This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2022.3203985

Quantum Algorithm for Fidelity Estimation

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

***Abstract*—For two unknown mixed quantum states ρ and σ in an N-dimensional Hilbert space, computing their fidelity $F(\rho, \sigma)$ is a basic problem with many important applications in quantum computing and quantum information, for example verification and characterization of the outputs of a quantum computer, and design and analysis of quantum algorithms. In this paper, we propose a quantum algorithm that solves this problem in $\operatorname{poly}(\log(N), r, 1/\varepsilon)$ time, where r is the lower rank of ρ and σ, and ε is the desired precision, provided that the purifications of ρ and σ are prepared by quantum oracles. This algorithm exhibits an exponential speedup over the best known algorithm (based on quantum state tomography) which has time complexity polynomial in N.**

***Index Terms*—Quantum computing, quantum algorithms, quantum fidelity, quantum states.**

I. INTRODUCTION

QUANTUM computers are believed to have more computing power than classical machines as quantum algorithms have been proven to achieve significant speedups over the best known classical algorithms for solving certain problems. However, only a few of them reach exponential speedups, such as the celebrated Shor's algorithm for integer factorization [1], the HHL algorithm for solving systems of linear equations [2] and those for quantum simulation [3], [4], [5], [6]. This paper proposes a quantum algorithm to efficiently estimate the quantum state fidelity on a quantum computer. Compared to classical and even known quantum algorithms for the same task, the algorithm can be exponentially faster.

Estimating the quantum state fidelity is a basic problem in quantum computing and quantum information, as this quantity is one of the most popular and important measures of the "closeness" of two unknown quantum states [7], [8], [9]. Formally, the fidelity of two mixed quantum states ρ and σ is defined as

$$F(\rho, \sigma) = \operatorname{tr}\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right).$$

Quantum state fidelity has been applied in many different fields, such as quantum information processing [10], quantum engineering [11] and quantum machine learning [12]. It also plays a necessary and essential role in verifying and characterizing the output state of a quantum computer.

We propose an efficient quantum algorithm for fidelity estimation of quantum states, stated as follows.

Theorem 1 (Informal)**.** *There is a quantum algorithm that, given "purified quantum query access" to two N-dimensional quantum states ρ and σ, computes their fidelity within additive error ε with time complexity $\operatorname{poly}(\log(N), r, 1/\varepsilon)$, where r is the lower rank of ρ and σ.*

The "purified quantum query access" model is widely used in quantum computational complexity theory and quantum algorithms (e.g., [13], [14], [15], [16], [17], [18], [19], [20]), where mixed quantum states (density operators) are given by quantum circuits (oracles) that prepare their purifications (see Section II-B for a formal definition). From the perspective of computational complexity theory, the purified quantum query access model is useful when comparing quantum and classical algorithms, especially in defining complexity classes (see [21] for example). This model was introduced in [16] to the context of density operator testing. The basic idea behind the model is that a density operator can be understood as the output of certain quantum process. If we are able to simulate this process on a quantum computer, then it indeed provides purified quantum query access to the density operator.

In this Introduction, we will first review the existing approaches for fidelity estimation and discuss about its computational hardness. Then an outline of our quantum algorithm for fidelity estimation will be given in Section I-C. The details of the algorithm will be carefully described in the subsequent sections.

A. Existing Approaches for Fidelity Estimation

There are no known efficient methods for estimating the fidelity $F(\rho, \sigma)$ in the general case. A straightforward way is to first obtain a complete classical description of quantum states as density matrices by quantum state tomography [22], [23], and then calculate the fidelity by matrix arithmetic operations. However, this kind of approach requires resources increasing exponentially with the scale of the quantum system, even if quantum states are restricted to be low-rank. A slightly more efficient tomography can be applied for low-rank quantum states [24], [25], [26]. Several approaches for estimating $F(\rho, \sigma)$ have been proposed for the special case where ρ or σ is pure. The first one is the SWAP test [27], [28] using the Hadamard and Toffoli gates, which computes the value of $\operatorname{tr}(\rho\sigma)$. Then a more practical technique called entanglement

---

Q. Wang is with the Department of Computer Science and Technology, Tsinghua University, China. E-mail: QishengWang1994@gmail.com.

