New Quantum Algorithms for Computing Quantum Entropies and Distances

Qisheng Wang, Ji Guan, Junyi Liu, Zhicheng Zhang, and Mingsheng Ying

***Abstract*— We propose a series of quantum algorithms for computing a wide range of quantum entropies and distances, including the von Neumann entropy, quantum Rényi entropy, trace distance, and fidelity. The proposed algorithms significantly outperform the prior best (and even quantum) ones in the low-rank case, some of which achieve exponential speedups. In particular, for N-dimensional quantum states of rank r, our proposed quantum algorithms for computing the von Neumann entropy, trace distance and fidelity within additive error ε have time complexity of $\tilde{O}(r/\varepsilon^2)$, $\tilde{O}(r^5/\varepsilon^6)$ and $\tilde{O}(r^{6.5}/\varepsilon^{7.5})$, respectively. By contrast, prior quantum algorithms for the von Neumann entropy and trace distance usually have time complexity $\Omega(N)$, and the prior best one for fidelity has time complexity $\tilde{O}(r^{12.5}/\varepsilon^{13.5})$. The key idea of our quantum algorithms is to extend block-encoding from unitary operators in previous work to quantum states (i.e., density operators). It is realized by developing several convenient techniques to manipulate quantum states and extract information from them. The advantage of our techniques over the existing methods is that no restrictions on density operators are required; in sharp contrast, the previous methods usually require a lower bound on the minimal non-zero eigenvalue of density operators.**

***Index Terms*— Quantum computing, quantum algorithms, quantum entropy, trace distance, quantum fidelity.**

I. Introduction

QUANTUM entropies and distances are basic concepts [1] in quantum physics and quantum information. Quantum entropies characterize the randomness of a quantum system, while quantum distances measure the closeness of quantum systems. It is essential to compute their values in many important applications, from the estimation of the capacity of quantum communication channels and verification of the outcomes of quantum computation to the characterization of quantum physical systems (see, e.g., [2], [3], [4]). Several kinds of quantum algorithms for computing quantum entropies and distances have been proposed under different computational resources, e.g., quantum algorithms with access to copies of quantum states [5], [6], [7], quantum algorithms with purified quantum query access [8], [9], [10], [11], and variational quantum algorithms [12], [13], [14].

A main consideration of those quantum algorithms with copy access for computing quantum entropies and distances is the number of copies of quantum states used in the algorithms. This type of input model is known as the "quantum sample access" model, where identical copies of quantum states are directly given. For example, a method of testing the closeness of N-dimensional mixed quantum states was provided in [5] with respect to trace distance and fidelity using $O(N/\varepsilon^2)$ and $O(N/\varepsilon)$ copies, respectively, based on quantum spectrum testing [15] and efficient quantum tomography [16], [17], [18]. A method of computing the von Neumann and quantum Rényi entropies of an N-dimensional quantum state was introduced in [6] using $O(N^2/\varepsilon^2)$ and $O(N^{2/\alpha}/\varepsilon^{2/\alpha})$ copies, respectively. Recently, a new method of computing entropies was proposed in [7], especially computing the von Neumann entropy uses $\tilde{O}(\kappa^2/\varepsilon^5)$ copies,[1] where $\kappa > 0$ is given such that $\Pi/\kappa \leq \rho \leq I$ for some projector Π. A distributed quantum algorithm for computing $\mathrm{tr}(\rho\sigma)$, i.e., the fidelity of pure quantum states, was proposed in [19] using $O(\max\{\sqrt{N}/\varepsilon, 1/\varepsilon^2\})$ copies.

Another class of quantum algorithms for computing quantum entropies and distances utilizes the conventional "purified quantum query access" model, where mixed quantum states are given by quantum oracles that prepare their purifications. Quantum algorithms for computing the von Neumann entropy and closeness testing with respect to trace distance were developed in [8] with query complexity $\tilde{O}(N/\varepsilon^{1.5})$ and $\tilde{O}(N/\varepsilon)$, respectively, both of which have complexity exponential in the number of qubits. Recently, a quantum algorithm for computing the von Neumann entropy within a multiplicative factor was proposed in [9], which reproduces the result within additive error of [8]. A method of computing the quantum α-Rényi entropy was proposed in [10] using $O\left(\frac{\kappa}{(x\varepsilon)^2}\log\left(\frac{N}{\varepsilon}\right)\right)$

Manuscript received 14 October 2022; revised 16 January 2024; accepted 23 April 2024. Date of publication 13 May 2024; date of current version 16 July 2024. The work of Qisheng Wang was supported in part by the Ministry of Education, Culture, Sports, Science and Technology (MEXT) Quantum Leap Flagship Program (MEXT Q-LEAP) under Grant JPMXS0120319794. The work of Ji Guan was supported in part by the Youth Innovation Promotion Association, Chinese Academy of Sciences, under Grant 2023116; and in part by the Key Research Program of the Chinese Academy of Sciences under Grant ZDRW-XX-2022-1. The work of Zhicheng Zhang was supported by Sydney Quantum Academy, Sydney, NSW, Australia. *(Corresponding author: Qisheng Wang.)*

Qisheng Wang was with the Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China. He is now with the Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan (e-mail: QishengWang1994@gmail.com).

Ji Guan is with the Key Laboratory of System Software, Chinese Academy of Sciences, Beijing 100190, China, and also with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China (e-mail: GuanJi1992@gmail.com).

Junyi Liu was with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China, and also with the University of Chinese Academy of Sciences, Beijing 100049, China. He is now with the Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD 20742 USA (e-mail: JunyiLiu1994@gmail.com).

Zhicheng Zhang and Mingsheng Ying are with the Centre for Quantum Software and Information, University of Technology Sydney, Sydney, NSW 2007, Australia (e-mail: iszczhang@gmail.com; Mingsheng.Ying@uts.edu.au).

Communicated by M. Tomamichel, Associate Editor for Quantum.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2024.3399014.

Digital Object Identifier 10.1109/TIT.2024.3399014

[1] $\tilde{O}(\cdot)$ suppresses polylogarithmic factors.

queries to the oracle, where $\kappa > 0$ is given such that $I/\kappa \leq \rho \leq I$ and $x = \mathrm{tr}(\rho^\alpha)/N$.

Compared to the "quantum sample access" model where only identical copies of quantum states are directly given, the "purified quantum query access" model allows more potential operations from which one can learn properties of quantum states. This is because any operation allowed in the former model can be trivially simulated in the latter model. Consequently, the latter model (in query complexity) usually uses fewer computational resources than the former (in sample complexity). For example, the best known query complexity for computing the von Neumann entropy is $\tilde{O}(N/\varepsilon^{1.5})$ [8], while the best known sample complexity for the same task is $O(N^2/\varepsilon^2)$ [6]. In addition, the latter model also plays an important role in computational complexity theory when comparing classical and quantum computing. For example, testing the closeness between two quantum states (in trace distance) is known to be QSZK-complete (in certain parameter regime) [20], [21], where the quantum states are given in the "purified quantum query access" model.

The recent quantum algorithms with purified quantum query access mentioned above are usually developed in the general framework of quantum singular value transformation (QSVT) [22]. The powerful technique of QSVT on unitary operators developed by [22] has been successfully applied as a unified framework in a wide range of quantum algorithms, including Grover's search algorithm [23], the quantum walk algorithms [24], [25], the HHL algorithm for solving systems of linear equations [26], and Hamiltonian simulation [27]. In the framework of QSVT, a unitary operator U can be regarded as a block-encoding that stores a matrix A in (the upper-left corner of) its matrix representation (see Definition II.1). QSVT can be understood as an algorithmic technique that transforms the matrix A to $f(A)$ for some function $f(\cdot)$ of interest, and it also provides a quantum circuit implementation of $\tilde{U}$ that block-encodes $f(A)$ using queries to U. The original QSVT deals with unitary operators, while a Hamiltonian variant of the QSVT was proposed in [28], which was then used in quantum polar decomposition [29], [30].

Except for unitary operators and Hamiltonians, density operators (mixed quantum states) are another important class of objects we can manipulate in quantum computation. A technique was developed in [31] to implement a unitary operator that block-encodes a density operator, using queries to its purified quantum query oracle. Equipped with QSVT, this technique enables us to implement unitary operators that block-encode certain matrix functions of quantum states, and thus strengthens the power of the "purified quantum query access" model. This technique has been employed in quantum algorithms for semidefinite programming [32] and quantum fidelity estimation [11]. Conversely, however, it seems difficult to prepare a quantum state from a unitary operator that block-encodes its density operator.

A natural idea of extracting information from a density operator is to directly manipulate the quantum state itself rather than a unitary operator that encodes it. This leads us to extend the definition of block-encoding proposed originally for unitary operators [22], [31], [33] to that for general operators (see Definition II.1), especially for quantum states (i.e., density operators). Regarding quantum states as block-encodings, we are able to design new quantum algorithms for computing a wide range of quantum entropies and distances, such as the von Neumann entropy, quantum Rényi entropy, quantum Tsallis entropy, trace distance, and fidelity. These quantum algorithms significantly outperform the best known ones in the low-rank case, and some of them can even achieve exponential speedups. Here, the low-rank case means that the rank of N-dimensional quantum states is much smaller than N, e.g., $r = \mathrm{polylog}(N)$, which is of great interest in both theoretical (e.g., [34], [35]) and experimental (e.g., [36]) physics.

In the remainder of this Introduction, we will first present our main results in Section I-A. The new techniques that enable us to achieve our results will be outlined in Section I-B. Then related works will be reviewed in Section I-C, and a discussion will be given in Section I-D.

A. Main Results

Let us first set the stage for presenting our main results. In order to manipulate quantum states, we extend the definition of block-encoding for unitary operators to that for general operators (see Definition II.1), and use this extended definition of block-encoding to describe our quantum algorithms. In our quantum algorithms, a mixed quantum state is given by a quantum unitary operator (oracle) which prepares a purification of the state (see Definition II.2). This conventional model is known as the "purified quantum query access" model and has been widely used in developing quantum algorithms [8], [9], [10], [32], [37], [38].

Throughout this paper, the quantum query complexity of a quantum query algorithm means the number of queries to the given quantum oracles. The time complexity of a quantum query algorithm is the sum of its quantum query complexity and the number of elementary quantum gates used in it. When quantum algorithms are compared with classical algorithms, quantum oracles are given as classical descriptions of quantum circuits. The actual number of elementary quantum gates performed in the quantum algorithm only has a polynomial overhead compared to its "time complexity" defined here. Then our main results can be summarized in the following:

Theorem I.1 (Informal): In the "purified quantum query access" model, given quantum oracles that prepare N-dimensional mixed quantum states of rank r, there are quantum query algorithms that compute

- von Neumann entropy,
- quantum α-Rényi entropies for $\alpha \in (0, 1) \cup (1, +\infty)$,
- quantum α-Tsallis entropies for $\alpha \in (0, 1) \cup (1, +\infty)$,
- α-trace distance for $\alpha > 0$ (defined by Eq. (1), including the trace distance), and
- α-fidelity for $0 < \alpha < 1$ (defined by Eq. (2), including the fidelity)

within additive error ε with time complexity $\operatorname{poly}(\log(N), r, 1/\varepsilon)$, where the time complexity hides a constant which depends only on α.[2]

Our quantum algorithms are compared with the existing algorithms in Table I. In particular, our algorithms outperform the best known ones in the low-rank case, e.g., $r = \operatorname{polylog}(N)$. To see this more clearly, let us recast the existing results in the low-rank case, and then compare them with ours. Table I compares the query complexity (in the "purified quantum query access" model) and the sample complexity (in the "quantum sample access" model). It is important to note the difference between the two models in the comparison. While it is trivial that a sample in the "quantum sample access" model can be simulated by a query in the "purified quantum query access" model, the vice versa remains unknown. In other words, the "quantum sample access" model can be seen as a restricted version of the "purified quantum query access" model where the oracle is only used to prepare the mixed quantum states. Therefore, any sample complexity in the "quantum sample access" model implies the same amount of query complexity in the "purified quantum query access" model. Regarding these, we still compare the query/sample complexities defined in the two models together. For further discussion regarding the two different quantum input models, please refer to [8].

- For the von Neumann entropy and quantum α-Rényi entropy, it was shown in [6] that their sample complexities are $O\left(N^2/\varepsilon^2\right)$ and $O\left((N/\varepsilon)^{\max\{2/\alpha,2\}}\right)$, respectively. Unitarily invariant properties of entropies considered, their method is based on weak Schur sampling (see [43]), and does not imply a straightforward method for low-rank quantum states. The query complexity for the von Neumann entropy was shown in [8] to be $\tilde{O}(N/\varepsilon^{1.5})$, which can be improved to $\tilde{O}(\sqrt{Nr}/\varepsilon^{1.5})$ for the low-rank case after a careful analysis. It was shown in [42] that $\tilde{O}(\kappa^2/\varepsilon)$ queries are sufficient to compute the von Neumann entropy of a quantum state ρ if some $\kappa > 0$ is known in advance such that $\rho \geq I/\kappa$. Similarly, the method in [10] for the quantum α-Rényi entropy can be improved to $\tilde{O}\left(\kappa N r^{\max\{\alpha-1,0\}}/\varepsilon^2\right)$ for the low-rank case.
- For the trace distance and fidelity, most algorithms are proposed for closeness testing with respect to them. The sample complexities $O\left(N/\varepsilon^2\right)$ and $O\left(N/\varepsilon\right)$ given in [5] can be improved (by their Corollary 1.6) to $O\left(r/\varepsilon^2\right)$ and $O\left(r/\varepsilon\right)$ for the low-rank case, respectively. The query complexity $\tilde{O}(N/\varepsilon)$ given in [8] can be improved to $\tilde{O}(\min\{\sqrt{Nr}/\varepsilon, r/\varepsilon^2\})$ for the low-rank case. The above results do not cover our results, because closeness testing can be solved by computing the closeness but the converse seems difficult.
- For the quantum algorithms in [7], [10], and [42] that attempt to reduce the dependence on N, they introduce an extra dependence on κ, where κ is the reciprocal of the minimal non-zero eigenvalue of quantum states. Our quantum algorithms can be easily adapted to their settings by taking $r = O(\kappa)$, thus with time complexity $\operatorname{poly}(\log(N), \kappa, 1/\varepsilon)$, while the converse seems not applicable.[3]

Although our quantum algorithms focus on low-rank quantum states, they are also comparable to those for the general case where one could only assume that the quantum states are full-rank, i.e., $r = N$.

- For the von Neumann entropy, our quantum algorithm has query complexity $\tilde{O}(N/\varepsilon^2)$ when the quantum state is full-rank, which is slightly worse than the query complexity $\tilde{O}(N/\varepsilon^{1.5})$ in [8].
- For the trace distance, our quantum algorithm has query complexity $\tilde{O}(N^5/\varepsilon^6)$ when the quantum state is full-rank. To the best of our knowledge, this is the first quantum algorithm for computing the trace distance between quantum states with time complexity $\operatorname{poly}(N)$ in the general case.

We will further discuss the above results for quantum entropies in Section I-A.1 and those for closeness (i.e. trace distance and fidelity) of quantum states in Section I-A.2.

1) *Computing Quantum Entropies:*

In quantum information theory, the entropy of a (mixed) quantum state is a measure of its uncertainty, and computing its value is crucial when characterizing and verifying an unknown quantum system. After von Neumann [44] introduced the famous von Neumann entropy

$$S(\rho) = -\operatorname{tr}\left(\rho \ln\left(\rho\right)\right),$$

which is a natural generalization of the classical Shannon entropy [45], several other entropies have been proposed, e.g., Rényi entropy [46], [47], [48], [49], Tsallis entropy [50], [51], [52], Min and Max (Hartley) entropies [53], [54], [55], and the unified entropy [56], [57]. The quantum α-Rényi entropy and the quantum α-Tsallis entropy are defined by

$$S_\alpha^R(\rho) = \frac{1}{1-\alpha} \ln\left(\operatorname{tr}\left(\rho^\alpha\right)\right),$$
$$S_\alpha^T(\rho) = \frac{1}{1-\alpha}\left(\operatorname{tr}\left(\rho^\alpha\right) - 1\right)$$

for $\alpha \in (0,1) \cup (1,+\infty)$, respectively. It is easy to see that the von Neumann entropy is a limiting case of the Rényi entropy [48] and the Tsallis entropy [50]:

$$S(\rho) = \lim_{\alpha\to 1} S_\alpha^R(\rho) = \lim_{\alpha\to 1} S_\alpha^T(\rho).$$

For $\alpha = 0$, the quantum Tsallis entropy degenerates to the rank of quantum states:

$$S_0^T(\rho) = \operatorname{rank}(\rho) - 1$$

[2] A few days after this paper was submitted to arXiv, the concurrent work of Gilyén and Poremba [39] appeared. They proposed a quantum algorithm for fidelity estimation using identical copies of quantum states based on density matrix exponentiation [40], [41]. We note that their techniques of converting identical copies to unitary block-encodings (Corollary IV.4 in [39]) can be applied to our quantum algorithms in Theorem I.1. As a result, we can obtain quantum algorithms for computing these quantum entropies and distances using $\operatorname{poly}(r, 1/\varepsilon)$ copies of quantum states, which only has a polynomial overhead compared to the query complexity of our quantum query algorithms.

[3] This is because κ implies an upper bound $r \leq \kappa$ of rank, but r does not imply any upper bound for κ.

TABLE I

OUR QUANTUM ALGORITHMS VS. PRIOR WORKS*

Quantum Information Quantity	Prior Best Sample Complexity	Prior Best Query Complexity	Our Query Complexity
Von Neumann Entropy	$O(N^2/\varepsilon^2)$, $\tilde{O}\left(\kappa^2/\varepsilon^5\right)$ [6], [7]	$\tilde{O}(\sqrt{Nr}/\varepsilon^{1.5})$, $\tilde{O}(\kappa^2/\varepsilon)$ [8], [42]	$\tilde{O}(r/\varepsilon^2)$
Quantum α-Rényi Entropy (for non-integer $\alpha > 0$)	$O\left((N/\varepsilon)^{\max\{2/\alpha,2\}}\right)$ [6]	$\tilde{O}\left(\kappa N r^{\max\{\alpha-1,0\}}/\varepsilon^2\right)$ [10]	$\tilde{O}\left(\frac{r^{\alpha-1+\alpha/\{\frac{\alpha-1}{2}\}}}{\varepsilon^{1+1/\{\frac{\alpha-1}{2}\}}}\right)$
Trace Distance	$O(r/\varepsilon^2)^\dagger$ [5]	$\tilde{O}(\min\{\sqrt{Nr}/\varepsilon, r/\varepsilon^2\})^\dagger$ [8]	$\tilde{O}(r^5/\varepsilon^6)$
Fidelity	$O(r/\varepsilon)^\dagger$ [5]	$\tilde{O}\left(r^{12.5}/\varepsilon^{13.5}\right)^\ddagger$ [11]	$\tilde{O}(r^{6.5}/\varepsilon^{7.5})$

* N is the dimension of quantum states. ε is the desired additive error. r is (an upper bound for) the rank of quantum states. $\{x\} = x - \lfloor x \rfloor$ denotes the decimal part of x. κ is the parameter associated with mixed quantum state ρ such that $I/\kappa \leq \rho \leq I$, which only appears in the best prior query complexity of quantum α-Rényi entropy.

† These are the sample/query complexities for closeness testing with respect to the trace distance (resp. fidelity). It is worth mentioning that closeness testing can be solved by computing the closeness, but the converse seems difficult.

‡ In the concurrent work of Gilyén and Poremba [39], they presented a different quantum algorithm for fidelity estimation with a better query complexity $\tilde{O}\left(r^{2.5}/\varepsilon^5\right)$.

TABLE II

QUANTUM QUERY COMPLEXITY FOR COMPUTING QUANTUM ENTROPIES*

Parameter α		Quantum Rényi Entropy $S_\alpha^R(\rho)$	Quantum Tsallis Entropy $S_\alpha^T(\rho)$
$\alpha = 0$		$\tilde{O}\left(\kappa^2/\varepsilon\right)$ (Theorem III.6) (Max Entropy)	$\tilde{O}\left(\kappa^2\right)$ (Corollary III.5) (Rank)
$0 < \alpha < 1$		$\tilde{O}\left(r^{\frac{3-\alpha^2}{2\alpha}}/\varepsilon^{\frac{3+\alpha}{2\alpha}}\right)$ (Theorem III.8 and III.9)	
$\alpha = 1$ (Von Neumann Entropy)		$\tilde{O}\left(r/\varepsilon^2\right)$ (Theorem III.1)	
$\alpha > 1$	$\alpha \equiv 1 \pmod 2$	$O\left(r^{\alpha-1}/\varepsilon\right)$ (Theorem III.8)	$O\left(1/\varepsilon\right)$ (Theorem III.9)
	$\alpha \not\equiv 1 \pmod 2$	$\tilde{O}\left(r^{\alpha-1+\alpha/\{\frac{\alpha-1}{2}\}}/\varepsilon^{1+1/\{\frac{\alpha-1}{2}\}}\right)$ (Theorem III.8 and III.9)	

* r is (an upper bound for) the rank of quantum states. ε is the desired additive error. $\{x\} = x - \lfloor x \rfloor$ denotes the decimal part of x. κ is the parameter associated with mixed quantum state ρ such that $\Pi/\kappa \leq \rho$ for some projector Π, which is only used in the case $\alpha = 0$.

and the quantum Rényi entropy becomes the logarithm of the rank, i.e., the quantum Max (Hartley) entropy:

$$S^{\max}(\rho) = S_0^R(\rho) = \ln(\operatorname{rank}(\rho)).$$

a) Overview: Given a quantum unitary oracle that prepares a mixed quantum state (see Definition II.2), we develop quantum algorithms for computing several quantum entropies. Their quantum query complexities are collected in Table II, which are also their quantum time complexities up to polylogarithmic factors. Most of our algorithms do not require any restrictions on the lower bound for the eigenvalues of quantum states except those for computing the quantum Max entropy and the rank of quantum states, where $\Pi/\kappa \leq \rho$ is required for some projector Π and $\kappa > 0$.

The prior best quantum algorithms for computing von Neumann entropy [6], [8], [9] and quantum Rényi entropy [6], [10] have time complexity $\Omega(N)$ even for rank $r = 2$. Compared to them, our quantum algorithms are exponentially faster in the low-rank case. In particular, our quantum algorithm for computing the von Neumann entropy with query complexity $\tilde{O}(r/\varepsilon^2)$ is comparable to the quantum algorithm given in [42] with query complexity $\tilde{O}(\kappa^2/\varepsilon)$, where we note that $r \leq \kappa$ always holds.

It is worth mentioning that for odd integer $\alpha > 1$, the query complexity of computing the quantum Tsallis entropy $S_\alpha^T(\rho)$ does not depend on rank r. In this case, there is a simple SWAP test-like quantum algorithm that computes $\operatorname{tr}(\rho^\alpha)$ using $O(1/\varepsilon^2)$ copies [41], [58]. Compared to it, our algorithm (Theorem III.7) yields a quadratic speedup (see Section III-C for more discussions). For non-integer α, we are not aware of any prior approaches for computing the quantum Tsallis entropy with complexity better than quantum state tomography.

b) Lower bounds: We are able to give a query lower bound $\tilde{\Omega}(r^c)$ for computing the quantum Rényi entropy $S_\alpha^R(\rho)$ including the von Neumann entropy $S(\rho)$ in terms of rank r, where $c \geq 1/3$ is a constant depending only on α (see Theorem III.11). This lower bound is simply derived from the quantum query complexity for computing the Rényi (and Shannon) entropy of classical probability distributions [59], [60].

TABLE III
QUANTUM QUERY COMPLEXITY FOR COMPUTING α-TRACE DISTANCE*

Parameter α	$T_\alpha(\rho,\sigma)$ (Theorem IV.1)
$0 < \alpha < 1$	$\tilde{O}\left(r^{5/\alpha+(1-\alpha)/2}/\varepsilon^{5/\alpha+1}\right)$
$\alpha \equiv 0 \pmod 2$	$\tilde{O}\left(r^3/\varepsilon^4\right)$
$\alpha \geq 1$ and $\alpha \not\equiv 0 \pmod 2$	$\tilde{O}\left(r^{3+1/\{\alpha/2\}}/\varepsilon^{4+1/\{\alpha/2\}}\right)$
$\alpha = 1$ (Trace Distance)	$\tilde{O}\left(r^5/\varepsilon^6\right)$

* r is (an upper bound for) the higher rank of the two quantum states. ε is the desired additive error. $\{x\} = x - \lfloor x \rfloor$ denotes the decimal part of x.

TABLE IV
QUANTUM QUERY COMPLEXITY FOR COMPUTING α-FIDELITY*

Parameter $\beta = (1-\alpha)/2\alpha$	$F_\alpha(\rho,\sigma)$ (Theorem IV.5)
$\beta \in \mathbb{N}$	$\tilde{O}\left(r^{\frac{3-\alpha}{2\alpha}}/\varepsilon^{\frac{3+\alpha}{2\alpha}}\right)$
$\beta \notin \mathbb{N}$	$\tilde{O}\left(r^{\frac{3-\alpha}{2\alpha}+\frac{1}{\alpha\{\beta\}}}/\varepsilon^{\frac{3+\alpha}{2\alpha}+\frac{1}{\alpha\{\beta\}}}\right)$
$\alpha = \beta = 1/2$ (Fidelity)	$\tilde{O}\left(r^{6.5}/\varepsilon^{7.5}\right)$

* r is (an upper bound for) the lower rank of the two quantum states. ε is the desired additive error. $\{x\} = x - \lfloor x \rfloor$ denotes the decimal part of x.

2) Computing Quantum Distances: Distance measures of quantum states are basic quantities in quantum computation and quantum information. Two of the most important distance measures are the trace distance and fidelity. For each of them, we propose quantum algorithms that compute it and its extensions. Here, we assume that there are two quantum oracles U_ρ and U_σ that prepare the density operators ρ and σ, respectively. The query complexity of a quantum algorithm means the total number of queries to both U_ρ and U_σ.

a) Trace distance: The α-trace distance of two quantum states ρ and σ is defined by

$$T_\alpha(\rho,\sigma) = \operatorname{tr}\left(\left|\frac{\rho-\sigma}{2}\right|^\alpha\right) = \left\|\frac{\rho-\sigma}{2}\right\|_{S,\alpha}^\alpha, \tag{1}$$

where $\|A\|_{S,\alpha} = \left(\operatorname{tr}\left(|A|^\alpha\right)\right)^{1/\alpha}$ is the Schatten α-norm. Here, the 1-trace distance is the well-known trace distance $T(\rho,\sigma) = T_1(\rho,\sigma)$.

We develop quantum algorithms for computing α-trace distance for $\alpha > 0$, with their query complexities shown in Table III. As a special case, our quantum algorithm (Theorem IV.1) for computing the trace distance (i.e., the 1-trace distance) has query complexity $\tilde{O}\left(r^5/\varepsilon^6\right)$. Note that the closeness testing of the α-trace distances of quantum states for integer α, e.g., the 1-, 2- and 3-trace distances, was studied in [8]. For other cases of α, we are not aware of any prior approaches to compute the α-trace distance with complexity better than quantum state tomography.

b) Fidelity: The α-fidelity of two quantum states ρ and σ is defined by

$$F_\alpha(\rho,\sigma) = \exp\left((\alpha-1)D_\alpha(\rho\|\sigma)\right) = \operatorname{tr}\left(\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right), \tag{2}$$

where $D_\alpha(\rho\|\sigma)$ is the sandwiched quantum Rényi relative entropy [48], [49]. Here, the $1/2$-fidelity is the well-known fidelity $F(\rho,\sigma) = F_{1/2}(\rho,\sigma)$ [61].

