2^{-q} \cdot \mathrm{H}_q(1/2) \cdot \left(1 - 2^{-\frac{qn}{2}} - \sqrt{1 - (1 - 2^{-2(n-1)})}\right) \\ &\ge 2^{-q} \cdot \mathrm{H}_q(1/2) \cdot \left(1 - 2^{-\frac{qn}{2}+1}\right). \end{aligned}$$

□

Theorem 4.24 (ConstRankTsallisQEA$_q$ is BQP-hard under Turing reduction for $1 \le q \le 2$)**.** *For any $q \in [1,2]$ and any $n \ge 3$, the following holds*:

ConstRankTsallisQEA$_q$ *with $g(n) = \Theta(1)$ is* BQP*-hard under Turing reduction.*

Proof. For any $1 \le q \le 2$ and $n \ge 3$, since ConstRankTsallisQED$_q[\hat{g}_q(n)]$ is BQP-hard under Karp reduction (Theorem 4.23), where $\hat{g}_q(n) \coloneqq 2^{-q}\mathrm{H}_q(1/2)\left(1 - 2^{-n/2+1}\right)$, it suffices to provide an algorithm for ConstRankTsallisQED$_q[\hat{g}_q(n)]$ by leveraging ConstRankTsallisQEA$_q[t(n), g(n)]$ as subroutines, with appropriately adaptive choices of $t(n)$ and $g(n)$.

Let Q_0 and Q_1 be the corresponding BQP-hard instance such that these circuits are polynomial-size and prepare the constant-rank states ρ_0 and ρ_1, respectively. Let $\texttt{TsallisQEA}_q(Q, t(n), g(n))$ be the subroutine for decide whether $\mathrm{S}_q(\rho) \ge t(n) + g(n)$ or $\mathrm{S}_q(\rho) \le t(n) - g(n)$. Next, we estimate $\mathrm{S}_q(\rho_b)$ to within additive error $\hat{g}_q(n)/2$ for $b \in \{0,1\}$. This procedure, inspired by [Amb14, Appendix A.2 Part 1], is denoted by `BiSearch`, as presented in Algorithm 4.4.1.

Algorithm 4.4.1: Tsallis entropy estimation $\texttt{BiSearch}(Q, \tau, g)$ via queries to $\texttt{TsallisQEA}_q$.

Input : A quantum circuit Q that prepares the purification of ρ, an upper bound τ on the q-Tsallis entropy $\mathrm{S}_q(\rho)$, and a precision parameter g.
Output: Return t such that $|t - \mathrm{S}_q(\rho)| \le g/2$.
1. Let $\delta \leftarrow g/2$, and set the interval $[a,b] \leftarrow [0, \tau]$.
2. $b - a > \hat{g}/2$ **:**
  2.1 Query $\texttt{TsallisQEA}_q\left(Q, \frac{a+b}{2}, \frac{\delta}{4}\right)$ to decide whether $\mathrm{S}_q(\rho) \ge \frac{a+b}{2} + \frac{\delta}{4}$ or $\mathrm{S}_q(\rho) \le \frac{a+b}{2} - \frac{\delta}{4}$.
  2.2 If $\mathrm{S}_q(\rho) \ge \frac{a+b}{2} + \frac{\delta}{4}$ **:**
    $[a,b] \leftarrow \left[\frac{a+b}{2} - \frac{\hat{g}}{4}, b\right]$.
  Elseif $\mathrm{S}_q(\rho) \le \frac{a+b}{2} - \frac{\delta}{4}$. **:**
    $[a,b] \leftarrow \left[a, \frac{a+b}{2} + \frac{\hat{g}}{4}\right]$.
3. Return $\frac{a+b}{2}$.

To solve ConstRankTsallisQED$_q[\hat{g}_q(n)]$, noting that $\max\{\mathrm{rank}(\rho_0), \mathrm{rank}(\rho_1)\} \le r \le O(1)$, we choose $\tau(n) = \mathrm{S}_q((I/2)^{\otimes r})$. Then, let $t_0(n) = \texttt{BiSearch}(Q_0, \tau(n), \hat{g}_q(n))$

and $t_1(n) = \texttt{BiSearch}(Q_1, \tau(n), \hat{g}_q(n))$, we obtain:

$$\begin{aligned} \mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1) \geq \hat{g}_q(n) \quad &\Rightarrow t_0(n) - t_1(n) \geq \mathrm{S}_q(\rho_0) - \frac{\hat{g}_q(n)}{2} - \left(\mathrm{S}_q(\rho_1) + \frac{\hat{g}_q(n)}{2}\right) \geq 0, \\ \mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1) \leq -\hat{g}_q(n) \quad &\Rightarrow t_0(n) - t_1(n) \leq \mathrm{S}_q(\rho_0) + \frac{\hat{g}_q(n)}{2} - \left(\mathrm{S}_q(\rho_1) - \frac{\hat{g}_q(n)}{2}\right) \leq 0. \end{aligned} \tag{4.53}$$

Note that $\hat{g}_q(n) = 2^{-q}\mathrm{H}_q(1/2)(1 - 2^{-n/2+1}) \geq \frac{2-\sqrt{2}}{2^{q+1}}\mathrm{H}_q(1/2)$ for $n \geq 3$ and $\tau(n) \leq \mathrm{S}((I/2)^r) \leq O(1)$. Since each query to $\texttt{TsallisQEA}_q$ in $\texttt{BiSearch}$ decreases the size of the interval $[a, b]$ by almost a half, we can conclude that the number of adaptive queries to $\texttt{TsallisQEA}_q$ in $\texttt{BiSearch}(Q_0, \tau(n), \hat{g}_q(n))$ and $\texttt{BiSearch}(Q_1, \tau(n), \hat{g}_q(n))$ is $O(\log(1/\hat{g}_q(n))) = O(1)$. □

QSZK hardness results

Theorem 4.25 ($\textsc{TsallisQED}_q$ is QSZK-hard for $1 < q \leq 1 + \frac{1}{n-1}$)**.** *For any $q \in \left(1, 1 + \frac{1}{n-1}\right]$ and any $n \geq 90$, it holds that*

$$\forall g(n) \in [1/\mathrm{poly}(n), 1/400],\ \textsc{TsallisQED}_q[g(n)] \text{ is QSZK-hard.}$$

Proof. Following Lemma 3.37, we have that $\mathrm{QSD}\left[1 - 2^{-\hat{n}^{0.49}}, 2^{-\hat{n}^{0.49}}\right]$ is QSZK-hard for $\hat{n} \geq 1$. Let Q_0 and Q_1 be the corresponding QSZK-hard instance such that these circuits are polynomial-size and prepare the purification of ρ_0 and ρ_1, respectively. Leveraging the reduction from QSD to $\textsc{TsallisQED}_q$ (Lemma 4.21), there are two polynomial-size quantum circuits Q_0' and Q_1', which prepare the purifications of n-qubit ρ_0' and ρ_1' where $n \coloneqq \hat{n} + 1$, respectively, such that:

$$\begin{aligned} \mathrm{T}(\rho_0, \rho_1) \geq 1 - 2^{-\hat{n}^{0.49}} \quad &\Rightarrow\ \mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1') \geq g_q(n) = g_q(\hat{n}+1), \\ \mathrm{T}(\rho_0, \rho_1) \leq 2^{-\hat{n}^{0.49}} \quad &\Rightarrow\ \mathrm{S}_q(\rho_1') - \mathrm{S}_q(\rho_0') \leq g_q(n) = g_q(\hat{n}+1). \end{aligned}$$

Since $\sqrt{2^{-\hat{n}^{0.49}}(2 - 2^{-\hat{n}^{0.49}})} \leq 2^{\frac{1-\hat{n}^{0.49}}{2}}$ and $\gamma(n) \leq \mathrm{S}_q\left((I/2)^{\otimes \hat{n}}\right) = \frac{1-2^{\hat{n}(1-q)}}{q-1}$, we have

$$g_q(\hat{n}) \geq \underbrace{\frac{1}{2}\mathrm{H}_q\left(\frac{1}{2}\right) - \frac{1 - 2^{\hat{n}(1-q)}}{q-1}\left(\frac{1}{2} - \frac{1}{2^q}\right)}_{G_1(q;\hat{n})} - \underbrace{\left(\frac{1}{2} + \frac{1}{2^q}\right)\frac{2^{-\hat{n}^{0.49}q}}{2^q}\ln_q(2^{\hat{n}})}_{G_2(q;\hat{n})} - \underbrace{\left(\frac{1}{2} + \frac{1}{2^q}\right)\mathrm{H}_q\left(\frac{1}{2}\right)2^{\frac{1-\hat{n}^{0.49}}{2}}}_{G_3(q;\hat{n})}.$$

It remains to show that $g_q(\hat{n}) \geq G_1(q;\hat{n}) - G_2(q;\hat{n}) - G_3(q;\hat{n}) > 0$ for $1 \leq q \leq 1 + \frac{1}{\hat{n}}$ and large enough n. By leveraging the Taylor expansion of $G_1(q;\hat{n})$, $G_2(q;\hat{n})$, and $G_3(q;\hat{n})$ at $q = 1$, we obtain:

$$\begin{aligned} g_q(\hat{n}) &\geq G_1(q;\hat{n}) - G_2(q;\hat{n}) - G_3(q;\hat{n}) \\ &\geq \left(\frac{\log(2)}{2} - \frac{1}{4}(2\hat{n}+1)\log^2(2)(q-1)\right) - \frac{\log(2)}{2} \cdot \hat{n}2^{-\hat{n}^{0.49}} - \log(2) \cdot 2^{\frac{1-\hat{n}^{0.49}}{2}} \\ &\coloneqq G(q;\hat{n}) \end{aligned}$$

Noting that $\frac{\partial}{\partial q}G(q;\hat{n}) = -\frac{1}{4}(2\hat{n}+1)\log^2(2) < 0$ for $\hat{n} \geq 1$, we know that $G(q;\hat{n})$ is monotonically decreasing on $q > 1$ for any fixed $\hat{n} \geq 1$. As a consequence, as $1 \leq q \leq 1 + \frac{1}{\hat{n}}$,

it is left to show that $G\left(1+\frac{1}{\hat{n}};\hat{n}\right) > 0$ for large enough $\hat{n}$, specifically:

$$G\left(1+\frac{1}{\hat{n}};\hat{n}\right) = \frac{\log(2)}{4}\left(2-2\log(2)-2^{1-\hat{n}^{0.49}}\hat{n}-4\cdot 2^{\frac{1-\hat{n}^{0.49}}{2}}-\frac{\log(2)}{\hat{n}}\right) > 0.$$

A direct calculation implies that

$$\begin{aligned}&\frac{\mathrm{d}}{\mathrm{d}\hat{n}}G\left(1+\frac{1}{\hat{n}};\hat{n}\right)\\ &= \frac{\log(2)}{200}\left(49\sqrt{2^{1-\hat{n}^{0.49}}}\hat{n}^{1.49}\log(2)+2^{-\hat{n}^{0.49}}\hat{n}^2\left(49\hat{n}^{0.49}\log(2)-100\right)+50\log(2)\right).\end{aligned}$$

Since it is evident that $49\hat{n}^{0.49}\log(2)-100 > 0$, we can deduce that $\frac{\mathrm{d}}{\mathrm{d}\hat{n}}G\left(1+\frac{1}{\hat{n}};\hat{n}\right) > 0$. As $49\hat{n}^{0.49}\log(2)-100 > 0$ holds when $\hat{n} \geq 10$, we obtain that $G\left(1+\frac{1}{\hat{n}};\hat{n}\right)$ is monotonically increasing for $\hat{n} \geq 10$. Therefore, we complete the proof by noticing $\hat{n} = n-1$ and the following: For any $q \in \left(1, 1+\frac{1}{\hat{n}}\right]$ and $\hat{n} \geq 89$,

$$g_q(\hat{n}) \geq G(q;\hat{n}) \geq G\left(1+\frac{1}{\hat{n}};\hat{n}\right) \geq G\left(1+\frac{1}{89};89\right) > \frac{1}{400}. \qquad \square$$

Theorem 4.26 ($\mathrm{TsallisQEA}_q$ is QSZK-hard under Turing reduction for $1 < q \leq 1+\frac{1}{n-1}$)**.** *For any $q \in \left(1, 1+\frac{1}{n-1}\right]$ and any $n \geq 90$, the following holds*:

$$\mathrm{TsallisQEA}_q \text{ with } g(n) = \Theta(1) \text{ is QSZK-hard under Turing reduction.}$$

Proof. This proof is very similar to the proof of Theorem 4.24. For any $1 < q \leq 1+\frac{1}{n-1}$ and $n \geq 90$, since $\mathrm{TsallisQED}_q[\hat{g}_q(n)]$ is QSZK-hard under Karp reduction (Theorem 4.25), where $\hat{g}_q(n) = 1/400$, it is sufficient to provide an algorithm for $\mathrm{TsallisQED}_q[\hat{g}_q(n)]$ by using $\mathrm{TsallisQEA}_q[t(n), g(n)]$ as subroutines, with appropriately adaptive choices of $t(n)$ and $g(n)$.

Let Q_0 and Q_1 be the corresponding QSZK-hard instance such that these circuits are of size $\mathrm{poly}(n)$ and prepare the states ρ_0 and ρ_1, respectively. Let $\texttt{TsallisQEA}_q(Q, t(n), g(n))$ be the subroutine for decide whether $\mathrm{S}_q(\rho) \geq t(n)+g(n)$ or $\mathrm{S}_q(\rho) \leq t(n)-g(n)$. Next, we estimate $\mathrm{S}_q(\rho_b)$ to within additive error $\hat{g}_q(n)/2$ for $b \in \{0,1\}$ via the procedure `BiSearch`, as specified in Algorithm 4.4.1. To solve $\mathrm{TsallisQED}_q[\hat{g}_q(n)]$, noting that $\max\{\mathrm{rank}(\rho_0), \mathrm{rank}(\rho_1)\} \leq 2^n$, we choose $\tau(n) = \mathrm{S}_q((I/2)^{\otimes n})$. Subsequently, let $t_0(n) = \texttt{BiSearch}(Q_0, \tau(n), \hat{g}_q(n))$ and $t_1(n) = \texttt{BiSearch}(Q_1, \tau(n), \hat{g}_q(n))$, we obtain the same inequalities in Equation (4.53).

Note that $\hat{g}_q(n) = 1/400$ for $n \geq 90$ and $\tau(n) \leq \mathrm{S}((I/2)^n) < 1/(q-1) \leq O(1)$. Since each query to $\texttt{TsallisQEA}_q$ in `BiSearch` decreases the size of the interval $[a, b]$ by almost a half, we complete the proof by concluding that the number of adaptive queries to $\texttt{TsallisQEA}_q$ in $\texttt{BiSearch}(Q_0, \tau(n), \hat{g}_q(n))$ and $\texttt{BiSearch}(Q_1, \tau(n), \hat{g}_q(n))$ is $O(\log(1/g_q(n))) = O(1)$. $\square$

NIQSZK hardness result

Theorem 4.27 ($\mathrm{TsallisQEA}_q$ is NIQSZK-hard for $q = 1+\frac{1}{n-1}$)**.** *For any $n \geq 5$, the following holds*:

$$\forall g(n) \in [1/\mathrm{poly}(n), 1/150],\ \mathrm{TsallisQEA}_{1+\frac{1}{n-1}} \text{ with } g(n) \text{ is NIQSZK-hard.}$$

Proof. Utilizing Lemma 3.39, we know that QSCMM$[1/n, 1-1/n]$ is NIQSZK-hard for $n \geq 3$. Following the reduction from QSCMM to TsallisQEA$_{1+\frac{1}{n-1}}$ for $n \geq 5$ (Lemma 4.22), and the specific choice of $t(n)$ in the reduction, we can conclude that $g(n) \geq 1/150$. □

4.4.4 Quantum query complexity lower bounds

In this subsection, we present two quantum query complexity lower bounds for estimating the quantum Tsallis entropy $\mathrm{S}_q(\rho)$: When q is constantly larger than 1, the lower bound is *independent* of the rank of ρ (Theorem 4.28). However, when $q > 1$ is inverse-polynomially close to 1 or even closer, the lower bound *depends polynomially* on the rank of ρ (Theorem 4.29).

Theorem 4.28 (Query complexity lower bound for estimating quantum Tsallis entropy with q constantly above 1)**.** *For any $q \geq 1+\Omega(1)$ and sufficiently small $\epsilon > 0$, the quantum query complexity for estimating the q-Tsallis entropy of a quantum state to within additive error ϵ, in the purified quantum query access model, is $\Omega(1/\sqrt{\epsilon})$.*

Proof. Consider the task of distinguishing two quantun unitary operators U_ϵ and U_0 corresponding to two probability distributions p_ϵ and p_0, where $p_x \coloneqq (1-x, x)$, U_x is a unitary operator satisfying

$$U_x|0\rangle = \sqrt{1-x}|0\rangle|\varphi_0\rangle + \sqrt{x}|1\rangle|\varphi_1\rangle,$$

with $|\varphi_0\rangle$ and $|\varphi_1\rangle$ being any orthogonal unit vectors. By the quantum query complexity of distinguishing probability distributions given in Lemma 3.41, we know that distinguishing U_ϵ and U_0 requires quantum query complexity $\Omega(1/\mathrm{H}(p_\epsilon, p_0))$, where $\mathrm{H}(\cdot,\cdot)$ is the Hellinger distance between two probability distributions. Direct calculation shows that if $\epsilon \in (0,1)$,

$$\mathrm{H}(p_\epsilon, p_0) = \frac{1}{\sqrt{2}}\sqrt{\left(\sqrt{1-\epsilon}-1\right)^2 + \left(\sqrt{\epsilon}-0\right)^2} \leq \sqrt{\epsilon}.$$

Thus the query complexity of distinguishing U_0 and U_ϵ is $\Omega(1/\sqrt{\epsilon})$.

On the other hand, U_x prepares a purification of $\rho_x \coloneqq (1-x)|0\rangle\langle 0| + x|1\rangle\langle 1|$. Then, for sufficiently small $\epsilon > 0$, we have

$$|\mathrm{S}_q(\rho_\epsilon) - \mathrm{S}_q(\rho_0)| = \frac{1-(1-\epsilon)^q - \epsilon^q}{q-1} = \Omega(\epsilon).$$

Therefore, any quantum query algorithm that can compute the q-Tsallis entropy of a quantum state to within additive error $\Theta(\epsilon)$ can be used to distinguish U_ϵ and U_0, thus requiring query complexity $\Omega(1/\sqrt{\epsilon})$. □

Theorem 4.29 (Query complexity lower bound for estimating quantum Tsallis entropy with $q > 1$ near 1)**.** *For any $q \in \left(1, 1+\frac{1}{n-1}\right]$, there exists a mixed quantum state ρ of sufficiently large rank r such that the quantum query complexity for estimating $\mathrm{S}_q(\rho)$, in the purified quantum query access model, is $\Omega(r^{0.17-c})$ for any constant $c > 0$.*

Remark 4.30 (τ-dependence in the lower bounds). The lower bounds on query and sample complexities in Theorems 4.29 and 4.32 are $\Omega\left(r^{\frac{1-\tau}{3}-c}\right)$ and $\Omega(r^{1-\tau-c'})$, respectively, where $\tau = 0.49$ is chosen to establish the QSZK hardness (Theorem 4.25) and $c' = 3c$. Notably, these bounds can be further improved by selecting a smaller τ that still satisfies all requirements in the reduction (Lemma 4.21), which is left for future work.

Proof of Theorem 4.29. By Lemma 3.40 with $\epsilon = 1/2$, there exists an $\hat{n}$-qubit state $\hat{\rho}$ of rank $\hat{r} \geq 2$ and the corresponding "uniform" state $\hat{\rho}_{\mathsf{U}}$ of rank r on the same support as $\hat{\rho}$ such that the quantum sample complexity to decide whether $\mathrm{T}\big(\hat{\rho}, \hat{\rho}_{\mathsf{U}}\big)$ is at least $1/2$ or exactly 0 is $\Omega(\hat{r}^{1/3})$. We apply the polarization lemma for the trace distance to the states $\hat{\rho}$ and $\hat{\rho}_{\mathsf{U}}$, particularly using only the direct product lemma [Wat02, Lemma 8]. Let $\rho := \hat{\rho}^{\otimes \hat{r}^k}$ and $\rho_{\mathsf{U}} := \hat{\rho}_{\mathsf{U}}^{\otimes \hat{r}^k}$ be the resulting states, where k is a parameter to be determined later. Then, for any constant $k > \frac{\tau}{1-\tau}$ with $\tau = 0.49$ and for sufficiently large $\hat{r}$, the following holds:

$$\begin{aligned} \mathrm{T}(\hat{\rho}, \hat{\rho}_{\mathsf{U}}) \geq 1/2 \quad &\Rightarrow \quad \mathrm{T}(\rho, \rho_{\mathsf{U}}) \geq 1 - \exp(-\hat{r}^k/8) \geq 1 - 2^{-r^\tau}, \\ \mathrm{T}(\hat{\rho}, \hat{\rho}_{\mathsf{U}}) = 0 \quad &\Rightarrow \quad \mathrm{T}(\rho, \rho_{\mathsf{U}}) \leq \hat{r}^k \cdot 0 = 0 \leq 2^{-r^\tau}. \end{aligned}$$

Hence, the sample complexity of deciding whether $\mathrm{T}(\rho, \rho_{\mathsf{U}})$ is at least $1 - 2^{-r^\tau}$ or at most 2^{-r^τ} is $\Omega\Big(r^{\frac{1}{3(1+k)}}\Big)$, where $r := \hat{r} \cdot \hat{r}^k = \hat{r}^{1+k}$. For any $q \in \Big(1, 1 + \frac{1}{n-1}\Big] \subseteq \Big(1, 1 + \frac{1}{r-1}\Big]$, using the reduction from QSD to $\textsc{TsallisQED}_q$ (Lemma 4.21) with parameters from Theorem 4.25, there are two corresponding states ρ_0' and ρ_1' of rank at most $2r$ such that the quantum query complexity for deciding whether $\mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1')$ is at least $1/400$ or at most $-1/400$ is $\Omega\Big(r^{\frac{1}{3(1+k)}}\Big) = \Omega\Big(r^{\frac{1-\tau}{3} - c}\Big) = \Omega(r^{0.17-c})$ for any constant $c > 0$. Thus, estimating $\mathrm{S}_q(\rho_b')$ for $b \in \{0, 1\}$ to within additive error $1/800$ requires at least the same number of quantum queries. □

4.4.5 Quantum sample complexity lower bounds

In this subsection, we present two quantum sample complexity lower bounds for estimating the quantum Tsallis entropy $\mathrm{S}_q(\rho)$: When q is constantly larger than 1, the lower bound is *independent* of the rank of ρ (Theorem 4.31). However, when $q > 1$ is inverse-polynomially close to 1, the lower bound *depends polynomially* on the rank of ρ (Theorem 4.32).

Theorem 4.31 (Sample complexity lower bound for estimating quantum Tsallis entropy with q constantly above 1)**.** *For any $q \geq 1 + \Omega(1)$ and sufficiently small $\epsilon > 0$, the quantum sample complexity for estimating the quantum q-Tsallis entropy of a quantum state to within additive error ϵ is $\Omega(1/\epsilon)$.*

Proof. Consider the hypothesis testing problem where the given quantum state ρ is promised to be either ρ_0 or ρ_ϵ, each with equal probability. Specifically, the states are defined as

$$\forall x \in [0, 1], \quad \rho_x := (1 - x)|0\rangle\langle 0| + x|1\rangle\langle 1|.$$

For sufficiently small $\epsilon > 0$, we know that $|\mathrm{S}_q(\rho_\epsilon) - \mathrm{S}_q(\rho_0)| = \Omega(\epsilon)$, as shown in the proof of Theorem 4.28. Now, assume that there is a quantum estimator for $\mathrm{S}_q(\rho)$ to within additive error $\Theta(\epsilon)$ with sample complexity S. This estimator can then be used to distinguish these two states ρ_0 and ρ_ϵ with success probability $p_{\mathrm{succ}} \geq 2/3$. On the other hand, by Theorem 3.12, we have

$$p_{\mathrm{succ}} \leq \frac{1}{2} + \frac{1}{2}\mathrm{T}\Big(\rho_0^{\otimes \mathsf{S}}, \rho_\epsilon^{\otimes \mathsf{S}}\Big).$$

By applying the Fuchs–van de Graaf inequalities [FvdG99, Theorem 1], we have

$$\mathrm{T}\Big(\rho_0^{\otimes \mathsf{S}}, \rho_\epsilon^{\otimes \mathsf{S}}\Big) \leq \sqrt{1 - \mathrm{F}\Big(\rho_0^{\otimes \mathsf{S}}, \rho_\epsilon^{\otimes \mathsf{S}}\Big)^2},$$

where $\mathrm{F}(\rho,\sigma) = \mathrm{Tr}(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}})$ is the fidelity of quantum states. A direct calculation shows that $\mathrm{F}(\rho_0,\rho_\epsilon) = \sqrt{1-\epsilon}$, which gives that

$$p_{\mathrm{succ}} \le \frac{1}{2} + \frac{1}{2}\sqrt{1-(1-\epsilon)^{\mathsf{S}}}.$$

By combining this with the condition $p_{\mathrm{succ}} \ge 2/3$, we conclude that $\mathsf{S} = \Omega(1/\epsilon)$. □

Theorem 4.32 (Sample complexity lower bound for estimating quantum Tsallis entropy with $q > 1$ near 1)**.** *For any $q \in \left(1, 1+\frac{1}{n-1}\right]$, there exists a mixed quantum state ρ of sufficiently large rank r such that the quantum sample complexity for estimating $\mathrm{S}_q(\rho)$ is $\Omega(r^{0.51-c})$ for any constant $c > 0$.*

Notably, Remark 4.30 on the τ-dependence in the lower bound also applies to Theorem 4.32. Moreover, the proof strategy of Theorem 4.32 is similar to that of Theorem 4.29, as both rely on the direct product lemma for the trace distance [Wat02, Lemma 8].[26]

Proof of Theorem 4.32. By Lemma 3.42 with $\epsilon = 1/2$, there exists an $\hat{n}$-qubit state $\hat{\rho}$ of rank $\hat{r} \ge 2$ and the corresponding "uniform" state $\hat{\rho}_{\mathtt{U}}$ of rank r on the same support as $\hat{\rho}$ such that the quantum sample complexity to decide whether $\mathrm{T}\left(\hat{\rho},\hat{\rho}_{\mathtt{U}}\right)$ is at least $1/2$ or exactly 0 is $\Omega(\hat{r})$. We apply the direct product lemma [Wat02, Lemma 8] to the states $\hat{\rho}$ and $\hat{\rho}_{\mathtt{U}}$. Let $\rho \coloneqq \hat{\rho}^{\otimes \hat{r}^k}$ and $\rho_{\mathtt{U}} \coloneqq \hat{\rho}_{\mathtt{U}}^{\otimes \hat{r}^k}$ be the resulting states, where k is a parameter to be determined later. Then, for any constant $k > \frac{\tau}{1-\tau}$ with $\tau = 0.49$ and for sufficiently large $\hat{r}$, the following holds:

$$\begin{aligned} \mathrm{T}(\hat{\rho},\hat{\rho}_{\mathtt{U}}) \ge 1/2 \quad &\Rightarrow \quad \mathrm{T}(\rho,\rho_{\mathtt{U}}) \ge 1 - \exp(-\hat{r}^k/8) \ge 1 - 2^{-r^\tau}, \\ \mathrm{T}(\hat{\rho},\hat{\rho}_{\mathtt{U}}) = 0 \quad &\Rightarrow \quad \mathrm{T}(\rho,\rho_{\mathtt{U}}) \le \hat{r}^k \cdot 0 = 0 \le 2^{-r^\tau}. \end{aligned}$$

As a consequence, the sample complexity of deciding whether $\mathrm{T}(\rho,\rho_{\mathtt{U}})$ is at least $1-2^{-r^\tau}$ or at most 2^{-r^τ} is $\Omega(r^{\frac{1}{1+k}})$, where $r \coloneqq \hat{r}\cdot\hat{r}^k = \hat{r}^{1+k}$. For any $q \in \left(1, 1+\frac{1}{n-1}\right] \subseteq \left(1, 1+\frac{1}{r-1}\right]$, utilizing the reduction from QSD to $\textsc{TsallisQED}_q$ (Lemma 4.21) with parameters from Theorem 4.25, there are two corresponding states ρ_0' and ρ_1' of rank at most $2r$ such that the quantum sample complexity for deciding whether $\mathrm{S}_q(\rho_0') - \mathrm{S}_q(\rho_1')$ is at least $1/400$ or at most $-1/400$ is $\Omega(r^{\frac{1}{1+k}}) = \Omega(r^{1-\tau-c}) = \Omega(r^{0.51-c})$ for any constant $c > 0$. Therefore, estimating $\mathrm{S}_q(\rho_b')$ for $b \in \{0,1\}$ to within additive error $1/800$ requires at least the same number of copies of ρ. □

[26] This inequalities can also be derived using the polarization lemma for the measured quantum triangular discrimination, specifically combining Theorem 3.3 and Lemma 4.11 in [Liu23].

Chapter 5

Space-efficient quantum singular value transformation

In this chapter, we establish a *space-efficient variant* of the quantum singular value transformation (QSVT) [GSLW19], distinguishing itself from prior works primarily focused on time-efficient QSVT. As time-efficient QSVT provides a unified framework for designing time-efficient quantum algorithms [GSLW19, MRTC21], we believe our work indicates a unified approach to designing space-bounded quantum algorithms, potentially facilitating the discovery of new complete problems for BQL and its one-sided error variants (see Section 2.1 for a brief survey on space-bounded quantum computation).

5.1 Introduction

The quantum singular value transformation (QSVT) [GSLW19] is a powerful and efficient framework for manipulating the singular values $\{\sigma_i\}_i$ of a linear operator A, using a corresponding projected unitary encoding U of $A = \tilde{\Pi}U\Pi$ for projections $\tilde{\Pi}$ and Π.[1] The singular value decomposition is $A = \sum_i \sigma_i |\tilde{\psi}_i\rangle\langle\psi_i|$ where $|\tilde{\psi}_i\rangle$ and $|\psi_i\rangle$ are left and right singular vectors, respectively. QSVT has numerous applications in quantum algorithm design, and is even considered a grand unification of quantum algorithms [MRTC21].

To implement the transformation $f^{(\mathrm{SV})}(A) = f^{(\mathrm{SV})}(\tilde{\Pi}U\Pi)$, we require a degree-$d$ polynomial P_d that satisfies two conditions. Firstly, P_d well-approximates f on the interval of interest $\mathcal{I}$, with $\max_{x\in\mathcal{I}\setminus\mathcal{I}_\delta} |P_d(x) - f(x)| \leq \epsilon$, where $\mathcal{I}_\delta \subseteq \mathcal{I} \subseteq [-1,1]$ and typically $\mathcal{I}_\delta := (-\delta,\delta)$. Secondly, P_d is bounded with $\max_{x\in[-1,1]} |P_d(x)| \leq 1$. The degree of P_d depends on the precision parameters δ and ϵ, with $d = O(\delta^{-1}\log\epsilon^{-1})$, and all coefficients of P_d can be computed efficiently.

According to [GSLW19], we can utilize alternating phase modulation to implement $P_d^{(\mathrm{SV})}(\tilde{\Pi}U\Pi)$,[2] which requires a sequence of rotation angles $\Phi \in \mathbb{R}^d$. For instance, consider $P_d(x) = T_d(x)$ where $T_d(x)$ is the d-th Chebyshev polynomial (of the first kind), then we know that $\phi_1 = (1-d)\pi/2$ and $\phi_j = \pi/2$ for all $j \in \{2,3,\cdots,d\}$. QSVT techniques, including the pre-processing and quantum circuit implementation, are gener-

[1] Regardless of QSVT, it is noteworthy that the concept of block-encoding, specifically a unitary dilation U of a contraction A (see Footnote 1), is already used in quantum logspace for powering contraction matrices [GRZ21].

[2] This procedure is a generalization of quantum signal processing, see [MRTC21, Section II.A].

ally *time-efficient*. Additionally, the quantum circuit implementation of QSVT is already *space-efficient* because implementing QSVT with a degree-d bounded polynomial for any $s(n)$-qubit projected unitary encoding requires $O(s(n))$ qubits, where $s(n) \geq \Omega(\log n)$. However, the pre-processing in the QSVT techniques is typically not space-efficient. Indeed, prior works on the pre-processing for QSVT, specifically angle-finding algorithms in [Haa19, CDG+20, DMWL21], which have time complexity polynomially dependent on the degree d, do not consider the space-efficiency. Therefore, the use of previous angle-finding algorithms may lead to an *exponential* increase in space complexity. This raises a fundamental question on making the pre-processing space-efficient as well:

Problem 5.1 (Space-efficient QSVT)**.** *Can we implement a degree-d QSVT for any $s(n)$-qubit projected unitary encoding with $d \leq 2^{O(s(n))}$, using only $O(s(n))$ space in both the pre-processing and quantum circuit implementation?*

QSVT via averaged Chebyshev truncation. A space-efficient QSVT associated with Chebyshev polynomials is implicitly shown in [GSLW19], as the angles for any Chebyshev polynomial $T_k(x)$ are explicitly known. This insight sheds light on Problem 5.1 and suggests an alternative pre-processing approach for QSVT: Instead of finding rotation angles, it seems sufficient to find projection coefficients of Chebyshev polynomials.

Recently, Metger and Yuen [MY23] realized this approach and constructed bounded polynomial approximations of the sign and *shifted* square root functions with exponential precision in polynomial space by utilizing Chebyshev truncation, which offers a partial solution to Problem 5.1.[3] The key ingredient behind their approach is the degree-d Chebyshev truncation $\tilde{P}_d(x) = \frac{c_0}{2} + \sum_{k=1}^{d} c_k T_k$ where T_k is the k-th Chebyshev polynomial (of the first kind) and $c_k \coloneqq \frac{2}{\pi} \int_{-1}^{1} \frac{f(x)T_k(x)}{\sqrt{1-x^2}} \mathrm{d}x$. This provides a *nearly best* uniform approximation compared to the best degree-d polynomial approximation with error $\varepsilon_d(f)$ for the function $f\colon [-1,1] \to \mathbb{R}$. In particular, $\tilde{P}_d$ satisfies $\max_{x\in[-1,1]} |\tilde{P}_d(x) - f(x)| \leq O(\log d)\varepsilon_d(f)$.

Our construction achieves an error bound *independent* of d via a carefully chosen *average* of the Chebyshev truncation, known as the *de La Vallée Poussin partial sum*, $\hat{P}_{d'}(x) = \frac{1}{d}\sum_{l=d}^{d'} \tilde{P}_d(x) = \frac{\hat{c}_0}{2} + \sum_{k=1}^{d'} \hat{c}_k T_k(x)$, with a slightly larger degree $d' = 2d-1$. The degree-d averaged Chebyshev truncation $\hat{P}_{d'}$ satisfies $\max_{x\in[-1,1]} |\hat{P}_{d'}(x) - f(x)| \leq 4\varepsilon_d(f)$.

Once we have a space-efficient polynomial approximation for the function f (pre-processing), we can establish a space-efficient QSVT associated with f for *bitstring indexed encodings* that additionally require projections $\tilde{\Pi}$ and Π spanning the corresponding subset of $\{|0\rangle, |1\rangle\}^{\otimes s}$,[4] as stated in Theorem 5.2: With the space-efficient QSVT associated with Chebyshev polynomials $T_k(x)$, it suffices to implement the averaged Chebyshev truncation polynomial by LCU techniques [BCC+15] and to renormalize the bitstring indexed encoding by robust oblivious amplitude amplification (if necessary and applicable).

A refined analysis indicates that applying an averaged Chebyshev truncation to a bitstring indexed encoding for any $d' \leq 2^{O(s(n))}$ and $\epsilon \geq 2^{-O(s(n))}$ requires $O(s(n))$ qubits

[3] To clarify, we can see from [MY23] that directly adapting their construction shows that implementing QSVT for any $s(n)$-qubit block-encoding with $O(s(n))$-bit precision requires $\mathrm{poly}(s(n))$ classical and quantum space for any $s(n) \geq \Omega(\log n)$. However, Problem 5.1 (space-efficient QSVT) seeks to reduce the dependence of $s(n)$ in the space complexity from *polynomial* to *linear*.

[4] To ensure that $\tilde{\Pi}U\Pi$ admits a matrix representation, we require the basis of projections $\tilde{\Pi}$ and Π to have a well-defined order, leading us to focus exclusively on bitstring indexed encoding. Additionally, for simplicity, we assume no ancillary qubits are used here, and refer to Definition 5.3 for a formal definition.

and deterministic $O(s(n))$ space, provided that an evaluation oracle Eval_{P_d} estimates coefficients $\{\hat{c}_k\}_{k=0}^{d'}$ of the averaged Chebyshev truncation with $O(\log(\epsilon^2/d))$ precision. Nevertheless, our approach causes a *quadratic* dependence of the degree d in the query complexity to U.

Theorem 5.2 (Space-efficient QSVT, informal of Theorem 5.4)**.** *Let $f\colon \mathbb{R} \to \mathbb{R}$ be a continuous function bounded on $\mathcal{I} \subseteq [-1,1]$. If there exists a degree-d polynomial P_d^* that approximates $h\colon [-1,1] \to \mathbb{R}$, where h approximates f only on $\mathcal{I}$ with additive error at most ϵ, such that $\max_{x\in[-1,1]} |h(x) - P_d^*(x)| \leq \epsilon$, then the degree-$d$ averaged Chebyshev truncation yields another degree-d' polynomial $P_{d'}$, with $d' = 2d-1$, satisfying the following conditions:*

$$\max_{x\in\mathcal{I}} |f(x) - P_{d'}(x)| \leq O(\epsilon) \text{ and } \max_{x\in[-1,1]} |P_{d'}(x)| \leq 1.$$

Furthermore, we have an algorithm $\mathcal{A}_f$ that computes any coefficient $\{\hat{c}_k\}_{k=0}^{d'}$ of the averaged Chebyshev truncation polynomial $P_{d'}$ space-efficiently. The algorithm is deterministic for continuously bounded f, and bounded-error randomized for piecewise-smooth f. Additionally, for any $s(n)$-qubit bitstring indexed encoding U of $A = \tilde{\Pi}U\Pi$ with $d' \leq 2^{O(s(n))}$, we can implement the quantum singular value transformation $P_{d'}^{(\mathrm{SV})}(A)$ using $O(d^2\|\hat{\mathbf{c}}\|_1)$ queries[5] to U with $O(s(n))$ qubits. It is noteworthy that $\|\hat{\mathbf{c}}\|_1$ is bounded by $O(\log d)$ in general, and we can further improve to a constant norm bound for twice continuously differentiable functions.

Our techniques in Theorem 5.2 offer three advantages over the techniques proposed by [MY23]. Firstly, our techniques can handle any *piecewise-smooth function*, such as the (normalized) logarithmic function $\ln(1/x)$, the multiplicative inverse function $1/x$, and the square-root function $\sqrt{x}$;[6] whereas the techniques from [MY23] are restricted to continuously bounded functions whose second derivative of the integrand in $\{\hat{c}_k\}_{k=1}^{d'}$ is at most $\mathrm{poly}(d)$ on the interval $\mathcal{I} = [-1,1]$, such as the sign function and the *shifted* square-root function $\sqrt{(x+1)/2}$.[7] Secondly, our techniques are *constant overhead* in terms of the space complexity of the bitstring indexed encoding U, while the techniques from [MY23] are only *poly-logarithmic overhead*. Thirdly, our techniques have an error bound independent of d, unlike the $\log d$ factor in [MY23], simplifying parameter trade-offs for applying the space-efficient QSVT to concrete problems.

In addition, it is noteworthy that applying the space-efficient QSVT with the sign function will imply a unified approach to error reduction for the classes $\mathsf{BQ_UL}$, $\mathsf{coRQ_UL}$, and $\mathsf{RQ_UL}$.

Computing the coefficients. We will implement the evaluation oracle Eval_{P_d} to prove Theorem 5.2. To estimate the coefficients $\{\hat{c}_k\}_{k=0}^{d'}$ in the averaged Chebyshev truncation for any function f that is bounded on the interval $\mathcal{I} = [-1,1]$, we can use standard numerical integral techniques,[8] given that the integrand's second derivative in $\{\hat{c}_k\}_{k=0}^{d'}$ is

[5] The dependence of $\|\hat{\mathbf{c}}\|_1$ arises from renormalizing the bitstring indexed encoding via amplitude amplification.

[6] Our technique can imply a better norm bound $\|\hat{\mathbf{c}}\| \leq O(1)$. See Remark 5.7 for the details.

[7] The second derivative $|f''(x)|$ of the shifted square-root function $f(x) \coloneqq \sqrt{(x+1)/2}$ is unbounded at $x = -1$. However, we can circumvent this point by instead considering $g_\delta(x) = \sqrt{(1-\delta)(x+1)/2 + \delta}$ with the second derivative $|g_\delta''(-1)| = O(\delta^{-3/2})$, as shown in [MY23, Lemma 2.11].

[8] We remark that using a more efficient numerical integral technique, such as the exponentially convergent trapezoidal rule, may improve the required space complexity for computing coefficients by a

bounded by poly(d).

However, implementing the evaluation oracle for piecewise-smooth functions f on an interval $\mathcal{I} \subsetneq [-1,1]$ is relatively complicated. We cannot simply apply averaged Chebyshev truncation to f. Instead, we consider a low-degree Fourier approximation g resulting from implementing smooth functions to Hamiltonians [vAGGdW20, Appendix B]. We then make the error vanish outside $\mathcal{I}$ by multiplying with a Gaussian error function, resulting in h which approximates f *only* on $\mathcal{I}$. Therefore, we can apply averaged Chebyshev truncation and our algorithm for bounded functions to h through a somewhat complicated calculation.

Finally, we need to compute the coefficients of the low-degree Fourier approximation g. Interestingly, this step involves the *stochastic matrix powering problem*, which lies at the heart of space-bounded derandomization, e.g.,[SZ99, CDSTS23, PP23]. We utilize space-efficient random walks on a directed graph to estimate the power of a stochastic matrix. Consequently, we can only develop a bounded-error randomized algorithm $\mathcal{A}_f$ for piecewise-smooth functions.[9]

5.2 Space-efficient quantum singular value transformations

We begin by defining the *projected unitary encoding* and its special forms, viz. the bitstring indexed encoding and the block-encoding.

Definition 5.3 (Projected unitary encoding and its special forms, adapted from [GSLW19])**.** *Let U be an (α, a, ϵ)-projected unitary encoding of a linear operator A if $\|A - \alpha\tilde{\Pi}U\Pi\| \leq \epsilon$, where U and orthogonal projections $\tilde{\Pi}$ and Π act on $s+a$ qubits, and both $\mathrm{rank}(\tilde{\Pi})$ and $\mathrm{rank}(\Pi)$ are at least 2^a (a is viewed as the number of ancillary qubits). Furthermore, we are interested in two special forms of the projected unitary encoding:*

- **Bitstring indexed encoding.** *We say that a projected unitary encoding is a bitstring indexed encoding if both orthogonal projections $\tilde{\Pi}$ and Π span on $\tilde{S}, S \subseteq \{|0\rangle, |1\rangle\}^{\otimes(a+s)}$, respectively.[10] In particular, for any $|\tilde{s}_i\rangle \in \tilde{S}$ and $|s_j\rangle \in S$, we have a matrix representation $A_{\tilde{S},S}(i,j) \coloneqq \langle \tilde{s}_i|U|s_j\rangle$ of A.*
- **Block encoding.** *We say that a projected unitary encoding is a block-encoding if both orthogonal projections are of the form $\Pi = \tilde{\Pi} = |0\rangle\langle 0|^{\otimes a} \otimes I_s$. We use the shorthand $A = (\langle \bar{0}| \otimes I_s)U(|\bar{0}\rangle \otimes I_s)$ for convenience.*

See Section 2.2 for definitions of singular value decomposition and transformation. With these definitions in place, we present the main (informal) theorem in this section:

Theorem 5.4 (Space-efficient QSVT)**.** *Let $f\colon \mathbb{R} \to \mathbb{R}$ be a continuous function bounded on the closed interval of interest $\mathcal{I} \subseteq [-1,1]$. If there exists a degree-d polynomial P_d^* that approximates $h\colon [-1,1] \to \mathbb{R}$, where h approximates f only on $\mathcal{I}$ with additive error at*

constant factor.

[9] The (classical) pre-processing in space-efficient QSVT is *not* part of the deterministic Turing machine producing the quantum circuit description in the BQL model (Definition 2.2). Instead, we treat it as a component of quantum computation, allowing the use of randomized algorithms since BPL $\subseteq$ BQL [FR21].

[10] Typically, to ensure these orthogonal projections coincide with space-bounded quantum computation, we additionally require the corresponding subsets $\tilde{S}$ and S admit space-efficient set membership, namely deciding the membership of these subsets is in deterministic $O(s+a)$ space.

most ϵ, such that $\max_{x\in[-1,1]} |h(x) - P_d^*(x)| \leq \epsilon$, then degree-$d$ averaged Chebyshev truncation yields another degree-d' polynomial $P_{d'}$, with $d' = 2d - 1$, satisfying the following conditions:

$$\max_{x\in\mathcal{I}} |f(x) - P_{d'}(x)| \leq O(\epsilon) \text{ and } \max_{x\in[-1,1]} |P_{d'}(x)| \leq 1.$$

Moreover, there is a space-efficient classical algorithm for computing any entry in the coefficient vector $\hat{\mathbf{c}}$ of the averaged Chebyshev truncation polynomial $P_{d'}$:

- *If f is a continuously bounded function with $\max_{x\in[-1,1]} |f''(x)| \leq \mathrm{poly}(d)$,[11] then any entry in the coefficient vector $\hat{\mathbf{c}}$ can be computed in deterministic $O(\log d)$ space;*
- *If f is a piecewise-smooth function, then any entry in the coefficient vector $\hat{\mathbf{c}}$ can be computed in bounded-error randomized $O(\log d)$ space.*

Furthermore, for any $(1, a, 0)$-bitstring indexed encoding U of $A = \tilde{\Pi}U\Pi$, acting on $s + a$ qubits where $a(n) \leq s(n)$, and any $P_{d'}$ with $d' \leq 2^{O(s(n))}$, we can implement an $(\alpha, a + \log d + O(1), \epsilon_\alpha)$-bitstring indexed encoding of the quantum singular value transformation $P_{d'}^{(\mathrm{SV})}(A)$ that acts on $O(s(n))$ qubits using $O(d^2\eta_\alpha)$ queries to U, where ϵ_α is specified in Theorem 5.12. Here, $\alpha = \|\hat{\mathbf{c}}\|_1$ with $\eta_\alpha = 1$ in general, and particularly $\alpha = 1$ with $\eta_\alpha = \|\hat{\mathbf{c}}\|_1$ if $P_{d'}^{(\mathrm{SV})}(A)$ is a partial isometry. It is noteworthy that $\|\hat{\mathbf{c}}\|_1$ is bounded by $O(\log d)$ in general, and can be improved to a constant bound for twice continuously differentiable functions.

We remark that we can apply Theorem 5.4 to general forms of the projected unitary encoding U with orthogonal projections Π and $\tilde{\Pi}$, as long as such an encoding meets the conditions: (1) The basis of Π and $\tilde{\Pi}$ admits a well-defined order; (2) Both controlled-Π and controlled-$\tilde{\Pi}$ admit computationally efficient implementation. We note that bitstring indexed encoding defined in Definition 5.3 trivially meets the first condition, and a sufficient condition for the second condition is that the corresponding subsets S and $\tilde{S}$ have space-efficient set membership.

Next, we highlight the main technical contributions leading to our space-efficient quantum singular value transformations (Theorem 5.4). To approximately implement a space-efficient QSVT $f^{(\mathrm{SV})}(A)$, we require *the pre-processing* to find a space-efficient polynomial approximation $P_{d'}^{(f)} \approx f$ on $\mathcal{I}$. These polynomial approximations are detailed in Section 5.2.1:

- We provide deterministic space-efficient polynomial approximations for *continuously bounded* functions (Lemma 5.5) using averaged Chebyshev truncation (see Section 2.3.1), including the sign function (Corollary 5.8).
- We present bounded-error randomized space-efficient polynomial approximations for *piecewise-smooth* functions (Theorem 5.9), such as the normalized logarithmic function (Corollary 5.11). To achieve this, we adapt the time-efficient technique in [vAGGdW20, Lemma 37] to the space-efficient scenario by leveraging space-efficient random walks (Lemma 5.10).

[11] This conclusion also applies to a linear combination of bounded functions, provided that the coefficients are bounded and can be computed deterministically and space-efficiently.

With an appropriate polynomial approximation $P_{d'}^{(f)}$, we can implement the space-efficient QSVT $P_{f,d'}^{(\mathrm{SV})}(A)$, as established in Section 5.2.2 (specifically Theorem 5.12). Note that a space-efficient QSVT for Chebyshev polynomials is implicitly shown in [GSLW19] (Lemma 5.14). We establish Theorem 5.12 by combining this result with the LCU technique (Lemma 5.15) and the renormalization procedure (Lemma 5.16, if necessary and applicable).

In addition to these general techniques, we provide explicit space-efficient QSVT examples in Section 5.3, including those for the sign function (Corollary 5.17) and the normalized logarithmic function (Corollary 5.18). Notably, the former leads to a simple proof of space-efficient error reduction for unitary quantum computations (Section 5.4).

5.2.1 Space-efficient bounded polynomial approximations

We provide a systematic approach for constructing *space-efficient* polynomial approximations of real-valued piecewise-smooth functions, which is a space-efficient counterpart of Corollary 23 in [GSLW19]. Notably, our algorithm (Lemma 5.5) is *deterministic* for continuous functions that are bounded on the interval $[-1,1]$. However, for general piecewise-smooth functions, we only introduce a *randomized* algorithm (Theorem 5.9). In addition, please refer to Section 2.3.1 as a brief introduction to Chebyshev polynomial and (averaged) Chebyshev truncation.

Continuously bounded functions

We propose a space-efficient algorithm for computing the coefficients of a polynomial approximation with high accuracy for continuously bounded functions. Our approach leverages the averaged Chebyshev truncation, specifically *the de La Vallée Poussin partial sum*, in conjunction with numerical integration, namely *the composite trapezium rule*.

Lemma 5.5 (Space-efficient polynomial approximations for bounded functions)**.** *For any continuous function f that f is bounded with $\max_{x\in[-1,1]}|f(x)|\le B$ for some known constant $B>0$. Let $P_{f,d}^*$ be a degree-d polynomial with the same parity as f satisfying $\max_{x\in[-1,1]}|f(x)-P_{f,d}^*(x)|\le\epsilon$. By employing the degree-d averaged Chebyshev truncation, we can obtain a degree-d' polynomial $P_{d'}^{(f)}$ that has the same parity as $P_{f,d}^*$ and satisfies $\max_{x\in[-1,1]}|f(x)-P_{d'}^{(f)}(x)|\le 4\epsilon$.*[12] *This polynomial $P_{d'}^{(f)}$ is defined as a linear combination of Chebyshev polynomials $T_k(\cos\theta)=\cos(k\theta)$ with $d'=2d-1$ and the integrand $F_k(\theta):=\cos(k\theta)f(\cos\theta)$:*

$$P_{d'}^{(f)}=\frac{\hat{c}_0}{2}+\sum_{k=1}^{d'}\hat{c}_kT_k \text{ where } c_k=\frac{2}{\pi}\int_{-\pi}^{0}F_k(\theta)\mathrm{d}\theta \text{ and } \hat{c}_k=\begin{cases}c_k, & 0\le k\le d'\\ \frac{2d-k}{d}c_k, & k>d\end{cases}. \quad (5.1)$$

If the integrand $F_k(\theta)$ satisfies $\max_{\xi\in[-\pi,0]}|F_k''(\theta)|\le O(d^\gamma)$ for some constant γ, then any entry of the coefficient vector $\hat{\mathbf{c}}=(\hat{c}_0,\cdots,\hat{c}_{d'})$, up to additive error ϵ for $\|\hat{\mathbf{c}}\|_1$, can be computed in deterministic time $O(d^{(\gamma+1)/2}\epsilon^{-1/2}t(\ell))$ and space $O(\log(d^{(\gamma+3)/2}\epsilon^{-3/2}B))$, where $\ell=O(\log(d^{(\gamma+3)/2}\epsilon^{-3/2}))$ and evaluating $F(\theta)$ in ℓ-bit precision is in deterministic time $t(\ell)$ and space $O(\ell)$. Moreover, the coefficient vector $\hat{\mathbf{c}}$ has the following norm bound:

[12] It is noteworthy that for any even function f, the degree of $P_{d'}^{(f)}$ is $2d-2$ rather than $2d-1$. Nevertheless, for the sake of convenience, we continue to choose $d'=2d-1$.

- *For any function f satisfying our conditions, it holds that*
$$\|\mathbf{c}\|_1 \leq O(B \log d);$$
- *If the function f is additionally (at least) twice continuously differentiable,*
$$\|\mathbf{c}\|_1 \leq O(B).$$

Proof. We begin with the polynomial approximation $P_{d'}^{(f)}$ obtained from the degree-d averaged Chebyshev truncation expressed in Equation (5.1). The degree d' is $2d-1$ if f is odd, and $2d-2$ if f is even. To bound the truncation error of $P_{d'}^{(f)}$, we require a degree-d polynomial $P_{f,d}^*$ such that $\max_{x\in[-1,1]} |f(x) - P_{f,d}^*(x)| \leq \epsilon$. By utilizing Lemma 2.11, we obtain the desired error bound $\max_{x\in[-1,1]} |f(x) - P_{d'}^{(f)}(x)| \leq 4\epsilon$.

Computing the coefficients. To compute the coefficients $\hat{c}_k$ for $0 \leq k \leq d'$, it suffices to compute the Chebyshev coefficients c_k for $0 \leq k \leq 2d-1$. Note that $c_k = \frac{2}{\pi}\int_{-\pi}^{0} F_k(\theta)\mathrm{d}\theta$ where $F_k(\theta) := \cos(k\theta) f(\cos\theta)$, we can estimate the numerical integration using the composite trapezium rule, e.g., [SM03, Section 7.5]. The application of this method yields the following:

$$\begin{aligned} \int_{-\pi}^{0} F_k(\theta)\mathrm{d}\theta &\approx \frac{\pi}{m}\Big(\frac{F_k(\theta_0)}{2} + \sum_{l=1}^{m} F_k(\theta_l) + \frac{F_k(\theta_m)}{2}\Big), \\ \text{where } \theta_l &:= \frac{\pi l}{m} - \pi \text{ for } l = 0, 1, \cdots, m. \end{aligned} \tag{5.2}$$

The upper bound on the numerical errors for computing the coefficient c_k is given by:

$$\varepsilon_{d',k}^{(f)} := \sum_{l=1}^{m} \Big| \int_{x_{i-1}}^{x_i} F_k(\theta)\mathrm{d}\theta - \frac{\pi}{2m}\cdot(F_k(\theta_{i-1}) + F_k(\theta_i)) \Big| \leq \frac{\pi^3}{12m^2} \max_{\xi\in[-\pi,\pi]} |F_k''(\xi)|\,. \tag{5.3}$$

To obtain an upper bound on the number of intervals m, we need to ensure that the error of the numerical integration is within

$$\varepsilon_{d'}^{(f)} = \sum_{k=0}^{d} \varepsilon_{d',k}^{(f)} + \sum_{k=d+1}^{d'} \frac{2d-k}{d}\varepsilon_{d',k}^{(f)} \leq \sum_{k=0}^{d'} \varepsilon_{d',k}^{(f)} \leq \epsilon.$$

Plugging the assumption $|F_k''(x)| \leq O(d^\gamma)$ into Equation (5.3), by choosing an appropriate value of $m = \Theta(\epsilon^{-1/2} d^{(\gamma+1)/2})$, we establish that $\varepsilon_{d'}^{(f)} \leq O(d^{\gamma+1})/m^2 \leq \epsilon$. Moreover, to guarantee that the accumulated error is $O(\epsilon/d)$ in Equation (5.2), we need to evaluate the integrand $F(\theta)$ with ℓ-bit precision, where $\ell = O(\log(dm/\epsilon)) = O(\log(\epsilon^{-3/2} d^{(\gamma+3)/2}))$. Lastly, the desired ℓ_1 norm bound of the coefficient vector $\hat{\mathbf{c}}$ directly follows from Lemma 2.12.

Analyzing time and space complexity. The presented numerical integration algorithm is deterministic, and therefore, the time complexity for computing the integral is $O(mt(\ell))$, where $t(\ell)$ is the time complexity for evaluating the integrand $F_k(\theta)$ within $2^{-\ell}$ accuracy (i.e., ℓ-bit precision) in $O(\ell)$ space. The space complexity required for computing the numerical integration is the number of bits required to index the integral intervals and represent the resulting coefficients. To be specific, the space complexity is

$$\begin{aligned} \max\Big\{O(\log m), O(\ell), \log\|\hat{\mathbf{c}}\|_\infty\Big\} &\leq O\Big(\max\Big\{\log\Big(\epsilon^{-\frac{3}{2}} d^{\frac{\gamma+3}{2}}\Big), \log B\Big\}\Big) \\ &\leq O\Big(\log\Big(\epsilon^{-\frac{3}{2}} d^{\frac{\gamma+3}{2}} B\Big)\Big). \end{aligned}$$

Here, $\|\hat{\mathbf{c}}\|_\infty = \max_{0\le k\le d'} \frac{2}{\pi}\left|\int_{-\pi}^{0} \cos(k\theta) f(\cos\theta)\mathrm{d}\theta\right| \le \max_{-\pi\le\theta\le 0} O(|f(\cos\theta)|) \le O(B)$, and the last inequality is due to the fact that

$$\forall A, B > 0, \quad \Theta(\max\{\log A, \log B\}) = \Theta(\log(AB)). \qquad \square$$

It is worth noting that evaluating a large family of functions, called holonomic functions, with ℓ-bit precision requires only *deterministic* $O(\ell)$ space:

Remark 5.6 (Space-efficient evaluation of holonomic functions). Holonomic functions encompass several commonly used functions,[13] such as polynomials, rational functions, sine and cosine functions (but not other trigonometric functions such as tangent or secant), exponential functions, logarithms (to any base), the Gaussian error function, and the normalized binomial coefficients. In [CGKZ05, Mez12], these works have demonstrated that evaluating a holonomic function with ℓ-bit precision is achievable in deterministic time $\widetilde{O}(\ell)$ and space $O(\ell)$. Prior works achieved the same time complexity, but with a space complexity of $O(\ell \log \ell)$.

In addition, we provide an example in Remark 5.7 that achieves only a logarithmically weaker bound on $\|\hat{\mathbf{c}}\|_1$ using Lemma 5.5, whereas a constant norm bound can be achieved by leveraging Theorem 5.9 for piecewise-smooth functions.

Remark 5.7 (On the norm bound of the square-root function's polynomial approximation). We consider a function $\mathrm{Sqrt}_\delta(x)$ that coincides with $\sqrt{x}$ on the interval $[\delta, 1]$.[14] Specifically, $\mathrm{Sqrt}_\delta(x)$ is defined as $\sqrt{x}$ for $x \ge \delta$, $-\sqrt{-x}$ for $x \le -\delta$, and $1/\sqrt{\delta}$ for $x \in (-\delta, \delta)$. $\mathrm{Sqrt}_\delta(x)$ is continuously bounded on $[-1, 1]$ and satisfies $|\mathrm{Sqrt}''_\delta(x)| \le \delta^{-3/2}/4$ with the maximum at $x = \pm\delta$. As $\mathrm{Sqrt}''_\delta(x)$ is not continuous, its polynomial approximation via Lemma 5.5 achieves only $\|\mathbf{c}\|_1 \le O(\log d)$.

We now present an example of bounded functions, specifically the sign function.

Corollary 5.8 (Space-efficient approximation to the sign function)**.** *For any $\delta > 0$ and $\epsilon > 0$, there is an explicit odd polynomial $P^{\mathrm{sgn}}_{d'}(x) = \hat{c}_0/2 + \sum_{k=1}^{d'} \hat{c}_k T_k(x) \in \mathbb{R}[x]$ of degree $d' \le \tilde{C}_{\mathrm{sgn}} \delta^{-1} \log \epsilon^{-1}$, where $d' = 2d - 1$ and $\tilde{C}_{\mathrm{sgn}}$ is a universal constant. Any entry of the coefficient vector $\hat{\mathbf{c}} := (\hat{c}_0, \cdots, \hat{c}_{d'})$ can be computed in deterministic time $\widetilde{O}\left(\epsilon^{-1/2} d^2\right)$ and space $O(\log(\epsilon^{-3/2} d^3))$. Furthermore, the polynomial $P^{\mathrm{sgn}}_{d'}$ satisfies the following conditions:*

$$\forall x \in [-1, 1] \setminus [-\delta, \delta], |\mathrm{sgn}(x) - P^{\mathrm{sgn}}_{d'}(x)| \le C_{\mathrm{sgn}}\epsilon, \text{ where } C_{\mathrm{sgn}} = 5;$$
$$\forall x \in [-1, 1], |P^{\mathrm{sgn}}_{d'}(x)| \le 1.$$

Additionally, the coefficient vector $\hat{\mathbf{c}}$ has a norm bounded by $\|\hat{\mathbf{c}}\|_1 \le \hat{C}_{\mathrm{sgn}}$, where $\hat{C}_{\mathrm{sgn}}$ is another universal constant. Without loss of generality, we assume that $\hat{C}_{\mathrm{sgn}}$ and $\tilde{C}_{\mathrm{sgn}}$ are at least 1.

Proof. We start from a degree-d polynomial $\tilde{P}^{\mathrm{sgn}}_d$ that well-approximates $\mathrm{sgn}(x)$:

Proposition 5.8.1 (Polynomial approximation of the sign function, adapted from Lemma 10 and Corollary 4 in [LC17])**.** *For any $\delta > 0$, $x \in \mathbb{R}$, $\epsilon \in (0, \sqrt{2e\pi})$. Let $\kappa =$*

[13] For a more detailed introduction, please refer to [BZ10, Section 4.9.2].

[14] Since the second derivative of the square-root function $\sqrt{x}$ is unbounded at $x = 0$, we cannot directly apply Lemma 5.5 to $\sqrt{x}$.

$\frac{2}{\delta}\log^{1/2}\left(\frac{\sqrt{2}}{\sqrt{\pi}\epsilon}\right)$, *Then*

$$g_{\delta,\epsilon}(x) \coloneqq \operatorname{erf}(\kappa x) \text{ satisfies that } |g_{\delta,\epsilon}(x)| \le 1 \text{ and } \max_{|x|\ge\delta/2} |g_{\delta,\epsilon}(x) - \operatorname{sgn}(x)| \le \epsilon.$$

Moreover, there is an odd polynomial $\tilde{P}_d^{\mathrm{sgn}} \in \mathbb{R}[x]$ *of degree* $d = O(\sqrt{(\kappa^2 + \log\epsilon^{-1})\log\epsilon^{-1}})$ *such that* $\max_{x\in[-1,1]} \left|\tilde{P}_d^{\mathrm{sgn}}(x) - \operatorname{erf}(\kappa x)\right| \le \epsilon$

By applying Proposition 5.8.1, we obtain a degree-d polynomial $\tilde{P}_d^{\mathrm{sgn}}$ that well approximates the function $\operatorname{erf}(\kappa x)$ where $\kappa = O(\delta^{-1}\sqrt{\log\epsilon^{-1}})$.

To utilize Lemma 5.5, it suffices to upper bound the second derivative $\max_{\xi\in[-\pi,0]} |F_k''(\xi)|$ for any $0 \le k \le d'$, as specified in Fact 5.8.1.