Z. Zhang is with Centre for Quantum Software and Information, University of Technology Sydney, Australia. E-mail: iszczhang@gmail.com. Part of this work was done while the author was at the University of Chinese Academy of Sciences, China.

K. Chen is with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China and the University of Chinese Academy of Sciences, China. E-mail: chenka@ios.ac.cn.

J. Guan is with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China. E-mail: guanj@ios.ac.cn.

W. Fang is with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China and the University of Chinese Academy of Sciences, China. E-mail: fangw@ios.ac.cn.

J. Liu is with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China and the University of Chinese Academy of Sciences, China. E-mail: liujy@ios.ac.cn.

M. Ying is with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China and the Department of Computer Science and Technology, Tsinghua University, China. E-mail: yingms@ios.ac.cn

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2022.3203985

witnesses [29], [30], [31] was introduced to compute the fidelity with few measurements, but only works for some specific pure quantum states. This limitation was overcome in [32], [33] where a direct fidelity estimation method was developed for arbitrary pure quantum states.

Recently, suspecting that computing fidelity of quantum states in the general case could be hard, several variational quantum algorithms for fidelity estimation have been successively proposed [34], [35], [36]. Naturally, the efficiency of these algorithms is unknown as training variational quantum algorithms is known to be **NP**-hard [37].

B. Hardness of Fidelity Estimation

Computing $F(\rho, \sigma)$ in general is known to be **QSZK**-hard [13], where **QSZK** (Quantum Statistical Zero-Knowledge) is a complexity class which contains **BQP**. A restricted version called LOW-RANK FIDELITY ESTIMATION, namely estimating the fidelity of low-rank quantum states, was shown in [34] to be **DQC1**-hard. Here, **DQC1** (Deterministic Quantum Computing with 1 Clean Bit) is the complexity class of problems that can be efficiently solved in the one-clean-qubit model of quantum computing [38], which is commonly believed to be strictly contained in **BQP**. However, it was observed in [39], [40] that efficient classical simulation of **DQC1**-complete problems implies that the polynomial hierarchy collapses to the second level, which is not believed to be true. Our algorithm presented in this paper shows that LOW-RANK FIDELITY ESTIMATION can be efficiently solved by quantum computers with complexity logarithmic in the dimension of quantum states, and therefore establishes a **BQP** upper bound for it. We summarize the results about for the hardness of fidelity estimation in Table I.

TABLE I
HARDNESS OF QUANTUM FIDELITY ESTIMATION.

Restriction	Lower Bound	Upper Bound
General Case	**QSZK**-hard [13]	**EXPTIME** [1]
Low-Rank Case	**DQC1**-hard [34]	**BQP** (this paper)

C. Overview of Our Algorithm

The input model used in our quantum algorithm is usually called the "purified quantum query access" model, which provides (mixed) quantum states by quantum oracles that prepare their purifications. This conventional model is commonly used in quantum algorithms, e.g., [14], [15], [16], [17], [18], [19], [20], and will be introduced in Section II-B.

We sketch the basic idea of our algorithm here, and then describe it in detail later. The goal is to obtain the subnormalized quantum state $\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}$ with a certain probability, and then we can estimate the fidelity $F(\rho, \sigma)$ by evaluating its trace. To achieve this, our algorithm consists of two parts. The first part is a technique that prepares a quantum state that block-encodes the square root of a positive semidefinite operator block-encoded in another quantum state. Here, the notion of block-encoding (see Definition 1) is allowed for encoding a general matrix into a scaled block in a larger matrix, and thus extends the block-encoding defined for unitary operators in [41], [42]. Specifically, suppose that we are given a quantum state which is a block-encoding of a positive semidefinite operator A. Then we are able to prepare another quantum state which is a block-encoding of $\sqrt{A}$. This is achieved through the technique of quantum singular value transformation [42] combined with our new idea of constructing density operators (instead of unitary operators) as block-encodings. The second part uses the technique developed in the first part for multiple times. Suppose we are given two N-dimensional quantum states ρ and σ. Since σ is a block-encoding of itself, we can prepare a quantum state which is a block-encoding of $\sqrt{\sigma}$. This also gives a unitary operator V_σ that is a block-encoding of $\sqrt{\sigma}$ by Lemma 25 of [42]. After applying V_σ on ρ, we obtain a quantum state which is a block-encoding of $\sqrt{\sigma}\rho\sqrt{\sigma}$. Applying the technique again, we obtain a quantum state which is a block-encoding of $\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}$. Finally, we can compute the fidelity $F(\rho, \sigma) = \operatorname{tr}\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)$ by quantum amplitude estimation [43].