We develop quantum algorithms for computing the α-fidelity for $0 < \alpha < 1$, with their query complexities shown in Table IV). As a special case, our quantum algorithm (Theorem IV.5) for computing the fidelity (i.e., the $1/2$-fidelity) has query complexity $\tilde{O}\left(r^{6.5}/\varepsilon^{7.5}\right)$, which is a polynomial speedup over the best known $\tilde{O}\left(r^{12.5}/\varepsilon^{13.5}\right)$ in [11]. For other cases of α, we do not know any prior approaches to compute the α-fidelity with complexity better than quantum state tomography.

c) Lower bounds and hardness: Our quantum algorithms for computing the fidelity and trace distance have a time complexity polynomial in the rank r. We show that there is no quantum algorithm that computes the fidelity or trace distance with time complexity $\operatorname{poly}(\log(r), 1/\varepsilon)$ unless $\mathsf{BQP} = \mathsf{QSZK}$ (see Theorem IV.7), based on the result of [20] that (α,β)-Quantum State Distinguishability is QSZK-complete for $0 \leq \alpha < \beta^2 \leq 1$.[4]

Our quantum algorithms for computing the fidelity and trace distance achieve a significant speedup under the low-rank assumption. We argue that these problems are unlikely to be efficiently solved by classical computers because computing the fidelity and trace distance are $\mathsf{DQC1}$-hard (see Theorem IV.8); and it was shown in [63] that $\mathsf{DQC1}$ is not (classically) weakly simulatable unless the polynomial hierarchy collapses to the second level, i.e., $\mathsf{PH} = \mathsf{AM}$.

B. Techniques

In this subsection, we give an overview of the techniques that enable us to achieve the results presented in the above subsection.

1) Quantum States as Block-Encodings: The key idea of our quantum algorithms is to regard quantum states as

[4] The available regime of α and β for the QSZK-completeness of (α,β)-Quantum State Distinguishability was recently improved to $0 \leq \sqrt{2\ln 2}\alpha < \beta^2 \leq 1$ in [62].

TABLE V

COMPARISON BETWEEN DENSITY OPERATORS AND UNITARY OPERATORS AS BLOCK-ENCODINGS*

Operation Type	Density Operators $\rho \approx \begin{bmatrix} A & \cdot \\ \cdot & \cdot \end{bmatrix}$	Unitary Operators $U \approx \begin{bmatrix} A & \cdot \\ \cdot & \cdot \end{bmatrix}$
Evolution	$A \to BAB^\dagger$	$A \to AB$ or BA
Trace Estimation	$\mathrm{tr}(A)$	$\mathrm{tr}(A)/2^a$ †
Linear Combination	$\alpha_1 A_1 + \cdots + \alpha_k A_k$ $(\alpha_i \in \mathbb{R}^+)$	$\alpha_1 A_1 + \cdots + \alpha_k A_k$ $(\alpha_i \in \mathbb{C})$
Eigenvalue Transformation	$A \to A(P(A))^2$	$A \to P(A)$
Positive Powers	$A \to A^c (0 < c < 1)$	$A \to \lvert A\rvert^c$ $(0 < c < 1)$
Eigenvalue Threshold Projector	$A \to$ (scaled) $\Pi_{\mathrm{supp}(A)}$	$A \to \Pi_{\mathrm{supp}(A)}$

* A is an Hermitian operator block-encoded in a density ρ or a unitary operator U. B is block-encoded in a unitary operator. $P(\cdot)$ is a polynomial.

† Suppose A is an a-qubit Hermitian operator block-encoded in unitary operator U. Then $\mathrm{tr}(A)/2^a = \mathrm{tr}\left((|0\rangle\langle 0| \otimes \frac{I_a}{2^a}) U \right)$ can be computed through the Hadamard test [58].

block-encodings. To this end, we extend the definition of block-encoding proposed for unitary operators to that for general ones (see Definition II.1). Suppose that a unitary operator U_A prepares a subnormalized density operator A (see Definition II.2). In this framework, we provide a convenient way to manipulate the subnormalized density operator A and extract information from it as follows.

- **Evolution**: If U is a unitary operator, which is a block-encoding of an operator B, we can prepare a subnormalized density operator $BAB^\dagger$ (see Lemma II.2). This evolution of the subnormalized density operator can be seen as a generalization of quantum unitary operation $\rho \mapsto U\rho U^\dagger$ for (normalized) density operator ρ.
- **Trace Estimation**: We provide an efficient method to estimate the trace of A based on quantum amplitude estimation [64] (see Lemma II.15). As will be seen, trace estimation is an important subroutine in our quantum algorithms (see Section I-A.1 and Section I-A.2).
- **Linear Combinations**: As an analog of Linear-Combination-of-Unitaries (LCU) algorithm through a series of work [22], [65], [66], [67], [68], [69], [70], we also provide a technique to prepare a linear (convex) combination of subnormalized density operators (see Lemma II.17). This technique will be used in computing the trace distance (see Section I-A.2 and Theorem IV.1).

The technique of "trace estimation" is the cornerstone in developing our quantum algorithms. To compute the values of quantum entropies and distances, the key part has the form $\mathrm{tr}(\varrho)$, where ϱ is a (subnormalized) density operator. Our strategy is to prepare a quantum state, which is a block-encoding of ϱ, through the technique of "evolution". Roughly speaking, we prepare the subnormalized density operator ϱ up to a scaling factor; we will use the phrase "prepare ϱ" regardless of the scaling factor in the following discussion of this section. For example, we prepare $-\rho\ln(\rho)$ for the von Neumann entropy, and prepare ρ^α for the quantum α-Rényi and Tsallis entropies. To achieve this, we develop techniques for eigenvalue transformation of density operators based on QSVT as follows.

- **Eigenvalue Transformation**: Based on the evolution, if we can construct a unitary operator U, which is a block-encoding of $P(A)$ for some polynomial $P(\cdot)$ as in QSVT [22], we can transform A to another subnormalized density operator $A(P(A))^2$ (see Theorem II.4).
- **Positive Powers**: We develop a technique to prepare the subnormalized density operator A^c for $0 < c < 1$ without any restrictions on A (see Lemma II.8). Inspired by this, we can also obtain a unitary operator, which is a block-encoding of $|A|^c$, using queries to a unitary operator U, which is a block-encoding of Hermitian operator A (see Lemma II.13). In order to obtain block-encodings of powers of A, previously known methods [22], [33], [38] usually require a lower bound for the minimal non-zero eigenvalues of density operators; for example, $I/\kappa \leq A \leq I$ for some $\kappa > 0$ in [33]. This technique for positive powers of subnormalized density operators will be frequently used in our quantum algorithms for computing quantum entropies, fidelity and trace distance (see Section I-A.1 and Section I-A.2), in order to avoid restrictions on density operators.

We also provide a method to block-encode the eigenvalue threshold projector $\Pi_{\mathrm{supp}(A)}$ of A in a quantum state, where $\mathrm{supp}(A)$ is the support of A, and Π_S is the projector onto subspace S.

- **Eigenvalue threshold projector**: We propose a method to (approximately) block-encode the eigenvalue threshold projector $\Pi_{\mathrm{supp}(A)}$ of A in a subnormalized density operator (see Lemma II.19). We note that a technique for block-encoding eigenvalue threshold projectors was also provided in [32], but they required that $A \geq q\Pi$ for some projector Π and the value of $q > 0$ is known in advance. In contrast, our method does not impose any restriction on A. This method will be used in computing the trace distance (see Section I-A.2 and Theorem IV.1).

A comparison between density operators and unitary operators as block-encodings is given in Table V.

2) Example — Computing Trace Distance: To give the readers a flavor, we take the quantum algorithm for computing the trace distance (see Theorem IV.1 for details) as an illustrative example. The key observation to compute the trace

$$\left.\begin{array}{lccccc} \text{Density:} & \rho,\sigma & \to & \mu=(\rho+\sigma)/2 & \to & \hat{\Pi}\approx\Pi_{\mathrm{supp}(\mu)} \\ & \downarrow & & & & \\ \text{Unitary:} & \rho,\sigma & \to & \nu=\left|\rho-\sigma\right|/2 & \to & \hat{\nu}\approx\left|\nu\right|^{1/2} \end{array}\right\} \to \hat{\nu}\hat{\Pi}\hat{\nu}^{\dagger} \to \mathrm{tr}\left(\hat{\nu}\hat{\Pi}\hat{\nu}^{\dagger}\right) \approx \mathrm{tr}(\eta) = T(\rho,\sigma)$$

Fig. 1. The computation process of computing trace distance.

distance is that

$$T(\rho,\sigma)=\mathrm{tr}\left(\left|\nu\right|^{1/2}\Pi_{\mathrm{supp}(\mu)}\left|\nu\right|^{1/2}\right),$$

where $\nu=(\rho-\sigma)/2$, $\mu=(\rho+\sigma)/2$. The idea is to prepare $\eta=\left|\nu\right|^{1/2}\Pi_{\mathrm{supp}(\mu)}\left|\nu\right|^{1/2}$ (up to a scaling factor), and then estimate $\mathrm{tr}(\eta)$ through the technique of "trace estimation" (Lemma II.15). The computation process is shown in Figure 1.

To (approximately) prepare η, we first prepare $\hat{\Pi}\approx\Pi_{\mathrm{supp}(\mu)}$ through the technique of "eigenvalue threshold projector" (Lemma II.19). Here, $\mu=(\rho+\sigma)/2$ can be prepared through the technique of "linear combinations" (Lemma II.17). Then we only need to construct a unitary operator, which is a block-encoding of $\hat{\nu}\approx\left|\nu\right|^{1/2}$. After that, by the technique of "evolution" (Lemma II.2), we can prepare $\hat{\nu}\hat{\Pi}\hat{\nu}^{\dagger}\approx\left|\nu\right|^{1/2}\hat{\Pi}\left|\nu\right|^{1/2}\approx\eta$.

In order to construct a unitary operator as a block-encoding of $\left|\nu\right|^{1/2}$, we first use the LCU technique (Theorem II.18) to block-encode $\nu=(\rho-\sigma)/2$ in a unitary operator U_ν. Then applying the technique of "positive powers" (Lemma II.13) on U_ν, we can construct a unitary operator which is a block-encoding of $\hat{\nu}\approx\left|\nu\right|^{1/2}$.

To get an estimation of the trace distance between ρ and σ, we should just note that $T(\rho,\sigma)=\mathrm{tr}(\eta)\approx\mathrm{tr}\left(\hat{\nu}\hat{\Pi}\hat{\nu}^{\dagger}\right)$, where we have already prepared $\hat{\nu}\hat{\Pi}\hat{\nu}^{\dagger}$ through the above process. Strictly speaking, we have prepared a mixed quantum state, whose density operator is a block-encoding of $\hat{\nu}\hat{\Pi}\hat{\nu}^{\dagger}$ up to a scaling factor. After carefully selecting appropriate parameters that determine the errors in the above process, we obtain a quantum algorithm for computing the trace distance with query complexity $\tilde{O}(r^5/\varepsilon^6)$, where r is (an upper bound for) the rank of quantum states ρ and σ, and ε is the desired additive error. Here, $\tilde{O}(\cdot)$ suppresses the polylogarithmic factor of N, where N is the dimension of the Hilbert space of ρ and σ.

C. Related Works

a) Classical property testing: The problems considered in this paper can be thought of as a quantum analog of testing properties of probability distributions. Classical algorithms for testing properties of probability distributions have been widely studied since the beginning of this century. The first algorithm was proposed in [71] for the closeness testing of probability distributions in ℓ^1 distance using $\tilde{O}(N^{2/3}/\varepsilon^4)$ samples, which was then improved to use $\tilde{O}(N^{2/3}/\varepsilon^{8/3})$ samples [72]. Later, it was shown in [73] that the optimal sample complexity for this problem is $\Theta\left(\max\{N^{2/3}/\varepsilon^{4/3},N^{1/2}/\varepsilon^2\}\right)$, and they also proved that the optimal sample complexity $\Theta(1/\varepsilon^2)$ for closeness testing in ℓ^2 distance. The identity testing is a special case of the closeness testing given that one of the distributions is known. It was shown in [74] that $\tilde{O}(N^{1/2}/\varepsilon^4)$ samples are sufficient for the identity testing in ℓ^1 distance, which was improved to optimal $\Theta(N^{1/2}/\varepsilon^2)$ in [75]. The independence testing, i.e., whether a distribution on $[N]\times[M]$ $(N\geq M)$ is equal to or ε-far from a product distribution in ℓ^1 distance, was shown to have sample complexity $\tilde{O}(N^{2/3}M^{1/3})\cdot\mathrm{poly}(1/\varepsilon)$ [74]. Recently, a modular reduction-based approach was proposed in [76], which covers the closeness, identity and independence testing. They also gave a tight sample complexity $\Theta\left(\max\{N^{2/3}M^{1/3}/\varepsilon^{4/3},(NM)^{1/2}/\varepsilon^2\}\right)$ for the independence testing. In addition, the monotonicity testing was also shown to have sample complexity $\tilde{O}(N^{1/2}/\varepsilon^4)$ [77].

Apart from property testing between distributions, properties of a single distribution are well studied in the literature, e.g., [78], [79], and [80]. An algorithm that computes the Shannon entropy using $O\left(\frac{N}{\varepsilon\log(N)}\right)$ samples for $\varepsilon=\Omega(N^{0.03})$ was proposed in [81] and [82]. After that, the optimal estimator of Shannon entropy using $\Theta\left(\frac{N}{\varepsilon\log(N)}+\frac{(\log(N))^2}{\varepsilon^2}\right)$ samples was given in [83] and [84]. Also, an estimator for $\exp\left((1-\alpha)S_\alpha^R(p)\right)$ was provided in [83], where $S_\alpha^R(p)$ is the α-Rényi entropy of distribution p.

b) Quantum property testing: The emerging topic of quantum property testing (see [43]) studies the quantum advantage in testing classical statistical and quantum information properties.

Quantum advantages in testing classical statistical properties have been extensively studied. Quantum algorithms for testing properties of classical distributions was first studied in [85], which gave quantum query complexity $O(N^{1/2}/\varepsilon^6)$ for the closeness testing, and $O(N^{1/3})$ for identity testing (to the uniform distribution) in ℓ^1 distance (for constant precision ε). Later, the quantum query complexity of the identity testing (to a known distribution) was improved to $\tilde{O}(N^{1/3}/\varepsilon^5)$ in [86]. The quantum query complexity for the closeness testing in ℓ^1 distance was further improved to $\tilde{O}(N^{1/2}/\varepsilon^{2.5})$ in [87], to $\tilde{O}(N^{1/2}/\varepsilon)$ in [8], and to $O(N^{1/2}/\varepsilon)$ in [88]. Recently, the quantum query complexity for computing the Shannon entropy and the Rényi entropy was studied in [59]; especially, an $\tilde{O}(N^{1/2}/\varepsilon^2)$ quantum query complexity was shown for the Shannon entropy.

There are also some quantum algorithms for testing quantum information properties not mentioned above. It was shown in [41] that testing the orthogonality of pure quantum states requires $\Theta(1/\varepsilon)$ copies, promised that either they are orthogonal or have fidelity $\geq\varepsilon$. Recently, it was shown in [89] that quantum identity testing only uses $O(N^{3/2}/\varepsilon^2)$ copies with the help of random choice of independent measurements.

D. Discussion

In this paper, we suggest a generalized definition of block-encoding, with which we can directly manipulate subnormalized density operators and extract information from them. Based on this, we develop new quantum algorithms that compute a large class of quantum entropies and distances, which achieve a significant speedup over the best known ones in the low-rank case. Several interesting problems remain open:

- Our upper and lower bounds are far from being tight, a similar issue for computing the von Neumann entropy arose in [8]. In the error analysis of our algorithms, the rank r appears in the upper bound for the error as a multiplicative factor. This makes our algorithms unlikely to have complexity sub-polynomial in r. Can we find more efficient algorithms (for example, with query complexity sub-polynomial in r) or improve the lower bounds (to, for example, $\Omega(r)$)?
- It would be interesting to study other distance measures of quantum states, e.g., the relative von Neumann entropy [1] (the quantum generalization of the Kullback-Leibler divergence [90])

$$S(\rho\|\sigma) = \operatorname{tr}\left(\rho\left(\ln(\rho) - \ln(\sigma)\right)\right).$$

- Can we apply the idea of manipulating quantum states to problems other than computing quantum entropies and distances?

E. Recent Developments

After the work described in this paper, a series of quantum algorithms for computing quantum entropies and distances have been developed and applied in practical tasks.

- **Von Neumann entropy**. In the "purified quantum query access" model, the query complexity for computing the von Neumann entropy was further analyzed in detail and shown to be $O(r\log(r)/\varepsilon^2)$ in [91]. Computing the von Neumann entropy in space-bounded quantum computation was investigated in [92], and they showed that the space-bounded version of von Neumann entropy difference is BQL-complete. In the "quantum sample access" model, the time complexity for computing the von Neumann entropy was improved to $\tilde{O}(N^2)$ in [93], compared to the $\tilde{O}(N^6)$ in [6], while retaining the same (up to polylogarithmic factors) sample complexity $\tilde{O}(N^2)$.
- **Rényi entropy**. In the "purified quantum query access" model, the query complexity for computing the α-Rényi entropy of a quantum state was improved to $\tilde{O}(r^{\frac{1}{\alpha}}/\varepsilon^{\frac{1}{\alpha}+1})$ for $0 < \alpha < 1$ and $\tilde{O}(r/\varepsilon^{1+\frac{1}{\alpha}})$ for $\alpha > 1$ in [94]. In the "quantum sample access" model, the time complexity for computing the α-Rényi entropy was improved to $\tilde{O}(N^{\frac{4}{\alpha}-2})$ for $0 < \alpha < 1$ and $\tilde{O}(N^{4-\frac{2}{\alpha}})$ for $\alpha > 1$ in [93], compared to the $\tilde{O}(N^{\frac{6}{\alpha}})$ for $0 < \alpha < 1$ and $\tilde{O}(N^6)$ for $\alpha > 1$ in [6], at the cost of larger sample complexity; they also showed sample lower bounds $\Omega(\max\{N, N^{\frac{1}{\alpha}-1}\})$ for computing the α-Rényi entropy. In addition, variational quantum algorithms for computing the von Neumann and Rényi entropies were proposed in [95].
- **Trace distance**. In the "purified quantum query access" model, the query complexity for computing the trace distance was improved to $\tilde{O}(r/\varepsilon^2)$ in [96], and they showed that low-rank trace distance estimation is BQP-complete based on the result of [97], improving the DQC1-hardness given in this paper. The space-bounded version of trace distance estimation was shown to be BQL-complete in [92], and its certification was shown to be coRQ$_{\mathrm{U}}$L-complete. In the "quantum sample access" model, the sample complexity for computing the fidelity was shown to be $\tilde{O}(r^2/\varepsilon^5)$ in [96], which was later employed in a hypothesis testing based auditing pipeline for quantum differential privacy with domain knowledge [98].
- **Fidelity**. In the "purified quantum query access" model, the query complexity for computing the fidelity was improved to $\tilde{O}(r^{2.5}/\varepsilon^5)$ in [39]. When quantum states are well-conditioned (i.e., $\rho, \sigma \geq I/\kappa$ for some known $\kappa > 0$), the query complexity was shown to be $\tilde{O}(\kappa^4/\varepsilon)$ in [99], with the dependence on ε optimal (up to polylogarithmic factors). It was shown in [97] that pure-state fidelity estimation is BQP-complete, which, together with the polynomial-time quantum algorithms for low-rank fidelity estimation in [11] and [39] and this paper, implies that low-rank fidelity estimation is also BQP-complete, improving the DQC1-hardness given in this paper. In the "quantum sample access" model, the sample complexity for computing the fidelity was shown to be $\tilde{O}(r^{5.5}/\varepsilon^{12})$ in [39].

F. Organization of This Paper

Section II introduces the idea that regards quantum states as block-encodings, and provides a series of basic techniques for manipulating them. Section III presents quantum algorithms that compute quantum entropies, including the von Neumann entropy, quantum Rényi entropy and quantum Tsallis entropy. Section IV presents quantum algorithms that compute the trace distance, fidelity and their extensions.

II. Quantum States as Block-Encodings

Since the introduction of qubitization in Hamiltonian simulation [31], block-encodings have been widely used as a basic notion in quantum algorithms, e.g., [22] and [33]. In the existing research, block-encodings are unitary operators that block-encode smaller ones.

Quantum states (i.e., density operators) are often used to contain necessary information in quantum algorithms. For this purpose, a technique was provided in [31] to implement a unitary operator that block-encodes a mixed quantum state. However, to the best of our knowledge, there is no known method to do the inverse, that is, to prepare a mixed quantum state using queries to the given unitary operator (quantum oracle) that block-encodes its density operator. As a result, it could be difficult to extract information from operators that are block-encoded in unitary operators. This motivate us to regard quantum states as block-encodings. As will be seen later in this section, it is convenient to extract information from the operators block-encoded in quantum states as well as to manipulate them.

In this section, we will extend the definition of block-encoding proposed for unitary operators as in [22], [31], and [33] to that for general operators, especially for density operators (i.e., quantum states). Then we show the possibility that information can be stored in and extracted from quantum states as block-encodings. Also, we can manipulate the information block-encoded in quantum states. Here, the “information” block-encoded in quantum states (i.e., density operators) is essentially subnormalized density operators.

A. Subnormalized Density Operators

We will use the language of the conventional block-encoding. Here, we give the definition of block-encoding for ordinary quantum operators as follows.

Definition II.1 (Block-Encoding): Suppose A is an n-qubit operator, $\alpha, \varepsilon \geq 0$ and $a \in \mathbb{N}$. An $(n+a)$-qubit operator B is said to be an (α, a, ε)-block-encoding of A, if

$$\left\| \alpha\, {}_a\langle 0| B |0\rangle_a - A \right\| \leq \varepsilon.$$

Intuitively, A is represented by the matrix in the upper left corner of B, i.e.

$$B \approx \begin{bmatrix} A/\alpha & * \\ * & * \end{bmatrix}.$$

Here, we write $|0\rangle_a$ to denote $|0\rangle^{\otimes a}$, where the subscript a indicates which (and how many) qubits are involved in the Dirac symbol. For example, if a system consists of two subsystems of a qubits and b qubits and it is in state $|0\rangle^{\otimes(a+b)}$, we can represent it as $|0\rangle_{a+b}$ or $|0\rangle_a |0\rangle_b$.

We are interested in matrices block-encoded in a mixed quantum state (density operator), which are indeed subnormalized density operators.

Definition II.2 (Subnormalized Density Operator): A subnormalized density operator A is a semidefinite operator with $\operatorname{tr}(A) \leq 1$. A (normalized) density operator is a subnormalized density operator with trace 1. An $(n+a+b)$-qubit unitary operator U is said to prepare an n-qubit subnormalized density operator A, if it prepares the purification $|\rho\rangle = U|0\rangle_{n+a+b}$ of a density operator $\rho = \operatorname{tr}_b(|\rho\rangle\langle\rho|)$, which is a $(1, a, 0)$-block-encoding of A.

Given a subnormalized density operator A prepared by a unitary operator U, we usually need to construct another unitary operator $\tilde{U}$ which is a block-encoding of A. This technique was first introduced by [31], then generalized for subnormalized density operators by [22] and [32].

Lemma II.1 (Block-Encoding of Subnormalized Density Operators [22], [31], [32]): Suppose U is an $(n+a)$-qubit unitary operator that prepares an n-qubit subnormalized density operator A. Then there is a $(2n+a)$-qubit unitary operator $\tilde{U}$ which is a $(1, n+a, 0)$-block-encoding of A, using 1 query to U and $U^\dagger$ and $O(a)$ elementary quantum gates.

B. Generalized Evolution

It is well known that after applying a unitary operator U on a mixed quantum state ρ, it will become another state $U\rho U^\dagger$. Here, we extend the basic unitary evolution to the case of subnormalized density operators, which transforms a subnormalized density operator A to $BAB^\dagger$, where B is block-encoded in a unitary operator.

Lemma II.2 (Evolution of Subnormalized Density Operators): Suppose that

1) U is an $(n+a)$-qubit unitary operator that prepares an n-qubit subnormalized density operator A, and
2) V is an $(n+b)$-qubit unitary operator which is a $(1, b, 0)$-block-encoding of B.

Then, $\tilde{U} = (V \otimes I_a)(U \otimes I_b)$ is an $(n+a+b)$-qubit unitary operator that prepares an n-qubit subnormalized density operator $BAB^\dagger$.

Proof: Let $a = a_1 + a_2$ such that U prepares an $(n+a_1)$-qubit density operator ρ, which is a $(1, a_1, 0)$-block-encoding of A. Suppose

$$A = \sum_j \lambda_j |u_j\rangle \langle u_j|.$$

Then we have

$$|\rho\rangle_{n+a_1+a_2} = \sum_j \sqrt{\lambda_j} |u_j\rangle_n |0\rangle_{a_1} |\psi_j\rangle_{a_2} + |\perp_{a_1}\rangle_{n+a_1+a_2},$$

where $|\psi_j\rangle$ is an orthogonal basis, and

$$\left\| {}_{a_1}\langle 0|\perp_{a_1}\rangle_{n+a_1+a_2} \right\| = 0.$$

Note that

$$\begin{aligned} |\tilde{\rho}\rangle := \tilde{U}|0\rangle_{n+a+b} &= (V \otimes I_a)|\rho\rangle_{n+a_1+a_2}|0\rangle_b \\ &= \sum_j \sqrt{\lambda_j} |0\rangle_{a_1} |\psi_j\rangle_{a_2} \left(V|u_j\rangle_n |0\rangle_b\right) \\ &\quad + V|\perp_{a_1}\rangle_{n+a_1+a_2}|0\rangle_b. \end{aligned}$$

Let $\tilde{\rho} = \operatorname{tr}_{a_2}(|\tilde{\rho}\rangle\langle\tilde{\rho}|)$, then

$${}_{a_1+b}\langle 0|\tilde{\rho}|0\rangle_{a_1+b} = \operatorname{tr}_{a_2}\left({}_{a_1+b}\langle 0|\tilde{\rho}\rangle\langle\tilde{\rho}|0\rangle_{a_1+b}\right),$$

where

$$\begin{aligned} {}_{a_1+b}\langle 0|\tilde{\rho}\rangle &= \sum_j \sqrt{\lambda_j} |\psi_j\rangle_{a_2} \otimes \left({}_b\langle 0|V|0\rangle_b\right)|u_j\rangle_n \\ &= \sum_j \sqrt{\lambda_j} |\psi_j\rangle_{a_2} \otimes B|u_j\rangle_n. \end{aligned}$$

We have that

$${}_{a_1+b}\langle 0|\tilde{\rho}|0\rangle_{a_1+b} = \sum_j \lambda_j B|u_j\rangle_n \langle u_j| B^\dagger = BAB^\dagger.$$

□

C. Polynomial Eigenvalue Transformation

Now we show how a subnormalized density operator A can be transformed to a new subnormalized density operator $A(P(A))^2$, where $P(x)$ is a polynomial. To this end, we recall the polynomial eigenvalue transformation of unitary operators in [22], and extend it to the case of preparing subnormalized density operators.

Theorem II.3 (Polynomial Eigenvalue Transformation of Unitary Operators [22]): Suppose that

1) U is an $(n+a)$-qubit unitary operator, which is a $(1, a, 0)$-block-encoding of an Hermitian operator A.
2) $P \in \mathbb{R}[x]$ [5] is a degree-d polynomial such that $\|P\|_{[-1,1]} \leq \frac{1}{2}$.[6] Moreover, if P is even or odd, the condition can be relaxed to $\|P\|_{[-1,1]} \leq 1$.

Then for every $\delta > 0$, there is a quantum circuit[7] $\tilde{U}$ such that

1) $\tilde{U}$ is a $(1, a+2, \delta)$-block-encoding of $P(A)$.
2) $\tilde{U}$ uses d queries to U and $U^\dagger$, 1 query to controlled-U and $O((a+1)d)$ elementary quantum gates.
3) A description of $\tilde{U}$ can be computed by a (classical) Turing machine in $O(\mathrm{poly}(d, \log(1/\delta)))$ time.

In the following, combining Theorem II.3 and Lemma II.2, we develop a technique of polynomial eigenvalue transformation of subnormalized density operators.