Fact 5.8.1. *Let* $F_k(\theta) = \operatorname{erf}(\kappa\cos\theta)\cos(k\theta)$*, it holds that:*

$$\max_{0\le k\le d'} \max_{\xi\in[-\pi,0]} |F_k''(\xi)| \le \frac{2}{\sqrt{\pi}}\kappa + k^2 + \frac{4}{\sqrt{\pi}}\kappa^3 + \frac{4}{\sqrt{\pi}}k\kappa.$$

Proof. Through a straightforward calculation, we have derived that

$$\begin{aligned} |F_k''(\theta)| =& \frac{2}{\sqrt{\pi}}\left|\kappa\exp(-\kappa^2\cos^2\theta)\cos\theta\cos(\kappa\theta)\right| + \left|k^2\cos(k\theta)\operatorname{erf}(\kappa\cos(\theta))\right| \\ &+ \frac{4}{\sqrt{\pi}}\left|\kappa^3\exp(-\kappa^2\cos^2\theta)\cos\theta\cos(k\theta)\sin^2\theta\right| \\ &+ \frac{4}{\sqrt{\pi}}\left|k\kappa\exp(-\kappa^2\cos^2\theta)\sin\theta\sin(k\theta)\right| \\ \le& \frac{2}{\sqrt{\pi}}\kappa + k^2 + \frac{4}{\sqrt{\pi}}\kappa^3 + \frac{4}{\sqrt{\pi}}k\kappa. \end{aligned} \tag{5.4}$$

The last line owes to the facts that $|\operatorname{erf}(x)| \le 1$, $\exp(-x^2) \le 1$, $|\sin x| \le 1$, and $|\cos x| \le 1$ for any x. We finish the proof by noting that Equation (5.4) holds for any $0 \le k \le d'$. □

Note that both κ and k are at most $O(d)$. By Fact 5.8.1, we have $\max_{\xi\in[-\pi,0]} |F_k''(\xi)| \le O(d^3)$ for any $0 \le k \le d'$. Utilizing Lemma 5.5, we obtain a polynomial approximation $P_{d'}^{\mathrm{sgn}}(x) = \hat{c}_0/2 + \sum_{k=1}^{d'} \hat{c}_k T_k(x)$ with a degree of $d' = 2d - 1 \le \tilde{C}_{\mathrm{sgn}}\delta^{-1}\log\epsilon^{-1}$, where $\tilde{C}_{\mathrm{sgn}}$ is a universal constant. This polynomial satisfies $\max_{x\in[-1,1]} |\operatorname{erf}(\kappa x) - P_{d'}^{\mathrm{sgn}}(x)| \le 4\epsilon$. Then we can derive:

$$\max_{x\in[-1,1]} |\operatorname{sgn}(x) - P_{d'}^{\mathrm{sgn}}(x)| \le \epsilon + \max_{x\in[-1,1]} |\operatorname{erf}(\kappa x) - P_{d'}^{\mathrm{sgn}}(x)| \le C_{\mathrm{sgn}}\epsilon, \text{ where } C_{\mathrm{sgn}} = 5.$$

Moreover, to bound the norm $\|\hat{\mathbf{c}}\|_1$, it suffices to consider the function $\operatorname{erf}(\kappa x)$ due to Proposition 5.8.1. We observe that the first and second derivatives of $\operatorname{erf}(\kappa x)$, namely $2\kappa e^{-\kappa^2x^2}/\sqrt{\pi}$ and $-4\kappa^3 x e^{-\kappa^2x^2}/\sqrt{\pi}$, respectively, are continuous, making $\operatorname{erf}(\kappa x)$ is twice continuously differentiable. Hence, according to Lemma 5.5, $\|\hat{\mathbf{c}}\|_1 \le \hat{C}_{\mathrm{sgn}}$ for some universal constant $\hat{C}_{\mathrm{sgn}}$.[15]

For the complexity of computing coefficients $\{\hat{c}_k\}_{k=1}^{d'}$, note that the evaluation of the integrand $F(\theta)$ requires ℓ-bit precision, where $\ell = O(\log(\epsilon^{-3/2}d^3))$. Following $t(\ell) =$

[15] Let $c_k' \coloneqq \langle T_k, \operatorname{sgn}\rangle$ be the coefficients corresponding to the sign function. A direct calculation, as shown in [MY23, Lemma 2.10], yields $\|\mathbf{c}'\|_1 = O(\log d)$. Our improved norm bound arises from utilizing smoother functions like $\operatorname{erf}(\kappa x)$, instead of relying on the sign function which is discontinuous at $x = 0$.

$\widetilde{O}(\ell)$ specified in Remark 5.6, any entry of the coefficient vector $\hat{\mathbf{c}}$ can be computed in deterministic time $O(\epsilon^{-1/2}d^2t(\ell)) = \widetilde{O}(\epsilon^{-1/2}d^2)$ and space $O(\log(\epsilon^{-3/2}d^3))$.

Finally, we note that $\max_{x\in[-1,1]}|P^{\mathrm{sgn}}_{d'}(x)| \le 1+\epsilon$ due to numerical errors in computing the coefficients $\{\hat{c}_k\}_{k=1}^{d'}$. We finish the proof by normalizing $\hat{P}^{\mathrm{sgn}}_{d'}$. Particularly, we consider $P^{\mathrm{sgn}}_{d'}(x) \coloneqq (1+\epsilon)^{-1}\hat{P}^{\mathrm{sgn}}_{d'}$ and adjust the coefficient vector $\hat{\mathbf{c}}$ of $P^{\mathrm{sgn}}_{d'}$ accordingly. □

Piecewise-smooth functions

We present a randomized algorithm for constructing bounded polynomial approximations of piecewise-smooth functions, offering a *space-efficient* alternative to Corollary 23 in [GSLW19], as described in Theorem 5.9. Our algorithm leverages Lemma 5.5 and Lemma 5.10. Since this subsection mostly focuses on polynomial approximations, we introduce some notation for convenience. For a function $f\colon \mathcal{I} \to \mathbb{R}$ and an interval $\mathcal{I}' \subseteq \mathcal{I}$, we define $\|f\|_{\mathcal{I}'} \coloneqq \sup\{|f(x)|\colon x \in \mathcal{I}'\}$ to denote the supremum of the function f on the interval $\mathcal{I}'$.

Theorem 5.9 (Taylor series based space-efficient bounded polynomial approximations)**.** *Consider a real-valued function $f\colon [-x_0-r-\delta, x_0+r+\delta] \to \mathbb{R}$ such that $f(x_0+x) = \sum_{l=0}^{\infty} a_l x^l$ for all $x \in [-r-\delta, r+\delta]$, where $x_0 \in [-1,1]$, $r \in (0,2]$, $\delta \in (0,r]$. Assume that $\sum_{l=0}^{\infty}(r+\delta)^l|a_l| \le B$ where $B > 0$. Let $\epsilon \in (0, \frac{1}{2B}]$ such that $B > \epsilon$, then there is a polynomial $P_{d'} \in \mathbb{R}[x]$ of degree $d' = 2d-1 \le O(\delta^{-1}\log(\epsilon^{-1}B))$, corresponding to some degree-d averaged Chebyshev truncation, such that any entry of the coefficient vector $\hat{\mathbf{c}}$ can be computed in bounded-error randomized time $\widetilde{O}(\max\{(\delta')^{-5}\epsilon^{-2}B^2, d^2\epsilon^{-1/2}\})$ and space $O(\log(d^3(\delta')^{-4}\epsilon^{-3/2}B))$ where $\delta' \coloneqq \frac{\delta}{2(r+\delta)}$, such that*

$$\begin{aligned} \|f(x)-P(x)\|_{[x_0-r,x_0+r]} &\le O(\epsilon), \\ \|P(x)\|_{[-1,1]} &\le O(\epsilon) + \|f(x)\|_{[x_0-r-\delta/2,x_0+r+\delta/2]} \le O(\epsilon)+B, \\ \|P(x)\|_{[-1,1]\setminus[x_0-r-\delta/2,x_0+r+\delta/2]} &\le O(\epsilon). \end{aligned}$$

Furthermore, the coefficient vector $\hat{\mathbf{c}}$ of $P_{d'}$ has a norm bounded by $\|\hat{\mathbf{c}}\|_1 \le O(B)$.

The main ingredient, and the primary challenge, for demonstrating Theorem 5.9 is to construct a low-weight approximation using Fourier series, as shown in Lemma 37 of [vAGGdW20], which requires computing the powers of sub-stochastic matrices in bounded space (Lemma 2.14).

Lemma 5.10 (Space-efficient low-weight approximation by Fourier series)**.** *Let $0 < \delta, \epsilon < 1$ and $f\colon \mathbb{R} \to \mathbb{R}$ be a real-valued function such that $|f(x) - \sum_{k=0}^{K} a_k x^k| \le \epsilon/4$ for all $x \in \mathcal{I}_\delta$, the interval $\mathcal{I}_\delta \coloneqq [-1+\delta, 1-\delta]$ and $\|\mathbf{a}\|_1 \le O(\max\{\epsilon^{-1}, \delta^{-1}\})$. Then there is a coefficient vector $\mathbf{c} \in \mathbb{C}^{2M+1}$ such that*

- *For even functions, $\left|f(x) - \sum_{m=-M}^{M} c_m^{(\mathrm{even})}\cos(\pi x m)\right| \le \epsilon$ for any $x \in \mathcal{I}_\delta$;*
- *For odd functions, $\left|f(x) - \sum_{m=-M}^{M} c_m^{(\mathrm{odd})}\sin\left(\pi x\left(m+\frac{1}{2}\right)\right)\right| \le \epsilon$ for any $x \in \mathcal{I}_\delta$;*
- *Otherwise, $\left|f(x) - \sum_{m=-M}^{M}\left(c_m^{(\mathrm{even})}\cos(\pi x m) + c_m^{(\mathrm{odd})}\sin\left(\pi x\left(m+\frac{1}{2}\right)\right)\right)\right| \le \epsilon$ for any $x \in \mathcal{I}_\delta$.*

Here $M \coloneqq \max\left(2\lceil\delta^{-1}\ln(4\|a\|_1\epsilon^{-1})\rceil, 0\right)$ and $\|\mathbf{c}\|_1 \le \|\mathbf{a}\|_1$.

Furthermore, the coefficient vector $\mathbf{c}$ *can be computed in bounded-error randomized time* $\widetilde{O}(\delta^{-5}\epsilon^{-2})$ *and space* $O(\log(\delta^{-4}\epsilon^{-1}))$.

Proof. We begin by noticing that the truncation error of $\sum_{k=0}^{K} a_k x^k$, as shown in [SM03, Theorem A.4], is $(1-\delta)^{k+1} \le e^{-\delta(k+1)} \le \epsilon$, implying that $K \ge \Omega(\delta^{-1}\ln\epsilon^{-1})$. Without loss of generality, we can assume that $\|\mathbf{a}\|_1 \ge \epsilon/2$.[16]

Construction of polynomial approximations. Our construction involves three approximations, as described in Lemma 37 of [vAGGdW20]. The first approximation combines the assumed $\sum_{k=0}^{K} a_k x^k$ with $\arcsin(x)$'s Taylor series.

Proposition 5.10.1 (First approximation)**.** *Let* $\hat{f}_1(x) \coloneqq \sum_{k=0}^{K} a_k x^k$ *such that* $\|f - \hat{f}_1\|_{\mathcal{I}_\delta} \le \epsilon/4$. *Then we know that* $\hat{f}_1(x) = \sum_{k=0}^{K} a_k \sum_{l=0}^{\infty} b_l^{(k)} \sin^l\left(\frac{x\pi}{2}\right)$ *where the coefficients* $b_l^{(k)}$ *satisfy that*

$$b_l^{(k+1)} = \sum_{l'=0}^{l} b_{l'}^{(k)} b_{l-l'}^{(1)} \text{ where } b_l^{(1)} = \begin{cases} 0 & \text{if } l \text{ is even,} \\ \binom{l-1}{\frac{l-1}{2}} \frac{2^{-l+1}}{l} \cdot \frac{2}{\pi} & \text{if } l \text{ is odd.} \end{cases} \tag{5.5}$$

Furthermore, the coefficients $\{b_l^{(k)}\}$ *satisfies the following:* (1) $\|\mathbf{b}^{(k)}\|_1 = 1$ *for all* $k \ge 1$; (2) $\mathbf{b}^{(k)}$ *is entry-wise non-negative for all* $k \ge 1$; (3) $b_l^{(k)} = 0$ *if* l *and* k *have different parities.*

Proof. We construct a Fourier series by a linear combination of the power of sines. We first note that $x = \frac{2}{\pi} \cdot \arcsin\left(\sin\left(\frac{x\pi}{2}\right)\right)$ for all $x \in [-1,1]$, and plug it into $\hat{f}_1(x) \coloneqq \sum_{k=0}^{K} a_k x^k$, which deduces that $\|f - \hat{f}_1\|_{\mathcal{I}_\delta} \le \epsilon/4$ by the assumption. Let $\mathbf{b}^{(k)}$ be the coefficients of $\left(\frac{\arcsin y}{\pi/2}\right)^k = \sum_{l=0}^{\infty} b_l^{(k)} y^l$ for all $y \in [-1,1]$, then we result in our first approximation. Moreover, we observe that $\frac{\pi}{2} \cdot \mathbf{b}^{(1)}$ is exactly the Taylor series of arcsin, whereas we know that $\left(\frac{\arcsin y}{\pi/2}\right)^{k+1} = \left(\frac{\arcsin y}{\pi/2}\right)^k \cdot \left(\sum_{l=0}^{\infty} b_l^{(1)} y^l\right)$ for $k > 1$, which derives Equation (5.5) by comparing the coefficients. In addition, notice that $\|\mathbf{b}^{(k)}\|_1 = \sum_{l=0}^{\infty} b_l^{(k)} 1^l = \left(\frac{\arcsin 1}{\pi/2}\right)^k = 1$, together with straightforward reasoning follows from Equation (5.5), we deduce the desired property for $\{b_l^{(k)}\}$. □

The second approximation truncates the series at $l = L$, and bounds the truncation error.

Proposition 5.10.2 (Second approximation)**.** *Let* $\hat{f}_2(x) \coloneqq \sum_{k=0}^{K} a_k \sum_{l=0}^{L} b_l^{(k)} \sin^l\left(\frac{x\pi}{2}\right)$ *where* $L \coloneqq \lceil \delta^{-2} \ln(4\|\mathbf{a}\|_1 \epsilon^{-1}) \rceil$, *then we have that* $\|\hat{f}_1 - \hat{f}_2\|_{\mathcal{I}_\delta} \le \epsilon/4$.

Proof. We truncate the summation over l in $f_1(x)$ at $l = L$, and it suffices to bound the truncation error. For all $k \in \mathbb{N}$ and $x \in [-1+\delta, 1-\delta]$, we obtain the error bound:

$$\left| \sum_{l=\lfloor L \rfloor}^{\infty} b_l^{(k)} \sin^l\left(\frac{x\pi}{2}\right) \right| \le \sum_{l=\lfloor L \rfloor}^{\infty} b_l^{(k)} \left| \sin^l\left(\frac{x\pi}{2}\right) \right| \le \sum_{l=\lfloor L \rfloor}^{\infty} b_l^{(k)} |1-\delta^2|^l \le (1-\delta^2)^L \sum_{l=\lfloor L \rfloor}^{\infty} b_l^{(k)} \le (1-\delta^2)^L.$$

[16] This is because if $\|\mathbf{a}\|_1 < \epsilon/2$, then $\|f\|_{\mathcal{I}_\delta} \le \|f(x) - \sum_{k=0}^{K} a_k x^k\|_{\mathcal{I}_\delta} + \|\sum_{k=0}^{K} a_k x^k\|_{\mathcal{I}_\delta} \le \epsilon/4 + \|\mathbf{a}\|_1 < \epsilon$, implying that $M = 0$ and $\mathbf{c} = 0$.

Here, the second inequality owing to $\forall \delta \in [0,1]$, $\sin\left((1-\delta)\frac{\pi}{2}\right) \leq 1-\delta^2$, and the last inequality is due to $\|\mathbf{b}^{(k)}\|_1 = 1$ in Proposition 5.10.1. By appropriately choosing $L \coloneqq \delta^{-2}\ln(4\|\mathbf{a}\|_1\epsilon^{-1})$, we obtain that

$$\|\hat{f}_1 - \hat{f}_2\|_{\mathcal{I}_\delta} \leq \sum_{k=0}^{K} a_k(1-\delta^2)^L \leq \|\mathbf{a}\|_1 \cdot \exp(-\delta^2 L) \leq \frac{\epsilon}{4}. \qquad \square$$

The third approximation approximates the functions $\sin^l(x)$ in $\hat{f}_2(x)$ using a tail bound of the binomial distribution. Notably, this construction not only quadratically improves the dependence on δ, but also ensures that the integrand's second derivative is *bounded* when combined with Lemma 5.5.

Proposition 5.10.3 (Third approximation)**.** *Let $\hat{f}_3(x)$ be polynomial approximations of f that depends on the parity of f such that $\|\hat{f}_2 - \hat{f}_3\|_{\mathcal{I}_\delta} \leq \epsilon/2$ and $M = \lfloor \delta^{-1}\ln(4\|\mathbf{a}\|_1\epsilon^{-1})\rfloor$, then we have*

$$\hat{f}_3^{(\text{even})}(x) \coloneqq \sum_{k=0}^{K} a_k \sum_{\hat{l}=0}^{L/2} (-1)^{\hat{l}} 2^{-2\hat{l}} b_{2\hat{l}}^{(k)} \sum_{m'=\hat{l}-M}^{\hat{l}+M} (-1)^{m'} \binom{2\hat{l}}{m'} \cos(\pi x(m'-\hat{l})),$$

$$\hat{f}_3^{(\text{odd})}(x) \coloneqq \sum_{k=0}^{K} a_k \sum_{\hat{l}=0}^{(L-1)/2} (-1)^{\hat{l}+1} 2^{-2\hat{l}-1} b_{2\hat{l}+1}^{(k)} \sum_{m'=\hat{l}+1-M}^{\hat{l}+1+M} (-1)^{m'} \binom{2\hat{l}+1}{m'} \sin\left(\pi x\left(m'-\hat{l}-\tfrac{1}{2}\right)\right).$$

Therefore, we have that $\hat{f}_3(x) \coloneqq \hat{f}_3^{(\text{even})}(x)$ if f is even, whereas $\hat{f}_3(x) \coloneqq \hat{f}_3^{(\text{odd})}(x)$ if f is odd. In addition, if f is neither even or odd, then $\hat{f}_3(x) \coloneqq \hat{f}_3^{(\text{even})}(x) + \hat{f}_3^{(\text{odd})}(x)$.

Proof. We upper-bound $\sin^l(x)$ in $\hat{f}_2(x)$ defined in Proposition 5.10.2 using a tail bound of binomial coefficients. We obtain that $\sin^l(z) = \left(\frac{e^{-\mathrm{i}z} - e^{\mathrm{i}z}}{-2\mathrm{i}}\right)^l = \left(\frac{\mathrm{i}}{2}\right)^l \sum_{m=0}^{l} \exp(\mathrm{i}z(2m-l))$ by a direct calculation, which implies the counterpart for real-valued functions:

$$\sin^l(z) = \begin{cases} 2^{-l}(-1)^{(l+1)/2} \sum_{m'=0}^{l} (-1)^{m'} \binom{l}{m'} \sin(z(2m'-l)), & \text{if } l \text{ is odd;} \\ 2^{-l}(-1)^{l/2} \sum_{m'=0}^{l} (-1)^{m'} \binom{l}{m'} \cos(z(2m'-l)), & \text{if } l \text{ is even.} \end{cases} \tag{5.6}$$

Recall that the Chernoff bound (e.g., Corollary A.1.7 [AS16]) which corresponds a tail bound of binomial coefficients, and assume that $l \leq L$, we have derived that:

$$\sum_{m'=0}^{\lfloor l/2\rfloor - M} 2^{-l}\binom{l}{m'} = \sum_{m'=\lceil l/2\rceil + M}^{l} 2^{-l}\binom{l}{m'} \leq e^{-\frac{2M^2}{l}} \leq e^{-\frac{2M^2}{L}} \leq \left(\frac{\epsilon}{4\|a\|_1}\right)^2 \leq \frac{\epsilon}{4\|a\|_1}. \tag{5.7}$$

Here, we choose $M = \lceil \delta^{-1}\ln(4\|\mathbf{a}\|_1\epsilon^{-1})\rceil$, and the last inequality is because of the assumption $\epsilon \leq 2\|\mathbf{a}\|_1$. As stated in Proposition 5.10.1, $b_l^{(k)} = 0$ if k and l have different parities. Consequently, we only need to consider all odd (resp., even) $l \leq L$ for odd (resp., even) functions. If the function f is neither even nor odd, we must consider all $l \leq L$. Plugging Equation 5.7 into Equation 5.6, we can derive that:

$$\begin{aligned} &\text{If } l \text{ is odd, } \left\| \sin^l(z) - 2^{-l}(-1)^{(l+1)/2} \sum_{m'=(l+1)/2-M}^{(l+1)/2+M} (-1)^{m'} \binom{l}{m'} \sin(z(2m'-l)) \right\|_{\mathcal{I}_\delta} \leq \frac{\epsilon}{2\|\mathbf{a}\|_1}; \\ &\text{If } l \text{ is even, } \left\| \sin^l(z) - 2^{-l}(-1)^{l/2} \sum_{m'=l/2-M}^{l/2+M} (-1)^{m'} \binom{l}{m'} \cos(z(2m'-l)) \right\|_{\mathcal{I}_\delta} \leq \frac{\epsilon}{2\|\mathbf{a}\|_1}; \end{aligned} \tag{5.8}$$

Plugging Equation (5.8) into $\hat{f}_2(x)$, and substituting $z = x\pi/2$, this equation leads

to $\hat{f}_3(x)$ as desired. In addition, combining $\sum_{k=0}^{K}|a_k|\sum_{l=0}^{\lfloor L\rfloor}|b_l^{(k)}| \le \sum_{k=0}^{K}|a_k| = \|\mathbf{a}\|_1$ with Equation (5.8), we achieve that $\|\hat{f}_2 - \hat{f}_3\|_{\mathcal{I}_\delta} \le \epsilon/2$. □

We adopt the third approximation as our construction by rearranging the summations and introducing a new parameter m. The value of m is defined as $m \coloneqq m' - \hat{l}$ if f is even and $m \coloneqq m' - \hat{l} - 1$ if f is odd. Moreover, the definition of m depends on the parity of $l = 2\hat{l}+1$ if f is neither even nor odd.[17] By applying this approach, we obtain:

$$\begin{aligned}
\hat{f}_3^{(\text{even})}(x) &= \sum_{m=-M}^{M} c_m^{(\text{even})}\cos(\pi x m),\\
\text{where } c_m^{(\text{even})} &\coloneqq (-1)^m \sum_{k=0}^{K} a_k \sum_{\hat{l}=0}^{L/2} b_{2\hat{l}}^{(k)} \binom{2\hat{l}}{m+\hat{l}} 2^{-2\hat{l}};\\
\hat{f}_3^{(\text{odd})}(x) &= \sum_{m=-M}^{M} c_m^{(\text{odd})}\sin\Big(\pi x\Big(m+\tfrac{1}{2}\Big)\Big),\\
\text{where } c_m^{(\text{odd})} &\coloneqq (-1)^m \sum_{k=0}^{K} a_k \sum_{\hat{l}=0}^{(L-1)/2} b_{2\hat{l}+1}^{(k)} \binom{2\hat{l}+1}{m+\hat{l}+1} 2^{-2\hat{l}-1}.
\end{aligned} \tag{5.9}$$

We then notice that the rearrangement of terms in Equation (5.9) can be directly applied to the definition of $\hat{f}_3(x)$ in Proposition 5.10.3. As a consequence, we obtain the following bound on the accumulative error:

$$\|f - \hat{f}_3\|_{\mathcal{I}_\delta} \le \|f - \hat{f}_1\|_{\mathcal{I}_\delta} + \|\hat{f}_1 - \hat{f}_2\|_{\mathcal{I}_\delta} + \|\hat{f}_2 - \hat{f}_3\|_{\mathcal{I}_\delta} \le \epsilon.$$

Additionally, we remark that $\|\mathbf{c}\|_1 \le \|\mathbf{a}\|_1$, since $\|\mathbf{b}^{(k)}\|_1 = 1$ (see Proposition 5.10.1) and $\sum_{m=0}^{l}\binom{l}{m} = 2^l$.

Analyzing time and space complexity. To evaluate the bounded polynomial approximation $\hat{f}_3(x)$ with ϵ accuracy, it is necessary to approximate the summand with ℓ-bit precision, where $\ell = O(\log(KLM\epsilon^{-1})) = O(\log(\delta^{-4}\epsilon^{-1}))$. Since the summand is a product of a constant number of holonomic functions, approximating $b_l^{(k)}$ with ℓ-bit precision is sufficient. Other quantities in the summand can be evaluated with the desired accuracy in deterministic time $\widetilde{O}(\ell)$ and space $O(\ell)$ as stated in Remark 5.6.

We now present a bounded-error randomized algorithm for estimating $b_l^{(k)}$. As $\mathbf{b}^{(1)}$ is entry-wise non-negative and $\sum_{i=1}^{l} b_i^{(1)} < \|\mathbf{b}^{(1)}\|_1 = 1$ following Proposition 5.10.1, we can express the recursive formula in Equation (5.5) as the matrix powering of a sub-stochastic matrix B_1:

$$B_1^k \coloneqq \begin{pmatrix} b_1^{(1)} & b_2^{(1)} & \cdots & b_{l-1}^{(1)} & b_l^{(1)} \\ 0 & b_1^{(1)} & \cdots & b_{l-2}^{(1)} & b_{l-1}^{(1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & b_1^{(1)} & b_2^{(1)} \\ 0 & 0 & \cdots & 0 & b_1^{(1)} \end{pmatrix}^k = \begin{pmatrix} b_1^{(k)} & b_2^{(k)} & \cdots & b_{l-1}^{(k)} & b_l^{(k)} \\ 0 & b_1^{(k)} & \cdots & b_{l-2}^{(k)} & b_{l-1}^{(k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & b_1^{(k)} & b_2^{(k)} \\ 0 & 0 & \cdots & 0 & b_1^{(k)} \end{pmatrix} \coloneqq B_k.$$

In addition, we approximate the sub-stochastic matrix B_1 by dyadic rationals with ℓ-bit precision, denoted as $\hat{B}_1$. Utilizing Lemma 2.14, we can compute any entry $\hat{B}_1^k[s,t]$

[17] The summand in $\hat{f}_3(x)$ is $c_m^{(\text{even})}\cos(\pi x m) + c_m^{(\text{odd})}\sin\big(\pi x\big(m+\frac{1}{2}\big)\big)$ if f is neither even nor odd.

with a randomized algorithm that runs in $O(\ell k)$ time and $\log(l+1)$ space with acceptance probability $\hat{B}_1^k[s,t]$. To evaluate $\hat{B}_1^k[s,t]$ with an additive error of ϵ, we use the sequential repetitions outlined in Lemma 2.13. Specifically, we repeat the algorithm $m = 2\epsilon^{-2}\ln(KLM) = O(\epsilon^{-2}\log(\delta^{-4}))$ times, and each turn succeeds with probability at least $1 - 1/(3KLM)$. Note that the number of the evaluation of $b_l^{(k)}$ for computing $\hat{f}_3(x)$ is $O(KLM)$, and by the union bound, we can conclude that the success probability of evaluating all coefficients in $\mathbf{c}$ is at least $2/3$.

Finally, we complete the proof by analyzing the overall computational complexity. It is evident that our algorithm utilizes $O(\ell + \log m) = O(\log(\delta^{-4}\epsilon^{-3}))$ space because indexing m repetitions requires additional $O(\log m)$ bits. Moreover, since there are $O(KLM)$ summands in $\hat{f}_3(x)$, and evaluating $b_l^{(k)}$ takes m repetitions with time complexity $O(\ell K)$ for a single turn, the overall time complexity is

$$O(KLM \cdot \ell K \cdot \epsilon^{-2}\log(KLM)) = \widetilde{O}(\delta^{-5}\epsilon^{-2}). \qquad \square$$

Now we present the proof of Theorem 5.9, a space-efficient and randomized algorithm for constructing bounded polynomial approximations for piecewise-smooth functions.

Proof of Theorem 5.9. Our approach is based on Theorem 40 in [vAGGdW20] and Corollary 23 in [GSLW19]. Firstly, we obtain a Fourier approximation $\hat{f}(x)$ of the given function $f(x)$ by truncating it using Lemma 5.10. Next, we ensure that $\hat{f}(x)$ is negligible outside the interval $[-x_0 - r, x_0 + r]$ by multiplying it with a suitable rectangle function, denoted as $h(x)$. Finally, we derive a space-efficient polynomial approximation $\hat{h}(x)$ of $h(x)$ by applying Lemma 5.5.

Construction of a bounded function. Let us begin by defining a linear transformation $L(x) \coloneqq \frac{x-x_0}{r+\delta}$ that maps $[x_0 - r - \delta, x_0 + r + \delta]$ to $[-1, 1]$. For convenience, we denote $g(y) \coloneqq f(L^{-1}(y))$ and $b_l \coloneqq a_l(r+\delta)^l$, then it is evident that $g(y) \coloneqq \sum_{l=0}^{\infty} b_l y^l$ for any $y \in [-1, 1]$.

To construct a Fourier approximation by Lemma 5.10, we need to bound the truncation error $\varepsilon_J^{(g)}$. We define $\delta' \coloneqq \frac{\delta}{2(r+\delta)}$ and $J \coloneqq \lceil (\delta')^{-1}\log(12B\epsilon^{-1})\rceil$. This ensures that the truncation error $\varepsilon_J^{(g)} \coloneqq \left|g(y) - \sum_{j=0}^{J-1} b_j y^j\right|$ for any $y \in [-1+\delta', 1-\delta']$ satisfies the following:

$$\varepsilon_J^{(g)} = \left|\sum_{j=J}^{\infty} b_j y^j\right| \le \sum_{j=J}^{\infty}\left|b_j(1-\delta')^j\right| \le (1-\delta')^J \sum_{j=J}^{\infty}|b_j| \le (1-\delta')^J B \le e^{-\delta' J}B \le \frac{\epsilon}{12} \coloneqq \frac{\epsilon'}{4}.$$

Afterward, let $\hat{\mathbf{b}} \coloneqq (b_0, b_1, \cdots, b_{J-1})$, then we know that $\|\hat{\mathbf{b}}\|_1 \le \|\mathbf{b}\|_1 \le B$ by the assumption. Now we utilize Lemma 5.10 and obtain the Fourier approximation $\hat{g}(y)$:

$$\hat{g}(y) \coloneqq \begin{cases} \sum_{m=-M}^{M} c_m^{(\mathrm{even})}\cos(\pi y m), & \text{if } f \text{ is even} \\ \sum_{m=-M}^{M} c_m^{(\mathrm{odd})}\sin\left(\pi y\left(m+\frac{1}{2}\right)\right), & \text{if } f \text{ is odd} \\ \sum_{m=-M}^{M}\left(c_m^{(\mathrm{even})}\cos(\pi y m) + c_m^{(\mathrm{odd})}\sin\left(\pi y\left(m+\frac{1}{2}\right)\right)\right), & \text{otherwise} \end{cases}. \tag{5.10}$$

By appropriately choosing $M = O\left((\delta')^{-1}\log\left(\|\hat{\mathbf{b}}\|_1/\epsilon'\right)\right) = O\left(r\delta^{-1}\log\left(B/\epsilon\right)\right)$, we obtain that the vectors of coefficients $\mathbf{c}^{(\mathrm{even})}$ and $\mathbf{c}^{(\mathrm{odd})}$ satisfy $\|\mathbf{c}^{(\mathrm{even})}\|_1 \le \|\hat{\mathbf{b}}\|_1 \le \|\mathbf{b}\|_1 \le B$

and similarly $\|\mathbf{c}^{(\mathrm{odd})}\|_1 \le B$. Plugging $f(x) = g(L(x))$ into Equation (5.10), we conclude that $\hat{f}(x) = \hat{g}(L(x))$ is a Fourier approximation of f with an additive error of $\epsilon/3$ on the interval $[x_0 - r - \delta/2, x_0 + r + \delta/2]$:

$$\hat{f}(x) = \hat{g}\Big(\frac{x-x_0}{r+\delta}\Big) = \begin{cases} \sum_{m=-M}^{M} c_m^{(\mathrm{even})} \cos\big(\pi m \big(\frac{x-x_0}{r+\delta}\big)\big), & \text{if } f \text{ is even} \\ \sum_{m=-M}^{M} c_m^{(\mathrm{odd})} \sin\big(\pi\big(m+\frac{1}{2}\big)\big(\frac{x-x_0}{r+\delta}\big)\big), & \text{if } f \text{ is odd} \\ \sum_{m=-M}^{M} c_m^{(\mathrm{even})} \cos\big(\pi m \big(\frac{x-x_0}{r+\delta}\big)\big) + c_m^{(\mathrm{odd})} \sin\big(\pi\big(m+\frac{1}{2}\big)\big(\frac{x-x_0}{r+\delta}\big)\big), & \text{otherwise} \end{cases}.$$

Making the error negligible outside the interval. Subsequently, we define the function $h(x) = \hat{f}(x) \cdot R(x)$ such that it becomes negligible outside the interval of interest, i.e., $[x_0 - r - \delta/2, x_0 + r + \delta/2]$. Here, the approximate rectangle function $R(x)$ is $\tilde{\epsilon}$-close to 1 on the interval $[x_0 - r, x_0 + r]$, and is $\tilde{\epsilon}$-close to 0 on the interval $[-1, 1] \setminus [x_0 - r - 2\tilde{\delta}, x_0 + r + 2\tilde{\delta}]$, where $\tilde{\epsilon} \coloneqq \epsilon/(3B)$ and $\tilde{\delta} \coloneqq \delta/4$. Moreover, $|R(x)| \le 1$ for any $x \in [-1, 1]$. Similar to Lemma 29 in [GSLW19], $R(x)$ can be expressed as a linear combination of Gaussian error functions:

$$R(x) \coloneqq \tfrac{1}{2}\Big[\operatorname{erf}\Big(\kappa(x - x_0 + r + \delta')\Big) - \operatorname{erf}\Big(\kappa(x - x_0 - r - \delta')\Big)\Big],$$
$$\text{where} \quad \kappa \coloneqq \tfrac{2}{\delta'} \log^{\frac{1}{2}} \tfrac{\sqrt{2}}{\sqrt{\pi}\epsilon'} = \tfrac{8}{\delta} \log^{\frac{1}{2}} \tfrac{\sqrt{18}B}{\sqrt{\pi}\epsilon}.$$

Bounded polynomial approximation via averaged Chebyshev truncation. We here present an algorithmic, space-efficient, randomized polynomial approximation method using averaged Chebyshev truncation to approximate the function $h(x) \coloneqq \hat{f}(x) \cdot R(x)$. As suggested in Proposition 5.9.1, we use an explicit polynomial approximation $P_d^*(x)$ of the bounded function $h(x)$ of degree $d = O(\delta^{-1} \log(B\epsilon^{-1}))$ that satisfies the conditions specified in Equation (5.11).

Proposition 5.9.1 (Bounded polynomial approximations based on a local Taylor series, adapted from [GSLW19, Corollary 23])**.** *Let $x_0 \in [-1, 1]$, $r \in (0, 2]$, $\delta \in (0, r]$ and let $f\colon [-x_0 - r - \delta, x_0 + r + \delta] \to \mathbb{R}$ and be such that $f(x_0 + x) \coloneqq \sum_{l=0}^{\infty} a_l x^l$ for all $x \in [-r - \delta, r + \delta]$. Suppose $B > 0$ is such that $\sum_{l=0}^{\infty} (r + \delta)^l |a_l| \le B$. Let $\epsilon \in \big(0, \frac{1}{2B}\big]$, there is a $\epsilon/3$-precise Fourier approximation $\tilde{f}(x)$ of $f(x)$ on the interval $[x_0 - r + \delta/2, x_0 + r + \delta/2]$, where $\hat{f}(x) \coloneqq \sum_{m=-M}^{M} \mathrm{Re}\Big[\tilde{c}_m e^{-\frac{i\pi m}{2(r+\delta)} x_0} e^{\frac{i\pi m}{2(r+\delta)} x}\Big]$ and $\|\tilde{\mathbf{c}}\|_1 \le B$. We have an explicit polynomial $P_d^* \in \mathbb{R}[x]$ of degree $d = O(\delta^{-1} \log(B\epsilon^{-1}))$ s.t.*

$$\begin{aligned} \|\hat{f}(x)R(x) - P_d^*(x)\|_{[x_0 - r, x_0 + r]} &\le \epsilon, \\ \|P_d^*(x)\|_{[-1,1]} &\le \epsilon + \|\hat{f}(x)R(x)\|_{[x_0 - r - \delta/2, x_0 + r + \delta/2]} \le \epsilon + B, \\ \|P_d^*(x)\|_{[-1,1] \setminus [x_0 - r - \delta/2, x_0 + r + \delta/2]} &\le \epsilon. \end{aligned} \tag{5.11}$$

To utilize Lemma 5.5, we need to bound the second derivative $\max_{\xi \in [-\pi, 0]} |F_k''(\xi)|$, where the integrand $F_k(\cos\theta) \coloneqq \cos(k\theta) h(\cos\theta)$ for any $0 \le k \le d'$ with $d' = 2d - 1$. We will calculate this upper bound directly in Fact 5.9.1, and the proof is deferred to the end of this subsection.

Fact 5.9.1. *Consider the integrand $F_k(\theta) = \sum_{m=-M}^{M} \frac{c_m}{2} \big(H_{k,m}^{(+)} - H_{k,m}^{(-)}\big)$ for any function f which is either even or odd. If f is even, we have that $c_m = c_m^{(\mathrm{even})}$ defined in Lemma 5.10,*

with the following holds:

$$H_{k,m}^{(\pm)}(\theta) \coloneqq \cos\left(\pi m\left(\frac{\cos\theta - x_0}{r+\delta}\right)\right) \cdot \cos(k\theta) \cdot \operatorname{erf}\left(\kappa\left(\cos\theta - x_0 \pm r \pm \frac{\delta}{4}\right)\right). \tag{5.12}$$

Likewise, if f is odd, we know that $c_m = c_m^{(\mathrm{odd})}$ defined in Lemma 5.10, and

$$H_{k,m}^{(\pm)}(\theta) \coloneqq \sin\left(\pi\left(m+\frac{1}{2}\right)\left(\frac{\cos\theta - x_0}{r+\delta}\right)\right) \cdot \cos(k\theta) \cdot \operatorname{erf}\left(\kappa\left(\cos\theta - x_0 \pm r \pm \frac{\delta}{4}\right)\right). \tag{5.13}$$

Moreover, the integrand is $F_k(\theta) = \sum_{m=-M}^{M}\left(\frac{c_m^{(\mathrm{even})}}{2}\left(\hat{H}_{k,m}^{(+)} - \hat{H}_{k,m}^{(-)}\right) + \frac{c_m^{(\mathrm{odd})}}{2}\left(\tilde{H}_{k,m}^{(+)} - \tilde{H}_{k,m}^{(-)}\right)\right)$ when f is neither even nor odd, where $\hat{H}_{k,m}^{(\pm)}$ and $\tilde{H}_{k,m}^{(\pm)}$ follow from Equation (5.12) and Equation (5.13), respectively. Regardless of the parity of f, we have that the second derivative $F_k''(\theta) \le O(Bd^3)$.

Together with Fact 5.9.1, we are ready to apply Lemma 5.5 to $h(x) = \hat{f}(x)R(x)$, resulting in a degree-d' polynomial $P_{d'} = \hat{c}_0/2 + \sum_{k=1}^{d'} \hat{c}_k T_k$ where $d' = 2d-1$ and $\hat{c}_k$ is defined as in Equation (5.1). Since $P_{d'}$ is the degree-d averaged Chebyshev truncation of the function h and satisfies Equation (5.11), we define intervals $\mathcal{I}_{\mathrm{int}} \coloneqq [x_0 - r, x_0 + r]$ and $\mathcal{I}_{\mathrm{ext}} \coloneqq [-1,1] \setminus [x_0 - r - \delta/2, x_0 + r + \delta/2]$ to obtain:

$$\begin{aligned} \|f(x) - P_{d'}(x)\|_{\mathcal{I}_{\mathrm{int}}} &\le \|f(x) - h(x)\|_{\mathcal{I}_{\mathrm{int}}} + \|h(x) - P_{d'}(x)\|_{\mathcal{I}_{\mathrm{int}}} \le \epsilon + 4\epsilon = O(\epsilon), \\ \|P_{d'}(x) - 0\|_{\mathcal{I}_{\mathrm{ext}}} &\le \|P_{d'}(x) - h(x)\|_{\mathcal{I}_{\mathrm{ext}}} + \|h(x) - 0\|_{\mathcal{I}_{\mathrm{ext}}} \le 4\epsilon + \epsilon/3B \le O(\epsilon). \end{aligned} \tag{5.14}$$

We can achieve the desired error bound by observing Equation (5.14) implies:

$$\|P_{d'}(x)\|_{[-1,1]} \le \|P_{d'}(x)\|_{\mathcal{I}_{\mathrm{ext}}} + \|P_{d'}(x)\|_{[-1,1]\setminus\mathcal{I}_{\mathrm{ext}}} \le O(\epsilon) + B.$$

Moreover, it is not too hard to see that the first and the second derivatives of the function $h(\cos\theta)$ are continuous, implying that $h(\cos\theta)$ is twice continuously differentiable. By using Lemma 5.5, we deduce that the norm of the coefficient vector $\hat{\mathbf{c}}$ of the polynomial $P_{d'}$ is bounded by $\|\hat{\mathbf{c}}\|_1 \le O(B) \cdot (1 + O(\epsilon)) = O(B)$.

Analyzing time and space complexity. The construction of $\hat{f}(x)$ can be implemented in bounded-error randomized time $\widetilde{O}((\delta')^{-5}\epsilon^{-2}B^2)$ and space $O(\log((\delta')^{-4}\epsilon^{-1}B))$, given that this construction uses Lemma 5.10 with $\delta' = \frac{\delta}{2(r+\delta)} \in (0, \frac{1}{2}]$ and $\epsilon' = \frac{\epsilon}{3B}$. Having $\hat{f}(x)$, we can construct a bounded polynomial approximation $\hat{h}(x)$ deterministically using Lemma 5.5. This construction can be implemented in deterministic time $O(d^{(\gamma+1)/2}\epsilon^{-1/2}t(\ell)) \le \widetilde{O}(d^2\epsilon^{-1/2})$ and space $O(\log(d^{(\gamma+3)/2}\epsilon^{-3/2}B)) \le O(\log(d^3\epsilon^{-3/2}B))$ since the integrand $F_k(\theta)$ is a product of a constant number of (compositions of) holonomic functions (Remark 5.6). Therefore, our construction can be implemented in bounded-error randomized time $\widetilde{O}(\max\left\{(\delta')^{-5}\epsilon^{-2}B^2, d^2\epsilon^{-1/2}\right\})$ and space

$$O(\max\{\log((\delta')^{-4}\epsilon^{-1}B), \log(d^3\epsilon^{-3/2}B)\}) \le O(\log(d^3(\delta')^{-4}\epsilon^{-3/2}B)). \qquad \square$$

With the aid of Theorem 5.9, we can provide a space-efficient polynomial approximation to the normalized logarithmic function utilized in Lemma 11 of [GL20].

Corollary 5.11 (Space-efficient polynomial approximation to the normalized logarithmic function)**.** *Let $\beta \in (0,1]$ and $\epsilon \in (0, 1/2)$, there is an even polynomial $P_{d'}^{\ln}$ of degree $d' = 2d-1 \le \tilde{C}_{\ln}\beta^{-1}\log\epsilon^{-1}$, where $P_{d'}^{\ln}$ corresponds to some degree-d averaged Chebyshev*

truncation and $\tilde{C}_{\ln}$ *is a universal constant, such that*

$$\forall x \in [\beta, 1], \left|P_{d'}^{\ln}(x) - \tfrac{\ln(1/x)}{2\ln(2/\beta)}\right| \le C_{\ln}\epsilon, \text{ where } C_{\ln} \text{ is a universal constant,}$$
$$\forall x \in [-1, 1], |P_{d'}^{\ln}(x)| \le 1.$$

Moreover, the coefficient vector $\mathbf{c}^{\ln}$ *of* $P_{d'}^{\ln}$ *has a norm bounded by* $\|\mathbf{c}^{\ln}\|_1 \le \hat{C}_{\ln}$*, where* $\hat{C}_{\ln}$ *is another universal constant. In addition, any entry of the coefficient vector* $\mathbf{c}^{\ln}$ *can be computed in bounded-error randomized time* $\widetilde{O}(\max\{\beta^{-5}\epsilon^{-2}, d^2\epsilon^{-1/2}\})$ *and space* $O(\log(d^3\beta^{-4}\epsilon^{-3/2}))$*. Without loss of generality, we assume that all constants* $C_{\ln}$*,* $\hat{C}_{\ln}$*, and* $\tilde{C}_{\ln}$ *are at least* 1*.*

Proof. Consider the function $f(x) := \frac{\ln(1/x)}{2\ln(2/\beta)}$. We apply Theorem 5.9 to f by choosing the same parameters as in Lemma 11 of [GL20], specifically $\epsilon' = \epsilon/2$, $x_0 = 1$, $r = 1-\beta$, $\delta = \beta/2$, and $B = 1/2$.[18] This results in a space-efficient randomized polynomial approximation $\tilde{P}_{d'} \in \mathbb{R}[x]$ of degree $d' = 2d - 1 = O(\delta^{-1}\log(\epsilon^{-1}B)) \le \tilde{C}_{\ln}\beta^{-1}\log\epsilon^{-1}$, where $\tilde{P}_{d'}$ corresponds to some degree-d averaged Chebyshev truncation and $\tilde{C}_{\ln}$ is a universal constant. By appropriately choosing $\eta \le 1/2$ such that $C'_{\ln}\epsilon = \eta/4$ for a universal constant $C'_{\ln}$, this polynomial approximation $\tilde{P}_{d'}$ satisfies the following inequalities:

$$\begin{aligned} \|f(x) - \tilde{P}_{d'}(x)\|_{[\beta,2-\beta]} &\le C'_{\ln}\epsilon = \tfrac{\eta}{4} \\ \|\tilde{P}_{d'}(x)\|_{[-1,1]} &\le B + C'_{\ln}\epsilon \le \tfrac{1}{2} + C'_{\ln}\epsilon = \tfrac{1}{2} + \tfrac{\eta}{4} \\ \|\tilde{P}_{d'}(x)\|_{[-1,\beta/2]} &\le C'_{\ln}\epsilon = \tfrac{\eta}{4}. \end{aligned} \tag{5.15}$$

Additionally, the coefficient vector $\mathbf{c}^{(\tilde{P})}$ of $\tilde{P}_{d'}$ satisfies that $\|\mathbf{c}^{(\tilde{P})}\|_1 \le O(B) \le \hat{C}_{\ln}$ where $\hat{C}_{\ln}$ is a universal constant. Notice that $\delta' = \frac{\delta}{2(r+\delta)} = \frac{\beta/2}{2(1-\beta+\beta/2)} = \frac{\beta}{4(1-\beta/2)} = \Theta(\beta)$, our utilization of Theorem 5.9 yields a bounded-error randomized algorithm that requires $O(\log(d^3(\delta')^{-4}\epsilon^{-3/2}B)) = O(\log(d^3\beta^{-4}\epsilon^{-3/2}))$ space and $\widetilde{O}(\max\{(\delta')^{-5}\epsilon^{-2}B^2, d^2\epsilon^{-1/2}\}) = \widetilde{O}(\max\{\beta^{-5}\epsilon^{-2}, d^2\epsilon^{-1/2}\})$ time.

Furthermore, note that the real-valued function $f(x)$ only defines when $x > 0$, then $\tilde{P}(x)$ is not an even polynomial in general. Instead, we consider $P_{d'}^{\ln}(x) := (1+\eta)^{-1}(\tilde{P}_{d'}(x) + \tilde{P}_{d'}(-x))$ for all $x \in [-1, 1]$. Together with Equation (5.15), we have derived the following:

$$\begin{aligned} &\|f(x) - P_{d'}^{\ln}(x)\|_{[\beta,1]} \\ &\le \left\|f(x) - \tfrac{1}{1+\eta}\tilde{P}_{d'}(x)\right\|_{[\beta,1]} + \left\|\tfrac{1}{1+\eta}\tilde{P}_{d'}(-x)\right\|_{[\beta,1]} \\ &\le \left\|f(x) - \tilde{P}_{d'}(x)\right\|_{[\beta,1]} + \left\|\tilde{P}_{d'}(x) - \tfrac{1}{1+\eta}\tilde{P}_{d'}(x)\right\|_{[\beta,1]} + \left\|\tfrac{1}{1+\eta}\tilde{P}_{d'}(-x)\right\|_{[\beta,1]} \\ &\le \tfrac{\eta}{4} + \tfrac{\eta}{1+\eta}\cdot\left(\tfrac{1}{2} + \tfrac{\eta}{4}\right) + \tfrac{1}{1+\eta}\cdot\tfrac{\eta}{4} \\ &= \tfrac{\eta}{4} + \tfrac{\eta}{1+\eta}\cdot\tfrac{1+\eta}{4} + \tfrac{1}{1+\eta}\cdot\tfrac{\eta}{2} \\ &\le \eta. \end{aligned} \tag{5.16}$$

Here, the last line owes to the fact that $\eta > 0$. Consequently, Equation (5.16) implies that $\|f(x) - P_{d'}^{\ln}(x)\|_{[\beta,1]} \le 4C'_{\ln}\epsilon := C_{\ln}\epsilon$ for another universal constant $C_{\ln}$. Notice $P_{d'}^{\ln}$

[18] As indicated in Lemma 11 of [GL20], since the Taylor series of $f(x)$ at $x = 1$ is $\frac{1}{2\ln(2/\beta)}\sum_{l=1}^{\infty}\frac{(-1)^l x^l}{l}$, we obtain the equalities $B = f(\frac{\beta}{2} - 1) = \frac{1}{2\ln(2/\beta)}\sum_{l=1}^{\infty}\frac{(1-\beta/2)^l}{l} = -\frac{1}{2\ln(2/\beta)}\sum_{l=1}^{\infty}\frac{(-1)^{l-1}}{l}(\beta/2-1)^l = -\frac{1}{2\ln(2/\beta)}\ln\frac{\beta}{2} = \frac{1}{2}$.

is an even polynomial with $\deg(P^{\ln}_{d'}) \le \tilde{C}_{\ln}\beta^{-1}\log\epsilon^{-1}$, Equation (5.15) yields that:

$$\|P^{\ln}_{d'}(x)\|_{[-1,1]} = \|P^{\ln}_{d'}(x)\|_{[0,1]} \le \|\tfrac{1}{1+\eta}\tilde{P}_{d'}(x)\|_{[0,1]} + \|\tfrac{1}{1+\eta}\tilde{P}_{d'}(x)\|_{[-1,0]} \le \tfrac{1}{1+\eta}\cdot\tfrac{1+\eta}{2} + \tfrac{1}{1+\eta}\cdot\tfrac{\eta}{2} \le 1.$$

Here, the last inequality is due to $\eta \le 1/2$.

Following the coefficient vector of $\tilde{P}_{d'}$ obtained by applying Theorem 5.9 to f, we complete the proof by noting the coefficient vector $\mathbf{c}^{\ln}$ of $P^{\ln}_{d'}$ satisfies all the desired properties. □

Lastly, we present the proof of Fact 5.9.1.

Proof of Fact 5.9.1. We begin by deriving an upper bound of the second derivative of the integrand $F_k(\theta)$:

$$|F_k''(\theta)| \le \sum_{m=-M}^{M} \tfrac{c_m}{2}\left|\tfrac{\mathrm{d}^2}{\mathrm{d}\theta^2}H^{(+)}_{k,m}(\theta) - \tfrac{\mathrm{d}^2}{\mathrm{d}\theta^2}H^{(-)}_{k,m}(\theta)\right| \le \tfrac{\|\mathbf{c}\|}{2}\max_{-\pi\le\theta\le 0}\left(\left|\tfrac{\mathrm{d}^2}{\mathrm{d}\theta^2}H^{(+)}_{k,m}(\theta)\right| + \left|\tfrac{\mathrm{d}^2}{\mathrm{d}\theta^2}H^{(-)}_{k,m}(\theta)\right|\right). \quad (5.17)$$

By a straightforward calculation, we have the second derivatives of $H^{\pm}_{k,m}(\theta)$ if f is even:

$$\begin{aligned}
\tfrac{\mathrm{d}^2}{\mathrm{d}\theta^2}H^{(\pm)}_{k,m}(\theta) =& -k^2\cos(k\theta)\cos\Big(\tfrac{\pi m(\cos\theta - x_0)}{\delta+r}\Big)\operatorname{erf}\Big(\kappa\big(\cos\theta - x_0 \mp r \mp \tfrac{\delta}{4}\big)\Big)\\
&- \tfrac{\pi^2m^2}{(\delta+r)^2}\sin^2(\theta)\cos(k\theta)\cos\Big(\tfrac{\pi m(\cos\theta - x_0)}{\delta+r}\Big)\operatorname{erf}\Big(\kappa\big(\cos\theta - x_0 \mp r \mp \tfrac{\delta}{4}\big)\Big)\\
&+ \tfrac{\pi m}{\delta+r}\cos\theta\cos(k\theta)\sin\Big(\tfrac{\pi m(\cos\theta - x_0)}{\delta+r}\Big)\operatorname{erf}\Big(\kappa\big(\cos\theta - x_0 \mp r \mp \tfrac{\delta}{4}\big)\Big)\\
&- \tfrac{2\pi km}{\delta+r}\sin(\theta)\sin(k\theta)\sin\Big(\tfrac{\pi m(\cos\theta - x_0)}{\delta+r}\Big)\operatorname{erf}\Big(\kappa\big(\cos\theta - x_0 \mp r \mp \tfrac{\delta}{4}\big)\Big)\\
&- \tfrac{2\kappa}{\sqrt{\pi}}\cos\theta\cos(k\theta)\cos\Big(\tfrac{\pi m(\cos\theta - x_0)}{\delta+r}\Big)e^{-\kappa^2\left(\cos\theta - x_0 \mp r \mp \frac{\delta}{4}\right)^2}\\
&- \tfrac{4\sqrt{\pi}\kappa m}{\delta+r}\sin^2(\theta)\cos(k\theta)\sin\Big(\tfrac{\pi m(\cos\theta - x_0)}{\delta+r}\Big)e^{-\kappa^2\left(\cos\theta - x_0 \mp r \mp \frac{\delta}{4}\right)^2}\\
&+ \tfrac{4\kappa k}{\sqrt{\pi}}\sin(\theta)\sin(k\theta)\cos\Big(\tfrac{\pi m(\cos\theta - x_0)}{\delta+r}\Big)e^{-\kappa^2\left(\cos\theta - x_0 \mp r \mp \frac{\delta}{4}\right)^2}\\
&- \tfrac{4\kappa^3}{\sqrt{\pi}}\sin^2(\theta)\cos(k\theta)\cos\Big(\tfrac{\pi m(\cos\theta - x_0)}{\delta+r}\Big)\Big(\cos\theta - x_0 \mp r \mp \frac{\delta}{4}\Big)e^{-\kappa^2\left(\cos\theta - x_0 \mp r \mp \frac{\delta}{4}\right)^2}.
\end{aligned}$$

Note that all functions appear in $\frac{\mathrm{d}^2}{\mathrm{d}\theta^2}H^{(\pm)}_{k,m}(\theta)$, viz. $\sin x$, $\cos x$, $\exp(-x^2)$, and $\operatorname{erf}(x)$, are at most 1, as well as $|x_0 \pm r \pm \delta/4| \le 7/2$, then we obtain that

$$\begin{aligned}
&\left|\tfrac{\mathrm{d}^2}{\mathrm{d}\theta^2}H^{(\pm)}_{k,m}(\theta)\right|\\
&\le k^2 + \tfrac{2\kappa}{\sqrt{\pi}} + \tfrac{4\kappa k}{\sqrt{\pi}} + \tfrac{18\kappa^3}{\sqrt{\pi}} + m\cdot\Big(\tfrac{\pi}{\delta+r} + \tfrac{2\pi k}{\delta+r} + \tfrac{4\sqrt{\pi}\kappa}{\delta+r}\Big) + m^2\cdot\tfrac{\pi^2}{(\delta+r)^2}\\
&\le (d')^2 + O(d) + O(d^2) + O(d^3) + \tfrac{M}{\delta+r}\cdot(O(1)+O(d)+O(d)) + M^2\cdot\tfrac{O(1)}{(\delta+r)^2}\\
&= O(d^3).
\end{aligned} \quad (5.18)$$

Here, the second line according to $k \le d' = 2d-1$ and $\kappa \le O(d)$, also the last line is due to facts that $M \le O(rd)$ and $1/2 \le r/(\delta+r) \le 1$ if $0 < \delta \le r$ and $0 < r \le 2$. Additionally, a similar argument shows that the upper bound in Equation (5.18) applies to odd functions and functions that are neither even nor odd as well. This is because a direct computation yields the second derivatives of $H^{(\pm)}_{k,m}(\theta)$ when f is odd:

$$\tfrac{\mathrm{d}^2}{\mathrm{d}\theta^2}H^{(\pm)}_{k,m}(\theta) = -k^2\cos(kx)\sin\Big(\tfrac{\pi\left(m+\frac{1}{2}\right)(\cos(x)-x_0)}{\delta+r}\Big)\operatorname{erf}\big(\kappa(\cos(x) - x_0 \mp r \mp \tfrac{\delta}{4})\big)$$

$$
\begin{aligned}
&- \tfrac{\pi\left(m+\frac{1}{2}\right)}{\delta+r}\cos(x)\cos(kx)\cos\!\left(\tfrac{\pi\left(m+\frac{1}{2}\right)(\cos(x)-x_0)}{\delta+r}\right)\operatorname{erf}\left(\kappa\left(\cos(x)-x_0\mp r\mp\tfrac{\delta}{4}\right)\right)\\
&- \tfrac{\pi^2\left(m+\frac{1}{2}\right)^2}{(\delta+r)^2}\sin^2(x)\cos(kx)\sin\!\left(\tfrac{\pi\left(m+\frac{1}{2}\right)(\cos(x)-x_0)}{\delta+r}\right)\operatorname{erf}\left(\kappa\left(\cos(x)-x_0\mp r\mp\tfrac{\delta}{4}\right)\right)\\
&+ \tfrac{2\pi k\left(m+\frac{1}{2}\right)}{\delta+r}\sin(x)\sin(kx)\cos\!\left(\tfrac{\pi\left(m+\frac{1}{2}\right)(\cos(x)-x_0)}{\delta+r}\right)\operatorname{erf}\left(\kappa\left(\cos(x)-x_0\mp r\mp\tfrac{\delta}{4}\right)\right)\\
&+ \tfrac{4\sqrt{\pi}\kappa\left(m+\frac{1}{2}\right)}{\delta+r}\sin^2(x)\cos(kx)\cos\!\left(\tfrac{\pi\left(m+\frac{1}{2}\right)(\cos(x)-x_0)}{\delta+r}\right)e^{-\kappa^2\left(\cos(x)-x_0\mp r\mp\frac{\delta}{4}\right)^2}\\
&- \tfrac{2\kappa}{\sqrt{\pi}}\cos(x)\cos(kx)\sin\!\left(\tfrac{\pi\left(m+\frac{1}{2}\right)(\cos(x)-x_0)}{\delta+r}\right)e^{-\kappa^2\left(\cos(x)-x_0\mp r\mp\frac{\delta}{4}\right)^2}\\
&+ \tfrac{4\kappa k}{\sqrt{\pi}}\sin(x)\sin(kx)\sin\!\left(\tfrac{\pi\left(m+\frac{1}{2}\right)(\cos(x)-x_0)}{\delta+r}\right)e^{-\kappa^2\left(\cos(x)-x_0\mp r\mp\frac{\delta}{4}\right)^2}\\
&- \tfrac{4\kappa^3}{\sqrt{\pi}}\sin^2(x)\cos(kx)\left(\cos(x)-x_0\mp r\mp\tfrac{\delta}{4}\right)\sin\!\left(\tfrac{\pi\left(m+\frac{1}{2}\right)(\cos(x)-x_0)}{\delta+r}\right)e^{-\kappa^2\left(\cos(x)-x_0\mp r\mp\frac{\delta}{4}\right)^2}.
\end{aligned}
$$

Substituting Equation (5.18) into Equation (5.17), and noticing that the coefficient vector $\|\mathbf{c}^{(\mathrm{even})}+\mathbf{c}^{(\mathrm{odd})}\|_1 \le B$ regardless of the parity of f, we conclude that

$$|F_k''(\theta)| \le O(Bd^3). \qquad \square$$

5.2.2 Applying averaged Chebyshev truncation to bitstring indexed encodings

With space-efficient bounded polynomial approximations of piecewise-smooth functions, it suffices to implement averaged Chebyshev truncation on bitstring indexed encodings, as specified in Theorem 5.12. The proof combines Lemma 5.14, Lemma 5.15, and Lemma 5.16.

Theorem 5.12 (Averaged Chebyshev truncation applied to bitstring indexed encodings)**.** *Let A be an Hermitian matrix acting on s qubits, and let U be a $(1,a,\epsilon_1)$-bitstring indexed encoding of A that acts on $s+a$ qubits. For any degree-d averaged Chebyshev truncation $P_{d'}(x)=\hat{c}_0/2+\sum_{k=1}^{d'}\hat{c}_kT_k(x)$ where $d'=2d-1\le 2^{O(s(n))}$ and T_k is the k-th Chebyshev polynomial (of the first kind), equipped with an evaluation oracle* Eval *that returns $\tilde{c}_k$ with precision $\varepsilon := O(\epsilon_2^2/d')$, we have the following bitstring indexed encoding of $P_{d'}(A)$ depending on whether $P_{d'}(A)$ is a partial isometry (up to a normalization factor):*[19]

- ***Partial isometry*** *$P_{d'}(A)$: We obtain a $(1,a',144d'\sqrt{\epsilon_1}\|\hat{\mathbf{c}}\|_1^2+36\epsilon_2\|\hat{\mathbf{c}}\|_1)$-bitstring indexed encoding V_{normed} of $P_{d'}(A)$ that acts on $s+a'$ qubits where $a' := a+\lceil\log d'\rceil+3$.*
- ***General*** *$P_{d'}(A)$: We obtain a $(\|\hat{\mathbf{c}}\|_1,\hat{a},4d'\sqrt{\epsilon_1}\|\hat{\mathbf{c}}\|_1^2+\epsilon_2\|\hat{\mathbf{c}}\|_1)$-bitstring indexed encoding V_{unnorm} of $P_{d'}(A)$ that acts on $s+a'$ qubits where $\hat{a} := a+\lceil\log d'\rceil+1$.*

Let V be the bitstring indexed encoding of $P_{d'}(A)$. The implementation of V requires $O(d^2\eta_V)$ uses of U, $U^\dagger$, $\mathrm{C_\Pi NOT}$, $\mathrm{C_{\tilde{\Pi}}NOT}$, and multi-controlled single-qubit gates.[20] *The description of the resulting quantum circuit of V can be computed in deterministic time $\widetilde{O}(d^2\eta_V\log(d/\epsilon_2))$, space $O(\max\{s(n),\log(d/\epsilon_2^2)\})$, and $O(d^2\eta_V)$ oracle calls to* Eval *with precision ε. Here, $\eta_V=\|\hat{\mathbf{c}}\|_1$ if $V=V_{\mathrm{normed}}$ whereas $\eta_V=1$ if $V=V_{\mathrm{unnorm}}$.*

[19] This condition differs from the one that A is a partial isometry. Specifically, $P_{d'}(A)$ is a partial isometry *(*up to a normalization factor*)* if A is a partial isometry, whereas $\mathrm{sgn}^{(\mathrm{SV})}(A)$ is a partial isometry for any A.

[20] As indicated in Figure 3(c) of [GSLW19] (see also Lemma 19 in [GSLW18]), we replace the single-qubit gates used in Lemma 5.14 with multi-controlled (or "multiply controlled") single-qubit gates.

Furthermore, our construction straightforwardly extends to any linear (possibly non-Hermitian) operator A by simply replacing $P_{d'}(A)$ with $P_{d'}^{(\mathrm{SV})}(A)$ defined in Definition 2.6.