An important factor in the performance of our fidelity estimation algorithm is the rank of quantum states. Let r be the lower rank of ρ and σ. Our algorithm has a time complexity $\operatorname{poly}(\log(N), r, 1/\varepsilon)$, where ε is the additive error. As the rank r grows, errors become harder to deal with and the algorithm becomes less efficient. Our algorithm exponentially outperforms the known classical and even quantum algorithms in the case that one of the two quantum states is low-rank, say $r = \operatorname{polylog}(N)$. A quantum state is said to be low-rank if it is supported on a low-dimensional space. Low-rank quantum states are nearly pure and with low entropy, which appear in various important physical settings [24], [44].

Compared to those approaches based on quantum state tomography [22], [23], [24], the strength of our algorithm is that it only uses $\operatorname{polylog}(N)$ qubits, and does not involve classical matrix representations of quantum states. On the other hand, our algorithm works in a more general case than the SWAP test [27], [28], entanglement witnesses [29], [30], [31] and the direct fidelity estimation [32], [33] where one of the states is required to be pure in the latter case. A comparison of various fidelity estimation algorithms is presented in Table II, where N is the dimension of quantum states and r is the lower rank of them. Note that $r = 1$ means one of the quantum states is pure. It should be pointed out that our quantum algorithm requires purified quantum query access to quantum states, while most of other quantum algorithms in Table II require identical copies of quantum states. We argue that our quantum algorithm is particularly useful when the quantum processes that produce these quantum states can be implemented on a quantum computer. Furthermore, given purified quantum query access to density operators, the algorithms that require identical copies can be easily converted to ones with purified quantum query access, while preserving their computational complexity. In this sense, our algorithm can be exponentially faster than the others listed in Table II. Also, if we adopt

---

[1] By direct classical simulation of quantum computation and matrix arithmetic operations.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2022.3203985

the conventional input model commonly used in quantum computational complexity theory where mixed quantum states are given by classical descriptions of quantum circuits that produce their purifications (see [21] for example), then our quantum algorithm can be regarded as a candidate of quantum advantages over classical computing.

D. Related Work

Estimating the "closeness" of quantum states is an important problem in quantum information; in particular, it is closely related to quantum property testing [45]. Except those mentioned above, here we briefly discuss some other related work. A method to test the closeness of N-dimensional mixed quantum states with respect to the trace distance and fidelity was proposed in [46], using $O(N/\varepsilon^2)$ and $O(N/\varepsilon)$ copies of quantum states, respectively. (It is worth mentioning that testing the closeness is weaker than estimating the closeness: taking the fidelity for example, the former task is to distinguish whether the fidelity is close to 1, while the latter one is to find the approximate value of the fidelity.) On the other hand, a quantum algorithm for estimating the trace distance between two quantum states was developed in [16] using $O(N/\varepsilon)$ queries to quantum oracles in the "purified quantum query access" model.

Testing other quantum properties is also a widely studied topic. Most of them focus on the sample complexity (i.e., the number of copies of quantum states that are used in the testing). For example, quantum state tomography and its extensions have been studied in [47], [25], [26], [48], [46]; the sample complexity of testing the orthogonality of two pure quantum states was investigated in [49]; and the sample complexity of estimating the von Neumann entropy and the quantum Rényi entropy was examined in [50]. Although these results were obtained employing the multiple-copy input model, several others were established in the "purified quantum query access" model; for instance, the quantum query complexity of estimating the von Neumann entropy was considered in [16], [19], and a quantum query algorithm for estimating the quantum Rényi entropy was proposed in [20].

In addition, quantum algorithms for testing classical statistical properties have been extensively studied. The first quantum algorithms for testing closeness and identity of probability distributions was given in [51], which were then improved by [52] and [53]. Quantum approach for estimating classical entropies was systematically studied in [54].