Theorem II.4 (Polynomial Eigenvalue Transformation of Subnormalized Density Operators): Suppose that

1) U is an $(n+a)$-qubit unitary operator that prepares an n-qubit subnormalized density operator A.
2) $P \in \mathbb{R}[x]$ is a degree-d polynomial such that $\|P\|_{[-1,1]} \leq \frac{1}{2}$. Moreover, if P is even or odd, the condition can be relaxed to $\|P\|_{[-1,1]} \leq 1$.

Then for every $\delta \in (0,1)$, there is a quantum circuit $\tilde{U}$ such that

1) $\tilde{U}$ prepares an n-qubit subnormalized density operator B, and B is a $(1, 0, \delta)$-block-encoding of $A(P(A))^2$.
2) $\tilde{U}$ uses $O(d)$ queries to U and $U^\dagger$, 1 query to controlled-U and controlled-$U^\dagger$, and $O((n+a)d)$ elementary quantum gates.
3) A description of $\tilde{U}$ can be computed by a (classical) Turing machine in $O(\mathrm{poly}(d, \log(1/\delta)))$ time.

Proof: By Lemma II.1, there is a quantum circuit V that is a $(1, O(n+a), 0)$-block-encoding of A, which consists of 1 query to U and $U^\dagger$ and $O(n+a)$ elementary quantum gates. Then by Theorem II.3, there is a quantum circuit $\tilde{V}$, which is a $(1, b, \delta)$-block-encoding of $P(A)$, with d queries to V and $V^\dagger$, 1 query to controlled-V, and $O((n+a)d)$ elementary quantum gates, where $b = O(n+a)$.

We claim that $\tilde{U} = (\tilde{V} \otimes I_a)(U \otimes I_b)$ is desired. To see this, by Lemma II.2, $\tilde{U}$ prepares an n-qubit subnormalized density operator $\left({}_b\langle 0|\tilde{V}|0\rangle_b\right) A \left({}_b\langle 0|\tilde{V}|0\rangle_b\right)^\dagger$. On the other hand,

$$\begin{aligned}&\left\|\left({}_b\langle 0|\tilde{V}|0\rangle_b\right) A \left({}_b\langle 0|\tilde{V}|0\rangle_b\right)^\dagger - A(P(A))^2\right\| \\ &\leq \left\|\left({}_b\langle 0|\tilde{V}|0\rangle_b - P(A)\right) A \left({}_b\langle 0|\tilde{V}|0\rangle_b\right)^\dagger\right\| + \\ &\quad \left\|P(A)A\left(\left({}_b\langle 0|\tilde{V}|0\rangle_b\right)^\dagger - P(A)\right)\right\| \\ &\leq \delta\|A\|\left(\|P(A)\| + \delta\right) + \|P(A)\|\,\|A\|\,\delta \\ &\leq \frac{5}{2}\delta = \Theta(\delta).\end{aligned}$$

We conclude that $\tilde{U}$ prepares the purification $|\tilde{\rho}\rangle$ of $\tilde{\rho}$, which is a $(1, O(n+a), \Theta(\delta))$-block-encoding of $A(P(A))^2$, which yields the proof. □

By Theorem II.4, we are able to transform a subnormalized density operator A to $A(f(A))^2$ for a large range of $f(x)$, provided $f(x)$ can be efficiently approximated by a polynomial.

Theorem II.5 (Eigenvalue Transformation of Subnormalized Density Operators): Suppose that

1) U is an $(n+a)$-qubit unitary operator that prepares an n-qubit subnormalized density operator A.
2) $f : [-1,1] \to \mathbb{R}$ can be approximated by a degree-d polynomial $P \in \mathbb{R}[x]$ such that there are two parameters $\delta, \varepsilon \in (0, \frac{1}{2}]$, it holds that $\|P(x) - f(x)\|_{[\delta,1]} \leq \varepsilon$ and $\|P\|_{[-1,1]} \leq \frac{1}{2}$. Moreover, if P is even or odd, the latter condition can be relaxed to $\|P\|_{[-1,1]} \leq 1$.

Then there is a quantum circuit $\tilde{U}$ such that

1) $\tilde{U}$ prepares an n-qubit subnormalized density operator B, and B is a $\left(1, 0, \Theta\left(\varepsilon + \delta + \left\|x(f(x))^2\right\|_{[0,\delta]}\right)\right)$-block-encoding of $A(f(A))^2$.
2) $\tilde{U}$ uses $O(d)$ queries to U and $U^\dagger$, 1 query to controlled-U and controlled-$U^\dagger$, and $O((n+a)d)$ elementary quantum gates.
3) A description of $\tilde{U}$ can be computed by a (classical) Turing machine in $O(\mathrm{poly}(d, \log(1/\delta)))$ time.

Proof: Let $\tilde{U}$ be the quantum circuit obtained by Theorem II.4, which prepares an n-qubit subnormalized density operator B as a $(1, 0, \delta)$-block-encoding of $A(P(A))^2$. We analyze the error by the fact that

$$\left\|x(P(x))^2 - x(f(x))^2\right\|_{[0,1]} \leq \Theta\left(\varepsilon + \delta + \left\|x(f(x))^2\right\|_{[0,\delta]}\right).$$

We consider two cases.

Case 1: $x \in [\delta, 1]$.

$$\begin{aligned}\left|x(P(x))^2 - x(f(x))^2\right| &\leq |x|\,|P(x) + f(x)|\,|P(x) - f(x)| \\ &\leq (1+\varepsilon)\varepsilon \leq 2\varepsilon = \Theta(\varepsilon).\end{aligned}$$

Case 2: $x \in [0, \delta)$.

$$\begin{aligned}\left|x(P(x))^2 - x(f(x))^2\right| &\leq \left|x(P(x))^2\right| + \left|x(f(x))^2\right| \\ &\leq \delta + \left\|x(f(x))^2\right\|_{[0,\delta]}.\end{aligned}$$

Then we have

$$\begin{aligned}\left\|B - A(f(A))^2\right\| &\leq \left\|B - A(P(A))^2\right\| \\ &\quad + \left\|A(P(A))^2 - A(f(A))^2\right\| \\ &\leq \delta + \Theta\left(\varepsilon + \delta + \left\|x(f(x))^2\right\|_{[0,\delta]}\right) \\ &= \Theta\left(\varepsilon + \delta + \left\|x(f(x))^2\right\|_{[0,\delta]}\right).\end{aligned}$$

□

As will be seen, Theorem II.5 can be used to develop a technique of preparing positive powers of Hermitian operators (see Section II-D).

[5] Let $\tilde{\mathbb{R}} \subseteq \mathbb{R}$ be the set of polynomial-time computable real numbers. That is, for every real number $x \in \tilde{\mathbb{R}}$, there is a polynomial-time (classical) Turing machine M such that $|M(1^n) - x| < 2^{-n}$, where $M(1^n)$ denotes the output floating point real number of M on input 1^n. Throughout this paper, we only consider polynomial-time computable real numbers, and for any $S \subseteq \mathbb{R}$, we write S to denote $S \cap \tilde{\mathbb{R}}$ for convenience. Especially, we just write $\mathbb{R}$ for $\tilde{\mathbb{R}}$.

[6] For a function $f : \mathbb{R} \to \mathbb{C}$ and a set $I \subseteq \mathbb{R}$, we define $\|f\|_I = \sup\{|f(x)| | x \in I\}$.

[7] Throughout this paper, without explicit explanation, quantum circuits are uniform. Here, a uniform quantum circuit is a family of quantum circuits whose descriptions can be computed by a polynomial-time (classical) Turing machine.

D. Positive Powers

We will use Theorem II.5 to develop an efficient approach for implementing positive powers of Hermitian matrix A, which removes the dependence on κ that $I/\kappa \leq A \leq I$ as in [33] (see Lemma II.13 of its full version). In this subsection, we will provide the positive power tricks for an Hermitian operator block-encoded in a density operator (Lemma II.8) and in a unitary operator (Lemma II.13). To this end, we recall some results of polynomial approximations of power functions.

Lemma II.6 (Polynomial Approximation of Positive Power Functions [33], [100]): Let $\delta, \varepsilon \in (0, \frac{1}{2}]$, $c \in (0,1)$ and $f(x) = \frac{1}{2}x^c$. Then there is an even/odd degree-$O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$ polynomial[8] $P \in \mathbb{R}[x]$ such that $\|P(x) - f(x)\|_{[\delta,1]} \leq \varepsilon$ and $\|P\|_{[-1,1]} \leq 1$.

Lemma II.7 (Polynomial Approximation of Negative Power Functions [22], [33], [100]): Let $\delta, \varepsilon \in (0, \frac{1}{2}]$, $c > 0$ and $f(x) = \frac{\delta^c}{2} x^{-c}$. Then there is an even/odd degree-$O\left(\frac{c+1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$ polynomial $P \in \mathbb{R}[x]$ such that $\|P(x) - f(x)\|_{[\delta,1]} \leq \varepsilon$ and $\|P\|_{[-1,1]} \leq 1$.

First, we develop a method of implementing positive powers of Hermitian matrix A, which is given as block-encoded in a density operator ρ. Here, the purification of ρ can be prepared by a unitary operator U.

Lemma II.8 (Positive Powers Block-Encoded in Density Operators): Suppose that

1) U is an $(n+a)$-qubit unitary operator that prepares an n-qubit subnormalized density operator A.
2) $\delta, \varepsilon \in \left(0, \frac{1}{2}\right]$ and $c \in (0,1)$.

Then there is a quantum circuit $\tilde{U}$ such that

1) $\tilde{U}$ prepares an n-qubit subnormalized density operator B, and B is a $(4\delta^{c-1}, 0, \Theta(\delta^c + \varepsilon\delta^{c-1}))$-block-encoding of A^c.
2) $\tilde{U}$ uses $O(d)$ queries to U and $U^\dagger$, 1 query to controlled-U and controlled-$U^\dagger$, and $O((n+a)d)$ elementary quantum gates, where $d = O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$.
3) A description of $\tilde{U}$ can be computed by a (classical) Turing machine in $O(\operatorname{poly}(d))$ time.

Proof: Let $f(x) = \frac{\delta^c}{2}x^{-c}$, where $c \in \left(0, \frac{1}{2}\right)$. Then $x(f(x))^2 = \frac{\delta^{2c}}{4}x^{1-2c}$, and $\left\|x(f(x))^2\right\|_{[0,\delta]} \leq \frac{\delta}{4} = \Theta(\delta)$. By Lemma II.7, we can obtain an even/odd polynomial $P(x)$ of degree $O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$ such that $\|P - f\|_{[\delta,1]} \leq \varepsilon$ and $\|P\|_{[-1,1]} \leq 1$. By Theorem II.5, there is a quantum circuit $\tilde{U}$, which prepares an n-qubit subnormalized density operator B, which is a $(1, 0, \Theta(\delta+\varepsilon))$-block-encoding of $A\left(f(A)\right)^2 = \frac{\delta^{2c}}{4}A^{1-2c}$. In other words, B is a $(4\delta^{-2c}, 0, \Theta(\delta^{1-2c} + \varepsilon\delta^{-2c}))$-block-encoding of A^{1-2c}. These yield the proof by letting $c' = 1 - 2c$. □

Remark II.1: In Lemma II.8, we provide a positive power trick for density operators, whose error depends on two parameters δ and ε. This allows us to prepare positive powers of density operators flexibly, without dealing with their "condition numbers" κ such that $\Pi/\kappa \leq \rho$ for some projector Π. The method used in Lemma II.8 is a straightforward application of Theorem II.5 with the observation that $x(f(x))^2 \to 0$ when $x \to 0$. In fact, any function $f(x)$ that satisfies this condition (and, of course, other conditions required in Theorem II.5) is applicable in this trick, without dealing with κ. As will be seen, this technique for positive powers of subnormalized density operators will be frequently used in our quantum algorithms (see Section III and Section IV), in order to avoid the κ restrictions on density operators.

Next, inspired by the above observation, we extend the result to the case that A is given as block-encoded in a unitary operator. Here, we need to implement a threshold projector. The following lemma is Corollary III.3 of [22].

Lemma II.9 (Polynomial Approximation of Threshold Projectors [22]): Let $\delta, \varepsilon \in (0, \frac{1}{2})$ and $t \in [0,1]$ such that $0 < t-\delta < t+\delta < 1$. There is an even polynomial $P \in \mathbb{R}[x]$ of degree $O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$ such that

1) $\|P\|_{[-1,1]} \leq 1$,
2) $P(x) \in [1-\varepsilon, 1]$ for $x \in [-t+\delta, t-\delta]$, and
3) $P(x) \in [0, \varepsilon]$ for $x \in [-1, -t-\delta] \cup [t+\delta, 1]$.

We take some special cases of Lemma II.9 as follows, which will be often used to design our quantum algorithms.

Corollary II.10: Let $\delta, \varepsilon \in (0, \frac{1}{4}]$. Then there is an even degree-$O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$ polynomial $R \in \mathbb{R}[x]$ such that $\|R\|_{[-1,1]} \leq 1$ and

$$R(x) \in \begin{cases} [1-\varepsilon, 1] & x \in [-1, -2\delta] \cup [2\delta, 1] \\ [0, \varepsilon] & x \in [-\delta, \delta] \end{cases}.$$

Corollary II.11: Let $\delta, \varepsilon \in (0, \frac{1}{4}]$. Then there is an even degree-$O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$ polynomial $R \in \mathbb{R}[x]$ such that $\|R\|_{[-1,1]} \leq 1$ and

$$R(x) \in \begin{cases} [1-\varepsilon, 1] & x \in [-1+2\delta, 1-2\delta] \\ [0, \varepsilon] & x \in [-1, -1+\delta] \cup [1-\delta, 1] \end{cases}.$$

We also need the following lemma to multiply block-encoded matrices.

Lemma II.12 (Product of Block-Encoded Matrices [22]): Suppose that

1) U is an $(n+a)$-qubit unitary operator that is a (α, a, δ)-block-encoding of an n-qubit operator A.
2) V is an $(n+b)$-qubit unitary operator that is a (β, b, ε)-block-encoding of an n-qubit operator B.

Then there is a quantum circuit $\tilde{U}$ such that

1) $\tilde{U}$ is an $(\alpha\beta, a+b, \alpha\varepsilon + \beta\delta)$-block-encoding of AB.
2) $\tilde{U}$ uses 1 query to each of U and V.

With the approximation of threshold functions, we are able to implement positive powers of Hermitian matrix A, which is given as block-encoded in a unitary operator.

Lemma II.13 (Positive Powers Block-Encoded in Unitary Operators): Suppose that

1) U is an $(n+a)$-qubit unitary operator which is a $(1, a, 0)$-block-encoding of an n-qubit Hermitian operator A.

[8] In this paper, a degree-d polynomial means a uniform family of (polynomial-time computable) polynomials with parameter d. That is, suppose $P_d(x) = \sum_{k=0}^{d} a_k x^k$, where a_k is a polynomial-time computable real number for $0 \leq k \leq d$, then there is a polynomial-time classical Turing machine that, on input 1^d, outputs descriptions M_k of a_k for $0 \leq k \leq d$, where M_k is a polynomial-time classical Turing machine that, on input 1^n, output a_k within additive error 2^{-n}.

2) $\delta, \varepsilon \in \left(0, \frac{1}{4}\right]$ and $c \in (0, 1)$.

Then there is a quantum circuit W such that

1) W is a $(2, O(a+1), \Theta(\varepsilon+\delta^c))$-block-encoding of $|A|^c$.
2) W uses $O(Q)$ queries to U and $U^\dagger$, $O(1)$ query to controlled-U and $O((a+1)Q)$ elementary quantum gates, where $Q = O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$.
3) A description of W can be computed by a (classical) Turing machine in $\operatorname{poly}(Q)$ time.

Proof: Let $f(x) = \frac{1}{2}|x|^c$ be an even function and $\delta, \varepsilon \in (0, \frac{1}{4}]$. By Lemma II.6, there is an even degree-d_P polynomial $P \in \mathbb{R}[x]$, where $d_P = O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$, such that $\|P(x) - f(x)\|_{[\delta,1]} \leq \varepsilon$, $\|P(x) - f(x)\|_{[-1,-\delta]} \leq \varepsilon$ and $\|P\|_{[-1,1]} \leq 1$. By Theorem II.3, for $\delta_U > 0$, there is a quantum circuit $\tilde{U}$ such that

1) $\tilde{U}$ is a $(1, a+2, 0)$-block-encoding of B, and B is a $(1, 0, \delta_U)$-block-encoding of $P(A)$.
2) $\tilde{U}$ uses d_P queries to U and $U^\dagger$, 1 query to controlled-U and $O((a+1)d_P)$ elementary quantum gates.
3) A description of $\tilde{U}$ can be computed by a (classical) Turing machine in $\operatorname{poly}(d_P, \log(1/\delta_U))$ time.

Let $R \in \mathbb{R}[x]$ be the even degree-d_R polynomial in Corollary II.10, where $d_R = O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$, such that $\|R\|_{[-1,1]} \leq 1$ and

$$R(x) \in \begin{cases} [1-\varepsilon, 1] & x \in [-1, -2\delta] \cup [2\delta, 1] \\ [0, \varepsilon] & x \in [-\delta, \delta] \end{cases}.$$

By Theorem II.3, for $\delta_V > 0$, there is a quantum circuit $\tilde{V}$ such that

1) $\tilde{V}$ is a $(1, a+2, 0)$-block-encoding of C, and C is a $(1, 0, \delta_V)$-block-encoding of $R(A)$.
2) $\tilde{V}$ uses d_R queries to U and $U^\dagger$, 1 query to controlled-U and $O((a+1)d_R)$ elementary quantum gates.
3) A description of $\tilde{V}$ can be computed by a (classical) Turing machine in $\operatorname{poly}(d_R, \log(1/\delta_V))$ time.

By Lemma II.12, using one query to each of $\tilde{U}$ and $\tilde{V}$, we can obtain a quantum circuit W, which is a $(1, 2a+4, 0)$-block-encoding of BC. In the following, we will show that $\|BC - f(A)\| \leq \Theta(\varepsilon + \delta^c)$. We note that

$$\|P(x)R(x) - f(x)\|_{[0,1]} \leq \Theta(\varepsilon + \delta^c).$$

This is seen by the following three cases:

1) $|x| > 2\delta$. We have $|P(x)R(x) - f(x)| \leq |(P(x) - f(x))R(x)| + |f(x)(R(x) - 1)| \leq \Theta(\varepsilon)$.
2) $|x| < \delta$. We have $|P(x)R(x) - f(x)| \leq |P(x)|\,|R(x)| + |f(x)| \leq \Theta(\varepsilon + \delta^c)$.
3) $\delta \leq |x| \leq 2\delta$. We have $|P(x)R(x) - f(x)| \leq |(P(x) - f(x))R(x)| + |f(x)|\,|R(x) - 1| \leq \Theta(\varepsilon + \delta^c)$.

Note that A is Hermitian, we have $\|P(A)R(A) - f(A)\| \leq \Theta(\varepsilon + \delta^c)$. Finally,

$$\begin{aligned}\|BC - f(A)\| &\leq \|BC - P(A)R(A)\| \\ &\quad + \|P(A)R(A) - f(A)\| \\ &\leq \Theta(\delta_U + \delta_V + \varepsilon + \delta^c).\end{aligned}$$

These conclude that W is a $(1, 2a+4, \Theta(\varepsilon + \delta^c))$-block-encoding of $f(A)$ by setting $\delta_U = \delta_V = \varepsilon$, and therefore a $(2, O(n+a), \Theta(\varepsilon + \delta^c))$-block-encoding of $|A|^c$. □

By setting $\kappa = 1/\delta$, Lemma II.13 reproduces the result of [33] (see Lemma II.13 of its full version). The strength of Lemma II.13 is to allow implement positive powers of A, regardless of whether the condition $I/\kappa \leq A \leq I$ holds. The technique used in Lemma II.13 by multiplying the polynomial approximation with a threshold function is similar to Corollary 42 of the full version of [22] for implementing the threshold pseudoinverse.

E. Trace Estimation

In this subsection, we will provide a method of estimating the trace of an Hermitian matrix which is block-encoded in a density operator. Before that, we recall the quantum amplitude estimation [64].

Theorem II.14 (Quantum Amplitude Estimation, [64]): Suppose U is an $(a+b)$-qubit unitary operator such that

$$U|0\rangle_{a+b} = \sqrt{p}\,|0\rangle_a |\phi_0\rangle_b + \sqrt{1-p}\,|1\rangle_a |\phi_1\rangle_b,$$

where $|\phi_0\rangle$ and $|\phi_1\rangle$ are normalized (pure) quantum states and $p \in [0, 1]$. There is a quantum algorithm that outputs $\tilde{p} \in [0, 1]$ such that

$$|\tilde{p} - p| \leq \frac{2\pi\sqrt{p(1-p)}}{M} + \frac{\pi^2}{M^2}$$

with probability $\geq \frac{8}{\pi^2}$, using $O(M)$ queries to U and $U^\dagger$.

If we know an upper bound B of p, then we can take $M = \left\lceil 2\pi\left(\frac{2\sqrt{B}}{\varepsilon} + \frac{1}{\sqrt{\varepsilon}}\right)\right\rceil = \Theta\left(\frac{\sqrt{B}}{\varepsilon} + \frac{1}{\sqrt{\varepsilon}}\right)$ to guarantee that $|\tilde{p} - p| \leq \varepsilon$.

Based on quantum amplitude estimation, we develop the trace estimation of subnormalized density operators as shown below, which will be useful to design quantum algorithms, see Section III and Section IV.

Lemma II.15 (Trace Estimation of Subnormalized Density Operators): Suppose U is an $(n+a)$-qubit unitary operator that prepares an n-qubit subnormalized density operator A, and $B > 0$ is a known constant that $\operatorname{tr}(A) \leq B$. For every $\varepsilon > 0$, there is a quantum algorithm that estimates $\operatorname{tr}(A)$ within additive error ε with $O\left(\frac{\sqrt{B}}{\varepsilon} + \frac{1}{\sqrt{\varepsilon}}\right)$ queries to U and $U^\dagger$.

Proof: Let $a = a_1 + a_2$ such that U prepares an $(n+a_1)$-qubit density operator ρ, which is a $(1, a_1, 0)$-block-encoding of A. Suppose

$$A = \sum_j \lambda_j |u_j\rangle\langle u_j|.$$

Then we have

$$\begin{aligned}U|0\rangle_{n+a_1+a_2} &= |\rho\rangle_{n+a_1+a_2} \\ &= \sum_j \sqrt{\lambda_j}\,|u_j\rangle_n |0\rangle_{a_1} |\psi_j\rangle_{a_2} + |\perp_{a_1}\rangle_{n+a_1+a_2},\end{aligned}$$

where $|\psi_j\rangle$ is an orthogonal basis, and

$$\left\| {}_{a_1}\langle 0|\perp_{a_1}\rangle_{n+a_1+a_2} \right\| = 0.$$

Moreover, we have

$$U|0\rangle_{n+a_1+a_2} = \sqrt{p}\,|0\rangle_{a_1} |\phi_0\rangle_{n+a_2} + \sqrt{1-p}\,|1\rangle_{a_1} |\phi_1\rangle_{n+a_2}$$

for some (pure) quantum states $|\phi_0\rangle$ and $|\phi_1\rangle$, where $p = \operatorname{tr}(A)$.

If we know an upper bound B of $\operatorname{tr}(A)$, then let $M = \left\lceil 2\pi\left(\frac{2\sqrt{B}}{\varepsilon}+\frac{1}{\sqrt{\varepsilon}}\right)\right\rceil = \Theta\left(\frac{\sqrt{B}}{\varepsilon}+\frac{1}{\sqrt{\varepsilon}}\right)$, and by Theorem II.14, we can computes $\tilde{p}$ such that

$$|\tilde{p}-p| \leq \frac{2\pi\sqrt{p(1-p)}}{M}+\frac{\pi^2}{M^2} \leq \varepsilon$$

with success probability $\geq \frac{8}{\pi^2}$, using M queries to U and $U^\dagger$. □

F. Linear Combinations

We will provide a technique (Lemma II.17) that prepares a linear combination of subnormalized density operators, which is a natural analog of Linear-Combination-of-Unitaries (LCU) algorithm through a series of work [22], [65], [66], [67], [68], [69], [70].

Before stating our linear combination result of subnormalized density operators, we introduce a technique that embeds a density operator in a larger space.

Lemma II.16: Suppose U is an $(n+a)$-qubit unitary operator that prepares an n-qubit density operator ρ. For every $b \geq 0$, there is an $(n+a+b)$-qubit unitary operator $U^{(b)} = U \otimes I_b$ such that

1) $U^{(b)}$ prepares an $(n+b)$-qubit density operator $\rho^{(b)}$, and $\rho^{(b)}$ is a $(1, b, 0)$-block-encoding of ρ.
2) $U^{(b)}$ uses 1 query to U.

Proof: Let $|\psi\rangle_{n+a} = U|0\rangle_{n+a}$ and then $\rho_n = \operatorname{tr}_a(|\psi\rangle_{n+a}\langle\psi|)$. Let $U^{(b)} = U \otimes I_b$ and $\left|\psi^{(b)}\right\rangle_{n+a+b} = U^{(b)}|0\rangle_{n+a+b} = |\psi\rangle_{n+a}|0\rangle_b$. We have

$$\begin{aligned}\rho^{(b)} &= \operatorname{tr}_a\left(\left|\psi^{(b)}\right\rangle_{n+a+b}\left\langle\psi^{(b)}\right|\right)\\ &= \operatorname{tr}_a\left(|\psi\rangle_{n+a}\langle\psi| \otimes |0\rangle_b\langle 0|\right)\\ &= \rho_n \otimes |0\rangle_b\langle 0|.\end{aligned}$$

The proof is completed by noting that ${}_b\langle 0|\rho^{(b)}|0\rangle_b = \rho_n$. □

Now we are ready to show the technique to prepare a linear combination of subnormalized density operators. The basic idea is to prepare a linear combination of (normalized) density operators, but a careful qubit alignment is needed with the help of Lemma II.16.

Lemma II.17 (Linear Combination of Subnormalized Density Operators): Suppose

1) V is an m-qubit unitary operator such that $V|0\rangle = \sum_{k\in[2^m]}\sqrt{\alpha_k}|k\rangle$.[9]
2) For every $k \in [2^m]$, U_k is an $(n+a_k+b_k)$-qubit unitary operator that prepares an $(n+a_k)$-qubit density operator ρ_k, and ρ_k is a $(1, a_k, 0)$-block-encoding of an n-qubit subnormalized density operator A_k.

Let $a = \max_{k\in[2^m]}\{a_k\}$ and $b = \max_{k\in[2^m]}\{b_k\}$. Then there is an $(m+n+a+b)$-qubit unitary operator U such that

1) $U(V \otimes I_{n+a+b})$ prepares an n-qubit subnormalized density operator
$$A = \sum_{k\in[2^m]}\alpha_k A_k.$$
2) U uses 1 query to each U_k for $k \in [2^m]$.

Proof: Let $a'_k = a - a_k$, $b'_k = b - b_k$, and

$$U = \sum_{k\in[2^m]}|k\rangle\langle k| \otimes U_k^{(a'_k+b'_k)}$$

be an $(m+n+a+b)$-qubit unitary operator, where $U^{(b)} = U \otimes I_b$ is defined as in Lemma II.16. Here, $U_k^{(a'_k+b'_k)}$ acts on $n+a+b$ qubits. To be precise, if we split the $n+a+b$ qubits into three parts: (i) n qubits, (ii) a qubits and (iii) b qubits, then $U_k^{(a'_k+b'_k)}$ uses 1 query to U_k which acts on: (i) the whole n qubits, (ii) the first a_k qubits and (iii) the first b_k qubits.