Remark 5.13 (QSVT implementations of averaged Chebyshev truncation preserve the parity). As shown in Proposition 5.14.1, we can implement the quantum singular value transformation $T_k^{(\mathrm{SV})}(A)$ *exactly* for any linear operator A that admits a bitstring indexed encoding, because the rotation angles corresponding to the k-th Chebyshev polynomials are either $\pi/2$ or $(1-k)\pi/2$, indicating that $T_k(0) = 0$ for any odd k. We then implement the QSVT corresponding to the averaged Chebyshev truncation polynomial $P_{d'}(x) = \sum_{l=0}^{(d'-1)/2} \hat{c}_{2l+1} T_{2l+1}(x)$, as described in Corollary 5.17, although the actual implementation results in a slightly different polynomial, $\tilde{P}_{d'}(x) = \sum_{l=0}^{(d'-1)/2} \tilde{c}_{2l+1} T_{2l+1}(x)$. However, we still have $\tilde{P}_{d'}(0) = 0 = P_{d'}(0)$, indicating that the implementations in Theorem 5.12 preserve the parity.

We first demonstrate an approach, based on Lemma 3.12 in [MY23], that constructs Chebyshev polynomials of bitstring indexed encodings in a space-efficient manner.

Lemma 5.14 (Chebyshev polynomials applied to bitstring indexed encodings)**.** *Let A be a linear operator acting on s qubits, and let U be a $(1, a, \epsilon)$-bitstring indexed encoding of A that acts on $s + a$ qubits. Then, for the k-th Chebyshev polynomial (of the first kind) $T_k(x)$ of degree $k \leq 2^{O(s)}$, there exists a new $(1, a+1, 4k\sqrt{\epsilon})$-bitstring indexed encoding V of $T_k^{(\mathrm{SV})}(A)$ that acts on $s + a + 1$ qubits. This implementation requires k uses of U, $U^\dagger$, $\mathrm{C}_\Pi\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and k single-qubit gates. Moreover, we can compute the description of the resulting quantum circuit in deterministic time k and space $O(s)$.*

Furthermore, consider $A' := \tilde{\Pi} U \Pi$, where $\tilde{\Pi}$ and Π are the corresponding orthogonal projections of the bitstring indexed encoding U. If A and A' satisfy the conditions $\|A - A'\| + \left\|\frac{A+A'}{2}\right\|^2 \leq 1$ and $\left\|\frac{A+A'}{2}\right\|^2 \leq \zeta$, then V is a $\left(1, a+1, \frac{\sqrt{2}}{\sqrt{1-\zeta}} k\epsilon\right)$-bitstring indexed encoding of $T_k^{(\mathrm{SV})}(A)$.

Proof. As specified in Proposition 5.14.1, we can derive the sequence of rotation angles corresponding to Chebyshev polynomials $T_k(x)$ by directly factorizing them:

Proposition 5.14.1 (Chebyshev polynomials in quantum signal processing, adapted from Lemma 6 in [GSLW19])**.** *Let $T_k \in \mathbb{R}[x]$ be the k-th Chebyshev polynomial (of the first kind). Consider the corresponding sequence of rotation angles $\Phi \in \mathbb{R}^k$ such that $\phi_1 := (1-k)\pi/2$, and $\phi_j := \pi/2$ for all $j \in [k] \setminus \{1\}$, then we know that*

$$\prod_{j=1}^{k} \left[\begin{pmatrix} \exp(i\phi_j) & 0 \\ 0 & \exp(-i\phi_j) \end{pmatrix} \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix} \right] = \begin{pmatrix} T_k & \cdot \\ \cdot & \cdot \end{pmatrix}.$$

Then we implement the quantum singular value transformation $T_k^{(\mathrm{SV})}(A)$, utilizing an alternating phase modulation (Proposition 5.14.2) with the aforementioned sequence of rotation angles, denoted by V.

Proposition 5.14.2 (QSVT by alternating phase modulation, adapted from Theorem 10 and Figure 3 in [GSLW19])**.** *Suppose $P \in \mathbb{C}[x]$ is a polynomial, and let $\Phi \in \mathbb{R}^n$ be the corresponding sequence of rotation angles. We can construct*

$$P^{(\mathrm{SV})}(\tilde{\Pi} U \Pi) = \begin{cases} \tilde{\Pi} U_\Phi \Pi, & \text{if } n \text{ is odd} \\ \Pi U_\Phi \Pi, & \text{if } n \text{ is even} \end{cases}$$

with a single ancillary qubit. Moreover, this implementation in [GSLW19, Figure 3] *makes k uses of U, $U^\dagger$, $\mathrm{C}_\Pi\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and single-qubit gates.*

Owing to the robustness of QSVT (Lemma 22 in [GSLW18], full version of [GSLW19]), we have that $\left\|T_k^{(\mathrm{SV})}(U) - T_k^{(\mathrm{SV})}(U')\right\| \leq 4k\sqrt{\|A - A'\|} = 4k\sqrt{\epsilon}$, where U' is a $(1, a, 0)$-bitstring indexed encoding of A. Moreover, with a tighter bound for A and A', namely $\|A - A'\| + \left\|\frac{A+A'}{2}\right\|^2 \leq 1$, we can deduce that

$$\|T_k^{(\mathrm{SV})}(U) - T_k^{(\mathrm{SV})}(U')\| \leq k\frac{\sqrt{2}}{\sqrt{1 - \|(A + A')/2\|^2}}\|A - A'\| \leq \frac{\sqrt{2}}{\sqrt{1-\zeta}}k\epsilon$$

following [GSLW18, Lemma 23], indicating an improved dependence of ϵ. Finally, we can compute the description of the resulting quantum circuits in $O(\log k) = O(s(n))$ space and $O(k)$ times because of the implementation specified in Proposition 5.14.2. □

We then proceed by presenting a linear combination of bitstring indexed encodings, which adapts the LCU technique proposed by Berry, Childs, Cleve, Kothari, and Somma in [BCC+15], and incorporates a space-efficient state preparation operator. We say that $P_{\mathbf{y}}$ is an ϵ-state preparation operator for $\mathbf{y}$ if $P_{\mathbf{y}}|\bar{0}\rangle := \sum_{i=1}^m \sqrt{\hat{y}_i}|i\rangle$ for some $\hat{\mathbf{y}}$ such that $\|\mathbf{y}/\|\mathbf{y}\|_1 - \hat{\mathbf{y}}\|_1 \leq \epsilon$.

Lemma 5.15 (Linear combinations of bitstring indexed encodings, adapted from Lemma 29 in [GSLW19])**.** *Given a matrix $A = \sum_{i=0}^{m-1} y_i A_i$ such that each linear operator A_i $(1 \leq i \leq m)$ acts on s qubits with the corresponding $(\|\mathbf{y}\|_1, a, \epsilon_1)$-bitstring indexed encoding U_i acting on $s+a$ qubits associated with projections $\tilde{\Pi}_i$ and Π_i. Also each y_i $(1 \leq i \leq m)$ can be expressed in $O(s(n))$ bits with an evaluation oracle* Eval *that returns $\hat{y}_i$ with precision $\varepsilon := O(\epsilon_2^2/m)$. Then utilizing an ϵ_2-state preparation operator $P_{\mathbf{y}}$ for $\mathbf{y}$ acting on $O(\log m)$ qubits, and a $(s + a + \lceil \log m \rceil)$-qubit unitary*

$$W = \sum_{i=0}^{m-1} |i\rangle\langle i| \otimes U_i + \left(I - \sum_{i=0}^{m-1} |i\rangle\langle i|\right) \otimes I,$$

we can implement a $(\|\mathbf{y}\|_1, a + \lceil \log m \rceil, \epsilon_1\|\mathbf{y}\|_1^2 + \epsilon_2\|\mathbf{y}\|_1)$-bitstring indexed encoding of A acting on $s + a + \lceil \log m \rceil$ qubits with a single use of W, $P_{\mathbf{y}}$, $P_{\mathbf{y}}^\dagger$. In addition, the (classical) pre-processing can be implemented in deterministic time $\widetilde{O}(m^2 \log(m/\epsilon_2))$ and space $O(\log(m/\epsilon_2^2))$, as well as m^2 oracle calls to Eval *with precision ε.*

Proof. For the ϵ_2-state preparation operator $P_{\mathbf{y}}$ such that $P_{\mathbf{y}}|\bar{0}\rangle = \sum_{i=1}^m \sqrt{\hat{y}_i}|i\rangle$, we utilize a scheme introduced by Zalka [Zal98] (also independently rediscovered in [GR02] and [KM01]). We make an additional analysis of the required classical computational complexity.

Proposition 5.15.1 (Space-efficient state preparation, adapted from [Zal98, KM01, GR02])**.** *Given an l-qubit quantum state $|\psi\rangle := \sum_{i=1}^m \sqrt{\hat{y}_i}|i\rangle$, where $l = \lceil \log m \rceil$ and $\hat{y}_i$ are real amplitudes associated with an evaluation oracle* Eval(i, ε) *that returns $\hat{y}_i$ up to accuracy ε we can prepare $|\psi\rangle$ up to accuracy ϵ in deterministic time $\widetilde{O}(m^2 \log(m/\epsilon))$ and space $O(\log(m/\epsilon^2))$, together with m^2 evaluation oracle calls with precision $\varepsilon := O(\epsilon^2/m)$.*

Proof. We follow the analysis presented in [MP16, Section III.A], with a particular focus on the classical computational complexity required for this state preparation procedure.

The algorithm for preparing the state $|\psi\rangle$ expresses the weight W_x as a telescoping product, given by: For any $x \in \{0,1\}^l$,

$$W_x = W_{x_1} \cdot \frac{W_{x_1x_2}}{W_{x_1}} \cdot \frac{W_{x_1x_2x_3}}{W_{x_1x_2}} \cdots \frac{W_x}{W_{x_1\cdots x_{n-1}}}, \text{ where } W_x \coloneqq \sum_{y\in\{0,1\}^{l-|x|}} |\langle xy|\psi\rangle|^2. \tag{5.19}$$

To estimate $|\psi\rangle$ up to accuracy ϵ in the ℓ_2 norm, it suffices to approximate each weight W_x up to additive error $\varepsilon \coloneqq O(\epsilon^2/m)$, as indicated in [MP16, Section III.A]. To compute $W_{x'}$, we need $2^{l-|x'|}$ oracle calls to $\mathrm{Eval}(\cdot,\varepsilon)$. Evaluating all terms in Equation (5.19) requires computing $W_{x_1}, W_{x_1x_2}, \cdots, W_x$ for any $x \in \{0,1\}^l$, which can be achieved by $2^{l-1}+2^{l-2}+\cdots+1 = 2^l$ oracle calls to $\mathrm{Eval}(\cdot,\varepsilon)$. As we need to compute Equation (5.19) for all $x \in \{0,1\}^l$, the overall number of oracle calls to $\mathrm{Eval}(\cdot,\varepsilon)$ is $2^{2l} = m^2$.

The remaining computation can be achieved in deterministic time $\widetilde{O}(m^2 \log(m/\epsilon))$ and space $O(\log(m/\epsilon))$ where the time complexity is because of the iterated integer multiplication. □

Now consider the bitstring indexed encoding $\left(P_{\mathbf{y}}^\dagger \otimes I_s\right) W \left(P_{\mathbf{y}} \otimes I_s\right)$ of A acting on $s + a + \lceil \log m \rceil$ qubits. Let $y_i' \coloneqq y_i/\|\mathbf{y}\|_1$, then we obtain the implementation error:

$$\begin{aligned}
&\left\| A - \|\mathbf{y}\|_1 \left(|\bar{0}\rangle\langle\bar{0}| \otimes \tilde{\Pi}\right) \left(P_y^\dagger \otimes I_s\right) W \left(P_y \otimes I_s\right) \left(|\bar{0}\rangle\langle\bar{0}| \otimes \Pi\right) \right\| \\
=&\left\| A - \|\mathbf{y}\|_1 \textstyle\sum_{i=0}^{m-1} \hat{y}_i \tilde{\Pi}_i U_i \Pi_i \right\| \\
\leq&\left\| A - \|\mathbf{y}\|_1 \textstyle\sum_{i=0}^{m-1} y_i' \tilde{\Pi}_i U_i \Pi_i \right\| + \|\mathbf{y}\|_1 \textstyle\sum_{i=0}^{m-1} (y_i' - \hat{y}_i) \|\tilde{\Pi}_i U_i \Pi_i\| \\
\leq&\|\mathbf{y}\|_1 \textstyle\sum_{i=0}^{m-1} y_i' \|A_i - \tilde{\Pi}_i U_i \Pi_i\| + \epsilon_2 \|\mathbf{y}\|_1 \\
\leq&\epsilon_1 \|\mathbf{y}\|_1^2 + \epsilon_2 \|\mathbf{y}\|_1.
\end{aligned}$$

Here, the third line is due to the triangle inequality, the fourth line owes to Proposition 5.15.1, and the fifth line is because U_i is a $(1, a, \epsilon_1)$-bitstring indexed encoding of A_i for $0 \leq i < m$. □

To make the resulting bitstring indexed encoding from Lemma 5.15 with $\alpha = 1$, we need to perform *a renormalization procedure* to construct a new encoding with the desired α. We achieve this by extending the proof strategy outlined by Gilyen [Gil19, Page 52] for block-encodings to bitstring indexed encodings. This approach works specifically for *partial isometries* (up to a normalization factor α) – since the singular values of a partial isometry is either 0 or 1, it suffices to consider a space-efficient QSVT associated with some Chebyshev polynomial T_k, with an appropriately chosen odd k, such that $T_k(1/\alpha) = 1$ and $T_k(0/\alpha) = 0$.[21]

The renormalization procedure is provided in Lemma 5.16. Additionally, a similar result has been established in [MY23, Lemma 7.10].

Lemma 5.16 (Renormalizing bitstring indexed encoding)**.** *Let U be an (α, a, ϵ)-bitstring indexed encoding of A, where $\alpha > 1$ and $0 < \epsilon < 1$, and A is a partial isometry acting on $s(n)$ qubits. We can implement a quantum circuit V, serving as a normalization of*

[21] Renormalizing bitstring indexed encodings of *non-partial isometries* for space-efficient QSVT seems achievable by mimicking [GSLW19, Theorem 17]. This approach cleverly uses space-efficient QSVT with the sign function (Corollary 5.17), where the corresponding encoding can be re-normalized by carefully using Lemma 5.16. Nevertheless, since this renormalization procedure is not required in this paper, we leave it for future work.

U, such that V is a $(1, a+2, 36\epsilon)$-bitstring indexed encoding of A. This implementation requires $O(\alpha)$ uses of U, $U^\dagger$, $\mathrm{C}_\Pi\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and $O(\alpha)$ single-qubit gates. Moreover, the description of the resulting quantum circuit can be computed in deterministic time $O(\alpha)$ and space $O(s)$.

Proof. Following Definition 5.3, we have $\|A - \alpha\tilde{\Pi}U\Pi\| \leq \epsilon$, where $\tilde{\Pi}$ and Π are the corresponding orthogonal projections. Because U is a $(1, a, \epsilon/\alpha)$-bitstring indexed encoding A/α, we obtain that $\|A/\alpha\| \leq \|U\| + \epsilon/\alpha = 1 + \epsilon/\alpha$, equivalently $\|A\| \leq \alpha + \epsilon$.

Adjusting the encoding through a single-qubit rotation. Consider an odd integer $k := 2\lceil \pi(\alpha+1)/2 \rceil + 1 \leq 9\alpha = O(\alpha)$ and $\gamma := (\alpha+\epsilon)\sin(\pi/2k) \leq 1$. We define new orthogonal projections $\tilde{\Pi}' := \tilde{\Pi} \otimes |0\rangle\langle 0|$ and $\Pi' := \Pi \otimes |0\rangle\langle 0|$, and combine them with $U' = U \otimes R_\gamma$, where $R_\gamma = \begin{pmatrix} \gamma & -\sqrt{1-\gamma^2} \\ \sqrt{1-\gamma^2} & \gamma \end{pmatrix}$. By noting that $\tilde{\Pi}'U'\Pi' = \gamma\tilde{\Pi}U\Pi \otimes |0\rangle\langle 0|$, we deduce that U' is a $(1, a+1, \gamma\epsilon/\alpha)$-bitstring indexed encoding of $\gamma A/\alpha \otimes |0\rangle\langle 0|$, which is consequently a $(1, a+1, 2\gamma\epsilon/\alpha)$-bitstring indexed encoding of $\sin(2\pi/k) \cdot (A \otimes |0\rangle\langle 0|)$. An error bound follows:

$$\left\| \frac{\gamma}{\alpha} A - \sin\left(\frac{\pi}{2k}\right) A \right\| = \left\| \frac{\epsilon}{\alpha} \sin\left(\frac{\pi}{2k}\right) A \right\| \leq \frac{\epsilon}{\alpha} \sin\left(\frac{\pi}{2k}\right)(\alpha+\epsilon) = \frac{\gamma\epsilon}{\alpha}.$$

Renormalizing the encoding via robust oblivious amplitude amplification. We follow the construction in [GSLW18, Theorem 28], the full version of [GSLW19], and perform a meticulous analysis of the complexity. We observe that it suffices to consider $k \geq 3$, as for U' is already a $(1, a+1, 2\gamma\epsilon/\alpha)$-bitstring indexed encoding of $A \otimes |0\rangle\langle 0|$ when $k = 1$. Let $\varepsilon := 2\gamma\epsilon/\alpha$, and for simplicity, we first start by considering the case with $\varepsilon = 0$. By Definition 5.3, we have $\tilde{\Pi}'U'\Pi' = \alpha \sin\left(\frac{\pi}{2k}\right)\tilde{\Pi}U\Pi \otimes |0\rangle\langle 0|$. Let $T_k \in \mathbb{R}[x]$ be the degree-k Chebyshev polynomial (of the first kind). By employing Lemma 5.14, we can apply the QSVT associated with T_k to the bitstring indexed encoding U', yielding:

$$\tilde{\Pi}'T_k^{(\mathrm{SV})}(U')\Pi' = \alpha T_k\left(\sin\left(\frac{\pi}{2k}\right)\right)\tilde{\Pi}U\Pi \otimes |0\rangle\langle 0| = \cos\left(\frac{k-1}{2}\pi\right) A \otimes |0\rangle\langle 0| = A \otimes |0\rangle\langle 0|.$$

Here, the second equality is due to $T_k\left(\sin\left(\frac{\pi}{2k}\right)\right) = T_k\left(\cos\left(\frac{\pi}{2} - \frac{\pi}{2k}\right)\right) = \cos\left(\frac{k-1}{2}\pi\right)$, and the last equality holds because k is odd.

Next, we move on the case with $\varepsilon > 0$ and restrict it to $\varepsilon \leq 1/3$.[22] Let $A' := \tilde{\Pi}'U'\Pi'$ and $\hat{A} := \gamma A \otimes |0\rangle\langle 0|$, then we have $\|A' - \hat{A}\| \leq \varepsilon$, indicating that $\left\|\frac{A'+\hat{A}}{2}\right\|^2 \leq \frac{4}{9} := \zeta$[23] and $\|A' - \hat{A}\| + \left\|\frac{A'+\hat{A}}{2}\right\|^2 \leq \frac{1}{3} + \frac{4}{9} < 1$. By employing Lemma 5.14, as well as the facts that $\frac{\sqrt{2}}{\sqrt{1-\zeta}} < 2$ and $2k\varepsilon = 4k\gamma\epsilon/\alpha \leq 36\epsilon$, we can construct a $(1, a+2, 36\epsilon)$-bitstring indexed encoding of A, denoted by V.

Finally, we provide the computational resources required for implementing V. As shown in Lemma 5.14, the implementation of V requires $O(\alpha)$ uses of U, $U^\dagger$, $\mathrm{C}_\Pi\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and $O(\alpha)$ single-qubit gates. Furthermore, the description of the resulting quantum circuit can be computed in deterministic time $O(\alpha)$ and space $O(s)$. □

[22] If $\varepsilon > 1/3$, then $\|\tilde{\Pi}'U'\Pi' - A \otimes |0\rangle\langle 0|\| \leq 2 = 2 \cdot 3 \cdot \frac{1}{3}$ always holds, implying that we can directly use U' as V.

[23] This is because $\|A' + \hat{A}\| \leq \|A'\| + \|A'\| + \|A' - \hat{A}\| \leq 2\sin(\pi/2k) + \varepsilon \leq 2\sin(\pi/6) + 1/3 = 4/3$.

Finally, we combine Lemma 5.14, Lemma 5.15, and Lemma 5.16 to proceed with the proof of Theorem 5.12.

Proof of Theorem 5.12. By using Lemma 5.14, we obtain $(1, a+1, 4k\sqrt{\epsilon_1})$-bitstring indexed encodings V_k corresponding to $T_k(A)$, where $1 \leq k \leq d' = 2d-1$. The descriptions of quantum circuits $\{V_k\}_{k=0}^{d'}$ can be computed in $O(s(n))$ space and $\sum_{k=0}^{d'} k = O(d^2)$ time. Employing Lemma 5.15, we obtain a $(\|\hat{\mathbf{c}}\|_1, \hat{a}, 4k\sqrt{\epsilon_1}\|\hat{\mathbf{c}}\|_1^2 + \epsilon_2\|\hat{\mathbf{c}}\|_1)$-bitstring indexed encoding V_{unnorm} for $P_{d'}(A) = \hat{c}_0/2 + \sum_{k=1}^{d'} \hat{c}_k T_k(A)$, where $\hat{a} \coloneqq a + \lceil \log d \rceil + 1$. The remaining analysis depends on whether $P_{d'}(A)$ is a partial isometry (up to a normalization factor):

- **Partial isometry $P_{d'}(A)$:** We can renormalize V_{unnorm} by utilizing Lemma 5.16 and obtain a $(1, a', 144k\sqrt{\epsilon_1}\|\hat{\mathbf{c}}\|_1^2 + 36\epsilon_2\|\hat{\mathbf{c}}\|_1)$-bitstring indexed encoding V_{normed} that acts on $s + a'$ qubits, where $a' \coloneqq \hat{a} + 2 = a + \lceil \log d' \rceil + 3$. A direct calculation shows that the implementation of V_{normed} makes $\sum_{k=1}^{d'} k \cdot O(\|\hat{\mathbf{c}}\|_1) = O(d^2\|\hat{\mathbf{c}}\|_1)$ uses of U, $U^\dagger$, $\mathrm{C}_\Pi\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and multi-controlled single-qubit gates. The description of the quantum circuit V_{normed} thus can be computed in deterministic time
$$\max\{\widetilde{O}\Big((d')^2\|\hat{\mathbf{c}}\|_1 \log(d'/\epsilon_2)\Big), O((d')^2\|\hat{\mathbf{c}}\|_1)\} = \widetilde{O}(d^2\|\hat{\mathbf{c}}\|_1 \log(d/\epsilon_2))$$
and space $O(\max\{s(n), d'/\epsilon_2^2\}) = O(\max\{s(n), d/\epsilon_2^2\})$, as well as $O\Big((d')^2\|\hat{\mathbf{c}}\|_1\Big) = O(d^2\|\hat{\mathbf{c}}\|_1)$ oracle calls to Eval with precision ε.
- **General $P_{d'}(A)$:** We simply use the bitstring indexed encoding V_{unnorm} without renormalizing it. Similarly, the implementation of V_{unnorm} makes $O(d^2)$ uses of U, $U^\dagger$, $\mathrm{C}_\Pi\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and multi-controlled single-qubit gates. Therefore, the description of the quantum circuit V_{unnorm} can be computed in deterministic time $\widetilde{O}(d^2 \log(d/\epsilon_2))$ and space $O(\max\{s(n), d/\epsilon_2^2\})$, as well as $O(d^2)$ oracle calls to Eval with precision ε.

Finally, we can extend our construction to any linear operator A by replacing $P_{d'}(A)$ with $P_{d'}^{(\mathrm{SV})}$ as defined in Definition 2.6, taking into account that the Chebyshev polynomial (of the first kind) T_k is either an even or an odd function. □

5.3 Examples: The sign function and the normalized logarithmic function

We now provide explicit examples that illustrate the usage of the space-efficient quantum singular value transformation (QSVT) technique. We define two functions:
$$\mathrm{sgn}(x) \coloneqq \begin{cases} 1, & x > 0 \\ -1, & x < 0 \\ 0, & x = 0 \end{cases} \quad \text{and} \quad \ln_\beta(x) \coloneqq \frac{\ln(1/x)}{2\ln(2/\beta)}.$$

In particular, the sign function is a bounded function, and we derive the corresponding bitstring indexed encoding with *deterministic* space-efficient (classical) pre-processing in Corollary 5.8. On the other hand, the logarithmic function is a piecewise-smooth function that is bounded by 1, and we deduce the corresponding bitstring indexed encoding with *randomized* space-efficient (classical) pre-processing in Corollary 5.11.

Corollary 5.17 (Sign polynomial with space-efficient coefficients applied to bitstring

indexed encodings). *Let A be an Hermitian matrix that acts on s qubits, where $s(n) \geq \Omega(\log(n))$. Let U be a $(1, a, \epsilon_1)$-bitstring indexed encoding of A that acts on $s + a$ qubits. Then, for any $d' \leq 2^{O(s(n))}$ and $\epsilon_2 \geq 2^{-O(s(n))}$, we have an $\Big(1, a+\lceil \log d' \rceil + 3, 144\hat{C}_{\mathrm{sgn}}^2 d\epsilon_1^{1/2} + (36\hat{C}_{\mathrm{sgn}} + 37)\epsilon_2)\Big)$-bitstring indexed encoding V of $P_{d'}^{\mathrm{sgn}}(A)$, where $P_{d'}^{\mathrm{sgn}}$ is a space-efficient bounded polynomial approximation of the sign function (corresponding to some degree-d averaged Chebyshev truncation) specified in Corollary 5.8, and $\hat{C}_{\mathrm{sgn}}$ is a universal constant. This implementation requires $O(d^2)$ uses of U, $U^\dagger$, $\mathrm{C}_{\Pi}\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and $O(d^2)$ multi-controlled single-qubit gates. The description of V can be computed in deterministic time $\widetilde{O}(\epsilon_2^{-1} d^{9/2})$ and space $O(s(n))$.*

Furthermore, our construction directly extends to any non-Hermitian (but linear) matrix A by simply replacing $P_d^{\mathrm{sgn}}(A)$ with $P_{\mathrm{sgn},d}^{(\mathrm{SV})}(A)$ defined in the same way as Definition 2.6.

Proof. Following Corollary 5.8, we have $P_{d'}^{\mathrm{sgn}}(x) = \hat{c}_0/2 + \sum_{k=1}^{d'} \hat{c}_k T_k(x)$, where $d' = 2d-1$ and $d' = O(\delta^{-1} \log \epsilon^{-1})$. The approximation error is given by:

$$\forall x \in [-1,1] \setminus [-\delta, \delta],\ |\mathrm{sgn}(x) - P_{d'}^{\mathrm{sgn}}(x)| \leq C_{\mathrm{sgn}}\epsilon \coloneqq \epsilon_2. \tag{5.20}$$

To implement Eval with precision $\varepsilon = O(\epsilon_2^2/d')$, we can compute the corresponding entry $\hat{c}_k$ of the coefficient vector, which requires deterministic time $\widetilde{O}\Big(\varepsilon^{-1/2}(d')^2\Big) = \widetilde{O}(\epsilon_2^{-1} d^{5/2})$ and space $O\Big(\log(\varepsilon^{-3/2}(d')^3)\Big) = O(\log(\epsilon_2^{-3} d^{9/2}))$.

Note that $P_{d'}^{\mathrm{sgn}}(A)$ is not a partial isometry (up to a normalization factor) and $\|\hat{\mathbf{c}}\|_1 \leq \hat{C}_{\mathrm{sgn}}$. Using Theorem 5.12, we have a $(\hat{C}_{\mathrm{sgn}}, a_{\mathrm{un}}, 4d'\hat{C}_{\mathrm{sgn}}^2\epsilon_1^{1/2} + \hat{C}_{\mathrm{sgn}}\epsilon_2)$-bitstring indexed encoding V_{un}, with projections $\tilde{\Pi}$ and Π, that acts on $s + a_{\mathrm{un}}$ qubits and $a_{\mathrm{un}} \coloneqq a + \lceil \log d' \rceil + 1$.

Renormalizing the encoding of $P_{d'}^{\mathrm{sgn}}(A)$. Notably, the renormalization procedure (Lemma 5.16) is *still applicable* when $P_{d'}^{\mathrm{sgn}}(A)$ is restricted to appropriately chosen subspaces Γ_L and Γ_R. Let $A = \sum_{i=1}^{\mathrm{rank}(A)} \sigma_i \mathbf{u}_i \mathbf{v}_i^\dagger$ be the singular value decomposition of A. We define $A_{>\delta} \coloneqq \sum_{i:\sigma_i > \delta} \sigma_i \mathbf{u}_i \mathbf{v}_i^\dagger$, as well as subspaces $\Gamma_L \coloneqq \mathrm{span}\{\mathbf{u}_i | \sigma_i > \delta\}$ and $\Gamma_R \coloneqq \mathrm{span}\{\mathbf{v}_i^\dagger | \sigma_i > \delta\}$. Consequently, we obtain the following for the bitstring indexed encoding V_{un} with projections $\tilde{\Pi}$ and Π:

$$\begin{aligned}
&\|\mathrm{sgn}^{(\mathrm{SV})}(A_{>\delta}) - \hat{C}_{\mathrm{sgn}}\tilde{\Pi}|_{\Gamma_L} V_{\mathrm{nu}} \Pi|_{\Gamma_R}\| \\
\leq &\|\mathrm{sgn}^{(\mathrm{SV})}(A_{>\delta}) - P_{d'}^{\mathrm{sgn}}(A_{>\delta})\| + \|P_{d'}^{\mathrm{sgn}}(A_{>\delta}) - \hat{C}_{\mathrm{sgn}}\tilde{\Pi}|_{\Gamma_L} V_{\mathrm{nu}} \Pi|_{\Gamma_R}\| \\
\leq &\epsilon_2 + \|P_{d'}^{\mathrm{sgn}}(A_{>\delta}) - \hat{C}_{\mathrm{sgn}}\tilde{\Pi} V_{\mathrm{nu}} \Pi\| \\
\leq &\epsilon_2 + 4d'C_{\mathrm{sgn}}^2\epsilon_1^{1/2} + \hat{C}_{\mathrm{sgn}}\epsilon_2.
\end{aligned} \tag{5.21}$$

Here, the second line owes to the triangle inequality, the third line is due to Equation (5.20), and the last line is because V_{nu} is a $(\hat{C}_{\mathrm{sgn}}, a_{\mathrm{un}}, 4d'C_{\mathrm{sgn}}^2\epsilon_1^{1/2} + \hat{C}_{\mathrm{sgn}}\epsilon_2)$-bitstring indexed encoding of $P_{d'}^{\mathrm{sgn}}(A_{>\delta})$. Note that $\mathrm{sgn}^{(\mathrm{SV})}(A_{>\delta})$ is a partial isometry, and Equation (5.21) implies that V_{nu} is a projected unitary encoding of $\mathrm{sgn}^{(\mathrm{SV})}(A_{>\delta})$. By applying Lemma 5.16 to V_{nu} with projections $\tilde{\Pi}|_{\Gamma_L}$ and $\Pi|_{\Gamma_R}$, we can obtain a $(1, a_{\mathrm{un}} + 2, 144d'C_{\mathrm{sgn}}^2\epsilon_1^{1/2} + 36(\hat{C}_{\mathrm{sgn}} + 1)\epsilon_2)$-projected unitary encoding of $\mathrm{sgn}^{(\mathrm{SV})}(A_{>\delta})$, denoted as

V. Consequently, we can derive that:

$$\begin{aligned}
&\|P^{\mathrm{sgn}}_{d'}(A_{>\delta}) - \tilde{\Pi}|_{\Gamma_L} V_{\mathrm{nu}} \Pi|_{\Gamma_R}\| \\
\leq &\|P^{\mathrm{sgn}}_{d'}(A_{>\delta}) - \mathrm{sgn}^{(\mathrm{SV})}(A_{>\delta})\| + \|\mathrm{sgn}^{(\mathrm{SV})}(A_{>\delta}) - \tilde{\Pi}|_{\Gamma_L} V_{\mathrm{nu}} \Pi|_{\Gamma_R}\| \\
\leq &\epsilon_2 + 144 d' C^2_{\mathrm{sgn}} \epsilon_1^{1/2} + 36(\hat{C}_{\mathrm{sgn}} + 1)\epsilon_2.
\end{aligned} \tag{5.22}$$

Here, the second line follows from the triangle inequality, and the third line additionally owes to Equation (5.20). Note that Lemma 5.16 essentially applies a Chebyshev polynomial to V_{nu} and preserves the projections $\tilde{\Pi}|_{\Gamma_L}$ and $\Pi|_{\Gamma_R}$, then we have $\|\tilde{\Pi} V \Pi\| \leq 1$. Therefore, following Equation (5.22), we conclude that $P^{\mathrm{sgn}}_{d'}(A)$ has a $\Big(1, a', 144 d' C^2_{\mathrm{sgn}} \epsilon_1^{1/2} + (36\hat{C}_{\mathrm{sgn}} + 37)\epsilon_2\Big)$-bitstring indexed encoding V that acts on $s + a'$ qubits, where $a' \coloneqq a + \lceil \log d \rceil + 3$.[24]

Lastly, we can complete the remained analysis similar to Theorem 5.12 with a partial isometry $P_{d'}(A)$. Since $\|\hat{\mathbf{c}}\|_1 \leq \hat{C}_{\mathrm{sgn}} \leq O(1)$, the quantum circuit of V makes $O(d^2)$ uses of U, $U^\dagger$, $\mathrm{C}_{\Pi}\mathrm{NOT}$, and $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$ as well as $O(d^2)$ multi-controlled single-qubit gates. We note that $d \leq 2^{O(s(n))}$ and $\epsilon_2 \geq 2^{-O(s(n))}$. Moreover, we can compute the description of V in $O(s(n))$ space since each oracle call to Eval with precision ε can be computed in $O(\log(\epsilon_2^{-3} d^{9/2}))$ space. Additionally, the time complexity for computing the description of V is

$$\max\{\widetilde{O}(d^2 \log(d/\epsilon_2)), O(d^2) \cdot \widetilde{O}(\epsilon_2^{-1} d^{5/2})\} = \widetilde{O}(\epsilon_2^{-1} d^{9/2}). \qquad \square$$

Corollary 5.18 (Log polynomial with space-efficient coefficients applied to bitstring indexed encodings)**.** *Let A be an Hermitian matrix that acts on s qubits, where $s(n) \geq \Omega(\log(n))$. Let U be a $(1, a, \epsilon_1)$-bitstring indexed encoding of A that acts on $s + a$ qubits. Then, for any $d' = 2d - 1 \leq 2^{O(s(n))}$, $\epsilon_2 \geq 2^{-O(s(n))}$, and $\beta \geq 2^{-O(s(n))}$, we have a $(\hat{C}_{\ln}, a + \lceil \log d \rceil + 1, 4d\hat{C}^2_{\ln}\epsilon_1^{1/2} + \hat{C}_{\ln}\epsilon_2)$-bitstring indexed encoding V of $P^{\ln}_{d'}(A)$, where $P^{\ln}_{d'}$ is a space-efficient bounded polynomial approximation of the normalized log function (corresponding to some degree-d averaged Chebyshev truncation) specified in Corollary 5.11, and $\hat{C}_{\ln}$ is a universal constant. This implementation requires $O(d^2)$ uses of U, $U^\dagger$, $\mathrm{C}_{\Pi}\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and multi-controlled single-qubit gates. Moreover, we can compute the description of the resulting quantum circuit in bounded-error randomized time $\widetilde{O}(\max\{\beta^{-5}\epsilon_2^{-4} d^4, \epsilon_2^{-1} d^{9/2}\})$ and space $O(s(n))$.*

Proof. Following Corollary 5.11, we have $P^{\ln}_{d'}(x) = c^{\ln}_0/2 + \sum_{k=1}^{d'} c^{\ln}_k T_k(x)$, where $P^{\ln}_{d'}$ corresponds to some degree-d averaged Chebyshev truncation and $d' = 2d - 1 \leq O(\delta^{-1} \log \epsilon^{-1})$. For any $\ln_\beta(x)$, we have $|\ln_\beta(x) - P^{\ln}_{d'}(x)| \leq C_{\ln}\epsilon \coloneqq \epsilon_2$ for all $x \in [\beta, 1]$. To implement Eval with precision $\varepsilon = O(\epsilon_2^2/d)$, we can compute the corresponding entry $c^{\ln}_k$ of the coefficient vector by a bounded-error randomized algorithm. This requires $O(\log(\beta^{-4}\varepsilon^{-3/2} d^3)) = O(\log(\beta^{-4}\epsilon_2^{-3} d^{9/2}))$ space and $\widetilde{O}(\max\{\beta^{-5}\varepsilon^{-2}, \varepsilon^{-1/2} d^2\}) = \widetilde{O}(\max\{\beta^{-5}\epsilon_2^{-4} d^2, \epsilon_2^{-1} d^{5/2}\})$ time. Applying Theorem 5.12 with $\|\mathbf{c}^{\ln}\|_1 \leq \hat{C}_{\ln}$, we obtain that $P^{\ln}_{d'}$ has a $(\hat{C}_{\ln}, \hat{a}, 4d\hat{C}^2_{\ln}\epsilon_1^{1/2} + \hat{C}_{\ln}\epsilon_2)$-bitstring indexed encoding V that acts on $s + \hat{a}$ qubits, where $\hat{a} \coloneqq a + \lceil \log d' \rceil + 1$.

Furthermore, the quantum circuit of V makes $O((d')^2) = O(d^2)$ uses of U, $U^\dagger$, $\mathrm{C}_{\Pi}\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and multi-controlled single-qubit gates. We note that $d' = 2d - 1 \leq 2^{O(s(n))}$, $\epsilon_2 \geq 2^{-O(s(n))}$, and $\beta \geq 2^{-O(s(n))}$. Additionally, we can compute the description

[24] We are somewhat abusing notations – strictly speaking, V corresponds $\tilde{P}^{\mathrm{sgn}}_{d'}(A)$, where $\tilde{P}^{\mathrm{sgn}}_{d'}$ is another polynomial satisfying all requirements in Corollary 5.8 but does not necessarily exactly coincide with $P^{\mathrm{sgn}}_{d'}$.

of V in $O(s(n))$ space since each oracle call to Eval with precision ε can be computed in $O(\log(\beta^{-4}\epsilon_2^{-3}d^{9/2}))$ space. The time complexity for computing the description of V is given by:

$$\begin{aligned} &\max\{\widetilde{O}(d^2\log(d/\epsilon_2)), O(d^2)\widetilde{O}(\max\{\beta^{-5}\epsilon_2^{-4}d^2, \epsilon_2^{-1}d^{5/2}\}) \\ &= \widetilde{O}(\max\{\beta^{-5}\epsilon_2^{-4}d^4, \epsilon_2^{-1}d^{9/2}\}). \end{aligned} \tag{5.23}$$

Finally, to guarantee that the probability that all $O((d')^2) = O(d^2)$ oracle calls to Eval succeed is at least $2/3$, we use a $(4\ln d')$-time sequential repetition of Eval for each oracle call. Together with the Chernoff-Hoeffding bound and the union bound, the resulting randomized algorithm succeeds with probability at least $1-(d')^2\cdot 2\exp(-4\ln d') \geq 2/3$. We further note that the time complexity specified in Equation (5.23) only increases by a $4\ln d'$ factor. □

5.4 Application: Space-efficient error reduction for unitary quantum computations

We provide a unified space-efficient error reduction for unitary quantum computations. More specifically, one-sided error scenarios (e.g., $\mathsf{RQ_UL}$ and $\mathsf{coRQ_UL}$) have been proven in [Wat01], and the two-sided error scenario (e.g., $\mathsf{BQ_UL}$) has been demonstrated in [FKL+16].

Theorem 5.19 (Space-efficient error reduction for unitary quantum computations)**.** *Let $s(n)$ be a space-constructible function, and let $a(n)$, $b(n)$, and $l(n)$ be deterministic $O(s(n))$ space computable functions such that $a(n)-b(n) \geq 2^{-O(s(n))}$, we know that for any $l(n) \leq O(s(n))$, there is $d := l(n)/\max\{\sqrt{a}-\sqrt{b}, \sqrt{1-b}-\sqrt{1-a}\}$ such that*

$$\mathsf{BQ_USPACE}[s(n), a(n), b(n)] \subseteq \mathsf{BQ_USPACE}\Big[s(n)+\lceil\log d\rceil+1, 1-2^{-l(n)}, 2^{-l(n)}\Big].$$

Furthermore, for one-sided error scenarios, we have that for any $l(n) \leq 2^{O(s(n))}$:

$$\mathsf{RQ_USPACE}[s(n), a(n)] \subseteq \mathsf{RQ_USPACE}\big[s(n)+\lceil\log d_0\rceil+1, 1-2^{-l(n)}\big] \text{ where } d_0 := \tfrac{l(n)}{\max\{\sqrt{a}, 1-\sqrt{1-a}\}},$$
$$\mathsf{coRQ_USPACE}[s(n), b(n)] \subseteq \mathsf{coRQ_USPACE}\big[s(n)+\lceil\log d_1\rceil+1, 2^{-l(n)}\big] \text{ where } d_1 := \tfrac{l(n)}{\max\{1-\sqrt{b}, \sqrt{1-b}\}}.$$

By choosing $s(n) = \Theta(\log(n))$, we derive error reduction for logarithmic-space quantum computation in a unified approach:

Corollary 5.20 (Error reduction for $\mathsf{BQ_UL}$, $\mathsf{RQ_UL}$, and $\mathsf{coRQ_UL}$)**.** *For deterministic logspace computable functions $a(n)$, $b(n)$, and $l(n)$ satisfying $a(n)-b(n) \geq 1/\mathrm{poly}(n)$ and $l(n) \leq O(\log n)$, we have the following inclusions:*

$$\begin{aligned} \mathsf{BQ_UL}[a(n), b(n)] &\subseteq \mathsf{BQ_UL}[1-2^{-l(n)}, 2^{-l(n)}], \\ \mathsf{RQ_UL}[a(n)] &\subseteq \mathsf{RQ_UL}[1-2^{-l(n)}], \\ \mathsf{coRQ_UL}[b(n)] &\subseteq \mathsf{coRQ_UL}[2^{-l(n)}]. \end{aligned}$$

The construction specified in Theorem 5.19 crucially relies on Lemma 5.21. And the proof of Lemma 5.21 directly follows from Theorem 20 in [GSLW19].

Lemma 5.21 (Space-efficient singular value discrimination)**.** *Let $0 \leq \alpha < \beta \leq 1$ and U be a $(1,0,0)$-bitstring indexed encoding of $A := \tilde{\Pi}U\Pi$, where U acts on s qubits and $s(n) \geq$*

$\Omega(\log n)$. *Consider an unknown quantum state* $|\psi\rangle$*, with the promise that it is a right singular vector of* A *with a singular value either above* α *or below* β*. There is a degree-*d' *polynomial* P*, where* $d' = O(\delta^{-1}\log\varepsilon^{-1})$ *and* $\delta := \max\{\beta-\alpha, \sqrt{1-\alpha^2}-\sqrt{1-\beta^2}\}/2$*, such that there is a singular value discriminator* U_P *that distinguishes the two cases with error probability at most* ε*. Moreover, the discriminator* U_P *achieves one-sided error when* $\alpha = 0$ *or* $\beta = 1$*.*

Moreover, the quantum circuit implementation of U_P *requires* $O(d^2)$ *uses of* U*,* $U^\dagger$*,* $\mathrm{C}_\Pi\mathrm{NOT}$*,* $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$*, and multi-controlled single-qubit gates. In addition, the description of the implementation can be computed in deterministic time* $\widetilde{O}(\varepsilon^{-1}\delta^{-9/2})$ *and space* $O(s(n))$*.*

Proof. Let the singular value decomposition of A be $A = W\Sigma V^\dagger = \sum_i \sigma_i |\tilde{\psi}_i\rangle\langle\psi_i|$. Note that U is a $(1,0,0)$-bitstring indexed encoding, with projections $\tilde{\Pi}$ and Π, of A. Let singular value threshold projectors $\Pi_{\geq\delta}$ and $\Pi'_{\geq\delta}$ be defined as $\Pi_{\geq\delta} := \Pi V\Sigma_{\geq\delta}V^\dagger\Pi$ and $\Pi'_{\geq\delta} := \Pi' W\sigma_{\geq\delta}W^\dagger\Pi'$, respectively, with similar definitions for $\Pi_{\leq\delta}$ and $\Pi'_{\leq\delta}$.

To discriminate whether the singular value corresponding to a given right singular vector of A exceeds a certain threshold, we need an *ε-singular value discriminator* U_P. Specifically, it suffices to construct a $(1,a,\tilde{\epsilon})$-bitstring indexed encoding U_P of A, associated with an appropriate odd polynomial P, that satisfies Equation (5.24). The parameters a and $\tilde{\epsilon}$ will be specified later.

$$\begin{aligned}\left\|\left(\langle 0|^{\otimes a}\otimes \Pi'_{\geq t+\delta}\right)U_P\left(|0\rangle^{\otimes a}\otimes\Pi_{\geq t+\delta}\right) - \textstyle\sum_{i\in\Lambda}|\tilde{\psi}_i\rangle\langle\psi_i|\right\| &\leq \varepsilon,\\ \left\|\left(\langle 0|^{\otimes a}\Pi'_{\leq t-\delta}\right)U_P\left(|0\rangle^{\otimes a}\otimes\Pi_{\leq t-\delta}\right) - 0\right\| &\leq \varepsilon.\end{aligned} \tag{5.24}$$

Here, the index set $\Lambda := \{i\colon \sigma_i \geq t+\delta\}$. Additionally, following the proof in [GSLW19, Theorem 20], Π' is defined as $\tilde{\Pi}$ if $\beta-\alpha \geq \sqrt{1-\alpha^2}-\sqrt{1-\beta^2}$, and as $I-\tilde{\Pi}$ otherwise.[25]

With the construction of this bitstring indexed encoding U_P, we can apply an ε-singular value discriminator with $\Pi' = \tilde{\Pi}$ by choosing $t := (\alpha+\beta)/2$ and $\delta := (\beta-\alpha)/2$. Next, we measure $|0\rangle\langle 0|^{\otimes a}\otimes\Pi'$: If the final state is in $\mathrm{Img}\left(|0\rangle\langle 0|^{\otimes a}\otimes\Pi'\right)$, there exists a singular value σ_i above α (resp., $\sqrt{1-\beta^2}$); otherwise, all singular value σ_i must be below β (resp., $\sqrt{1-\alpha^2}$). Furthermore, we can make the error one-sided when $\alpha = 0$ or $\beta = 1$, since a space-efficient QSVT associated with an *odd* polynomial always preserves 0 singular values (see Remark 5.13). It remains to implement an ε-singular value discriminator U_P for some odd polynomial P.

Implementing ε-singular value discriminator. We begin by considering the following odd function $Q(x)$ such that $Q(A) \approx U_P$ and $Q(A)$ satisfies Equation (5.24):

$$Q(x) := \tfrac{1}{2}\left[\left(1-\tfrac{\varepsilon}{2}\right)\cdot\mathrm{sgn}(x+t) + \left(1-\tfrac{\varepsilon}{2}\right)\cdot\mathrm{sgn}(x-t) + \varepsilon\cdot\mathrm{sgn}(x)\right].$$

Let $\epsilon := \frac{\varepsilon}{2(C_{\mathrm{sgn}}+36\tilde{C}_{\mathrm{sgn}}+37)}$. Using the space-efficient polynomial approximation $P^{\mathrm{sgn}}_{d'}$ of the sign function (Corollary 5.8 with $\epsilon_1 := 0$ and $\epsilon_2 := \epsilon$), we obtain the following

[25] By applying [GSLW18, Definition 12] (the full version of [GSLW19]) to $\Pi' := I-\tilde{\Pi}$, we know that $|\psi\rangle$ is a right singular vector of $\Pi' U\Pi$ with a singular value of at least $\sqrt{1-a^2}$ in the first case, or with a singular value of at most $\sqrt{1-b^2}$ in the second case. Additionally, in one-sided error scenarios, if $a=0$, then $b-a = b \geq 1-\sqrt{1-b^2} = \sqrt{1-a^2}-\sqrt{1-b^2}$; while if $b=1$, then $b-a = 1-a \leq \sqrt{1-a^2} = \sqrt{1-a^2}-\sqrt{1-b^2}$.

degree-d' polynomial P associated with some degree-d averaged Chebyshev truncation:

$$P(x) = \tfrac{1}{2}\left[\left(1-\tfrac{\varepsilon}{2}\right)\cdot P^{\mathrm{sgn}}_{d'}(x+t) + \left(1-\tfrac{\varepsilon}{2}\right)\cdot P^{\mathrm{sgn}}_{d'}(x-t) + \varepsilon\cdot P^{\mathrm{sgn}}_{d'}(x)\right].$$

Note that $P(x)$ is a convex combination of $P^{\mathrm{sgn}}_{d'}(x+t)$, $P^{\mathrm{sgn}}_{d'}(x-t)$, and $P^{\mathrm{sgn}}_{d'}(x)$, the constants $\tilde{C}_{\mathrm{sgn}}$ and $\hat{C}_{\mathrm{sgn}}$ specified in Corollary 5.8 remain the same. Hence, P is a polynomial of degree $d' = 2d-1 \le \tilde{C}_{\mathrm{sgn}}\frac{1}{\delta}\log\frac{1}{\epsilon}$, and the coefficient vector $\hat{\mathbf{c}}^{(P)}$ satisfies $\|\hat{\mathbf{c}}^{(P)}\|_1 \le \hat{C}_{\mathrm{sgn}}$.

Recall the notation $\|f\|_{\mathcal{I}}$ defined in Section 5.2.1, namely $\|f\|_{\mathcal{I}} \coloneqq \sup\{|f(x)| : x\in\mathcal{I}\}$. Let $D(x) \coloneqq \mathrm{sgn}(x) - P^{\mathrm{sgn}}_{d'}$, $\mathcal{I}_0 \coloneqq (0, t-\delta]$, and $\mathcal{I}_1 \coloneqq [t+\delta, 1]$. Following Corollary 5.8, we obtain:

$$\begin{aligned}
&\|P(x)-Q(x)\|_{[\delta-t,0)} = \|P(x)-Q(x)\|_{\mathcal{I}_0}\\
\le\ &\tfrac{2-\varepsilon}{4}\|D(x+t)\|_{\mathcal{I}_0} + \tfrac{2-\varepsilon}{4}\|D(x-t)\|_{\mathcal{I}_0} + \tfrac{\varepsilon}{2}\|D(x)\|_{\mathcal{I}_0} \le \left(1-\tfrac{\varepsilon}{2}\right)C_{\mathrm{sgn}}\epsilon + \tfrac{\varepsilon}{2},\\
&\|P(x)-Q(x)\|_{[-1,-t-\delta]} = \|P(x)-Q(x)\|_{\mathcal{I}_1}\\
\le\ &\tfrac{2-\varepsilon}{4}\|D(x+t)\|_{\mathcal{I}_1} + \tfrac{2-\varepsilon}{4}\|D(x-t)\|_{\mathcal{I}_1} + \tfrac{\varepsilon}{2}\|D(x)\|_{\mathcal{I}_1} \le \left(1-\tfrac{\varepsilon}{2}+\tfrac{\varepsilon}{2}\right)C_{\mathrm{sgn}}\epsilon.
\end{aligned} \tag{5.25}$$

Here, the equalities hold because both P and Q are odd functions.

Using Corollary 5.17 with P, we obtain a $(1, a, \tilde{\epsilon})$-bitstring indexed encoding U_P of A, with $a \coloneqq \lceil \log d'\rceil + 3$ and $\tilde{\epsilon} \coloneqq (36\hat{C}_{\mathrm{sgn}}+37)\epsilon$. Together with Equation (5.25), we obtain:

$$\begin{aligned}
&\left\|\left(\langle 0|^{\otimes a}\otimes \Pi'_{\ge t+\delta}\right)U_P\left(|0\rangle^{\otimes a}\otimes \Pi_{\ge t+\delta}\right) - \sum_{i\in\Lambda}|\tilde{\psi}_i\rangle\langle\psi_i|\right\|\\
\le\ &\left(1-\tfrac{\varepsilon}{2}+\tfrac{\varepsilon}{2}\right)C_{\mathrm{sgn}}\epsilon + (36\hat{C}_{\mathrm{sgn}}+37)\epsilon \le \varepsilon,\\
&\left\|\left(\langle 0|^{\otimes a}\Pi'_{\le t-\delta}\right)U_P\left(|0\rangle^{\otimes a}\otimes \Pi_{\le t-\delta}\right) - 0\right\|\\
\le\ &C_{\mathrm{sgn}}\epsilon + \tfrac{\varepsilon}{2} + (36\hat{C}_{\mathrm{sgn}}+37)\epsilon \le \varepsilon.
\end{aligned}$$

Hence, we conclude that our construction of U_P indeed satisfies Equation (5.24).

Finally, we analyze the complexity of this ε-singular value discriminator U_P. Following Corollary 5.17, the quantum circuit implementation of U_P requires $O(d^2)$ uses of U, $U^\dagger$, $\mathrm{C}_\Pi\mathrm{NOT}$, $\mathrm{C}_{\tilde{\Pi}}\mathrm{NOT}$, and multi-controlled single-qubit gates. Moreover, we can compute the description of the circuit implementation in deterministic time $\widetilde{O}(\epsilon^{-1}d^{9/2}) = \widetilde{O}(\varepsilon^{-1}\delta^{-9/2})$ and space $O(s(n))$, where $\delta = \max\{\beta-\alpha, \sqrt{1-\alpha^2}-\sqrt{1-\beta^2}\}/2$. □

Finally, we provide the proof of Theorem 5.19, which closely relates to Theorem 38 in [GSLW18] (the full version of [GSLW19]).

Proof of Theorem 5.19. It suffices to do error reduction by QSVT. Note that the probability that a $\mathsf{BQ_USPACE}[s(n)]$ circuit C_x accepts is $\Pr[C_x \text{ accepts}] = \||1\rangle\langle 1|_{\mathrm{out}}C_x|0^{k+m}\rangle\|_2^2 \ge a$ for *yes* instances, whereas $\Pr[C_x \text{ accepts }] = \||1\rangle\langle 1|_{\mathrm{out}}C_x|0^{k+m}\rangle\|_2^2 \le b$ for *no* instances. Then consider a $(1,0,0)$-bitstring indexed encoding $M_x \coloneqq \Pi_{\mathrm{out}}C_x\Pi_{\mathrm{in}}$ such that $\|M_x\| \ge \sqrt{a}$ for *yes* instances while $\|M_x\| \le \sqrt{b}$ for *no* instances, where $\Pi_{\mathrm{in}} \coloneqq |0\rangle\langle 0|^{\otimes k+m}$ and $\Pi_{\mathrm{out}} \coloneqq |1\rangle\langle 1|_{\mathrm{out}}\otimes I_{m+k-1}$. Since $\|M_x\| = \sigma_{\max}(M_x)$ where $\sigma_{\max}(M_x)$ is the largest singular value of M_x, it suffices to distinguish the largest singular value of M_x is either above $\sqrt{a}$ or below $\sqrt{b}$. By setting $\alpha \coloneqq \sqrt{a}$, $\beta \coloneqq \sqrt{b}$ and $\varepsilon \coloneqq 2^{-l(n)}$, this task is a direct corollary of Lemma 5.21. □

Chapter 6

Space-bounded quantum state testing and its applications

6.1 Introduction

Previous studies on complete characterizations of space-bounded quantum computation [Wat99, Wat03, vMW12] have primarily focused on well-conditioned versions of standard linear algebraic problems [TS13, FL18, FR21] and have been limited to the two-sided error scenario. In contrast, we propose a novel family of complete problems that not only characterize the *one-sided error scenario* (*and extend to the two-sided scenario*) but also arise from a quantum property testing perspective. Our new complete problems are arguably more natural and simpler, driven by recent intriguing challenges of verifying the intended functionality of quantum devices.

In this chapter, we investigate quantum state testing problems where quantum states ρ_0 and ρ_1 are preparable by *computationally constrained resources*, specifically state-preparation circuits (viewed as the "source code" of devices) that are (*log*)*space-bounded*. Our main result conveys a conceptual message that testing quantum states prepared in bounded space is (computationally) as *easy* as preparing these states in a space-bounded manner. Consequently, we can introduce the first family of natural $\mathsf{coRQ_UL}$-complete promise problems since Watrous [Wat01] introduced unitary RQL and coRQL (known as $\mathsf{RQ_UL}$ and $\mathsf{coRQ_UL}$, respectively) in 2001, as well as a new family of natural BQL-complete promise problems.

6.1.1 Main results

We will commence by providing definitions for time- and space-bounded quantum circuits. We say that a quantum circuit Q is (*poly*)*time-bounded* if Q is polynomial-size and acts on $\mathrm{poly}(n)$ qubits. Likewise, we say that a quantum circuit Q is (*log*)*space-bounded* if Q is polynomial-size and acts on $O(\log n)$ qubits. It is worthwhile to note that primary complexity classes, e.g., BQL, $\mathsf{coRQ_UL}$, and BPL, mentioned in this paper correspond to *promise problems*.

Complete characterizations of quantum logspace from state testing. While prior works [TS13, FL18, FR21] on BQL-complete problems have mainly focused on well-

conditioned versions of standard linear algebraic problems (in DET^*), our work takes a different perspective by exploring quantum property testing. Specifically, we investigate the problem of *space-bounded quantum state testing*, which aims to test the closeness between two quantum states that are preparable by (log)space-bounded quantum circuits (devices), with access to the corresponding "source code" of these devices.

We begin by considering a computational problem that serves as a "white-box" space-bounded counterpart of *quantum state certification* [BOW19], equivalent to quantum state testing with one-sided error. Our first main theorem (Theorem 6.1) demonstrates the *first* family of natural $\mathsf{coRQ_UL}$-complete problems in the context of space-bounded quantum state certification with respect to the trace distance (T) and the squared Hilbert-Schmidt distance (HS^2).

Theorem 6.1 (Informal of Theorem 6.11)**.** *The following space-bounded quantum state certification problems are* $\mathsf{coRQ_UL}$*-complete: for any* $\alpha(n) \geq 1/\mathrm{poly}(n)$*, decide whether*

(1) $\overline{\textsc{CertQSD}}_{\log}$: $\rho_0 = \rho_1$ *or* $\mathrm{T}(\rho_0, \rho_1) \geq \alpha(n)$*;*

(2) $\overline{\textsc{CertQHS}}_{\log}$: $\rho_0 = \rho_1$ *or* $\mathrm{HS}^2(\rho_0, \rho_1) \geq \alpha(n)$*.*

By extending the error requirement from one-sided to two-sided, we broaden the scope of space-bounded quantum state testing to include two more distance-like measures: the quantum entropy difference, denoted by $\mathrm{S}(\rho_0) - \mathrm{S}(\rho_1)$, and the quantum Jensen-Shannon divergence ($\mathrm{QJS}_{\mathrm{bit}}$). As a result, we establish our second main theorem, introducing a new family of natural BQL-complete problems:[1]

Theorem 6.2 (Informal of Theorem 6.12)**.** *The following space-bounded quantum state testing problems are* BQL*-complete: for any* $\alpha(n)$ *and* $\beta(n)$ *such that* $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$*, or for any* $g(n) \geq 1/\mathrm{poly}(n)$*, decide whether*

(1) $\textsc{GapQSD}_{\log}$: $\mathrm{T}(\rho_0, \rho_1) \geq \alpha(n)$ *or* $\mathrm{T}(\rho_0, \rho_1) \leq \beta(n)$*;*

(2) $\textsc{GapQED}_{\log}$: $\mathrm{S}(\rho_0) - \mathrm{S}(\rho_1) \geq g(n)$ *or* $\mathrm{S}(\rho_1) - \mathrm{S}(\rho_0) \geq g(n)$*;*

(3) $\textsc{GapQJS}_{\log}$: $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \geq \alpha(n)$ *or* $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \leq \beta(n)$*;*

(4) $\textsc{GapQHS}_{\log}$: $\mathrm{HS}^2(\rho_0, \rho_1) \geq \alpha(n)$ *or* $\mathrm{HS}^2(\rho_0, \rho_1) \leq \beta(n)$*.*

Algorithmic Holevo-Helstrom measurement and its implication. The celebrated Holevo-Helstrom bound [Hol73b, Hel69] states that the maximum success probability to discriminate quantum states ρ_0 and ρ_1 is given by $\frac{1}{2} + \frac{1}{2}\mathrm{T}(\rho_0, \rho_1)$. There is then an optimal two-outcome measurement $\{\Pi_0, \Pi_1\}$, referred to as the Holevo-Helstrom measurement, such that $\mathrm{T}(\rho_0, \rho_1) = \mathrm{Tr}(\Pi_0\rho_0) - \mathrm{Tr}(\Pi_0\rho_1)$. Interestingly, by leveraging the BQL containment in Theorem 6.2(1), we can obtain an (approximately) explicit implementation of the Holevo-Helstrom measurement, called *algorithmic Holevo-Helstrom measurement*:

Theorem 6.3 (Informal of Theorem 6.26)**.** *For quantum states* ρ_0 *and* ρ_1 *specified in* $\textsc{GapQSD}$ *such that their purification can be prepared by* n*-qubit polynomial-size quantum*

[1] It is noteworthy that our algorithm for $\textsc{GapQSD}_{\log}$ in Theorem 6.2(1) exhibits a *polynomial advantage* in space over the best known classical algorithms [Wat02]. Watrous implicitly showed in [Wat02, Proposition 21] that $\textsc{GapQSD}_{\log}$ is contained in the class NC, which corresponds to (classical) polylogarithmic space.

circuits Q_0 and Q_1, we can approximately implement the Holevo-Helstrom measurement $\{\Pi_0, \Pi_1\}$ in quantum single-exponential time and linear space with additive error 2^{-n}.

As an implication, we provide a slightly improved upper bound for the class QSZK by inspecting the "distance test" in [Wat02] since GapQSD is QSZK-hard:

Theorem 6.4 (Informal of Theorem 6.27)**.** GapQSD *is in* QIP(2) *with a quantum single-exponential-time and linear-space honest prover.*

The best known upper bound for the class QSZK is QIP(2) [Wat02, Wat09b, JUW09], where the computational power of the honest prover is *unbounded*. It is noteworthy that Theorem 6.4 also applies to GapQSD instances that are not known to be in QSZK.[2]

Space-bounded unitary quantum statistical zero-knowledge. We also introduce (*honest-verifier*) *space-bounded unitary quantum statistical zero-knowledge*, denoted as $\mathsf{QSZK_UL_{HV}}$. This term refers to a specific form of space-bounded quantum proofs, as introduced in [LLNW24], that possess statistical zero-knowledge against an honest verifier. Specifically, a space-bounded unitary quantum interactive proof system possesses this zero-knowledge property if there exists a quantum logspace simulator that approximates the snapshot states ("the verifier's view") on the registers M and W after each turn of this proof system, where each state approximation must be very close ("indistinguishable") to the corresponding snapshot state with respect to the trace distance.

Our definition $\mathsf{QSZK_UL_{HV}}$ serves as a space-bounded variant of honest-verifier (unitary) quantum statistical zero-knowledge, denoted by $\mathsf{QSZK_{HV}}$, as introduced in [Wat02]. Our fifth theorem establishes that the statistical zero-knowledge property completely negates the computational advantage typically gained through the interaction:

Theorem 6.5 (Informal of Theorem 6.29)**.** $\mathsf{QSZK_UL} = \mathsf{QSZK_UL_{HV}} = \mathsf{BQL}$.

In addition to $\mathsf{QSZK_UL_{HV}}$, we can define $\mathsf{QSZK_UL}$ in line with [Wat09b], particularly considering space-bounded unitary quantum statistical zero-knowledge against *any verifier* (rather than an honest verifier). Following this definition, $\mathsf{BQL} \subseteq \mathsf{QSZK_UL} \subseteq \mathsf{QSZK_UL_{HV}}$. Interestingly, Theorem 6.5 serves as a direct space-bounded counterpart to $\mathsf{QSZK} = \mathsf{QSZK_{HV}}$ [Wat09b].

The intuition behind Theorem 6.5 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, as established in Chapter 5, 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].