E. Recent Developments

After the work described in this paper, several improvements have been made, compared to the complexity $\tilde{O}(r^{12.5}/\varepsilon^{13.5})$[2] stated in Theorem 5.

- Wang et al. [55] improved the quantum query complexity of fidelity estimation in the purified quantum query access model to $\tilde{O}(r^{6.5}/\varepsilon^{7.5})$. Moreover, they proposed quantum algorithms for estimating a wide range of quantum entropies and distances.
- In the concurrent work of Gilyén and Poremba [56], they improved the quantum query complexity of fidelity estimation to $\tilde{O}(r^{2.5}/\varepsilon^{5})$. Moreover, they converted their quantum algorithm for fidelity estimation in the purified quantum access model to the one using $\tilde{O}(r^{5.5}/\varepsilon^{12})$ identical copies of quantum states based on the technique of density matrix exponentiation [57], [49].

F. Organization of This Paper

The rest of this paper is organised as follows. Section II will provide necessary preliminaries. We will formally state our main result in Section III. Then, we will show our technique for solving square roots of positive semidefinite operators in Section IV. Our quantum algorithm for fidelity estimation and an analysis of its complexity will be elaborated in Section V. In Section VI, we will further discuss the hardness of quantum fidelity estimation. We will conclude in Section VII with a brief discussion about applications and extensions of our algorithm.

II. PRELIMINARIES

A. Block-encoding and its extension

The notion of block-encoding was defined in [41], [42] to describe quantum unitary operators, in which certain operators of interest are encoded as scaled matrix blocks. It is proved to be a useful tool in developing quantum algorithms. Different from the original form of block-encoding, our quantum algorithm needs to block-encode a positive semidefinite operator in a density operator rather than in a unitary operator. For this purpose, we extend the definition of block-encodings to general operators as follows.

Definition 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*

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

where the operator norm is defined by

$$\|A\| = \sup_{\sqrt{\langle \psi | \psi \rangle} = 1} \sqrt{\langle \psi | A^\dagger A | \psi \rangle}$$

and $A^\dagger$ is the Hermitian conjugate of A.

Remark 1. *Note that the above definition of block-encodings coincides with that in [41], [42], whenever the block-encoding B is restricted to be unitary. In our extended definition, however, we allow the block-encoding B to be a density operator. When an operator A is block-encoded in a density operator ρ, it means that A can be obtained by measuring ρ on a subsystem (subscripted by a in Definition 1) and post-selecting the outcome 0.*

We will use this extended definition of block-encodings throughout the paper when describing both unitary and density operators.

---

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

TABLE II
COMPARISON OF ALGORITHMS FOR QUANTUM FIDELITY ESTIMATION.

Algorithm	Complexity	Prerequisites	Required Operations
Quantum State Tomography [22], [23], [24]	$\mathrm{poly}(N)$	None	Pauli Measurements
Low-rank Quantum State Tomography [24]	$\mathrm{poly}(N, r)$	r is small	Pauli Measurements
SWAP Test [27], [28]	$\mathrm{polylog}(N)$	$r = 1$	Arbitrary Quantum Operations
Entanglement Witnesses [29], [30], [31]	$\mathrm{polylog}(N)$	Specific Pure States	Pauli Measurements
Direct Fidelity Estimation [32], [33]	$\mathrm{poly}(N)$	$r = 1$	Pauli Measurements
Variational Quantum Algorithm [34], [35], [36]	N/A	r is small	Arbitrary Quantum Operations
Our Algorithm	$\mathrm{poly}(\log(N), r)$	r is small	Arbitrary Quantum Operations