Let $|\psi_k\rangle_{n+a_k+b_k} = U_k|0\rangle_{n+a_k+b_k}$. Then we note that

$$\begin{aligned}|\psi\rangle &= U(V \otimes I_{n+a+b})|0\rangle_m|0\rangle_n|0\rangle_a|0\rangle_b\\ &= U\sum_{k\in[2^m]}\sqrt{\alpha_k}|k\rangle_m|0\rangle_n|0\rangle_a|0\rangle_b\\ &= \sum_{k\in[2^m]}\sqrt{\alpha_k}|k\rangle_m\left(U_k^{(a'_k+b'_k)}|0\rangle_n|0\rangle_a|0\rangle_b\right)\\ &= \sum_{k\in[2^m]}\sqrt{\alpha_k}|k\rangle_m|\psi_k\rangle_{n+a_k+b_k}|0\rangle_{a'_k}|0\rangle_{b'_k},\end{aligned}$$

and

$$\begin{aligned}\rho &= \operatorname{tr}_{m+b}(|\psi\rangle\langle\psi|)\\ &= \sum_{k\in[2^m]}\alpha_k\operatorname{tr}_b\left(|\psi_k\rangle_{n+a_k+b_k}\langle\psi_k| \otimes |0\rangle_{a'_k+b'_k}\langle 0|\right)\\ &= \sum_{k\in[2^m]}\alpha_k\operatorname{tr}_{b_k}\left(|\psi_k\rangle_{n+a_k+b_k}\langle\psi_k|\right) \otimes |0\rangle_{a'_k}\langle 0|\\ &= \sum_{k\in[2^m]}\alpha_k(\rho_k)_{n+a_k} \otimes |0\rangle_{a'_k}\langle 0|\\ &= \sum_{k\in[2^m]}\alpha_k\left(\rho_k^{(a'_k)}\right)_{n+a},\end{aligned}$$

where $\rho^{(b)} = \rho \otimes |0\rangle_b\langle 0|$ is defined as in Lemma II.16. To see that ρ is a $(1, a, 0)$-block-encoding of $A = \sum_{k\in[2^m]}A_k$, we note that

$$\begin{aligned}{}_a\langle 0|\rho|0\rangle_a &= \sum_{k\in[2^m]}\alpha_k\,{}_{a_k}\langle 0|(\rho_k)_{n+a_k}|0\rangle_{a_k}\\ &= \sum_{k\in[2^m]}\alpha_k A_k = A.\end{aligned}$$

Therefore, $U(V \otimes I_a \otimes I_b)$ prepares a subnormalized density operator A. □

As it will be also used to design quantum algorithms in this paper, we provide the LCU algorithm for comparison. Here, we use the notion as in the full version of [22].

Definition II.3 (State Preparation Pair): Let $y \in \mathbb{C}^m$ with $\|y\|_1 \leq \beta$, and $\varepsilon \geq 0$. A pair of unitary operator (P_L, P_R) is called a (β, b, ε)-state-preparation-pair if $P_L|0\rangle_b = \sum_{j\in[2^b]}c_j|j\rangle$ and $P_R|0\rangle_b = \sum_{j\in[2^b]}d_j|j\rangle$ such that $\sum_{j\in[m]}\left|\beta c_j^* d_j - y_j\right| \leq \varepsilon$ and $c_j^* d_j = 0$ for all $m \leq j < 2^b$.

Theorem II.18 (Linear Combination of Unitary Operators [22]): Suppose

[9] Here, we use the notation $[n] = \{0, 1, 2, \ldots, n-1\}$.

1) $y \in \mathbb{C}^m$ with $\|y\|_1 \le \beta$, and (P_L, P_R) is a $(\beta, b, \varepsilon_1)$-state-preparation-pair for y.
2) For every $k \in [m]$, U_k is an $(n+a)$-qubit unitary operator that is an $(\alpha, a, \varepsilon_2)$-block-encoding of an n-qubit operator A_k.

Then there is an $(n+a+b)$-qubit quantum circuit W such that

1) W is a $(\alpha\beta, a+b, \alpha\varepsilon_1 + \alpha\beta\varepsilon_2)$-block-encoding of $A = \sum_{k\in[m]} y_k A_k$.
2) W uses 1 query to each of $P_L^\dagger$, P_R and (controlled-)U_k for $k \in [m]$, and $O(b^2)$ elementary quantum gates.

G. Eigenvalue Threshold Projector

In this subsection, we show how to block-encode an eigenvalue threshold projector $\Pi_{\mathrm{supp}(A)}$ of a subnormalized density operator A in another. We note that a technique for block-encoding eigenvalue threshold projectors in subnormalized density operators was also provided in [32]. The major difference is that our approach does not have any further requirements on the subnormalized density operator A, while the method of [32] requires that $A \ge q\Pi$ for some projector Π and the value of $q > 0$ is known in advance.

First, we introduce the notion of truncated support. Let $\delta > 0$ and A be an Hermitian operator with spectral decomposition $A = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$. The δ-support of A is

$$\mathrm{supp}_\delta(A) = \mathrm{span}\{|\psi_j\rangle : |\lambda_j| > \delta\}.$$

Note that $\mathrm{supp}_\delta(A) \subseteq \mathrm{supp}_0(A) = \mathrm{supp}(A)$. Here, we write Π_S to denote the projector onto a subspace S.

Lemma II.19 (Eigenvalue Threshold Projector): Suppose

1) U is an $(n+a)$-qubit unitary operator that prepares an n-qubit subnormalized density operator A.
2) $\delta, \varepsilon \in (0, \frac{1}{10}]$ and $32\varepsilon^2 \le \delta$.

For every $\delta' > 0$, there is a quantum circuit $\tilde{U}$ such that

1) $\tilde{U}$ prepares an n-qubit subnormalized density operator, which is a $(1, 0, \delta')$-block-encoding of B such that
$$\left(\frac{\delta}{4}(1-2\varepsilon) - \delta^{1/2}\varepsilon\right)\Pi_{\mathrm{supp}_{2\delta}(A)} \le B \le \left(\frac{\delta}{4} + \varepsilon^2 + \delta^{1/2}\varepsilon\right)\Pi_{\mathrm{supp}(A)}.$$
2) $\tilde{U}$ uses $O(d)$ queries to U and $U^\dagger$, 1 query to controlled-U and $O((n+a)d)$ elementary quantum gates, where $d = O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$.
3) A description of $\tilde{U}$ can be computed by a (classical) Turing machine in $\mathrm{poly}(d, \log(1/\delta'))$ time.

Proof: Let $f(x) = \frac{\delta^{1/2}}{2}x^{-1/2}$, and by Lemma II.7, there is a degree-$O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$ even polynomial $P \in \mathbb{R}[x]$ such that $\|P - f\|_{[\delta,1]} \le \varepsilon$ and $\|P\|_{[-1,1]} \le 1$. By Corollary II.10, there is a degree-$O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$ even polynomial $R \in \mathbb{R}[x]$ such that $\|R\|_{[-1,1]} \le 1$ and

$$R(x) \in \begin{cases} [1-\varepsilon, 1] & x \in [-1, -2\delta] \cup [2\delta, 1] \\ [0, \varepsilon] & x \in [-\delta, \delta] \end{cases}.$$

Note that $Q = PR \in \mathbb{R}[x]$ is a degree-d even polynomial, where $d = O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$. By Theorem II.3, for $\delta_Q > 0$, there is a quantum circuit U_Q such that

1) U_Q is a $(1, O(n+a), 0)$-block-encoding of A_1, and A_1 is a $(1, 0, \delta_Q)$-block-encoding of $Q(A)$.
2) U_Q uses d queries to U and $U^\dagger$, 1 query to controlled-U and $O((n+a)d)$ elementary quantum gates.
3) A description of U_Q can be computed by a (classical) Turing machine in $\mathrm{poly}(d, \log(1/\delta_Q))$ time.

By Lemma II.2, using 1 query to each of U_Q and U, we obtain a unitary operator $\tilde{U}$ that prepares $A_1 A A_1^\dagger$. We note that

$$\begin{aligned} \left\|A_1 A A_1^\dagger - A(Q(A))^2\right\| &\le \left\|A_1 A A_1^\dagger - Q(A) A A_1^\dagger\right\| \\ &\quad + \left\|Q(A) A A_1^\dagger - Q(A) A Q(A)\right\| \\ &\le 2\delta_Q. \end{aligned}$$

Moreover, $A_1 A A_1^\dagger$ can be regarded as a (scaled) projector. To see this, let $\mathbb{1}_S$ be the indicator function that

$$\mathbb{1}_S(x) = \begin{cases} 1, & x \in S, \\ 0, & \text{otherwise.} \end{cases}$$

Then $\Pi_{\mathrm{supp}_\delta(A)} = \mathbb{1}_{[\delta,1]}(A)$. We note that if $32\varepsilon^2 \le \delta$, then

$$\begin{aligned} \left(\tfrac{\delta}{4}(1-2\varepsilon) - \delta^{1/2}\varepsilon\right)\Pi_{\mathrm{supp}_{2\delta}(A)} &\le A(Q(A))^2 \\ &\le \left(\tfrac{\delta}{4} + \varepsilon^2 + \delta^{1/2}\varepsilon\right)\Pi_{\mathrm{supp}(A)}. \end{aligned} \tag{3}$$

We need to show that

$$\begin{aligned} \left(\frac{\delta}{4}(1-2\varepsilon) - \delta^{1/2}\varepsilon\right)\mathbb{1}_{[2\delta,1]}(x) &\le x(Q(x))^2 \\ &\le \left(\frac{\delta}{4} + \varepsilon^2 + \delta^{1/2}\varepsilon\right)\mathbb{1}_{(0,1]}(x) \end{aligned}$$

for every $x \in [0,1]$. This is seen by the following four cases.

1) $x = 0$. This case is trivial as each hand side is equal to 0.
2) $x \in (0, \delta]$. We have $0 \le x(Q(x))^2 \le x(R(x))^2 \le x\varepsilon^2 \le \delta\varepsilon^2$.
3) $x \in (\delta, 2\delta]$. We have
$$\begin{aligned} 0 \le x(Q(x))^2 &\le x(P(x))^2 \le x(f(x)+\varepsilon)^2 \\ &= x(f(x))^2 + x\varepsilon^2 + 2xf(x)\varepsilon \le \frac{\delta}{4} + \varepsilon^2 + \delta^{1/2}\varepsilon. \end{aligned}$$
4) $x \in (2\delta, 1]$. The right hand side is $x(Q(x))^2 \le \frac{\delta}{4} + \varepsilon^2 + \delta^{1/2}\varepsilon$ is similar to Case 3. The left hand side is as follows.
$$\begin{aligned} x(Q(x))^2 &\ge x(P(x))^2(1-\varepsilon)^2 \\ &\ge x(f(x)-\varepsilon)^2(1-\varepsilon)^2 \\ &\ge x((f(x))^2 - 2f(x)\varepsilon)(1-2\varepsilon) \\ &= \left(\frac{\delta}{4} - \delta^{1/2}x^{1/2}\varepsilon\right)(1-2\varepsilon) \\ &\ge \frac{\delta}{4}(1-2\varepsilon) - \delta^{1/2}\varepsilon. \end{aligned}$$

Therefore, we conclude that Eq. (3) holds. We claim the lemma by setting $B = A(Q(A))^2$ and $\delta' = 2\delta_Q$. □

III. Quantum Entropies

In the Introduction, we have already introduced several quantum entropies such as the von Neumann entropy, quantum Rényi entropy and quantum Tsallis entropy. In addition to this, the quantum Min entropy $S^{\min}(\rho)$ and the quantum Max (Hartley) entropy $S^{\max}(\rho)$ are defined as limits of Rényi entropies by

$$S^{\min}(\rho) = S^R_\infty(\rho) = \lim_{\alpha\to\infty} S^R_\alpha(\rho) = -\ln\left(\|\rho\|\right),$$
$$S^{\max}(\rho) = S^R_0(\rho) = \lim_{\alpha\to 0} S^R_\alpha(\rho) = \ln\left(\operatorname{rank}(\rho)\right).$$

The unified entropy [56] is defined by

$$S^s_\alpha(\rho) = \frac{1}{(1-\alpha)s}\left(\left(\operatorname{tr}\left(\rho^\alpha\right)\right)^s - 1\right)$$

for $\alpha \in (0,1)\cup(1,+\infty)$ and $s \neq 0$, which includes the von Neumann entropy $S(\rho) = \lim_{\alpha\to1} S^s_\alpha(\rho)$, the Rényi entropy $S^R_\alpha(\rho) = \lim_{s\to0} S^s_\alpha(\rho)$ and the Tsallis entropy $S^T_\alpha(\rho) = S^1_\alpha(\rho)$.

In this section, we will propose a series of quantum algorithms for computing several quantum entropies. Section III-A provides a quantum algorithm for computing the von Neumann entropy. Section III-B is for the Max entropy. Section III-C is for the quantum Rényi and Tsallis entropies.

A. Von Neumann Entropy

The von Neumann entropy is one of the most important quantum information quantities. As mentioned above, both quantum algorithms for estimating von Neumann entropy provided by [6] and [8] have time complexity exponential in the number $n = \log_2(N)$ of qubits of the quantum state. Here, we provide a different approach that exponentially improves the dependence on n given that the density operator of the mixed quantum state is low-rank. Our key technique used here is different from that of [8], where they approximated a function $\propto -\ln(x)$ and constructed a unitary operator that is a block-encoding of $S(\rho)$, while we approximate a function $\propto \sqrt{-\ln(x)}$ and prepare a density operator that is a block-encoding of $S(\rho)$.

Theorem III.1: Suppose that

1) U_ρ is an $(n+n_\rho)$-qubit unitary operator that prepares an n-qubit density operator ρ with $\operatorname{rank}(\rho)\le r$.
2) n_ρ is a polynomial in n.[10]

There is a quantum algorithm that computes the von Neumann entropy $S(\rho)$ within additive error ε using $\tilde{O}(\frac{r}{\varepsilon^2})$ queries to U_ρ and $\tilde{O}(\frac{r}{\varepsilon^2}\operatorname{poly}(n))$ elementary quantum gates.[11]

Before the proof of Theorem III.1, we need the following method of approximating functions by polynomials based on Taylor series.

Lemma III.2 (Corollary 66 of the Full Version of [22]): Let $x_0 \in [-1,1]$, $r\in(0,2]$, $\delta\in(0,r]$ and $f : [x_0-r-\delta, x_0+r+\delta] \to \mathbb{C}$ such that

$$f(x_0+x) = \sum_{k=0}^{\infty} a_k x^k$$

for all $x \in [-r-\delta, r+\delta]$. Suppose $B>0$ and

$$\sum_{k=0}^{\infty} |a_k|\,(r+\delta)^k \le B.$$

Let $\varepsilon\in(0,\frac{1}{2B}]$, then there is an efficient computable polynomial $P\in\mathbb{C}[x]$ of degree $O\left(\frac{1}{\delta}\log\left(\frac{B}{\varepsilon}\right)\right)$ such that

$$\|f(x)-P(x)\|_{[x_0-r,x_0+r]} \le \varepsilon,$$
$$\|P\|_{[-1,1]} \le \varepsilon + \|f\|_{[x_0-r-\delta/2,x_0+r+\delta/2]} \le \varepsilon + B,$$
$$\|P\|_{[-1,1]\setminus[x_0-r-\delta/2,x_0+r+\delta/2]} \le \varepsilon.$$

By Lemma III.2, we are able to give an approximation of scaled $\sqrt{-\ln(x)}$ as follows.

Lemma III.3: For every $\delta',\varepsilon\in(0,\frac14]$, there is an efficient computable polynomial $P\in\mathbb{R}[x]$ of degree $O\left(\frac{1}{\delta'}\log\left(\frac{1}{\delta'\varepsilon}\right)\right)$ such that

$$\left\|P(x) - \frac{\sqrt{-\ln(x)}}{2\sqrt{-\ln(\delta')}}\right\|_{[\delta',1-\delta']} \le \varepsilon,$$
$$\|P\|_{[-1,1]} \le 1.$$

Proof: Let $f(x) = \frac{\sqrt{-\ln(x)}}{2\sqrt{-\ln(\delta')}}$ whose Taylor series expanded around $x_0=\frac12$ is $f(x_0+x)=\sum_{k=0}^\infty a_k x^k$. We note that $f(x)$ is holomorphic in $\mathbb{C}\setminus(-\infty,0]\setminus[1,\infty)$ if we choose the definitions of $\ln(\cdot)$ and $\sqrt{(\cdot)}$ to be their principle branches in complex analysis. Thus the radius of convergence of the Taylor series of $f(x)$ expanded around $x_0=\frac12$ is $R=\frac12$. We have

$$\limsup_{k\to\infty}\sqrt[k]{|a_k|} = \frac{1}{R} = 2.$$

Therefore, there exists $k_0\in\mathbb{N}$ such that for every $k>k_0$, it holds that $\sqrt[k]{|a_k|} < 2+\delta'$. Now we set $r=\frac12-\delta'$ and $\delta=\delta'/2$, and we have

$$\begin{aligned}\sum_{k=0}^{\infty}|a_k|\,(r+\delta)^k &\le \sum_{k=0}^{\infty}(2+\delta')^k\left(\frac12-\frac{\delta'}{2}\right)^k + O(1)\\ &\le \sum_{k=0}^{\infty}\left(1-\frac{\delta'}{2}\right)^k + O(1)\\ &= \frac{2}{\delta'} + O(1) =: B.\end{aligned}$$

Now applying Lemma III.2, there is an efficiently computable polynomial $P\in\mathbb{C}[x]$ of degree $O\left(\frac{1}{\delta}\log\left(\frac{B}{\varepsilon}\right)\right) = O\left(\frac{1}{\delta'}\log\left(\frac{1}{\delta'\varepsilon}\right)\right)$ such that

$$\|f(x)-P(x)\|_{[\delta',1-\delta']} \le \varepsilon,$$
$$\|P(x)\|_{[-1,1]} \le \varepsilon + \|f\|_{[3\delta'/4,1-3\delta'/4]},$$
$$\|P\|_{[-1,1]\setminus[3\delta'/4,1-3\delta'/4]} \le \varepsilon.$$

Here, we note that

$$\|f\|_{[3\delta'/4,1-3\delta'/4]} = f\left(\frac{3\delta'}{4}\right) \le \frac34$$

[10] Theoretically, any n-qubit mixed quantum state has a purification with at most n ancilla qubits, so it is sufficient to assume that $n_\rho \le n$. Here, we just assume that $n_\rho = \operatorname{poly}(n)$ for convenience.

[11] Since the quantum algorithm is complicated, we do not distinguish between the queries to a unitary operator and those to its controlled versions, and we ignore poly-logarithmic factors.

and we obtain $\|P\|_{[-1,1]} \leq 1$ combining the three cases above. Finally, since we are only interested in the real part of $P(x)$ and x is always a real number, just selecting the real part of the coefficients of $P(x)$ will obtain a desired polynomial with real coefficients. □

Now we are ready to give the proof of Theorem III.1.

Proof of Theorem III.1: Let $\delta, \varepsilon_1 \in (0, \frac{1}{4})$ and

$$f(x) = \frac{\sqrt{-\ln(x)}}{2\sqrt{-\ln(\delta)}}.$$

By Lemma III.3, there is a polynomial $P(x)$ of degree $O\left(\frac{1}{\delta}\log\left(\frac{1}{\delta\varepsilon_1}\right)\right)$ such that $\|P\|_{[-1,1]} \leq 1$ and $\|P(x) - f(x)\|_{[\delta,1-\delta]} \leq \varepsilon_1$. By Corollary II.11, there is an even polynomial $R(x)$ of degree $O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon_1}\right)\right)$ such that $\|R\|_{[-1,1]} \leq 1$ and

$$R(x) \in \begin{cases} [1-\varepsilon_1, 1] & x \in [-1+2\delta, 1-2\delta] \\ [0, \varepsilon_1] & x \in [-1, -1+\delta] \cup [1-\delta, 1] \end{cases}.$$

We note that $\frac{1}{2}P(x)R(x)$ is a polynomial of degree $d = O\left(\frac{1}{\delta}\log\left(\frac{1}{\delta\varepsilon_1}\right)\right)$ satisfying $\left\|\frac{1}{2}P(x)R(x)\right\|_{[-1,1]} \leq \frac{1}{2}$. Let $\delta_1 \in (0,1)$ and by Lemma II.4, there is a quantum circuit $\tilde{U}$ such that

1) $\tilde{U}$ prepares an n-qubit subnormalized density operator A_1, and A_1 is a $(1, 0, \delta_1)$-block-encoding of $\rho\left(\frac{1}{2}P(\rho)R(\rho)\right)^2$.
2) $\tilde{U}$ uses $O(d)$ queries to U_ρ and $U_\rho^\dagger$, 1 query to controlled-U and controlled-$U_\rho^\dagger$, and $O((n+a)d)$ elementary quantum gates.
3) A description of $\tilde{U}$ can be computed by a (classical) Turing machine in $O(\mathrm{poly}(d, \log(1/\delta_1)))$ time.

Now we are going to show that

$$\left\|x(P(x)R(x))^2 - x(f(x))^2\right\|_{[0,1]} \leq \Theta\left(\varepsilon_1 + \frac{\delta}{\ln\left(\frac{1}{\delta}\right)}\right),$$

which immediately yields

$$\left\|\rho(P(\rho)R(\rho))^2 - \rho(f(\rho))^2\right\| \leq \Theta\left(\varepsilon_1 + \frac{\delta}{\ln\left(\frac{1}{\delta}\right)}\right).$$

We consider four cases.

1) $x \in [0, \delta]$. In this case,

$$\begin{aligned}
&\left|x(P(x)R(x))^2 - x(f(x))^2\right| \\
&\quad \leq \left|x(P(x)R(x))^2\right| + \left|x(f(x))^2\right| \\
&\quad \leq \delta + \delta(f(\delta))^2 \\
&\quad = \delta + \delta/4 \\
&\quad = \Theta(\delta).
\end{aligned}$$

2) $x \in [\delta, 1-2\delta]$. In this case,

$$\begin{aligned}
&\left|x(P(x)R(x))^2 - x(f(x))^2\right| \\
&\quad \leq |x|\left(\left|(P(x))^2 - (f(x))^2\right|\left|(R(x))^2\right|\right. \\
&\qquad \left. + \left|(R(x))^2 - 1\right|\left|(f(x))^2\right|\right) \\
&\quad \leq 2\left|P(x) - f(x)\right| + 2\left|R(x) - 1\right| \\
&\quad \leq 2\varepsilon_1 + 2\varepsilon_1 = \Theta(\varepsilon_1).
\end{aligned}$$

3) $x \in [1-2\delta, 1-\delta]$. We note that $-x\ln(x) < 1 - x$ for every $x \in (0,1)$. In this case,

$$\begin{aligned}
&\left|x(P(x)R(x))^2 - x(f(x))^2\right| \\
&\quad \leq \left|x(P(x)R(x))^2\right| + \left|x(f(x))^2\right| \\
&\quad \leq \left|x(P(x))^2\right| + \left|x(f(x))^2\right| \\
&\quad \leq 2\left|x(f(x))^2\right| + \left|x(P(x))^2 - x(f(x))^2\right| \\
&\quad \leq 2\frac{-x\ln(x)}{-4\ln(\delta)} + 2\left|P(x) - f(x)\right| \\
&\quad \leq \frac{1-x}{-2\ln(\delta)} + 2\varepsilon_1 \\
&\quad \leq \frac{2\delta}{-2\ln(\delta)} + 2\varepsilon_1 \\
&\quad = \Theta\left(\frac{\delta}{\ln\left(\frac{1}{\delta}\right)} + \varepsilon_1\right).
\end{aligned}$$

4) $x \in [1-\delta, 1]$. In this case,

$$\begin{aligned}
&\left|x(P(x)R(x))^2 - x(f(x))^2\right| \\
&\quad \leq \left|x(P(x)R(x))^2\right| + \left|x(f(x))^2\right| \\
&\quad \leq \left|(R(x))^2\right| + \left|x(f(x))^2\right| \\
&\quad \leq \Theta\left(\varepsilon_1 + \frac{\delta}{\ln\left(\frac{1}{\delta}\right)}\right).
\end{aligned}$$

We note that $\mathrm{tr}\left(\rho(f(\rho))^2\right) = \frac{S(\rho)}{4\ln\left(\frac{1}{\delta}\right)}$. Based on this, we have

$$\begin{aligned}
&\left|16\ln\left(\frac{1}{\delta}\right)\mathrm{tr}(A_1) - S(\rho)\right| \\
&\quad \leq \Theta\left(r\left((\varepsilon_1 + \delta_1)\ln\left(\frac{1}{\delta}\right) + \delta\right)\right).
\end{aligned}$$

On the other hand, $\mathrm{tr}(A_1)$ has an upper bound that

$$\mathrm{tr}(A_1) \leq \frac{S(\rho)}{16\ln\left(\frac{1}{\delta}\right)} + O(1) \leq \frac{\ln(r)}{16\ln\left(\frac{1}{\delta}\right)} + O(1) =: B.$$

Let $\varepsilon_2 \in (0,1)$. By Lemma II.15, we can compute $\tilde{p}$ such that $|\mathrm{tr}(A_1) - \tilde{p}| \leq \varepsilon_2$ with $O\left(\frac{\sqrt{B}}{\varepsilon_2} + \frac{1}{\sqrt{\varepsilon_2}}\right)$ queries to $\tilde{U}$ and $\tilde{U}^\dagger$.

Finally, we choose $16\ln\left(\frac{1}{\delta}\right)\tilde{p}$ to be the approximation of $S(\rho)$. The error is bounded by

$$\begin{aligned}
&\left|16\ln\left(\tfrac{1}{\delta}\right)\tilde{p} - S(\rho)\right| \\
&\quad \leq \Theta\left(r\left((\varepsilon_1 + \delta_1)\ln\left(\tfrac{1}{\delta}\right) + \delta\right) + \varepsilon_2\ln\left(\tfrac{1}{\delta}\right)\right). \qquad (4)
\end{aligned}$$

Let the right hand side of Eq. (4) become $\leq \varepsilon$, then the number of queries to U_ρ is

$$O(d) \cdot O\left(\frac{\sqrt{B}}{\varepsilon_2} + \frac{1}{\sqrt{\varepsilon_2}}\right) = \tilde{O}\left(\frac{d}{\varepsilon_2}\right) = \tilde{O}\left(\frac{r}{\varepsilon^2}\right).$$

□

B. Max Entropy and Rank of Quantum States

The Max (Hartley) entropy $S^{\max}(\rho) = \ln(\mathrm{rank}(\rho))$ of a quantum state ρ is the logarithm of its rank. Low-rank quantum states turn out to be useful in quantum algorithms, e.g. [11], [34], [37], [40], and [101]. Estimating the rank of quantum states is important in checking whether a quantum state fits in a certain low-rank condition of a quantum algorithm. Recently, a variational quantum algorithm was proposed in [14] to estimate the rank of quantum states. Here, we provide a quantum algorithm for rank estimation. For $\delta > 0$, the δ-rank of a matrix A is defined by

$$\operatorname{rank}_\delta(A) = \min\{\operatorname{rank}(B) : \|A - B\| \le \delta\}.$$

In particular, $\operatorname{rank}_0(A) = \operatorname{rank}(A)$. We note that if A is Hermitian and has the spectrum decomposition $A = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$, then $\operatorname{rank}_\delta(A) = \operatorname{tr}\left(\Pi_{\operatorname{supp}_\delta(A)}\right)$ is the number of eigenvalues λ_j such that $|\lambda_j| > \delta$.

Theorem III.4 (Rank Estimation): Suppose that

1) U is an $(n+a)$-qubit unitary operator that prepares an n-qubit density operator ρ.
2) $\delta \in (0, \frac{1}{10}]$.

For $\varepsilon, \varepsilon' \in (0,1)$, there is a quantum algorithm that outputs $\tilde{r}$ such that

$$(1-\varepsilon)\operatorname{rank}_\delta(\rho) - \varepsilon' \le \tilde{r} \le (1+\varepsilon)\operatorname{rank}(\rho) + \varepsilon',$$

using $O\left(\frac{1}{\delta^2\varepsilon'}\log\left(\frac{1}{\delta\varepsilon}\right)\right)$ queries to U and $O\left(\frac{1}{\delta^2\varepsilon'}\log\left(\frac{1}{\delta\varepsilon}\right)\operatorname{poly}(n)\right)$ elementary quantum gates.