Connections to space-efficient quantum singular value transformation. Proving our main theorems mentioned above poses a significant challenge: establishing the

[2] See Section 1.1.1 for classical scenarios and Chapter 7 for recent advancements in quantum scenarios.

containment in the relevant class (BQL or $\mathsf{coRQ_UL}$), which is also the difficult direction for showing the known family of BQL-complete problems [TS13, FL18, FR21].

Proving the containment in the one-sided error scenario is not an effortless task: such a task is not only already relatively complicated for $\overline{\text{CertQHS}}_{\log}$, but also requires to develop novel techniques for $\overline{\text{CertQSD}}_{\log}$. On the other hand, in two-sided error scenarios, showing containment is straightforward for $\text{GapQHS}_{\log}$. However, demonstrating this for other problems, such as $\text{GapQSD}_{\log}$, $\text{GapQED}_{\log}$, and $\text{GapQJS}_{\log}$, requires sophisticated techniques, notably the space-efficient quantum singular value transformation introduced in Chapter 5. This is because their time-bounded counterparts appear significantly more challenging than merely preparing the states.

6.1.2 Time-bounded and space-bounded testing: A comparison

We summarize prior works and our main results for time-bounded and space-bounded distribution and state testing with respect to ℓ_1 norm, entropy difference, and ℓ_2 norm in Table 6.1. For a brief overview of time-bounded testing, see Section 1.1.

Interestingly, the sample complexity of testing the closeness of quantum states (resp., distributions) depends on the choice of distance-like measures,[3] including the one-sided error counterpart known as *quantum state certification*[BOW19]. In particular, for distance-like measures such as the ℓ_1 norm, called total variation distance in the case of distributions [CDVV14] and trace distance in the case of states [BOW19], as well as classical entropy difference [JVHW15, WY16] and its quantum analog [AISW20, OW21], the sample complexity of distribution and state testing is polynomial in the dimension N. However, for distance-like measures such as the ℓ_2 norm, called Euclidean distance in the case of distributions [CDVV14] and Hilbert-Schmidt distance in the case of states [BOW19], the sample complexity is *independent* of dimension N.

	ℓ_1 norm	ℓ_2 norm	Entropy
Classical Time-bounded	SZK-complete[4] [SV03, GSV98]	BPP-complete Folklore	SZK-complete [GV99, GSV98]
Quantum Time-bounded	QSZK-complete[5] [Wat02, Wat09b]	BQP-complete [BCWdW01, RASW23]	QSZK-complete [BASTS10, Wat02, Wat09b]
Quantum Space-bounded	BQL-complete Theorem 6.2(1)	BQL-complete [BCWdW01] and Theorem 6.2(4)	BQL-complete Theorem 6.2(2)

Table 6.1: Time- and space-bounded distribution or state testing.

As depicted in Table 6.1, this phenomenon that the required sample complexity for distribution and state testing, with polynomial precision and exponential dimension, depends on the choice of distance-like measure has reflections on time-bounded state testing:

- For the ℓ_1 norm and entropy difference, the time-bounded scenario is *seemingly*

[3] It is noteworthy that the quantum entropy difference is not a distance.

[4] The SZK containment of $\text{SD}[\alpha, \beta]$ applies only in the regime $\alpha^2(n) - \beta(n) \geq 1/\text{poly}(n)$, rather than the natural parameter regime $\alpha(n) - \beta(n) \geq 1/\text{poly}(n)$. For further details, see Section 1.1.1.

[5] The QSZK containment of $\text{QSD}[\alpha, \beta]$ holds only in the regime $\alpha^2(n) - \sqrt{2 \ln 2}\beta(n) \geq 1/\text{poly}(n)$. However, the differences between classical and quantum distances make it challenging to push the bound further. For more details, see Chapter 7.

much harder than preparing states or distributions, given that the inclusions $\mathsf{QSZK} \subseteq \mathsf{BQP}$ and $\mathsf{SZK} \subseteq \mathsf{BPP}$ are unlikely.

- For the ℓ_2 norm, the time-bounded scenario is computationally *as easy as* preparing states or distributions.

However, interestingly, a similar phenomenon *does not appear* for space-bounded quantum state testing. Although no direct classical counterpart has been investigated before in a complexity-theoretic fashion, namely space-bounded distribution testing, there is another closely related model (a version of streaming distribution testing) that does not demonstrate an analogous phenomenon either, as discussed in Section 3.4.

Among the prior works on streaming distribution testing, particularly entropy estimation, the key takeaway is that the space complexity of the corresponding computational problem is $O(\log(N/\epsilon))$. This observation leads to a conjecture that the computational hardness of space-bounded distribution and state testing is *independent* of the choice of commonplace distance-like measures. Our results, in turn, provide a positive answer for space-bounded quantum state testing.

6.1.3 Proof overview: A general framework for quantum state testing

Our framework enables space-bounded quantum state testing, specifically for proving Theorem 6.1 and Theorem 6.2, and is based on the one-bit precision phase estimation [Kit95], also known as the *Hadamard test*[AJL09]. Prior works [TS13, FL18] have employed (one-bit precision) phase estimation in space-bounded quantum computation.

To address quantum state testing problems, we reduce them to estimating $\mathrm{Tr}(P_{d'}(A)\rho)$, where ρ is a (mixed) quantum state prepared by a quantum circuit Q_ρ, A is an Hermitian operator block-encoded in a unitary operator U_A, and $P_{d'}$ is a space-efficiently computable degree-d' polynomial obtained from some degree-d averaged Chebyshev truncation with $d' = 2d-1$. Similar approaches have been applied in *time-bounded* quantum state testing, including fidelity estimation [GP22] and subsequently trace distance estimation [WZ24a].

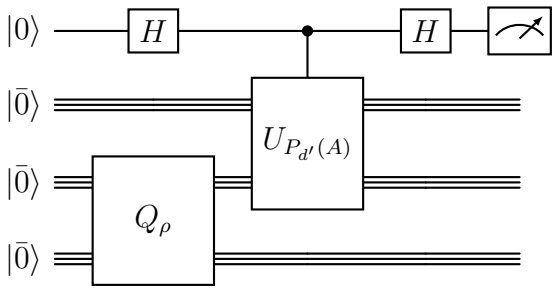

Figure 6.1: General framework for quantum state testing $\mathcal{T}(Q_\rho, U_A, P_{d'})$.

To implement a unitary operator $U_{P_{d'}(A)}$ that (approximately) block-encodes $P_{d'}(A)$ in a space-efficient manner, we require $P_{d'}$ to meet the conditions specified in Theorem 5.2. As illustrated in Figure 6.1, we denote the quantum circuit as $\mathcal{T}(Q_\rho, U_A, P_{d'})$, where we exclude the precision for simplicity. The measurement outcome of $\mathcal{T}(Q_\rho, U_A, P_{d'})$ will be 0 with a probability close to $\frac{1}{2}\Big(1 + \mathrm{Tr}(P_{d'}(A)\rho)\Big)$. This property allows us to estimate

$\mathrm{Tr}(P_{d'}(A)\rho)$ within an additive error ϵ using $O(1/\epsilon^2)$ sequential repetitions, resulting in a BQL containment.

As an example of the application, $\mathcal{T}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P^{\mathrm{sgn}}_{d'})$ is utilized in GapQSD, where $U_{\frac{\rho_0-\rho_1}{2}}$ is a block-encoding of $\frac{\rho_0-\rho_1}{2}$, and $P^{\mathrm{sgn}}_{d'}$ is a space-efficient polynomial approximation of the sign function. Notably, this algorithm can be viewed as a two-outcome measurement $\{\hat{\Pi}_0, \hat{\Pi}_1\}$ where $\hat{\Pi}_0 = \frac{1}{2}I + \frac{1}{2}P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0-\rho_1}{2}\right)$, which is essentially the algorithmic Holevo-Helstrom measurement in Theorem 6.3. Similarly, $\mathcal{T}(Q_i, U_{\rho_i}, P^{\mathrm{ln}}_{d'})$ is utilized in GapQED, where U_{ρ_i} is a block-encoding of ρ_i for $i \in \{0,1\}$, and $P^{\mathrm{ln}}_{d'}$ is a space-efficient polynomial approximation of the normalized logarithmic function. Both $P^{\mathrm{sgn}}_{d'}$ and $P^{\mathrm{ln}}_{d'}$ can be obtained by employing Theorem 5.2.

Making the error one-sided. The main challenge is constructing a unitary U of interest, such as $\mathcal{T}(Q_\rho, U_A, P_{d'})$, that accepts with a *certain fixed* probability p for *yes* instances ($\rho_0 = \rho_1$), while having a probability that polynomially deviates from p for *no* instances. As an example, we consider $\overline{\mathrm{CertQHS}}_{\log}$ and express $\mathrm{HS}^2(\rho_0, \rho_1)$ as a linear combination of $\mathrm{Tr}(\rho_0^2)$, $\mathrm{Tr}(\rho_1^2)$, and $\mathrm{Tr}(\rho_0\rho_1)$. We can then design a unitary quantum algorithm that satisfies the requirement for *yes* instances based on the SWAP test [BCWdW01], and consequently, we can achieve perfect completeness by applying the exact amplitude amplification [BBHT98, BHMT02]. The analysis demonstrates that the acceptance probability polynomially deviates from 1 for *no* instances. By applying error reduction for $\mathsf{coRQ_UL}$, the resulting algorithm is indeed in $\mathsf{coRQ_UL}$.

Moving on to $\overline{\mathrm{CertQSD}}_{\log}$, we consider the quantum circuit $U_i = \mathcal{T}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P^{\mathrm{sgn}}_{d'})$ for $i \in \{0,1\}$. Since our space-efficient QSVT *preserves parity*, specifically, the approximation polynomial $P^{\mathrm{sgn}}_{d'}$ satisfies $P^{\mathrm{sgn}}_{d'}(0) = 0$,[6] the requirement for *yes* instances is satisfied. Then we can similarly achieve the $\mathsf{coRQ_UL}$ containment of $\overline{\mathrm{CertQSD}}_{\log}$.

6.1.4 Proof overview: The equivalence of $\mathsf{QSZK_UL}$ and BQL

We demonstrate Theorem 6.5 by introducing a $\mathsf{QSZK_UL_{HV}}$-complete problem:

Theorem 6.6 (Informal of Theorem 6.30)**.** IndivProdQSD *is* $\mathsf{QSZK_UL_{HV}}$*-complete.*

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

$$\mathrm{T}(\sigma_1 \otimes \cdots \otimes \sigma_k, \sigma'_1 \otimes \cdots \otimes \sigma'_k) \geq \alpha. \tag{6.1}$$

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

$$\forall j \in [k], \quad \mathrm{T}\left(\sigma_j, \sigma'_j\right) \leq \delta. \tag{6.2}$$

[6] Let f be any odd function such that space-efficient QSVT associated with f can be implemented by Theorem 5.2. It follows that the corresponding approximation polynomial $P^{(f)}_{d'}$ is also odd. See Remark 5.13.

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

$\overline{\text{IndivProdQSD}}$ is $\mathsf{QSZK}_{\mathrm{U}}\mathsf{L}_{\mathrm{HV}}$-hard. The hardness proof draws inspiration from [Wat02, Section 5]. Consider a $\mathsf{QSZK}_{\mathrm{U}}\mathsf{L}_{\mathrm{HV}}[2k, c, s]$ proof system, denoted by $\mathcal{B}$. The logspace-bounded simulator $S_{\mathcal{B}}$ produces good state approximations ξ_j and ξ'_j of the snapshot states $\rho_{\mathtt{M}_j\mathtt{W}_j}$ and $\rho_{\mathtt{M}'_j\mathtt{W}_j}$ after the $(2j-1)$-st turn and the $(2j)$-th turn in $\mathcal{B}$, respectively, satisfying $\xi_j \approx_\delta \rho_{\mathtt{M}_j\mathtt{W}_j}$ and $\xi'_j \approx_\delta \rho_{\mathtt{M}'_j\mathtt{W}_j}$, where $\delta_{\mathcal{B}}(n)$ is a negligible function.

Since the verifier's actions are unitary and the verifier is honest, it suffices to check that the prover's actions do not change the verifier's private register, corresponding to the type (ii) constraints in the SDP formulation for QIPL proof systems, as presented in [LLNW24, Equation 1.1]. For convenience, let $\sigma_j := \mathrm{Tr}_{\mathtt{M}_j}(\xi_j)$ and $\sigma'_j := \mathrm{Tr}_{\mathtt{M}'_j}(\xi'_j)$ for $j \in [k]$. We then establish $\mathsf{QSZKL}_{\mathrm{HV}}$ hardness as follows:

- For *yes* instances, the message-wise closeness condition of the simulator $S_{\mathcal{B}}$ implies Equation (6.2) 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 (6.1) with $\alpha(n) := (\sqrt{c} - \sqrt{s})^2/4(l-1)$.

IndivProdQSD $\in$ BQL. Since it holds that BQL = QMAL [FKL+16, FR21], it suffices to establish that IndivProdQSD $\in$ QMAL. By applying an averaging argument in combination with Equation (6.1), we derive the following:

$$\sum_{j\in[k]} \mathrm{T}\left(\sigma_j, \sigma'_j\right) \geq \mathrm{T}(\sigma_1\otimes\cdots\otimes\sigma_k, \sigma'_1\otimes\cdots\otimes\sigma'_k) \geq \alpha \quad \Rightarrow \quad \exists j\in[k] \text{ s.t. } \mathrm{T}\left(\sigma_j, \sigma'_j\right) \geq \frac{\alpha}{k}. \tag{6.3}$$

The QMAL protocol works as follows:

(1) The prover sends an index $i \in [k]$ to the verifier;

(2) The verifier accepts if $\mathrm{Tr}(\sigma_i, \sigma'_i) \geq \alpha/k$ and rejects if $\mathrm{Tr}(\sigma_i, \sigma'_i) \leq \delta$, in accordance with Equation (6.3) and Equation (6.2).

The resulting promise problem to be verified is precisely an instance of $\text{GapQSD}_{\log}$, which is known to be BQL-complete, as stated in Theorem 6.2(1).

6.2 Space-bounded quantum state testing

We begin by defining the quantum state testing problem in a space-bounded manner:

Definition 6.7 (Space-bounded Quantum State Testing)**.** *Given polynomial-size quantum circuits (devices) Q_0 and Q_1 that act on $O(\log n)$ qubits and have a succinct description (the "source code" of devices), with $r(n)$ specified output qubits, where $r(n)$ is a deterministic logspace computable function such that $0 < r(n) \leq O(\log(n))$. For clarity, n represents the (total) number of gates in Q_0 and Q_1.*[7] *Let ρ_i denote the mixed state*

[7] It is noteworthy that in the time-bounded scenario, the input length of circuits, the size of circuit

obtained by running Q_i on the all-zero state $|\bar{0}\rangle$ and tracing out the non-output qubits.

We define a space-bounded quantum state testing problem, with respect to a specified distance-like measure, to decide whether ρ_0 and ρ_1 are easily distinguished or almost indistinguishable. Likewise, we also define a space-bounded quantum state certification problem to decide whether ρ_0 and ρ_1 are easily distinguished or exactly indistinguishable.

We remark that space-bounded state certification, defined in Definition 6.7, represents a "white-box" space-bounded counterpart of quantum state certification [BOW19].

Remark 6.8 (Lifting to exponential-size instances by succinct encodings). For $s(n)$ space-uniform quantum circuits Q_0 and Q_1 acting on $O(s(n))$ qubits, if these circuits admit a succinct encoding,[8] namely there is a deterministic $O(s(n))$-space Turing machine with time complexity $\mathrm{poly}(s(n))$ can uniformly generate the corresponding gate sequences, then Definition 6.7 can be extended to any $s(n)$ satisfying $\Omega(\log n) \leq s(n) \leq \mathrm{poly}(n)$.[9]

Next, we define space-bounded quantum state testing problems, based on Definition 6.7, with respect to four commonplace distance-like measures.

Definition 6.9 (Space-bounded Quantum State Distinguishability Problem, $\textsc{GapQSD}_{\log}$)**.** *Consider deterministic logspace computable functions $\alpha(n)$ and $\beta(n)$, satisfying $0 \leq \beta(n) < \alpha(n) \leq 1$ and $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$. Then the promise is that one of the following holds:*

- 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 $\mathrm{T}(\rho_0, \rho_1) \leq \beta(n)$.*

Moreover, we also define the certification counterpart of $\textsc{GapQSD}_{\log}$, referred to as $\textsc{CertQSD}_{\log}$, given that $\beta = 0$. Specifically, $\textsc{CertQSD}_{\log}[\alpha(n)] \coloneqq \textsc{GapQSD}_{\log}[\alpha(n), 0]$.

In a similar manner to Definition 6.9, we can define $\textsc{GapQJS}_{\log}$ and $\textsc{GapQHS}_{\log}$, also the certification version $\overline{\textsc{CertQHS}}_{\log}$ by replacing the distance-like measure accordingly:

- $\textsc{GapQJS}_{\log}[\alpha(n), \beta(n)]$: Decide whether $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \geq \alpha(n)$ or $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \leq \beta(n)$;
- $\textsc{GapQHS}_{\log}[\alpha(n), \beta(n)]$: Decide whether $\mathrm{HS}^2(\rho_0, \rho_1) \geq \alpha(n)$ or $\mathrm{HS}^2(\rho_0, \rho_1) \leq \beta(n)$.

Furthermore, we adopt the notation $\overline{\textsc{CertQSD}}_{\log}$ to represent the *complement* of $\textsc{CertQSD}_{\log}$ with respect to the chosen parameter $\alpha(n)$, and so does $\overline{\textsc{CertQHS}}_{\log}$.

Definition 6.10 (Space-bounded Quantum Entropy Difference Problem, $\textsc{GapQED}_{\log}$)**.** *Consider a deterministic logspace computable function $g : \mathbb{N} \to \mathbb{R}^+$, satisfying $g(n) \geq 1/\mathrm{poly}(n)$. Then the promise is that one of the following cases holds:*

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

descriptions, and the number of gates in circuits are polynomially equivalent. However, in the space-bounded scenario, only the last two quantities are polynomially equivalent, and their dependence on the first quantity may be exponential.

[8] For instance, the construction in [FL18, Remark 11], or [PY86, BLT92] in general.

[9] It is noteworthy that Definition 6.7 (mostly) coincides with the case of $s(n) = \Theta(\log n)$ and directly takes the corresponding gate sequence of Q_0 and Q_1 as an input.

New complete problems for space-bounded quantum computation. We now present the main theorems in this section and the chapter. Theorem 6.11 establishes the first family of natural $\mathsf{coRQ_UL}$-complete problems. By relaxing the error requirement from one-sided to two-sided, Theorem 6.12 identifies a new family of natural BQL-complete problems on space-bounded quantum state testing. It is noteworthy that Theorems 6.11 and 6.12 also have natural exponential-size up-scaling counterparts.[10]

Theorem 6.11. *The computational hardness of the following space-bounded quantum state certification problems, for any deterministic logspace computable $\alpha(n) \geq 1/\mathrm{poly}(n)$, is as follows:*

(1) $\overline{\textsc{CertQSD}}_{\log}[\alpha(n)]$ *is* $\mathsf{coRQ_UL}$*-complete;*

(2) $\overline{\textsc{CertQHS}}_{\log}[\alpha(n)]$ *is* $\mathsf{coRQ_UL}$*-complete.*

Theorem 6.12. *The computational hardness of the following space-bounded quantum state testing problems, where $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$ or $g(n) \geq 1/\mathrm{poly}(n)$ as well as $\alpha(n)$, $\beta(n)$, $g(n)$ can be computed in deterministic logspace, is as follows:*

(1) $\textsc{GapQSD}_{\log}[\alpha(n), \beta(n)]$ *is* BQL*-complete;*

(2) $\textsc{GapQED}_{\log}[g(n)]$ *is* BQL*-complete;*

(3) $\textsc{GapQJS}_{\log}[\alpha(n), \beta(n)]$ *is* BQL*-complete;*

(4) $\textsc{GapQHS}_{\log}[\alpha(n), \beta(n)]$ *is* BQL*-complete.*

To establish Theorems 6.11 and 6.12, we introduce a general framework for space-bounded quantum state testing in Section 6.2.1. Interestingly, BQL and $\mathsf{coRQ_UL}$ containments for these problems with respect to different distance-like measures, utilizing our general framework, correspond to approximate implementations of distinct two-outcome measurements. The main technical challenges then mostly involve *parameter trade-offs* when using our space-efficient QSVT to construct these approximate measurement implementations. We summarize this correspondence in Table 6.2 and the associated subsection, which provides the detailed proof.

Distance-like measure	State testing	State certification	Two-outcome measurement Π_b for $b \in \{0,1\}$
Trace distance	$\textsc{GapQSD}_{\log}$ Section 6.2.2	$\overline{\textsc{CertQSD}}_{\log}$ Section 6.2.4	$\frac{I}{2} + \frac{(-1)^b}{2}\mathrm{sgn}^{(\mathrm{SV})}\left(\frac{\rho_0-\rho_1}{2}\right)$ for ρ_0 and ρ_1
Quantum entropy difference Quantum JS divergence	$\textsc{GapQED}_{\log}$ $\textsc{GapQJS}_{\log}$ Section 6.2.3	None	$\frac{I}{2} - \frac{(-1)^b}{2} \cdot \frac{\ln(\rho_i)}{2\ln(2/\beta)}$ for ρ_i where $i \in \{0,1\}$ and $\lambda(\rho_i) \in [-\beta, \beta]$
Hilbert-Schmidt distance	$\textsc{GapQHS}_{\log}$ Section 6.2.4	$\overline{\textsc{CertQHS}}_{\log}$ Section 6.2.4	$\frac{I}{2} + \frac{(-1)^b}{2}\mathrm{SWAP}$ for $\rho_0 \otimes \rho_1$

Table 6.2: The correspondence between the distance-like measures and measurements.

[10] We can naturally extend Theorems 6.11 and 6.12 to their exponential-size up-scaling counterparts with $2^{-O(s(n))}$-precision, employing the extended version of Definition 6.7 outlined in Remark 6.8, thus achieving the complete characterizations for $\mathsf{coRQ_USPACE}[s(n)]$ and $\mathsf{BQPSPACE}[s(n)]$, respectively.

Notably, the measurement corresponding to the trace distance in Table 6.2 can be viewed as an *algorithmic Holevo-Helstrom measurement*, as discussed further in Section 6.3. Lastly, the corresponding hardness proof for all these problems is provided in Section 6.2.5.

6.2.1 Space-bounded quantum state testing: a general framework

In this subsection, we introduce a general framework for quantum state testing that utilizes a quantum tester $\mathcal{T}$. Specifically, the space-efficient tester $\mathcal{T}$ succeeds (outputting the value "0") with probability x, which is linearly dependent on some quantity closely related to the distance-like measure of interest. Consequently, we can obtain an additive-error estimation $\widetilde{x}$ of x with high probability through sequential repetition (Lemma 2.13).

To construct $\mathcal{T}$, we combine the one-bit precision phase estimation [Kit95], commonly known as the Hadamard test [AJL09], for block-encodings (see Lemma 2.19), with our space-efficient quantum singular value transformation (QSVT) technique, which we describe in Chapter 5.

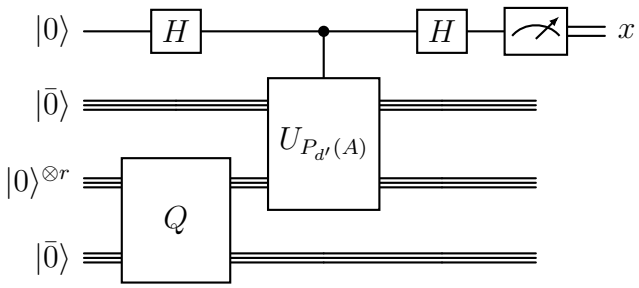

Figure 6.2: Quantum tester $\mathcal{T}(Q, U_A, P_{d'}, \epsilon)$: the circuit implementation.

Constructing a space-efficient quantum tester. We now provide a formal definition and the detailed construction of the quantum tester $\mathcal{T}$. The quantum circuit shown in Figure 6.2 defines the quantum tester $\mathcal{T}(Q, U_A, P_{d'}, \epsilon)$ using the following parameters with $s(n) = \Theta(\log n)$:

- A $s(n)$-qubit quantum circuit Q prepares the purification of an $r(n)$-qubit quantum state ρ where ρ is the quantum state of interest;
- U_A is a $(1, s(n) - r(n), 0)$-block-encoding of an $r(n)$-qubit Hermitian operator A where A relates to the quantum states of interest and $r(n) \leq s(n)$;
- $P_{d'}$ is the space-efficiently computable degree-d' polynomial defined by Equation (2.3) obtained from some degree-d averaged Chebyshev truncation $P_{d'}$ with $d' = 2d - 1$, where $P_{d'}(x) = \hat{c}_0/2 + \sum_{k=1}^{d'} \hat{c}_k T_k(x) \in \mathbb{R}[x]$ and T_k is the k-th Chebyshev polynomial, with $d' \leq 2^{O(s(n))}$, such that the coefficients $\hat{\mathbf{c}} := (\hat{c}_0, \cdots, \hat{c}_{d'})$ can be computed in bounded-error randomized space $O(s(n))$;
- ϵ is the precision parameter used in the estimation of x, with $\epsilon \geq 2^{-O(s(n))}$.

Leveraging our space-efficient QSVT, we assume that there is an $(\alpha, *, *)$-block-encoding of $P_{d'}(A)$, which is an approximate implementation of $U_{P_{d'}(A)}$ in Figure 6.2. Now, we can define the corresponding estimation procedure, $\hat{\mathcal{T}}(Q, U_A, P_{d'}, \epsilon, \epsilon_H, \delta)$, namely a

quantum algorithm that computes an additive-error estimate $\alpha\widetilde{x}$ of $\mathrm{Re}(\mathrm{Tr}(P_{d'}(A)\rho))$ from the tester $\mathcal{T}(Q, U_A, P_{d'}, \epsilon)$. Technically speaking, $\hat{\mathcal{T}}$ outputs $\widetilde{x}$ such that

$$|\alpha\widetilde{x} - \mathrm{Re}(\mathrm{Tr}(P_{d'}(A)\rho))| \leq \|\hat{\mathbf{c}}\|_1\epsilon + \alpha\epsilon_H$$

with probability at least $1-\delta$. Now we will demonstrate that both the tester $\mathcal{T}$ and the corresponding estimation procedure $\hat{\mathcal{T}}$ are space-efficient:

Lemma 6.13 (Quantum tester $\mathcal{T}$ and estimation procedure $\hat{\mathcal{T}}$ are space-efficient)**.** *Assume that there is an $(\alpha, *, *)$-block-encoding of $P_{d'}(A)$ that approximately implements $U_{P_{d'}}(A)$, where α is either $\|\hat{\mathbf{c}}\|_1$ or 1 based on conditions of $P_{d'}$ and A. The quantum tester $\mathcal{T}(Q, U_A, P_{d'}, \epsilon)$, as specified in Figure 6.2, accepts (outputting the value "0") with probability $\frac{1}{2}\Big(1+\frac{1}{\alpha}\mathrm{Re}(\mathrm{Tr}(P_{d'}(A)\rho))\Big) \pm \frac{1}{2\alpha}\|\hat{\mathbf{c}}\|_1\epsilon$. In addition, $\hat{\mathcal{T}}(Q, U_A, P_{d'}, \epsilon, \epsilon_H, \delta)$ outputs $\widetilde{x}$ such that, with probability at least $1-\delta$, it holds that*

$$\|\alpha\widetilde{x} - \mathrm{Re}(\mathrm{Tr}(P_{d'}(A)\rho))\| \leq \|\hat{\mathbf{c}}\|_1\epsilon + \alpha\epsilon_H.$$

Moreover, we can compute the quantum circuit description of $\mathcal{T}$ in deterministic space $O(s + \log(1/\epsilon))$ given the coefficient vector $\hat{\mathbf{c}}$ of $P_{d'}$. Furthermore, we can implement the corresponding estimation procedure $\hat{\mathcal{T}}$ in bounded-error quantum space $O(s + \log(1/\epsilon) + \log(1/\epsilon_H) + \log\log(1/\delta))$.

Proof. Note that U_A is a $(1, a, 0)$-block-encoding of A, where $a = s - r$.

We first consider the case where $\alpha = \|\hat{\mathbf{c}}\|_1$, which holds for any $P_{d'}$ and A. By Theorem 5.12 with $\epsilon_1 := 0$ and $\epsilon_2 := \epsilon$, we can implement an $O(s)$-qubit quantum circuit U' that is a $(\|\hat{\mathbf{c}}\|_1, \hat{a}, \epsilon\|\hat{\mathbf{c}}\|_1)$-block-encoding of $P_{d'}(A)$, using $O(d^2)$ queries to U_A, where $\hat{a} = a + \lceil \log d' \rceil + 1$. Assume that U' is a $(1, \hat{a}, 0)$-block-encoding of A', then $\|\|\hat{\mathbf{c}}\|_1 A' - P_{d'}(A)\| \leq \|\hat{\mathbf{c}}\|_1\epsilon$. Additionally, we can compute the quantum circuit description of U' in deterministic space $O(s + \log(1/\epsilon))$ given the coefficient vector $\hat{\mathbf{c}}$ of $P_{d'}$. As the quantum tester $\mathcal{T}(Q, U_A, P_{d'}, \epsilon)$ is mainly based on the Hadamard test, by employing Lemma 2.19, we have that $\mathcal{T}$ outputs 0 with probability

$$\Pr[x=0] = \frac{1}{2}\Big(1 + \mathrm{Re}(\mathrm{Tr}(A'\rho))\Big) = \frac{1}{2}\left(1 + \mathrm{Re}\left(\mathrm{Tr}\left(\frac{P_{d'}(A)}{\|\hat{\mathbf{c}}\|_1}\rho\right)\right)\right) \pm \frac{1}{2}\epsilon.$$

It is left to construct the estimation procedure $\hat{\mathcal{T}}$. As detailed in Lemma 2.13, we can obtain an estimation $\widetilde{x}$ by sequentially repeating the quantum tester $\mathcal{T}(Q, U_A, P_{d'}, \epsilon)$ for $O(1/\epsilon_H^2)$ times. This repetition ensures that $|\widetilde{x} - \mathrm{Re}(\mathrm{Tr}(A'\rho))| \leq \epsilon_H$ holds with probability at least $\Omega(1)$, and derives an further implication on $P_{d'}(A)$:

$$\Pr[\|\|\hat{\mathbf{c}}\|_1\widetilde{x} - \mathrm{Re}(\mathrm{Tr}(P_{d'}(A)\rho))| \leq (\epsilon + \epsilon_H)\|\hat{\mathbf{c}}\|_1] \geq \Omega(1).$$

We thus conclude that construction of the estimation procedure $\hat{\mathcal{T}}(Q, U_A, P_{d'}, \epsilon, \epsilon_H, \delta)$ by using $O(\log(1/\delta)/\epsilon_H^2)$ sequential repetitions of $\mathcal{T}(Q, U_A, P_{d'}, \epsilon)$. Similarly, by Lemma 2.13, $\hat{\mathcal{T}}(Q, U_A, P_d, \epsilon, \epsilon_H, \delta)$ outputs an estimation $\widetilde{x}$ satisfies the following condition:

$$\Pr[|\|\hat{\mathbf{c}}\|_1\widetilde{x} - \mathrm{Re}(\mathrm{Tr}(P_{d'}(A)\rho))| \leq (\epsilon + \epsilon_H)\|\hat{\mathbf{c}}\|_1] \geq 1 - \delta.$$

In addition, a direct calculation indicates that we can implement $\hat{\mathcal{T}}(Q, U_A, P_{d'}, \epsilon, \epsilon_H, \delta)$ in quantum space $O(s + \log(1/\epsilon) + \log(1/\epsilon_H) + \log\log(1/\delta))$ as desired.

Next, we move to the case where $\alpha = 1$, applicable to certain $P_{d'}$ and A, namely when $P_{d'}(A)$ is a partial isometry in Theorem 5.12 or $P_{d'} = P_{d'}^{\mathrm{sgn}}$ in Corollary 5.17. The proof is similar, and we just sketch the key points as follows. Using Theorem 5.12 with $\epsilon_1 := 0$ and

$\epsilon_2 := \epsilon/36$, we can implement an $O(s)$-qubit quantum circuit U' that is a $(1, a', \epsilon\|\hat{\mathbf{c}}\|_1)$-block-encoding of $P_{d'}(A)$, using $O(d^2\|\hat{\mathbf{c}}\|_1)$ queries to U_A, where $a' = a + \lceil \log d' \rceil + 3$. Assume that U' is a $(1, a', 0)$-block-encoding of A', then $\|A' - P_{d'}(A)\| \leq \|\hat{\mathbf{c}}\|_1 \epsilon$. Similarly, $\mathcal{T}$ outputs 0 with probability

$$\Pr[x = 0] = \frac{1}{2}\Big(1 + \mathrm{Re}(\mathrm{Tr}(A'\rho))\Big) = \frac{1}{2}\left(1 + \mathrm{Re}\left(\mathrm{Tr}\left(P_{d'}(A)\rho\right)\right)\right) \pm \frac{1}{2}\|\hat{\mathbf{c}}\|_1\epsilon. \tag{6.4}$$

Therefore, we can obtain an estimate $\widetilde{x}$ such that

$$\Pr[|\widetilde{x} - \mathrm{Re}(\mathrm{Tr}(P_{d'}(A)\rho))| \leq \|\hat{\mathbf{c}}\|_1\epsilon + \epsilon_H] \geq 1 - \delta. \tag{6.5}$$

Similarly, using Corollary 5.17 with $\epsilon_1 := 0$ and $\epsilon_2 := \epsilon/(36\hat{C}_{\mathrm{sgn}} + 37)$ when $P_{d'} = P^{\mathrm{sgn}}_{d'}$, we can also obtain the corresponding formulas of Equation (6.4) and Equation (6.5) by substituting $\|\hat{\mathbf{c}}\|_1$ with $\hat{C}_{\mathrm{sgn}}$, where $\|\hat{\mathbf{c}}^{\mathrm{sgn}}\| \leq \hat{C}_{\mathrm{sgn}}$ is a constant defined in Corollary 5.8. □

6.2.2 GapQSD$_{\log}$ is in BQL

In this subsection, we demonstrate Theorem 6.14 by constructing a quantum algorithm that incorporates testers $\mathcal{T}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P^{\mathrm{sgn}}_d, \epsilon)$ for $i \in \{0, 1\}$, where the construction of testers utilizes the space-efficient QSVT associated with the sign function.

Theorem 6.14. *For any functions $\alpha(n)$ and $\beta(n)$ that can be computed in deterministic logspace and satisfy $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$, we have that*

$$\textsc{GapQSD}_{\log}[\alpha(n), \beta(n)] \text{ is in } \mathsf{BQL}.$$

Proof. Inspired by time-efficient algorithms for the low-rank variant of GapQSD [WZ24a], we devise a space-efficient algorithm for GapQSD$_{\log}$, presented formally in Algorithm 6.2.1.

Algorithm 6.2.1: Space-efficient algorithm for GapQSD$_{\log}$.

Input : Quantum circuits Q_i that prepare the purification of ρ_i for $i \in \{0, 1\}$.
Output: An additive-error estimation of $\mathrm{T}(\rho_0, \rho_1)$.
Params: $\varepsilon := \frac{\alpha-\beta}{4}$, $\delta := \frac{\varepsilon}{2^{r+3}}$, $\epsilon := \frac{\varepsilon}{2(36\hat{C}_{\mathrm{sgn}}+2C_{\mathrm{sgn}}+37)}$, $d' := \tilde{C}_{\mathrm{sgn}} \cdot \frac{1}{\delta} \log \frac{1}{\epsilon} = 2d - 1$, $\varepsilon_H := \frac{\varepsilon}{4}$.

1. Construct block-encodings of ρ_0 and ρ_1, denoted by U_{ρ_0} and U_{ρ_1}, respectively, using $O(1)$ queries to Q_0 and Q_1 and $O(s(n))$ ancillary qubits by Lemma 2.18;
2. Construct a block-encoding of $\frac{\rho_0-\rho_1}{2}$, denoted by $U_{\frac{\rho_0-\rho_1}{2}}$, using $O(1)$ queries to U_{ρ_0} and U_{ρ_1} and $O(s(n))$ ancillary qubits by Lemma 5.15;

Let $P^{\mathrm{sgn}}_{d'}$ be the degree-d' polynomial specified in Corollary 5.8 with parameters δ and ϵ, and its coefficients $\{\hat{c}_k\}_{k=0}^{d'}$ are computable in deterministic space $O(\log(d/\epsilon))$;

3. Set $x_0 := \hat{\mathcal{T}}(Q_0, U_{\frac{\rho_0-\rho_1}{2}}, P^{\mathrm{sgn}}_{d'}, \epsilon, \epsilon_H, 1/10)$, $x_1 := \hat{\mathcal{T}}(Q_1, U_{\frac{\rho_0-\rho_1}{2}}, P^{\mathrm{sgn}}_{d'}, \epsilon, \epsilon_H, 1/10)$;
4. Compute $x = (x_0 - x_1)/2$. Return "yes" if $x > (\alpha + \beta)/2$, and "no" otherwise.

Let us prove the correctness of Algorithm 6.2.1 and analyze the computational complexity. We focus on the setting with $s(n) = \Theta(\log n)$. We set $\varepsilon := (\alpha - \beta)/4 \geq 2^{-O(s)}$ and assume that Q_0 and Q_1 are $s(n)$-qubit quantum circuits that prepare the purifications of ρ_0 and ρ_1, respectively. According to Lemma 2.18, we can construct $O(s)$-qubit quantum

circuits U_{ρ_0} and U_{ρ_1} that encode ρ_0 and ρ_1 as $(1, O(s), 0)$-block-encodings, using $O(1)$ queries to Q_0 and Q_1 as well as $O(1)$ one- and two-qubit quantum gates. Next, we apply Lemma 5.15 to construct a $(1, O(s), 0)$-block-encoding $U_{\frac{\rho_0-\rho_1}{2}}$ of $\frac{\rho_0-\rho_1}{2}$, using $O(1)$ queries to Q_{ρ_0} and Q_{ρ_1}, as well as $O(1)$ one- and two-qubit quantum gates.

Let $\delta := \frac{\varepsilon}{2^{r+3}}$, $\epsilon := \frac{\varepsilon}{2(36\hat{C}_{\mathrm{sgn}}+2C_{\mathrm{sgn}}+37)}$, and $d' := \tilde{C}_{\mathrm{sgn}} \cdot \frac{1}{\delta} \log \frac{1}{\epsilon} \leq 2^{O(s(n))}$, where $\tilde{C}_{\mathrm{sgn}}$ comes from Corollary 5.8. Let $P^{\mathrm{sgn}}_{d'} \in \mathbb{R}[x]$ be the polynomial specified in Corollary 5.8 with $d' = 2d-1$. Let $\epsilon_H = \varepsilon/4$. By employing Corollary 5.17 (with $\epsilon_1 := 0$ and $\epsilon_2 := \epsilon$) and the corresponding estimation procedure $\hat{\mathcal{T}}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P^{\mathrm{sgn}}_{d'}, \Theta(\epsilon), \epsilon_H, 1/10)$ from Lemma 6.13, we obtain the values x_i for $i \in \{0,1\}$, ensuring the following inequalities:

$$\Pr\left[\left|x_i - \mathrm{Tr}\left(P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0-\rho_1}{2}\right)\rho_i\right)\right| \leq (36\hat{C}_{\mathrm{sgn}}+37)\epsilon + \epsilon_H\right] \geq 0.9 \text{ for } i \in \{0,1\}. \tag{6.6}$$

Here, the implementation uses $O(d^2)$ queries to $U_{\frac{\rho_0-\rho_1}{2}}$ and $O(d^2)$ multi-controlled single-qubit gates. Moreover, the circuit descriptions of $\hat{\mathcal{T}}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P^{\mathrm{sgn}}_{d'}, \epsilon, \epsilon_H, 1/10)$ can be computed in deterministic time $\tilde{O}(d^{9/2}/\epsilon)$ and space $O(s(n))$.

Now let $x := (x_0 - x_1)/2$. We will finish the correctness analysis of Algorithm 6.2.1 by showing $\Pr[|x - \mathrm{T}(\rho_0, \rho_1)| \leq \varepsilon] > 0.8$ through Equation (6.6). By considering the approximation error of $P^{\mathrm{sgn}}_{d'}$ in Corollary 5.8 and the QSVT implementation error in Corollary 5.17, we derive the following inequality in Proposition 6.14.1, and the proof is deferred to the end of this subsection:

Proposition 6.14.1. $\Pr\left[|x - \mathrm{T}(\rho_0, \rho_1)| \leq (36\hat{C}_{\mathrm{sgn}} + 2C_{\mathrm{sgn}} + 37)\epsilon + \epsilon_H + 2^{r+1}\delta\right] > 0.8.$

Under the aforementioned choice of δ, ϵ, and ϵ_H, we have $\epsilon_H = \varepsilon/4$, $2^{r+1}\delta = \varepsilon/4$, and $(36\hat{C}_{\mathrm{sgn}} + 2C_{\mathrm{sgn}} + 37)\epsilon \leq \varepsilon/2$, and thus $\Pr[|x - \mathrm{T}(\rho_0, \rho_1)|] > 0.8$.

Finally, we analyze the computational resources required for Algorithm 6.2.1. According to Lemma 6.13, we can compute x in BQL, with the resulting algorithm requiring $O(d^2/\epsilon_H^2) = \tilde{O}(2^{2r}/\varepsilon^4)$ queries to Q_0 and Q_1. In addition, its circuit description can be computed in deterministic time $\tilde{O}(d^{9/2}/\varepsilon) = \tilde{O}(2^{4.5r}/\varepsilon^{5.5})$. □

Proof of Proposition 6.14.1. Using the triangle inequality, we obtain the following:

$$\begin{aligned}
\left|\frac{x_0-x_1}{2} - \mathrm{T}(\rho_0,\rho_1)\right| &= \left|\frac{x_0-x_1}{2} - \mathrm{Tr}\left(\frac{\rho_0-\rho_1}{2}\mathrm{sgn}\left(\frac{\rho_0-\rho_1}{2}\right)\right)\right| \\
&\leq \left|\frac{x_0-x_1}{2} - \mathrm{Tr}\left(\frac{\rho_0-\rho_1}{2}P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0-\rho_1}{2}\right)\right)\right| \\
&\quad + \left|\mathrm{Tr}\left(\frac{\rho_0-\rho_1}{2}P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0-\rho_1}{2}\right)\right) - \mathrm{Tr}\left(\frac{\rho_0-\rho_1}{2}\mathrm{sgn}\left(\frac{\rho_0-\rho_1}{2}\right)\right)\right|.
\end{aligned}$$

For the first term, by noting the QSVT implementation error in Corollary 5.17, we know by Equation (6.6) that, with probability at least $0.9^2 > 0.8$, it holds that

$$\left|\frac{x_0-x_1}{2} - \mathrm{Tr}\left(\frac{\rho_0-\rho_1}{2}P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0-\rho_1}{2}\right)\right)\right| \leq (36\hat{C}_{\mathrm{sgn}}+37)\epsilon + \epsilon_H. \tag{6.7}$$

For the second term, let $\frac{\rho_0-\rho_1}{2} = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$, where $\{|\psi_j\rangle\}$ is an orthonormal basis.

Then, we can derive the following

$$\begin{aligned}&\left|\mathrm{Tr}\left(\frac{\rho_0-\rho_1}{2}P_{d'}^{\mathrm{sgn}}\left(\frac{\rho_0-\rho_1}{2}\right)\right)-\mathrm{Tr}\left(\frac{\rho_0-\rho_1}{2}\mathrm{sgn}\left(\frac{\rho_0-\rho_1}{2}\right)\right)\right|\\ \leq&\sum_j\left|\lambda_j P_{d'}^{\mathrm{sgn}}(\lambda_j)-\lambda_j\mathrm{sgn}(\lambda_j)\right|.\end{aligned}\tag{6.8}$$

We split the summation over j into three separate summations:

$$\sum_j=\sum_{\lambda_j<-\delta}+\sum_{\lambda_j>\delta}+\sum_{-\delta\leq\lambda_j\leq\delta}.$$

By noticing the approximation error of $P_{d'}^{\mathrm{sgn}}$ in Corollary 5.8 and $\sum_j|\lambda_j|=\mathrm{T}(\rho_0,\rho_1)\leq 1$, we can then obtain the following results for each of the three summations:

$$\sum_{\lambda_j>\delta}|\lambda_j P_{d'}^{\mathrm{sgn}}(\lambda_j)-\lambda_j\mathrm{sgn}(\lambda_j)|=\sum_{\lambda_j>\delta}|\lambda_j|\,|P_{d'}^{\mathrm{sgn}}(\lambda_j)-1|\leq\sum_{\lambda_j>\delta}|\lambda_j|C_{\mathrm{sgn}}\epsilon\leq C_{\mathrm{sgn}}\epsilon,$$

$$\sum_{\lambda_j<-\delta}|\lambda_j P_{d'}^{\mathrm{sgn}}(\lambda_j)-\lambda_j\mathrm{sgn}(\lambda_j)|=\sum_{\lambda_j<-\delta}|\lambda_j|\,|P_{d'}^{\mathrm{sgn}}(\lambda_j)+1|\leq\sum_{\lambda_j<-\delta}|\lambda_j|C_{\mathrm{sgn}}\epsilon\leq C_{\mathrm{sgn}}\epsilon,$$

$$\sum_{-\delta\leq\lambda_j\leq\delta}|\lambda_j P_{d'}^{\mathrm{sgn}}(\lambda_j)-\lambda_j\mathrm{sgn}(\lambda_j)|\leq\sum_{-\delta\leq\lambda_j\leq\delta}2|\lambda_j|\leq 2^{r+1}\delta.$$

Hence, we derive the following inequality by summing over these three inequalities:

$$\sum_j|\lambda_j P_{d'}^{\mathrm{sgn}}(\lambda_j)-\lambda_j\mathrm{sgn}(\lambda_j)|\leq 2^{r+1}\delta+2C_{\mathrm{sgn}}\epsilon.\tag{6.9}$$

By combining Equation (6.7), Equation (6.8), and Equation (6.9), we conclude that

$$\left|\frac{x_0-x_1}{2}-\mathrm{T}(\rho_0,\rho_1)\right|\leq(36\hat{C}_{\mathrm{sgn}}+37)\epsilon+\epsilon_H+2C_{\mathrm{sgn}}\epsilon+2^{r+1}\delta.\qquad\square$$

6.2.3 GapQED$_{\log}$ and GapQJS$_{\log}$ are in BQL

In this subsection, we will demonstrate Theorem 6.15 by devising a quantum algorithm that encompasses testers $\mathcal{T}(Q_i,U_{\rho_i},P_{d'}^{\ln},\epsilon)$ for $i\in\{0,1\}$, where the construction of testers employs the space-efficient QSVT associated with the normalized logarithmic function. Consequently, we can deduce that GapQJS$_{\log}$ is in BQL via a reduction from GapQJS$_{\log}$ to GapQED$_{\log}$.

Theorem 6.15. *For any deterministic logspace computable function $g(n)$ that satisfies $g(n)\geq 1/\mathrm{poly}(n)$, we have that*

$$\text{GapQED}_{\log}[g(n)]\ \textit{is in}\ \mathsf{BQL}.$$

Proof. We begin by presenting a formal algorithm in Algorithm 6.2.2.

Let us now demonstrate the correctness and computational complexity of Algorithm 6.2.2. We concentrate on the scenario with $s(n)=\Theta(\log n)$ and $\varepsilon=g/4\geq 2^{-O(s)}$. Our strategy is to estimate the entropy of each of ρ_0 and ρ_1, respectively. We assume that Q_0 and Q_1 are s-qubit quantum circuits that prepare the purifications of ρ_0 and ρ_1, respectively. By Lemma 2.18, we can construct $(1,O(s),0)$-block-encodings U_{ρ_0} and U_{ρ_1} of ρ_0 and ρ_1, respectively, using $O(1)$ queries to Q_0 and Q_1 as well as $O(1)$ one- and two-qubit quantum gates.

Let $\beta=\min\{\frac{\varepsilon}{2^{r+6}\ln(2^{r+6}/\varepsilon)},\frac{1}{4}\}$, $\epsilon:=\frac{\varepsilon}{4\ln(2/\beta)(\hat{C}_{\ln}+C_{\ln})}$ and $d':=\tilde{C}_{\ln}\cdot\frac{1}{\beta}\log\frac{1}{\epsilon}=2^{O(s(n))}$ where $\tilde{C}_{\ln}$ comes from Corollary 5.11. Let $P_{d'}^{\ln}\in\mathbb{R}[x]$ be the polynomial specified in

Algorithm 6.2.2: Space-efficient algorithm for $\textsc{GapQED}_{\log}$.

Input : Quantum circuits Q_i that prepare the purification of ρ_i for $i \in \{0,1\}$.
Output: An additive-error estimation of $\mathrm{S}(\rho_0) - \mathrm{S}(\rho_1)$.
Params: $\varepsilon := \frac{g}{4}$, $\beta := \min\{\frac{\varepsilon}{2^{r+6}\ln(2^{r+6}/\varepsilon)}, \frac{1}{4}\}$, $d' := \tilde{C}_{\ln} \cdot \frac{1}{\beta} \log \frac{1}{\epsilon} = 2d-1$, $\epsilon := \frac{\varepsilon}{4\ln(2/\beta)(\hat{C}_{\ln}+C_{\ln})}$, $\epsilon_H := \frac{\varepsilon}{8\ln(2/\beta)}$.

1. Construct block-encodings of ρ_0 and ρ_1, denoted by U_{ρ_0} and U_{ρ_1}, respectively, using $O(1)$ queries to Q_0 and Q_1 and $O(s(n))$ ancillary qubits by Lemma 2.18;
Let $P^{\ln}_{d'}$ be the degree-d' polynomial specified in Corollary 5.11 with parameters β and ϵ, and its coefficients $\{c^{\ln}_k\}_{k=0}^{d'}$ are computable in bounded-error randomized space $O(\log(d/\epsilon))$;
2. Set $x_0 := \hat{\mathcal{T}}(Q_0, U_{\rho_0}, P^{\ln}_{d'}, \epsilon, \epsilon_H, 1/10)$, $x_1 := \hat{\mathcal{T}}(Q_1, U_{\rho_1}, P^{\ln}_{d'}, \epsilon, \epsilon_H, 1/10)$;
3. Compute $x = 2\ln(\frac{2}{\beta})(x_0 - x_1)$. Return "yes" if $x > 0$, and "no" otherwise.

Corollary 5.11 with $d' = 2d-1$. Let $\epsilon_H := \frac{\varepsilon}{8\ln(2/\beta)}$. By utilizing Corollary 5.18 (with $\epsilon_1 := 0$ and $\epsilon_2 := \epsilon$) and the corresponding estimation procedure $\hat{\mathcal{T}}(Q_i, U_{\rho_i}, P^{\ln}_{d'}, \epsilon, \epsilon_H, 1/10)$ from Lemma 6.13, we obtain the values x_i for $i \in \{0,1\}$, ensuring the following inequalities:

$$\Pr\left[\left|x_i - \mathrm{Tr}\left(P^{\ln}_{d'}(\rho_i)\,\rho_i\right)\right| \le \hat{C}_{\ln}\epsilon + \epsilon_H\right] \ge 0.9 \text{ for } i \in \{0,1\}. \tag{6.10}$$

Here, the implementation uses $O(d^2)$ queries to U_{ρ_i} and $O(d^2)$ multi-controlled single-qubit gates. Moreover, the circuit descriptions of $\hat{\mathcal{T}}(Q_i, U_{\rho_i}, P^{\ln}_{d'}, \epsilon, \epsilon_H, 1/10)$ can be computed in bounded-error time $\tilde{O}(d^9/\epsilon^4)$ and space $O(s(n))$.

We will finish the correctness analysis of Algorithm 6.2.2 by demonstrating

$$\Pr[|x_i - \mathrm{S}(\rho_i)| \le \varepsilon] \ge 0.9$$

through Equation (6.10). By considering the approximation error of $P^{\ln}_{d'}$ in Corollary 5.11 and the QSVT implementation error in Corollary 5.18, we derive the following inequality in Proposition 6.15.1, and the proof is deferred:

Proposition 6.15.1. *The following inequality holds for $i \in \{0,1\}$:*

$$\Pr\left[\left|2\ln\left(\tfrac{2}{\beta}\right)x_i - \mathrm{S}(\rho_i)\right| \le 2\ln\left(\tfrac{2}{\beta}\right)\left((\hat{C}_{\ln}+C_{\ln})\epsilon + \epsilon_H + 2^{r+1}\beta\right)\right] \ge 0.9.$$

Consequently, it is left to show that $2\ln\left(\frac{2}{\beta}\right)\left((\hat{C}_{\ln}+C_{\ln})\epsilon + \epsilon_H + 2^{r+1}\beta\right) \le \varepsilon$ for the specified value of β, ϵ, and ϵ_H. This can be seen by noticing that $2\ln(2/\beta)\epsilon_H = \varepsilon/4$, $2\ln(2/\beta)(\hat{C}_{\ln}+C_{\ln})\epsilon = \varepsilon/2$, and $2\ln(2/\beta)\cdot 2^{r+1}\beta \le \varepsilon/4$. The first two inequalities are trivial. For the third inequality, we state it below and its proof is deferred:

Proposition 6.15.2. $2\ln(\frac{2}{\beta})\cdot 2^{r+1}\beta \le \frac{\varepsilon}{4}$.

Finally, we analyze the computational resources required for Algorithm 6.2.2. As per Lemma 6.13, we can compute x in BQL, with the resulting algorithm requiring $O(d^2/\epsilon_H^2) = \tilde{O}(2^{2r}/\varepsilon^4)$ queries to Q_0 and Q_1. Furthermore, its circuit description can be computed in bounded-error randomized time $\tilde{O}(d^9/\varepsilon^4) = \tilde{O}(2^{9r}/\varepsilon^{13})$. □

Lastly, we present the proof of Proposition 6.15.1 and Proposition 6.15.2.

Proof of Proposition 6.15.1. We only prove the case with $i = 0$ while the case with $i = 1$ follows straightforwardly. By applying the triangle inequality with $i = 0$, we have:

$$\begin{aligned}&\left|2\ln\left(\tfrac{2}{\beta}\right)x_0 - \mathrm{S}(\rho_0)\right| \\ =\ &\left|2\ln\left(\tfrac{2}{\beta}\right)x_0 - 2\ln\left(\tfrac{2}{\beta}\right)\mathrm{Tr}\left(P_{d'}^{\ln}(\rho_0)\rho_0\right)\right| + \left|2\ln\left(\tfrac{2}{\beta}\right)\mathrm{Tr}\left(P_{d'}^{\ln}(\rho_0)\rho_0\right) - \mathrm{S}(\rho_0)\right|.\end{aligned}$$

For the first term, by noting the QSVT implementation error in Corollary 5.18, we have by Equation (6.10) that with probability at least 0.9, it holds that

$$\left|2\ln\left(\tfrac{2}{\beta}\right)x_0 - 2\ln\left(\tfrac{2}{\beta}\right)\mathrm{Tr}\left(P_{d'}^{\ln}(\rho_0)\rho_0\right)\right| \leq 2\ln\left(\tfrac{2}{\beta}\right)\left(\hat{C}_{\ln}\epsilon + \epsilon_H\right). \tag{6.11}$$

For the second term, let $\rho_0 = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$, where $\{|\psi_j\rangle\}$ is an orthonormal basis. Then,

$$\left|2\ln\left(\tfrac{2}{\beta}\right)\mathrm{Tr}\left(P_{d'}^{\ln}(\rho_0)\rho_0\right) - \mathrm{S}(\rho_0)\right| \leq \sum_j \left|2\ln\left(\tfrac{2}{\beta}\right)\lambda_j P_{d'}^{\ln}(\lambda_j) - \lambda_j \ln(1/\lambda_j)\right|. \tag{6.12}$$

We split the summation over j into two separate summations: $\sum_j = \sum_{\lambda_j > \beta} + \sum_{\lambda \leq \beta}$. By noticing the approximation error of $P_{d'}^{\ln}$ in Corollary 5.11 and $\sum_j |\lambda_j| = \mathrm{Tr}(\rho) \leq 1$, we can then obtain the following results for each of the two summations:

$$\begin{aligned}\sum_{\lambda_j > \beta}\left|2\ln\left(\tfrac{2}{\beta}\right)\lambda_j P_{d'}^{\ln}(\lambda_j) - \lambda_j \ln(1/\lambda_j)\right| &= \sum_{\lambda_j > \beta} |\lambda_j| \cdot \left|2\ln\left(\tfrac{2}{\beta}\right)P_{d'}^{\ln}(\lambda_j) - \ln(1/\lambda_j)\right| \\ &\leq \sum_{\lambda_j > \beta} |\lambda_j| \cdot 2\ln\left(\tfrac{2}{\beta}\right)C_{\ln}\epsilon \\ &\leq 2\ln\left(\tfrac{2}{\beta}\right)C_{\ln}\epsilon,\end{aligned}$$

$$\begin{aligned}\sum_{\lambda_j \leq \beta}\left|2\ln\left(\tfrac{2}{\beta}\right)\lambda_j P_{d'}^{\ln}(\lambda_j) - \lambda_j \ln(1/\lambda_j)\right| &\leq \sum_{\lambda_j \leq \beta}\left(2\ln\left(\tfrac{2}{\beta}\right)|\lambda_j| + |\lambda_j|\ln(1/\beta)\right) \\ &\leq 2\ln\left(\tfrac{2}{\beta}\right)2^{r+1}\beta.\end{aligned}$$

Hence, we have derived the following inequality by summing over these two inequalities:

$$\sum_j \left|2\ln\left(\tfrac{2}{\beta}\right)\lambda_j P_{d'}^{\ln}(\lambda_j) - \lambda_j \ln(1/\lambda_j)\right| \leq 2\ln\left(\tfrac{2}{\beta}\right)C_{\ln}\epsilon + 2\ln\left(\tfrac{2}{\beta}\right)2^{r+1}\beta. \tag{6.13}$$

By combining Equation (6.11), Equation (6.12), and Equation (6.13), we conclude that

$$\left|2\ln\left(\tfrac{2}{\beta}\right)x_0 - \mathrm{S}(\rho_0)\right| \leq 2\ln\left(\tfrac{2}{\beta}\right)\left(\hat{C}_{\ln}\epsilon + \epsilon_H + C_{\ln}\epsilon + 2^{r+1}\beta\right). \qquad \square$$

Proof of Proposition 6.15.2. Note that the choice of β is given by $\beta := \frac{\varepsilon}{2^{r+6}\ln(\frac{2^{r+6}}{\varepsilon})}$. Then, to demonstrate the inequality $2\ln(\frac{2}{\beta}) \cdot 2^{r+1}\beta \leq \frac{\varepsilon}{4}$, it suffices to prove that

$$2\ln\left(\frac{2^{r+7}\ln(\frac{2^{r+6}}{\varepsilon})}{\varepsilon}\right) \cdot \frac{\varepsilon}{2^5\ln(\frac{2^{r+6}}{\varepsilon})} \leq \frac{\varepsilon}{4}. \tag{6.14}$$

Let $x := 2^{-r-6}\varepsilon \in (0,1)$, then Equation (6.14) becomes $\ln\left(\frac{2}{x}\ln\left(\frac{1}{x}\right)\right) \leq 4\ln\left(\frac{1}{x}\right)$. This simplifies further to $2x^3\ln\left(\frac{1}{x}\right) \leq 1$.

To complete the proof, let $f(x) = 2x^3\ln(\frac{1}{x})$, then its first derivative is

$$f'(x) = 2x^2\left(3\ln\left(\frac{1}{x}\right) - 1\right).$$

Note that $f'(x) > 0$ for $x \in (0, e^{-1/3})$ and $f'(x) < 0$ for $x \in (e^{-1/3}, 1)$. Thus $f(x)$ is mono-

tonically increasing for $x \in (0, e^{-1/3})$ and monotonically decreasing for $x \in (e^{-1/3}, 1)$. Therefore, $f(x)$ takes the maximum value at $x = e^{-1/3}$, and consequently,

$$f(x) \leq f(e^{-1/3}) = \frac{2}{3e} \leq 1. \qquad \square$$

$\textsc{GapQJS}_{\log}$ is in BQL. It is noteworthy that we can achieve $\textsc{GapQJS}_{\log} \in \mathsf{BQL}$ by employing the estimation procedure $\hat{\mathcal{T}}$ in Algorithm 6.2.2 for *three according states*, given that the quantum Jensen-Shannon divergence $\mathrm{QJS}(\rho_0, \rho_1)$ is a linear combination of $\mathrm{S}(\rho_0), \mathrm{S}(\rho_1)$, and $\mathrm{S}\left(\frac{\rho_0+\rho_1}{2}\right)$. Nevertheless, the logspace Karp reduction from $\textsc{GapQJS}_{\log}$ to $\textsc{GapQED}_{\log}$ (Corollary 6.16) allows us to utilize $\hat{\mathcal{T}}$ for only *two* states. Furthermore, our construction is adapted from the time-bounded scenario, specifically Lemma 7.22.

Corollary 6.16. *For any functions $\alpha(n)$ and $\beta(n)$ that can be computed in deterministic logspace and satisfy $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$, we have that*

$$\textsc{GapQJS}_{\log}[\alpha(n), \beta(n)] \text{ is in } \mathsf{BQL}.$$

Proof. Let Q_0 and Q_1 be the given $s(n)$-qubit quantum circuits where $s(n) = \Theta(\log n)$. Consider a classical-quantum mixed state on a classical register B and a quantum register Y, denoted by $\rho'_1 := \frac{1}{2}|0\rangle\langle 0| \otimes \rho_0 + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_1$, where ρ_0 and ρ_1 are the state obtained by running Q_0 and Q_1, respectively, and tracing out the non-output qubits.

We utilize our reduction to output classical-quantum mixed states ρ'_0 and ρ'_1, which are the output of $(s+2)$-qubit quantum circuits Q'_0 and Q'_1,[11] respectively, where $\rho'_0 := (p_0|0\rangle\langle 0| + p_1|1\rangle\langle 1|) \otimes (\frac{1}{2}\rho_0 + \frac{1}{2}\rho_1)$ and $\mathsf{B}' := (p_0, p_1)$ is an independent random bit with entropy $\mathrm{H}(\mathsf{B}') = 1 - \frac{1}{2}[\alpha(n) + \beta(n)]$. Let $\mathrm{S}_{\mathrm{bit}}(\rho) := \mathrm{S}(\rho)/\ln 2$ for any quantum state ρ, we then have derived that:

$$\begin{aligned}
\mathrm{S}_{\mathrm{bit}}(\rho'_0) - \mathrm{S}_{\mathrm{bit}}(\rho'_1) &= \mathrm{S}_{\mathrm{bit}}(\mathsf{B}', \mathsf{Y})_{\rho'_0} - \mathrm{S}_{\mathrm{bit}}(\mathsf{B}, \mathsf{Y})_{\rho'_1} \\
&= [\mathrm{H}(\mathsf{B}') + \mathrm{S}_{\mathrm{bit}}(\mathsf{Y}|\mathsf{B}')_{\rho'_0}] - [\mathrm{H}(\mathsf{B}) + \mathrm{S}_{\mathrm{bit}}(\mathsf{Y}|\mathsf{B})_{\rho'_1}] \\
&= \mathrm{S}_{\mathrm{bit}}(\mathsf{Y})_{\rho'_0} - \mathrm{S}_{\mathrm{bit}}(\mathsf{Y}|\mathsf{B})_{\rho'_1} + \mathrm{H}(\mathsf{B}') - \mathrm{H}(\mathsf{B}) \\
&= \mathrm{S}_{\mathrm{bit}}(\mathsf{Y})_{\rho'_0} - \mathrm{S}_{\mathrm{bit}}(\mathsf{Y}|\mathsf{B})_{\rho'_1} - \tfrac{1}{2}[\alpha(n) + \beta(n)] \\
&= \mathrm{S}_{\mathrm{bit}}\left(\tfrac{1}{2}\rho_0 + \tfrac{1}{2}\rho_1\right) - \tfrac{1}{2}(\mathrm{S}_{\mathrm{bit}}(\rho_0) + \mathrm{S}_{\mathrm{bit}}(\rho_1)) - \tfrac{1}{2}[\alpha(n) + \beta(n)] \\
&= \mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) - \tfrac{1}{2}[\alpha(n) + \beta(n)].
\end{aligned} \tag{6.15}$$

Here, the second line derives from the definition of quantum conditional entropy and acknowledges that both B and B' are classical registers. The third line owes to the independence of B' as a random bit. Furthermore, the fifth line relies on the Joint entropy theorem (Lemma 3.22).