B. Purified quantum query access

The "purified quantum query access" model is widely used in quantum computational complexity and quantum algorithms (e.g., [13], [14], [15], [16], [17], [18], [19], [20]). In this model, mixed quantum states are given by quantum circuits (oracles) that prepare their purifications. Formally, suppose ρ is a mixed quantum state in an N-dimensional Hilbert space. A quantum unitary oracle O_ρ that prepares $|\rho\rangle$ is given as

$$|\rho\rangle = O_\rho |0\rangle_n |0\rangle_{n_\rho},$$

where $N = 2^n$, and $|0\rangle_{n_\rho}$ are ancilla qubits. Here, we write $|0\rangle_a$ to denote $|0\rangle^{\otimes a}$, with the subscript a indicating which (and how many) qubits are involved in the Dirac symbol. This notation is convenient in analysis when more than two disjoint sets of qubits are considered simultaneously. Then ρ is obtained from its purification by tracing out those ancilla qubits:

$$\rho = \mathrm{tr}_{n_\rho}(|\rho\rangle\langle\rho|).$$

We assume that n_ρ is a polynomial in n [3]. In the following, a unitary operator U is said to prepare a mixed quantum state, if U prepares its purification.

Next, we will introduce a useful tool, which can convert a unitary operator that prepares a density operator to another unitary operator that is a block-encoding of the density operator [41], [15], [42].

Theorem 2 (Block-encoding of density operators, Lemma 25 of [42])**.** *Suppose U is an $(n+a)$-qubit unitary operator that prepares an n-qubit density operator ρ. Then there is a $(2n+a)$-qubit unitary operator $\tilde{U}$, which is a $(1, n+a, 0)$-block-encoding of ρ, using 1 query to each of U and $U^\dagger$ and $O(a)$ elementary quantum gates.*

Remark 2. *It is worth mentioning that there is no known method that conversely converts a unitary operator, which is a block-encoding of a density operator, to another unitary operator, which prepares the density operator. This motivates us to directly manipulate density operators rather than unitary operators. It is also why we chose to extend the definition of block-encodings (see Definition 1).*

C. Polynomial eigenvalue transformation

Quantum singular value transformation (QSVT) [42] is a powerful framework in designing quantum algorithms. What we need is the QSVT technique for polynomial eigenvalue transformation.

Theorem 3 (Polynomial eigenvalue transformation, Theorem 31 of [42])**.** *Suppose U is a unitary operator, which is an (α, a, ε)-block-encoding of Hermitian operator A. If $\delta \geq 0$ and $P \in \mathbb{R}[x]$ is a polynomial of degree d such that $|P(x)| \leq 1/2$ for all $x \in [-1, 1]$. Then there is a quantum circuit $\tilde{U}$, which is a $(1, a+2, 4d\sqrt{\varepsilon/\alpha}+\delta)$-block-encoding of $P(A/\alpha)$, using d queries to U and $U^\dagger$, 1 query to controlled-U, and $O((a+1)d)$ elementary quantum gates. Moreover, the description of $\tilde{U}$ can be computed by a classical Turing machine in $\mathrm{poly}(d, \log(1/\delta))$ time.*

Especially, if P is an even or odd polynomial, then $|P(x)| \leq 1/2$ for $x \in [-1, 1]$ can be relaxed to $|P(x)| \leq 1$ for $x \in [-1, 1]$.

In order to apply the polynomial eigenvalue transformation for our purpose, the polynomial approximation of negative power functions is required.

Theorem 4 (Polynomial approximation of negative power functions, Corollary 67 in the full version of [42])**.** *Let $\delta, \varepsilon \in (0, 1/2]$, $c > 0$ and $f(x) = \delta^c x^{-c}/2$. Then there is an even/odd polynomial $P \in \mathbb{R}[x]$ of degree $O\left(\frac{\max\{1,c\}}{\delta}\log\left(\frac{1}{\varepsilon}\right)\right)$ such that $|P(x) - f(x)| \leq \varepsilon$ for $x \in [\delta, 1]$ and $|P(x)| \leq 1$ for $x \in [-1, 1]$.*