Proof: Step 1: By Lemma II.19, introducing parameters $\delta_1, \varepsilon_1 \in (0, \frac{1}{10}]$ with $32\varepsilon_1^2 \le \delta$, there is a quantum circuit $\tilde{U}$ such that

1) $\tilde{U}$ prepares an n-qubit subnormalized density operator A, which is a $(1, 0, \delta_1)$-block-encoding of $\tilde{\Pi}$ such that
$$\begin{aligned}\left(\tfrac{\delta}{8}(1-2\varepsilon_1) - \left(\tfrac{\delta}{2}\right)^{1/2}\varepsilon_1\right)\Pi_{\operatorname{supp}_\delta(\rho)} &\le \tilde{\Pi} \\ &\le \left(\tfrac{\delta}{8} + \varepsilon_1^2 + \left(\tfrac{\delta}{2}\right)^{1/2}\varepsilon_1\right)\Pi_{\operatorname{supp}(\rho)}. \qquad (5)\end{aligned}$$
2) $\tilde{U}$ uses $O(d)$ queries to U and $U^\dagger$, 1 query to controlled-U and $O((n+a)d)$ elementary quantum gates, where $d = O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon_1}\right)\right)$.
3) A description of $\tilde{U}$ can be computed by a (classical) Turing machine in $\operatorname{poly}(d, \log(1/\delta_1))$ time.

We note that $\left|\operatorname{tr}(A) - \operatorname{tr}(\tilde{\Pi})\right| \le 2^n\delta_1$ and by Eq. (5) we have

$$\begin{aligned}\left(1 - 2\varepsilon_1 - 4\sqrt{2}\delta^{-1/2}\varepsilon_1\right)\operatorname{rank}_\delta(\rho) &\le 8\delta^{-1}\operatorname{tr}(\tilde{\Pi}) \\ &\le \left(1 + 8\delta^{-1}\varepsilon_1^2 + 4\sqrt{2}\delta^{-1/2}\varepsilon_1\right)\operatorname{rank}(\rho).\end{aligned}$$

Step 2: Introducing a parameter ε_2, by Lemma II.15, we can compute $\tilde{p}$ that estimates $\operatorname{tr}(A)$ such that $|\tilde{p} - \operatorname{tr}(A)| \le \varepsilon_2$ with $O\left(\frac{\sqrt{B}}{\varepsilon_2} + \frac{1}{\sqrt{\varepsilon_2}}\right)$ queries to $\tilde{U}$ and $\tilde{U}^\dagger$, where B is an upper bound for $\operatorname{tr}(A)$. Here, we just choose $B = 1$.

Step 3: Output $\tilde{r} = 8\delta^{-1}\tilde{p}$ as the estimation of the rank of ρ. Here, we see that

$$\begin{aligned}&\left(1 - 2\varepsilon_1 - 4\sqrt{2}\delta^{-1/2}\varepsilon_1\right)\operatorname{rank}_\delta(\rho) - 8\delta^{-1}\left(2^n\delta_1 + \varepsilon_2\right) \le \tilde{r} \\ &\le \left(1 + 8\delta^{-1}\varepsilon_1^2 + 4\sqrt{2}\delta^{-1/2}\varepsilon_1\right)\operatorname{rank}(\rho) + 8\delta^{-1}\left(2^n\delta_1 + \varepsilon_2\right).\end{aligned}$$

By letting $\varepsilon_1 = \frac{1}{32}\delta\varepsilon < 1$ (note that it also holds that $32\varepsilon_1^2 < 32\varepsilon_1 = \delta\varepsilon < \delta$), $\varepsilon_2 = \frac{1}{16}\delta\varepsilon'$, and $\delta_1 = \frac{1}{2^{n+4}}\delta\varepsilon'$, the above inequality becomes $(1-\varepsilon)\operatorname{rank}_\delta(\rho) - \varepsilon' \le \tilde{r} \le (1+\varepsilon)\operatorname{rank}(\rho) + \varepsilon'$. To see this, we have to show the following three inequalities.

1) $2\varepsilon_1 + 4\sqrt{2}\delta^{-1/2}\varepsilon_1 \le \varepsilon$. Note that $\delta^{-1} \ge \delta^{-1/2} \ge 3$. We have $2\varepsilon_1 + 4\sqrt{2}\delta^{-1/2}\varepsilon_1 \le \delta^{-1}\varepsilon_1 + 4\sqrt{2}\delta^{-1}\varepsilon_1 = (1+4\sqrt{2})\delta^{-1}\varepsilon_1 \le 32\delta^{-1}\varepsilon_1 = \varepsilon$.
2) $8\delta^{-1}\varepsilon_1^2 + 4\sqrt{2}\delta^{-1/2}\varepsilon_1 \le \varepsilon$. Note that $\varepsilon_1^2 < \varepsilon_1 < 1$ and $\delta^{-1} \ge \delta^{-1/2} \ge 3$. We have $8\delta^{-1}\varepsilon_1^2 + 4\sqrt{2}\delta^{-1/2}\varepsilon_1 \le 8\delta^{-1}\varepsilon_1 + 4\sqrt{2}\delta^{-1}\varepsilon_1 = (8+4\sqrt{2})\delta^{-1}\varepsilon_1 \le 32\delta^{-1}\varepsilon_1 = \varepsilon$.
3) $8\delta^{-1}\left(2^n\delta_1 + \varepsilon_2\right) \le \varepsilon'$. This is simple by directly taking the values of ε_2 and δ_1.

Finally, the number of queries to U is

$$O\left(\frac{1}{\delta}\log\left(\frac{1}{\varepsilon_1}\right)\cdot\left(\frac{\sqrt{B}}{\varepsilon_2} + \frac{1}{\sqrt{\varepsilon_2}}\right)\right) = O\left(\frac{1}{\delta^2\varepsilon'}\log\left(\frac{1}{\delta\varepsilon}\right)\right).$$

And similarly, the number of elementary quantum gates is $O\left(\frac{1}{\delta^2\varepsilon'}\log\left(\frac{1}{\delta\varepsilon}\right)\operatorname{poly}(n)\right)$. □

Based on Theorem III.4, we can obtain the exact rank of ρ if $\Pi/\kappa \le \rho$ for some projector Π and $\kappa > 0$.

Corollary III.5 (Exact Rank): Suppose U is an $(n+a)$-qubit unitary operator that prepares an n-qubit density operator ρ. If $\Pi/\kappa \le \rho$ for some projector Π and $\kappa > 0$, then there is a quantum algorithm that outputs $r = \operatorname{rank}(\rho)$ using $\tilde{O}(\kappa^2)$ queries to U and $\tilde{O}(\kappa^2\operatorname{poly}(n))$ elementary quantum gates.

Proof: The claim holds immediately by letting $\delta = \varepsilon = \frac{1}{10\kappa}$ and $\varepsilon' = 1/10$ in Theorem III.4. □

Now we furthermore define the δ-Max entropy by $S^{\max}_\delta(\rho) = \ln(\operatorname{rank}_\delta(\rho))$. Based on Theorem III.4, we are able to give an estimation of the Max entropy.

Theorem III.6 (Max Entropy Estimation): Suppose that

1) U is an $(n+a)$-qubit unitary operator that prepares an n-qubit density operator ρ.
2) $\delta \in (0, \frac{1}{10}]$.

For $\varepsilon > 0$, there is a quantum algorithm that outputs $\tilde{s}$ such that

$$S^{\max}_\delta(\rho) - \varepsilon \le \tilde{s} \le S^{\max}(\rho) + \varepsilon,$$

using $\tilde{O}(\frac{1}{\delta^2\varepsilon})$ queries to U and $\tilde{O}(\frac{1}{\delta^2\varepsilon}\operatorname{poly}(n))$ elementary quantum gates.

Moreover, if $\Pi/\kappa \le \rho$ for some projector Π and $\kappa > 0$, there is a quantum algorithm that computes the Max entropy $S^{\max}(\rho)$ within additive error ε using $\tilde{O}(\frac{\kappa^2}{\varepsilon})$ queries to U and $\tilde{O}(\frac{\kappa^2}{\varepsilon}\operatorname{poly}(n))$ elementary quantum gates.

Proof: By Theorem III.4, there is a quantum algorithm that outputs $\tilde{r}$ such that

$$\begin{aligned}\left(1 - \frac{\varepsilon}{2}\right)\operatorname{rank}_\delta(\rho) &\le \left(1 - \frac{\varepsilon}{4}\right)\operatorname{rank}_\delta(\rho) - \frac{\varepsilon}{4} \le \tilde{r} \\ &\le \left(1 + \frac{\varepsilon}{4}\right)\operatorname{rank}(\rho) + \frac{\varepsilon}{4} \\ &\le \left(1 + \frac{\varepsilon}{2}\right)\operatorname{rank}(\rho),\end{aligned}$$

using $\tilde{O}(\frac{1}{\delta^2\varepsilon})$ queries to U and $\tilde{O}(\frac{1}{\delta^2\varepsilon}\operatorname{poly}(n))$ elementary quantum gates. After taking logarithm of both sides, we have

$$\begin{aligned}\ln\left(\operatorname{rank}_\delta(\rho)\right) + \ln\left(1 - \frac{\varepsilon}{2}\right) &\le \ln(\tilde{r}) \\ &\le \ln\left(\operatorname{rank}(\rho)\right) + \ln\left(1 + \frac{\varepsilon}{2}\right),\end{aligned}$$

which is

$$S_{\delta}^{\max}(\rho) - \varepsilon \leq \ln(\tilde{r}) \leq S^{\max}(\rho) + \varepsilon.$$

We only need to output $\tilde{s} = \ln(\tilde{r})$ as an estimation of the Max entropy $S^{\max}(\rho)$.

Moreover, if $\Pi/\kappa \leq \rho$ for some projector Π and $\kappa > 0$, the claim is obtained by letting $\delta = \frac{1}{\kappa}$ (and then $S_{\delta}^{\max}(\rho) = S^{\max}(\rho)$). □

C. Quantum Rényi Entropy and Quantum Tsallis Entropy

Now we are going to discuss how quantum algorithms can compute the quantum Rényi entropy $S_{\alpha}^{R}(\rho)$ and the quantum Tsallis entropy $S_{\alpha}^{T}(\rho)$. The key is to compute $\mathrm{tr}(\rho^{\alpha})$, which is given as follows.

Theorem III.7 (Trace of Positive Powers): Suppose that

1) U_{ρ} is an $(n+n_{\rho})$-qubit unitary operator that prepares an n-qubit density operator ρ with $\mathrm{rank}(\rho) \leq r$.
2) n_{ρ} is a polynomial in n.

For $a \in (0,1) \cup (1,+\infty)$, there is a quantum algorithm that computes $\mathrm{tr}(\rho^{\alpha})$ within additive error ε using Q queries to U_{ρ} and $Q \cdot \mathrm{poly}(n)$ elementary quantum gates, where

$$Q = \begin{cases} \tilde{O}\left(r^{\frac{3-\alpha^2}{2\alpha}} / \varepsilon^{\frac{3+\alpha}{2\alpha}}\right), & 0 < \alpha < 1, \\ O\left(1/\varepsilon\right), & \alpha > 1 \wedge \alpha \text{ is odd}, \\ \tilde{O}\left(r^{1/\left\{\frac{\alpha-1}{2}\right\}} / \varepsilon^{1+1/\left\{\frac{\alpha-1}{2}\right\}}\right), & \text{otherwise}. \end{cases}$$

and $\{x\} = x - \lfloor x \rfloor$ is the decimal part of real number x.

Proof: We will discuss in three cases as stated in the statement of this theorem.

Case 1: $0 < \alpha < 1$. In this case, we have $\mathrm{tr}(\rho^{\alpha}) \leq r^{1-\alpha}$. By Lemma II.8 and introducing δ_1 and ε_1, there is a quantum circuit $\tilde{U}$ such that

1) $\tilde{U}$ prepares an n-qubit subnormalized density operator A, and A is a $\left(4\delta_1^{\alpha-1}, 0, \Theta\left(\delta_1^{\alpha} + \varepsilon_1\delta_1^{\alpha-1}\right)\right)$-block-encoding of ρ^{α}.
2) $\tilde{U}$ uses $O(d)$ queries to U_{ρ} and $O((n+n_{\rho})d)$ elementary quantum gates, where $d = O\left(\frac{1}{\delta_1}\log\left(\frac{1}{\varepsilon_1}\right)\right)$.
3) The description of $\tilde{U}$ can be computed by a classical Turing machine in $O(\mathrm{poly}(d))$ time.

Note that A is a $\left(4\delta_1^{\alpha-1}, 0, \Theta\left(\delta_1^{\alpha} + \varepsilon_1\delta_1^{\alpha-1}\right)\right)$-block-encoding of ρ^{α}, i.e., $\left\|4\delta_1^{\alpha-1}A - \rho^{\alpha}\right\| \leq \Theta(\delta_1^{\alpha} + \varepsilon_1\delta_1^{\alpha-1})$, we have $\left|4\delta_1^{\alpha-1}\,\mathrm{tr}(A) - \mathrm{tr}(\rho^{\alpha})\right| \leq \Theta(r(\delta_1^{\alpha} + \varepsilon_1\delta_1^{\alpha-1}))$. Therefore,

$$\begin{aligned} \mathrm{tr}(A) &\leq \frac{1}{4\delta_1^{\alpha-1}}\left(\mathrm{tr}(\rho^{\alpha}) + \Theta(r(\delta_1^{\alpha} + \varepsilon_1\delta_1^{\alpha-1}))\right) \\ &\leq \Theta(r^{1-\alpha}\delta_1^{1-\alpha} + r\delta_1 + r\varepsilon_1) =: B. \end{aligned}$$

By Lemma II.15 and introducing ε_2, we can obtain $\tilde{x}$ as an approximation of $\mathrm{tr}(A)$ with $Q = O\left(\frac{\sqrt{B}}{\varepsilon_2} + \frac{1}{\sqrt{\varepsilon_2}}\right)$ queries to $\tilde{U}$ such that $|\mathrm{tr}(A) - \tilde{x}| \leq \varepsilon_2$. Then we output $4\delta_1^{\alpha-1}\tilde{x}$ as an approximation of $\mathrm{tr}(\rho^{\alpha})$ by noting that

$$\left|4\delta_1^{\alpha-1}\tilde{x} - \mathrm{tr}(\rho^{\alpha})\right| \leq \Theta\left(\delta_1^{\alpha-1}\varepsilon_2 + r(\delta_1^{\alpha} + \varepsilon_1\delta_1^{\alpha-1})\right).$$

The number of queries to U_{ρ} is

$$Qd = \tilde{O}\left(\frac{1}{\delta_1}\left(\frac{\sqrt{B}}{\varepsilon_2} + \frac{1}{\sqrt{\varepsilon_2}}\right)\right) = \tilde{O}\left(r^{\frac{3-\alpha^2}{2\alpha}} / \varepsilon^{\frac{3+\alpha}{2\alpha}}\right)$$

by taking $\delta_1 = \tilde{\Theta}\left((\varepsilon/r)^{1/\alpha}\right)$, $\varepsilon_1 = \tilde{\Theta}\left((\varepsilon/r)^{1/\alpha}\right)$ and $\varepsilon_2 = \tilde{\Theta}\left(\varepsilon^{1/\alpha}/r^{1/\alpha-1}\right)$.

Case 2: $\alpha > 1$ and α is an odd number. Let $\alpha = 2\beta + 1$. By Lemma II.1, there is a unitary operator U_1, which is a $(1, n+n_{\rho}, 0)$-block-encoding of ρ with 1 query to U_{ρ}. By Lemma II.12, there is a unitary operator U_{β}, which is a $(1, \Theta(\beta(n+n_{\rho})), 0)$-block-encoding of ρ^{β} with β queries to U_1. By Lemma II.2, there is a quantum circuit U that prepares $\rho^{2\beta+1} = \rho^{\alpha}$ with 1 query to U_{ρ} and 1 query to U_{β}. Note that $\mathrm{tr}(\rho^{\alpha}) \leq 1$ and by Lemma II.15, we can obtain $\tilde{x}$ as an approximation of $\mathrm{tr}(\rho^{\alpha})$ with $O(1/\varepsilon)$ queries to U such that $|\tilde{x} - \mathrm{tr}(\rho^{\alpha})| \leq \varepsilon$. In total, the number of queries to U_{ρ} is $O(1/\varepsilon) \cdot \beta = O(1/\varepsilon)$.

Case 3: $\alpha > 1$ and α is not an odd number. Let $\beta = \left\lfloor\frac{\alpha-1}{2}\right\rfloor$ and $c = \left\{\frac{\alpha-1}{2}\right\}$. By Lemma II.13 and introducing δ_1 and ε_1, there is a unitary operator U_c that is a $(2, O(n+n_{\rho}), \Theta(\varepsilon_1 + \delta_1^{c}))$-block-encoding of ρ^{c} with $Q_1 = O\left(\frac{1}{\delta_1}\log\left(\frac{1}{\varepsilon_1}\right)\right)$ queries to U_1. By Lemma II.12, there is a unitary operator $U_{\beta+c}$ that is a $(2, O(\beta(n+n_{\rho})), \Theta(\varepsilon_1+\delta_1^{c}))$-block-encoding of $\rho^{\beta+c}$ with 1 query to U_{β} and 1 query to U_c. By Lemma II.2, there is a unitary operator U that prepares a subnormalized density operator A with 1 query to U_{ρ} and 1 query to $U_{\beta+c}$, and A is a $(4, 0, \Theta(\varepsilon_1+\delta_1^{c}))$-block-encoding of $\rho^{2(\beta+c)+1} = \rho^{\alpha}$, i.e., $\|4A - \rho^{\alpha}\| \leq \Theta(\varepsilon_1 + \delta_1^{c})$. Note that

$$\mathrm{tr}(A) \leq \frac{1}{4}\left(\mathrm{tr}(\rho^{\alpha}) + \Theta(r(\varepsilon_1 + \delta_1^{c}))\right) =: B.$$

By Lemma II.15 and introducing ε_2, we can obtain $\tilde{x}$ as an approximation of $\mathrm{tr}(A)$ with $Q_2 = O\left(\frac{\sqrt{B}}{\varepsilon_2} + \frac{1}{\sqrt{\varepsilon_2}}\right)$ queries to U such that $|\tilde{x} - \mathrm{tr}(A)| \leq \varepsilon_2$. Then we output $4\tilde{x}$ as an approximation of $\mathrm{tr}(\rho^{\alpha})$ by noting that

$$|4\tilde{x} - \mathrm{tr}(\rho^{\alpha})| \leq \Theta(\varepsilon_2 + r(\varepsilon_1 + \delta_1^{c})).$$

The number of queries to U_{ρ} is

$$\begin{aligned} (\beta + Q_1)Q_2 &= \tilde{O}\left(\left(\beta + \frac{1}{\delta_1}\right)\left(\frac{\sqrt{B}}{\varepsilon_2} + \frac{1}{\sqrt{\varepsilon_2}}\right)\right) \\ &= \tilde{O}\left(\frac{r^{1/c}}{\varepsilon^{1+1/c}}\right) \end{aligned}$$

by taking $\delta_1 = \tilde{\Theta}\left((\varepsilon/r)^{1/c}\right)$, $\varepsilon_1 = \tilde{\Theta}\left(\varepsilon/r\right)$ and $\varepsilon_2 = \tilde{\Theta}\left(\varepsilon\right)$. □

In the following, we are going to show how to estimate the quantum Rényi and Tsallis entropies based on Theorem III.7.

Theorem III.8 (Quantum Rényi Entropy): Suppose that

1) U_{ρ} is an $(n+n_{\rho})$-qubit unitary operator that prepares an n-qubit density operator ρ with $\mathrm{rank}(\rho) \leq r$.
2) n_{ρ} is a polynomial in n.

For $a \in (0,1) \cup (1,+\infty)$, there is a quantum algorithm that computes $S_{\alpha}^{R}(\rho)$ within additive error ε using Q queries to U_{ρ} and $Q \cdot \mathrm{poly}(n)$ elementary quantum gates, where

$$Q = \begin{cases} \tilde{O}\left(r^{\frac{3-\alpha^2}{2\alpha}} / \varepsilon^{\frac{3+\alpha}{2\alpha}}\right), & 0 < \alpha < 1, \\ O\left(r^{\alpha-1}/\varepsilon\right), & \alpha > 1 \wedge \alpha \text{ is odd}, \\ \tilde{O}\left(r^{\alpha-1+\alpha/\left\{\frac{\alpha-1}{2}\right\}} / \varepsilon^{1+1/\left\{\frac{\alpha-1}{2}\right\}}\right), & \text{otherwise}. \end{cases}$$

and $\{x\} = x - \lfloor x \rfloor$ is the decimal part of real number x.

Proof: We will discuss in cases as stated in the statement of this theorem.

Case 1: $0 < \alpha < 1$. In this case, $1 \leq \operatorname{tr}(\rho^\alpha) \leq r^{1-\alpha}$. By Theorem III.7, there is a quantum algorithm that outputs $1 \leq x \leq r^{1-\alpha}$ such that $|x - \operatorname{tr}(\rho^\alpha)| \leq \varepsilon'$. Then

$$\left|\frac{1}{1-\alpha}\ln(x) - S_\alpha^R(\rho)\right| \leq \Theta\left(\frac{\varepsilon'}{1-\alpha}\right).$$

Let $\varepsilon' = \Theta((1-\alpha)\varepsilon)$. The number of queries to U_ρ is

$$\tilde{O}\left(r^{\frac{3-\alpha^2}{2\alpha}}/\varepsilon'^{\frac{3+\alpha}{2\alpha}}\right) = \tilde{O}\left(r^{\frac{3-\alpha^2}{2\alpha}}/\varepsilon^{\frac{3+\alpha}{2\alpha}}\right).$$

Case 2: $\alpha > 1$. In this case, $r^{1-\alpha} \leq \operatorname{tr}(\rho^\alpha) \leq 1$. By Theorem III.7, there is a quantum algorithm that outputs $r^{1-\alpha} \leq x \leq 1$ such that $|x - \operatorname{tr}(\rho^\alpha)| \leq \varepsilon'$. Then

$$\left|\frac{1}{1-\alpha}\ln(x) - S_\alpha^R(\rho)\right| \leq \Theta\left(\frac{r^{\alpha-1}\varepsilon'}{\alpha-1}\right).$$

Let $\varepsilon' = \Theta((\alpha-1)r^{1-\alpha}\varepsilon)$.

Subcase 2.1: $\alpha > 1$ and α is an odd number. The number of queries to U_ρ is

$$O\left(\frac{\alpha}{\varepsilon'}\right) = O\left(\frac{r^{\alpha-1}}{\varepsilon}\right).$$

Subcase 2.2: $\alpha > 1$ and α is not an odd number. The number of queries to U_ρ is

$$\tilde{O}\left(\left(\alpha + (r/\varepsilon')^{1/\{\frac{\alpha-1}{2}\}}\right)/\varepsilon'\right) = \tilde{O}\left(r^{\alpha-1+\alpha/\{\frac{\alpha-1}{2}\}}/\varepsilon^{1+1/\{\frac{\alpha-1}{2}\}}\right).$$

□

Theorem III.9 (Quantum Tsallis Entropy): Suppose that

1) U_ρ is an $(n+n_\rho)$-qubit unitary operator that prepares an n-qubit density operator ρ with $\operatorname{rank}(\rho) \leq r$.
2) n_ρ is a polynomial in n.

For $\alpha \in (0,1) \cup (1,+\infty)$, there is a quantum algorithm that computes $S_\alpha^T(\rho)$ within additive error ε using Q queries to U_ρ and $Q \cdot \operatorname{poly}(n)$ elementary quantum gates, where

$$Q = \begin{cases} \tilde{O}\left(r^{\frac{3-\alpha^2}{2\alpha}}/\varepsilon^{\frac{3+\alpha}{2\alpha}}\right), & 0 < \alpha < 1, \\ O(1/\varepsilon), & \alpha > 1 \land \alpha \text{ is odd}, \\ \tilde{O}\left(r^{1/\{\frac{\alpha-1}{2}\}}/\varepsilon^{1+1/\{\frac{\alpha-1}{2}\}}\right), & \text{otherwise}. \end{cases}$$

and $\{x\} = x - \lfloor x \rfloor$ is the decimal part of real number x.

Proof: By Theorem III.7, there is a quantum algorithm that outputs $1 \leq x \leq r^{1-\alpha}$ such that $|x - \operatorname{tr}(\rho^\alpha)| \leq \varepsilon'$. Then

$$\left|\frac{x-1}{1-\alpha}\right| - S_\alpha^T(\rho) \leq \Theta\left(\frac{\varepsilon'}{|1-\alpha|}\right).$$

Let $\varepsilon' = \Theta(|1-\alpha|\,\varepsilon)$. We will discuss in three cases as stated in the statement of this theorem.

Case 1: $0 < \alpha < 1$. The number of queries to U_ρ is

$$\tilde{O}\left(r^{\frac{3-\alpha^2}{2\alpha}}/\varepsilon'^{\frac{3+\alpha}{2\alpha}}\right) = \tilde{O}\left(r^{\frac{3-\alpha^2}{2\alpha}}/\varepsilon^{\frac{3+\alpha}{2\alpha}}\right).$$

Case 2: $\alpha > 1$ and α is an odd number. The number of queries to U_ρ is

$$O\left(\frac{\alpha}{\varepsilon'}\right) = O\left(\frac{1}{\varepsilon}\right).$$

Case 3: $\alpha > 1$ and α is not an odd number. The number of queries to U_ρ is

$$\tilde{O}\left(\left(\alpha + (r/\varepsilon')^{1/\{\frac{\alpha-1}{2}\}}\right)/\varepsilon'\right) = \tilde{O}\left(r^{1/\{\frac{\alpha-1}{2}\}}/\varepsilon^{1+1/\{\frac{\alpha-1}{2}\}}\right).$$

□

We note that when $\alpha > 1$ is an odd number, the query complexities of our quantum algorithms for $\operatorname{tr}(\rho^\alpha)$ and $S_\alpha^T(\rho)$ do not depend on r. This result can be applied to computing the classical Tsallis entropy of a distribution $p : [N] \to [0,1]$. Suppose a quantum oracle U is given as

$$U|0\rangle = \sum_{i\in[N]} \sqrt{p(i)}\,|i\rangle. \tag{6}$$

For convenience, we assume that $N = 2^n$. This kind of quantum oracle is called "classical distribution with pure state preparation access". We start from the quantum state $|0\rangle_n |0\rangle_n$, and the algorithm for estimating the classical Tsallis entropy of p is as follows.

1) Apply U on the first part of the quantum state, then the state becomes
$$\sum_{i\in[N]} \sqrt{p(i)}\,|i\rangle_n |0\rangle_n.$$
2) Apply a CNOT gate with control qubit the j-th qubit of the first part and target qubit the j-th qubit of the second part for each $j \in [n]$, then the state becomes
$$\sum_{i\in[N]} \sqrt{p(i)}\,|i\rangle_n |i\rangle_n.$$
3) Note that if the second part of the quantum state after step 2 is traced out, it becomes a mixed quantum state (density operator)
$$\rho = \sum_{i\in[N]} p(i)\,|i\rangle\langle i|.$$
Apply the algorithm of Theorem III.9, we are able to obtain an estimation of the quantum Tsallis entropy $S_\alpha^T(\rho)$ (i.e., the classical α-Tsallis entropy of p) within additive error ε with $O(1/\varepsilon)$ queries to U and $O(1/\varepsilon \cdot \operatorname{poly}(n))$ elementary quantum gates.

Corollary III.10: For odd integer $\alpha > 1$, given the quantum oracle U to a probability distribution $p : [N] \to [0,1]$ as in Eq. (6), there is a quantum algorithm that computes the Tsallis entropy $S_\alpha^T(p)$ of p within additive error ε, using $O(1/\varepsilon)$ queries to U and $O(1/\varepsilon \cdot \operatorname{poly}(n))$ elementary quantum gates.