By plugging Equation (6.15) into the promise of $\textsc{GapQJS}_{\log}[\alpha(n), \beta(n)]$, we can define $g(n') := \frac{\ln 2}{2}\left(\alpha(n) - \beta(n)\right)$ and conclude that:

[11] To construct Q'_1, we follow these steps: We start by applying a H gate on B followed by a $\mathrm{CNOT}_{\mathsf{B}\to\mathsf{R}}$ gate where B and R are single-qubit quantum registers initialized on $|0\rangle$. Next, we apply the controlled-Q_1 gate on the qubits from B to S, where $\mathsf{S} = (\mathsf{Y}, \mathsf{Z})$ is an $s(n)$-qubit register initialized on $|\bar{0}\rangle$. We then apply X gate on B followed by the controlled-Q_0 gate on the qubits from B to S, and we apply X gate on B again. Finally, we obtain ρ'_1 by tracing out R and the qubits in Z. In addition, we can construct Q'_0 similarly.

- If $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \geq \alpha(n)$, then $\mathrm{S}(\rho_0') - \mathrm{S}(\rho_1') \geq \frac{\ln 2}{2}\Big(\alpha(n) - \beta(n)\Big) = g(n')$;
- If $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \leq \beta(n)$, then $\mathrm{S}(\rho_0') - \mathrm{S}(\rho_1') \leq -\frac{\ln 2}{2}\Big(\alpha(n) - \beta(n)\Big) = -g(n')$.

As ρ_1' and ρ_0' are $r'(n')$-qubit states where $n' \coloneqq 3n$[12] and $r'(n') \coloneqq r(n) + 1$, the output length of the corresponding space-bounded quantum circuits Q_0' and Q_1' is $r'(n)$. Therefore, $\textsc{GapQJS}_s[\alpha, \beta]$ is logspace Karp reducible to $\textsc{GapQED}_{s+3}[g]$ by mapping (Q_0, Q_1) to (Q_0', Q_1'). □

6.2.4 $\overline{\textsc{CertQSD}}_{\log}$ and $\overline{\textsc{CertQHS}}_{\log}$ are in $\mathsf{coRQ_UL}$

To make the error one-sided, we adapt the Grover search when the number of solutions is one quarter [BBHT98], also known as the exact amplitude amplification [BHMT02]. A detailed lemma, as stated in Lemma 2.17, can be found in Section 2.4.2.

Notably, when dealing with the unitary of interest with the property specified in Lemma 2.17, which is typically a quantum algorithm with acceptance probability linearly dependent on the chosen distance-like measure (e.g., a tester $\mathcal{T}$ from Lemma 6.13), Lemma 2.17 guarantees that the resulting algorithm $\mathcal{A}$ accepts with probability exactly 1 for *yes* instances ($\rho_0 = \rho_1$). However, achieving $\mathcal{A}$ to accept with probability polynomially deviating from 1 for *no* instances requires additional efforts, leading to the $\mathsf{coRQ_UL}$ containment established through error reduction for $\mathsf{coRQ_UL}$ (Corollary 5.20).

In a nutshell, demonstrating $\mathsf{coRQ_UL}$ containments require to satisfy the desired property, which is achieved differently for $\overline{\textsc{CertQSD}}_{\log}$ and $\overline{\textsc{CertQHS}}_{\log}$.

$\overline{\textsc{CertQSD}}_{\log}$ is in $\mathsf{coRQ_UL}$

Our algorithm in Theorem 6.17 relies on the quantum tester $\mathcal{T}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P_d^{\mathrm{sgn}}, \epsilon)$, as specified in Algorithm 6.2.1. Note that the exact implementation of the space-efficient QSVT associated with odd polynomials preserves the original point (Remark 5.13). Consequently, $\mathcal{T}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P_d^{\mathrm{sgn}}, \epsilon)$ outputs 0 with probability exactly $1/2$ when $\rho_0 = \rho_1$, enabling us to derive the $\mathsf{coRQ_UL}$ containment through a relatively involved analysis for cases when $\mathrm{T}(\rho_0, \rho_1) \geq \alpha$:

Theorem 6.17. *For any deterministic logspace computable function $\alpha(n) \geq 1/\mathrm{poly}(n)$, the following holds*:

$$\overline{\textsc{CertQSD}}_{\log}[\alpha(n)] \text{ is in } \mathsf{coRQ_UL}.$$

Proof. We first provide a formal algorithm, as presented in Algorithm 6.2.3.

Constructing the unitary of interest via the space-efficient QSVT. We consider the setting with $s(n) = \Theta(\log n)$ and $\varepsilon = \alpha/2$. Suppose Q_0 and Q_1 are $s(n)$-qubit quantum circuits that prepare the purifications of ρ_0 and ρ_1, respectively. Similar to Algorithm 6.2.1, we first construct an $O(s)$-qubit quantum circuit $U_{\frac{\rho_0-\rho_1}{2}}$ that is a

[12] By inspecting the circuit description of Q_0' and Q_1' (see Figures 7.1 and 7.2 for details), the maximum number of gates in Q_0' and Q_1' is $2n + 9 + \mathrm{polylog}(1/\epsilon) \leq 3n$ for large enough n. Specifically, the implementation of R_θ in Figure 7.1 requires $\mathrm{polylog}(1/\epsilon) = \mathrm{polylog}(n)$ gates due to the space-efficient Solovay-Kitaev theorem [vMW12, Theorem 4.3].

Algorithm 6.2.3: Space-efficient algorithm for $\overline{\text{CERTQSD}}_{\log}$.

Input : Quantum circuits Q_i that prepare the purification of ρ_i for $i \in \{0,1\}$.
Output: Return "yes" if $\rho_0 = \rho_1$, and "no" otherwise.
Params: $\varepsilon := \frac{\alpha}{2}$, $\delta := \frac{\varepsilon}{2^{r+3}}$, $\epsilon := \frac{\varepsilon}{2(36\tilde{C}_{\text{sgn}}+2C_{\text{sgn}}+37)}$, $d' := \tilde{C}_{\text{sgn}} \cdot \frac{1}{\delta} \log \frac{1}{\epsilon} = 2d-1$.

1. Construct block-encodings of ρ_0 and ρ_1, denoted by U_{ρ_0} and U_{ρ_1}, respectively, using $O(1)$ queries to Q_0 and Q_1 and $O(s(n))$ ancillary qubits by Lemma 2.18;

2. Construct a block-encoding of $\frac{\rho_0-\rho_1}{2}$, denoted by $U_{\frac{\rho_0-\rho_1}{2}}$, using $O(1)$ queries to U_{ρ_0} and U_{ρ_1} and $O(s(n))$ ancillary qubits by Lemma 5.15;

Let $P_{d'}^{\text{sgn}}$ be the degree-d' odd polynomial specified in Corollary 5.8 with parameters δ and ϵ, and its coefficients $\{\hat{c}_k\}_{k=0}^{d'}$ are computable in deterministic space $O(\log(d/\epsilon))$;

3. Let $U_0 := \mathcal{T}(Q_0, U_{\frac{\rho_0-\rho_1}{2}}, P_{d'}^{\text{sgn}}, \epsilon)$ and $U_1 := \mathcal{T}(Q_1, U_{\frac{\rho_0-\rho_1}{2}}, P_{d'}^{\text{sgn}}, \epsilon)$;

4. Let $G_i := -(H \otimes U_i)(I - 2|\bar{0}\rangle\langle\bar{0}|)(H \otimes U_i^\dagger)(I - 2\Pi_0)$ for $i \in \{0,1\}$, where Π_0 is the projection onto the subspace spanned by $\{|0\rangle|0\rangle|\varphi\rangle\}$ over all $|\varphi\rangle$;

5. Measure the first two qubits of $G_i(H \otimes U_i)|0\rangle|0\rangle|\bar{0}\rangle$, and let x_{i0} and x_{i1} be the outcomes, respectively. Return "yes" if $x_{00} = x_{01} = x_{10} = x_{11} = 0$, and "no" otherwise.

$(1, O(s), 0)$-block-encoding of $\frac{\rho_0-\rho_1}{2}$, using $O(1)$ queries to Q_0 and Q_1 and $O(1)$ one- and two-qubit quantum gates.

Let $\delta = \frac{\varepsilon}{2^{r+3}}$, $\epsilon := \frac{\varepsilon}{2(36\tilde{C}_{\text{sgn}}+2C_{\text{sgn}}+37)}$ and $d' := \tilde{C}_{\text{sgn}} \cdot \frac{1}{\delta} \log \frac{1}{\epsilon} = 2^{O(s(n))}$ where $\tilde{C}_{\text{sgn}}$ comes from Corollary 5.8. Let $P_{d'}^{\text{sgn}} \in \mathbb{R}[x]$ be the odd polynomial specified in Corollary 5.8. Let $U_i := \mathcal{T}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P_{d'}^{\text{sgn}}, \epsilon)$ for $i \in \{0,1\}$, then we have the following equalities with $0 \le p_0, p_1 \le 1$:

$$\begin{aligned} U_0|0\rangle|\bar{0}\rangle &= \sqrt{p_0}|0\rangle|\psi_0\rangle + \sqrt{1-p_0}|1\rangle|\psi_1\rangle, \\ U_1|0\rangle|\bar{0}\rangle &= \sqrt{p_1}|0\rangle|\phi_0\rangle + \sqrt{1-p_1}|1\rangle|\phi_1\rangle. \end{aligned}$$

Let H be the HADAMARD gate, then we derive the following equality for $i \in \{0,1\}$:

$$(H \otimes U_i)|0\rangle|0\rangle|\bar{0}\rangle = \sqrt{\frac{p_i}{2}}|0\rangle|0\rangle|\psi_0\rangle + \underbrace{\sqrt{\frac{p_i}{2}}|0\rangle|1\rangle|\psi_0\rangle + \sqrt{\frac{1-p_i}{2}}|1\rangle|0\rangle|\psi_1\rangle + \sqrt{\frac{1-p_i}{2}}|1\rangle|1\rangle|\psi_1\rangle}_{\sqrt{1-\frac{p_i}{2}}|\perp_i\rangle}.$$

Making the error one-sided by exact amplitude amplification. Consider the Grover operator $G_i := -(H \otimes U_i)(I - 2|\bar{0}\rangle\langle\bar{0}|)(H \otimes U_i^\dagger)(I - 2\Pi_0)$, where Π_0 is the projection onto the subspace spanned by $\{|0\rangle|0\rangle|\varphi\rangle\}$ over all $|\varphi\rangle$. By employing the exact amplitude amplification (Lemma 2.17), we can obtain that:

$$\begin{aligned} &G_i(H \otimes U_i)|0\rangle|0\rangle|\bar{0}\rangle = \sin(3\theta_i)|0\rangle|0\rangle|\psi_0\rangle + \cos(3\theta_i)|\perp_i\rangle, \\ &\text{where } \sin^2(\theta_i) = p_i/2 \text{ when } \theta_i \in [0, \pi/4]. \end{aligned} \tag{6.16}$$

Let x_{i0} and x_{i1} be the measurement outcomes of the first two qubits of

$$G_i(H \otimes U_i)|0\rangle|0\rangle|\bar{0}\rangle \text{ for } i \in \{0,1\}.$$

Algorithm 6.2.3 returns "yes" if $x_{00} = x_{01} = x_{10} = x_{11} = 0$, and "no" otherwise. Let $U_{P_{d'}^{\text{sgn}}\left(\frac{\rho_0-\rho_1}{2}\right)}$ be the unitary operator being controlled in the implementation of $U_i :=$

$\mathcal{T}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P_{d'}^{\mathrm{sgn}}, \epsilon)$, and note that by Corollary 5.17, $U_{P_{d'}^{\mathrm{sgn}}\left(\frac{\rho_0-\rho_1}{2}\right)}$ is a $(1, O(s), (36\hat{C}_{\mathrm{sgn}}+37)\epsilon)$-block-encoding of $P_{d'}^{\mathrm{sgn}}\left(\frac{\rho_0-\rho_1}{2}\right)$. The correctness of our algorithm is established as follows:

- For *yes* instances ($\rho_0 = \rho_1$), $U_{P_{d'}^{\mathrm{sgn}}\left(\frac{\rho_0-\rho_1}{2}\right)}$ is a $(1, O(s), 0)$-block-encoding of the zero operator, following from Remark 5.13. Consequently, $\mathcal{T}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P_{d'}^{\mathrm{sgn}}, \epsilon)$ outputs 0 with probability 1/2 for $i \in \{0,1\}$, i.e., $p_0 = p_1 = 1/2$. As a result, we have $\theta_0 = \theta_1 = \pi/6$ and $\sin^2(3\theta_0) = \sin^2(3\theta_1) = 1$. Substituting these values into Equation (6.16), we can conclude that $x_{00} = x_{01} = x_{10} = x_{11} = 0$ with certainty, which completes the analysis.

- For *no* instances ($\mathrm{T}(\rho_0, \rho_1) \geq \alpha$), $U_{P_{d'}^{\mathrm{sgn}}\left(\frac{\rho_0-\rho_1}{2}\right)}$ is a $(1, O(s), 0)$-block-encoding of A satisfying $\left\|A - P_{d'}^{\mathrm{sgn}}\left(\frac{\rho_0-\rho_1}{2}\right)\right\| \leq (36\hat{C}_{\mathrm{sgn}} + 37)\epsilon$. Let p_i be the probability that $\mathcal{T}(Q_i, U_{\frac{\rho_0-\rho_1}{2}}, P_{d'}^{\mathrm{sgn}}, \epsilon)$ outputs 0 for $i \in \{0,1\}$, then $p_i = \frac{1}{2}\Big(1 + \mathrm{Re}(\mathrm{Tr}(\rho_i A))\Big)$ following from Lemma 6.13. A straightforward calculation similar to Proposition 6.14.1 indicates that:

  $$|(p_0 - p_1) - \mathrm{T}(\rho_0, \rho_1)| \leq (36\hat{C}_{\mathrm{sgn}} + 2C_{\mathrm{sgn}} + 37)\epsilon + 2^{r+1}\delta.$$

  Under the choice of δ and ϵ (the same as in the proof of Theorem 6.15), we obtain that $|(p_0 - p_1) - \mathrm{T}(\rho_0, \rho_1)| \leq \varepsilon$ which yields that $\max\{|p_0 - 1/2|, |p_1 - 1/2|\} \geq \varepsilon/2$.[13] Noting that $\Pr[x_{i0} = x_{i1} = 0] = \sin^2(3\theta_i)$ for $i \in \{0,1\}$, Algorithm 6.2.3 will return "yes" with probability $p_{\mathrm{yes}} = \sin^2(3\theta_0)\sin^2(3\theta_1)$. We now provide an upper bound for p_{yes}:

  Proposition 6.17.1. *Let $f(\theta_0, \theta_1) := \sin^2(3\theta_0)\sin^2(3\theta_1)$ be a function such that $\sin^2(\theta_i) = p_i/2$ for $i \in \{0,1\}$ and $\max\{|p_0 - 1/2|, |p_1 - 1/2|\} \geq \varepsilon/2$, then*

  $$f(\theta_0, \theta_1) \leq 1 - \varepsilon^2/4.$$

  Proof. We begin by stating the facts that $\sin^2(\theta_i) = p_i/2$ for $i \in \{0,1\}$ and $\sin^2(3\theta) = \sin^6(\theta) - 6\cos^2(\theta)\sin^4(\theta) + 9\cos^4(\theta)\sin^2(\theta)$. Then we notice that $0 \leq p_0, p_1 \leq 1$ and complete the proof by a direct calculation:

  $$\begin{aligned} f(\theta_0, \theta_1) &= \left(2p_0^3 - 6p_0^2 + \tfrac{9}{2}p_0\right)\left(2p_1^3 - 6p_1^2 + \tfrac{9}{2}p_1\right) \\ &\leq \left(1 - \left(p_0 - \tfrac{1}{2}\right)^2\right)\left(1 - \left(p_1 - \tfrac{1}{2}\right)^2\right) \\ &\leq 1 - \left(\max\left\{\left|p_0 - \tfrac{1}{2}\right|, \left|p_1 - \tfrac{1}{2}\right|\right\}\right)^2 \\ &\leq 1 - \tfrac{\varepsilon^2}{4}. \end{aligned}$$

  □

  Consequently, we finish the analysis by noticing

  $$p_{\mathrm{yes}} = f(\theta_0, \theta_1) \leq 1 - \varepsilon^2/4 = 1 - \alpha^2/16.$$

Now we analyze the complexity of Algorithm 6.2.3. Following Lemma 6.13, we can compute $x_{00}, x_{01}, x_{10}, x_{11}$ in BQL. The quantum circuit that computes $x_{00}, x_{01}, x_{10}, x_{11}$

[13] This inequality is because $|p_0 - p_1| \geq \mathrm{T}(\rho_0, \rho_1) - \varepsilon \geq 2\varepsilon - \varepsilon = \varepsilon$.

takes $O(d^2) = \tilde{O}(2^{2r}/\alpha^2)$ queries to Q_0 and Q_1, and its circuit description can be computed in deterministic time $\tilde{O}(d^{9/2}/\alpha) = \tilde{O}(2^{4.5r}/\alpha^{5.5})$.

Finally, we conclude the $\mathsf{coRQ_UL}$ containment of $\overline{\textsc{CertQSD}}_{\log}$ by applying error reduction for $\mathsf{coRQ_UL}$ (Corollary 5.20) to Algorithm 6.2.3. □

$\overline{\textsc{CertQHS}}_{\log}$ is in $\mathsf{coRQ_UL}$

We begin with the two-sided scenario, particularly providing the BQL containment of $\textsc{GapQHS}_{\log}$, as stated in Theorem 6.18. We then proceed to the one-sided error scenario.

Theorem 6.18. *For any functions $\alpha(n)$ and $\beta(n)$ that can be computed in deterministic logspace and satisfy $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$, we have that*

$$\textsc{GapQHS}_{\log}[\alpha(n), \beta(n)] \text{ is in } \mathsf{BQL}.$$

Proof. We start by noting that

$$\mathrm{HS}^2(\rho_0, \rho_1) = \frac{1}{2}\Big(\mathrm{Tr}(\rho_0^2) + \mathrm{Tr}(\rho_1^2)\Big) - \mathrm{Tr}(\rho_0\rho_1).$$

Let $\varepsilon := (\alpha - \beta)/100$. According to Lemma 2.15, we can use the SWAP test to estimate $\mathrm{Tr}(\rho_0^2)$, $\mathrm{Tr}(\rho_1^2)$, and $\mathrm{Tr}(\rho_0\rho_1)$, and hence $\mathrm{HS}^2(\rho_0, \rho_1)$, within additive error ε with high probability by performing $O(1/\varepsilon^2)$ sequential repetitions. Therefore, we can conclude that $\textsc{GapQHS}_{\log}[\alpha(n), \beta(n)]$ is in BQL. □

Our algorithm in Theorem 6.19 is based on the observation that by expressing $\mathrm{HS}^2(\rho_0, \rho_1)$ as a summation of $\frac{1}{2}\mathrm{Tr}(\rho_0^2)$, $\frac{1}{2}\mathrm{Tr}(\rho_1^2)$, and $-\mathrm{Tr}(\rho_0\rho_1)$, we can devise a hybrid algorithm with *two random coins* using the SWAP test. However, to ensure *unitary*, we design another algorithm employing the LCU technique, which serves as the unitary of interest with the desired property.

Theorem 6.19. *For any deterministic logspace computation function $\alpha(n) \geq 1/\mathrm{poly}(n)$, the following holds*:

$$\overline{\textsc{CertQHS}}_{\log}[\alpha(n)] \text{ is in } \mathsf{coRQ_UL}.$$

Proof. We first provide a formal algorithm, as presented in Algorithm 6.2.4.

Constructing the unitary of interest via the SWAP test. We consider the setting with $s(n) = \Theta(s(n))$. Our main building block is the circuit implementation of the SWAP test (Lemma 2.15). Specifically, we utilize the subroutine $\mathrm{SWAP}(\rho_i, \rho_j)$ for $i, j \in \{0, 1\}$, which involves applying Q_i and Q_j to prepare quantum states ρ_i and ρ_j, respectively, and then employing the SWAP test on these states ρ_i and ρ_j. We denote by p_{ij} the probability that $\mathrm{SWAP}(\rho_i, \rho_j)$ outputs 0 based on the measurement outcome of the control qubit in the SWAP test. Following Lemma 2.15, we have $p_{ij} = \frac{1}{2}\Big(1 + \mathrm{Tr}(\rho_i\rho_j)\Big)$ for $i, j \in \{0, 1\}$.

We define $T_{ij} := \mathrm{SWAP}(\rho_i, \rho_j)$ for $(i, j) \in \mathcal{I} := \{(0, 0), 1, 1, 0, 1\}$, with the control qubit in $\mathrm{SWAP}(\rho_i, \rho_j)$ serving as the output qubit of T_{ij}. By introducing another ancillary qubit, we construct $T'_{ij} := \mathrm{CNOT}(I \otimes T_{ij})$ for $(i, j) \in \mathcal{I}$, where CNOT is controlled by the output qubit of T_{ij} and targets on the new ancillary qubit. It is effortless to see

Algorithm 6.2.4: Space-efficient algorithm for $\overline{\text{CERTQHS}}_{\log}$.

Input : Quantum circuits Q_i that prepare the purification of ρ_i for $i \in \{0,1\}$.
Output: Return "yes" if $\rho_0 = \rho_1$, and "no" otherwise.

1. Construct subroutines $T_{ij} \coloneqq \text{SWAP}(\rho_i, \rho_j)$ for $(i,j) \in \{(0,0),(1,1),(0,1)\}$, which output 0 with probability p_{ij}. The subroutine $\text{SWAP}(\rho_i, \rho_j)$ involves applying Q_i and Q_j to prepare quantum states ρ_i and ρ_j, respectively, and then employing the SWAP test (Lemma 2.15) on these states ρ_i and ρ_j;
2. Construct a block-encoding of $\varrho\left(\frac{1}{2} + \frac{\text{HS}^2(\rho_0,\rho_1)}{4}\right)$ where $\varrho(p) \coloneqq p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$, denoted by U, using $O(1)$ queries to T_{00}, T_{11}, and T_{01} by Lemma 5.15;
3. Let $G \coloneqq -U(I - 2|\bar{0}\rangle\langle\bar{0}|)U^\dagger(I - 2|\bar{0}\rangle\langle\bar{0}|)$;
4. Measure all qubits of $GU|\bar{0}\rangle$ in the computational basis. Return "yes" if the measurement outcome is an all-zero string, and "no" otherwise.

that T'_{ij} prepares the purification of $\varrho(p_{ij})$ with $\varrho(p_{ij}) \coloneqq p_{ij}|0\rangle\langle 0| + (1-p_{ij})|1\rangle\langle 1|$ for $(i,j) \in \mathcal{I}$.

By applying Lemma 2.18, we can construct quantum circuits T''_{ij} for $(i,j) \in \mathcal{I}$ that serve as $(1, O(s), 0)$-block-encoding of $\varrho(p_{ij})$, using $O(1)$ queries to T'_{ij} and $O(1)$ one- and two-qubit quantum gates. Notably, $(X \otimes I)T''_{01}$, with X acting on the qubit of $\varrho(p_2)$, prepares the purification of $X\varrho(p_{01})X^\dagger = p_{01}|1\rangle\langle 1| + (1-p_{01})|0\rangle\langle 0| = \varrho(1-p_{01})$, leading to the equality:

$$\varrho(\rho_0,\rho_1) \coloneqq \frac{1}{4}\varrho(p_{00}) + \frac{1}{4}\varrho(p_{11}) + \frac{1}{2}\varrho(1-p_{01}) = \varrho\left(\frac{1}{2} + \frac{\text{HS}^2(\rho_0,\rho_1)}{4}\right).$$

Consequently, we employ Lemma 5.15 to construct a unitary quantum circuit U that is a $(1,m,0)$-block-encoding of $\varrho\left(\frac{1}{2} + \frac{\text{HS}^2(\rho_0,\rho_1)}{4}\right)$ using $O(1)$ queries to T''_{00}, T''_{11}, $(X\otimes I)T''_{01}$, and $O(1)$ one- and two-qubit quantum gates, where $m \coloneqq O(s)$. The construction ensures the following:

$$U|0\rangle|0\rangle^{\otimes m} = \underbrace{\left(\frac{1}{2} + \frac{\text{HS}^2(\rho_0,\rho_1)}{4}\right)}_{\sin(\theta)}|0\rangle|0\rangle^{\otimes m} + \cos(\theta)|\perp\rangle, \text{ where } \langle 0|\langle 0|^{\otimes m}|\perp\rangle = 0. \quad (6.17)$$

Making the error one-sided. Let us consider the Grover operator $G \coloneqq -U(I - 2|\bar{0}\rangle\langle\bar{0}|)U^\dagger(I - 2|\bar{0}\rangle\langle\bar{0}|)$. By applying Lemma 2.17, we derive that

$$GU|0\rangle|0\rangle^{\otimes m} = \sin(3\theta)|0\rangle|0\rangle^{\otimes m} + \cos(3\theta)|\perp\rangle.$$

Subsequently, we measure all qubits of $GU|0\rangle|0\rangle^{\otimes m}$ in the computational basis, represented as $x \in \{0,1\}^{m+1}$. Hence, Algorithm 6.2.4 returns "yes" if the outcome x is 0^{m+1} and "no" otherwise. Algorithm 6.2.4 accepts with probability $\sin^2(3\theta)$. Now we analyze the correctness of the algorithm:

- For *yes* instances ($\rho_0 = \rho_1$), we have $\text{HS}^2(\rho_0,\rho_1) = 0$. Following Equation (6.17), we obtain $\sin(\theta) = 1/2$ and thus $\sin^2(3\theta) = 1$. We conclude that Algorithm 6.2.4 will always return "yes".

- For *no* instances, we have $\mathrm{HS}^2(\rho_0, \rho_1) \geq \alpha$. According to Equation (6.17), we obtain:

$$\begin{aligned} \sin(\theta) &= \frac{1}{2} + \frac{\mathrm{HS}^2(\rho_0, \rho_1)}{4} \geq \frac{1}{2} + \frac{\alpha}{4}, \\ \frac{1}{4} \leq \sin^2(\theta) &= \left(\frac{1}{2} + \frac{\mathrm{HS}^2(\rho_0, \rho_1)}{4}\right)^2 \leq \left(\frac{1}{2} + \frac{1}{4}\right)^2 = \frac{9}{16}. \end{aligned} \tag{6.18}$$

  As a result, considering the fact that

$$\sin^2(3\theta) = f(\sin^2(\theta)) \text{ where } f(x) \coloneqq 16x^3 - 24x^2 + 9x,$$

  we require Proposition 6.19.1 and the proof is deferred to the end of this subsection:

Proposition 6.19.1. *The polynomial function $f(x) \coloneqq 16x^3 - 24x^2 + 9x$ is monotonically decreasing in $[1/4, 9/16]$. Moreover, we have*

$$f\left(\left(\frac{1}{2} + \frac{\alpha}{4}\right)^2\right) \leq 1 - \frac{\alpha^2}{2} \text{ for any } 0 \leq \alpha \leq 1.$$

  Combining Equation (6.18) and Proposition 6.19.1, we have that

$$\sin^2(3\theta) = f(\sin^2(\theta)) \leq f\left(\left(\frac{1}{2} + \frac{\alpha}{4}\right)^2\right) \leq 1 - \frac{\alpha^2}{2}.$$

  Hence, Algorithm 6.2.4 will return "no" with probability at least $\alpha^2/2$.

Regarding the computational complexity of Algorithm 6.2.4, this algorithm requires $O(s(n))$ qubits and performs $O(1)$ queries to Q_0 and Q_1. Finally, we finish the proof by applying error reduction from $\mathsf{coRQ_UL}$ (Corollary 5.20) to Algorithm 6.2.3. □

Lastly, we provide the proof of Proposition 6.19.1:

Proof of Proposition 6.19.1. Through a direct calculation, we have $f'(x) = 48x^2 - 48x + 9 \leq 0$ for $x \in [1/4, 3/4]$, then $f(x)$ is monotonically decreasing in $[1/4, 9/16] \subseteq [1/4, 3/4]$. Moreover, it is left to show that:

$$f\left(\left(\tfrac{1}{2} + \tfrac{\alpha}{4}\right)^2\right) = \tfrac{\alpha^6}{256} + \tfrac{3\alpha^5}{64} + \tfrac{9\alpha^4}{64} - \tfrac{\alpha^3}{8} - \tfrac{3\alpha^2}{4} + 1 \leq 1 - \tfrac{\alpha^2}{2}.$$

Equivalently, it suffices to show that $g(x) \coloneqq -\frac{x^4}{256} - \frac{3x^3}{64} - \frac{9x^2}{64} + \frac{x}{8} + \frac{1}{4} \geq 0$ for $0 \leq x \leq 1$. We first compute the first derivative of $g(x)$, which is $g'(x) = -\frac{x^3}{64} - \frac{9x^2}{64} - \frac{9x}{32} + \frac{1}{8}$. Setting $g'(x)$ equal to zero, we obtain three roots: $x_1 = -4$, $x_2 = \frac{1}{2}(-\sqrt{33} - 5) < 0$, and $x_3 = \frac{1}{2}(\sqrt{33} - 5) \in (0, 1)$.

Since $g'(0) = 1/8 > 0$ and $g'(1) = -5/16 < 0$, we conclude that $g(x)$ is monotonically increasing in $[0, x_3]$ and monotonically decreasing in $[x_3, 1]$. Therefore, we can determine the minimum value of $g(x)$ by evaluating $g(0) = \frac{1}{4}$ and $g(1) = \frac{47}{256}$. Since both values are greater than zero, we conclude that $\min\{g(0), g(1)\} = \left\{\frac{1}{4}, \frac{47}{256}\right\} > 0$, as desired. □

6.2.5 BQL- and coRQ$_{\mathrm{U}}$L-hardness of space-bounded state testing problems

We will prove that space-bounded state testing problems mentioned in Theorem 6.12 are BQ$_{\mathrm{U}}$L-hard, which implies their BQL-hardness since BQL=BQ$_{\mathrm{U}}$L [FR21]. Similarly, all space-bounded state certification problems mentioned in Theorem 6.11 are coRQ$_{\mathrm{U}}$L-hard.

Hardness results for GapQSD$_{\log}$, GapQHS$_{\log}$, and their certification version

Employing analogous constructions, we can establish the BQ$_{\mathrm{U}}$L-hardness of both GapQSD$_{\log}$ and GapQHS$_{\log}$. The former involves a single-qubit pure state and a single-qubit mixed state, while the latter involves two pure states.

Lemma 6.20 ($\overline{\text{GapQSD}}_{\log}$ is BQ$_{\mathrm{U}}$L-hard)**.** *For any deterministic logspace computable functions $a(n)$ and $b(n)$ such that $a(n) - b(n) \geq 1/\mathrm{poly}(n)$, we have that*

$$\overline{\text{GapQSD}}_{\log}[1-\sqrt{a(n)}, \sqrt{1-b(n)}] \text{ is } \mathsf{BQ_UL}[a(n), b(n)]\text{-hard.}$$

Proof. Consider a promise problem $(\mathcal{P}_{yes}, \mathcal{P}_{no}) \in \mathsf{BQ_UL}[a(n), b(n)]$, then we know that the acceptance probability $\Pr[C_x \text{ accepts}] \geq a(n)$ if $x \in \mathcal{P}_{yes}$, whereas $\Pr[C_x \text{ accepts}] \leq b(n)$ if $x \in \mathcal{P}_{no}$. Now we notice that the acceptance probability is the fidelity between a single-qubit pure state ρ_0 and a single-qubit mixed state ρ_1 that is prepared by two logarithmic-qubit quantum circuits Q_0 and Q_1, respectively:

$$\begin{aligned}\Pr[C_x \text{ accepts}] =& \left\| |1\rangle\langle 1|_{\text{out}} C_x|\bar{0}\rangle \right\|_2^2 \\ =& \mathrm{Tr}\left(|1\rangle\langle 1|_{\text{out}} \mathrm{Tr}_{\overline{\text{out}}}\left(C_x|\bar{0}\rangle\langle\bar{0}|C_x^\dagger\right)\right) \\ =& \mathrm{F}^2\left(|1\rangle\langle 1|_{\text{out}}, \mathrm{Tr}_{\overline{\text{out}}}\left(C_x|\bar{0}\rangle\langle\bar{0}|C_x^\dagger\right)\right) \\ :=& \mathrm{F}^2(\rho_0, \rho_1).\end{aligned} \tag{6.19}$$

In particular, the corresponding Q_0 is simply flipping the designated output qubit, as well as the corresponding Q_1 is exactly the circuit C_x, then we prepare ρ_0 and ρ_1 by tracing out all non-output qubits. By utilizing Lemma 3.17, we have derived that:

- For *yes* instances, $\mathrm{F}^2(\rho_0, \rho_1) \geq a(n)$ deduces that $\mathrm{T}(\rho_0, \rho_1) \leq 1 - \sqrt{a(n)}$;
- For *no* instances, $\mathrm{F}^2(\rho_0, \rho_1) \leq b(n)$ yields that $\mathrm{T}(\rho_0, \rho_1) \geq \sqrt{1-b(n)}$

Therefore, we prove that $\overline{\text{GapQSD}}_{\log}[1-\sqrt{a(n)}, \sqrt{1-b(n)}]$ is $\mathsf{BQL}[a(n), b(n)]$-hard. □

To construct pure states, we adapt the approach from Lemma 6.20 by replacing the final measurement in the BQL circuit C_x with a quantum gate (CNOT). We then design a new algorithm based on C_x, with the final measurement on *all* qubits in the computational basis, as demonstrated in the proof of Lemma 6.21.

Lemma 6.21 ($\overline{\text{GapQHS}}_{\log}$ is BQ$_{\mathrm{U}}$L-hard)**.** *For any deterministic logspace computable functions $a(n)$ and $b(n)$ such that $a(n) - b(n) \geq 1/\mathrm{poly}(n)$, we have that*

$$\overline{\text{GapQHS}}_{\log}[1-a^2(n), 1-b^2(n)] \text{ is } \mathsf{BQ_UL}[a(n), b(n)]\text{-hard.}$$

Proof. For any promise problem $(\mathcal{P}_{yes}, \mathcal{P}_{no}) \in \mathsf{BQ_UL}[a(n), b(n)]$, we have that the acceptance probability $\Pr[C_x \text{ accepts}] \geq a(n)$ if $x \in \mathcal{P}_{yes}$, whereas $\Pr[C_x \text{ accepts}] \leq b(n)$ if $x \in \mathcal{P}_{no}$. For simplicity, let the output qubit be the register O. Now we construct a new quantum circuit C'_x with an additional ancillary qubit on the register F initialized to zero:

$$C'_x \coloneqq C_x^\dagger X_{\mathsf{O}}^\dagger \mathrm{CNOT}_{\mathsf{O}\to\mathsf{F}} X_{\mathsf{O}} C_x.$$

And we say that C'_x accepts if the measurement outcome of all qubits (namely the working qubit of C_x and F) are all zero. Through a direct calculation, we obtain:

$$\begin{aligned}
\Pr[C'_x \text{ accepts}] &= \left\| (|\bar{0}\rangle\langle\bar{0}| \otimes |0\rangle\langle 0|_{\mathsf{F}}) C_x^\dagger X_{\mathsf{O}} \mathrm{CNOT}_{\mathsf{O}\to\mathsf{F}} X_{\mathsf{O}} C_x (|\bar{0}\rangle \otimes |0\rangle_{\mathsf{F}}) \right\|_2^2 \\
&= \left| (\langle\bar{0}| \otimes \langle 0|_{\mathsf{F}}) C_x^\dagger (|1\rangle\langle 1|_{\mathsf{O}} \otimes I_{\mathsf{F}} + |0\rangle\langle 0|_{\mathsf{O}} \otimes X_{\mathsf{F}}) C_x (|\bar{0}\rangle \otimes |0\rangle_{\mathsf{F}}) \right|^2 \\
&= \left| \langle\bar{0}| C_x^\dagger |1\rangle\langle 1|_{\mathsf{O}} C_x |\bar{0}\rangle \right|^2 \\
&= \Pr^2 [C_x \text{ accepts}] .
\end{aligned} \tag{6.20}$$

Here, the second line owes to $\mathrm{CNOT}_{\mathsf{O}\to\mathsf{F}} = |0\rangle\langle 0|_{\mathsf{O}} \otimes I_{\mathsf{F}} + |1\rangle\langle 1|_{\mathsf{O}} \otimes X_{\mathsf{F}}$, and the last line is because of Equation (6.19). Interestingly, by defining two pure states $\rho_0 \coloneqq |\bar{0}\rangle\langle\bar{0}| \otimes |0\rangle\langle 0|_{\mathsf{F}}$ and $\rho_1 \coloneqq C'_x(|\bar{0}\rangle\langle\bar{0}| \otimes |0\rangle\langle 0|_{\mathsf{F}})C'^\dagger_x$ corresponding to $Q_0 = I$ and $Q_1 = C'_x$, respectively, we deduce the following from Equation (6.20):

$$\Pr[C'_x \text{ accepts}] = \mathrm{Tr}(\rho_0\rho_1) = 1 - \mathrm{HS}^2(\rho_0, \rho_1). \tag{6.21}$$

Combining Equation (6.20) and Equation (6.21), we complete the proof by concluding the following:

- For *yes* instances, $\Pr[C_x \text{ accepts}] \geq a(n)$ implies that $\mathrm{HS}^2(\rho_0, \rho_1) \leq 1 - a^2(n)$;
- For *no* instances, $\Pr[C_x \text{ accepts}] \leq b(n)$ yields that $\mathrm{HS}^2(\rho_0, \rho_1) \geq 1 - b^2(n)$. □

Our constructions in the proof of Lemma 6.20 and Lemma 6.21 are somewhat analogous to [RASW23, Theorem 12 and 13]. Then we proceed with a few direct corollaries of Lemmas 6.20 and 6.21.

Corollary 6.22 ($\mathsf{BQ_UL}$- and $\mathsf{coRQ_UL}$-hardness)**.** *For any functions $a(n)$ and $b(n)$ are computable in deterministic logspace such that $a(n) - b(n) \geq 1/\mathrm{poly}(n)$, the following holds for some polynomial $p(n)$ which can be computed in deterministic logspace:*

(1) $\textsc{GapQSD}_{\log}[\alpha(n), \beta(n)]$ *is* $\mathsf{BQ_UL}$*-hard for* $\alpha \leq 1 - 1/p(n)$ *and* $\beta \geq 1/p(n)$*;*

(2) $\overline{\textsc{CertQSD}}_{\log}[\gamma(n)]$ *is* $\mathsf{coRQ_UL}$*-hard for* $\gamma \leq 1 - 1/p(n)$*;*

(3) $\textsc{GapQHS}_{\log}[\alpha(n), \beta(n)]$ *is* $\mathsf{BQ_UL}$*-hard for* $\alpha \leq 1 - 1/p(n)$ *and* $\beta \geq 1/p(n)$*;*

(4) $\overline{\textsc{CertQHS}}_{\log}[\gamma(n)]$ *is* $\mathsf{coRQ_UL}$*-hard for* $\gamma \leq 1 - 1/p(n)$.

Proof. Firstly, it is important to note that $\mathsf{BQ_UL}$ is closed under complement, as demonstrated in [Wat99, Corollary 4.8]. By combining error reduction for $\mathsf{BQ_UL}$ (Corollary 5.20) and Lemma 6.20 (resp., Lemma 6.21), we can derive the first statement (resp., the third statement).

Furthermore, to obtain the second statement (resp., the fourth statement), we can utilize error reduction for $\mathsf{coRQ_UL}$ (Corollary 5.20) and set $a = 1$ in Lemma 6.20 (resp., Lemma 6.21). □

Hardness results for $\textsc{GapQJS}_{\log}$ and $\textsc{GapQED}_{\log}$

We prove the $\mathsf{BQ_UL}$-hardness of $\textsc{GapQJS}_{\log}$ by reducing $\textsc{GapQSD}_{\log}$ to $\textsc{GapQJS}_{\log}$, following a similar approach as shown in Lemma 7.31.

Lemma 6.23 ($\textsc{GapQJS}_{\log}$ is $\mathsf{BQ_UL}$-hard)**.** *For any functions $\alpha(n)$ and $\beta(n)$ are computable in deterministic logspace, we have that: For $\alpha(n) \leq 1 - \frac{\sqrt{2}}{\sqrt{p(n)}}$ and $\beta(n) \geq \frac{1}{p(n)}$,*

$$\textsc{GapQJS}_{\log}[\alpha(n), \beta(n)] \text{ is } \mathsf{BQ_UL}\text{-hard.}$$

Here, $p(n)$ is some deterministic logspace computable polynomial.

Proof. By employing Corollary 6.22, it suffices to reduce $\textsc{GapQSD}_{\log}[1 - 1/p(n), 1/p(n)]$ to $\textsc{GapQJS}_{\log}[\alpha(n), \beta(n)]$. Consider logarithmic-qubit quantum circuits Q_0 and Q_1, which is a $\textsc{GapQSD}_{\log}$ instance. We can obtain ρ_k for $k \in \{0, 1\}$ by performing Q_k on $|0^n\rangle$ and tracing out the non-output qubits. We then have the following:

- If $\mathrm{T}(\rho_0, \rho_1) \geq 1 - 1/p(n)$, then Lemma 3.25 yields that
$$\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \geq 1 - \mathrm{H}_{\mathrm{bit}}\left(\tfrac{1-\mathrm{T}(\rho_0,\rho_1)}{2}\right) \geq 1 - \mathrm{H}_{\mathrm{bit}}\left(\tfrac{1}{2p(n)}\right) \geq 1 - \tfrac{\sqrt{2}}{\sqrt{p(n)}} \geq \alpha(n),$$
where the third inequality owing to $\mathrm{H}_{\mathrm{bit}}(x) \leq 2\sqrt{x}$ for all $x \in [0, 1]$.
- If $\mathrm{T}(\rho_0, \rho_1) \leq 1/p(n)$, then Lemma 3.26 indicates that
$$\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \leq \mathrm{T}(\rho_0, \rho_1) \leq \tfrac{1}{p(n)} \leq \beta(n).$$

Therefore, we can utilize the same quantum circuits Q_0 and Q_1, along with their corresponding quantum states ρ_0 and ρ_1, respectively, to establish a logspace Karp reduction from $\textsc{GapQSD}_{\log}[1 - 1/p(n), 1/p(n)]$ to $\textsc{GapQJS}_{\log}[\alpha(n), \beta(n)]$, as required. □

By combining the reduction from $\textsc{GapQSD}_{\log}$ to $\textsc{GapQJS}_{\log}$ (Lemma 6.23) and the reduction from $\textsc{GapQJS}_{\log}$ to $\textsc{GapQED}_{\log}$ (Corollary 6.16), we will demonstrate that the $\mathsf{BQ_UL}$-hardness of $\textsc{GapQED}_{\log}$ through reducing $\textsc{GapQSD}_{\log}$ to $\textsc{GapQED}_{\log}$. This proof resembles the approach outlined in Corollary 7.21.

Corollary 6.24 ($\textsc{GapQED}_{\log}$ is $\mathsf{BQ_UL}$-hard)**.** *For any function $g(n)$ are computable in deterministic logspace, we have that:*

$$\text{For any } g(n) \leq \tfrac{\ln 2}{2}\left(1 - \tfrac{\sqrt{2}}{\sqrt{p(n/3)}} - \tfrac{1}{p(n/3)}\right), \textsc{GapQED}_{\log}[g(n)] \text{ is } \mathsf{BQ_UL}\text{-hard.}$$

Here, $p(n)$ is some polynomial that can be computed in deterministic logspace.

Proof. By combining Corollary 6.22 and Lemma 6.23, we establish that:

$$\text{For any } \alpha(n) \leq 1 - \tfrac{\sqrt{2}}{\sqrt{p(n)}} \text{ and } \beta(n) \geq \tfrac{1}{p(n)}, \textsc{GapQJS}_{\log}[\alpha(n), \beta(n)] \text{ is } \mathsf{BQ_UL}\text{-hard.}$$

Here, $p(n)$ is some deterministic logspace computable polynomial. The $\textsc{GapQSD}_{\log}$-hard (and simultaneously $\textsc{GapQJS}_{\log}$-hard) instances, as specified in Corollary 6.22, consist of $s(n)$-qubit quantum circuits Q_0 and Q_1 that prepare a purification of $r(n)$-qubit quantum (mixed) states ρ_0 and ρ_1, respectively, where $1 \leq r(n) \leq s(n) = \Theta(\log n)$.

Subsequently, by employing Corollary 6.16, we construct $(s+3)$-qubit quantum circuits Q_0' and Q_1' that prepare a purification of $(r+1)$-qubit quantum states $\rho_0' = \Big(p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|\Big) \otimes \big(\frac{1}{2}\rho_0 + \frac{1}{2}\rho_1\big)$ satisfying $\mathrm{H}_{\mathrm{bit}}(p) = 1 - \frac{\ln 2}{2}\Big(\alpha(n) + \beta(n)\Big)$ and $\rho_1' = \frac{1}{2}|0\rangle\langle 0| \otimes \rho_0 + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_1$, respectively. Following Corollary 6.16, $\textsc{GapQED}_{\log}[g(n)]$ is $\mathsf{BQ_UL}$-hard as long as

$$g(n) = \tfrac{\ln 2}{2}\Big(\alpha(n/3) - \beta(n/3)\Big) \leq \tfrac{\ln 2}{2}\Big(1 - \tfrac{\sqrt{2}}{\sqrt{p(n/3)}} - \tfrac{1}{p(n/3)}\Big).$$

Therefore, $\textsc{GapQSD}_s$ is logspace Karp reducible to $\textsc{GapQED}_{s+1}$ by mapping (Q_0, Q_1) to (Q_0', Q_1'). □

6.3 Application: Algorithmic Holevo-Helstrom measurement and an improved upper bound of QSZK

In this section, we introduce an *algorithmic* Holevo-Helstrom measurement that achieves the optimal probability (with an additive error) for discriminating between quantum states ρ_0 and ρ_1, as outlined in Theorem 3.12. We assume knowledge of the corresponding polynomial-size quantum circuits, viewed as "source codes" for quantum devices, used to prepare (purifications of) these states. We now define the Computational Quantum Hypothesis Testing Problem:

Problem 6.25 (Computational Quantum Hypothesis Testing Problem)**.** *Given polynomial-size quantum circuits Q_0 and Q_1 acting on n qubits and having r designated output qubits. Let ρ_b denote the quantum state obtained by performing Q_b on the initial state $|0^n\rangle$ 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 $\rho = \rho_b$.*

For the Quantum Hypothesis Testing Problem analogous to Problem 6.25, 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, as stated in Theorem 3.12.

Next, we specify the optimal two-outcome measurement $\{\Pi_0, \Pi_1\}$ that achieves the maximum discrimination probability in Theorem 3.12:

$$\Pi_0 = \frac{I}{2} + \frac{1}{2}\mathrm{sgn}^{(\mathrm{SV})}\Big(\frac{\rho_0 - \rho_1}{2}\Big) \text{ and } \Pi_1 = \frac{I}{2} - \frac{1}{2}\mathrm{sgn}^{(\mathrm{SV})}\Big(\frac{\rho_0 - \rho_1}{2}\Big). \tag{6.22}$$

It is straightforward to see that $\mathrm{T}(\rho_0, \rho_1) = \frac{1}{2}\mathrm{Tr}|\rho_0 - \rho_1| = \mathrm{Tr}(\Pi_0\rho_0) - \mathrm{Tr}(\Pi_0\rho_1)$.

By leveraging our space-efficient quantum singular value transformation in Chapter 5, we can approximately implement the Holevo-Helstrom measurement specified in Equation (6.22) in quantum *single-exponential* time and *linear* space. We refer to this explicit implementation of the Holevo-Helstrom measurement as the *algorithmic Holevo-Helstrom measurement*:

Theorem 6.26 (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 6.25. An approximate version of the Holevo-Helstrom measurement Π_0 specified in*

Equation (6.22)*, denoted as* $\tilde{\Pi}_0$*, can be implemented such that*

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

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 quantum gates. Furthermore, the circuit description can be computed in deterministic time* $2^{O(n)}$ *and space* $O(n)$*.*

In addition, we show an implication of our algorithmic Holevo-Helstrom measurement in Theorem 6.26. By inspecting the (honest-verifier) quantum statistical zero-knowledge protocol ("distance test") for (α,β)-QSD where $\alpha^2 > \beta$ in [Wat02], we established a slightly improved upper bound for the class QSZK since GapQSD is QSZK-hard:

Theorem 6.27 (GapQSD is in QIP(2) with a quantum linear-space honest prover)**.** *There is a two-message quantum interactive proof system for* $\mathrm{GapQSD}[\alpha(n),\beta(n)]$ *with completeness* $c(n) = \left(1+\alpha(n)-2^{-n}\right)/2$ *and soundness* $s(n) = (1+\beta(n))/2$*. Moreover, the optimal prover strategy for this protocol can be implemented in quantum single-exponential time and linear space.*

Consequently, for any $\alpha(n)$ *and* $\beta(n)$ *satisfying* $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$*,*

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

Here, n' *is the total input length of the quantum circuits that prepare the corresponding tuple of quantum states.*[14]

In the rest of this section, we provide the proof of Theorem 6.26 and the proof of Theorem 6.27 in Section 6.3.1 and Section 6.3.2, respectively.

6.3.1 Algorithmic Holevo-Helstrom measurement: Proof of Theorem 6.26

Our algorithmic Holevo-Helstrom measurement primarily utilizes the space-efficient quantum state tester (see Figure 6.2) in Section 6.2. By leveraging the space-efficient polynomial approximation $P^{\mathrm{sgn}}_{d'}$ of the sign function (Corollary 5.8), it suffices to implement another two-outcome measurement $\{\hat{\Pi}_0,\hat{\Pi}_1\}$:

$$\hat{\Pi}_0 = \frac{I}{2} + \frac{1}{2}P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0-\rho_1}{2}\right) \text{ and } \hat{\Pi}_1 = \frac{I}{2} - \frac{1}{2}P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0-\rho_1}{2}\right).$$

By applying the space-efficient QSVT associated with the polynomial $P^{\mathrm{sgn}}_{d'}$ to the block-encoding of $(\rho_0-\rho_1)/2$ (Corollary 5.17), we obtain the unitary U_{HH} which is a block-encoding of $A_{\mathrm{HH}} :\approx P^{\mathrm{sgn}}_{d'}\left(\frac{\rho_0-\rho_1}{2}\right)$. We now instead 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.

We now proceed to the actual proof.

Proof of Theorem 6.26. Our algorithmic Holevo-Helstrom measurement is inspired by Algorithm 6.2.1 in the proof of Theorem 6.14 ($\mathrm{GapQSD}_{\log}$ is in BQL), as presented in Figure 6.3.

[14] This tuple of quantum states results from a standard parallel repetition of the two-message quantum interactive proof system for $\mathrm{GapQSD}[\alpha(n),\beta(n)]$ with $c(n) - s(n) \geq 1/poly(n)$.

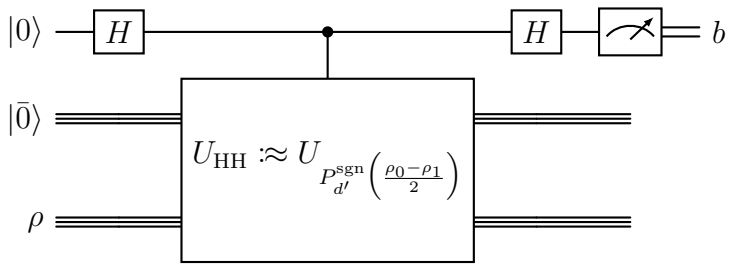

Figure 6.3: Algorithmic Holevo-Helstrom measurement.

Note that the input state ρ to the circuit specified in Figure 6.3 is an $r(n)$-qubit quantum state, either ρ_0 or ρ_1, prepared by an n-qubit polynomial-size quantum circuit (Q_0 or Q_1) after tracing out all $n-r$ non-output qubits, where Q_0 and Q_1 are defined in Problem 6.25. The key ingredient in Figure 6.3 is to implement the unitary U_{HH}, which can be achieved as follows:

(1) Applying Lemma 2.18, we can construct n-qubit quantum circuits U_{ρ_0} and U_{ρ_1} that encode ρ_0 and ρ_1 as $(1, n-r, 0)$-block-encodings, using $O(1)$ queries to Q_0 and Q_1, together with $O(1)$ one- and two-qubit quantum gates.

(2) Applying Lemma 5.15, we can construct a $(1, n-r+1, 0)$-block-encoding $U_{\frac{\rho_0-\rho_1}{2}}$ of $\frac{\rho_0-\rho_1}{2}$, using $O(1)$ queries to Q_0 and Q_1, as well as $O(1)$ one- and two-qubit quantum gates.

(3) Let $P_{d'}^{\mathrm{sgn}} \in \mathbb{R}[x]$ be the degree-d' polynomial obtained from some degree-d averaged Chebyshev truncation, with $d' = 2d-1$, as specified in Corollary 5.8. We choose parameters $\varepsilon := 2^{-n}$, $\delta := \frac{\varepsilon}{2^{r+3}}$, $\epsilon := \frac{\varepsilon}{2(36\tilde{C}_{\mathrm{sgn}}+2C_{\mathrm{sgn}}+37)}$, and $d' := \tilde{C}_{\mathrm{sgn}} \cdot \frac{1}{\delta} \log \frac{1}{\epsilon} = 2^{O(n)}$ where $\tilde{C}_{\mathrm{sgn}}$ comes from Corollary 5.8. Applying the space-efficient QSVT associated with the sign function (Corollary 5.17 with $\epsilon_1 := 0$ and $\epsilon_2 := \epsilon$), we obtain the unitary U_{HH}.

Error analysis. We first bound the error caused by space-efficient polynomial approximation in Corollary 5.8. Consider the spectral decomposition $\frac{\rho_0-\rho_1}{2} = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$, where $\{|\psi_j\rangle\}$ is an orthonormal basis. We can define index sets $\Lambda_- := \{j\colon \lambda_j < -\delta\}$, $\Lambda_0 := \{j\colon -\delta \le \lambda_j \le \delta\}$, and $\Lambda_+ := \{j\colon \lambda_j > \delta\}$. Next, we have derived that:

$$
\begin{aligned}
&\left|\mathrm{T}(\rho_0,\rho_1) - (\mathrm{Tr}(\hat{\Pi}_0\rho_0) - \mathrm{Tr}(\hat{\Pi}_0\rho_1))\right| \\
=\ &\left|\mathrm{Tr}\left(\mathrm{sgn}\Big(\frac{\rho_0-\rho_1}{2}\Big)\frac{\rho_0-\rho_1}{2}\right) - \mathrm{Tr}\left(P_{d'}^{\mathrm{sgn}}\Big(\frac{\rho_0-\rho_1}{2}\Big)\frac{\rho_0-\rho_1}{2}\right)\right| \\
\le\ &\sum_{j\in\Lambda_-} |\lambda_j \mathrm{sgn}(\lambda_j) - \lambda_j P_{d'}^{\mathrm{sgn}}(\lambda_j)| + \sum_{j\in\Lambda_0} |\lambda_j \mathrm{sgn}(\lambda_j) - \lambda_j P_{d'}^{\mathrm{sgn}}(\lambda_j)| + \sum_{j\in\Lambda_+} |\lambda_j \mathrm{sgn}(\lambda_j) - \lambda_j P_{d'}^{\mathrm{sgn}}(\lambda_j)| \\
\le\ &\sum_{j\in\Lambda_-} |\lambda_j| \cdot |-1 - P_{d'}^{\mathrm{sgn}}(\lambda_j)| + \sum_{j\in\Lambda_0} |\lambda_j \mathrm{sgn}(\lambda_j) - \lambda_j P_{d'}^{\mathrm{sgn}}(\lambda_j)| + \sum_{j\in\Lambda_+} |\lambda_j| \cdot |1 - P_{d'}^{\mathrm{sgn}}(\lambda_j)| \\
\le\ &\sum_{j\in\Lambda_-} |\lambda_j| C_{\mathrm{sgn}}\epsilon + \sum_{j\in\Lambda_0} 2|\lambda_j| + \sum_{j\in\Lambda_+} |\lambda_j| C_{\mathrm{sgn}}\epsilon \\
\le\ &2C_{\mathrm{sgn}}\epsilon + 2^{r+1}\delta.
\end{aligned}
$$

Here, the third line owes to the triangle inequality, the fourth line applies the sign

function, the fifth line is guaranteed by Corollary 5.8, and the last line is because $\sum_j |\lambda_j| = \mathrm{T}(\rho_0, \rho_1) \leq 1$ and $\mathrm{rank}\left(\frac{\rho_0-\rho_1}{2}\right)$ is at most 2^r. We then bound the error caused by space-efficient QSVT implementation in Corollary 5.17:

$$\begin{aligned}
&\left|\left(\mathrm{Tr}(\hat{\Pi}_0\rho_0) - \mathrm{Tr}(\hat{\Pi}_0\rho_1)\right) - \left(\mathrm{Tr}(\tilde{\Pi}_0\rho_0) - \mathrm{Tr}(\tilde{\Pi}_0\rho_1)\right)\right| \\
=&\left|\mathrm{Tr}\left(P_{d'}^{\mathrm{sgn}}\left(\frac{\rho_0-\rho_1}{2}\right)\frac{\rho_0-\rho_1}{2}\right) - \mathrm{Tr}\left((\langle\bar{0}|\otimes I_r)U_{\mathrm{HH}}(|\bar{0}\rangle\otimes I_r)\frac{\rho_0-\rho_1}{2}\right)\right| \\
\leq&\left\|P_{d'}^{\mathrm{sgn}}\left(\frac{\rho_0-\rho_1}{2}\right) - (\langle\bar{0}|\otimes I_r)U_{\mathrm{HH}}(|\bar{0}\rangle\otimes I_r)\right\| \cdot \mathrm{T}(\rho_0,\rho_1) \\
\leq&(36\hat{C}_{\mathrm{sgn}}+37)\epsilon\cdot 1.
\end{aligned}$$

Here, the third line is due to a matrix Hölder inequality (e.g., Corollary IV.2.6 in [Bha96]) and the last line is guaranteed by Corollary 5.17.

Combining the above error bounds caused by Corollary 5.8 and Corollary 5.17, respectively, we obtain the following under the aforementioned choice of parameters:

$$\begin{aligned}
&\left|\mathrm{T}(\rho_0,\rho_1) - (\mathrm{Tr}(\tilde{\Pi}_0\rho_0) - \mathrm{Tr}(\tilde{\Pi}_0\rho_1))\right| \\
\leq&\left|\mathrm{T}(\rho_0,\rho_1) - (\mathrm{Tr}(\hat{\Pi}_0\rho_0) - \mathrm{Tr}(\hat{\Pi}_0\rho_1))\right| + \left|(\mathrm{Tr}(\hat{\Pi}_0\rho_0) - \mathrm{Tr}(\hat{\Pi}_0\rho_1)) - (\mathrm{Tr}(\tilde{\Pi}_0\rho_0) - \mathrm{Tr}(\tilde{\Pi}_0\rho_1))\right| \\
\leq&\ 2C_{\mathrm{sgn}}\epsilon + 2^{r+1}\delta + (36\hat{C}_{\mathrm{sgn}}+37)\epsilon\cdot 1 \\
\leq&\ \varepsilon.
\end{aligned}$$

Complexity analysis. We complete the proof by analyzing the computational complexity of our algorithm. According to Corollary 5.17, our algorithm specified in Figure 6.3 requires $O(n)$ qubits and $O(d^2) \leq \widetilde{O}(2^{2r}/\varepsilon^2) \leq 2^{O(n)}$ queries to Q_0 and Q_1. In addition, the circuit description of our algorithm can be computed in deterministic time

$$\widetilde{O}(d^{9/2}/\varepsilon) = \widetilde{O}(2^{4.5r}/\varepsilon^{5.5}) \leq 2^{O(n)}. \qquad \square$$

6.3.2 A slightly improved upper bound for QSZK: Proof of Theorem 6.27

We start by presenting the quantum interactive proof protocol used in Theorem 6.27, as shown in Protocol 6.3.1. This protocol draws inspiration from [Wat02, Figure 2], and the honest prover now employs the algorithmic Holevo-Helstrom measurement $\{\tilde{\Pi}_0, \tilde{\Pi}_1\}$ from Theorem 6.26, rather than the optimal measurement $\{\Pi_0, \Pi_1\}$ in Equation (6.22) as per Theorem 3.12.

Protocol 6.3.1: Two-message protocol for GapQSD with a quantum linear-space prover.

1. The verifier V first chooses $b \in \{0,1\}$ uniformly at random. Subsequently, V applies Q_b to $|0^n\rangle$, and traces out all non-output qubits. The resulting state ρ_b in the remaining qubits is then sent to the prover P;
2. The prover $\mathcal{P}$ measures the received state ρ using the algorithmic Holevo-Helstrom measurement $\{\tilde{\Pi}_0, \tilde{\Pi}_1\}$ specified in Theorem 6.26. Let $\hat{b}$ be the measurement outcome, specifically, the outcome is $\hat{b}$ if the measurement indicates ρ is $\rho_{\hat{b}}$, with $\hat{b} \in \{0,1\}$. $\mathcal{P}$ then sends $\hat{b}$ to V;
3. The verifier V accepts if $b = \hat{b}$; otherwise V rejects.

Following that, we delve into the analysis of Protocol 6.3.1:

Proof of Theorem 6.27. Note that $\Pr\left[\hat{b}=a'|b=a\right]$ denotes the probability that the prover P uses a two-outcome measurement $\{\Pi_0',\Pi_1'\}$, which is arbitrary in general, to measure the state ρ_a, resulting in the measurement outcome a' for $a,a'\in\{0,1\}$. We then derive the corresponding acceptance probability of Protocol 6.3.1:

$$\Pr\left[b=\hat{b}\right]=\frac{1}{2}\Pr\left[\hat{b}=0|b=0\right]+\frac{1}{2}\Pr\left[\hat{b}=1|b=1\right]=\frac{1}{2}+\frac{1}{2}\Big(\mathrm{Tr}(\Pi_0'\rho_0)-\mathrm{Tr}(\Pi_0'\rho_1)\Big). \quad (6.23)$$

For *yes* instances where $\mathrm{T}(\rho_0,\rho_1)\geq\alpha(n)$, as the prover P is honest, we have

$$\begin{aligned}
&\Pr\left[b=\hat{b}\right]\\
=&\tfrac{1}{2}+\tfrac{1}{2}\Big(\mathrm{Tr}(\tilde{\Pi}_0\rho_0)-\mathrm{Tr}(\tilde{\Pi}_0\rho_1)\Big)\\
\geq&\tfrac{1}{2}+\tfrac{1}{2}\Big(\mathrm{Tr}(\Pi_0\rho_0)-\mathrm{Tr}(\Pi_0\rho_1)\Big)-\Big|\tfrac{1}{2}\Big(\mathrm{Tr}(\Pi_0\rho_0)-\mathrm{Tr}(\Pi_0\rho_1)\Big)-\tfrac{1}{2}\Big(\mathrm{Tr}(\tilde{\Pi}_0\rho_0)-\mathrm{Tr}(\tilde{\Pi}_0\rho_1)\Big)\Big|\\
=&\tfrac{1}{2}+\tfrac{1}{2}\mathrm{T}(\rho_0,\rho_1)-\Big|\tfrac{1}{2}\mathrm{T}(\rho_0,\rho_1)-\tfrac{1}{2}\Big(\mathrm{Tr}(\tilde{\Pi}_0\rho_0)-\mathrm{Tr}(\tilde{\Pi}_0\rho_1)\Big)\Big|\\
\geq&\tfrac{1}{2}+\tfrac{1}{2}\Big(\alpha(n)-2^{-n}\Big).
\end{aligned}$$

Here, the first line follows Equation (6.23), the second line owes to the triangle equality and the fact that $\mathrm{Tr}(\tilde{\Pi}_0\rho_0)-\mathrm{Tr}(\tilde{\Pi}_0\rho_1)>0$,[15] the third line is because of Theorem 3.12 and Equation (6.22), and the last line uses Theorem 6.26. Hence, we have the completeness $c(n)=\frac{1}{2}+\frac{1}{2}\Big(\alpha(n)-2^{-n}\Big)$.