III. MAIN RESULT

As discussed in Section II-B), we work in the "purified quantum query access" model. Suppose two (mixed) quantum states ρ and σ in an N-dimensional Hilbert space are given by their corresponding purifications $|\rho\rangle$ and $|\sigma\rangle$; that is, two quantum unitary oracles (circuits) O_ρ and O_σ that prepare $|\rho\rangle$ and $|\sigma\rangle$, respectively, are assumed as follows:

$$|\rho\rangle = O_\rho |0\rangle_n |0\rangle_{n_\rho}, \qquad |\sigma\rangle = O_\sigma |0\rangle_n |0\rangle_{n_\sigma},$$

where $N = 2^n$, $|0\rangle_{n_\rho}$ and $|0\rangle_{n_\sigma}$ are ancilla qubits, and n_ρ and n_σ are polynomials in n. Then ρ and σ are obtained from their purifications by tracing out their corresponding ancilla qubits:

$$\rho = \mathrm{tr}_{n_\rho}(|\rho\rangle\langle\rho|), \qquad \sigma = \mathrm{tr}_{n_\sigma}(|\sigma\rangle\langle\sigma|).$$

In this paper, we use the following definition for $\tilde{O}$:

$$\tilde{O}_{d,e}(f(a,b,c)) = O(f(a,b,c)\mathrm{polylog}(f(a,b,c),d,e)).$$

---

[3] Theoretically, any n-qubit mixed quantum state has a purification with at most n ancilla qubits, so it is sufficient to assume that the number of ancilla qubits is no more than n. However, it could be more convenient to use more than n ancilla qubits in order to prepare a purification of an n-qubit mixed quantum state in practice. That is why we make a more relaxed assumption on the number of ancilla qubits, which is just a polynomial in n.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2022.3203985

Then our main result can be stated as the following:

Theorem 5. *Given quantum oracles O_ρ and O_σ that prepare N-dimensional quantum states ρ and σ, respectively, there is a quantum algorithm that computes the fidelity $F(\rho, \sigma)$ within additive error ε using $\tilde{O}_{r,1/\varepsilon}\left(r^{12.5}/\varepsilon^{13.5}\right)$ queries to these oracles and $\tilde{O}_{N,r,1/\varepsilon}\left(r^{12.5}/\varepsilon^{13.5}\right)$ additional elementary quantum gates, where r is the lower rank of ρ and σ.*

Our algorithm will be presented in the following way. First, we develop a technique to compute the square root of a positive semidefinite operator (see Section IV). Then, we apply this technique multiple times in order to estimate the fidelity (see Section V).

IV. SQUARE ROOT OF POSITIVE SEMIDEFINITE OPERATORS

The key technique of our algorithm is to compute the square root of a positive semidefinite operator stored in a quantum state in the sense of block-encoding. This technique can be described as the following:

Theorem 6 (Square root of positive semidefinite operators block-encoded in density operators)**.** *Suppose:*

1) *ρ is an $(n+a)$-qubit density operator with an $(n+a+b)$-qubit pure quantum state $|\rho\rangle$ being its purification; that is, $\rho = \operatorname{tr}_b(|\rho\rangle\langle\rho|)$. An $(n+a+b)$-qubit unitary operator U_ρ is given to prepare $|\rho\rangle = U_\rho|0\rangle$;*
2) *A is an n-qubit positive semidefinite operator such that ρ is a $(1, a, 0)$-block-encoding of A.*

Then for every real number $\delta, \varepsilon \in (0, 1/2]$, there is an $O(n+a+b)$-qubit quantum circuit U_ϱ such that

- *U_ϱ uses $O(d)$ queries to (controlled-)U_ρ and its inverse and $O(d(n+a+b))$ elementary quantum gates, where $d = O(\log(1/\varepsilon)/\delta)$; and*
- *U_ϱ prepares the purification $|\varrho\rangle = U_\varrho|0\rangle$ of a $(4\delta^{-1/2}, O(n+a+b), \Theta(\delta^{1/2}+\varepsilon\delta^{-1/2}))$-block-encoding ϱ of $\sqrt{A}$.*
- *The description of U_ϱ can be computed by a classical Turing machine in $\operatorname{poly}(d)$ time.*

Proof. Recall Theorem 2 that a unitary operator that prepares a mixed quantum state ρ implies another unitary operator that is a block-encoding of ρ. Then there is a unitary operator $\tilde{U}_A$, which is a $(1, n+a+b, 0)$-block-encoding of ρ, and therefore a $(1, n+2a+b, 0)$-block-encoding of A, using 1 query to U_ρ, and $O(a+b)$ elementary quantum gates.