For integer $\alpha \geq 2$, according to [58] (see also [41]), there is a simple SWAP test like quantum circuit that outputs 0 and 1 with probability $(1 \pm \operatorname{tr}(\rho^\alpha))/2$, respectively, using α copies of ρ. With a straightforward statistical method, we can estimate $\operatorname{tr}(\rho^\alpha)$ within additive error ε by $O(1/\varepsilon^2)$ repetitions of that quantum circuit. Directly applying this method also implies a quantum algorithm, which computes the Tsallis entropy (both quantum and classical) within additive error ε, using $O(1/\varepsilon^2)$ queries to quantum oracles. Compare to this simple algorithm, our quantum algorithm (of Theorem III.9 and Corollary III.10) yields a quadratic speedup for odd $\alpha > 1$.

D. Lower Bounds

We establish lower bounds for estimating quantum entropies in the low-rank case, which are derived from known lower bounds for estimating entropies of classical distributions [59], [60].

Theorem III.11: Suppose U_ρ is a quantum oracle that prepares the density operator ρ (see Definition II.2), and $r = \operatorname{rank}(\rho)$. For $\alpha \geq 0$, any quantum algorithm that computes $S_\alpha^R(\rho)$ within additive error $\varepsilon = \Theta(1)$ requires $\Omega(Q(r))$ queries to U_ρ, where

$$Q(r) = \begin{cases} r^{1/3}, & \alpha = 0, \\ \max\{r^{1/7\alpha - o(1)}, r^{1/3}\}, & 0 < \alpha < 1, \\ \tilde{\Omega}(r^{1/2}), & \alpha = 1, \\ \max\{r^{\frac{1}{2} - \frac{1}{2\alpha}}, r^{1/3}\}, & \alpha > 1. \end{cases}$$

Proof: We obtain lower bounds from those for classical distributions. The quantum query model for classical distributions we adopt is called the "classical distribution with quantum query access", which is defined as follows. Suppose $p\colon [N] \to [0,1]$ is a probability distribution on $[N]$. The quantum oracle U is defined by a function $f\colon [S] \to [N]$ such that

$$U\left|s, 0\right\rangle = \left|s, f(s)\right\rangle$$

for $s \in [S]$ and $S \in \mathbb{N}$, satisfying

$$p(i) = \frac{1}{S}\left|\{s \in [S] : f(s) = i\}\right|$$

for $i \in [N]$. It is pointed out in [8] that we can easily construct a "purified quantum query access" oracle by preparing a uniform superposition through the Hadamard gates, and then makes a query to U. Therefore, all lower bounds in the "classical distribution with quantum query access" model also hold in the "purified quantum query access" model.

Let $B(N)$ be the lower bound for estimating the Rényi entropy. It is straightforward to see that if there is a quantum algorithm that computes the quantum Rényi entropy using $Q(r)$ queries to U_ρ, then with the same algorithm, we can compute the Rényi entropy of a probability distribution $p : [N] \to [0,1]$ using $Q(N)$ queries to the "classical distribution with quantum query access" oracle. Therefore, we have $Q(r) \geq B(r)$. Our claim immediately holds by taking the lower bounds of $B(N)$ given in [59] and [60]. □

IV. Quantum Distances

Distance measures of quantum states are quantum information quantities that indicate their closeness. Testing the closeness of quantum states is a basic problem in quantum property testing. Two of the most important distance measures of quantum states are the trace distance and fidelity.

In this section, we will provide quantum algorithms for computing them as well as their extensions. Section IV-A presents quantum algorithms for computing the trace distance and its extension. Section IV-B presents quantum algorithms for computing the fidelity and its extensions.

A. Trace Distance

The α-trace distance of two quantum states ρ and σ is defined by

$$T_\alpha(\rho, \sigma) = \operatorname{tr}\left(\left|\frac{\rho - \sigma}{2}\right|^\alpha\right).$$

Here, $T_1(\rho, \sigma) = T(\rho, \sigma)$ is the trace distance. The trace distance of two pure quantum states (i.e., quantum states of rank 1) can be computed directly from their fidelity, which can be solved by the SWAP test [102]. The closeness testing of the 1-, 2-, and 3-trace distances were studied in [8].

Our quantum algorithms for computing the α-trace distance are given as follows.

Theorem IV.1: Suppose that

1) U_ρ is an $(n + n_\rho)$-qubit unitary operator that prepares an n-qubit density operator ρ.
2) U_σ is an $(n + n_\sigma)$-qubit unitary operator that prepares an n-qubit density operator σ.
3) n_ρ and n_σ are polynomials in n.
4) $r = \max\{\operatorname{rank}(\rho), \operatorname{rank}(\sigma)\}$.

For $\alpha > 0$, there is a quantum algorithm that computes $T_\alpha(\rho, \sigma)$ within additive error ε using Q queries to both U_ρ and U_σ, and $Q \cdot \operatorname{poly}(n)$ elementary quantum gates, where

$$Q = \begin{cases} \tilde{O}(r^3/\varepsilon^4), & \alpha \equiv 0 \pmod 2 \\ \tilde{O}(r^{5/\alpha}/\varepsilon^{5/\alpha+1}), & 0 < \alpha < 1 \\ \tilde{O}\left(r^{3+1/\{\alpha/2\}}/\varepsilon^{4+1/\{\alpha/2\}}\right), & \text{otherwise} \end{cases}$$

and $\{\beta\} = \beta - \lfloor \beta \rfloor$.

Especially, taking $\alpha = 1$, we obtain a quantum algorithm for trace distance estimation using $\tilde{O}(r^5/\varepsilon^6)$ queries to U_ρ and U_σ.

The key observation of our quantum algorithm is that

$$\begin{aligned} T_\alpha(\rho, \sigma) &= \operatorname{tr}\left(\left|\frac{\rho - \sigma}{2}\right|^\alpha\right) \\ &= \operatorname{tr}\left(\left|\frac{\rho - \sigma}{2}\right|^{\alpha/2} \Pi_{\operatorname{supp}(\mu)} \left|\frac{\rho - \sigma}{2}\right|^{\alpha/2}\right), \end{aligned}$$

where $\mu = (\rho + \sigma)/2$, $\operatorname{supp}(\mu)$ is the support of μ and Π_S is the projector onto a subspace S. A straightforward idea is to first prepare a subnormalized density operator that is a block-encoding of $\Pi_{\operatorname{supp}(\mu)}$, and then prepare another subnormalized density operator that is a block-encoding of $\left|\nu\right|^{\alpha/2} \Pi_{\operatorname{supp}(\mu)} \left|\nu\right|^{\alpha/2}$ by the evolution of subnormalized density operators (Lemma II.2), where $\nu = (\rho - \sigma)/2$. However, we are only able to prepare subnormalized density operator that is a block-encoding of a projector onto a truncated support by Lemma II.19. In this way, we can prepare a subnormalized density operator $\left|\nu\right|^{\alpha/2} \Pi_{\operatorname{supp}_\delta(\mu)} \left|\nu\right|^{\alpha/2}$ for some $\delta > 0$, instead of $\left|\nu\right|^{\alpha/2} \Pi_{\operatorname{supp}(\mu)} \left|\nu\right|^{\alpha/2}$.

When δ is fixed, the inherent error of this approach is

Proposition IV.2:

$$\begin{aligned} \left|\operatorname{tr}\left(\left|\nu\right|^{\alpha/2} \Pi_{\operatorname{supp}(\mu)} \left|\nu\right|^{\alpha/2}\right) - \operatorname{tr}\left(\left|\nu\right|^{\alpha/2} \Pi_{\operatorname{supp}_\delta(\mu)} \left|\nu\right|^{\alpha/2}\right)\right| \\ \leq 2\, r\delta^{\min\{\alpha,1\}/2}. \end{aligned}$$

Proof: Let $\mu = \sum_j \lambda_j |\psi_j\rangle \langle \psi_j|$, where $\lambda_j \in [0,1]$ and $\sum_j \lambda_j = 1$. Then $\| |\nu| |\psi_j\rangle \| \leq \sqrt{\lambda_j}$. This is seen by the following.

$$\begin{aligned}
\| |\rho - \sigma| |\psi_j\rangle \|^2 &= \langle \psi_j| (\rho-\sigma)^2 |\psi_j\rangle \\
&= \langle \psi_j| \rho^2 |\psi_j\rangle + \langle \psi_j| \sigma^2 |\psi_j\rangle \\
&\quad - \langle \psi_j| (\rho\sigma + \sigma\rho) |\psi_j\rangle \\
&\leq \langle \psi_j| \rho^2 |\psi_j\rangle + \langle \psi_j| \sigma^2 |\psi_j\rangle \\
&\quad + |\langle \psi_j| \rho\sigma |\psi_j\rangle| + |\langle \psi_j| \sigma\rho |\psi_j\rangle| \\
&\leq \langle \psi_j| \rho^2 |\psi_j\rangle + \langle \psi_j| \sigma^2 |\psi_j\rangle \\
&\quad + 2 \|\rho |\psi_j\rangle\| \|\sigma |\psi_j\rangle\| \\
&= \langle \psi_j| \rho^2 |\psi_j\rangle + \langle \psi_j| \sigma^2 |\psi_j\rangle \\
&\quad + 2\sqrt{\langle \psi_j| \rho^2 |\psi_j\rangle \langle \psi_j| \sigma^2 |\psi_j\rangle} \\
&\leq 2 \left(\langle \psi_j| \rho^2 |\psi_j\rangle + \langle \psi_j| \sigma^2 |\psi_j\rangle \right) \\
&\leq 2 \left(\langle \psi_j| \rho |\psi_j\rangle + \langle \psi_j| \sigma |\psi_j\rangle \right) \\
&= 4 \langle \psi_j| \mu |\psi_j\rangle \\
&\leq 4 \|\mu |\psi_j\rangle\| \\
&= 4\lambda_j.
\end{aligned}$$

Note that

$$\begin{aligned}
&\left| \operatorname{tr}\left(|\nu|^{\alpha/2} \Pi_{\mathrm{supp}(\mu)} |\nu|^{\alpha/2} \right) - \operatorname{tr}\left(|\nu|^{\alpha/2} \Pi_{\mathrm{supp}_\delta(\mu)} |\nu|^{\alpha/2} \right) \right| \\
&\qquad = \operatorname{tr}\left(\left(\Pi_{\mathrm{supp}(\mu)} - \Pi_{\mathrm{supp}_\delta(\mu)} \right) |\nu|^{\alpha} \right).
\end{aligned}$$

Then for $\alpha \geq 1$, we have

$$\begin{aligned}
\operatorname{tr}\left(\left(\Pi_{\mathrm{supp}(\mu)} - \Pi_{\mathrm{supp}_\delta(\mu)} \right) |\nu|^{\alpha} \right) &= \sum_{0<\lambda_j<\delta} \langle \psi_j| |\nu|^{\alpha} |\psi_j\rangle \\
&\leq \sum_{0<\lambda_j<\delta} \langle \psi_j| |\nu| |\psi_j\rangle \\
&\leq \sum_{0<\lambda_j<\delta} \| |\nu| |\psi_j\rangle \| \\
&\leq \sum_{0<\lambda_j<\delta} \sqrt{\lambda_j} \\
&\leq \sqrt{\delta}\, \mathrm{rank}(\mu) \\
&\leq 2\, r\sqrt{\delta}.
\end{aligned}$$

Before deriving bounds for $0 < \alpha < 1$, we need the following lemma.

Lemma IV.3: Suppose that A is an n-dimensional positive semidefinite operator, $|\psi\rangle$ is an n-dimensional vector, and $0 < \alpha < 1$. Then

$$\| A^{\alpha} |\psi\rangle \| \leq \| A |\psi\rangle \|^{\alpha} \| |\psi\rangle \|^{1-\alpha}.$$

Proof: Let

$$A = \sum_{j=1}^{n} \lambda_j |\psi_j\rangle \langle \psi_j|,$$

where $\{|\psi_j\rangle\}$ is an orthonormal basis, and $\lambda_j \geq 0$ for all $1 \leq j \leq n$. Let

$$|\psi\rangle = \sum_{j=1}^{n} \beta_j |\psi_j\rangle.$$

By Hölder's inequality, we have

$$\begin{aligned}
\| A^{\alpha} |\psi\rangle \|^2 &= \sum_{j=1}^{n} \left| \lambda_j^{\alpha} \beta_j \right|^2 \\
&= \sum_{j=1}^{n} \left| \lambda_j^{2\alpha} \beta_j^{2\alpha} \right| \cdot \left| \beta_j^{2(1-\alpha)} \right| \\
&\leq \left(\sum_{j=1}^{n} \left| \lambda_j^{2\alpha} \beta_j^{2\alpha} \right|^{1/\alpha} \right)^{\alpha} \\
&\qquad \left(\sum_{j=1}^{n} \left| \beta_j^{2(1-\alpha)} \right|^{1/(1-\alpha)} \right)^{1-\alpha} \\
&= \left(\sum_{j=1}^{n} |\lambda_j \beta_j|^2 \right)^{\alpha} \left(\sum_{j=1}^{n} |\beta_j|^2 \right)^{1-\alpha} \\
&= \| A |\psi\rangle \|^{2\alpha} \| |\psi\rangle \|^{2(1-\alpha)}.
\end{aligned}$$

□

For $0 < \alpha < 1$, by Lemma IV.3, we have

$$\begin{aligned}
&\operatorname{tr}\left(\left(\Pi_{\mathrm{supp}(\mu)} - \Pi_{\mathrm{supp}_\delta(\mu)} \right) |\nu|^{\alpha} \right) \\
&\quad = \sum_{0<\lambda_j<\delta} \langle \psi_j| |\nu|^{\alpha} |\psi_j\rangle \\
&\quad \leq \sum_{0<\lambda_j<\delta} \| |\nu|^{\alpha} |\psi_j\rangle \| \\
&\quad \leq \sum_{0<\lambda_j<\delta} \| |\nu| |\psi_j\rangle \|^{\alpha} \| |\psi_j\rangle \|^{1-\alpha} \\
&\quad \leq \sum_{0<\lambda_j<\delta} \lambda_j^{\alpha/2} \\
&\quad \leq 2\, r\delta^{\alpha/2}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\left| \operatorname{tr}\left(|\nu|^{\alpha/2} \Pi_{\mathrm{supp}(\mu)} |\nu|^{\alpha/2} \right) - \operatorname{tr}\left(|\nu|^{\alpha/2} \Pi_{\mathrm{supp}_\delta(\mu)} |\nu|^{\alpha/2} \right) \right| \\
&\qquad \leq 2\, r\delta^{\min\{\alpha,1\}/2}.
\end{aligned}$$

□

Hence, we could obtain a reasonable error by setting δ small enough.

Step 1: By Lemma II.17 with the Hadamard gate

$$H|0\rangle = \sqrt{\frac{1}{2}} |0\rangle + \sqrt{\frac{1}{2}} |1\rangle,$$

we obtain an $O(n + n_\rho + n_\sigma)$-qubit unitary operator U_μ that prepares density operator $\mu = (\rho+\sigma)/2$, using 1 query to U_ρ and U_σ, and $O(1)$ elementary quantum gates.

Introducing three parameters $\delta_1, \varepsilon_1, \delta_Q \in (0, \frac{1}{10}]$, by Lemma II.19, there is a quantum circuit U_1, which prepares a subnormalized density operator A_1 and A_1 is a $(1, 0, \delta_Q)$-block-encoding of Π_1, where

$$\begin{aligned}
\left(\frac{\delta_1}{4}(1 - 2\varepsilon_1) - \delta_1^{1/2}\varepsilon_1 \right) \Pi_{\mathrm{supp}_{2\delta_1}(\mu)} &\leq \Pi_1 \\
&\leq \left(\frac{\delta_1}{4} + \varepsilon_1^2 + \delta_1^{1/2}\varepsilon_1 \right) \Pi_{\mathrm{supp}(\mu)}.
\end{aligned}$$

Here, U_1 uses Q_1 queries to U_μ and $O(Q_1(n+n_\rho+n_\sigma))$ elementary quantum gates, where $Q_1 = O\left(\frac{1}{\delta_1}\log\left(\frac{1}{\varepsilon_1}\right)\right)$. Moreover, U_1 can be computed by a classical Turing machine in $\operatorname{poly}\left(Q_1, \log\left(\frac{1}{\delta_Q}\right)\right)$ time.

Next, we are going to construct a unitary operator that is a block-encoding of $|\nu|^{\alpha/2}$. By Lemma II.1, there are two unitary operators V_σ and V_ρ which are a $(1, n+n_\sigma, 0)$-block-encoding of σ and a $(1, n+n_\rho, 0)$-block-encoding of ρ, respectively. Here, V_σ uses 1 query to each of U_σ and $U_\sigma^\dagger$ and n_σ elementary quantum gates, and V_ρ uses 1 query to each of U_ρ and $U_\rho^\dagger$ and n_ρ elementary quantum gates. Let $n' = \max(n_\rho, n_\sigma)$, then $V_\rho \otimes I_{n'-n_\rho}$ and $V_\sigma \otimes I_{n'-n_\sigma}$ are $(1, n+n', 0)$-block-encodings of ρ and σ, respectively. According to Definition II.3, we note that (HX, H) is a $(2,1,0)$-state-preparation-pair for $y = (1,-1)$, where H is the Hadamard gate and X is the Pauli matrix. By Theorem II.18, there is a $(2n+n'+1)$-qubit quantum circuit W which is a $(1, n+n'+1, 0)$-block-encoding of $\nu = (\rho-\sigma)/2$, using 1 query to each of V_ρ and V_σ and $O(1)$ elementary quantum gates.

Now we analyze the error if we replace $\Pi_{\operatorname{supp}(\mu)}$ by $4\delta_1^{-1}\Pi_1$ in the following.

Proposition IV.4:

$$\left|\operatorname{tr}\left(|\nu|^{\alpha/2}\left(4\delta_1^{-1}\Pi_1\right)|\nu|^{\alpha/2}\right) - T_\alpha(\rho,\sigma)\right| \\ \leq \begin{cases} \Theta\left(\varepsilon_1\delta_1^{-1/2} + r\delta_1^{1/2}\right), & \alpha \geq 1, \\ \Theta\left(r^{1-\alpha}\varepsilon_1\delta_1^{-1/2} + r\delta_1^{\alpha/2}\right), & 0 < \alpha < 1. \end{cases}$$

Proof: Note that $\Pi_L \leq 4\delta_1^{-1}\Pi_1 \leq \Pi_U$, where

$$\Pi_L = \left(1 - 2\varepsilon_1 - 4\varepsilon_1\delta_1^{-1/2}\right)\Pi_{\operatorname{supp}_{2\delta_1}(\mu)},$$
$$\Pi_U = \left(1 + 4\varepsilon_1^2\delta_1^{-1} + 4\varepsilon_1\delta_1^{-1/2}\right)\Pi_{\operatorname{supp}(\mu)}.$$

This leads to

$$f(\Pi_L) \leq f\left(4\delta_1^{-1}\Pi_1\right) \leq f(\Pi_U),$$

where $f(\Pi) = \operatorname{tr}\left(|\nu|^{\alpha/2}\,\Pi\,|\nu|^{\alpha/2}\right)$ for convenience. Therefore,

$$\left|f\left(4\delta_1^{-1}\Pi_1\right) - f\left(\Pi_{\operatorname{supp}(\mu)}\right)\right| \leq \max\{T_L, T_U\},$$

where

$$T_L = \left|f\left(\Pi_L\right) - f\left(\Pi_{\operatorname{supp}(\mu)}\right)\right|,$$
$$T_U = \left|f\left(\Pi_U\right) - f\left(\Pi_{\operatorname{supp}(\mu)}\right)\right|.$$

By Proposition IV.2, we have

$$\begin{aligned} T_L &\leq \left|f\left(\Pi_L\right) - f\left(\Pi_{\operatorname{supp}_{2\delta_1}(\mu)}\right)\right| \\ &\quad + \left|f\left(\Pi_{\operatorname{supp}_{2\delta_1}(\mu)}\right) - f\left(\Pi_{\operatorname{supp}(\mu)}\right)\right| \\ &\leq f\left(\left(2\varepsilon_1 + 4\varepsilon_1\delta_1^{-1/2}\right)\Pi_{\operatorname{supp}_{2\delta_1}(\mu)}\right) + 2\ r(2\delta_1)^{\min\{\alpha,1\}/2} \\ &\leq \Theta\left(\varepsilon_1\delta_1^{-1/2}T_\alpha(\rho,\sigma) + r\delta_1^{\min\{\alpha,1\}/2}\right). \end{aligned}$$

Also we have

$$\begin{aligned} T_U &\leq f\left(\left(4\varepsilon_1^2\delta_1^{-1} + 4\varepsilon_1\delta_1^{-1/2}\right)\Pi_{\operatorname{supp}(\mu)}\right) \\ &\leq \Theta\left(\varepsilon_1\delta_1^{-1/2}T_\alpha(\rho,\sigma)\right). \end{aligned}$$

Combining the both, we have

$$\begin{aligned} &\left|f\left(4\delta_1^{-1}\Pi_1\right) - f\left(\Pi_{\operatorname{supp}(\mu)}\right)\right| \\ &\qquad \leq \Theta\left(\varepsilon_1\delta_1^{-1/2}T_\alpha(\rho,\sigma) + r\delta_1^{\min\{\alpha,1\}/2}\right). \end{aligned}$$

We note that $T_\alpha(\rho,\sigma) \leq 1$ if $\alpha \geq 1$, and $T_\alpha(\rho,\sigma) \leq (2r)^{1-\alpha}$ if $0 < \alpha < 1$. These yield the claim. □

In the following, we separately consider different cases of α.

Case 1 (α Is an Even Integer):

Step 2: By Lemma II.12, there is a unitary operator $W_{\alpha/2}$, which is a $(1, O(\alpha(n+n')), 0)$-block-encoding of $|\nu|^{\alpha/2}$, using $\alpha/2$ queries to W. By Lemma II.2, using 1 query to each of $W_{\alpha/2}$ and U_1, we obtain a quantum circuit $\tilde{U}$, which prepares a subnormalized density operator $|\nu|^{\alpha/2}A_1|\nu|^{\alpha/2}$. We note that

$$\left\||\nu|^{\alpha/2}A_1|\nu|^{\alpha/2} - |\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2}\right\| \leq \|A_1 - \Pi_1\| \leq \delta_Q.$$

Step 3: Introducing a parameter ε_3, by Lemma II.15, we can compute $\tilde{p}$ that estimates $\operatorname{tr}(|\nu|^{\alpha/2}A_1|\nu|^{\alpha/2})$ such that $\left|\tilde{p} - \operatorname{tr}(|\nu|^{\alpha/2}A_1|\nu|^{\alpha/2})\right| \leq \varepsilon_3$ with $O\left(\frac{\sqrt{B}}{\varepsilon_3} + \frac{1}{\sqrt{\varepsilon_3}}\right)$ queries to $\tilde{U}$, where $B = \Theta\left(\delta_1 + \varepsilon_1^2 + \delta_1^{1/2}\varepsilon_1 + r\delta_Q\right)$ is an upper bound for $\operatorname{tr}(|\nu|^{\alpha/2}A_1|\nu|^{\alpha/2})$. Note that

$$\begin{aligned} \operatorname{tr}(|\nu|^{\alpha/2}A_1|\nu|^{\alpha/2}) &\leq \operatorname{tr}\left(|\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2}\right) + \Theta\left(r\delta_Q\right) \\ &\leq \Theta\left(\delta_1 + \varepsilon_1^2 + \delta_1^{1/2}\varepsilon_1 + r\delta_Q\right). \end{aligned}$$

Step 4: Output $4\delta_1^{-1}\tilde{p} \approx T_\alpha(\rho,\sigma)$ as the estimation. The additive error is

$$\begin{aligned} &\left|4\delta_1^{-1}\tilde{p} - T_\alpha(\rho,\sigma)\right| \\ &\leq 4\delta_1^{-1}\left|\tilde{p} - \operatorname{tr}(|\nu|^{\alpha/2}A_1|\nu|^{\alpha/2})\right| \\ &\quad + 4\delta_1^{-1}\left|\operatorname{tr}(|\nu|^{\alpha/2}A_1|\nu|^{\alpha/2}) - \operatorname{tr}(|\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2})\right| \\ &\quad + \left|\operatorname{tr}\left(|\nu|^{\alpha/2}\left(4\delta_1^{-1}\Pi_1\right)|\nu|^{\alpha/2}\right)\right. \\ &\qquad \left. - \operatorname{tr}\left(|\nu|^{\alpha/2}\Pi_{\operatorname{supp}(\mu)}|\nu|^{\alpha/2}\right)\right| \\ &\leq \Theta\left(r\delta_1^{1/2} + \varepsilon_1\delta_1^{-1/2} + \delta_1^{-1}(\varepsilon_3 + r\delta_Q)\right). \end{aligned}$$

In order to make $\left|4\delta_1^{-1}\tilde{p} - T_\alpha(\rho,\sigma)\right| \leq \varepsilon$, it is sufficient to let $\delta_1 = \Theta(\varepsilon^2/r^2)$, $\varepsilon_3 = \Theta(\varepsilon^3/r^2)$, and other parameters become small enough polynomials in r and $1/\varepsilon$. Under these conditions, the number of queries to U_ρ and U_σ is

$$Q = O\left(Q_1\alpha\left(\frac{\sqrt{B}}{\varepsilon_3} + \frac{1}{\sqrt{\varepsilon_3}}\right)\right) = \tilde{O}\left(\frac{r^3}{\varepsilon^4}\right),$$

and the number of elementary quantum gates is $O(Q \cdot \operatorname{poly}(n))$.