For *no* instances where $\mathrm{T}(\rho_0,\rho_1)\leq\beta(n)$, we obtain the following from Equation (6.23):

$$\Pr\left[b=\hat{b}\right]=\frac{1}{2}+\frac{1}{2}\Big(\mathrm{Tr}(\Pi_0'\rho_0)-\mathrm{Tr}(\Pi_0'\rho_1)\Big)\leq\frac{1}{2}+\frac{1}{2}\mathrm{T}(\rho_0,\rho_1)\leq\frac{1}{2}\Big(1+\beta(n)\Big):=s(n).$$

Here, the first inequality is guaranteed by the Holevo-Helstrom bound (Theorem 3.12).

Therefore, since the honest prover (for *yes* instances) utilizes the algorithmic Holevo-Helstrom measurement $\{\tilde{\Pi}_0,\tilde{\Pi}_1\}$, the optimal prover strategy aligned with Protocol 6.3.1 is indeed implementable in quantum single-exponential time and linear space due to Theorem 6.26.

Error reduction for Protocol 6.3.1. Note that the class $\mathsf{QIP}(2)$ consists of two-message quantum interactive proof systems with completeness $c\geq 2/3$ and soundness $s\leq 1/3$ [JUW09, Section 3.1]. We aim to reduce the completeness and soundness errors in Protocol 6.3.1.

Following [JUW09, Section 3.2], we can achieve this task by a standard parallel repetition of Protocol 6.3.1. Specifically, we define new verifier V' and honest prover $\mathcal{P}'$ such that for any polynomial-bounded function $l(n)$, the resulting two-message quantum interactive proof system has completeness $c'(n)\geq 1-2^{-l(n)}$ and soundness $s'(n)\leq 2^{-l(n)}$. Let $c(n)-s(n)\geq 1/q(n)$ for some polynomially-bounded function q and define $[l]:=\{1,\cdots,l\}$, a description of V' follows:

(1) Let $t_0:=2lq$ and $t_1:=8lq^2t_0$. Run t_0t_1 independent and parallel executions of

[15] This is because the difference between $\mathrm{Tr}(\Pi_0\rho_0)-\mathrm{Tr}(\Pi_0\rho_1)$ and $\mathrm{Tr}(\tilde{\Pi}_0\rho_0)-\mathrm{Tr}(\tilde{\Pi}_0\rho_1)$ is much smaller than $\mathrm{Tr}(\Pi_0\rho_0)-\mathrm{Tr}(\Pi_0\rho_1)=\mathrm{T}(\rho_0,\rho_1)\geq\alpha(n)$, guaranteeing by the parameters chosen in Theorem 6.26.

Protocol 6.3.1 for V', one for each pair (i,j) with $i \in [t_0]$ and $j \in [t_1]$. Measure the output qubit for each execution, and let the measurement outcome for execution (i,j) be denoted by $y_{i,j} \in \{0,1\}$.

(2) For each $i \in [t_0]$, set $z_i := \begin{cases} 1, & \text{if } \sum_{j=1}^{t_1} y_{i,j} \geq t_1 \cdot \frac{c+s}{2} \\ 0, & \text{otherwise .} \end{cases}$

(3) V' accepts if $\wedge_{i=1}^{t_0} z_i = 1$; otherwise, it rejects.

The correctness of V' directly follows from [JUW09, Section 3.2].

We now analyze the complexity of the honest prover $\mathcal{P}'$. Since $t_0 t_1$ independent and parallel executions of Protocol 6.3.1 can be viewed as discriminating $t_0 t_1$ pairs of quantum states $(\rho_0^{(j)}, \rho_1^{(j)})$ for $1 \leq j \leq t_0 t_1$, the total input length of the quantum circuits to independently and parallelly prepare the states $\rho_b^{(1)}, \cdots, \rho_b^{(t_0 t_1)}$ for $b \in \{0,1\}$ is $n \cdot t_0 t_1 = 16nl^2(n)q^3(n) \leq O(n^\tau) := \hat{n}$ for some constant τ. Replacing n with $\mathit{hat}n$, the space complexity of the honest prover $\mathcal{P}'$ is still $O(\hat{n})$.

Lastly, we completely the proof by choosing an appropriate $l(n)$ such that the completeness $c(\hat{n}) \geq 1 - 2^{-l(\hat{n}^{1/\tau})} \geq 2/3$ and the soundness $s(\hat{n}) \leq 2^{-l(\hat{n}^{1/\tau})} \leq 1/3$ for sufficiently large n. □

6.4 Application: Space-bounded unitary quantum statistical zero-knowledge

In this section, we will introduce (honest-verifier) space-bounded unitary quantum statistical zero-knowledge, denoted as $\mathsf{QSZK_UL}$ and $\mathsf{QSZK_UL_{HV}}$, as specific types of space-bounded unitary quantum interactive proofs ($\mathsf{QIP_UL}$) that possess an additional statistical zero-knowledge property. Further characterizations of the space-bounded quantum interactive proofs can be found in [LLNW24].

Before presenting our results, we start by defining the promise problem IndivProdQSD, which is analogous to QSD [Wat02] and $\text{GapQSD}_{\log}$ (see Definition 6.9):

Definition 6.28 (Individual Product State Distinguishability, 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 $Q_1, \cdots, Q_k$ and $Q'_1, \cdots, Q'_k$ be polynomial-size unitary quantum circuits acting on $O(\log n)$ qubits, each with $r(n)$ specified output qubits. For $j \in [k]$, let σ_j and σ'_j denote the states obtained by running Q_j and Q'_j on the all-zero state $|\overline{0}\rangle$, respectively, and tracing out the non-output qubits, then the promise is that one of the following holds:*

- Yes: *Two k-tuples of quantum circuits $(Q_1, \cdots, Q_k)$ and $(Q'_1, \cdots, Q'_k)$ such that*
$$\mathrm{T}(\sigma_1 \otimes \cdots \otimes \sigma_k, \sigma'_1 \otimes \cdots \otimes \sigma'_k) \geq \alpha(n);$$
- No: *Two k-tuples of quantum circuits $(Q_1, \cdots, Q_k)$ and $(Q'_1, \cdots, Q'_k)$ such that*
$$\forall j \in [k], \quad \mathrm{T}\left(\sigma_j, \sigma'_j\right) \leq \delta(n).$$

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 6.29 (The equivalence of $\mathsf{QSZK_UL}$ and BQL)**.** *The following holds:*

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

$$\cup_{c(n)-s(n)\geq 1/\mathrm{poly}(n)} \mathsf{QSZK_UL_{HV}}[m, c, s] \subseteq \mathsf{BQL}.$$

(2) $\mathsf{BQL} \subseteq \mathsf{QSZK_UL} \subseteq \mathsf{QSZK_UL_{HV}}$.

The class $\mathsf{QSZK_UL}$ consists of space-bounded unitary quantum interactive proof systems that possess statistical zero-knowledge against *any* verifier, whereas QSZKL proof systems possess statistical zero-knowledge against only an *honest* verifier. Consequently, the inclusion in Theorem 6.29(2) is straightforward, following directly from these definitions. To establish the direction $\mathsf{QSZK_UL_{HV}} \subseteq \mathsf{BQL}$, we proceed by proving the following:

Theorem 6.30 ($\textsc{IndivProdQSD}$ is $\mathsf{QSZK_UL_{HV}}$-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 $3 \leq m(n) \leq \mathrm{poly}(n)$,*

$$\overline{\textsc{IndivProdQSD}}[m/2, \alpha, 2\delta] \text{ is } \mathsf{QSZK_UL_{HV}}[m, c, s]\text{-hard.}$$

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

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

$$\textsc{IndivProdQSD}[k, \alpha, \delta] \in \mathsf{BQL} \subseteq \mathsf{QSZK_UL_{HV}}.$$

In the remainder of this section, we first provide the definition of space-bounded unitary quantum interactive proofs, with useful results taken from [LLNW24]. We then provide the definition of honest-verifier space-bounded quantum statistical zero-knowledge proofs (the class $\mathsf{QSZK_UL_{HV}}$) in Section 6.4.2. Next, we establish that $\textsc{IndivProdQSD}$ is $\mathsf{QSZK_UL_{HV}}$-hard (Theorem 6.30(1)) in Section 6.4.3. Subsequently, we present the BQL upper bound for $\mathsf{QSZK_UL_{HV}}$ (Theorem 6.30(2)) in Section 6.4.4.

6.4.1 Definitions of space-bounded unitary quantum interactive proofs

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.

We introduce space-bounded *unitary* quantum interactive proof systems, denoted by $\mathsf{QIP_UL}$. The verifier has *direct access* to the messages exchanged during interactions, which limits each message size to $O(\log n)$. Additionally, the verifier's actions are implemented using space-bounded *unitary* quantum circuits.

Formal definition $\mathsf{QIP_UL}$. Given a promise problem $\mathcal{P} = (\mathcal{P}_{\mathrm{yes}}, \mathcal{P}_{\mathrm{no}})$, a quantum verifier is *logspace-computable* mapping V, where for each input string $x \in \mathcal{P} \subseteq \{0,1\}^*$, $V(x)$ is interpreted as an encoding of a $k(|x|)$-tuple $(V(x)_1, \cdots, V(x)_k)$ of quantum circuits.

These circuits represent the verifier's actions at each round of the proof system. Specifically, each $V(x)_j$ is a space-bounded *unitary* quantum circuit acting on two registers M and W, which hold $q_{\mathsf{M}}(|x|)$ and $q_{\mathsf{W}}(|x|)$ qubits, respectively. The total number of qubits satisfies $q_{\mathsf{M}}(|x|) + q_{\mathsf{W}}(|x|) \leq O(\log n)$, 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 $(V(x)_1, \cdots, V(x)_k)$.[16] 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.

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 $q_{\mathsf{M}}(|x|)$ 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 $x \in \mathcal{P}$ to an $l(|x|)$-tuple $(P(x)_1, \cdots, P(x)_l)$ 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 $q_{\mathsf{Q}}(|x|)$ and $q_{\mathsf{M}}(|x|)$ 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.

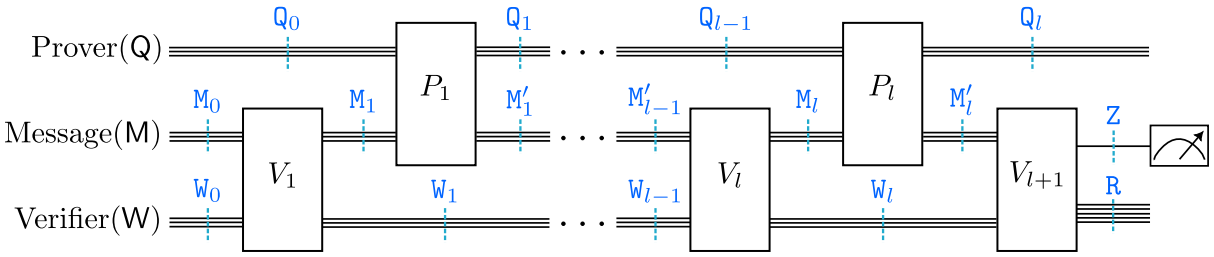

Figure 6.4: A $2l$-turn space-bounded quantum interactive proof system (with snapshots).

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

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

Without the loss of generality, we assume that the prover always sends the last message. See also Figure 6.4 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 $m(|x|)$.

[16] This uniformity requirement is slightly stronger and less general than merely requiring all quantum circuits $V(x)_1, \cdots, V(x)_k$ 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 a polynomial-time deterministic Turing machine would suffice).

Assuming the mapping $V(x) = (V(x)_1, \cdots, V(x)_k)$ in a $\mathsf{QIP}_{\mathrm{U}}\mathsf{L}$ proof system is a collection of unitary quantum circuits,[17] the state of the qubits in the circuit $P \rightleftharpoons V$ is a *pure state* on the registers $(\mathsf{Q}, \mathsf{M}, \mathsf{V})$ after the verifier's j-th action. 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 $(P \rightleftharpoons V)(x)|\bar{0}\rangle_{\mathsf{Q}}|\bar{0}\rangle_{\mathsf{M}}|\bar{0}\rangle_{\mathsf{W}}$ in the computational basis yields the outcome 1.

Let $\omega(V)$ denote the maximum acceptance probability of the verifier V in the proof system $P \rightleftharpoons V$. We are now ready to define space-bounded unitary quantum interactive proof systems:

Definition 6.31 (Space-bounded unitary quantum interactive proofs, $\mathsf{QIP}_{\mathrm{U}}\mathsf{L}$)**.** *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 $1 \leq m(n) \leq \mathrm{poly}(n)$. A promise problem $\mathcal{P} = (\mathcal{P}_{\mathrm{yes}}, \mathcal{P}_{\mathrm{no}})$ is in $\mathsf{QIP}_{\mathrm{U}}\mathsf{L}_m[c, s]$, if there exists an $m(n)$-turn logspace-computable* unitary *quantum verifier V such that*:

- **Completeness**. *For any $x \in \mathcal{P}_{\mathrm{yes}}$, there is an $m(n)$-message prover P such that*
$$\omega(V) \geq c(n).$$
- **Soundness**. *For any $x \in \mathcal{P}_{\mathrm{no}}$ and any $m(n)$-message prover P,*
$$\omega(V) \leq s(n).$$

Furthermore, we define $\mathsf{QIP}_{\mathrm{U}}\mathsf{L}_m := \mathsf{QIP}_{\mathrm{U}}\mathsf{L}_m[2/3, 1/3]$ and $\mathsf{QIP}_{\mathrm{U}}\mathsf{L} := \cup_{m \leq \mathrm{poly}(n)} \mathsf{QIP}_{\mathrm{U}}\mathsf{L}_m$.

In addition to the formal definition, as established in [LLNW24], $\mathsf{QIP}_{\mathrm{U}}\mathsf{L}$ admits error reduction based through sequential repetition:

Lemma 6.32 (Error reduction for $\mathsf{QIP}_{\mathrm{U}}\mathsf{L}$)**.** *Let $c(n)$, $s(n)$, and $m(n)$ be logspace-computable functions such that $0 \leq s(n) < c(n) \leq 1$, $c(n) - s(n) \geq 1/\mathrm{poly}(n)$, and $1 \leq m(n) \leq \mathrm{poly}(n)$. For any polynomial $k(n)$, it holds that*
$$\mathsf{QIP}_{\mathrm{U}}\mathsf{L}_m[c, s] \subseteq \mathsf{QIP}_{\mathrm{U}}\mathsf{L}_{m'}\left[1, 2^{-k}\right].$$
Here, the number of turns $m' := O\left(km/\log \frac{1}{1-(c-s)^2/2}\right)$.

6.4.2 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 6.4.1, that satisfies an additional *zero-knowledge* property. Intuitively, the zero-knowledge property in $\mathsf{QIP}_{\mathrm{U}}\mathsf{L}$ proof systems requires that, after each message is sent, the quantum states representing the verifier's view – including snapshot states in the message register M and the verifier's private register W – should be approximately indistinguishable by a space-bounded unitary quantum circuit on accepted inputs.

[17] This assumption about the verifier's actions is crucial for adapting several techniques from standard quantum interactive proofs. For further details, see [VW16, Section 4.1.4].

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 $S_x := (S_{x,1}, \cdots, S_{x,m})$, where each $S_{x,i}$ for $i \in [m]$ is a space-bounded unitary quantum circuit (see Definition 2.1) 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 $\{S_x\}_{x\in\mathcal{P}}$ as the *space-bounded simulator* for the promise problem $\mathcal{P}$.

Next, for any space-bounded quantum interactive proof system $P \rightleftharpoons V$, we define the verifier's view after the i-th turn, denoted by $\mathtt{view}_{P\rightleftharpoons V}(x, i)$, as the reduced state in registers (M, 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 6.33 (Honest-verifier space-bounded unitary quantum statistical zero-knowledge, $\mathsf{QSZK_UL_{HV}}$)**.** *Let $c(n)$, $s(n)$, and $m(n)$ be logspace-computable functions of the input length $n := |x|$ such that $0 \le s(n) < c(n) \le 1$ and $1 \le m(n) \le \mathrm{poly}(n)$. A promise problem $\mathcal{P} = (\mathcal{P}_{\mathrm{yes}}, \mathcal{P}_{\mathrm{no}})$ is in $\mathsf{QSZK_UL_{HV}}[m, c, s]$, if there exists an $m(n)$-message space-bounded unitary quantum interactive proof system $(P \rightleftharpoons V)(x)$ such that*:

- **Completeness**. *For any $x \in \mathcal{P}_{\mathrm{yes}}$, there is an $m(n)$-message prover P such that*
$$\Pr\,(P \rightleftharpoons V)(x) \text{ accepts} \ge c(n).$$
- **Soundness**. *For any $x \in \mathcal{P}_{\mathrm{no}}$ and any $m(n)$-message prover P,*
$$\Pr\,(P \rightleftharpoons V)(x) \text{ accepts} \le s(n).$$
- **Zero-knowledge**. *There exists a space-bounded simulator $\{S_x\}_{x\in\mathcal{P}}$ and a negligible function $\delta(n)$ such that for any $x \in \mathcal{P}_{\mathrm{yes}}$ and each message $i \in [m]$, the circuit $S_x(i)$ produces the corresponding state $\sigma_{x,i}$ satisfying*
$$\mathrm{T}(\sigma_{x,i}, \mathtt{view}_{P\rightleftharpoons V}(x, i)) \le \delta(n).$$

We define $\mathsf{QSZK_UL_{HV}}[m] := \mathsf{QSZK_UL_{HV}}\left[m, \frac{2}{3}, \frac{1}{3}\right]$ *and* $\mathsf{QSZK_UL_{HV}} := \cup_{m\le \mathrm{poly}(n)} \mathsf{QSZK_UL_{HV}}[m]$.

Since the inequality condition in the zero-knowledge property holds independently for each message in Definition 6.33, error reduction via sequential repetition (Lemma 6.32) directly applies to an honest-verifier space-bounded quantum statistical zero-knowledge proof system, with the zero-knowledge property automatically preserved.

Remark 6.34 (Robustness of the zero-knowledge property in $\mathsf{QSZK_UL_{HV}}$). Let $\mathsf{QSZK_UL^\star_{HV}}$ denote a weaker version of $\mathsf{QSZK_UL_{HV}}$, where the threshold function
$$\delta(n) := \left(\sqrt{c} - \sqrt{s}\right)^2 / \left(2m^2\right),$$ [18]
rather than being negligible. While it is clear that $\mathsf{QSZK_UL_{HV}} \subseteq \mathsf{QSZK_UL^\star_{HV}}$, the standard approach to establish the reverse direction does not apply to $\mathsf{QSZK_UL_{HV}}$.[19] Instead, the inclusion $\mathsf{QSZK_UL^\star_{HV}} \subseteq \mathsf{QSZK_UL_{HV}}$ only follows from $\mathsf{QSZK_UL^\star_{HV}} = \mathsf{BQL}$ (Theorem 6.29).

[18] This bound results from the reduction to the $\mathsf{QSZK_UL_{HV}}$-hard problem IndivProdQSD, see Theorem 6.35.

[19] 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.

6.4.3 $\overline{\text{IndivProdQSD}}$ is $\mathsf{QSZK_UL_{HV}}$-hard

Instead of directly proving that $\overline{\text{IndivProdQSD}}$ is $\mathsf{QSZK_UL_{HV}}$-hard, we establish a slightly stronger result: the promise problem $\overline{\text{IndivProdQSD}}$ is hard for the class $\mathsf{QSZK_UL^\star_{HV}}$ that contains $\mathsf{QSZK_UL_{HV}}$ (Remark 6.34), as detailed in Theorem 6.35. This result mirrors the relationship between $\overline{\text{QSD}}$ and the class QSZK.

Theorem 6.35 ($\overline{\text{IndivProdQSD}}$ is $\mathsf{QSZK_UL^\star_{HV}}$-hard)**.** *Let $c(n)$, $s(n)$, and $m(n)$ be logspace computable functions such that $0 \le s(n) < c(n) \le 1$, $c(n) - s(n) \ge 1/\mathrm{poly}(n)$, and $3 \le m(n) \le \mathrm{poly}(n)$.*[20] *Then, it holds that*

$$\overline{\text{IndivProdQSD}}[\lceil m(n)/2 \rceil, \alpha(n), 2\delta(n)] \text{ is } \mathsf{QSZK_UL^\star_{HV}}[m(n), c(n), s(n)]\text{-hard.}$$

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 $\mathcal{P} \in \mathsf{QSZK_UL^\star_{HV}}[m(n), c(n), s(n)]$ 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. Additionally, we adopt the notations introduced in Figure 6.4 and [LLNW24, Section 3.2].

We now focus on the space-bounded simulator $\{S_x\}_{x\in\mathcal{P}}$. Let $\xi'_0, \cdots, \xi'_l$ and $\xi_1, \cdots, \xi_{l+1}$ denote the simulator's approximation to the reduced snapshot states in registers (M, W) after the $(2j-1)$-st and the $(2j)$-th turn, respectively, during the execution of $P \rightleftharpoons V$, as specified in Figure 6.5. 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 ξ_{l+1} satisfies $\mathrm{Tr}(|1\rangle\langle 1|_{\mathsf{Z}}\xi_{l+1}) = c(n)$ for *all* instances.

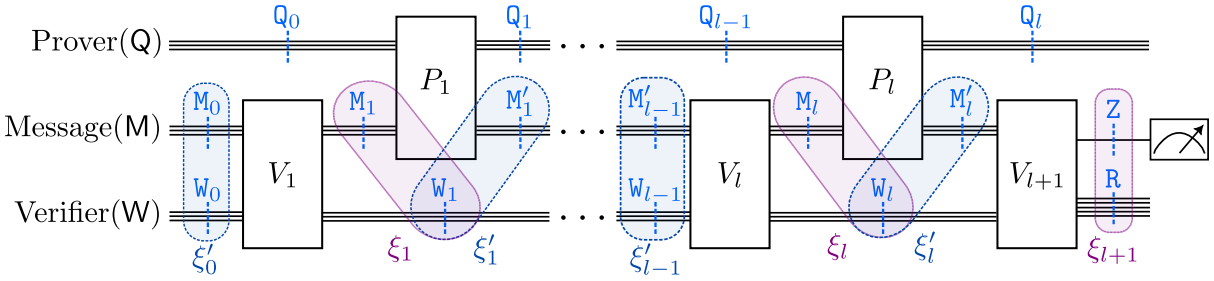

Figure 6.5: Quantum states $\xi'_0, \cdots, \xi'_l$ and $\xi, \cdots, \xi_{l+1}$ prepared by the simulator.

In addition, given that the verifier is always assumed to act honestly, we can take[21]

$$\xi'_0 = (|0\rangle\langle 0|)^{\otimes(q_{\mathsf{M}}+q_{\mathsf{W}})} \text{ and } \xi_j = V_j \xi'_{j-1} V_j^\dagger \text{ for } j \in [l+1]. \tag{6.24}$$

Proof intuition. Notably, the space-bounded simulator $\{S_x\}_{x\in\mathcal{P}}$ essentially produces an approximation solution, in the form of snapshot states, to the SDP program (see Equation 3.2 in [LLNW24]) for computing the maximum acceptance probability $\omega(V)$ of

[20] Without loss of generality, we can assume that $m \ge 3$ by adding one or two dummy messages when $m < 3$, as discussed in Footnote 22.

[21] Hence, the simulator only needs to prepare ξ'_{j-1}, since ξ_j is obtained by applying V_j to this state.

the space-bounded unitary quantum interactive proof systems $P \rightleftharpoons V$ for $\mathcal{P} \in \mathsf{QIP}_{\mathrm{U}}\mathsf{L}$. As presented in the proof of [LLNW24, Lemma 3.9], there are only two types of constraints, in particular: (1) Verifier's actions are honest; and (2) Prover's actions do not affect the verifier's private qubits.

As mentioned in Equation (6.24), 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 6.5:

$$\mathrm{Tr}_{\mathsf{M}}(\xi_1) \otimes \cdots \otimes \mathrm{Tr}_{\mathsf{M}}(\xi_l) \text{ and } \mathrm{Tr}_{\mathsf{M}}(\xi'_1) \otimes \cdots \otimes \mathrm{Tr}_{\mathsf{M}}(\xi'_l). \tag{6.25}$$

For *yes* instances, the zero-knowledge property ensures a component-wise closeness bound $\mathrm{Tr}_{\mathsf{M}}(\xi_j) \approx \mathrm{Tr}_{\mathsf{M}}(\xi'_j)$ for $j \in [l]$. For *no* instances, we need to show that the two states in Equation (6.25) 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 6.35.1 (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 $\xi'_0, \cdots, \xi'_l$ and $\xi_k, \cdots, \xi_{l+1}$ be the states produced by the simulators as defined in Figure 6.5. Assume that $\mathrm{Tr}\left(|\bar{0}\rangle\langle\bar{0}|_{\mathsf{M}_0\mathsf{W}_0}\xi'_0\right) = 1$ and $\mathrm{Tr}(|1\rangle\langle 1|_{\mathsf{Z}}\xi_{l+1}) = c$. Then, it holds that*

$$\mathrm{T}(\mathrm{Tr}_{\mathsf{M}}(\xi_1) \otimes \cdots \otimes \mathrm{Tr}_{\mathsf{M}}(\xi_l), \mathrm{Tr}_{\mathsf{M}}(\xi'_1) \otimes \cdots \otimes \mathrm{Tr}_{\mathsf{M}}(\xi'_l)) \geq \frac{(\sqrt{c} - \sqrt{s})^2}{4(l-1)}.$$

Then, we proceed with the formal proof of Theorem 6.35:

Proof of Theorem 6.35. Let $P \rightleftharpoons V$ be an $m(n)$-turn honest-verifier unitary quantum statistical zero-knowledge proof system for a promise problem $\mathcal{P} \in \mathsf{QSZKL}^{\star}_{\mathrm{HV}}[m, c, s]$, with completeness $c(n)$ and soundness $s(n)$. Without loss of generality, we assume that m is even for all $x \in \mathcal{P}$.[22] Hence, we can denote the verifier's actions by $V_1, \cdots, V_{l+1}$ for $l = m/2$, and the verifier initiates the protocol. Let $\{\sigma_{x,i}\}_{x\in\mathcal{P}, i\in[m+2]}$ represent the mixed states produced by the simulator $\{S_x\}_{x\in\mathcal{P}}$, with the threshold function $\delta(n) := 1/m(n)^2$. For any $x \in \mathcal{P}$, we can define states $\xi'_0, \cdots, \xi'_l$ and $\xi_1, \cdots, \xi_{l+1}$ as illustrated in Figure 6.5:

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

$$\forall x \in \mathcal{P}_{\mathrm{yes}}, \quad \mathrm{T}(\sigma_{x,2j-1}, \mathtt{view}_{P\rightleftharpoons V}(x, 2j)) = \mathrm{T}\left(\sigma_{x,2j-1}, \rho_{\mathsf{M}_j\mathsf{W}_j}\right) \leq \delta(n). \tag{6.26}$$

- $(2j+1)$-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

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

Let $Q_1, \cdots, Q_k$ and $Q'_1, \cdots, Q'_k$ 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

[22] More specifically, 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.

qubits are qubits in the verifier's private register W. It is evident that Q_j and Q'_j prepare the states $\mathrm{Tr}_{\mathsf{M}}(\xi_j)$ and $\mathrm{Tr}_{\mathsf{M}}\left(\xi'_j\right)$, respectively. We claim that the l-tuples $(Q_1, \cdots, Q_l)$ and $(Q'_1, \cdots Q'_l)$ form an instance of $\overline{\textsc{IndivProdQSD}}[l(n), \alpha(n), \delta'(n)]$, satisfying the following conditions:

$$\forall x \in \mathcal{P}_{\text{yes}}, \qquad \mathrm{T}\left(\mathrm{Tr}_{\mathsf{M}}(\xi_j), \mathrm{Tr}_{\mathsf{M}}\left(\xi'_j\right)\right) \leq 2\delta = \frac{(\sqrt{c}-\sqrt{s})^2}{4l^2} := \delta' \text{ for } j \in [l]; \quad (6.27)$$

$$\forall x \in \mathcal{P}_{\text{no}}, \quad \mathrm{T}(\mathrm{Tr}_{\mathsf{M}}(\xi_1)\otimes\cdots\otimes\mathrm{Tr}_{\mathsf{M}}(\xi_l), \mathrm{Tr}_{\mathsf{M}}(\xi'_1)\otimes\cdots\otimes\mathrm{Tr}_{\mathsf{M}}(\xi'_l)) \geq \frac{(\sqrt{c}-\sqrt{s})^2}{4(l-1)} := \alpha. \quad (6.28)$$

By substituting Equation (6.27) into Lemma 3.13, it follows that:

$$\begin{aligned} \mathrm{T}(\mathrm{Tr}_{\mathsf{M}}(\xi_1) \otimes \cdots \otimes \mathrm{Tr}_{\mathsf{M}}(\xi_l), \mathrm{Tr}_{\mathsf{M}}(\xi'_1) \otimes \cdots \otimes \mathrm{Tr}_{\mathsf{M}}(\xi'_l)) &\leq \sum_{j\in[l]} \mathrm{T}\left(\mathrm{Tr}_{\mathsf{M}}(\xi_j), \mathrm{Tr}_{\mathsf{M}}\left(\xi'_j\right)\right) \\ &\leq \frac{(\sqrt{c}-\sqrt{s})^2}{4l}. \end{aligned} \quad (6.29)$$

Consequently, by comparing Equations (6.27) to (6.29), we can conclude the parameter requirement of $\overline{\textsc{IndivProdQSD}}[l(n), \alpha(n), \delta'(n)]$, specifically that

$$\alpha(n) - \delta'(n) \cdot l(n) \geq 1/\mathrm{poly}(n).$$

It remains to establish Equation (6.27) and Equation (6.28). The latter follows directly from Proposition 6.35.1. 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 $j \in \{2, \cdots, l\}$:

$$\begin{aligned} \mathrm{T}\left(\mathrm{Tr}_{\mathsf{M}}(\xi_j), \mathrm{Tr}_{\mathsf{M}}\left(\xi'_j\right)\right) &\leq \mathrm{T}\left(\xi_j, \xi'_j\right) \\ &\leq \mathrm{T}\left(\xi_j, \rho_{\mathtt{M}_j\mathtt{W}_j}\right) + \mathrm{T}\left(\rho_{\mathtt{M}_j\mathtt{W}_j}, \rho_{\mathtt{M}'_j\mathtt{W}_j}\right) + \mathrm{T}\left(\rho_{\mathtt{M}'_j\mathtt{W}_j}, \xi'_j\right) \\ &= \mathrm{T}\left(\xi'_{j-1}, \rho_{\mathtt{M}'_{j-1}\mathtt{W}_{j-1}}\right) + \mathrm{T}\left(\rho_{\mathtt{M}_j\mathtt{W}_j}, \rho_{\mathtt{M}'_j\mathtt{W}_j}\right) + \mathrm{T}\left(\rho_{\mathtt{M}'_j\mathtt{W}_j}, \xi'_j\right) \\ &\leq \delta(n) + 0 + \delta(n) \\ &= 2\delta(n). \end{aligned}$$

Here, the first line follows from the data-process inequality (Lemma 3.14), the second line is due to the triangle inequality, the third line owes to the unitary invariance (Lemma 3.15) and the fact that $\rho_{\mathtt{M}_j\mathtt{W}_j} = V_j\rho_{\mathtt{M}'_{j-1}\mathtt{W}_{j-1}}V_j^\dagger$, and the fourth line is because of Equation (6.26). We complete the proof by noting that similar reasoning applies to the case of $j = 1$, using $\mathrm{T}(\xi_1, \rho_{\mathtt{M}_1\mathtt{W}_1}) = 0$ instead of at most $\delta(n)$. □

6.4.4 $\mathsf{QSZK}_{\mathrm{U}}\mathsf{L}_{\mathrm{HV}}$ is in BQL

We will establish the hard direction in the equivalence of $\mathsf{QSZK}_{\mathrm{U}}\mathsf{L}_{\mathrm{HV}}$ and BQL. The key lemma underlying the proof involves a logspace (many-to-one) reduction IndivProdQSD to an "existential" version of $\textsc{GapQSD}_{\log}$, where $\textsc{GapQSD}_{\log}$ is a BQL-complete problem (see Section 6.2). This reduction leads to a BQL containment of IndivProdQSD:

Lemma 6.36 (IndivProdQSD is in BQL)**.** *Let $k(n)$, $\alpha(n)$ and $\delta(n)$ be logspace computable functions such that $1 \leq k(n) \leq \mathrm{poly}(n)$, $0 \leq \alpha(n), \delta(n) \leq 1$, and $\alpha(n) - \delta(n) \cdot$*

$k(n) \geq 1/\mathrm{poly}(n)$. *Then, it holds that*

$$\textsc{IndivProdQSD}[k(n), \alpha(n), \delta(n)] \in \mathsf{BQL}.$$

As $\overline{\textsc{IndivProdQSD}}$ is $\mathsf{QSZK_UL_{HV}}$-hard (Theorem 6.35), and given that $\mathsf{BQ_UL}$ is closed under complement [Wat99, Corollary 4.8] and the equivalence $\mathsf{BQL} = \mathsf{BQ_UL}$ [FR21], we can directly conclude the following corollary:

Corollary 6.37. $\mathsf{QSZK_UL_{HV}} \subseteq \mathsf{BQL}$.

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

Proof of Lemma 6.36. We first establish a logspace (many-to-one) reduction from IndivProdQSD to an "existential" version of $\textsc{GapQSD}_{\log}$. Let $(Q_1, \cdots, Q_k)$ and $(Q'_1, \cdots, Q'_k)$ be an instance of $\textsc{IndivProdQSD}[k, \alpha, \delta]$. For each $j \in [k]$, let σ_j and σ'_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 (6.30) and Equation (6.31) holds:

$$\mathrm{T}(\sigma_1 \otimes \cdots \otimes \sigma_k, \sigma'_1 \otimes \cdots \otimes \sigma'_k) \geq \alpha(n). \tag{6.30}$$

$$\forall j \in [k], \quad \mathrm{T}\left(\sigma_j, \sigma'_j\right) \leq \delta(n). \tag{6.31}$$

By combining Lemma 3.13 with Equation (6.30), we obtain:

$$\sum_{j \in [k]} \mathrm{T}\left(\sigma_j, \sigma'_j\right) \geq \mathrm{T}(\sigma_1 \otimes \cdots \otimes \sigma_k, \sigma'_1 \otimes \cdots \otimes \sigma'_k) \geq \alpha(n). \tag{6.32}$$

Applying an averaging argument to Equation (6.32), we can conclude that

$$\exists j \in [k], \quad \mathrm{T}\left(\sigma_j, \sigma'_j\right) \geq \alpha/k. \tag{6.33}$$

Clearly, a violation of Equation (6.33) implies a violation of Equation (6.30), without contradicting Equation (6.31). For each $j \in [k]$, the pair of circuits Q_j and Q'_j forms an instance of $\textsc{GapQSD}_{\log}$. The resulting promise problem is thus an "existential" version of $\textsc{GapQSD}_{\log}$, where *yes* instances satisfy Equation (6.33) and *no* instances satisfy Equation (6.31).

Next, we proceed by showing the BQL containment. Given the equivalence of BQL and QMAL [FKL+16, FR21], it remains to establish a QMAL containment of this "existential" version of $\textsc{GapQSD}_{\log}$. The verification protocol is outlined in Algorithm 6.4.1.

Protocol 6.4.1: A QMAL proof system for IndivProdQSD.

1. The verifier receives an index $j \in [k]$ from the prover.
2. The verifier executes the quantum logspace algorithm $\mathcal{A}$ for $\textsc{GapQSD}_{\log}[\alpha/k, \delta]$ underlying in Theorem 6.14, using the pair of circuits Q_j and Q'_j as the $\textsc{GapQSD}_{\log}$ instance. The verifier accepts (or rejects) if $\mathcal{A}$ accepts (or rejects).

To complete the proof, we establish the correctness of Algorithm 6.4.1. Since the algorithm $\mathcal{A}$ is a BQL containment of $\textsc{GapQSD}_{\log}[\alpha/k, \delta]$ (Theorem 6.14), we conclude the following:

- For *yes* instances, Equation (6.33) ensures that there exists an $j \in [k]$ (the witness) such that $\mathrm{T}\Big(\sigma_j, \sigma'_j\Big) \geq \alpha/k$. Consequently, $\mathcal{A}$ accepts with probability at least 2/3.
- For *no* instances, Equation (6.31) yields that for all $j \in [k]$, $\mathrm{T}\Big(\sigma_j, \sigma'_j\Big) \leq \delta$. This statement implies that $\mathcal{A}$ accepts with probability at most 1/3. □

Chapter 7

Quantum state testing beyond the polarizing regime

7.1 Introduction

This chapter focuses on improving the QSZK containment regime for the time-bounded state testing problem with respect to the trace distance (Quantum State Distinguishability, QSDP). For a brief overview of time-bounded distribution and state testing problems, such as the time-bounded distribution testing problem with respect to the total variation distance (Statistical Difference, SDP), see Section 1.1.

Error reduction for SDP$[\alpha, \beta]$, referred to as the *polarization lemma* [SV03], polarizes the total variation distance between two classical probability distributions. Put it differently, for any constants α and β satisfying $\alpha^2 > \beta$, the lemma constructs new distributions such that they are either very far apart (approaching 1) for *yes* instances or very close (approaching 0) for *no* instances, thereby reducing errors on both sides.

By employing the polarization lemma, the SZK containment of SDP$[\alpha, \beta]$ in the regime where $\alpha^2 > \beta$, denoted as the *constant polarizing regime*, is established in [SV03]. Furthermore, an analog of the direct product lemma for the Hellinger affinity leads to error reduction for StoqMA when the error for *yes* instances is negligible [Liu21].

Sahai and Vadhan left an open problem concerning reducing error parameters α and β beyond the constant polarizing regime, specifically considering the *non-polarizing regime* where $\alpha > \beta > \alpha^2$. This challenge also extends to the quantum counterpart (QSDP). Recently, Berman, Degwekar, Rothblum, and Vasudevan [BDRV19] made significant progress in addressing this problem by examining the limitations of existing polarization approaches. As a result, they extended the SZK containment of SDP beyond the constant polarizing regime:[1]

Theorem 7.1 (Informal of [BDRV19])**.** *The* SZK *containment of* SDP$[\alpha, \beta]$ *holds for the following parameter regimes*:

(1) $\alpha^2(n) - \beta(n) \geq 1/\mathrm{poly}(n)$*;*

(2) (α, β) *in the non-polarizing regime where* $\alpha > \beta > \alpha^2$*, provided that* $\alpha(n) - \beta(n) \geq$

[1] As indicated in [BDRV19], SDP is in SZK for $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$ by inspecting the construction in [SV03].

$1/\mathrm{poly}(n)$ *and certain criteria on the total variation distance* (TV) *and the triangular discrimination* (TD). *Specifically, two pairs of distributions* (p_0, p_1) *and* (p_0', p_1') *satisfy the following conditions*

$$\mathrm{TV}(p_0, p_1) > \mathrm{TV}(p_0', p_1') > \mathrm{TV}^2(p_0, p_1) \text{ and } \mathrm{TD}(p_0, p_1) > \mathrm{TD}(p_0', p_1').$$

The proof of Theorem 7.1 involves a series of tailored reductions to two time-bounded distribution testing problems: the Jensen-Shannon Divergence Problem (JSP) and the Triangular Discrimination Problem (TDP). These distances are important because they capture the limitation of two known approaches to polarization:

- The original polarization approach [SV03] reduces errors alternately for *yes* instances (via the direct product lemma, which drives the distance toward 1) and *no* instances (via the XOR lemma, which drives the distance toward 0). This approach is fully characterized by the triangular discrimination [BDRV19], as $\mathrm{TDP}[\alpha, \beta]$ is in SZK for the natural parameter regime with *logarithmic* precision, satisfying
$$\alpha(n) - \beta(n) \geq 1/O(\log n).$$
- The entropy extraction approach [GSV99] (see also [GV99]) is designed for scenarios in which one of the two probability distributions is guaranteed to be uniform and remains so throughout. This approach relies fundamentally on the Jensen-Shannon divergence, which serves as a distance version of entropy difference. This connection arises from interpreting the Jensen-Shannon divergence as the (conditional) entropy difference, as noted implicitly in [Vad99]. Consequently, $\mathrm{JSP}[\alpha, \beta]$ is in SZK for the natural parameter regime with *polynomial* precision, satisfying
$$\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n).$$

This work explores a similar challenge in the quantum world. While classical distances (more formally, classical closeness measures) often have multiple quantum counterparts, the trace distance *uniquely* serves as the quantum analog of the total variation distance. Consequently, the polarization lemma extends almost directly to the trace distance, as noted in [Wat02]. In contrast, quantum counterparts of the Jensen-Shannon divergence and the triangular discrimination – key tools for examining the limitations of existing techniques in polarizing quantum distances – either have several choices or have not been defined yet. Defining *proper* quantum analogs for JSP and TDP is therefore a nontrivial task, as these analogs may exhibit behavior distinct from their classical counterparts.

7.1.1 Main results

Quantum state testing beyond the constant polarizing regime. We introduce two time-bounded state testing problems: the Quantum Jensen-Shannon Divergence Problem (QJSP) and the Measured Quantum Triangular Discrimination Problem (measQTDP). QJSP is based on the quantum Jensen-Shannon divergence defined in [MLP05], while measQTDP involves a quantum analog of the triangular discrimination, which will be described later. The QSZK containments of these problems, as stated in Theorem 7.2, lead to improved QSZK containments of QSDP:[2]

[2]The reader may feel confused with [VW16, Theorem 5.4] on the QSZK containment of QSDP which builds upon adapting techniques in [SV03]. However, it was claimed in [GV11] that the proof in [SV03]

Theorem 7.2 (Improved QSZK containments of QSDP, informal)**.** *For time-bounded state testing problems with respect to the quantum Jensen-Shannon divergence and the measured triangular discrimination problem, specifically* QJSP *and* measQTDP*, the following holds, where n denotes the number of qubits used by the states ρ_0 and ρ_1:*

(1) $\mathrm{QJSP}[\alpha, \beta]$ *is in* QSZK *if* $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$.
Consequently, $\mathrm{QSDP}[\alpha, \beta]$ *is in* QSZK *if* $\alpha^2(n) - \sqrt{2 \ln 2}\beta(n) \geq 1/\mathrm{poly}(n)$.

(2) $\mathrm{measQTDP}[\alpha, \beta]$ *is in* QSZK *if* $\alpha(n) - \beta(n) \geq 1/O(\log n)$.
This containment further implies that $\mathrm{QSDP}[\alpha, \beta]$ *is in* QSZK *for certain instances where* $\alpha^2 \leq \beta \leq \alpha$ *and* $\alpha(n) - \beta(n) \geq 1/O(\log n)$*. Specifically, for two pairs of states* (ρ_0, ρ_1) *and* (ρ'_0, ρ'_1)*, the following conditions hold:*[3]

$$\mathrm{T}(\rho_0, \rho_1) > \mathrm{T}(\rho'_0, \rho'_1) > \mathrm{T}^2(\rho_0, \rho_1) \text{ and } \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) > \mathrm{QTD}^{\mathrm{meas}}(\rho'_0, \rho'_1).$$

Furthermore, both QJSP *and* measQTDP *are* QSZK*-complete.*

Importantly, our definitions of measQTDP and QJSP serve as *proper* quantum analogs of TDP and JSP, respectively. The measured quantum triangular discrimination exposes the limitation of the original polarization lemma approach [SV03, Wat02], achieving a *quadratic* improvement in the direct product lemma (Lemma 7.29) and resulting in an improved QSZK containment under the natural parameter regime with logarithmic precision. In contrast, another quantum analog, QTD, exhibits *no* improvement over the trace distance scenario.

Our reductions used to establish that QJSP is QSZK-complete also provide a simple QSZK-hardness proof for the Quantum Entropy Difference Problem (QEDP) introduced in [BASTS10], as stated in Corollary 7.21. Consequently, the quantum Jensen-Shannon divergence captures the limitation of the quantum entropy extraction approach to polarization [BASTS10]. However, our result, stated in Theorem 7.2(1), is slightly weaker than the classical counterpart described in Theorem 7.1(1). This difference arises from the *distinct* behaviors exhibited by quantum analogs of the triangular discrimination compared to their classical equivalent.

Easy regimes for the class QSZK. The existence of an oracle separating SZK from PP, as provided in [BCH+19], highlights the difficulty of establishing SZK-hardness of SDP instances that are contained in PP (referred to as the *easy regime*). This challenge is due to the need for non-black-box techniques. When the error parameter ϵ is at most some inverse-exponential, $\mathrm{SDP}[1-\epsilon, \epsilon]$ is in PP. Let $\overline{\mathrm{QSDP}}$ and $\overline{\mathrm{SDP}}$ denote the complement of QSDP and SDP, respectively. We establish a similar result for $\mathrm{QSDP}[1-\epsilon, \epsilon]$, where these instances become even easier to solve when error-free:

Theorem 7.3 (Easy regimes for QSZK, informal)**.** *Let $\epsilon(n)$ be an error parameter satisfying $\epsilon(n) \leq 2^{-n/2-1}$. Then, the following holds*:

$$\overline{\mathrm{QSDP}}[1-\epsilon, \epsilon] \text{ is in } \mathsf{PP}.$$

does extend to the parameter regime of $\alpha^2(n) - \beta(n) \geq 1/\mathrm{poly}(n)$, but this claim was later retracted, see [Gol19].

[3] If $\frac{\rho_0+\rho_1}{2}$ is diagonal of full rank (see Footnote 7), it is fairly effortless to find examples by numerical simulations. For instance, (ρ_0, ρ_1) where $\rho_0 = \frac{1}{2}(I + \frac{\sigma_X}{7} + \frac{\sigma_Y}{3} + \frac{\sigma_Z}{4})$ and $\rho_1 = \frac{1}{2}(I - \frac{\sigma_X}{7} - \frac{\sigma_Y}{3} - \frac{\sigma_Z}{4})$, together with (ρ'_0, ρ'_1) where $\rho'_0 = \frac{1}{2}(I - \frac{\sigma_X}{7} - \frac{\sigma_Y}{5} - \frac{\sigma_Z}{6})$ and $\rho'_1 = \frac{1}{2}(I + \frac{\sigma_X}{7} + \frac{\sigma_Y}{5} - \frac{\sigma_Z}{6})$.

Furthermore, $\overline{\mathrm{QSDP}}[1,0]$ *is in* NQP *when there is no error.*

We notice that NQP (defined in [ADH97, YY99]) serves as a precise variant of BQP with perfect soundness, specifically having an *exact zero* acceptance probability for *no* instances. Furthermore, researchers initially regarded NQP as a quantum analog of NP.[4] Prior works [FGHP99, YY99] have established the relationships $\mathsf{NQP} = \mathsf{coC_{=}P} \subseteq \mathsf{PP}$.

Parameter regimes	$\overline{\mathrm{SDP}}[1-\epsilon,\epsilon]$	$\overline{\mathrm{QSDP}}[1-\epsilon,\epsilon]$
$\epsilon = 0$	in NP Folklore	in NQP This work (Theorem 7.33(2))
$\epsilon(n) \leq 2^{-n/2-1}$	in PP Theorem 7.1 in [BCH+19]	in PP This work (Theorem 7.33(1))
$\epsilon(n) \geq 2^{-n^{1/2-\gamma}}$ for $\gamma \in (0,1/2)$	SZK-hard Implicitly stated in [SV03]	QSZK-hard Implicitly stated in [Wat02]

Table 7.1: Easy and hard regimes for SZK and QSZK.

We summarize our results and compare them with the counterpart SZK results in Table 7.1. The improved SZK-hardness and QSZK-hardness are obtained from skillfully applying the polarization lemma for the relevant distance, as shown in [BDRV19, Theorem 3.14]. To demonstrate the PP containment, we first note that $\mathrm{HS}^2(\rho_0,\rho_1) = \frac{1}{2}(\mathrm{Tr}(\rho_0^2) + \mathrm{Tr}(\rho_1^2)) - \mathrm{Tr}(\rho_0\rho_1)$. The remaining results are mainly derived from a hybrid algorithm based on the SWAP test [BCWdW01], specifically tossing two random coins and performing the SWAP test on the corresponding states.

In essence, the phenomenon that parameter regimes with some negligible errors are easier to solve is not unique to QSZK. Analogous phenomena can also be observed in other complexity classes, such as QMA(2) [KMY09] and StoqMA [AGL20]. Nevertheless, it is important to note that these similar results in other classes do not always necessitate the dimension-preserving property. In particular, polarization lemma for some quantum distance is considered *dimension-preserving* if the resulting quantum states use the same number of qubits as the original quantum states. Since SZK is a subclass of QSZK, Theorem 7.3 suggests that QSDP may not remain QSZK-hard when the acceptance probability deviates *tinily* from 0 or 1.

7.1.2 Proof techniques

The QSZK completeness of QJSP and measQTDP crucially relies on the inequalities between quantum analogs of common classical f-divergences.[5] We start by reviewing and defining these quantum analogs. The most widely used quantum distances are the trace distance (T) and the Bures distance (B, essentially the fidelity), which are quantum counterparts of the total variation distance (TV) and the Hellinger distance (H),

[4] NQP is incomparable to QMA due to its equivalence to PreciseQMA with perfect soundness [KMY09]. Two main distinctions between these classes are: (1) NQP allows an exponentially small gap between acceptance probabilities for *yes* and *no* instances, while QMA permits only an inverse-polynomial gap; and (2) NQP guarantees rejection for *no* instances, whereas QMA allows any reasonable choice.

[5] An f-divergence is a function $\mathrm{D}_f(p_0\|p_1)$ that measures the difference between two probability distributions p_0 and p_1, and this divergence is defined as $\mathrm{D}_f(p_0\|p_1) := \mathbb{E}_{x\sim p_1} f(p_0(x)/p_1(x))$.

respectively. Other commonly used f-divergences are the KL divergence (also known as the relative entropy) and the χ^2-divergence, which are unbounded, so we instead focus on their symmetrized versions, the Jensen-Shannon divergence (JS) and the triangular discrimination (TD), respectively.

The relationship between two quantum analogs of the Jensen-Shannon divergence constitutes a specific instance of the Holevo's bound, namely the measured quantum Jensen-Shannon divergence is upper bounded by the quantum Jensen-Shannon divergence. To the best of our knowledge, there is no known quantum analog of triangular discrimination. We thus introduce the definition of the quantum triangular discrimination (QTD) and the measured quantum triangular discrimination ($\mathrm{QTD}^{\mathrm{meas}}$), based on their connection to the quantum analogs of χ^2-divergence [TKR+10]. We further examine their relationship with other aforementioned quantum distances and divergences:

Theorem 7.4 (Inequalities on quantum analogs of the triangular discrimination, informal)**.** *For any quantum states ρ_0 and ρ_1, the following holds*:

(1) $\mathrm{T}^2(\rho_0,\rho_1) \le \mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) \le \mathrm{QTD}(\rho_0,\rho_1) \le \mathrm{T}(\rho_0,\rho_1)$;

(2) $\frac{1}{2}\mathrm{QTD}^2(\rho_0,\rho_1) \le \mathrm{QJS}(\rho_0,\rho_1) \le \mathrm{QTD}(\rho_0,\rho_1)$;

(3) $\frac{1}{2}\mathrm{B}^2(\rho_0,\rho_1) \le \mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) \le \mathrm{B}^2(\rho_0,\rho_1)$ *and* $\frac{1}{2}\mathrm{B}^2(\rho_0,\rho_1) \le \mathrm{QTD}(\rho_0,\rho_1) \le \mathrm{B}(\rho_0,\rho_1)$.

We summarize our new results and known inequalities in Table 7.2, together with the usages of these inequalities in our proof. In addition, we highlight that the quantum triangular discrimination behaves differently from its classical counterpart since the triangular discrimination is a constant multiplicative error approximation of the Jensen-Shannon divergence. This difference breaks down the quantum equivalent of the ingenious reduction from TDP to JSP presented in [BDRV19], leading to a slightly worse parameter in the improved QSZK containment of QSDP, as stated in Theorem 7.2(1).

	Classical	Quantum	Usages related to QSZK
SDP vs. H^2	$\mathrm{H}^2 \le \mathrm{SDP} \le \sqrt{2}\mathrm{H}$ [Kai67]	$\frac{1}{2}\mathrm{B}^2 \le \mathrm{T} \le \mathrm{B}$ [FvdG99]	A polarization lemma for the trace distance [Wat02]
SDP vs. JS	$1-\mathrm{H}_{\mathrm{bit}}\left(\frac{1-\mathrm{SDP}}{2}\right) \le \mathrm{JS}_{\mathrm{bit}} \le \mathrm{SDP}$ [FvdG99, Top00]	$1-\mathrm{H}_{\mathrm{bit}}\left(\frac{1-\mathrm{T}}{2}\right) \le \mathrm{QJS}_{\mathrm{bit}} \le \mathrm{T}$ [BH09, FvdG99]	QJSP is QSZK-hard This work (Lemma 7.31)
SDP vs. TD	$\mathrm{SDP}^2 \le \mathrm{TD} \le \mathrm{SDP}$ [Top00]	$\mathrm{T}^2 \le \mathrm{QTD}^{\mathrm{meas}} \le \mathrm{QTD} \le \mathrm{T}$ This work (Theorem 7.7)	MEASQTDP is QSZK-hard This work (Lemma 7.32)
JS vs. TD	$\frac{1}{2}\mathrm{TD} \le \mathrm{JS} \le \ln 2 \cdot \mathrm{TD}$ [Top00]	$\frac{1}{2}\mathrm{QTD}^2 \le \mathrm{QJS} \le \mathrm{QTD}$ This work (Theorem 7.8)	None
TD vs. H^2	$\mathrm{H}^2 \le \mathrm{TD} \le 2\mathrm{H}^2$ [LC86]	$\frac{1}{2}\mathrm{B}^2 \le \mathrm{QTD}^{\mathrm{meas}} \le \mathrm{B}^2$ $\frac{1}{2}\mathrm{B}^2 \le \mathrm{QTD} \le \mathrm{B}$ This work (Theorem 7.9)	Polarization lemmas for $\mathrm{QTD}^{\mathrm{meas}}$ and QTD This work (Lemmas 7.25 and 7.26)

Table 7.2: A comparison between classical and quantum distances with usages related to QSZK.

Leveraging inequalities in Table 7.2, we establish that QJSP, MEASQTDP, and QTDP are QSZK-complete. The QSZK containments of MEASQTDP and QTDP are achieved through *new* polarization lemmas for the measured quantum triangular discrimination ($\mathrm{QTD}^{\mathrm{meas}}$) and the quantum triangular discrimination (QTD), while the QSZK containment of QJSP is established via a reduction to QEDP [BASTS10], using the

joint entropy theorem on classical-quantum states. Furthermore, the QSZK-hardness of these problems directly mirrors that of their classical counterparts [BDRV19], due to the corresponding inequalities in Table 7.2.

7.2 Quantum analogs of the triangular discrimination

In this section, we introduce *two quantum analogs of the triangular discrimination* and prove their relationships with several commonly used distances, such as trace distance, Bures distance (closely related to the fidelity), and quantum Jensen-Shannon divergence.

To the best of our knowledge, there is no known quantum analog of the triangular discrimination (also known as Vincent-Le Cam divergence). Since the triangular discrimination is a symmetrized version of the χ^2 divergence, specifically

$$\mathrm{TD}(p_0, p_1) = \chi^2\left(p_0 \middle\| \frac{p_0+p_1}{2}\right) = \chi^2\left(p_1 \middle\| \frac{p_0+p_1}{2}\right).$$

The first quantum analog is derived from the quantum χ^2 divergence in [TKR+10]:

Definition 7.5 (Quantum Triangular Discrimination)**.** *Let ρ_0 and ρ_1 be two quantum states. The quantum triangular discrimination between ρ_0 and ρ_1 is defined as*

$$\mathrm{QTD}(\rho_0, \rho_1) \coloneqq \frac{1}{2}\mathrm{Tr}\left((\rho_0-\rho_1)(\rho_0+\rho_1)^{-1/2}(\rho_0-\rho_1)(\rho_0+\rho_1)^{-1/2}\right).$$

Furthermore, if $\rho_0+\rho_1$ is not full-rank, then the inverse is defined only on its support.

It is noteworthy that this quantum analog of the triangular discrimination can be defined as $\mathrm{QTD}_\alpha(\rho_0,\rho_1) = \chi^2_\alpha\left(\rho_z \middle\| \frac{\rho_0+\rho_1}{2}\right)$ for $z \in \{0,1\}$ in general, following the approach presented in [TKR+10]. However, QTD_α is only upper-bounded by the trace distance for $\alpha = 1/2$.[6] Therefore, we use $\mathrm{QTD}_{\alpha=1/2}(\rho_0,\rho_1)$ for defining QTD in this chapter.

In addition, we establish another quantum analog of triangular discrimination, denoted by the *Measured Quantum Triangular Discrimination* ($\mathrm{QTD}^{\mathrm{meas}}$), based on distributions induced by quantum measurements in terms of Equation (3.2). By utilizing Lemma 5 in [TV15], we can derive an explicit formula for $\mathrm{QTD}^{\mathrm{meas}}$.[7] As is typical, QTD is lower-bounded by its measured variant $\mathrm{QTD}^{\mathrm{meas}}$, following from a data-processing inequality for the quantum χ^2-divergence [TKR+10, Proposition 6]:

Lemma 7.6. *Let ρ_0 and ρ_1 be two quantum states. Then, it holds that*:

$$\mathrm{QTD}(\rho_0,\rho_1) \geq \mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1).$$

Proof. According to [TKR+10, Proposition 6], a data-processing inequality for the quantum $\chi^2_{\alpha=1/2}$-divergence, we have: for any states ρ_0 and ρ_1,

$$\begin{aligned}\mathrm{QTD}(\rho_0,\rho_1) &= \chi^2_{\alpha=1/2}\left(\rho_0 \middle\| \tfrac{\rho_0+\rho_1}{2}\right)\\ &\geq \chi^2_{\alpha=1/2}\left(\mathcal{M}(\rho_0) \middle\| \mathcal{M}(\tfrac{\rho_0+\rho_1}{2})\right)\end{aligned}$$

[6] See Remark 7.11 for the details.

[7] Given $\mathrm{TD}(p_0,p_1) = \chi^2(p_z\|\frac{p_0+p_1}{2})$ for $z\in\{0,1\}$, an explicit formula for $\mathrm{QTD}^{\mathrm{meas}}$ follows Lemma 5 in [TV15]: $\mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) = \mathrm{Tr}\left(\frac{\rho_0-\rho_1}{2}\Omega_{\rho_+}\left(\frac{\rho_0-\rho_1}{2}\right)\right)$ where $\rho_+ \coloneqq \frac{\rho_0+\rho_1}{2}$ and the linear operator Ω_ρ satisfies $\Omega_\rho^{-1}(A) = (\rho A + A\rho)/2$. In particular, as observed in [BOW19, Section 3.1.2], if $\rho_+ = (\beta_1,\cdots,\beta_d)$ is diagonal of full rank, then $\mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) = \sum_{i,j=1}^d \frac{2}{\beta_i+\beta_j}|(\rho_-)_{ij}|^2$ where $\rho_- \coloneqq \frac{\rho_0-\rho_1}{2}$.

$$= \tilde{\chi}^2_{\alpha=1/2}\left(\rho_0 \middle\| \tfrac{\rho_0+\rho_1}{2}\right)$$
$$= \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1).$$

Here, we denote the measured χ^2-divergence as $\tilde{\chi}^2_\alpha(\cdot,\cdot)$, defining in terms of Equation (3.2). Additionally, we choose the quantum channel $\mathcal{M}$ that corresponds to the optimal POVM in $\tilde{\chi}^2_\alpha\left(\rho_0 \middle\| \tfrac{\rho_0+\rho_1}{2}\right)$. □

We now present three theorems that examine the relationships between the quantum triangular discrimination (QTD) and other commonly used quantum distances and divergences. Theorem 7.7 compares QTD with the trace distance (T) and is established through a combination of Lemma 7.10 and Lemma 7.13 in Section 7.2.1. The latter relies on the trace distance being also a measured version of the total variation distance.

Theorem 7.7 (QTD vs. trace distance)**.** *For any quantum states ρ_0 and ρ_1,*

$$\mathrm{T}^2(\rho_0, \rho_1) \leq \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) \leq \mathrm{QTD}(\rho_0, \rho_1) \leq \mathrm{T}(\rho_0, \rho_1).$$

Theorem 7.8 proves the relationship between QTD and the quantum Jensen-Shannon divergence (QJS), which is based on a combination of Lemma 7.17 and Lemma 7.18 in Section 7.2.2. The proof of these lemmas takes advantage of inequalities on the trace distance, thereby linking QJS and QTD.

Theorem 7.8 (QTD vs. QJS)**.** *For any quantum states ρ_0 and ρ_1,*

$$\frac{1}{2}\mathrm{QTD}^2(\rho_0, \rho_1) \leq \mathrm{QJS}(\rho_0, \rho_1) \leq \mathrm{QTD}(\rho_0, \rho_1).$$

Theorem 7.9 explores the relationship between the QTD and the Bures distance. The bounds of $\mathrm{QTD}^{\mathrm{meas}}$ (Lemma 7.14) rely on the Bures distance being the measured version of the Hellinger distance, while the upper and lower bounds for QTD (Lemma 7.15) are established using inequalities involving the trace distance. The detailed proof can be found in Section 7.2.3.

Theorem 7.9 (QTD vs. Bures distance)**.** *For any quantum states ρ_0 and ρ_1,*

$$\frac{1}{2}\mathrm{B}^2(\rho_0, \rho_1) \leq \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) \leq \mathrm{B}^2(\rho_0, \rho_1) \text{ and } \frac{1}{2}\mathrm{B}^2(\rho_0, \rho_1) \leq \mathrm{QTD}(\rho_0, \rho_1) \leq \mathrm{B}(\rho_0, \rho_1).$$

7.2.1 QTD vs. trace distance

We begin by establishing the challenging direction in Theorem 7.7, particularly the quantum triangular discrimination is upper bounded by the trace distance (Lemma 7.10), and then highlighting two important subtleties of QTD. The proof of the converse direction will be provided at the end of this subsection.

Lemma 7.10 (QTD ≤ T)**.** *For any quantum states ρ_0 and ρ_1,*

$$\mathrm{QTD}(\rho_0, \rho_1) \leq \mathrm{T}(\rho_0, \rho_1).$$

The first subtlety of QTD lies in the fact that the inequality in Lemma 7.10 holds solely for a particular choice of $\alpha = 1/2$ for QTD_α, which leads to the minimum:

Remark 7.11 ($\mathrm{QTD}_\alpha \leq \mathrm{T}$ holds only for $\alpha = 1/2$). As [TKR+10, Proposition 7] implies that $\mathrm{QTD}_{\alpha=1/2} \leq \mathrm{QTD}_\alpha$, we may wonder whether Lemma 7.10 holds for any $\alpha \in [0,1]$. Here is a counterexample: Consider two single-qubit pure states

$$\rho_0^* \coloneqq \frac{1}{2}\Big(I + \frac{6}{7}\sigma_X + \frac{3}{7}\sigma_Y + \frac{2}{7}\sigma_Z\Big) \text{ and } \rho_1^* \coloneqq \frac{1}{2}\Big(I - \frac{3}{7}\sigma_X - \frac{2}{7}\sigma_Y + \frac{6}{7}\sigma_Z\Big),$$

where σ_X, σ_Y and σ_Z are Pauli matrices. Then we simply have

$$\mathrm{QTD}_{\alpha=1/2}(\rho_0^*, \rho_1^*) = \mathrm{T}(\rho_0^*, \rho_1^*) < \mathrm{QTD}_{\alpha>1/2}(\rho_0^*, \rho_1^*).$$

The second subtlety of QTD concerns the notable difference in the equality condition of this inequality (Lemma 7.12) compared to its classical counterpart. Specifically, the classical counterpart merely requires Lemma 7.12(1).[8] However, the inequalities in Theorem 7.7 exhibit a similar behavior to the inequalities between the corresponding classical distances, namely triangular discrimination (TD) and total variation distance (TV).