Let $f(x) = (\delta/x)^{1/4}/2$. By Theorem 4, there is an even polynomial $P(x)$ of degree $O(d)$ such that $|P(x) - f(x)| \le \varepsilon$ for every $x \in [\delta, 1]$ and $|P(x)| \le 1$ for every $x \in [-1, 1]$. By Theorem 3, there is a unitary operator $\tilde{U}_{P(A)}$, which is a $(1, O(n+a+b), \varepsilon)$-block-encoding of $P(A)$ using d queries to $\tilde{U}_A$ and $O(d(n+a+b))$ elementary quantum gates.

Applying $\tilde{U}_{P(A)}$ on ρ, we obtain a density operator ϱ, which is a $(1, O(n+a+b), 0)$-block-encoding of $A(P(A))^2$, and therefore a $(4\delta^{-1/2}, O(n+a+b), \Theta(\delta^{1/2}+\varepsilon\delta^{-1/2}))$-block-encoding of $\sqrt{A}$. To see this, we need to show that

$$\left\| 4\delta^{-1/2} A(P(A))^2 - \sqrt{A} \right\| \le \Theta(\delta^{1/2} + \varepsilon\delta^{-1/2}).$$

Since $0 \le A \le I$, it is sufficient to show that

$$\left| 4\delta^{-1/2} x(P(x))^2 - \sqrt{x} \right| \le \Theta(\delta^{1/2} + \varepsilon\delta^{-1/2})$$

for every $x \in [0, 1]$. We consider two cases as follows.

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

$$\begin{aligned} &\left| 4\delta^{-1/2} x(P(x))^2 - \sqrt{x} \right| \\ &\quad = \left| 4\delta^{-1/2} x(P(x))^2 - 4\delta^{-1/2} x(f(x))^2 \right| \\ &\quad \le 4\delta^{-1/2} |x| \, |P(x) + f(x)| \, |P(x) - f(x)| \\ &\quad \le 8\delta^{-1/2}\varepsilon. \end{aligned}$$

Case 2. $x \in [0, \delta]$. In this case,

$$\begin{aligned} &\left| 4\delta^{-1/2} x(P(x))^2 - \sqrt{x} \right| \\ &\quad \le \left| 4\delta^{-1/2} x(P(x))^2 \right| + \left| \sqrt{x} \right| \le 5\delta^{1/2}. \end{aligned}$$

These yield the proof. □

Theorem 6 is derived following the basic procedure of quantum singular value transformation (QSVT) [42]. But a different idea we used in Theorem 6 is the extension of the block-encoding for *unitary operators* employed in QSVT to that for *density operators*. This new idea enables us to obtain a better complexity. Specifically, if we try to derive the $\sqrt{A}$ in Theorem 6 by QSVT in a similar way of implementing the power function (in our case, the square root function) of an Hermitian matrix block-encoded in a unitary operator [42], [58], [59] (which is, for example, later used to implement the Petz recovery channels [17]), we will meet an additional restriction of $I/\kappa \le A \le I$ for some $\kappa > 0$ [58]. As a result, an unfavorable factor κ is introduced in the complexity, and κ can be arbitrarily large for any density operator A. In contrast, Theorem 6 circumvents this difficulty by preparing density operators as block-encodings rather than unitary operators as in QSVT, and thus makes the complexity of our algorithm independent of the parameter κ.

Our new idea brings another benefit — statistical properties of the operator block-encoded in the density operator of a quantum state can be extracted more easily by measurements; while the same task seems hard for the operator block-encoded in a unitary operator (as in QSVT). For example, given that A is block-encoded in a density operator ϱ of a mixed quantum state, whose purification is prepared by a unitary operator U_ϱ, the trace $\operatorname{tr}(A)$ can be simply evaluated by quantum amplitude estimation [43] (see step 4 in Section V below). However, computing $\operatorname{tr}(A)$ seems to be hard if A is block-encoded in an n-qubit unitary operator U, as there is no known efficient quantum algorithm even to compute $\operatorname{tr}(U)$ within additive error $1/\operatorname{poly}(n)$ — the best known approach has additive error $2^n/\operatorname{poly}(n)$ [38], which is exponentially worse than required. Furthermore, computing $\operatorname{tr}(U)/2^n$ was shown to be **DQC1**-complete [38].