Case 2 ($\alpha \geq 1$ and α Is Not an Even Integer):

Step 2: Now introducing two parameters $\delta_2, \varepsilon_2 \in (0, \frac{1}{4}]$, by Lemma II.13, there is a quantum circuit $W_{\{\alpha/2\}}$ that is a $(1, O(n+n'), 0)$-block-encoding of A_2, and A_2 is a $(2, 0, \Theta(\varepsilon_2 + \delta_2^{\{\alpha/2\}}))$-block-encoding of $|\nu|^{\{\alpha/2\}}$, using

Q_2 queries to W and $O\left(Q_2(n+n')\right)$ elementary quantum gates, where $Q_2 = O\left(\frac{1}{\delta_2}\log\left(\frac{1}{\varepsilon_2}\right)\right)$. By Lemma II.12, there is a unitary operator $W_{\lfloor\alpha/2\rfloor}$, which is a $(1, O(\alpha(n+n')), 0)$-block-encoding of $|\nu|^{\lfloor\alpha/2\rfloor}$, using $\lfloor\alpha/2\rfloor$ queries to W. Again by Lemma II.12, there is a unitary operator $W_{\alpha/2}$, which is a $(2, O(\alpha(n+n')), \Theta(\varepsilon_2+\delta_2^{\{\alpha/2\}}))$-block-encoding of $|\nu|^{\alpha/2}$, using 1 query to $W_{\{\alpha/2\}}$ and 1 query to $W_{\lfloor\alpha/2\rfloor}$. By Lemma II.2, using 1 query to each of $W_{\alpha/2}$ and U_1, we obtain a quantum circuit $\tilde{U}$, which prepares a subnormalized density operator $A_2A_1A_2^\dagger$. We note that

$$\begin{aligned}
&\left\|A_2A_1A_2^\dagger - \frac{1}{4}|\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2}\right\| \\
&\leq \left\|A_2A_1A_2^\dagger - A_2\Pi_1A_2^\dagger\right\| + \left\|A_2\Pi_1A_2^\dagger - \frac{1}{4}|\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2}\right\| \\
&\leq \|A_1-\Pi_1\| + \left\|A_2 - \frac{1}{2}|\nu|^{\alpha/2}\right\|\|\Pi_1\|\left\|A_2^\dagger\right\| \\
&\quad + \left\|A_2^\dagger - \frac{1}{2}|\nu|^{\alpha/2}\right\|\|\Pi_1\|\left\|\frac{1}{2}|\nu|^{\alpha/2}\right\| \\
&\leq \Theta\left(\delta_Q + (\delta_1+\varepsilon_1^2+\delta_1^{1/2}\varepsilon_1)(\varepsilon_2+\delta_2^{\{\alpha/2\}})\right).
\end{aligned}$$

Step 3: Introducing a parameter ε_3, by Lemma II.15, we can compute $\tilde{p}$ that estimates $\operatorname{tr}(A_2A_1A_2^\dagger)$ such that

$$\left|\tilde{p} - \operatorname{tr}(A_2A_1A_2^\dagger)\right| \leq \varepsilon_3$$

with $O\left(\frac{\sqrt{B}}{\varepsilon_3} + \frac{1}{\sqrt{\varepsilon_3}}\right)$ queries to $\tilde{U}$, where

$$B = \Theta\left((\delta_1+\varepsilon_1^2+\delta_1^{1/2}\varepsilon_1)(1+r(\varepsilon_2+\delta_2^{\{\alpha/2\}})) + r\delta_Q\right)$$

is an upper bound for $\operatorname{tr}(A_2A_1A_2^\dagger)$. Note that

$$\begin{aligned}
&\operatorname{tr}(A_2A_1A_2^\dagger) \\
&\leq \operatorname{tr}\left(\frac{1}{4}|\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2}\right) \\
&\qquad + \Theta\left(r\left(\delta_Q + (\delta_1+\varepsilon_1^2+\delta_1^{1/2}\varepsilon_1)(\varepsilon_2+\delta_2^{\{\alpha/2\}})\right)\right) \\
&\leq \Theta\left((\delta_1+\varepsilon_1^2+\delta_1^{1/2}\varepsilon_1)(1+r(\varepsilon_2+\delta_2^{\{\alpha/2\}})) + r\delta_Q\right).
\end{aligned}$$

Step 4: Output $4\delta_1^{-1}\tilde{p} \approx T_\alpha(\rho,\sigma)$ as the estimation. The additive error is

$$\begin{aligned}
&\left|4\delta_1^{-1}\tilde{p} - T_\alpha(\rho,\sigma)\right| \\
&\leq 4\delta_1^{-1}\left|\tilde{p} - \operatorname{tr}(A_2A_1A_2^\dagger)\right| \\
&\qquad + 4\delta_1^{-1}\left|\operatorname{tr}(A_2A_1A_2^\dagger) - \operatorname{tr}(|\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2})\right| \\
&\qquad + \left|\operatorname{tr}\left(|\nu|^{\alpha/2}\left(4\delta_1^{-1}\Pi_1\right)|\nu|^{\alpha/2}\right)\right. \\
&\qquad\qquad \left. - \operatorname{tr}\left(|\nu|^{\alpha/2}\Pi_{\operatorname{supp}(\mu)}|\nu|^{\alpha/2}\right)\right| \\
&\leq \Theta\Big(r\delta_1^{1/2} + \varepsilon_1\delta_1^{-1/2} + r(\varepsilon_2+\delta_2^{\{\alpha/2\}})(1+\varepsilon_1\delta_1^{-1/2}) \\
&\qquad + \delta_1^{-1}(\varepsilon_3+r\delta_Q)\Big).
\end{aligned}$$

In order to make $\left|4\delta_1^{-1}\tilde{p} - T_\alpha(\rho,\sigma)\right| \leq \varepsilon$, it is sufficient to let $\delta_1 = \Theta(\varepsilon^2/r^2)$, $\delta_2 = \Theta((\varepsilon/r)^{1/\{\alpha/2\}})$, $\varepsilon_3 = \Theta(\varepsilon^3/r^2)$, and other parameters become small enough polynomials in r and $1/\varepsilon$. Under these conditions, the number of queries to U_ρ and U_σ is

$$\begin{aligned}
Q &= O\left(Q_1(Q_2+\alpha)\left(\frac{\sqrt{B}}{\varepsilon_3} + \frac{1}{\sqrt{\varepsilon_3}}\right)\right) \\
&= \tilde{O}\left(\frac{r^{3+1/\{\alpha/2\}}}{\varepsilon^{4+1/\{\alpha/2\}}}\right),
\end{aligned}$$

and the number of elementary quantum gates is $O(Q \cdot \operatorname{poly}(n))$.

Case 3 ($\mathbf{0 < \alpha < 1}$):

Step 2: Introducing two parameters $\delta_2, \varepsilon_2 \in (0, \frac{1}{4}]$, by Lemma II.13, there is a quantum circuit $W_{\alpha/2}$ that is a $(1, O(n+n'), 0)$-block-encoding of A_2, and A_2 is a $(2, 0, \Theta(\varepsilon_2+\delta_2^{\alpha/2}))$-block-encoding of $|\nu|^{\alpha/2}$, using Q_2 queries to W and $O\left(Q_2(n+n')\right)$ elementary quantum gates, where $Q_2 = O\left(\frac{1}{\delta_2}\log\left(\frac{1}{\varepsilon_2}\right)\right)$. By Lemma II.2, using 1 query to each of $W_{\alpha/2}$ and U_1, we obtain a quantum circuit $\tilde{U}$, which prepares a subnormalized density operator $A_2A_1A_2^\dagger$. We note that

$$\begin{aligned}
&\left\|A_2A_1A_2^\dagger - \frac{1}{4}|\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2}\right\| \\
&\leq \left\|A_2A_1A_2^\dagger - A_2\Pi_1A_2^\dagger\right\| \\
&\qquad + \left\|A_2\Pi_1A_2^\dagger - \frac{1}{4}|\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2}\right\| \\
&\leq \|A_1-\Pi_1\| + \left\|A_2 - \frac{1}{2}|\nu|^{\alpha/2}\right\|\|\Pi_1\|\left\|A_2^\dagger\right\| \\
&\qquad + \left\|A_2^\dagger - \frac{1}{2}|\nu|^{\alpha/2}\right\|\|\Pi_1\|\left\|\frac{1}{2}|\nu|^{\alpha/2}\right\| \\
&\leq \Theta\left(\delta_Q + (\delta_1+\varepsilon_1^2+\delta_1^{1/2}\varepsilon_1)(\varepsilon_2+\delta_2^{\alpha/2})\right).
\end{aligned}$$

Step 3: Introducing a parameter ε_3, by Lemma II.15, we can compute $\tilde{p}$ that estimates $\operatorname{tr}(A_2A_1A_2^\dagger)$ such that

$$\left|\tilde{p} - \operatorname{tr}(A_2A_1A_2^\dagger)\right| \leq \varepsilon_3$$

with $O\left(\frac{\sqrt{B}}{\varepsilon_3} + \frac{1}{\sqrt{\varepsilon_3}}\right)$ queries to $\tilde{U}$, where

$$B = \Theta\left(r^{1-\alpha}\delta_1 + r(\delta_1+\varepsilon_1^2+\delta_1^{1/2}\varepsilon_1)(\varepsilon_2+\delta_2^{\alpha/2}) + r\delta_Q\right)$$

is an upper bound for $\operatorname{tr}(A_2A_1A_2^\dagger)$. Note that

$$\begin{aligned}
&\operatorname{tr}(A_2A_1A_2^\dagger) \\
&\leq \operatorname{tr}\left(\frac{1}{4}|\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2}\right) \\
&\qquad + \Theta\left(r\left(\delta_Q + (\delta_1+\varepsilon_1^2+\delta_1^{1/2}\varepsilon_1)(\varepsilon_2+\delta_2^{\alpha/2})\right)\right) \\
&\leq \Theta\left(r^{1-\alpha}\delta_1 + r(\delta_1+\varepsilon_1^2+\delta_1^{1/2}\varepsilon_1)(\varepsilon_2+\delta_2^{\alpha/2}) + r\delta_Q\right).
\end{aligned}$$

Step 4: Output $4\delta_1^{-1}\tilde{p} \approx T_\alpha(\rho,\sigma)$ as the estimation. The additive error is

$$\begin{aligned}
&\left|4\delta_1^{-1}\tilde{p} - T_\alpha(\rho,\sigma)\right| \\
&\leq 4\delta_1^{-1}\left|\tilde{p} - \operatorname{tr}(A_2A_1A_2^\dagger)\right| \\
&\qquad + 4\delta_1^{-1}\left|\operatorname{tr}(A_2A_1A_2^\dagger) - \operatorname{tr}(|\nu|^{\alpha/2}\Pi_1|\nu|^{\alpha/2})\right|
\end{aligned}$$

$$\begin{aligned}&+\left|\operatorname{tr}\left(|\nu|^{\alpha/2}\left(4\delta_1^{-1}\Pi_1\right)|\nu|^{\alpha/2}\right)\right.\\&\qquad\left.-\operatorname{tr}\left(|\nu|^{\alpha/2}\,\Pi_{\mathrm{supp}(\mu)}\,|\nu|^{\alpha/2}\right)\right|\\&\le\Theta\Big(r\delta_1^{\alpha/2}+r^{1-\alpha}\varepsilon_1\delta_1^{-1/2}+r(\varepsilon_2+\delta_2^{\alpha/2})(1+\varepsilon_1\delta_1^{-1/2})\\&\qquad+\delta_1^{-1}(\varepsilon_3+r\delta_Q)\Big).\end{aligned}$$

In order to make $\left|4\delta_1^{-1}\tilde{p}-T_\alpha(\rho,\sigma)\right|\le\varepsilon$, it is sufficient to let $\delta_1=\Theta((\varepsilon/r)^{2/\alpha})$, $\delta_2=\Theta((\varepsilon/r)^{2/\alpha})$, $\varepsilon_3=\Theta(\varepsilon^{2/\alpha+1}/r^{2/\alpha})$, and other parameters become small enough polynomials in r and $1/\varepsilon$. Under these conditions, the number of queries to U_ρ and U_σ is

$$Q=O\left(Q_1Q_2\left(\frac{\sqrt{B}}{\varepsilon_3}+\frac{1}{\sqrt{\varepsilon_3}}\right)\right)=\tilde{O}\left(\frac{r^{5/\alpha+(1-\alpha)/2}}{\varepsilon^{5/\alpha+1}}\right),$$

and the number of elementary quantum gates is $O(Q\cdot\mathrm{poly}(n))$.

B. Fidelity

Quantum fidelity estimation is a problem to compute the fidelity of two mixed quantum states given their purifications. The well-known SWAP test [102] can solve this problem when one of the quantum states is pure. Recently, a polynomial-time quantum algorithm was proposed in [11] for the case that one of the quantum states is low-rank. However, their algorithm has very large exponents of r (rank) and ε (additive error) in the complexity. Here, we are able to improve the complexity with much smaller exponents, compared to the $\tilde{O}(r^{12.5}/\varepsilon^{13.5})$ quantum algorithm for fidelity estimation proposed by [11].

In addition, the sandwiched quantum Rényi relative entropy $D_\alpha(\rho\|\sigma)$ [48], [49] is a generalization of quantum state measures, defined by

$$F_\alpha(\rho,\sigma)=\exp\left((\alpha-1)D_\alpha(\rho\|\sigma)\right)=\operatorname{tr}\left(\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right).$$

Here, $F_{1/2}(\rho,\sigma)=F(\rho,\sigma)$ is the quantum state fidelity. It is clear that $0\le F_\alpha(\rho,\sigma)\le 1$ for $\alpha\in(0,1)$ (see [48]). Recently, the sandwiched quantum Rényi relative entropy is used in quantum machine learning [103].

Our quantum algorithms for computing the α-fidelity are given as follows.

Theorem IV.5: Suppose that

1) U_ρ is an $(n+n_\rho)$-qubit unitary operator that prepares an n-qubit density operator ρ with $\mathrm{rank}(\rho)=r$.
2) U_σ is an $(n+n_\sigma)$-qubit unitary operator that prepares an n-qubit density operator σ.
3) n_ρ and n_σ are polynomials in n.

For $\alpha\in(0,1)$, there is a quantum algorithm that computes $F_\alpha(\rho,\sigma)$ within additive error ε, using $\tilde{O}\left(r^{\frac{3-\alpha}{2\alpha}}/\varepsilon^{\frac{3+\alpha}{2\alpha}}\right)$ queries to U_ρ, Q queries to U_σ, and $Q\cdot\mathrm{poly}(n)$ elementary quantum gates, where

$$Q=\begin{cases}\tilde{O}\left(r^{\frac{3-\alpha}{2\alpha}}/\varepsilon^{\frac{3+\alpha}{2\alpha}}\right), & \beta\in\mathbb{N},\\ \tilde{O}\left(r^{\frac{3-\alpha}{2\alpha}+\frac{1}{\alpha\{\beta\}}}/\varepsilon^{\frac{3+\alpha}{2\alpha}+\frac{1}{\alpha\{\beta\}}}\right), & \beta\notin\mathbb{N},\end{cases}$$

and $\beta=(1-\alpha)/2\alpha$, $\{\beta\}=\beta-\lfloor\beta\rfloor$.

Especially, taking $\alpha=\frac{1}{2}$, we obtain a quantum algorithm for fidelity estimation using $\tilde{O}\left(r^{2.5}/\varepsilon^{3.5}\right)$ queries to U_ρ and $\tilde{O}\left(r^{6.5}/\varepsilon^{7.5}\right)$ queries to U_σ.

We put the detailed proofs into the following subsubsections. In fact, such techniques used in estimating the relative sandwiched Rényi entropy can also be used to compute the relative Rényi entropy.

*Case 1 (**β** Is an Integer):*

Step 1: By Lemma II.1, there is a unitary operator U_1, which is a $(1,n+n_\sigma,0)$-block-encoding of σ, using $O(1)$ queries to U_σ and $O(n_\sigma)$ elementary quantum gates. By Lemma II.12, there is a unitary operator U_β, which is a $(1,O(\beta(n+n_\sigma)),0)$-block-encoding of σ^β, using β queries to U_1. By Lemma II.2, there is a unitary operator U_η, which prepares a subnormalized density operator $\eta=\sigma^\beta\rho\sigma^\beta$, using 1 query to U_β and 1 query to U_ρ.

Now introducing two parameters δ_1 and ε_1, by Lemma II.8, there is a unitary operator $\tilde{U}$, which prepares a subnormalized density operator η' and η' is a $(4\delta_1^{\alpha-1},0,\Theta(\delta_1^\alpha+\varepsilon_1\delta_1^{\alpha-1}))$-block-encoding of η^α, using $O(d_1)$ queries to U_η, where $d_1=O(\frac{1}{\delta_1}\log\frac{1}{\varepsilon_1})$.

Step 2: Introducing a parameter ε_2, by Lemma II.15, we can compute $\tilde{p}$ such that $|\tilde{p}-\operatorname{tr}(\eta')|\le\varepsilon_2$, using $O\left(\frac{\sqrt{B}}{\varepsilon_2}+\frac{1}{\sqrt{\varepsilon_2}}\right)$ queries to $\tilde{U}$, where $B=\Theta\left(\delta_1^{1-\alpha}+r(\delta_1+\varepsilon_1)\right)$ is an upper bound for $\operatorname{tr}(\eta')$. Note that

$$\begin{aligned}\operatorname{tr}(\eta')&\le\frac{1}{4}\delta_1^{1-\alpha}\operatorname{tr}\left(\eta^\alpha\right)+\Theta\left(r(\delta_1+\varepsilon_1)\right)\\&\le\Theta\left(\delta_1^{1-\alpha}+r(\delta_1+\varepsilon_1)\right).\end{aligned}$$

Step 3: Output $4\delta_1^{\alpha-1}\tilde{p}\approx F_\alpha(\rho,\sigma)$ as the estimation. The additive error is

$$\begin{aligned}\left|4\delta_1^{\alpha-1}\tilde{p}-F_\alpha(\rho,\sigma)\right|&\le4\delta_1^{\alpha-1}\left|\tilde{p}-\operatorname{tr}(\eta')\right|\\&\quad+\left|\operatorname{tr}(4\delta_1^{\alpha-1}\eta')-\operatorname{tr}(\eta^\alpha)\right|\\&\le\Theta\left(r(\delta_1^\alpha+\varepsilon_1\delta_1^{\alpha-1})+\delta_1^{\alpha-1}\varepsilon_2\right).\end{aligned}$$

In order to make $\left|4\delta_1^{\alpha-1}\tilde{p}-F_\alpha(\rho,\sigma)\right|\le\varepsilon$, it is sufficient to let $\delta_1=\Theta((\varepsilon/r)^{1/\alpha})$, $\varepsilon_1=\Theta((\varepsilon/r)^{1/\alpha})$, and $\varepsilon_2=\Theta(\varepsilon^{1/\alpha}/r^{1/\alpha-1})$. Under these conditions, the number of queries to U_σ is

$$O\left(\beta d_1\left(\frac{\sqrt{B}}{\varepsilon_2}+\frac{1}{\sqrt{\varepsilon_2}}\right)\right)=\tilde{O}\left(\frac{r^{\frac{3-\alpha}{2\alpha}}}{\varepsilon^{\frac{3+\alpha}{2\alpha}}}\right),$$

and the number of queries to U_ρ is

$$O\left(d_1\left(\frac{\sqrt{B}}{\varepsilon_2}+\frac{1}{\sqrt{\varepsilon_2}}\right)\right)=\tilde{O}\left(\frac{r^{\frac{3-\alpha}{2\alpha}}}{\varepsilon^{\frac{3+\alpha}{2\alpha}}}\right),$$

and the number of elementary quantum gates is

$$\begin{aligned}&O\left(\beta d_1\left(\frac{\sqrt{B}}{\varepsilon_2}+\frac{1}{\sqrt{\varepsilon_2}}\right)\right)\cdot\mathrm{poly}(n,n_\sigma,n_\rho)\\&\quad=\tilde{O}\left(\frac{r^{\frac{3-\alpha}{2\alpha}}}{\varepsilon^{\frac{3+\alpha}{2\alpha}}}\mathrm{poly}(n)\right).\end{aligned}$$

*Case 2 (**β** Is Not an Integer):*

Let $\{\beta\}=\beta-\lfloor\beta\rfloor$ denote the decimal part of β.

Step 1: By Lemma II.1, there is a unitary operator U_1, which is a $(1, n+n_\sigma, 0)$-block-encoding of σ, using $O(1)$ queries to U_σ and $O(n_\sigma)$ elementary quantum gates. By Lemma II.13, introducing two parameters δ_1 and ε_1, there is a unitary operator $U_{\{\beta\}}$, which is a $(1, O(n+n_\sigma), 0)$-block-encoding of A_1, using $O(Q_1)$ queries to U_1 and $O(Q_1(n+n_\sigma))$ elementary quantum gates, where $Q_1 = O\left(\frac{1}{\delta_1}\log\frac{1}{\varepsilon_1}\right)$ and A_1 is a $(2, 0, \Theta(\varepsilon_1+\delta_1^{\{\beta\}}))$-block-encoding of $\sigma^{\{\beta\}}$. By Lemma II.12, there is a unitary operator $U_{\lfloor\beta\rfloor}$, which is a $(1, O(\beta(n+n_\sigma)), 0)$-block-encoding of $\sigma^{\lfloor\beta\rfloor}$, using $\lfloor\beta\rfloor$ queries to U_1. Again by Lemma II.12, there is a unitary operator U_β, which is a $(2, O(\beta(n+n_\sigma)), 0)$-block-encoding of $A_1\sigma^{\lfloor\beta\rfloor}$, using 1 query to $U_{\lfloor\beta\rfloor}$ and 1 query to $U_{\{\beta\}}$. By Lemma II.2, there is a unitary operator $\tilde{U}$, which prepares a subnormalized density operator $A_1\sigma^{\lfloor\beta\rfloor}\rho\sigma^{\lfloor\beta\rfloor}A_1^\dagger$, using 1 query to $\tilde{U}$ and 1 query to U_ρ. Note that

$$\begin{aligned}
&\left\| A_1\sigma^{\lfloor\beta\rfloor}\rho\sigma^{\lfloor\beta\rfloor}A_1^\dagger - \frac{1}{4}\sigma^\beta\rho\sigma^\beta \right\| \\
&\leq \left\| A_1\sigma^{\lfloor\beta\rfloor} - \frac{1}{2}\sigma^\beta \right\| \|\rho\| \left\| \sigma^{\lfloor\beta\rfloor}A_1^\dagger \right\| \\
&\qquad + \left\| \sigma^{\lfloor\beta\rfloor}A_1^\dagger - \frac{1}{2}\sigma^\beta \right\| \|\rho\| \left\| \frac{1}{2}\sigma^\beta \right\| \\
&\leq \Theta\left(\varepsilon_1 + \delta_1^{\{\beta\}}\right).
\end{aligned}$$

Step 2: By Lemma II.8, introducing two parameters δ_2 and ε_2, there is a unitary operator U_2, which prepares a subnormalized density operator A_2, using $O(Q_2)$ queries to $\tilde{U}$ and $O(Q_2(n+n_\sigma+n_\rho))$ elementary quantum gates, where $Q_2 = O\left(\frac{1}{\delta_2}\log\frac{1}{\varepsilon_2}\right)$ and A_2 is a $(4\delta_2^{\alpha-1}, 0, \Theta(\delta_2^{\alpha-1}(\delta_2+\varepsilon_2)))$-block-encoding of $\left(A_1\sigma^{\lfloor\beta\rfloor}\rho\sigma^{\lfloor\beta\rfloor}A_1^\dagger\right)^\alpha$.

In order to analysis the error, we need the following lemma.

Lemma IV.6: Suppose that A and B are two positive semidefinite operators of rank $\leq r$, and $0 < \alpha < 1$. Then

$$|\operatorname{tr}(A^\alpha) - \operatorname{tr}(B^\alpha)| \leq 3\ r \|A - B\|^\alpha.$$

Proof: Let $J = A - B$. Let the eigenvalues of A, B and J be

$$\begin{aligned}
\mu_1 \geq \mu_2 \geq \cdots \geq \mu_N,\\
\nu_1 \geq \nu_2 \geq \cdots \geq \nu_N,\\
\xi_1 \geq \xi_2 \geq \cdots \geq \xi_N,
\end{aligned}$$

respectively. Then we have $\mu_{r+1} = \cdots = \mu_N = \nu_{r+1} = \cdots = \nu_N = 0$. By Weyl's inequality [104], we have

$$\nu_j - \|J\| \leq \nu_j + \xi_N \leq \mu_j \leq \nu_j + \xi_1 \leq \nu_j + \|J\|$$

for every $1 \leq j \leq N$. Furthermore, it holds that $\left|\mu_j^\alpha - \nu_j^\alpha\right| \leq 5\|J\|^\alpha$. This is seen by the following two cases.

1) $\nu_j \geq \|J\|$. In this case, $\nu_j^\alpha - \|J\|^\alpha \leq (\nu_j - \|J\|)^\alpha \leq \mu_j^\alpha \leq (\nu_j + \|J\|)^\alpha \leq \nu_j^\alpha + \|J\|^\alpha$. Then we obtain that $\left|\mu_j^\alpha - \nu_j^\alpha\right| \leq \|J\|^\alpha$.
2) $\nu_j < \|J\|$. In this case, $\left|\mu_j^\alpha - \nu_j^\alpha\right| \leq |\mu_j|^\alpha + |\nu_j|^\alpha \leq |\nu_j + \|J\||^\alpha + |\nu_j|^\alpha < (2^\alpha + 1)\|J\|^\alpha < 3\|J\|^\alpha$.

These yield that

$$\begin{aligned}
|\operatorname{tr}(A^\alpha) - \operatorname{tr}(B^\alpha)| &= \left|\sum_{j=1}^N \mu_j^\alpha - \sum_{j=1}^N \nu_j^\alpha\right| \\
&\leq \sum_{j=1}^r \left|\mu_j^\alpha - \nu_j^\alpha\right| \\
&\leq 3\ r \|J\|^\alpha.
\end{aligned}$$

□

By Lemma IV.6, we have

$$\begin{aligned}
&\left|\operatorname{tr}\left(\left(A_1\sigma^{\lfloor\beta\rfloor}\rho\sigma^{\lfloor\beta\rfloor}A_1^\dagger\right)^\alpha\right) - \operatorname{tr}\left(\left(\frac{1}{4}\sigma^\beta\rho\sigma^\beta\right)^\alpha\right)\right| \\
&\leq 3\ r \left\| A_1\sigma^{\lfloor\beta\rfloor}\rho\sigma^{\lfloor\beta\rfloor}A_1^\dagger - \frac{1}{4}\sigma^\beta\rho\sigma^\beta \right\|^\alpha \\
&\leq \Theta\left(r\left(\varepsilon_1 + \delta_1^{\{\beta\}}\right)^\alpha\right).
\end{aligned}$$

Step 3: Introducing a parameter ε_3, by Lemma II.15, we can compute $\tilde{p}$ such that $|\tilde{p} - \operatorname{tr}(A_2)| \leq \varepsilon_3$, using $O\left(\frac{\sqrt{B}}{\varepsilon_3} + \frac{1}{\sqrt{\varepsilon_3}}\right)$ queries to U_2, where

$$B = \Theta\left(\delta_2^{1-\alpha} + r\left(\varepsilon_1 + \delta_1^{\{\beta\}}\right)^\alpha + r(\delta_2 + \varepsilon_2)\right)$$

is an upper bound for $\operatorname{tr}(A_2)$. Note that

$$\begin{aligned}
&\operatorname{tr}(A_2) \\
&\leq \frac{1}{4}\delta_2^{1-\alpha}\operatorname{tr}\left(\left(A_1\sigma^{\lfloor\beta\rfloor}\rho\sigma^{\lfloor\beta\rfloor}A_1^\dagger\right)^\alpha\right) + \Theta(r(\delta_2 + \varepsilon_2)) \\
&\leq \frac{1}{4}\delta_2^{1-\alpha}\left(\operatorname{tr}\left(\left(\frac{1}{4}\sigma^\beta\rho\sigma^\beta\right)^\alpha\right) + \Theta\left(r\left(\varepsilon_1 + \delta_1^{\{\beta\}}\right)^\alpha\right)\right) \\
&\qquad + \Theta(r(\delta_2 + \varepsilon_2)) \\
&\leq \Theta\left(\delta_2^{1-\alpha} + r\left(\varepsilon_1 + \delta_1^{\{\beta\}}\right)^\alpha + r(\delta_2 + \varepsilon_2)\right).
\end{aligned}$$

Step 4: Output $4^{\alpha+1}\delta_2^{\alpha-1}\tilde{p} \approx F_\alpha(\rho, \sigma)$ as the estimation. The additive error is

$$\begin{aligned}
&\left|4^{\alpha+1}\delta_2^{\alpha-1}\tilde{p} - F_\alpha(\rho, \sigma)\right| \\
&\leq 4^{\alpha+1}\delta_2^{\alpha-1}|\tilde{p} - \operatorname{tr}(A_2)| \\
&\quad + 4^\alpha\left|\operatorname{tr}(4\delta_2^{\alpha-1}A_2) - \operatorname{tr}\left(\left(A_1\sigma^{\lfloor\beta\rfloor}\rho\sigma^{\lfloor\beta\rfloor}A_1^\dagger\right)^\alpha\right)\right| \\
&\quad + 4^\alpha\left|\operatorname{tr}\left(\left(A_1\sigma^{\lfloor\beta\rfloor}\rho\sigma^{\lfloor\beta\rfloor}A_1^\dagger\right)^\alpha\right) - \operatorname{tr}\left(\left(\frac{1}{4}\sigma^\beta\rho\sigma^\beta\right)^\alpha\right)\right| \\
&\leq \Theta\left(r\left(\varepsilon_1 + \delta_1^{\{\beta\}}\right)^\alpha + r\delta_2^{\alpha-1}(\varepsilon_2 + \delta_2) + \delta_2^{\alpha-1}\varepsilon_3\right).
\end{aligned}$$

In order to make $\left|4^{\alpha+1}\delta_2^{\alpha-1}\tilde{p} - F_\alpha(\rho, \sigma)\right| \leq \varepsilon$, it is sufficient to let $\delta_1 = \Theta((\varepsilon/r)^{1/\alpha\{\beta\}})$, $\varepsilon_1 = \Theta((\varepsilon/r)^{1/\alpha\{\beta\}})$, $\delta_2 = \Theta\left((\varepsilon/r)^{1/\alpha}\right)$, $\varepsilon_2 = \Theta\left((\varepsilon/r)^{1/\alpha}\right)$ and $\varepsilon_3 = \Theta\left(\varepsilon^{1/\alpha}/r^{1/\alpha-1}\right)$. Under these conditions, the number of queries to U_σ is

$$O\left(Q_1Q_2\left(\frac{\sqrt{B}}{\varepsilon_3} + \frac{1}{\sqrt{\varepsilon_3}}\right)\right) = \tilde{O}\left(\frac{r^{\frac{3-\alpha}{2\alpha}+\frac{1}{\alpha\{\beta\}}}}{\varepsilon^{\frac{3+\alpha}{2\alpha}+\frac{1}{\alpha\{\beta\}}}}\right),$$

and the number of queries to U_ρ is

$$O\left(Q_2\left(\frac{\sqrt{B}}{\varepsilon_3} + \frac{1}{\sqrt{\varepsilon_3}}\right)\right) = \tilde{O}\left(\frac{r^{\frac{3-\alpha}{2\alpha}}}{\varepsilon^{\frac{3+\alpha}{2\alpha}}}\right),$$

and the number of elementary quantum gates is

$$O\left(Q_1Q_2\left(\frac{\sqrt{B}}{\varepsilon_3}+\frac{1}{\sqrt{\varepsilon_3}}\right)\right)\cdot\mathrm{poly}(n,n_\sigma,n_\rho)$$
$$=\tilde{O}\left(\frac{r^{\frac{3-\alpha}{2\alpha}+\frac{1}{\alpha\{\beta\}}}}{\varepsilon^{\frac{3+\alpha}{2\alpha}+\frac{1}{\alpha\{\beta\}}}}\mathrm{poly}(n)\right).$$

C. Lower Bounds and Hardness

Our quantum algorithms for both fidelity estimation and trace distance estimation requires time complexity polynomial in the rank r of quantum states. Here, we show that unless $\mathsf{BQP} = \mathsf{QSZK}$, there is no quantum algorithm for both fidelity estimation and trace distance estimation with time complexity polylogarithmic in r.