Lemma 7.12 (Equality condition for $\mathrm{QTD} \leq \mathrm{T}$)**.** *Let ρ_0 and ρ_1 be two quantum states. Then, the equality $\mathrm{QTD}(\rho_0, \rho_1) = \mathrm{T}(\rho_0, \rho_1)$ holds if and only if these quantum states satisfy the following conditions*:

(1) $(\rho_0 - \rho_1)(\rho_0 + \rho_1)^{-1}(\rho_0 - \rho_1) = (\rho_0 + \rho_1)$;

(2) $(\rho_0 - \rho_1)^\dagger(\rho_0 - \rho_1) = \frac{\mathrm{Tr}\left((\rho_0-\rho_1)^\dagger(\rho_0-\rho_1)\right)}{|\mathrm{supp}(\rho_0-\rho_1)|} I$;

(3) *For any $k \in \mathrm{supp}\,(\rho_0 - \rho_1)$, it holds that*

$$\mathrm{sgn}\lambda_k(\rho_0 - \rho_1) = \mathrm{sgn}\lambda_k\Big((\rho_0 + \rho_1)^{-1/2}(\rho_0 - \rho_1)(\rho_0 + \rho_1)^{1/2}\Big).$$

Here, $\lambda_k(A)$ is the k-th eigenvalue of the matrix A.

We now outline the proof of Lemma 7.10: Firstly, we establish an upper bound of QTD by the trace distance with an infinite norm (multiplicative) factor using a matrix version of Hölder inequality. Subsequently, we bound this infinite norm factor by analyzing its largest singular value employing the Weyl's inequalities. The detailed proof follows below.

Proof of Lemma 7.10. Using a matrix Hölder inequality (e.g., Corollary IV.2.6 in [Bha96]), we obtain the following:

$$\begin{aligned} \mathrm{QTD}(\rho_0, \rho_1) &= \frac{1}{2}\mathrm{Tr}\left((\rho_0 - \rho_1)(\rho_0 + \rho_1)^{-1/2}(\rho_0 - \rho_1)(\rho_0 + \rho_1)^{-1/2}\right) \\ &\leq \frac{1}{2}\|\rho_0 - \rho_1\|_1 \cdot \|(\rho_0 + \rho_1)^{-1/2}(\rho_0 - \rho_1)(\rho_0 + \rho_1)^{-1/2}\|_\infty \end{aligned} \tag{7.1}$$

It is sufficient to show that

$$\|(\rho_0 + \rho_1)^{-1/2}(\rho_0 - \rho_1)(\rho_0 + \rho_1)^{-1/2}\|_\infty = \sigma_{\max}\left((\rho_0 + \rho_1)^{-1/2}(\rho_0 - \rho_1)(\rho_0 + \rho_1)^{-1/2}\right) \leq 1,$$

where $\sigma_{\max}(A)$ is the largest singular value of A. Let $\rho \coloneqq \frac{1}{2}(\rho_0 + \rho_1)$, then we have

$$(\rho_0 + \rho_1)^{-1/2}(\rho_0 - \rho_1)(\rho_0 + \rho_1)^{-1/2} = \rho^{-1/2}(\rho - \rho_1)\rho^{-1/2} = I - \rho^{-1/2}\rho_1\rho^{-1/2}.$$

Note that $\rho^{-1/2}\rho_1\rho^{-1/2}$ is positive semi-definite, and $I - \rho^{-1/2}\rho_1\rho^{-1/2}$ thus is Hermitian.

[8] In particular, $(p_0(x) - p_1(x))^2 = (p_0(x) + p_1(x))^2$ holds for any $x \in \mathrm{supp}\,(p_0) \cup \mathrm{supp}\,(p_1)$.

We then obtain that $|I - \rho^{-1/2}\rho_1\rho^{-1/2}| \preceq I$.[9] With the help of [HJ12, Corollary 4.3.12], a corollary of Weyl's inequalities, this inequality implies that:

$$\begin{aligned}\sigma_{\max}\left(I - \rho^{-1/2}\rho_1\rho^{-1/2}\right) &= \lambda_{\max}\left(I - \rho^{-1/2}\rho_1\rho^{-1/2}\right) \\ &\leq \lambda_{\max}\left(\left(I - \rho^{-1/2}\rho_1\rho^{-1/2}\right) + \rho^{-1/2}\rho_1\rho^{-1/2}\right) \\ &\leq 1.\end{aligned} \tag{7.2}$$

Here, the first line is derived from the fact that the singular values of a Hermitian matrix are equal to the absolute values of the corresponding eigenvalues of the same matrix, and the last line is due to $\lambda_{\max}(I) = 1$. □

To derive the equality condition of Lemma 7.10, and thereby prove Lemma 7.12, a thorough analysis of the equality condition of the matrix Hölder inequality in [Cio21] is required. The detailed proof is provided subsequently.

Proof of Lemma 7.12. We begin with the equality condition of the matrix Hölder inequality in [Cio21, Theorem 2.11]. Let $A = \frac{\rho_0-\rho_1}{2}$ and $B = \left(\frac{\rho_0+\rho_1}{2}\right)^{-1/2}\left(\frac{\rho_0-\rho_1}{2}\right)\left(\frac{\rho_0+\rho_1}{2}\right)^{-1/2}$. Then, it holds that

$$\frac{A^\dagger B}{\mathrm{Tr}|A|\|B\|_\infty} = \frac{B^\dagger A}{\mathrm{Tr}|A|\|B\|_\infty} = \frac{|A|}{\mathrm{Tr}|A|} = \frac{|B|^\infty}{\mathrm{Tr}\left(|B|^\infty\right)}. \tag{7.3}$$

Moreover, $B^\dagger A$ is supposed to be symmetric and positive semi-definite. Note that A and B are Hermitian, we obtain $[A, B] = 0$ by using the first equality in Equation (7.3). This equality implies that $B^\dagger A$ is indeed symmetric, as well as the singular value decomposition

$$A = \sum_k \sigma_k(A)|v_k\rangle\langle v_k| \text{ and } B = \sum_k \sigma_k(B)|v_k\rangle\langle v_k|.$$

Then, by Equation (7.3), we obtain

$$\begin{aligned}B^\dagger A &= \sum_k \sigma_k(B)\sigma_k(A)|v_k\rangle\langle v_k| = \sigma_{\max}(B)\sum_k \sigma_k(A)|v_k\rangle\langle v_k| = \|B\|_\infty|A|, \\ \frac{|A|}{\mathrm{Tr}|A|} &= \sum_k \frac{\sigma_k(A)}{\sum_i \sigma_i(A)}|v_i\rangle\langle v_i| = \sum_k \frac{\sigma_k^\infty}{\sum_j \sigma_k^\infty(B)}|v_k\rangle\langle v_k| = \frac{|B|^\infty}{\mathrm{Tr}(|B|^\infty)}.\end{aligned}$$

Noting that $\{|v_i\rangle\}_{v_i\in\mathrm{supp}(\rho_0-\rho_1)}$ is an orthonormal basis, by comparing the coefficients, we have the following:

$$\forall k:\ \sigma_k(A) = \sigma_{\max}(A) \text{ and } \sigma_k(B) = \sigma_{\max}(B) = 1. \tag{7.4}$$

Here, $\sigma_{\max}(B) = 1$ due to Equation (7.2) with the equality. Therefore, we obtain that B is an orthogonal matrix, which is equivalent to

$$(\rho_0 - \rho_1)(\rho_0 + \rho_1)^{-1}(\rho_0 - \rho_1) = (\rho_0 + \rho_1).$$

Moreover, noting that $\mathrm{Tr}(A^\dagger A) = \sum_k \sigma_k^2(A)$, this equality implies the desired equality:

$$A^\dagger A = \frac{\mathrm{Tr}\left(A^\dagger A\right)}{|\mathrm{supp}\left(\rho_0 - \rho_1\right)|}I.$$

[9] It suffices to show that $-I \preceq I - \rho^{-1/2}\rho_1\rho^{-1/2} \preceq I$. The right-hand side is evident, while the left-hand side follows from $\rho^{-1/2}\rho_1\rho^{-1/2} \preceq 2I$, which holds by applying $\Phi(\sigma) := \rho^{1/2}\sigma\rho^{1/2}$ on both sides.

Finally, to make $B^\dagger A$ to be positive semi-definite, we finish the proof by noting that

$$\operatorname{sign}\lambda_k(A) = \operatorname{sign}\lambda_k(B) \text{ for any } k \in \operatorname{supp}(\rho_0 - \rho_1). \qquad \square$$

Lastly, we present the proof of Lemma 7.13 (the converse direction in Theorem 7.7). In particular, by leveraging Lemma 7.6, we can derive a lower bound for the quantum counterparts of triangular discrimination in terms of the trace distance.

Lemma 7.13 ($\mathrm{T}^2 \leq \mathrm{QTD}$)**.** *For quantum states ρ_0 and ρ_1, it holds that*:

$$\forall \alpha \in [0,1], \quad \mathrm{T}(\rho_0,\rho_1)^2 \leq \mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) \leq \mathrm{QTD}(\rho_0,\rho_1).$$

Proof. Owing to Lemma 7.6, it suffices to show that $\mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) \geq \mathrm{T}(\rho_0,\rho_1)$. Analogous to the approach presented in [Top00], we obtain the following for any POVM $\mathcal{E}$:

$$\begin{aligned}
\mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) &\geq \mathrm{TD}\left(p_0^{(\mathcal{E})}, p_1^{(\mathcal{E})}\right) \\
&= \frac{1}{2}\sum_x \frac{\left(p_0^{(\mathcal{E})}(x) - p_1^{(\mathcal{E})}(x)\right)^2}{p_0^{(\mathcal{E})}(x) + p_1^{(\mathcal{E})}(x)} \\
&= \sum_x \frac{p_0^{(\mathcal{E})}(x) + p_1^{(\mathcal{E})}(x)}{2} \cdot \left(\frac{p_0^{(\mathcal{E})}(x) - p_1^{(\mathcal{E})}(x)}{p_0^{(\mathcal{E})}(x) + p_1^{(\mathcal{E})}(x)}\right)^2 \\
&\geq \left(\sum_x \frac{p_0^{(\mathcal{E})}(x) + p_1^{(\mathcal{E})}(x)}{2} \cdot \frac{p_0^{(\mathcal{E})}(x) - p_1^{(\mathcal{E})}(x)}{p_0^{(\mathcal{E})}(x) + p_1^{(\mathcal{E})}(x)}\right)^2 \\
&= \left(\frac{1}{2}\sum_x \left|p_0^{(\mathcal{E})}(x) - p_1^{(\mathcal{E})}(x)\right|\right)^2,
\end{aligned} \tag{7.5}$$

where the fourth line is because of $\mathbb{E}[X^2] \geq (\mathbb{E}[X])^2$ for any random variable X. We then complete the proof by choosing $\mathcal{E}$ that maximizes the last line in Equation (7.5). $\square$

7.2.2 QTD vs. (squared) Bures distance

We now present inequalities concerning two different quantum analogs of the triangular discrimination (TD), namely QTD and the measured version $\mathrm{QTD}^{\mathrm{meas}}$, expressed in terms of the Bures distance. Interestingly, these inequalities exhibit divergent behaviors for QTD (Lemma 7.14) and $\mathrm{QTD}^{\mathrm{meas}}$ (Lemma 7.15), and we can identify an example (in Remark 7.16) that distinguishes between these two quantum analogs of TD. These divergent behaviors have implications in quantum complexity theory, particularly in the corresponding polarization lemma and the complexity class QSZK.[10]

We begin by establishing the inequalities between $\mathrm{QTD}^{\mathrm{meas}}$ and the Bures distance, as stated in Lemma 7.14. The proof crucially relies on the fact that the Bures distance corresponds to the measured version of Hellinger distance [FC94].

Lemma 7.14 ($\mathrm{QTD}^{\mathrm{meas}}$ vs. B^2)**.** *For any quantum states ρ_0 and ρ_1,*

$$\frac{1}{2}\mathrm{B}^2(\rho_0,\rho_1) \leq \mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) \leq \mathrm{B}^2(\rho_0,\rho_1).$$

[10] See Lemmas 7.25 and 7.26 in Section 7.3.3 for further details.

Proof. Let $\mathcal{E}^*$ be the optimized measurement for $\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1)$. We first notice that

$$\begin{aligned}\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) &= \frac{1}{2}\sum_x \frac{\left(p_0^{(\mathcal{E}^*)}(x) - p_1^{(\mathcal{E}^*)}(x)\right)^2}{p_0^{(\mathcal{E}^*)}(x) + p_1^{(\mathcal{E}^*)}(x)} \\ &= \frac{1}{2}\sum_x \frac{\left(\sqrt{p_0^{(\mathcal{E}^*)}(x)} - \sqrt{p_1^{(\mathcal{E}^*)}(x)}\right)^2 \left(\sqrt{p_0^{(\mathcal{E}^*)}(x)} + \sqrt{p_1^{(\mathcal{E}^*)}(x)}\right)^2}{p_0^{(\mathcal{E}^*)}(x) + p_1^{(\mathcal{E}^*)}(x)}.\end{aligned}$$

Noting that $a^2 + b^2 \leq (a+b)^2 \leq 2(a^2+b^2)$ for $a, b \geq 0$, we have derived that

$$\frac{1}{2}\sum_x \left(\sqrt{p_0^{(\mathcal{E})}(x)} - \sqrt{p_1^{(\mathcal{E})}(x)}\right)^2 \leq \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) \leq \sum_x \left(\sqrt{p_0^{(\mathcal{E}^*)}(x)} - \sqrt{p_1^{(\mathcal{E}^*)}(x)}\right)^2. \quad (7.6)$$

Note that the Bures distance is the measured Hellinger distance [FC94], we have:

- For the lower bound, since the first inequality in Equation (7.6) holds for arbitrary POVM $\mathcal{E}$, we choose $\mathcal{E}'$ that maximizes the measured Hellinger distance, then:

$$\begin{aligned}\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) &\geq \frac{1}{2}\sum_x \left(\sqrt{p_0^{(\mathcal{E}')}(x)} - \sqrt{p_1^{(\mathcal{E}')}(x)}\right)^2 \\ &= \sup_{\mathrm{POVM}\ \mathcal{E}} \mathrm{H}^2\left(p_0^{(\mathcal{E})}, p_1^{(\mathcal{E})}\right) \\ &= \tfrac{1}{2}\mathrm{B}^2(\rho_0, \rho_1).\end{aligned}$$

- For the upper bound, let $\mathcal{E}'$ be the POVM measurement that maximizes the measured Hellinger distance. By the second inequality in Equation (7.6), we deduce:

$$\begin{aligned}\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) &\leq \sum_x \left(\sqrt{p_0^{(\mathcal{E}')}(x)} - \sqrt{p_1^{(\mathcal{E}')}(x)}\right)^2 \\ &= \sup_{\mathrm{POVM}\ \mathcal{E}} 2\mathrm{H}^2\left(p_0^{(\mathcal{E})}, p_1^{(\mathcal{E})}\right) \\ &= \mathrm{B}^2(\rho_0, \rho_1).\end{aligned}$$

□

Next, we present the inequalities between QTD and the Bures distance, as detailed in Lemma 7.15. It is noteworthy that the upper bound in these inequalities is as weak as the trace distance, and we further provide an example (in Remark 7.16) to distinguish these two quantum analogs of the triangle discrimination in terms of the Bures distance.

Lemma 7.15 (QTD vs. B)**.** *For any quantum states ρ_0 and ρ_1,*

$$\frac{1}{2}\mathrm{B}^2(\rho_0, \rho_1) \leq \mathrm{QTD}(\rho_0, \rho_1) \leq \mathrm{B}(\rho_0, \rho_1).$$

Proof. We establish the left-hand side inequality by plugging Lemma 7.6 into Lemma 7.14. The right-hand side inequality follows from combining Lemma 3.17 and Lemma 7.10. □

Remark 7.16 ($\mathrm{QTD}^{\mathrm{meas}}$ vs. QTD). The squared Bures distance is an example that separates between $\mathrm{QTD}^{\mathrm{meas}}$ and QTD: Utilizing the counterexample ρ_0^* and ρ_1^* defined in Remark 7.11, we can obtain

$$\mathrm{QTD}^{\mathrm{meas}}(\rho_0^*, \rho_1^*) \leq \mathrm{B}^2(\rho_0^*, \rho_1^*) < \mathrm{QTD}_{\alpha=1/2}(\rho_0^*, \rho_1^*) = \mathrm{T}(\rho_0^*, \rho_1^*) < \mathrm{B}(\rho_0^*, \rho_1^*).$$

7.2.3 QTD vs. QJS

We now establish the inequalities between QTD and QJS. It is worth noting that the corresponding classical distance, the triangular discrimination (TD), serves as a constant multiplicative-error approximation of the Jensen-Shannon divergence (JS), as illustrated by the inequalities $\frac{1}{2}\mathrm{TD}(p_0,p_1) \leq \mathrm{JS}(p_0,p_1) \leq \ln 2 \cdot \mathrm{TD}(p_0,p_1)$ in [Top00, Theorem 2]. However, such a property does not extend to QTD and QJS.[11]

We start with the lower bound of QJS in terms of QTD, as stated in Lemma 7.17. The proof straightforwardly follows from inequalities concerning the trace distance.

Lemma 7.17. *For any quantum states ρ_0 and ρ_1,*

$$\frac{1}{2}\mathrm{QTD}^2(\rho_0,\rho_1) \leq \mathrm{QJS}(\rho_0,\rho_1).$$

Proof. Plugging Lemma 7.10 into Lemma 3.25, we obtain that: for any states ρ_0 and ρ_1,

$$\mathrm{QJS}(\rho_0,\rho_1) \geq \sum_{v=1}^{\infty} \frac{\mathrm{T}(\rho_0,\rho_1)^{2v}}{2v(2v-1)} \geq \sum_{v=1}^{\infty} \frac{\mathrm{QTD}(\rho_0,\rho_1)^{2v}}{2v(2v-1)} \geq \tfrac{1}{2}\mathrm{QTD}^2(\rho_0,\rho_1),$$

where the last inequality uses the first-order approximation. This completes the proof. □

Next, we present the upper bound of QJS in terms of QTD, as detailed in Lemma 7.18. The proof strategies is analogous to the proof of Theorem 8 in [TKR+10].

Lemma 7.18. *For any quantum states ρ_0 and ρ_1,*

$$\mathrm{QJS}(\rho_0,\rho_1) \leq \mathrm{QTD}(\rho_0,\rho_1).$$

Proof. We begin with an upper bound for the quantum relative entropy in [RS90]:

$$\mathrm{D}(\rho_0\|\rho_1) \leq \frac{1}{\gamma}\mathrm{Tr}\left(\rho_0^{1+\gamma}\rho_1^{-\gamma} - \rho_0\right) = \frac{1}{\gamma}\left[\mathrm{Tr}\left(\rho_0^{1+\gamma}\rho_1^{-\gamma}\right) - 1\right] \text{ for } 0 < \gamma \leq 1. \tag{7.7}$$

Since the quantum Jensen-Shannon divergence is a symmetrized version of the quantum relative entropy, we deduce the following by setting $\gamma = 1/2$ in Equation (7.7):

$$\begin{aligned}
\mathrm{QJS}(\rho_0,\rho_1) &= \frac{1}{2}\sum_{z\in\{0,1\}} \mathrm{D}\left(\rho_z \middle\| \tfrac{\rho_0+\rho_1}{2}\right) \\
&\leq \sum_{z\in\{0,1\}} \left[\mathrm{Tr}\left(\rho_z^{3/2}\left(\tfrac{\rho_0+\rho_1}{2}\right)^{-1/2}\right) - 1\right] \\
&\leq \frac{1}{2}\sum_{z\in\{0,1\}} \left[\mathrm{Tr}\left(\rho_z\left(\tfrac{\rho_0+\rho_1}{2}\right)^{-1/2}\rho_z\left(\tfrac{\rho_0+\rho_1}{2}\right)^{-1/2}\right) - 1\right] \\
&= \mathrm{QTD}(\rho_0,\rho_1),
\end{aligned}$$

where the third line follows from $\mathrm{Tr}\left[\left(\rho_z^{1/2}\rho^{-1/2}\rho_z^{1/2} - \rho_z^{1/2}\right)^\dagger\left(\rho_z^{1/2}\rho^{-1/2}\rho_z^{1/2} - \rho_z^{1/2}\right)\right] \geq 0$ since $\rho_z^{1/2}\rho^{-1/2}\rho_z^{1/2}$ is positive semi-definite and thus $\rho_z^{1/2}\rho^{-1/2}\rho_z^{1/2} - \rho_z^{1/2}$ is Hermitian. □

[11] For further details, please refer to Footnote 12.

7.3 Complete problems for QSZK on the quantum state testing

In this section, we introduce two new QSZK complete problems: the Quantum Jensen-Shannon Divergence Problem (QJSP) and the Measured Quantum Triangular Discrimination Problem (measQTDP). These results establish the *proper* quantum analog of the classical problems investigated in [BDRV19] and exhibit how their behavior differs from the classical counterparts.

Theorem 7.19 (QJSP is QSZK-complete)**.** *Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions such that $0 \leq \beta < \alpha \leq 1$, where n denotes the number of qubits used by quantum states ρ_0 and ρ_1. Then, it holds that*:

$$\textit{For any } \alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n), \mathrm{QJSP}[\alpha, \beta] \textit{ is in } \mathsf{QSZK}.$$

Furthermore, $\mathrm{QJSP}[\alpha, \beta]$ *is* QSZK*-hard if* $\alpha(n) \leq 1 - 2^{-n^{1/2-\epsilon}}$ *and* $\beta(n) \geq 2^{-n^{1/2-\epsilon}}$ *for every* $n \in \mathbb{N}$ *and some constant* $\epsilon \in (0, 1/2)$.

Theorem 7.20 (measQTDP is QSZK-complete)**.** *Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions such that $0 \leq \beta < \alpha \leq 1$, where n denotes the number of qubits used by quantum states ρ_0 and ρ_1. Then, it holds that*:

$$\textit{For any } \alpha(n) - \beta(n) \geq 1/O(\log n), \mathrm{measQTDP}[\alpha, \beta] \textit{ is in } \mathsf{QSZK}.$$

Furthermore, $\mathrm{measQTDP}[\alpha, \beta]$ *is* QSZK*-hard if* $\alpha(n) \leq 1 - 2^{-n^{1/2-\epsilon}}$ *and* $\beta(n) \geq 2^{-n^{1/2-\epsilon}}$ *for every* $n \in \mathbb{N}$ *and some constant* $\epsilon \in (0, 1/2)$.

In addition to measQTDP, we also investigate the Quantum Triangular Discrimination Problem (QTDP), defined using another quantum analog of triangular discrimination, and establish that this problem is QSZK-complete. However, the QSZK containment of QTDP holds only for the parameter regime $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$, encountering the same limitation as the trace distance case (QSDP) in [Wat02].

It is noteworthy that by using the reductions for proving Theorem 7.19, we achieve a simple QSZK-hardness proof for the Quantum Entropy Difference Problem (QEDP) introduced by Ben-Aroya, Schwartz, and Ta-Shma [BASTS10]:

Corollary 7.21 (Simple QSZK-hardness of QEDP)**.** $\mathrm{QEDP}[g(n)]$ *is* QSZK*-hard when* $g(n) \leq \frac{\ln 2}{2}\left(1 - 2^{(n-1)^{1/2-\epsilon}+1}\right)$ *for some* $\epsilon \in (0, 1/2)$ *and* $n \geq n(\epsilon) + 3$.

Subsequently, we proceed to demonstrate the proof of these theorems.

7.3.1 QSZK containment using the quantum entropy extraction

Along the line of [BDRV19], we implicitly employ the quantum entropy extraction approach to polarize quantum distances [BASTS10]. This approach leads to the QSZK containment of QJSP, as stated in Lemma 7.22, with a promise gap that is *inverse-polynomial*. This containment is accomplished through establishing a reduction from QJSP to QEDP. For a concise overview of QEDP, please refer to Section 3.3.

Lemma 7.22 (QJSP is in QSZK)**.** *For any $0 \leq \beta(n) < \alpha(n) \leq 1$ satisfying $\alpha(n) - \beta(n) \geq 1/p(n)$, where $p(n)$ is some polynomial of n, it holds that*:

$$\mathrm{QJSP}[\alpha, \beta] \textit{ is in } \mathsf{QSZK}.$$

Using inequalities between the trace distance and the quantum Jensen-Shannon divergence, we further derive a QSZK containment with an inverse-polynomial promise gap for QSDP on some parameter regime:

Theorem 7.23. *For any* $0 \leq \sqrt{2\ln 2}\beta(n) < \alpha^2(n) \leq 1$ *satisfying* $\alpha^2(n) - \sqrt{2\ln 2}\beta(n) \geq 1/p(n)$*, where* $p(n)$ *is some polynomial of* n*, it holds that*:

$$\mathrm{QSDP}[\alpha^2, \sqrt{2\ln 2}\beta] \text{ is in } \mathsf{QSZK}.$$

Proof. The reduction from QSDP to QJSP directly follows from the inequalities on QJS:

- For *yes* instances, $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \geq \alpha^2$ implies that $\mathrm{T}(\rho_0, \rho_1) \geq \alpha^2$ due to Lemma 3.26.
- For *no* instances, $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \leq 2\ln 2 \cdot \beta^2$ yields that

$$2\ln 2 \cdot \beta^2 \geq \sum_{v=1}^{\infty} \frac{\mathrm{T}(\rho_0, \rho_1)^{2v}}{v(2v-1)} \geq \mathrm{T}(\rho_0, \rho_1)^2$$

  as desired, where the last inequality utilizes the first-order approximation. □

It is noteworthy that $\mathrm{TDP}[\alpha, \beta]$ is in SZK when $\alpha(n) - \beta(n)$ is at least some inverse polynomial [BDRV19]. However, we are unlikely to have a similar reduction from QTDP to QJSP since these distances behave differently from their classical counterpart:

Remark 7.24 (An obstacle to a reduction from QTDP to QJSP). The SZK containment of TDP follows from a tailor-made (Karp) reduction from TDP to JSP. The key observation is that $\mathrm{TD}(p_0, p_1)$ is a *constant multiplicative-error approximation* of $\mathrm{JS}_{\mathrm{bit}}(p_0, p_1)$, and specifically, the lower bound $\mathrm{TD}(p_0, p_1)/2$ is exactly the first-order approximation of the series used in the upper bound $\ln 2 \cdot \mathrm{TD}(p_0, p_1)$.

Utilizing this fact, Lemma 4.5 in [BDRV19] show that $\lambda^2\mathrm{TD}(p_0, p_1)$ is a $1/\mathrm{poly}(n)$-*additive error approximation* of $\mathrm{JS}_{\mathrm{bit}}(q_0, q_1)$ where λ is some specific $1/\mathrm{poly}(n)$ factor and q_0 (also q_1) is a convex combination of p_0 and p_1 parameterized by λ. However, $\mathrm{QTD}(\rho_0, \rho_1)$ is *not* a constant multiplicative error approximation of $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1)$.[12]

7.3.2 QJSP is in QSZK

For any given QJSP instance and its corresponding states ρ_0 and ρ_1, the QSZK containment of QJSP essentially follows from an equality concerning $\mathrm{S}(\rho_0') - \mathrm{S}(\rho_1')$ and $\mathrm{QJS}(\rho_0, \rho_1)$, where the preparation of ρ_0' and ρ_1' requires additional gadgets using ρ_0 and ρ_1 as building blocks. This approach resembles the classical proof from Proposition 4.1 and Lemma 4.2 in [BDRV19].

However, several modifications are required due to discrepancies between classical and quantum probabilities. In particular, the classical proof relies on a probability that conditions on distributions are supposed to be distinguished, whereas its quantum counterpart – quantum conditional probability – is not well-defined in general. To address the challenge, we circumvent this issue by instead considering a conditional entropy of classical-quantum states conditioned on a classical register.

[12] Numerical simulations suggest that the tight bound is $\mathrm{QTD}^2(\rho_0, \rho_1) \leq \mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \leq \mathrm{QTD}(\rho_0, \rho_1)$, while we only managed to prove a slightly weaker bound $\frac{1}{2}\mathrm{QTD}^2(\rho_0, \rho_1) \leq \mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \leq \mathrm{QTD}(\rho_0, \rho_1)$ in Theorem 7.8.

Proof of Lemma 7.22. The proof is primarily a reduction from $\mathrm{QJSP}[\alpha, \beta]$ to $\mathrm{QEDP}[g]$, where $0 \leq \beta < \alpha \leq 1$ and $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$. We will specify the function g later.

Let Q_0 and Q_1 be the given quantum circuits acting on n all-zero qubits and having k specified output qubits. These circuits produce quantum (mixed) states ρ_0 and ρ_1, respectively, after tracing out the non-output qubits.

Now, consider a classical-quantum mixed state on a classical register B and a quantum register Y, denoted as $\rho'_1 = \frac{1}{2}|0\rangle\langle 0| \otimes \rho_0 + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_1$. We apply our reduction to produce quantum circuits Q'_0 and Q'_1, which prepare classical-quantum mixed states ρ'_0 and ρ'_1, respectively. In particular, $\rho'_0 = (p_0|0\rangle\langle 0| + p_1|1\rangle\langle 1|) \otimes (\frac{1}{2}\rho_0 + \frac{1}{2}\rho_1)$, and $\mathsf{B}' = (p_0, p_1)$ is an independent random bit with $\mathrm{H}(\mathsf{B}') = 1 - \frac{1}{2}[\alpha(n) + \beta(n)]$.

By utilizing a rotation gate R_θ such that $R_\theta|0\rangle = \sqrt{p_0}|0\rangle + \sqrt{p_1}|1\rangle$, we provide the quantum circuit description of Q'_0 and Q'_1 in Figure 7.1 and Figure 7.2, respectively. Here, A and A' are ancillary single-qubit registers, and quantum registers Y and Z collectively act on n qubits.

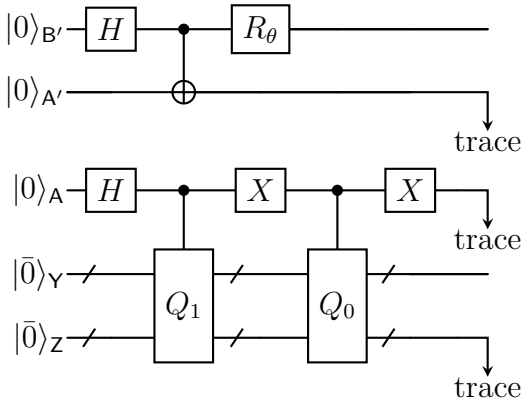

Figure 7.1: Quantum circuit Q'_0.

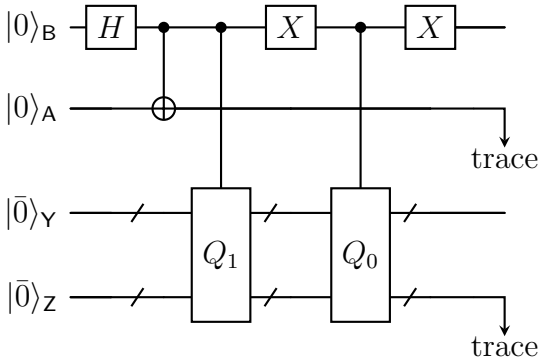

Figure 7.2: Quantum circuit Q'_1.

We then obtain the following:

$$\begin{aligned}
\mathrm{S}_{\mathrm{bit}}(\rho'_0) - \mathrm{S}_{\mathrm{bit}}(\rho'_1) &= \mathrm{S}_{\mathrm{bit}}(\mathsf{B}', \mathsf{Y})_{\rho'_0} - \mathrm{S}_{\mathrm{bit}}(\mathsf{B}, \mathsf{Y})_{\rho'_1} \\
&= [\mathrm{H}(\mathsf{B}') + \mathrm{S}_{\mathrm{bit}}(\mathsf{Y}|\mathsf{B}')_{\rho'_0}] - [\mathrm{H}(\mathsf{B}) + \mathrm{S}_{\mathrm{bit}}(\mathsf{Y}|\mathsf{B})_{\rho'_1}] \\
&= \mathrm{S}_{\mathrm{bit}}(\mathsf{Y})_{\rho'_0} - \mathrm{S}_{\mathrm{bit}}(\mathsf{Y}|\mathsf{B})_{\rho'_1} + \mathrm{H}(\mathsf{B}') - \mathrm{H}(\mathsf{B}) \\
&= \mathrm{S}_{\mathrm{bit}}(\mathsf{Y})_{\rho'_0} - \mathrm{S}_{\mathrm{bit}}(\mathsf{Y}|\mathsf{B})_{\rho'_1} - \tfrac{1}{2}[\alpha(n) + \beta(n)] \\
&= \mathrm{S}_{\mathrm{bit}}\left(\tfrac{1}{2}\rho_0 + \tfrac{1}{2}\rho_1\right) - \tfrac{1}{2}(\mathrm{S}_{\mathrm{bit}}(\rho_0) + \mathrm{S}_{\mathrm{bit}}(\rho_1)) - \tfrac{1}{2}[\alpha(n) + \beta(n)] \\
&= \mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) - \tfrac{1}{2}[\alpha(n) + \beta(n)],
\end{aligned} \tag{7.8}$$

Here, the second line is due to the definition of quantum conditional entropy and both B and B' are classical registers, the third line owes to the fact that B' is an independent random bit, the fifth line follows from the joint entropy theorem (Lemma 3.22).

Plugging Equation (7.8) into the promise of $\mathrm{QJSP}[\alpha, \beta]$, we obtain the following and choose $g(n') = \frac{\ln 2}{2}(\alpha(n) - \beta(n))$:

- If $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \geq \alpha(n)$, then $\mathrm{S}(\rho'_0) - \mathrm{S}(\rho'_1) \geq \frac{\ln 2}{2}(\alpha(n) - \beta(n)) = g(n')$;
- If $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \leq \beta(n)$, then $\mathrm{S}(\rho'_0) - \mathrm{S}(\rho'_1) \leq -\frac{\ln 2}{2}(\alpha(n) - \beta(n)) = -g(n')$.

By inspecting the description of quantum circuits Q'_0 and Q'_1, we know that the number of output qubit is $n' := n+1$ and these circuits act on at most $m'(n') = n+3 = n'+2$ qubits. Therefore, $\mathrm{QJSP}[\alpha,\beta]$ is Karp reducible to $\mathrm{QEDP}[g(n)]$ by mapping (Q_0, Q_1) to (Q'_0, Q'_1). □

7.3.3 QSZK containments using the polarization lemma

We introduce new polarization lemmas for the measured quantum triangular discrimination ($\mathrm{QTD}^{\mathrm{meas}}$) and the quantum triangular discrimination (QTD), as stated in Lemmas 7.25 and 7.26, respectively. This techniques can similarly lead to QSZK containments of measQTDP and QTDP. A notable feature of this technique is that the polarization lemma for $\mathrm{QTD}^{\mathrm{meas}}$ requires only $\alpha > \beta$, in contrast to the parameter requirements for the trace distance and QTD, which demand $\alpha^2 > \beta$.

Lemma 7.25 (A polarization lemma for $\mathrm{QTD}^{\mathrm{meas}}$)**.** *Given quantum circuits Q_0 and Q_1 that prepare quantum states ρ_0 and ρ_1, respectively, there exists a deterministic procedure that takes as input $(Q_0, Q_1, \alpha, \beta, k)$, where $\alpha > \beta$, and outputs quantum circuits $\tilde{Q}_0$ and $\tilde{Q}_1$, which prepare quantum states $\tilde{\rho}_0$ and $\tilde{\rho}_1$, respectively. The resulting states satisfy*:

$$\begin{aligned} \mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) \geq \alpha \quad &\Longrightarrow \quad \mathrm{QTD}^{\mathrm{meas}}(\tilde{\rho}_0,\tilde{\rho}_1) \geq 1-2^{-k}, \\ \mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) \leq \beta \quad &\Longrightarrow \quad \mathrm{QTD}^{\mathrm{meas}}(\tilde{\rho}_0,\tilde{\rho}_1) \leq 2^{-k}. \end{aligned}$$

Here, the states $\tilde{\rho}_0$ and $\tilde{\rho}_1$ are defined over $\widetilde{O}\left(nk^{O\left(\frac{\beta\ln(2/\alpha)}{\alpha-\beta}\right)}\right)$ qubits. Furthermore, when $k \leq O(1)$ or $\alpha-\beta \geq \Omega(1)$, the time complexity of the procedure is polynomial in the size of Q_0 and Q_1, k, and $\exp\left(\frac{\beta\log(1/\alpha)}{\alpha-\beta}\right)$.

Lemma 7.26 (A polarization lemma for QTD)**.** *Given quantum circuits Q_0 and Q_1 that prepare quantum states ρ_0 and ρ_1, respectively, there exists a deterministic procedure that takes as input $(Q_0, Q_1, \alpha, \beta, k)$, where $\alpha^2 > \beta$, and outputs quantum circuits $\tilde{Q}_0$ and $\tilde{Q}_1$, which prepare quantum states $\tilde{\rho}_0$ and $\tilde{\rho}_1$, respectively. The resulting states satisfy*:

$$\begin{aligned} \mathrm{QTD}(\rho_0,\rho_1) \geq \alpha \quad &\Longrightarrow \quad \mathrm{QTD}(\tilde{\rho}_0,\tilde{\rho}_1) \geq 1-2^{-k}, \\ \mathrm{QTD}(\rho_0,\rho_1) \leq \beta \quad &\Longrightarrow \quad \mathrm{QTD}(\tilde{\rho}_0,\tilde{\rho}_1) \leq 2^{-k}. \end{aligned}$$

Here, the states $\tilde{\rho}_0$ and $\tilde{\rho}_1$ are defined over $\widetilde{O}\left(nk^{O\left(\frac{\beta\ln(2/\alpha^2)}{\alpha^2-\beta}\right)}\right)$ qubits. Furthermore, when $k \leq O(1)$ or $\alpha-\beta \geq \Omega(1)$, the time complexity of the procedure is polynomial in the size of Q_0 and Q_1, k, and $\exp\left(\frac{\beta\log(1/\alpha^2)}{\alpha^2-\beta}\right)$.

Analogous to the QSZK containment of QSDP, we can establish QSZK containments of measQTDP and QTDP by leveraging their respective polarization lemmas:

Lemma 7.27 (measQTDP and QTDP are in QSZK)**.** *Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions satisfying $0 \leq \beta < \alpha \leq 1$. Then, the following holds*:

(1) *For any $\alpha(n) - \beta(n) \geq 1/O(\log n)$, $\mathrm{measQTDP}[\alpha,\beta]$ is in QSZK.*

(2) *For any $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$, $\mathrm{QTDP}[\alpha,\beta]$ is in QSZK.*

Proof. For any $\mathrm{measQTDP}[\alpha,\beta]$ instance satisfying $\alpha(n) - \beta(n) \geq 1/O(\log n)$, the polarization lemmas for $\mathrm{QTD}^{\mathrm{meas}}$ (Lemma 7.25) enables mapping it to a $\mathrm{measQTDP}[1-$

$2^{-l(n)}, 2^{-l(n)}]$ instance, where $2^{-l(n)}$ is a negligible function. Similarly, for any $\mathrm{QTDP}[\alpha, \beta]$ instance with $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$, the polarization lemmas for QTD (Lemma 7.26) allows mapping it to a $\textsc{meas}\mathrm{QTDP}[1 - 2^{-l(n)}, 2^{-l(n)}]$ instance. Using the inequalities in Theorem 7.7, we establish reductions from $\textsc{meas}\mathrm{QTDP}$ and QTDP to QSDP:

- For *yes* instances, it holds that
$$\mathrm{T}(\rho_0, \rho_1) \geq \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) \geq 1 - 2^{-l} \quad \text{and} \quad \mathrm{T}(\rho_0, \rho_1) \geq \mathrm{QTD}(\rho_0, \rho_1) \geq 1 - 2^{-l}.$$
- For *no* instances, the inequality $\mathrm{T}(\rho_0, \rho_1) \leq 2^{-l/2}$ is guaranteed by
$$\mathrm{T}^2(\rho_0, \rho_1) \leq \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) \leq 2^{-l} \quad \text{and} \quad \mathrm{T}^2(\rho_0, \rho_1) \leq \mathrm{QTD}(\rho_0, \rho_1) \leq 2^{-l}.$$

Finally, by following [Wat02, Theorem 10], specifically the protocol in [Wat02, Figure 2], we conclude that $\textsc{meas}\mathrm{QTDP}[1-2^{-l(n)}, 2^{-l(n)}]$ and $\mathrm{QTDP}[1-2^{-l(n)}, 2^{-l(n)}]$ are indeed contained in QSZK. □

Polarization lemmas for $\mathrm{QTD}^{\mathrm{meas}}$ and QTD

We now present the proof of the polarization lemmas for $\mathrm{QTD}^{\mathrm{meas}}$ (Lemma 7.25) and QTD (Lemma 7.26). The proof technique utilizes one-sided error reduction, for both *yes* instances and *no* instances, separately and alternately.

No-instance error reduction for $\textsc{meas}\mathrm{QTDP}$ and QTDP. We begin with *no*-instance error reduction, commonly referred to as the XOR lemma in the polarization lemma for SDP. It is noteworthy that the corresponding results for both $\mathrm{QTD}^{\mathrm{meas}}$ and QTD share the same equality.

Lemma 7.28 (No-instance error reduction for $\textsc{meas}\mathrm{QTDP}$ and QTDP)**.** *Given quantum circuits Q_0 and Q_1 that prepare the quantum states ρ_0 and ρ_1, respectively, there exists a deterministic procedure that, on input (Q_0, Q_1, l), produces new quantum circuits $\tilde{Q}_0$ and $\tilde{Q}_1$ preparing the states $\tilde{\rho}_0$ and $\tilde{\rho}_1$, respectively. These states are defined as $\tilde{\rho}_b = 2^{-l+1} \sum_{b_1 \oplus \cdots \oplus b_l = b} \rho_{b_1} \otimes \cdots \otimes \rho_{b_l}$ for $b \in \{0, 1\}$, and satisfy the following equalities:*
$$\mathrm{QTD}^{\mathrm{meas}}(\tilde{\rho}_0, \tilde{\rho}_1) = \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1)^l \quad \textit{and} \quad \mathrm{QTD}(\tilde{\rho}_0, \tilde{\rho}_1) = \mathrm{QTD}(\rho_0, \rho_1)^l.$$

Proof. It suffices to prove that for quantum states ρ_0, ρ_1, ρ_0', and ρ_1', defining
$$\tilde{\rho}_0 \coloneqq \frac{1}{2}(\rho_0' \otimes \rho_0 + \rho_1' \otimes \rho_1) \text{ and } \tilde{\rho}_1 \coloneqq \frac{1}{2}(\rho_0' \otimes \rho_1 + \rho_1' \otimes \rho_0),$$
the following equalities hold:
$$\mathrm{QTD}^{\mathrm{meas}}(\tilde{\rho}_0, \tilde{\rho}_1) = \mathrm{QTD}^{\mathrm{meas}}(\rho_0', \rho_1') \cdot \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1), \tag{7.9}$$
$$\mathrm{QTD}(\tilde{\rho}_0, \tilde{\rho}_1) = \mathrm{QTD}(\rho_0', \rho_1') \cdot \mathrm{QTD}(\rho_0, \rho_1). \tag{7.10}$$
Consequently, we can conclude the proof by inductively applying Equation (7.9) to $\mathrm{QTD}^{\mathrm{meas}}\left(\tilde{\rho}_0^{(l)}, \tilde{\rho}_1^{(l)}\right)$, and Equation (7.10) to $\mathrm{QTD}\left(\tilde{\rho}_0^{(l)}, \tilde{\rho}_1^{(l)}\right)$.

It remains to demonstrate the equalities in Equations (7.9) and (7.10). For Equation (7.9), mirroring the approach of Proposition 4.12 in [BDRV19], we obtain:
$$\mathrm{QTD}^{\mathrm{meas}}(\tilde{\rho}_0, \tilde{\rho}_1) = \sup_{\text{POVM } \mathcal{E}} \mathrm{TD}\left(\tilde{p}_0^{(\mathcal{E})}, \tilde{p}_1^{(\mathcal{E})}\right)$$

$$
\begin{aligned}
&= \sup_{\text{POVM } \mathcal{E}} \mathrm{TD}\left(p_0^{(\mathcal{E})}, p_1^{(\mathcal{E})}\right) \cdot \mathrm{TD}\left(p_0'^{(\mathcal{E})}, p_1'^{(\mathcal{E})}\right) \\
&= \sup_{\text{POVM } \mathcal{E}_1} \mathrm{TD}\left(p_0^{(\mathcal{E}_1)}, p_1^{(\mathcal{E}_1)}\right) \cdot \sup_{\text{POVM } \mathcal{E}_2} \mathrm{TD}\left(p_0'^{(\mathcal{E}_2)}, p_1'^{(\mathcal{E}_2)}\right) \\
&= \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) \cdot \mathrm{QTD}^{\mathrm{meas}}(\rho_0', \rho_1').
\end{aligned}
$$

For Equation (7.10), the equality follows from the equalities:

$$
\tilde{\rho}_0 - \tilde{\rho}_1 = \frac{1}{2}(\rho_0' - \rho_1') \otimes (\rho_0 - \rho_1) \quad \text{and} \quad \tilde{\rho}_0 + \tilde{\rho}_1 = \frac{1}{2}(\rho_0' + \rho_1') \otimes (\rho_0 + \rho_1). \qquad \square
$$

Yes-instance error reduction for MEASQTDP and QTDP. We then proceed with *yes*-instance error reduction, which is referred to as the direct product lemma in polarization lemma for SDP. Notably, the $\mathrm{QTD}^{\mathrm{meas}}$ case (Lemma 7.29) achieves a lower bound with a *quadratic* improvement compared to both the trace distance case [Wat02, Lemma 9] and the QTD case (Lemma 7.30). However, the upper bound is slightly worse than the trace distance case, reflecting a key distinction: while the trace distance and total variation distance are metrics, the triangular discrimination and its quantum analogs ($\mathrm{QTD}^{\mathrm{meas}}$ and QTD) are (conjectured to be) the *squares* of a metric.

Lemma 7.29 (Yes-instance error reduction for MEASQTDP)**.** *Given quantum circuits Q_0 and Q_1 that prepare the quantum states ρ_0 and ρ_1, respectively, there exists a deterministic procedure that, on input (Q_0, Q_1, l), produces new quantum circuits $\tilde{Q}_0$ and $\tilde{Q}_1$ preparing the states $\tilde{\rho}_0$ and $\tilde{\rho}_1$. These states are defined as $\tilde{\rho}_b \coloneqq \rho_b^{\otimes l}$ for $b \in \{0,1\}$, and satisfy the inequalities*:

$$
1 - \exp\left(-\frac{l}{2} \cdot \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1)\right) \leq \mathrm{QTD}^{\mathrm{meas}}(\tilde{\rho}_0, \tilde{\rho}_1) \leq 2l \cdot \mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1).
$$

Proof. The proof follows the approach of [BDRV19, Lemma 4.10], utilizing a key property of the Bures distance on tensor-product states $\rho_0^{\otimes l}$ and $\rho_1^{\otimes l}$:

$$
\frac{1}{2}\mathrm{B}^2\left(\rho_0^{\otimes l}, \rho_1^{\otimes l}\right) = 1 - \mathrm{F}\left(\rho_0^{\otimes l}, \rho_1^{\otimes l}\right) = 1 - \mathrm{F}(\rho_0, \rho_1)^l = 1 - \left(1 - \frac{1}{2}\mathrm{B}^2(\rho_0, \rho_1)\right)^l. \tag{7.11}
$$

By utilizing the inequalities in Lemma 7.14, we obtain the following upper bound:

$$
\begin{aligned}
\mathrm{QTD}^{\mathrm{meas}}(\rho_0^{\otimes l}, \rho_1^{\otimes l}) &\leq \mathrm{B}^2(\rho_0^{\otimes l}, \rho_1^{\otimes l}) \\
&= 2\left(1 - \left(1 - \tfrac{1}{2}\mathrm{B}^2(\rho_0, \rho_1)\right)^l\right) \\
&\leq l\mathrm{B}^2(\rho_0, \rho_1) \\
&\leq 2l\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1).
\end{aligned}
$$

Here, the third line is because $(1-x)^k \geq 1 - kx$ for any x and integer k.

Likewise, we can also deduce the following lower bound:

$$
\begin{aligned}
\mathrm{QTD}^{\mathrm{meas}}(\rho_0^{\otimes l}, \rho_1^{\otimes l}) &\geq \tfrac{1}{2}\mathrm{B}^2(\rho_0^{\otimes l}, \rho_1^{\otimes l}) \\
&= \left(1 - \left(1 - \tfrac{1}{2}\mathrm{B}^2(\rho_0, \rho_1)\right)^l\right) \\
&\geq \left(1 - \left(1 - \tfrac{1}{2}\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1)\right)^l\right) \\
&\geq 1 - \exp\left(-\tfrac{l}{2}\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1)\right).
\end{aligned}
$$

We complete the proof by noting that the last line owes to $1 - x \leq e^{-x}$ for any x. □

Interestingly, the lower bound in Lemma 7.30 matches that of the trace distance case, even though the proof techniques differ. The trace distance case relies on the triangle inequality, which is only *conjectured* to hold for $\sqrt{\mathrm{QTD}}$. In contrast, our proof circumvents this barrier by leveraging the inequalities between QTD and the Bures distance.

Lemma 7.30 (Yes-instance error reduction for QTDP)**.** *Given quantum circuits Q_0 and Q_1 that prepare the quantum states ρ_0 and ρ_1, respectively, there exists a deterministic procedure that, on input (Q_0, Q_1, l), produces new quantum circuits $\tilde{Q}_0$ and $\tilde{Q}_1$ preparing the states $\tilde{\rho}_0$ and $\tilde{\rho}_1$. These states are defined as $\tilde{\rho}_b := \rho_b^{\otimes l}$ for $b \in \{0, 1\}$, and satisfy the inequalities*:

$$1 - \exp\left(-\frac{l}{2} \cdot \mathrm{QTD}(\rho_0, \rho_1)^2\right) \leq \mathrm{QTD}(\tilde{\rho}_0, \tilde{\rho}_1) \leq \sqrt{2l} \cdot \sqrt{\mathrm{QTD}(\rho_0, \rho_1)}.$$

Proof. Our proof strategy closely follows the approach used in Lemma 7.29. For the upper bound, we use the inequalities from Lemma 7.15 and Equation (7.11), which give

$$\mathrm{QTD}\left(\rho_0^{\otimes l}, \rho_1^{\otimes l}\right) \leq \mathrm{B}\left(\rho_0^{\otimes l}, \rho_1^{\otimes l}\right) \leq \sqrt{l} \cdot \mathrm{B}(\rho_0, \rho_1) \leq \sqrt{2l} \cdot \sqrt{\mathrm{QTD}(\rho_0, \rho_1)}.$$

For the lower bound, we again apply Lemma 7.15 and Equation (7.11), obtaining

$$\begin{aligned}
\mathrm{QTD}\left(\rho_0^{\otimes l}, \rho_1^{\otimes l}\right) \geq \frac{1}{2}\mathrm{B}^2\left(\rho_0^{\otimes l}, \rho_1^{\otimes l}\right) &= 1 - \left(1 - \frac{1}{2}\mathrm{B}^2(\rho_0, \rho_1)\right)^l \\
&\geq 1 - \left(1 - \frac{1}{2}\mathrm{QTD}(\rho_0, \rho_1)^2\right)^l \\
&\geq 1 - \exp\left(-\frac{l}{2} \cdot \mathrm{QTD}(\rho_0, \rho_1)^2\right).
\end{aligned}$$

□

Putting everything together. We can now establish Lemmas 7.25 and 7.26 by selecting appropriate parameters based on the polarization lemma for the triangular discrimination, as established in [BDRV19, Lemma 4.9].

Specifically, we first apply *no*-instance error reduction (Lemma 7.28), then use *yes*-instance error reduction (Lemma 7.29 or Lemma 7.30) to ensure that the soundness parameter is at most 1/2, and finally apply *no*-instance error reduction (Lemma 7.28) again. The time complexity analysis aligns with [CCKV08, Lemma 38].

Proof of Lemma 7.25. Let $\lambda := \min\{\alpha/\beta, 2\} \in (1, 2]$, and choose $l := \lceil \log_\lambda 8k \rceil$. Applying the *no*-instance error reduction for MEASQTDP (Lemma 7.28) to the input (Q_0, Q_1, l), where the quantum circuits Q_0 and Q_1 prepare the states ρ_0 and ρ_1, respectively, produces new quantum circuits (Q_0', Q_1') with corresponding states (ρ_0', ρ_1') such that:

$$\begin{aligned}
\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) \geq \alpha \quad &\Longrightarrow \quad \mathrm{QTD}^{\mathrm{meas}}(\rho_0', \rho_1') \geq \alpha^l; \\
\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) \leq \beta \quad &\Longrightarrow \quad \mathrm{QTD}^{\mathrm{meas}}(\rho_0', \rho_1') \leq \beta^l.
\end{aligned}$$

Let $m := \lambda^l/(4\alpha^l) \leq 1/(4\beta^l)$, and define the states $\rho_0'' := (\rho_0')^{\otimes m}$ and $\rho_1'' := (\rho_1')^{\otimes m}$, along with the corresponding circuits Q_0'' and Q_1''. Applying the *yes*-instance error reduction for MEASQTDP (Lemma 7.29) to the input (Q_0', Q_1', m) yields that:

$$\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) \geq \alpha \quad \Longrightarrow \quad \mathrm{QTD}^{\mathrm{meas}}(\rho_0'', \rho_1'') \geq 1 - \exp(-\alpha^l m/2) \geq 1 - e^{-k};$$

$$\mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1)\le\beta \quad\Longrightarrow\quad \mathrm{QTD}^{\mathrm{meas}}(\rho_0'',\rho_1'')\le 2m\beta^l\le 1/2.$$

Finally, applying the *no*-instance error reduction for MEASQTDP (Lemma 7.28) again to the input (Q_0'',Q_1'',k) produces new quantum circuits $(\tilde{Q}_0,\tilde{Q}_1)$ with the corresponding states $(\tilde{\rho}_0,\tilde{\rho}_1)$, satisfying:

$$\begin{aligned}&\mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1)\ge\alpha \quad\Longrightarrow\quad \mathrm{QTD}^{\mathrm{meas}}(\tilde{\rho}_0,\tilde{\rho}_1)\ge(1-e^{-k})^k\ge 1-ke^{-k}\ge 1-2^{-k};\\ &\mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1)\le\beta \quad\Longrightarrow\quad \mathrm{QTD}^{\mathrm{meas}}(\tilde{\rho}_0,\tilde{\rho}_1)\le 2^{-k}.\end{aligned}$$

The last step holds for sufficiently large k, which we can be determined by selecting an appropriate value at the beginning of our construction.

The time complexity analysis follows a similar approach to [CCKV08, Lemma 38]. Specifically, noting that $\lambda\in(1,2]$, we have

$$\ln(\lambda)=\ln(1+(\lambda-1))\ge\frac{\lambda-1}{2}\ge\Omega\left(\frac{\alpha-\beta}{\beta}\right).$$

Here, the first inequality is due to $\ln(1+x)\ge x/2$ for all $x\in[0,1]$. Then, we obtain $l=O\left(\frac{\ln k}{\ln\lambda}\right)=O\left(\frac{\beta\ln k}{\alpha-\beta}\right)$ and further conclude that

$$m\le\frac{1}{4}\cdot\left(\frac{2}{\alpha}\right)^l=\exp\left(O\left(\frac{\beta\ln k}{\alpha-\beta}\cdot\ln\left(\frac{2}{\alpha}\right)\right)\right).$$ □

Proof of Lemma 7.26. Our proof strategy closely mirrors the approach used in Lemma 7.25, but with different parameters λ,l,m, and some intermediate steps are omitted for brevity.

We set $\lambda:=\min\{\alpha^2/\beta,2\}\in(1,2]$, and choose $l:=\lceil\log_\lambda(16k)\rceil$. By applying the *no*-instance error reduction for QTDP (Lemma 7.28) to the input (Q_0,Q_1,l), we obtain the circuits (Q_0',Q_1') and the corresponding states (ρ_0',ρ_1'), satisfying:

$$\begin{aligned}&\mathrm{QTD}(\rho_0,\rho_1)\ge\alpha \quad\Longrightarrow\quad \mathrm{QTD}(\rho_0',\rho_1')\ge\alpha^l;\\ &\mathrm{QTD}(\rho_0,\rho_1)\le\beta \quad\Longrightarrow\quad \mathrm{QTD}(\rho_0',\rho_1')\le\beta^l.\end{aligned}$$

Next, let $m:=\lambda^l/(8\alpha^{2l})\le 1/(8\beta^l)$. Applying the *yes*-instance error reduction for QTDP (Lemma 7.30) to the input (Q_0',Q_1',m), where the resulting circuits and states are denoted by (Q_0'',Q_1'') and (ρ_0'',ρ_1''), respectively, yields the following:

$$\begin{aligned}&\mathrm{QTD}(\rho_0,\rho_1)\ge\alpha \quad\Longrightarrow\quad \mathrm{QTD}(\rho_0'',\rho_1'')\ge 1-\exp(-\alpha^{2l}m/2)\ge 1-e^{-k};\\ &\mathrm{QTD}(\rho_0,\rho_1)\le\beta \quad\Longrightarrow\quad \mathrm{QTD}(\rho_0'',\rho_1'')\le\sqrt{2m}\beta^{l/2}\le 1/2.\end{aligned}$$

Lastly, applying the *no*-instance error reduction for QTDP (Lemma 7.28) again to the input (Q_0'',Q_1'',k) results in the circuits $(\tilde{Q}_0,\tilde{Q}_1)$ and the corresponding states $(\tilde{\rho}_0,\tilde{\rho}_1)$, where it holds that:

$$\begin{aligned}&\mathrm{QTD}(\rho_0,\rho_1)\ge\alpha \quad\Longrightarrow\quad \mathrm{QTD}(\tilde{\rho}_0,\tilde{\rho}_1)\ge(1-e^{-k})^k\ge 1-ke^{-k}\ge 1-2^{-k};\\ &\mathrm{QTD}(\rho_0,\rho_1)\le\beta \quad\Longrightarrow\quad \mathrm{QTD}(\tilde{\rho}_0,\tilde{\rho}_1)\le 2^{-k}.\end{aligned}$$

The time complexity analysis follows similarly to the proof of Lemma 7.25. Since $\lambda\in(1,2]$, we obtain $\ln\lambda\ge\Omega\left(\frac{\alpha^2-\beta}{\beta}\right)$, and thus $l=O\left(\frac{\ln k}{\ln\lambda}\right)=O\left(\frac{\beta\ln k}{\alpha^2-\beta}\right)$. Consequently, we conclude that $m\le(2/\alpha^2)^l/8\le\exp\left(O\left(\frac{\beta\ln k}{\alpha^2-\beta}\cdot\ln(2/\alpha^2)\right)\right)$. □

7.3.4 QSZK-hardness of QJSP, QEDP, measQTDP, and QTDP

QJSP is QSZK-hard. We begin by establishing the QSZK-hardness of the Quantum Jensen-Shannon Divergence Problem (QJSP):

Lemma 7.31 (QJSP is QSZK-hard)**.** *Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions, there exists a constant $\epsilon \in (0, 1/2)$ such that*

$$\mathrm{QJSP}[\alpha, \beta] \text{ is } \mathsf{QSZK}\text{-hard},$$

when $\alpha(n) \leq 1 - 2^{-n^{1/2-\epsilon}}$ and $\beta(n) \geq 2^{-n^{1/2-\epsilon}}$ for large enough n.

Following the approach for showing that JSP is SZK-hard [BDRV19, Lemma 4.3], we prove Lemma 7.31 by utilizing inequalities between the trace distance and $\mathrm{QJS}_{\mathrm{bit}}$ (combining Lemma 3.25 and Lemma 3.26), which mirror the inequalities between the total variation distance and the Jensen-Shannon divergence [FvdG99, Top00].

Proof of Lemma 7.31. By Lemma 3.37, it suffices to reduce $\mathrm{QSDP}\left[1-2^{-n^{1/2-\epsilon/2}}, 2^{-n^{1/2-\epsilon/2}}\right]$ to $\mathrm{QJSP}[\alpha, \beta]$, where α and β will be specified later. Consider quantum circuits Q_0 and Q_1 acting on n qubits, which is a QSDP instance. We can obtain ρ_i for $i \in \{0, 1\}$ by performing Q_i on $|0^n\rangle$ and tracing out the non-output qubits. This yields the following:

- If $\mathrm{T}(\rho_0, \rho_1) \geq 1 - 2^{-n^{1/2-\epsilon/2}}$, then Lemma 3.25 indicates that

$$\begin{aligned}
\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) &\geq 1 - \mathrm{H}_{\mathrm{bit}}\left(\frac{1 - \mathrm{T}(\rho_0, \rho_1)}{2}\right) \\
&\geq 1 - \mathrm{H}_{\mathrm{bit}}\left(2^{-n^{1/2-\epsilon/2}-1}\right) \\
&\geq 1 - 2 \cdot 2^{-(n^{1/2-\epsilon/2}+1)/2} \\
&\geq \alpha(n),
\end{aligned}$$

  where the third inequality owes to $\mathrm{H}_{\mathrm{bit}}(x) \leq 2\sqrt{x}$ for all $x \in [0, 1]$. Then we choose a constant $n(\epsilon)$ such that the last inequality holds. Specifically, there exists a constant $n(\epsilon)$ such that $1 - 2 \cdot 2^{-(n^{1/2-\epsilon/2}+1)/2} \geq 1 - 2^{-n^{1/2-\epsilon}}$ for all $n \geq n(\epsilon)$.

- If $\mathrm{T}(\rho_0, \rho_1) \leq 2^{-n^{1/2-\epsilon/2}}$, then according to Lemma 3.26, we have

$$\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1) \leq \mathrm{T}(\rho_0, \rho_1) \leq 2^{-n^{1/2-\epsilon/2}} \leq \beta(n).$$

  Here, the last inequality holds for any $n \geq n(\epsilon)$ since $\beta(n) \geq 2^{-n^{1/2-\epsilon/2}}$.

Therefore, by utilizing the same quantum circuits Q_0 and Q_1 and their corresponding states ρ_0 and ρ_1, we establish a Karp reduction from $\mathrm{QSDP}\left[1 - 2^{-n^{1/2-\epsilon/2}}, 2^{-n^{1/2-\epsilon/2}}\right]$ to $\mathrm{QJSP}[\alpha, \beta]$ for $n \geq n(\epsilon)$. □

A simple QSZK-hardness proof for QEDP. Furthermore, we can establish a new and simple reduction from QSDP to QEDP via QJSP by combining Lemma 7.22 and Lemma 7.31. This reduction leads to a simple QSZK-hardness proof for QEDP, as stated in Corollary 7.21. Now we present the detailed proof:

Proof of Corollary 7.21. Using Lemma 7.31, we obtain that $\mathrm{QJSP}[\alpha, \beta]$ is QSZK-hard when $\alpha(n) \leq 1 - 2^{-n^{1/2-\epsilon}}$ and $\beta(n) \geq 2^{-n^{1/2-\epsilon}}$ for some $\epsilon \in (0, 1/2)$ and $n \geq n(\epsilon)$. The

hard instances for QSDP (simultaneously hard for QJSP), as specified in Lemma 7.31, consist of quantum circuits Q_0 and Q_1, acting on n qubits, that prepare a purification of $r(n)$-qubit states ρ_0 and ρ_1, respectively.

Subsequently, by using Lemma 7.22, we construct quantum circuits Q'_0 and Q'_1 acting on $m'(n') = n' + 2$ qubits, where $n' := n + 1$, preparing a purification of n'-qubit states

$$\rho'_0 = (p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|) \otimes (\frac{1}{2}\rho_0 + \frac{1}{2}\rho_1),$$
$$\rho'_1 = \frac{1}{2}|0\rangle\langle 0| \otimes \rho_0 + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_1.$$

Here, the parameter p satisfies $\mathrm{H}_{\mathrm{bit}}(p) = 1 - \frac{\ln 2}{2}(\alpha + \beta)$.