Theorem IV.7: If there is a quantum algorithm that computes fidelity or trace distance of quantum states of rank $\leq r$ within additive error ε with time complexity $\mathrm{poly}\,(\log r, 1/\varepsilon)$, then $\mathsf{BQP} = \mathsf{QSZK}$.

Proof: Here, we recall a decision problem called (α, β)-Quantum State Distinguishability ((α, β)-QSD). Given U_ρ and U_σ that prepares the purifications of density operators ρ and σ and a promise that either $T(\rho, \sigma) \leq \alpha$ or $T(\rho, \sigma) \geq \beta$, the problem is to determine which is the case. It was shown in [20] that (α, β)-QSD is QSZK-complete if $0 \leq \alpha < \beta^2 \leq 1$.

If there is a quantum algorithm for computing trace distance with time complexity $\mathrm{poly}\,(\log r, 1/\varepsilon)$, then we can distinguish the two cases with time complexity $\mathrm{poly}(n)$ by letting $r = 2^n$ be the dimension of the two quantum states and $\varepsilon = (\beta - \alpha)/2 > 0$.

If there is a quantum algorithm for computing fidelity with time complexity $\mathrm{poly}\,(\log r, 1/\varepsilon)$, then we can distinguish the two cases with time complexity $\mathrm{poly}(n)$ by letting $r = 2^n$ be the dimension of the two quantum states and $\varepsilon = \left((1-\alpha) - \sqrt{1-\beta^2}\right)/2 > 0$. This is because $T(\rho, \sigma) \leq \alpha$ implies $F(\rho, \sigma) \geq 1 - \alpha$, and $T(\rho, \sigma) \geq \beta$ implies $F(\rho, \sigma) \leq \sqrt{1-\beta^2}$. Then (α, β)-QSD is reduced to distinguish which is the case with promise that either $F(\rho, \sigma) \leq \sqrt{1-\beta^2}$ and $F(\rho, \sigma) \geq 1 - \alpha$. □

Our quantum algorithms for estimating the fidelity and trace distance achieve a significant speedup under the low-rank assumption. One might wonder whether our algorithms can be "dequantized" through quantum-inspired low-rank techniques such as [105] and [106]. We suspect that it might be unachievable because the following theorem shows that computing fidelity and trace distance are $\mathsf{DQC1}$-hard.

Theorem IV.8: Computing the fidelity and trace distance are $\mathsf{DQC1}$-hard, even for pure quantum states.

Proof: It was already proved in [12] that estimating the fidelity is $\mathsf{DQC1}$-hard, even for pure quantum states. Here, we reduce the problem of estimating the fidelity to that of estimating the trace distance, and therefore show the $\mathsf{DQC1}$-hardness of estimating the trace distance.

For any two pure quantum states $\psi = |\psi\rangle\langle\psi|$ and $\phi = |\phi\rangle\langle\phi|$, their trace distance is essentially

$$T(\psi, \phi) = \sqrt{1 - (F(\psi, \phi))^2}.$$

Therefore, any algorithm that computes the trace distance $T(\psi, \phi)$ will immediately yield the fidelity $F(\psi, \phi) = \sqrt{1 - (T(\psi, \phi))^2}$. As a result, estimating the trace distance is $\mathsf{DQC1}$-hard even for pure quantum states. □

It was shown in [63] that $\mathsf{DQC1}$ is not (classically) weakly simulatable unless the polynomial hierarchy collapses to the second level, i.e., $\mathsf{PH} = \mathsf{AM}$. This, together with Theorem IV.8, means that there is unlikely an efficient classical algorithm that estimates the fidelity or trace distance. It should be noted that this does not rule out the existence of a dequantized version of our quantum algorithms because dequantized algorithms often assume a different input model from Theorem IV.8. More specifically, dequantized algorithms assume "sampling and query access" [105], [106] to the input matrix (in our case, the density operator of the quantum state) stored in a pre-computed data structure.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable suggestions and for pointing out some mistakes in an earlier version of this paper. They also thank Wang Fang, Kean Chen, and Minbo Gao for helpful discussions.

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[2] M. Ohya and D. Petz, *Quantum Entropy and Its Use*. Cham, Switzerland: Springer, 2004.

[3] X. Zhang et al., "Direct fidelity estimation of quantum states using machine learning," *Phys. Rev. Lett.*, vol. 127, no. 13, Sep. 2021, Art. no. 130503.

[4] A. R. Kuzmak, "Measuring distance between quantum states on a quantum computer," *Quantum Inf. Process.*, vol. 20, no. 8, p. 269, Aug. 2021.

[5] C. Bădescu, R. O'Donnell, and J. Wright, "Quantum state certification," in *Proc. 51st Annu. ACM SIGACT Symp. Theory Comput. (STOC)*, Jun. 2019, pp. 503–514.

[6] J. Acharya, I. Issa, N. V. Shende, and A. B. Wagner, "Estimating quantum entropy," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 454–468, Aug. 2020.

[7] Y. Wang, B. Zhao, and X. Wang, "Quantum algorithms for estimating quantum entropies," *Phys. Rev. Appl.*, vol. 19, no. 4, Apr. 2023, Art. no. 044041.

[8] A. Gilyén and T. Li, "Distributional property testing in a quantum world," in *Proc. 11th Innov. Theor. Comput. Science Conf.*, 2020, pp. 25:1–25:19.

[9] T. Gur, M.-H. Hsieh, and S. Subramanian, "Sublinear quantum algorithms for estimating von Neumann entropy," 2021, *arXiv:2111.11139*.

[10] S. Subramanian and M.-H. Hsieh, "Quantum algorithm for estimating α-Rényi entropies of quantum states," *Phys. Rev. A, Gen. Phys.*, vol. 104, no. 2, Aug. 2021, Art. no. 022428.

[11] Q. Wang et al., "Quantum algorithm for fidelity estimation," *IEEE Trans. Inf. Theory*, vol. 69, no. 1, pp. 273–282, Jan. 2023.

[12] M. Cerezo, A. Poremba, L. Cincio, and P. J. Coles, "Variational quantum fidelity estimation," *Quantum*, vol. 4, p. 248, Mar. 2020.

[13] R. Chen, Z. Song, X. Zhao, and X. Wang, "Variational quantum algorithms for trace distance and fidelity estimation," *Quantum Sci. Technol.*, vol. 7, no. 1, Jan. 2022, Art. no. 015019.

[14] K. C. Tan and T. Volkoff, "Variational quantum algorithms to estimate rank, quantum entropies, fidelity, and Fisher information via purity minimization," *Phys. Rev. Res.*, vol. 3, no. 3, Sep. 2021, Art. no. 033251.

[15] R. O'Donnell and J. Wright, "Quantum spectrum testing," *Commun. Math. Phys.*, vol. 387, no. 1, pp. 1–75, Oct. 2021.

[16] R. O'Donnell and J. Wright, "Efficient quantum tomography," in *Proc. 48th Annu. ACM Symp. Theory Comput. (STOC)*, Jun. 2016, pp. 899–912.

[17] R. O'Donnell and J. Wright, "Efficient quantum tomography II," in *Proc. 47th Annu. ACM Symp. Theory Comput. (STOC)*, 2017, pp. 962–974.

[18] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, "Sample-optimal tomography of quantum states," *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 5628–5641, Sep. 2017.

[19] A. Anshu, Z. Landau, and Y. Liu, "Distributed quantum inner product estimation," in *Proc. 54th Annu. ACM SIGACT Symp. Theory Comput.*, Jun. 2022, pp. 44–51.

[20] J. Watrous, "Limits on the power of quantum statistical zero-knowledge," in *Proc. 43rd Annu. IEEE Symp. Found. Comput. Sci.*, Mar. 2002, pp. 459–468.

[21] J. Watrous, "Simpler semidefinite programs for completely bounded norms," *Chicago J. Theor. Comput. Sci.*, vol. 2013, no. 8, pp. 1–19, Jul. 2013.

[22] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe, "Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics," in *Proc. 51st Annu. ACM SIGACT Symp. Theory Comput.*, Jun. 2019, pp. 193–204.

[23] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 8th Annu. ACM Symp. Theory Comput.*, 1996, pp. 212–219.

[24] A. Ambainis, "Quantum walk algorithm for element distinctness," *SIAM J. Comput.*, vol. 37, no. 1, pp. 210–239, Jan. 2007.

[25] M. Szegedy, "Quantum speed-up of Markov chain based algorithms," in *Proc. 45th Annu. IEEE Symp. Found. Comput. Sci.*, Oct. 2004, pp. 32–41.

[26] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Phys. Rev. Lett.*, vol. 103, no. 15, Oct. 2009, Art. no. 150502.

[27] G. H. Low and I. L. Chuang, "Optimal Hamiltonian simulation by quantum signal processing," *Phys. Rev. Lett.*, vol. 118, no. 1, Jan. 2017, Art. no. 010501.

[28] S. Lloyd et al., "Hamiltonian singular value transformation and inverse block encoding," 2021, *arXiv:2104.01410*.

[29] S. Lloyd et al., "Quantum polar decomposition algorithm," 2020, *arXiv:2006.00841*.

[30] Y. Quek and P. Rebentrost, "Fast algorithm for quantum polar decomposition and applications," *Phys. Rev. Res.*, vol. 4, no. 1, Feb. 2022, Art. no. 013144.

[31] G. H. Low and I. L. Chuang, "Hamiltonian simulation by qubitization," *Quantum*, vol. 3, p. 163, Jul. 2019.

[32] J. van Apeldoorn and A. Gilyén, "Improvements in quantum SDP-solving with applications," in *Proc. 46th Int. Colloq. Automata, Lang., Program.*, 2019, pp. 99:1–99:15.

[33] S. Chakraborty, A. Gilyén, and S. Jeffery, "The power of block-encoded matrix powers: Improved regression techniques via faster Hamiltonian simulation," in *Proc. 46th Int. Colloq. Automata, Lang., Program.*, 2019, pp. 33:1–33:14.

[34] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, "Quantum state tomography via compressed sensing," *Phys. Rev. Lett.*, vol. 105, no. 15, Oct. 2010, Art. no. 150401.

[35] N. Ezzell, Z. Holmes, and P. J. Coles, "The quantum low-rank approximation problem," 2022, *arXiv:2203.00811*.

[36] C. Butucea, M. Guţă, and T. Kypraios, "Spectral thresholding quantum tomography for low rank states," *New J. Phys.*, vol. 17, no. 11, Nov. 2015, Art. no. 113050.

[37] F. G. S. L. Brand ao, A. Kalev, T. Li, C. Y.-Y. Lin, K. M. Svore, and X. Wu, "Quantum SDP solvers: Large speed-ups, optimality, and applications to quantum learning," in *Proc. 46th Int. Colloq. Automata, Lang., Program.*, 2019, pp. 27:1–27:14.

[38] A. Gilyén, S. Lloyd, I. Marvian, Y. Quek, and M. M. Wilde, "Quantum algorithm for petz recovery channels and pretty good measurements," *Phys. Rev. Lett.*, vol. 128, no. 22, Jun. 2022, Art. no. 220502.

[39] A. Gilyén and A. Poremba, "Improved quantum algorithms for fidelity estimation," 2022, *arXiv:2203.15993*.

[40] S. Lloyd, M. Mohseni, and P. Rebentrost, "Quantum principal component analysis," *Nat. Phys.*, vol. 10, no. 9, pp. 631–633, 2014.

[41] S. Kimmel, C. Y.-Y. Lin, G. H. Low, M. Ozols, and T. J. Yoder, "Hamiltonian simulation with optimal sample complexity," *NPJ Quantum Inf.*, vol. 3, no. 1, pp. 1–7, Mar. 2017.

[42] A. N. Chowdhury, G. Hao Low, and N. Wiebe, "A variational quantum algorithm for preparing quantum Gibbs states," 2020, *arXiv:2002.00055*.

[43] A. Montanaro and R. de Wolf, "A survey of quantum property testing," in *Theory of Computing Library* (Graduate Surveys), no. 7. Chicago, IL, USA: Univ. Chicago, 2016, pp. 1–81.

[44] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik (Mathematical Foundations of Quantum Mechanics)*. Princeton, NJ, USA: Princeton Univ. Press, 1932.

[45] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Oct. 1948.

[46] A. Rényi, "On measures of entropy and information," in *Proc. 4th Berkeley Symp. Math. Statist. Probab.*, vol. 1, 1961, pp. 547–561.

[47] N. Linden, M. Mosonyi, and A. Winter, "The structure of Rényi entropic inequalities," *Proc. Roy. Soc. A Math., Phys., Eng. Sci.*, vol. 469, no. 2158, 2158, Art. no. 20120737.

[48] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," *J. Math. Phys.*, vol. 54, no. 12, Dec. 2013, Art. no. 122203.

[49] M. M. Wilde, A. Winter, and D. Yang, "Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy," *Commun. Math. Phys.*, vol. 331, no. 2, pp. 593–622, Oct. 2014.

[50] C. Tsallis, "Possible generalization of Boltzmann-Gibbs statistics," *J. Stat. Phys.*, vol. 52, nos. 1–2, pp. 479–487, Jul. 1988.

[51] K. M. R. Audenaert, "Subadditivity of q-entropies for $q > 1$," *J. Math. Phys.*, vol. 48, no. 8, 2007, Art. no. 083507.

[52] D. Petz and D. Virosztek, "Some inequalities for quantum tsallis entropy related to the strong subadditivity," *Math. Inequal. Appl.*, vol. 18, no. 2, pp. 555–568, 2015.

[53] W. van Dam and P. Hayden, "Rényi-entropic bounds on quantum communication," 2002, *arXiv:quant-ph/0204093*.

[54] N. Datta, "Min- and max-relative entropies and a new entanglement monotone," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2816–2826, Jun. 2009.

[55] R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4337–4347, Sep. 2009.

[56] X. Hu and Z. Ye, "Generalized quantum entropy," *J. Math. Phys.*, vol. 47, no. 2, Feb. 2006, Art. no. 023502.

[57] A. E. Rastegin, "Some general properties of unified entropies," *J. Stat. Phys.*, vol. 143, no. 6, pp. 1120–1135, Jun. 2011.

[58] A. K. Ekert, C. M. Alves, D. K. L. Oi, M. Horodecki, P. Horodecki, and L. C. Kwek, "Direct estimations of linear and nonlinear functionals of a quantum state," *Phys. Rev. Lett.*, vol. 88, no. 21, May 2002, Art. no. 217901.

[59] T. Li and X. Wu, "Quantum query complexity of entropy estimation," *IEEE Trans. Inf. Theory*, vol. 65, no. 5, pp. 2899–2921, May 2019.

[60] M. Bun, R. Kothari, and J. Thaler, "The polynomial method strikes back: Tight quantum query bounds via dual polynomials," *Theory Comput.*, vol. 16, no. 10, pp. 1–71, 2020.

[61] R. Jozsa, "Fidelity for mixed quantum states," *J. Mod. Optic*, vol. 41, no. 12, pp. 2315–2323, 1994.

[62] Y. Liu, "Quantum state testing beyond the polarizing regime and quantum triangular discrimination," 2023, *arXiv:2303.01952*.

[63] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, "Impossibility of classically simulating one-clean-qubit model with multiplicative error," *Phys. Rev. Lett.*, vol. 120, no. 20, May 2018, Art. no. 200502.

[64] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *Contemp. Math.*, vol. 305, pp. 53–74, Oct. 2002.

[65] R. Somma, G. Ortiz, J. E. Gubernatis, E. Knill, and R. Laflamme, "Simulating physical phenomena by quantum networks," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 4, Apr. 2002, Art. no. 042323.

[66] A. M. Childs and N. Wiebe, "Hamiltonian simulation using linear combinations of unitary operations," *Quantum Inf. Comput.*, vol. 12, nos. 11–12, pp. 901–924, Nov. 2012.

[67] R. Kothari, "Efficient algorithms in quantum query complexity," Ph.D. dissertation, Inst. Quantum Comput., Univ. Waterloo, Waterloo, ON, Canada, 2014. [Online]. Available: https://core.ac.uk/download/pdf/144147587.pdf

[68] D. W. Berry, A. M. Childs, R. Cleve, R. Kothari, and R. D. Somma, "Simulating Hamiltonian dynamics with a truncated Taylor series," *Phys. Rev. Lett.*, vol. 114, no. 9, Mar. 2015, Art. no. 090502.

[69] D. W. Berry, A. M. Childs, and R. Kothari, "Hamiltonian simulation with nearly optimal dependence on all parameters," in *Proc. IEEE 56th Annu. Symp. Found. Comput. Sci.*, Aug. 2015, pp. 792–809.

[70] A. M. Childs, R. Kothari, and R. D. Somma, "Quantum algorithm for systems of linear equations with exponentially improved dependence on precision," *SIAM J. Comput.*, vol. 46, no. 6, pp. 1920–1950, Jan. 2017.

[71] T. Batu, L. Fortnow, R. Rubinfeld, W. D. Smith, and P. White, "Testing that distributions are close," in *Proc. 41st Annu. Symp. Found. Comput. Sci. (FOCS)*, 2000, pp. 259–269.

[72] T. Batu, L. Fortnow, R. Rubinfeld, W. D. Smith, and P. White, “Testing closeness of discrete distributions,” *J. ACM*, vol. 60, no. 1, pp. 1–25, Feb. 2013.

[73] S.-O. Chan, I. Diakonikolas, P. Valiant, and G. Valiant, “Optimal algorithms for testing closeness of discrete distributions,” in *Proc. 25th Annu. ACM-SIAM Symp. Discrete Algorithms (SODA)*, Jan. 2014, pp. 1193–1203.

[74] T. Batu, E. Fischer, L. Fortnow, R. Kumar, R. Rubinfeld, and P. White, “Testing random variables for independence and identity,” in *Proc. 42nd IEEE Symp. Found. Comput. Sci. (FOCS)*, Oct. 2001, pp. 442–451.

[75] L. Paninski, “A coincidence-based test for uniformity given very sparsely sampled discrete data,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4750–4755, Oct. 2008.

[76] I. Diakonikolas and D. M. Kane, “A new approach for testing properties of discrete distributions,” in *Proc. IEEE 57th Annu. Symp. Found. Comput. Sci. (FOCS)*, Oct. 2016, pp. 685–694.

[77] T. Batu, R. Kumar, and R. Rubinfeld, “Sublinear algorithms for testing monotone and unimodal distributions,” in *Proc. 36th Annu. ACM Symp. Theory Comput. (STOC)*, Jun. 2004, pp. 381–390.

[78] T. Batu, S. Dasgupta, R. Kumar, and R. Rubinfeld, “The complexity of approximating the entropy,” *SIAM J. Comput.*, vol. 35, no. 1, pp. 132–150, Jan. 2005.

[79] L. Paninski, “Estimation of entropy and mutual information,” *Neural Comput.*, vol. 15, no. 6, pp. 1191–1253, Jun. 2003.

[80] L. Paninski, “Estimating entropy on m bins given fewer than m samples,” *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2200–2203, Aug. 2004.

[81] G. Valiant and P. Valiant, “Estimating the unseen: An n/log(n)-sample estimator for entropy and support size, shown optimal via new CLTs,” in *Proc. 43rd Annu. ACM Symp. Theory Comput. (STOC)*, Jun. 2011, pp. 685–694.

[82] G. Valiant and P. Valiant, “The power of linear estimators,” in *Proc. IEEE 52nd Annu. Symp. Found. Comput. Sci. (FOCS)*, Oct. 2011, pp. 403–412.

[83] J. Jiao, K. Venkat, Y. Han, and T. Weissman, “Minimax estimation of functionals of discrete distributions,” *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2835–2885, May 2015.

[84] Y. Wu and P. Yang, “Minimax rates of entropy estimation on large alphabets via best polynomial approximation,” *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3702–3720, Jun. 2016.

[85] S. Bravyi, A. W. Harrow, and A. Hassidim, “Quantum algorithms for testing properties of distributions,” *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3971–3981, Jun. 2011.

[86] S. Chakraborty, E. Fischer, A. Matsliah, and R. de Wolf, “New results on quantum property testing,” in *Proc. 30th Int. Conf. Found. Softw. Technol. Theor. Comput. Sci.*, vol. 8, 2010, pp. 145–156.

[87] A. Montanaro, “Quantum speedup of Monte Carlo methods,” *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 471, no. 2181, Sep. 2015, Art. no. 20150301.

[88] J. Luo, Q. Wang, and L. Li, “Succinct quantum testers for closeness and k-wise uniformity of probability distributions,” *IEEE Trans. Inf. Theory*, 2024, doi: 10.1109/TIT.2024.3393756.

[89] N. Yu, “Sample efficient identity testing and independence testing of quantum states,” in *Proc. 12th Innov. Theor. Comput. Sci. Conf. (ITCS)* (Leibniz International Proceedings in Informatics), vol. 185, J. R. Lee, Ed. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum Für Informatik, 2021, pp. 11:1–11:20.

[90] S. Kullback and R. A. Leibler, “On information and sufficiency,” *Ann. Math. Statist.*, vol. 22, no. 1, pp. 79–86, 1951.

[91] X. Lu and H. Lin, “Quantum amplitude estimation by generalized qubitization,” 2023, *arXiv:2306.16695*.

[92] F. Le Gall, Y. Liu, and Q. Wang, “Space-bounded quantum state testing via space-efficient quantum singular value transformation,” 2023, *arXiv:2308.05079*.

[93] Q. Wang and Z. Zhang, “Time-efficient quantum entropy estimator via samplizer,” 2024, *arXiv:2401.09947*.

[94] X. Wang, S. Zhang, and T. Li, “A quantum algorithm framework for discrete probability distributions with applications to Rényi entropy estimation,” *IEEE Trans. Inf. Theory*, vol. 70, no. 5, pp. 3399–3426, May 2024.

[95] Z. Goldfeld, D. Patel, S. Sreekumar, and M. M. Wilde, “Quantum neural estimation of entropies,” *Phys. Rev. A, Gen. Phys.*, vol. 109, no. 3, Mar. 2024, Art. no. 032431.

[96] Q. Wang and Z. Zhang, “Fast quantum algorithms for trace distance estimation,” *IEEE Trans. Inf. Theory*, vol. 70, no. 4, pp. 2720–2733, Apr. 2024.

[97] S. Rethinasamy, R. Agarwal, K. Sharma, and M. M. Wilde, “Estimating distinguishability measures on quantum computers,” *Phys. Rev. A, Gen. Phys.*, vol. 108, no. 1, Jul. 2023, Art. no. 012409.

[98] T. Nuradha, Z. Goldfeld, and M. M. Wilde, “Quantum pufferfish privacy: A flexible privacy framework for quantum systems,” 2023, *arXiv:2306.13054*.

[99] N. Liu, Q. Wang, M. M. Wilde, and Z. Zhang, “Quantum algorithms for matrix geometric means,” 2024, *arXiv:2405.00673*.

[100] A. Gilyén, “Quantum singular value transformation & its algorithmic applications,” Ph.D. dissertation, Inst. Log., Lang. Comput., Univ. Amsterdam, Amsterdam, The Netherlands, 2019. [Online]. Available: https://pure.uva.nl/ws/files/35292358/Thesis.pdf

[101] P. Rebentrost, A. Steffens, I. Marvian, and S. Lloyd, “Quantum singular-value decomposition of nonsparse low-rank matrices,” *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 1, Jan. 2018, Art. no. 012327.

[102] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, “Quantum fingerprinting,” *Phys. Rev. Lett.*, vol. 87, no. 16, Sep. 2001, Art. no. 167902.

[103] M. Kieferova, O. M. Carlos, and N. Wiebe, “Quantum generative training using Rényi divergences,” 2021, *arXiv:2106.09567*.

[104] H. Weyl, “Das asymptotische verteilungsgesetz der eigenwerte linearer partieller differentialgleichungen (mit einer anwendung auf die theorie der Hohlraumstrahlung),” *Mathematische Annalen*, vol. 71, no. 4, pp. 441–479, Dec. 1912.

[105] E. Tang, “A quantum-inspired classical algorithm for recommendation systems,” in *Proc. 51st Annu. ACM SIGACT Symp. Theory Comput.*, Jun. 2019, pp. 219–228.

[106] N.-H. Chia, A. P. Gilyén, T. Li, H.-H. Lin, E. Tang, and C. Wang, “Sampling-based sublinear low-rank matrix arithmetic framework for dequantizing quantum machine learning,” *J. ACM*, vol. 69, no. 5, pp. 1–72, Oct. 2022.

Qisheng Wang received the B.Sc. and Ph.D. degrees from the Department of Computer Science and Technology, Tsinghua University, Beijing, China, in 2017 and 2022, respectively. He is currently an Assistant Professor with the Graduate School of Mathematics, Nagoya University, Nagoya, Japan. His current research interests include quantum computing, algorithms, and complexity.

Ji Guan received the bachelor’s degree in mathematics from Sichuan University, China, in 2014, and the Ph.D. degree in computer science from the University of Technology Sydney, Australia, in 2018. He is currently an Associate Research Professor with the Key Laboratory of System Software and State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences. His primary research interests include trustworthy quantum machine learning and model checking quantum systems.

Junyi Liu received the B.E. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China, in 2017, and the Ph.D. degree in computer science from the Institute of Software, Chinese Academy of Sciences, China, in 2023. He is currently a Post-Doctoral Scholar with the Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, USA. His current research interests include quantum programming and quantum algorithms.

Zhicheng Zhang received the B.E. degree from the University of Chinese Academy of Sciences, Beijing, China, in 2021. He is currently pursuing the Ph.D. degree with the Centre for Quantum Software and Information, University of Technology Sydney, Sydney, Australia. His current research interests include quantum computing and quantum algorithms.

Mingsheng Ying received the Graduate degree from Fuzhou Teachers College, Jiangxi, China, in 1981. He is currently a Distinguished Professor with the Centre for Quantum Software and Information, University of Technology Sydney (UTS), Australia. Before returning to UTS, he was a Research Professor and the Deputy Director for Research of the Institute of Software, Chinese Academy of Sciences; and a Cheung Kong Professor with the Department of Computer Science and Technology, Tsinghua University, China. He is the author of the books *Model Checking Quantum Systems: Principles and Algorithms* (Cambridge University Press, 2021), *Foundations of Quantum Programming* (Morgan Kaufmann, 2016), and *Topology in Process Calculus: Approximate Correctness and Infinite Evolution of Concurrent Programs* (Springer-Verlag, 2001). His current research interests include quantum computing, programming theory, and logics in artificial intelligence. He serves as the (Co-)Editor-in-Chief for *ACM Transactions on Quantum Computing*.