According to Lemma 7.22, QEDP$[g(n)]$ is QSZK-hard as long as

$$g(n') = \frac{\ln 2}{2}(\alpha(n'-1) - \beta(n'-1)) \leq \frac{\ln 2}{2}\left(1 - 2^{-(n'-1)^{1/2-\epsilon}+1}\right).$$

As a consequence, QSDP is Karp reducible to QEDP by mapping (Q_0, Q_1) to (Q'_0, Q'_1). To finish the proof, we redefine $n := n'$, replacing n' with n in the QSZK-hardness condition for QEDP. □

measQTDP and QTDP are QSZK-hard Next, we prove the QSZK-hardness of both the Measured Quantum Triangular Discrimination Problem (measQTDP) and the Quantum Triangular Discrimination Problem (QTDP):

Lemma 7.32 (measQTDP and QTDP are QSZK-hard)**.** *Let $\alpha(n)$ and $\beta(n)$ be efficiently computable functions, there exists a constant $\epsilon \in (0, 1/2)$ such that*

$$\text{measQTDP}[\alpha, \beta] \text{ and } \text{QTDP}[\alpha, \beta] \text{ are QSZK-hard,}$$

when $\alpha(n) \leq 1 - 2^{-n^{1/2-\epsilon}}$ and $\beta(n) \geq 2^{-n^{1/2-\epsilon}}$ for large enough n.

The proof parallels the approach to demonstrate that TDP is SZK-hard [BDRV19, Lemma 4.4]. We employ the inequalities between the trace distance and $\mathrm{QTD}^{\mathrm{meas}}$, as presented in Theorem 7.7, analogous to the inequalities between the counterpart classical distances in [Top00].

Proof of Lemma 7.32. Since the inequalities between the trace distance and QTD coincides with those of $\mathrm{QTD}^{\mathrm{meas}}$, we focus on proving that measQTDP is QSZK-hard in the desired regime. The proof can then be straightforwardly extended to the QTDP case.

By leveraging Lemma 3.37, it suffices to reduce $\mathrm{QSDP}\left[1 - 2^{-n^{1/2-\epsilon/2}}, 2^{-n^{1/2-\epsilon/2}}\right]$ to measQTDP$[\alpha, \beta]$, where α and β will be specified later. Consider quantum circuits Q_0 and Q_1 acting on n qubits, which is a QSDP instance. We can obtain ρ_i for $i \in \{0, 1\}$ by performing Q_i on $|0^n\rangle$ and tracing out the non-output qubits. This yields the following:

- If $\mathrm{T}(\rho_0, \rho_1) \geq 1 - 2^{-n^{1/2-\epsilon/2}}$, then Lemma 7.13 indicates that

  $$\mathrm{QTD}^{\mathrm{meas}}(\rho_0, \rho_1) \geq \mathrm{T}(\rho_0, \rho_1)^2 \geq \left(1 - 2^{-n^{1/2-\epsilon/2}}\right)^2 \geq 1 - 2^{-n^{1/2-\epsilon/2}+1} \geq \alpha(n).$$

  We can choose a constant $n(\epsilon)$ such that $1 - 2^{-n^{1/2-\epsilon/2}+1} \geq 1 - 2^{-n^{1/2-\epsilon}}$ for all $n \geq n(\epsilon)$.

- If $\mathrm{T}(\rho_0,\rho_1) \leq 2^{-n^{1/2-\epsilon/2}}$, then according to Lemma 7.10 and Lemma 7.6, we have

$$\mathrm{QTD}^{\mathrm{meas}}(\rho_0,\rho_1) \leq \mathrm{T}(\rho_0,\rho_1) \leq 2^{-n^{1/2-\epsilon/2}} \leq \beta(n).$$

  Here, the last inequality holds for any $n \geq n(\epsilon)$ because $\beta(n) \geq 2^{-n^{1/2-\epsilon/2}}$.

Therefore, by employing the same quantum circuits Q_0 and Q_1 and their corresponding states ρ_0 and ρ_1, we establish a Karp reduction from $\mathrm{QSDP}\left[1-2^{-n^{1/2-\epsilon/2}}, 2^{-n^{1/2-\epsilon/2}}\right]$ to $\mathrm{MEAS}\mathrm{QTDP}[\alpha,\beta]$ for $n \geq n(\epsilon)$. □

7.4 Easy regimes for the class QSZK

We begin with the main results in this section:

Theorem 7.33 (Easy regimes for QSZK)**.** *For any efficiently computable functions α and β, we have the following easy regimes for* QSZK *in terms of* $\overline{\mathrm{QSDP}}$*:*

(1) $\overline{\mathrm{QSDP}}[\alpha,\beta]$ *is in* PP *when* $1-2^{-n/2-1} \leq \alpha(n) \leq 1$ *and* $0 \leq \beta(n) \leq 2^{-n/2-1}$.

(2) $\overline{\mathrm{QSDP}}[1,0]$ *is in* NQP.

Theorem 7.33 aligns with classical counterparts regarding SZK. Particularly, Theorem 7.33(1) is a quantum analog of [BCH+19, Theorem 7.1], stating that $\overline{\mathrm{SDP}}$ with some inverse-exponential errors is in PP. Meanwhile, Theorem 7.33(2) parallels a folklore result that $\overline{\mathrm{SDP}}$ without error is in NP, as NQP can be viewed as a quantum analog of NP.

Furthermore, Theorem 7.33(1) suggests that achieving a *dimension-preserving* polarization for the Quantum State Distinguishability Problem (QSDP) demands non-black-box techniques due to the existing oracle separation [BCH+19]. This is because the existence of such a polarization would imply, by Theorem 7.33(1), that QSZK ⊆ PP.

7.4.1 $\overline{\mathrm{QSDP}}$ without error is in NQP

As a prelude to Theorem 7.33(1), we will first establish Theorem 7.33(2). Specifically, through a crucial observation concerning $\mathrm{T}(\rho_0,\rho_1)$ and $\mathrm{Tr}(\rho_0\rho_1)$, we can devise a unitary quantum algorithm $\mathcal{A}$ using the SWAP test. The acceptance probability of A is at least slightly higher than $1/2$ for *yes* instances, while exactly $1/2$ for *no* instances. We then apply exact amplitude amplification (Lemma 2.17) on $\mathcal{A}$ to construct another algorithm $\mathcal{A}'$ that achieves one-sided error.

Proof of Theorem 7.33(2). For any states ρ_0 and ρ_1, we can observe the following:

- For *yes* instances where $\mathrm{T}(\rho_0,\rho_1) = 0$, we have $\rho_0 = \rho_1$ due to the trace distance being a metric. This equality leads to $\mathrm{Tr}(\rho_0\rho_1) \geq 2^{-n}$, with equality achieved when both ρ_0 and ρ_1 correspond to the maximally mixed state $2^{-n}I_n$, where I_n denotes the identity matrix on n qubits.
- For *no* instances where $\mathrm{T}(\rho_0,\rho_1) = 1$, we know that ρ_0 and ρ_1 have orthogonal supports because of the triangle inequality, leading to $\mathrm{Tr}(\rho_0\rho_1) = 0$.

Unitary construction using the SWAP test. We utilize the SWAP test [BCWdW01] to test the closeness of quantum (mixed) states ρ_0 and ρ_1. Our approach involves a single-

qubit quantum register C, along with quantum registers $\mathsf{A} = (\mathsf{A}_0, \mathsf{A}_1)$ and $\mathsf{S} = (\mathsf{S}_0, \mathsf{S}_1)$, all initialized to the state $|0\rangle$. Subsequently, we apply state-preparation circuits Q_i on registers A_i and S_i for $i \in \{0,1\}$. Then, we perform the SWAP test on registers C, S_0, and S_1, where C serves as the control qubit. Leveraging Proposition 9 in [KMY09], we obtain the following unitary (i.e., algorithm $\mathcal{A}$):

$$U|0\rangle_{\mathsf{C}}|\bar{0}\rangle_{\mathsf{A},\mathsf{S}} = \sqrt{p}|0\rangle_{\mathsf{C}}|\psi_0\rangle_{\mathsf{A},\mathsf{S}} + \sqrt{1-p}|1\rangle_{\mathsf{C}}|\psi_1\rangle_{\mathsf{A},\mathsf{S}} \text{ where } p = \tfrac{1}{2}\Big(1 + \mathrm{Tr}(\rho_0\rho_1)\Big). \tag{7.12}$$

Next, we introduce another single-qubit register F, initialized to zero, leading to:

$$\begin{aligned} &(H \otimes U)|0\rangle_{\mathsf{F}}|0\rangle_{\mathsf{C}}|\bar{0}\rangle_{\mathsf{A},\mathsf{S}} \\ &= \sum_{k_0 \in \{0,1\}} \sqrt{\frac{p}{2}}|0\rangle_{\mathsf{F}}|k_0\rangle_{\mathsf{C}}|\psi_0\rangle_{\mathsf{A},\mathsf{S}} + \sum_{k_1 \in \{0,1\}} \sqrt{\frac{1-p}{2}}|1\rangle_{\mathsf{F}}|k_1\rangle_{\mathsf{C}}|\psi_1\rangle_{\mathsf{A},\mathsf{S}} \\ &\coloneqq \sqrt{\frac{p}{2}}|0\rangle_{\mathsf{F}}|0\rangle_{\mathsf{C}}|\psi_0\rangle_{\mathsf{A},\mathsf{S}} + \sqrt{1-\frac{p}{2}}|\perp\rangle_{\mathsf{F},\mathsf{C},\mathsf{A},\mathsf{S}}. \end{aligned} \tag{7.13}$$

Making the error one-sided through exact amplitude amplification. Now we devise a one-sided error algorithm $\mathcal{A}'$ by utilizing $\mathcal{A}$ as a building block. Let us consider the Grover operator

$$G \coloneqq -(H \otimes U)(I - 2|\bar{0}\rangle\langle\bar{0}|_{\mathsf{F},\mathsf{C},\mathsf{A},\mathsf{S}})(H \otimes U^\dagger)(I - 2\Pi_0).$$

Here, Π_0 is the projector onto the subspace spanned by $\{|0\rangle_{\mathsf{F}}|0\rangle_{\mathsf{C}}|\phi\rangle_{\mathsf{A},\mathsf{S}}\}$ over all $|\phi\rangle$. By utilizing the exact amplitude amplification (Lemma 2.17), it holds that

$$G(H \otimes U)|0\rangle_{\mathsf{F}}|0\rangle_{\mathsf{C}}|\bar{0}\rangle_{\mathsf{A},\mathsf{S}} = \sin(3\theta)|0\rangle_{\mathsf{F}}|0\rangle_{\mathsf{C}}|\psi_0\rangle_{\mathsf{A},\mathsf{S}} + \cos(3\theta)|\perp\rangle_{\mathsf{F},\mathsf{C},\mathsf{A},\mathsf{S}}, \text{ where } \theta \in [0, \pi/4].$$

According to Equation (7.13), p satisfies $\sin(\theta)^2 = p/2$. Let x_{F} and x_{C} be the measurement outcomes of the registers F and C, respectively, after a single iteration of G. The resulting algorithm $\mathcal{A}'$ rejects if $x_{\mathsf{F}} = x_{\mathsf{C}} = 0$; otherwise, it accepts. Therefore, the acceptance probability of $\mathcal{A}'$ is $p_{\mathrm{acc}} = 1 - \Pr[x_{\mathsf{F}} = x_{\mathsf{C}} = 0]$ where $\Pr[x_{\mathsf{F}} = x_{\mathsf{C}} = 0]$ satisfies:

$$\begin{aligned} \Pr[x_{\mathsf{F}} = x_{\mathsf{C}} = 0] &= \sin^2(3\theta) \\ &= \sin^6\theta - 6\cos^2\theta\sin^4\theta + 9\cos^4\theta\sin^2\theta \\ &= 2p^3 - 6p^2 + \frac{9}{2}p \end{aligned} \tag{7.14}$$

Finally, we complete the analysis of $\mathcal{A}'$ as follows:

- For *yes* instances, we can plug $\mathrm{Tr}(\rho_0\rho_1) \geq 2^{-n}$ into Equation (7.12), which implies $p \geq \frac{1}{2} + 2^{-n-1}$. Noting that $2p^3 - p^2 + \frac{9}{2}p \leq 1 - (p - \frac{1}{2})^2$ for any $0 \leq p \leq 1$, together with Equation (7.14), we obtain $p_{\mathrm{acc}} \geq (p - \frac{1}{2})^2 \geq 2^{-2n-2}$.
- For *no* instances, we can set $\mathrm{Tr}(\rho_0\rho_1) = 0$ in Equation (7.12), resulting in $p = 1/2$ and $\theta = \pi/6$. Following Equation (7.14), we know that $\mathcal{A}'$ rejects with certainty, equivalently $p_{\mathrm{acc}} = 0$.

We thus conclude that $\mathcal{A}'$ is an NQP algorithm as desired. □

As mentioned earlier, Theorem 7.33(2) has a classical counterpart, namely $\overline{\mathrm{SDP}}[1,0]$ is in NP. The proof of this folklore result is outlined below. Let p_0 and p_1 be two probability distributions. The collision distance between p_0 and p_1 is defined as $\mathrm{Col}(p_0, p_1) \coloneqq \sum_x p_0(x)p_1(x)$. Then, it follows that

- If $\mathrm{TV}(p_0, p_1) = 1$, we obtain $\mathrm{Col}(p_0, p_1) = 0$.
- If $\mathrm{TV}(p_0, p_1) = 0$, we have $\mathrm{Col}(p_0, p_1) \geq 1/|\mathrm{supp}\,(p_0) \cap \mathrm{supp}\,(p_1)\,|$, with equality occurring when p_0 and p_1 are uniform on $\mathrm{supp}\,(p_0) \cap \mathrm{supp}\,(p_1)$.

This observation suffices for establishing the NP containment of $\overline{\mathrm{SDP}}[1, 0]$. Specifically, noting that there exists $x \in \mathrm{supp}\,(p_0) \cup \mathrm{supp}\,(p_1)$ for $\mathrm{TV}(p_0, p_1) = 0$, then the prover could provide the corresponding w_0 and w_1 as a witness such that $C_0(w_0) = C_1(w_1) = x$. Additionally, such a witness does not exist for *no* instances, i.e., $\mathrm{TV}(p_0, p_1) = 1$.

7.4.2 $\overline{\mathrm{QSDP}}$ with some inverse-exponential errors is in PP

The crucial insight for comprehending the PP containment of $\overline{\mathrm{QSDP}}$ with tinily errors is given by the expression

$$\mathrm{HS}^2(\rho_0, \rho_1) = \frac{1}{2}\mathrm{Tr}(\rho_0 - \rho_1)^2 = \frac{1}{2}\Big(\mathrm{Tr}(\rho_0^2) + \mathrm{Tr}(\rho_1^2)\Big) - \mathrm{Tr}(\rho_0\rho_1).$$

It is noteworthy that by employing the SWAP test [BCWdW01] for mixed states, such as [KMY09, Proposition 9], one can estimate these three terms: $\mathrm{Tr}(\rho_0^2)$, $\mathrm{Tr}(\rho_1^2)$, and $\mathrm{Tr}(\rho_0\rho_1)$. This estimation enables the development of a hybrid algorithm. Subsequently, we proceed to establish Theorem 7.33(1), which can be viewed as the quantum counterpart of [BCH+19, Theorem 7.1].

Proof of Theorem 7.33(1). Consider two n-qubit quantum states, denoted as ρ_0 and ρ_1, defined in a finite-dimensional Hilbert space $\mathcal{H}$ according to Definition 3.33. Following Lemma 3.20, it holds that:

$$\mathrm{HS}(\rho_0, \rho_1) \leq \mathrm{T}(\rho_0, \rho_1) \leq \sqrt{\dim \mathcal{H}} \cdot \mathrm{HS}(\rho_0, \rho_1). \tag{7.15}$$

We present a hybrid classical-quantum algorithm $\mathcal{A}$ as follows. First, we toss two random coins that the outcomes denoted as r_1 and r_2. Subsequently, we apply the SWAP test on the corresponding states in the following manner:

- If the first coin lands on heads ($r_1 = 1$), we perform the SWAP test on ρ_0 and ρ_1. We accept if the final measurement outcome is 0.
- If the first coin lands on tails ($r_1 = 0$), we perform the SWAP test on two copies of ρ_{r_2}. We accept if the final measurement outcome is 1.

Let $p^{(o)}_{\mathrm{SWAP}}(\rho_0, \rho_1)$ be the probability of the SWAP test on ρ_0 and ρ_1 where the final measurement outcome o. We then obtain the acceptance probability of our algorithm $\mathcal{A}$:

$$\begin{aligned}\frac{1}{2}p^{(0)}_{\mathrm{SWAP}}(\rho_0, \rho_1) + \frac{1}{2}\sum_{i\in\{0,1\}}\frac{p^{(1)}_{\mathrm{SWAP}}(\rho_i, \rho_i)}{2} &= \frac{1 + \mathrm{Tr}(\rho_0\rho_1)}{4} + \sum_{i\in\{0,1\}}\frac{1 - \mathrm{Tr}(\rho_i^2)}{8} \\ &= \frac{1}{2} - \frac{\mathrm{HS}^2(\rho_0, \rho_1)}{4}.\end{aligned} \tag{7.16}$$

It suffices to show that algorithm $\mathcal{A}$ is indeed a PP containment distinguishing *yes* instances from *no* instances within an inverse-exponential gap. Combining Equation (7.15) and Equation (7.16), we then analyze the acceptance probability:

- For *yes* instances, noting that $\mathrm{T}(\rho_0, \rho_1) \leq 2^{-n/2-1}$, it holds that:

$$p_{\mathcal{A}}^{(\mathsf{Y})}(\rho_0, \rho_1) = \frac{1}{2} - \frac{1}{4}\mathrm{HS}(\rho_0, \rho_1)^2 \geq \frac{1}{2} - \frac{1}{4}\mathrm{T}^2(\rho_0, \rho_1) \geq \frac{1}{2} - 2^{-n-4}.$$

- For *no* instances, noticing that $\mathrm{T}(\rho_0, \rho_1) \geq 1 - 2^{-n/2-1}$, it holds that:

$$\begin{aligned} p_{\mathcal{A}}^{(\mathsf{N})}(\rho_0, \rho_1) &= \frac{1}{2} - \frac{1}{4}\mathrm{HS}(\rho_0, \rho_1)^2 \\ &\leq \frac{1}{2} - \frac{1}{4} \cdot \frac{\mathrm{T}(\rho_0, \rho_1)^2}{\dim \mathcal{H}} \\ &\leq \frac{1}{2} - 2^{-n-2} \cdot \left(1 - 2^{-\frac{n}{2}-1}\right)^2. \end{aligned}$$

Since $\mathsf{PreciseBQP} \subseteq \mathsf{PP}$ (e.g., Lemma 3.3 in [GSS+22]), we then complete the proof by showing that the gap $p_{\mathcal{A}}^{(\mathsf{Y})}(\rho_0, \rho_1) - p_{\mathcal{A}}^{(\mathsf{N})}(\rho_0, \rho_1)$ is exponentially small as desired:

$$p_{\mathcal{A}}^{(\mathsf{Y})}(\rho_0, \rho_1) - p_{\mathcal{A}}^{(\mathsf{N})}(\rho_0, \rho_1) = 2^{-2n-4} + 2^{-n-2} \cdot \left(\frac{3}{4} - 2^{-n/2}\right) \geq 2^{-2n-4},$$

where the last inequality holds for $n \geq 1$. □

Chapter 8

Conclusions

In this dissertation, we investigated quantum state testing problems from complexity-theoretic perspectives, with a primary focus on the closeness testing of quantum states. Specifically, our work addressed the following questions:

(i) What is the computational hardness of approximating the von Neumann entropy?

(ii) Does the dichotomy-like behavior, which is observed in the time-bounded state testing with respect to the trace distance (ℓ_1 norm) and the Hilbert-Schmidt distance (ℓ_2 norm), also arise in quantum state testing under other resource constraints?

(iii) How can the QSZK containment regime for the time-bounded state testing problem with respect to the trace distance (QSD) be improved?

We formulated these questions into more specific problems, as listed in Sections 1.1 and 1.2, and were able to provide very satisfying answers to most of them. We now briefly review our results and suggest future research directions.

A dichotomy theorem on approximating von Neumann entropy

In the context of (white-box) quantum state testing problems, briefly outlined in Section 3.3, the trace distance [Wat02] and the von Neumann entropy [BASTS10] emerge as the most important closeness measures considered in time-bounded state testing. While a dichotomy theorem on approximating the von Neumann entropy is established (Theorem 4.2), this brings up a parallel question concerning the trace distance:

Open Problem 8.1. *What computational power is required to approximate the trace distance in time-bounded state testing problems, particularly with respect to closeness measures that are looser than the ℓ_1-norm (trace distance) but tighter than the ℓ_2-norm (Hilbert-Schmidt distance)?*

Our first main theorem (Theorem 4.1) in Chapter 4 provides an efficiently computable lower bound for the von Neumann entropy $\mathrm{S}(\rho)$. This naturally raises the question:

Open Problem 8.2. *Is there an efficiently computable upper bound for $\mathrm{S}(\rho)$, perhaps based on some relaxed notion of the von Neumann entropy?*

The quantum Tsallis entropy $\mathrm{S}_q(\rho)$ in the regime $1 < q < 2$ exhibits distinct behavior compared to both $\mathrm{S}(\rho)$ and $\mathrm{S}_2(\rho) = 1 - \mathrm{Tr}(\rho^2)$, which was believed to be computationally challenging for quantum computers until our work, leading to another open problem:

Open Problem 8.3. *Are there further applications of estimating the quantum Tsallis entropy $\mathrm{S}_q(\rho)$ in the regime $1 < q < 2$?*

Furthermore, there are two open problems arise regarding quantitative bounds for the easy regime and (NI)QSZK containments for the hard regime:

Open Problem 8.4. *Can the query and sample bounds in Table 4.2 be improved, especially for the regime $q \geq 1 + \Omega(1)$?*

Open Problem 8.5. *Is it possible to establish that* TsallisQED$_q$ *(or* TsallisQEA$_q$*) is contained in* QSZK *(or* NIQSZK*) for the regime $1 < q \leq 1 + \frac{1}{n-1}$, which has been shown to be* QSZK*-hard (or* NIQSZK*-hard) as stated in Theorem 4.2(2)?*

For the hard regime (Open Problem 8.5), it is noteworthy that the QSZK containment of QED ($q = 1$) cannot be directly extended to TsallisQED$_q$ for the regime $1 < q \leq 1 + \frac{1}{n-1}$, since $\mathrm{S}_q(\rho)$ only provides a lower bound of $\mathrm{S}(\rho)$, while TsallisQED$_q$ in this regime appears to be easier than QED.[1]

Finally, it is worth exploring generalizations of the von Neumann entropy that are tighter than the quantum Tsallis entropy $\mathrm{S}_q(\rho)$ for $q > 1$. Two promising candidates are $\mathrm{S}_q(\rho)$ for $0 < q < 1$ and the quantum Rényi entropy, defined as $\mathrm{S}^R_\alpha(\rho) := \frac{\ln \mathrm{Tr}(\rho^\alpha)}{1-\alpha}$, which prompts the following questions:

Open Problem 8.6. *What are the containment and hardness of estimating the quantum Tsallis entropy $\mathrm{S}_q(\rho)$ in the regime $0 < q < 1$?*

Open Problem 8.7. *Since the corresponding time-bounded state testing problem with respect to the quantum Rényi entropy $\mathrm{S}^R_\alpha(\rho)$, denoted as* RényiQEA$_\alpha$ *is intuitively* QSZK*-hard for the regime $1 < \alpha \leq 1 + \frac{1}{n-1}$, as per Theorem 4.2(2), can computational hardness results be established for estimating $\mathrm{S}^R_\alpha(\rho)$ with $\alpha > 0$?*

Space-bounded quantum state testing via space-efficient quantum singular value transformation

Since space-efficient quantum singular value transformation (QSVT) offers a unified framework for designing quantum logspace algorithms, it suggests a new direction to find applications of space-bounded quantum computation.

[1] However, a *partial regime* QSZK containment of time-bounded state testing with respect to the quantum Jensen-Tsallis divergence (QJT$_q$) for $1 < q \leq 1 + \frac{1}{n-1}$ can be derived by applying the inequalities between the trace distance and QJT$_q$. This type of reduction, though, cannot be directly extended to $\mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1)$, and thus, a partial regime QSZK containment of TsallisQED$_q$ does not immediately follow. This is because $\mathrm{QJT}_q(\rho_0, \rho_1)$ does not exhibit a linear dependence on $\mathrm{S}_q(\rho_0) - \mathrm{S}_q(\rho_1)$ for the regime $1 < q \leq 1 + \frac{1}{n-1}$ in general (see, e.g., Equation (4.45)), unlike the case of $q = 1$.

Space-efficient QSVT. An intriguing candidate is solving positive semi-definite programming (SDP) programs with constant precision [JY11, AZLO16]. A major challenge in achieving a BQL containment of this problem is that iteratively applying the space-efficient QSVT super-constantly many times may lead to a bitstring indexed encoding requiring $\omega(\log n)$ ancillary qubits, raising the question:

Open Problem 8.8. *Is it possible to have an approximation scheme (possibly under certain conditions) that introduces merely $O(1)$ additional ancillary qubits in the bitstring indexed encoding per iteration, such that applying space-efficient QSVT $O(\log n)$ times results in a bitstring indexed encoding with at most $O(\log n)$ ancillary qubits?*

Recently, a query complexity lower bound $\Omega(d)$ for matrix functions [MS23] implies that time-efficient QSVT [GSLW19] is time-optimal. This raises the question of how to improve the efficiency of the space-efficient QSVT:

Open Problem 8.9. *Can the query complexity of U and $U^\dagger$ in space-efficient QSVT for smooth functions be improved from $O(d^2)$ to $O(d)$?*

Such an improvement would make QSVT optimal for both (quantum) time and space: Notably, the pre-processing – finding an appropriate polynomial approximation – in QSVT techniques, which is not necessarily classical in general, usually involves finding the sequence of z-axis rotation angles. Our approach, however, uses averaged Chebyshev truncation and the LCU technique. A general solution thus seems to involve developing a space-efficient (quantum) angle-finding algorithm.

Space-bounded testings beyond quantum states. Furthermore, as quantum distances investigated in this work are all instances of a quantum analog of symmetric f-divergence, there is a natural question on other closeness measures of quantum states or even testing the closeness of quantum channels:

Open Problem 8.10. *Is it possible to establish that space-bounded quantum state testing problems with respect to other quantum distance-like measures are* BQL*-complete?*

Open Problem 8.11 (Inspired by Tom Gur)**.** *What is the computational complexity of time- or space-bounded quantum* channel *testing problems with respect to various closeness measures?*

The QSZK containment of QSD beyond the polarizing regime

We developed a quantum counterpart to the classical work [BDRV19], improving the QSZK containment of the time-bounded state testing problem with respect to the trace distance (QSD). However, not all results in [BDRV19] extend to the quantum setting. This difference stems from the *distinct* behaviors exhibited by quantum analogs of the triangular discrimination compared to their classical equivalent.

QSZK and QSD. Nevertheless, fully characterizing the computational hardness of the promise problem QSD or the complexity class QSZK remains a significant challenge. The best known upper bound for $\mathrm{QSD}[\alpha, \beta]$ when $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$, denoted as GapQSD, is PSPACE. This result is implicitly shown in [Wat02], see also Theorem 6.2(1)

for an alternative proof. However, the best known upper bound for QSZK is QIP(2) with a quantum linear-space honest prover (Theorem 6.27), while the prior best upper bound was QIP(2) [Wat02, Wat09b, JUW09], which is contained in PSPACE. This leads to an intriguing question:

Open Problem 8.12. *Can the upper bound for* GapQSD *be improved?*

A more ambitious question concerns achieving a tighter characterization of the class QSZK. The best known upper bound for its classical counterpart, SZK, is AM ∩ coAM, as established in [For87, AH91].

Open Problem 8.13. *Can the classical or quantum upper bound for* QSZK *be improved?*

The set lower bound protocol [GS86] plays a crucial role in proving that SZK is in AM∩coAM. A natural approach to improving the quantum upper bound, such as variants of QIP(2) introduced in [KLN19], would involve developing a quantum analog of the set lower bound protocol. A more challenging question is how to improve the classical upper bound beyond PSPACE, given the lack of techniques for establishing containments in terms of complexity classes between PP and PSPACE, such as the counting hierarchy.

Quantum analogs of the triangular discrimination. In addition to general questions on QSZK and GapQSD, as we defined two quantum analogs of the triangular discrimination, a natural question is finding more applications of them:

Open Problem 8.14. *Is there any other application of the (measured) quantum triangular discrimination besides its usage related to the class* QSZK*?*

For instance, Yehudayoff [Yeh20] utilized triangular discrimination to obtain a sharper communication complexity lower bound of the point chasing problem. Can we expect a similar implication in the quantum world? Moreover, we note that $\mathrm{QTD}^{\mathrm{meas}}$ is a symmetric version of the measured Bures χ^2-divergence and the latter is used for the nonzero testing of quantum mutual information [FO23]. Might $\mathrm{QTD}^{\mathrm{meas}}$ also play a role in quantum property testing?

Lastly, two questions arise regarding the tightening of the characterization of quantum triangular discrimination introduced in Chapter 7. First, numerical simulations suggest that the inequalities in Theorem 7.4(2) are not tight, leading to the natural question:

Open Problem 8.15. *Is it possible to prove that for any quantum states ρ_0 and ρ_1, the following inequalities hold*:

$$\ln(2) \cdot \mathrm{QTD}^2(\rho_0, \rho_1) \leq \mathrm{QJS}(\rho_0, \rho_1) \leq \ln(2) \cdot \mathrm{QTD}(\rho_0, \rho_1)?$$

The bounds in Open Problem 8.15 can be saturated by choosing states ρ_0 and ρ_1 with orthogonal support, which suffices to make $\mathrm{QJS}_{\mathrm{bit}}(\rho_0, \rho_1)$ and $\mathrm{QTD}(\rho_0, \rho_1)$ equal to 1.

Second, since the square root of triangular discrimination is a metric [LC86], it raises an interesting question whether a similar property holds in the quantum case:

Open Problem 8.16. *Is it possible to prove that the square root of quantum triangular discrimination, denoted as $\sqrt{\mathrm{QTD}}$, is a distance metric? Specifically, for any quantum states ρ_0, ρ_1, and ρ_2, can it be shown that the following inequality holds*:

$$\sqrt{\mathrm{QTD}(\rho_0, \rho_1)} + \sqrt{\mathrm{QTD}(\rho_1, \rho_2)} \geq \sqrt{\mathrm{QTD}(\rho_0, \rho_2)}?$$

Bibliography

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 1st edition, 2009. 14

[ABIS19] Jayadev Acharya, Sourbh Bhadane, Piotr Indyk, and Ziteng Sun. Estimating entropy of distributions in constant space. *Advances in Neural Information Processing Systems*, 32, 2019. arXiv:1911.07976. 41

[ADH97] Leonard M Adleman, Jonathan Demarrais, and Ming-Deh A Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997. 12, 154

[AGL20] Dorit Aharonov, Alex B Grilo, and Yupan Liu. StoqMA vs. MA: the power of error reduction. *arXiv preprint arXiv:2010.02835*, 2020. arXiv:2010.02835. 154

[AH91] 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*. 3, 180

[AISW20] Jayadev Acharya, Ibrahim Issa, Nirmal V Shende, and Aaron B Wagner. Estimating quantum entropy. *IEEE Journal on Selected Areas in Information Theory*, 1(2):454–468, 2020. arXiv:1711.00814. 8, 43, 44, 45, 113

[AJL09] 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. 10, 24, 46, 114, 119

[AKN98] Dorit Aharonov, Alexei Kitaev, and Noam Nisan. Quantum circuits with mixed states. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998. arXiv:quant-ph/9806029. 16

[Amb14] Andris Ambainis. On physical problems that are slightly more difficult than QMA. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, pages 32–43. IEEE, 2014. arXiv:1312.4758. 75

[AMNW22] Maryam Aliakbarpour, Andrew McGregor, Jelani Nelson, and Erik Waingarten. Estimation of entropy in constant space with improved sample complexity. *Advances in Neural Information Processing Systems*, 35:32474–32486, 2022. arXiv:2205.09804. 41

[AOST17] Jayadev Acharya, Alon Orlitsky, Ananda Theertha Suresh, and Himanshu Tyagi. Estimating Renyi entropy of discrete distributions. *IEEE Transactions on Information Theory*, 63(1):38–56, 2017. arXiv:1408.1000. 44, 45

[vAGGdW20] Joran van Apeldoorn, András Gilyén, Sander Gribling, and Ronald de Wolf. Quantum SDP-solvers: Better upper and lower bounds. *Quantum*, 4:230, 2020. Preliminary version in *FOCS 2017*. arXiv:1705.01843. 84, 85, 90, 91, 94

[AS16] Noga Alon and Joel H Spencer. *The Probabilistic Method*. John Wiley & Sons, 2016. 92

[AS17] Guillaume Aubrun and Stanisław J Szarek. *Alice and Bob Meet Banach: The Interface of Asymptotic Geometric Analysis and Quantum Information Theory*, volume 223 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2017. 4, 14, 16, 32, 58, 60

[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 27th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1824–1831. SIAM, 2016. arXiv:1507.02259. 179

[BASTS10] 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*. i, 4, 12, 37, 39, 42, 44, 49, 66, 70, 113, 153, 155, 163, 177

[Bau11] Bernhard Baumgartner. An inequality for the trace of matrix products, using absolute values. *arXiv preprint arXiv:1106.6189*, 2011. arXiv:1106.6189. 53

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997. arXiv:quant-ph/9701001. 46

[BBHT98] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik: Progress of Physics*, 46(4–5):493–505, 1998. arXiv:quant-ph/9605034. 7, 24, 115, 127

[BCC+15] 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. 82, 101

[BCH+19] Adam Bouland, Lijie Chen, Dhiraj Holden, Justin Thaler, and Prashant Nalini Vasudevan. On the power of statistical zero knowledge. *SIAM Journal on Computing*, 49(4):FOCS17–1, 2019. Preliminary version in *FOCS 2017*. arXiv:1609.02888. 5, 44, 153, 154, 173, 175

[BCWdW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001. arXiv:quant-ph/0102001. i, 4, 5, 8, 10, 23, 42, 45, 113, 115, 154, 173, 175

[BDRV19] 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. ii, 3, 4, 11, 33, 38, 151, 152, 154, 155, 156, 163, 164, 167, 168, 169, 171, 172, 179

[Bec02] Christian Beck. Generalized statistical mechanics and fully developed turbulence. *Physica A: Statistical Mechanics and its Applications*, 306:189–198, 2002. arXiv:cond-mat/0110073. 8

[Bel19] Aleksandrs Belovs. Quantum algorithms for classical probability distributions. In *Proceedings of the 27th Annual European Symposium on Algorithms, ESA 2019*, volume 144 of *LIPIcs*, pages 16:1–16:11. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. arXiv:1904.02192. 40, 67

[Ber14] Serge Bernstein. Sur la meilleure approximation de $|x|$ par des polynomes de degrés donnés. *Acta Mathematica*, 37(1):1–57, 1914. 9, 19, 47

[Ber38] Serge Bernstein. Sur la meilleure approximation de $|x|^p$ par des polynômes de degrés très élevés. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 2(2):169–190, 1938. 9, 19, 47

[BGJ19] Rajendra Bhatia, Stephane Gaubert, and Tanvi Jain. Matrix versions of the Hellinger distance. *Letters in Mathematical Physics*, 109(8):1777–1804, 2019. arXiv:1901.01378. 31

[BH09] Jop Briët and Peter Harremoës. Properties of classical and quantum Jensen-Shannon divergence. *Physical Review A*, 79(5):052311, 2009. arXiv:0806.4472. 9, 29, 34, 35, 48, 49, 55, 58, 59, 155

[Bha96] Rajendra Bhatia. *Matrix Analysis*, volume 169. Springer Science & Business Media, 1996. 18, 139, 158

[BHMT02] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Quantum Computation and Information*, 305:53–74, 2002. arXiv:quant-ph/0005055. 23, 24, 45, 115, 127

[BKT20] 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. 45

[BL13] Andrej Bogdanov and Chin Ho Lee. Limits of provable security for homomorphic encryption. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference*, volume 8042 of *Lecture Notes in Computer Science*, pages 111–128. Springer, 2013. ECCC:TR12-156. 3

[BLT92] José L Balcázar, Antoni Lozano, and Jacobo Torán. The complexity of algorithmic problems on succinct instances. In *Computer Science: Research and Applications*, pages 351–377. Springer, 1992. 117

[BOW19] Costin Bădescu, Ryan O'Donnell, and John Wright. Quantum state certification. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 503–514, 2019. arXiv:1708.06002. 9, 111, 113, 117, 156

[BR82] J. Burbea and C. Rao. On the convexity of some divergence measures based on entropy functions. *IEEE Transactions on Information Theory*, 28(3):489–495, 1982. 29

[BZ10] Richard P Brent and Paul Zimmermann. *Modern Computer Arithmetic*, volume 18. Cambridge University Press, 2010. 88

[Can20] Clément L Canonne. A survey on distribution testing: Your data is big. but is it blue? *Theory of Computing*, pages 1–100, 2020. ECCC:TR15-063. i, 2

[CCC19] Patrick J Coles, M Cerezo, and Lukasz Cincio. Strong bound between trace distance and Hilbert-Schmidt distance for low-rank states. *Physical Review A*, 100(2):022103, 2019. arXiv:1903.11738. 4, 32

[CCKV08] 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. 39, 44, 49, 56, 169, 170

[CDG+20] Rui Chao, Dawei Ding, Andras Gilyen, Cupjin Huang, and Mario Szegedy. Finding angles for quantum signal processing with machine precision. *arXiv preprint arXiv:2003.02831*, 2020. arXiv:2003.02831. 82

[CDSTS23] Gil Cohen, Dean Doron, Ori Sberlo, and Amnon Ta-Shma. Approximating iterated multiplication of stochastic matrices in small space. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 35–45, 2023. ECCC:TR22-149. 84

[CDVV14] Siu-On Chan, Ilias Diakonikolas, Paul Valiant, and Gregory Valiant. Optimal algorithms for testing closeness of discrete distributions. In *Proceedings of the 25th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1193–1203. SIAM, 2014. arXiv:1308.3946. 113

[CFMdW10] 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. 40, 67

[CGKZ05] Howard Cheng, Barry Gergel, Ethan Kim, and Eugene Zima. Space-efficient evaluation of hypergeometric series. *ACM SIGSAM Bulletin*, 39(2):41–52, 2005. 88

[Cio21] Krzysztof J Ciosmak. Matrix Hölder's inequality and divergence formulation of optimal transport of vector measures. *SIAM Journal on Mathematical Analysis*, 53(6):6932–6958, 2021. arXiv:2109.06588. 159

[CLM10] Steve Chien, Katrina Ligett, and Andrew McGregor. Space-efficient estimation of robust statistics and distribution testing. In *Proceedings of the First Innovations in Computer Science Conference*, pages 251–265, 2010. 41

[CS20] Sam Cree and Jamie Sikora. A fidelity measure for quantum states based on the matrix geometric mean. *arXiv preprint arXiv:2006.06918*, 2020. arXiv:2006.06918. 31

[CT14] Richard Y. Chen and Joel A. Tropp. Subadditivity of matrix ϕ-entropy and concentration of random matrices. *Electronic Journal of Probability*, 19(27):1–30, 2014. arXiv:1308.2952. 50, 56, 57

[Dar70] Zoltán Daróczy. Generalized information functions. *Information and Control*, 16(1):36–51, 1970. 8, 28

[DGKR19] Ilias Diakonikolas, Themis Gouleakis, Daniel M Kane, and Sankeerth Rao. Communication and memory efficient testing of discrete distributions. In *Proceedings of the Thirty-Second Conference on Learning Theory*, pages 1070–1106. PMLR, 2019. arXiv:1906.04709. 41

[DLLM23] Hugo Delavenne, François Le Gall, Yupan Liu, and Masayuki Miyamoto. Quantum Merlin-Arthur proof systems for synthesizing quantum states. *To appear in Quantum*, 2023. arXiv:2303.01877. iii

[DMWL21] Yulong Dong, Xiang Meng, K Birgitta Whaley, and Lin Lin. Efficient phase-factor evaluation in quantum signal processing. *Physical Review A*, 103(4):042419, 2021. arXiv:2002.11649. 82

[EAO+02] Artur K. Ekert, Carolina Moura Alves, Daniel K. L. Oi, Michał Horodecki, Paweł Horodecki, and Leong Chuan Kwek. Direct estimations of linear and nonlinear functionals of a quantum state. *Physical Review Letters*, 88(21):217901, 2002. arXiv:quant-ph/0203016. 5, 8, 42, 45

[FC94] Christopher A Fuchs and Carlton M Caves. Ensemble-dependent bounds for accessible information in quantum mechanics. *Physical Review Letters*, 73(23):3047, 1994. 31, 33, 160, 161

[FGHP99] Stephen Fenner, Frederic Green, Steven Homer, and Randall Pruim. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 455(1991):3953–3966, 1999. arXiv:quant-ph/9812056. 154

[FvdG99] 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. 28, 31, 33, 49, 58, 79, 155, 171

[FKL+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, page 14, 2016. arXiv:1604.08192. 6, 16, 107, 116, 149

[FKSV02] Joan Feigenbaum, Sampath Kannan, Martin J Strauss, and Mahesh Viswanathan. An approximate l_1-difference algorithm for massive data streams. *SIAM Journal on Computing*, 32(1):131–151, 2002. Preliminary version in *FOCS 1999*. 41

[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, page 4, 2018. arXiv:1604.01384. 6, 16, 22, 110, 113, 114, 117

[FO23] Steven T Flammia and Ryan O'Donnell. Quantum chi-squared tomography and mutual information testing. *arXiv preprint arXiv:2305.18519*, 2023. arXiv:2305.18519. 180

[For87] Lance Fortnow. The complexity of perfect zero-knowledge. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 204–209, 1987. 3, 180

[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. 6, 7, 16, 17, 22, 84, 110, 113, 116, 133, 149

[Fur05] Shigeru Furuichi. On uniqueness theorems for Tsallis entropy and Tsallis relative entropy. *IEEE Transactions on Information Theory*, 51(10):3638–3645, 2005. arXiv:cond-mat/0410270. 35

[FYK04] Shigeru Furuichi, Kenjiro Yanagi, and Ken Kuriyama. Fundamental properties of Tsallis relative entropy. *Journal of Mathematical Physics*, 45(12):4868–4877, 2004. arXiv:cond-mat/0406178. 35, 57

[FYK07] Shigeru Furuichi, Kenjiro Yanagi, and Ken Kuriyama. A generalized Fannes' inequality. *Journal of Inequalities in Pure and Applied Mathematics*, 8(1):5, 2007. arXiv:1001.1390. 35, 36

[Gan02] Michael I. Ganzburg. The Bernstein constant and polynomial interpolation at the Chebyshev nodes. *Journal of Approximation Theory*, 119(2):193–213, 2002. 48

[Gil19] András Gilyén. *Quantum Singular Value Transformation & Its Algorithmic Applications*. PhD thesis, University of Amsterdam, 2019. 102

[GL20] András Gilyén and Tongyang Li. Distributional property testing in a quantum world. In *Proceedings of the 11th Innovations in Theoretical Computer Science Conference*, volume 151, pages 25:1–25:19, 2020. arXiv:1902.00814. 40, 45, 96, 97

[GMV06] Sudipto Guha, Andrew McGregor, and Suresh Venkatasubramanian. Streaming and sublinear approximation of entropy and information distances. In *Proceedings of the 17th Annual ACM-SIAM Symposium on Discrete Algorithm*, pages 733–742, 2006. arXiv:cs/0508122. 41

[Gol08] Oded Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, 2008. 15

[Gol13] Oded Goldreich. A short tutorial of zero-knowledge. In *Secure Multi-Party Computation*, volume 10 of *Cryptology and Information Security Series*, pages 28–60. IOS Press, 2013. 3

[Gol17] Oded Goldreich. *Introduction to property testing*. Cambridge University Press, 2017. 2

[Gol19] Oded Goldreich. Errata (3-Feb-2019). http://www.wisdom.weizmann.ac.il/~/oded/entropy.html, 2019. 3, 153

[GP22] András Gilyén and Alexander Poremba. Improved quantum algorithms for fidelity estimation. *arXiv preprint arXiv:2203.15993*, 2022. arXiv:2203.15993. 24, 25, 46, 114

[GR02] Lov Grover and Terry Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions. *arXiv preprint quant-ph/0208112*, 2002. arXiv:quant-ph/0208112. 101

[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, pages 76:1–76:18, 2022. arXiv:2106.11877. 6

[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, pages 73:1–73:20, 2021. arXiv:2006.04880. 6, 81

[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. 180

[GSLW18] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. *arXiv preprint arXiv:1806.01838*, 2018. 99, 101, 103, 108, 109

[GSLW19] 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. ii, 9, 10, 18, 19, 24, 25, 46, 47, 81, 82, 84, 86, 90, 94, 95, 99, 100, 101, 102, 103, 107, 108, 109, 179

[GSS+22] 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. 176

[GSV98] 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. 3, 113

[GSV99] Oded Goldreich, Amit Sahai, and Salil P. Vadhan. Can statistical zero knowledge be made non-interactive? or on the relationship of SZK and NISZK. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference*, volume 1666 of *Lecture Notes in Computer Science*, pages 467–484. Springer, 1999. 11, 152

[GV99] Oded Goldreich and Salil Vadhan. Comparing entropies in statistical zero knowledge with applications to the structure of SZK. In *Proceedings of the Fourteenth Annual IEEE Conference on Computational Complexity*, pages 54–73. IEEE, 1999. ECCC:TR98-063. 4, 113, 152

[GV11] Oded Goldreich and Salil P Vadhan. On the complexity of computational problems regarding distributions. *Studies in Complexity and Cryptography*, 6650:390–405, 2011. ECCC:TR11-004. 2, 10, 152

[Haa19] Jeongwan Haah. Product decomposition of periodic functions in quantum signal processing. *Quantum*, 3:190, 2019. arXiv:1806.10236. 82

[Hal87] Paul R. Halmos. *Finite-Dimensional Vector Spaces*. Undergraduate Texts in Mathematics. Springer-Verlag New York, NY, 1987. 18

[Hay24] Masahito Hayashi. Measuring quantum relative entropy with finite-size effect. *arXiv preprint arXiv:2406.17299*, 2024. arXiv:2406.17299. 44

[HC67] Jan Havrda and František Charvát. Quantification method of classification processes. concept of structural a-entropy. *Kybernetika*, 3(1):30–35, 1967. 8

[Hel69] Carl W Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1:231–252, 1969. 10, 30, 111

[HHL09] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical Review Letters*, 103(15):150502, 2009. arXiv:0811.3171. 6

[Hia21] Fumio Hiai. *Quantum f-divergences in von Neumann Algebras*. Springer, 2021. 30

[HJ12] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge University Press, 2012. 18, 159

[Hol73a] Alexander S Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973. 5, 32, 33, 49

[Hol73b] Alexander S Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, 3(4):337–394, 1973. 10, 30, 111

[JMDA21] Reza Asgharzadeh Jelodar, Hossein Mehri-Dehnavi, and Hamzeh Agahi. Some properties of Tsallis and Tsallis–Lin quantum relative entropies. *Physica A: Statistical Mechanics and its Applications*, 567:125719, 2021. 35

[JUW09] 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. ii, 3, 4, 10, 44, 112, 140, 141, 180

[JVHW15] Jiantao Jiao, Kartik Venkat, Yanjun Han, and Tsachy Weissman. Minimax estimation of functionals of discrete distributions. *IEEE Transactions on Information Theory*, 61(5):2835–2885, 2015. arXiv:1406.6956. 113

[JY11] Rahul Jain and Penghui Yao. A parallel approximation algorithm for positive semidefinite programming. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*, pages 463–471. IEEE, 2011. arXiv:1104.2502. 179

[Kai67] Thomas Kailath. The divergence and Bhattacharyya distance measures in signal selection. *IEEE transactions on communication technology*, 15(1):52–60, 1967. 27, 155

[Kim16] Jeong San Kim. Tsallis entropy and general polygamy of multiparty quantum entanglement in arbitrary dimensions. *Physical Review A*, 94(6):062338, 2016. arXiv:1612.04480. 36

[Kit95] Alexei Yu Kitaev. Quantum measurements and the Abelian stabilizer problem. *arXiv preprint quant-ph/9511026*, 1995. arXiv:quant-ph/9511026. 10, 24, 46, 114, 119

[Kit97] Alexei Yu Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191, 1997. 6

[KLL+17] Shelby Kimmel, Cedric Yen-Yu Lin, Guang Hao Low, Maris Ozols, and Theodore J. Yoder. Hamiltonian simulation with optimal sample complexity. *npj Quantum Information*, 3(1):1–7, 2017. arXiv:1608.00281. 25

[KLN19] 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. 44, 49, 50, 56, 64, 180

[KM01] Phillip Kaye and Michele Mosca. Quantum networks for generating arbitrary quantum states. In *Optical Fiber Communication Conference and International Conference on Quantum Information*. Optica Publishing Group, 2001. arXiv:quant-ph/0407102. 101

[KMY09] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? *Chicago Journal of Theoretical Computer Science*, 2009:3, 2009. Preliminary version in *ISAAC 2003*. arXiv:quant-ph/0306051. 23, 154, 174, 175

[Kob03] 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. arXiv:quant-ph/0207158. 5, 37, 39, 42, 46, 49

[KS16] Yasuhito Kawano and Hiroshi Sekigawa. Quantum Fourier transform over symmetric groups — improved result. *Journal of Symbolic Computation*, 75:219–243, 2016. 44

[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. 142

[LC86] Lucien Le Cam. *Asymptotic methods in statistical decision theory*. Springer Science & Business Media, 1986. 27, 155, 180

[LC17] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by uniform spectral amplification. *arXiv preprint arXiv:1707.05391*, 2017. arXiv:1707.05391. 88

[LC19] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by qubitization. *Quantum*, 3:163, 2019. arXiv:1610.06546. 24

[Lie73] Elliott H. Lieb. Convex trace functions and the Wigner-Yanase-Dyson conjecture. *Advances in Mathematics*, 11(3):267–288, 1973. 50, 56

[Lin75] Göran Lindblad. Completely positive maps and entropy inequalities. *Communications in Mathematical Physics*, 40:147–151, 1975. 57

[Lin91] Jianhua Lin. Divergence measures based on the Shannon entropy. *IEEE Transactions on Information Theory*, 37(1):145–151, 1991. 49, 56, 61

[Liu21] Yupan Liu. StoqMA meets distribution testing. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021. arXiv:2011.05733. 151

[Liu23] Yupan Liu. Quantum state testing beyond the polarizing regime and quantum triangular discrimination. *arXiv preprint arXiv:2303.01952*, 2023. arXiv:2303.01952. iii, 12, 49, 80

[LLNW24] François Le Gall, Yupan Liu, Harumichi Nishimura, and Qisheng Wang. Space-bounded quantum interactive proof systems. *arXiv preprint arXiv:2410.23958*, 2024. arXiv:2410.23958. iii, 12, 112, 116, 141, 142, 144, 146, 147

[LLW23] 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. iii, 12, 38, 44, 46

[LMR14] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum principal component analysis. *Nature Physics*, 10(9):631–633, 2014. arXiv:1307.0401. 25

[LW25] Yupan Liu and Qisheng Wang. On estimating the trace of quantum state powers. In *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 947–993. SIAM, 2025. arXiv:2410.13559. iii, 12

[LWL24] Jingquan Luo, Qisheng Wang, and Lvzhou Li. Succinct quantum testers for closeness and k-wise uniformity of probability distributions. *IEEE Transactions on Information Theory*, 70(7):5092–5103, 2024. arXiv:2304.12916. 40

[vMW12] Dieter van Melkebeek and Thomas Watson. Time-space efficient simulations of quantum computations. *Theory of Computing*, 8(1):1–51, 2012. Preliminary version in arXiv:0712.2545. 6, 15, 16, 17, 110, 127

[Mez12] Marc Mezzarobba. A note on the space complexity of fast D-finite function evaluation. In *Computer Algebra in Scientific Computing: 14th International Workshop, CASC 2012, Maribor, Slovenia, September 3-6, 2012. Proceedings 14*, pages 212–223. Springer, 2012. arXiv:1209.5097. 88

[MLP05] Ana P Majtey, Pedro W Lamberti, and Domingo P Prato. Jensen-Shannon divergence as a measure of distinguishability between mixed quantum states. *Physical Review A*, 72(5):052310, 2005. arXiv:quant-ph/0508138. 5, 9, 32, 35, 50, 152

[MP16] Ashley Montanaro and Sam Pallister. Quantum algorithms and the finite element method. *Physical Review A*, 93(3):032324, 2016. arXiv:1512.05903. 101, 102

[MRTC21] John M Martyn, Zane M Rossi, Andrew K Tan, and Isaac L Chuang. Grand unification of quantum algorithms. *PRX Quantum*, 2(4):040203, 2021. arXiv:2105.02859. 81

[MS23] Ashley Montanaro and Changpeng Shao. Quantum and classical query complexities of functions of matrices. *arXiv preprint arXiv:2311.06999*, 2023. arXiv:2311.06999. 179

[MU17] Michael Mitzenmacher and Eli Upfal. *Probability and computing: Randomization and probabilistic techniques in algorithms and data analysis*. Cambridge University Press, 2017. 22, 55

[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. 6

[MdW16] Ashley Montanaro and Ronald de Wolf. A survey of quantum property testing. *Theory of Computing*, pages 1–81, 2016. arXiv:1310.2035. i, 2, 42, 44

[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. 82, 83, 89, 100, 102, 112

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2010. 5, 14, 30, 31, 32, 33, 59

[Ngu23] Quynh T Nguyen. The mixed Schur transform: efficient quantum circuit and applications. *arXiv preprint arXiv:2310.01613*, 2023. arXiv:2310.01613. 44

[OW21] Ryan O'Donnell and John Wright. Quantum spectrum testing. *Communications in Mathematical Physics*, 387(1):1–75, 2021. Preliminary version in *STOC 2015*. arXiv:1501.05028. 40, 67, 113

[Pet07] Dénes Petz. *Quantum information theory and quantum statistics*. Springer Science & Business Media, 2007. 34, 56, 57

[PP23] Aaron Putterman and Edward Pyne. Near-optimal derandomization of medium-width branching programs. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 23–34, 2023. ECCC:TR22-150. 84

[PY86] Christos H Papadimitriou and Mihalis Yannakakis. A note on succinct representations of graphs. *Information and Control*, 71(3):181–185, 1986. 117

[QKW24] Yihui Quek, Eneet Kaur, and Mark M. Wilde. Multivariate trace estimation in constant quantum depth. *Quantum*, 8:1220, 2024. arXiv:2206.15405. 45

[Rag95] Guido A. Raggio. Properties of q-entropies. *Journal of Mathematical Physics*, 36(9):4785–4791, 1995. 8, 35

[Ras11] Alexey E. Rastegin. Some general properties of unified entropies. *Journal of Statistical Physics*, 143:1120–1135, 2011. arXiv:1012.5356. 36

[RASW23] Soorya Rethinasamy, Rochisha Agarwal, Kunal Sharma, and Mark M Wilde. Estimating distinguishability measures on quantum computers. *Physical Review A*, 108(1):012409, 2023. arXiv:2108.08406. 5, 38, 49, 113, 134

[Rei08] Omer Reingold. Undirected connectivity in log-space. *Journal of the ACM (JACM)*, 55(4):1–24, 2008. Preliminary version in *STOC 2005*. ECCC:TR04-094. 7

[Riv90] Theodore J Rivlin. *Chebyshev polynomials: from approximation theory to algebra and number theory*. Courier Dover Publications, 1990. 20, 21, 48

[Roc70] Ralph Tyrell Rockafellar. *Convex Analysis*. Princeton University Press, 1970. 64

[RS90] Mary B Ruskai and Frank H Stillinger. Convexity inequalities for estimating free energy and relative entropy. *Journal of Physics A: Mathematical and General*, 23(12):2421, 1990. 162

[Rus22] Mary Beth Ruskai. Yet another proof of the joint convexity of relative entropy. *Letters in Mathematical Physics*, 112(4):81, 2022. arXiv:2112.13763. 56, 57

[Sak96] Michael Saks. Randomization and derandomization in space-bounded computation. In *Proceedings of Computational Complexity (Formerly Structure in Complexity Theory)*, pages 128–149. IEEE, 1996. 23

[SM03] Endre Süli and David F Mayers. *An Introduction to Numerical Analysis*. Cambridge University Press, 2003. 87, 91

[Sra21] Suvrit Sra. Metrics induced by jensen-shannon and related divergences on positive definite matrices. *Linear Algebra and its Applications*, 616:125–138, 2021. arXiv:1911.02643. 33, 35

[SS03] Elias M Stein and Rami Shakarchi. *Fourier Analysis: An Introduction*, volume 1. Princeton University Press, 2003. 22

[SV03] Amit Sahai and Salil Vadhan. A complete problem for statistical zero knowledge. *Journal of the ACM (JACM)*, 50(2):196–249, 2003. Preliminary version in *FOCS 1997*. ECCC:TR00-084. ii, 2, 3, 11, 12, 36, 37, 113, 151, 152, 153, 154

[SZ99] Michael Saks and Shiyu Zhou. $\mathrm{BP_HSPACE}(s) \subseteq \mathrm{DSPACE}(s^{3/2})$. *Journal of Computer and System Sciences*, 58(2):376–403, 1999. Preliminary version in *FOCS 1995*. 84

[Tim63] Aleksandr F. Timan. *Theory of Approximation of Functions of a Real Variable*, volume 34 of *International Series of Monographs on Pure and Applied Mathematics*. Pergamon Press, 1963. 19, 47, 48

[TKR+10] Kristan Temme, Michael James Kastoryano, Mary Beth Ruskai, Michael Marc Wolf, and Frank Verstraete. The χ^2-divergence and mixing times of quantum markov processes. *Journal of Mathematical Physics*, 51(12):122201, 2010. arXiv:1005.2358. 155, 156, 158, 162

[Top00] Flemming Topsøe. Some inequalities for information divergence and related measures of discrimination. *IEEE Transactions on information theory*, 46(4):1602–1609, 2000. 27, 28, 29, 155, 160, 162, 171, 172

[Top01] Flemming Topsøe. Bounds for entropy and divergence for distributions over a two-element set. *Journal of Inequalities in Pure and Applied Mathematics*, 2(2), 2001. 49, 56, 60, 61

[TS13] 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. 6, 7, 110, 113, 114

[Tsa88] Constantino Tsallis. Possible generalization of Boltzmann-Gibbs statistics. *Journal of Statistical Physics*, 52:479–487, 1988. 8, 28

[Tsa01] Constantino Tsallis. *Nonextensive Statistical Mechanics and Its Applications*, chapter I. Nonextensive Statistical Mechanics and Thermodynamics: Historical Background and Present Status, page 3–98. Springer, 2001. 8, 14

[TV15] Kristan Temme and Frank Verstraete. Quantum chi-squared and goodness of fit testing. *Journal of Mathematical Physics*, 56(1):012202, 2015. arXiv:1112.6343. 156

[Uhl77] A. Uhlmann. Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory. *Communications in Mathematical Physics*, 54:21–32, 1977. 50, 56, 57

[Vad99] Salil P Vadhan. *A study of statistical zero-knowledge proofs*. PhD thesis, Massachusetts Institute of Technology, 1999. 3, 11, 34, 59, 112, 152

[Vaj70] Igor Vajda. Note on discrimination information and variation. *IEEE Transactions on Information Theory*, 16(6):771–773, 1970. 49, 50

[Vir19] Dániel Virosztek. Jointly convex quantum Jensen divergences. *Linear Algebra and its Applications*, 576:67–78, 2019. arXiv:1712.05324. 50, 56, 57

[Vir21] Dániel Virosztek. The metric property of the quantum jensen-shannon divergence. *Advances in Mathematics*, 380:107595, 2021. arXiv:1910.10447. 33

[VW16] Thomas Vidick and John Watrous. Quantum proofs. *Foundations and Trends® in Theoretical Computer Science*, 11(1-2):1–215, 2016. arXiv:1610.01664. 3, 112, 144, 152

[Wan24] Qisheng Wang. Optimal trace distance and fidelity estimations for pure quantum states. *IEEE Transactions on Information Theory*, 2024. arXiv:2408.16655. 40

[Wat99] John Watrous. Space-bounded quantum complexity. *Journal of Computer and System Sciences*, 59(2):281–326, 1999. Preliminary version in *CCC 1998*. 6, 15, 110, 134, 149

[Wat01] John Watrous. Quantum simulations of classical random walks and undirected graph connectivity. *Journal of Computer and System Sciences*, 62(2):376–391, 2001. Preliminary version in *CCC 1999*. arXiv:cs/9812012. 7, 17, 107, 110

[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. IEEE, 2002. arXiv:quant-ph/0202111. i, ii, 3, 10, 11, 12, 36, 37, 38, 39, 42, 49, 79, 80, 111, 112, 113, 116, 137, 139, 141, 142, 144, 145, 146, 147, 152, 153, 154, 155, 163, 167, 168, 177, 179, 180

[Wat03] 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. 6, 15, 110

[Wat09a] John Watrous. Quantum computational complexity. *Encyclopedia of Complexity and Systems Science*, pages 7174–7201, 2009. arXiv:0804.3401. 14

[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. i, 3, 38, 42, 49, 112, 113, 180

[WGL+24] 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*, 2024. arXiv:2203.13522. 8, 43, 44, 45

[Wil13] Mark M Wilde. *Quantum Information Theory*. Cambridge University Press, 1st edition, 2013. 30, 57

[dW19] Ronald de Wolf. Quantum computing: Lecture notes. *arXiv preprint arXiv:1907.09415*, 2019. arXiv:1907.09415. 14

[WY16] Yihong Wu and Pengkun Yang. Minimax rates of entropy estimation on large alphabets via best polynomial approximation. *IEEE Transactions on Information Theory*, 62(6):3702–3720, 2016. arXiv:1407.0381. 113

[WZ23] Qisheng Wang and Zhicheng Zhang. Quantum lower bounds by sample-to-query lifting. *arXiv preprint arXiv:2308.01794*, 2023. arXiv:2308.01794. 25

[WZ24a] 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. 4, 38, 46, 114, 121

[WZ24b] Qisheng Wang and Zhicheng Zhang. Time-efficient quantum entropy estimator via samplizer. In *Proceedings of the 32nd Annual European Symposium on Algorithms*, pages 101:1–101:15, 2024. arXiv:2401.09947. 8, 25, 43, 44, 45, 46, 48, 50

[WZL24] Xinzhao Wang, Shengyu Zhang, and Tongyang Li. A quantum algorithm framework for discrete probability distributions with applications to Rényi entropy estimation. *IEEE Transactions on Information Theory*, 70(5):3399–3426, 2024. arXiv:2212.01571. 8, 43, 44, 45

[Yam02] Takuya Yamano. Some properties of q-logarithm and q-exponential functions in tsallis statistics. *Physica A: Statistical Mechanics and its Applications*, 305(3-4):486–496, 2002. 14

[Yeh20] Amir Yehudayoff. Pointer chasing via triangular discrimination. *Combinatorics, Probability and Computing*, 29(4):485–494, 2020. ECCC:TR16-151. 180

[YY99] Tomoyuki Yamakami and Andrew C Yao. $\mathsf{NQP}_{\mathbb{C}} = \mathsf{coC}_{=}\mathsf{P}$. *Information Processing Letters*, 71(2):63–69, 1999. arXiv:quant-ph/9812032. 12, 154

[Zal98] Christof Zalka. Simulating quantum systems on a quantum computer. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 454(1969):313–322, 1998. arXiv:quant-ph/9603026. 101

[Zha07] Zhengmin Zhang. Uniform estimates on the Tsallis entropies. *Letters in Mathematical Physics*, 80:171–181, 2007. 36

[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. 6