V. FIDELITY ESTIMATION

A. The Algorithm

Now we are able to describe the main algorithm for fidelity estimation. Without loss of generality, we assume that the rank

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2022.3203985

of ρ is lower than or equal to that of σ and let $r = \operatorname{rank}(\rho)$. Note that in this case the state σ only contributes to the fidelity on the support of ρ, because $F(\rho, \sigma) = F(\rho, \Pi_\rho \sigma \Pi_\rho)$, where Π_ρ is the projector onto the support of ρ.

Our algorithm is presented as Algorithm 1. For a better understanding, let us explain it in five steps:

Algorithm 1 Quantum algorithm for fidelity estimation.

```
Input: Quantum oracles $O_\rho$ and $O_\sigma$ that prepare mixed quantum states $\rho$ and $\sigma$, respectively, the desired additive error $\varepsilon > 0$, and $r = \operatorname{rank}(\rho)$.
Output: An approximation of $F(\rho, \sigma)$ within additive error $\varepsilon$ with high probability.
  $\delta_\sigma \leftarrow \tilde{\Theta}(\varepsilon^4/r^4)$.
  $\varepsilon_\sigma \leftarrow \tilde{\Theta}(\varepsilon^4/r^4)$.
  $\delta_\eta \leftarrow \tilde{\Theta}(\varepsilon^6/r^6)$.
  $\varepsilon_\eta \leftarrow \tilde{\Theta}(\varepsilon^6/r^6)$.
  $M \leftarrow \tilde{\Theta}(\varepsilon^{2.5}/r^{3.5})$.
  $V_\sigma$, a unitary operator using $O(\log(1/\varepsilon_\sigma)/\delta_\sigma)$ queries to $O_\sigma$ (by Theorem 6), prepares $\sigma'$ such that $\sigma'$ is a $(4\delta_\sigma^{-1/2}, b, \Theta(\delta_\sigma^{1/2} + \varepsilon_\sigma \delta_\sigma^{-1/2}))$-block-encoding of $\sqrt{\sigma}$, where $b = O(n + n_\sigma)$.
  $W_\sigma$, a unitary operator using $O(1)$ queries to $V_\sigma$ (by Theorem 2), is a $(4\delta_\sigma^{-1/2}, O(n+n_\sigma), \Theta(\delta_\sigma^{1/2}+\varepsilon_\sigma\delta_\sigma^{-1/2}))$-block-encoding of $\sqrt{\sigma}$.
  $U_\eta \leftarrow (W_\sigma \otimes I_{n_\rho})(O_\rho \otimes I_a)$ prepares $\eta$ that (by Claim 7) is a $(16\delta_\sigma^{-1}, a, \Theta(\delta_\sigma^{1/2} + \varepsilon_\sigma\delta_\sigma^{-1/2}))$-block-encoding of $\sqrt{\sigma}\rho\sqrt{\sigma}$, where $a = O(n + n_\sigma)$.
  $V_\eta$, a unitary operator using $O(\log(1/\varepsilon_\eta)/\delta_\eta)$ queries to $U_\eta$ (by Theorem 6), prepares $\eta'$ such that $\eta'$ is a $(4\delta_\eta^{-1/2}, c, \Theta(\delta_\eta^{1/2} + \varepsilon_\eta\delta_\eta^{-1/2}))$-block-encoding of $\sqrt{{}_a\langle 0|\eta|0\rangle_a}$, where $c = O(n + n_\rho + n_\sigma)$.
  $\tilde{x} \leftarrow x \pm \delta$ with high probability, using $O(M)$ queries to $V_\eta$ (by quantum amplitude estimation [43]), where $x = \operatorname{tr}\left({}_c\langle 0|\eta'|0\rangle_c\right)$ and
      $$\delta = 2\pi\frac{\sqrt{x(1-x)}}{M} + \frac{\pi^2}{M^2}.$$
  return $16\tilde{x}/\sqrt{\delta_\eta\delta_\sigma}$.
```

Step 1. Note that σ is a $(1, 0, 0)$-block-encoding of itself, and O_σ prepares its purification $|\sigma\rangle$. By Theorem 6 and introducing two parameters δ_σ and ε_σ, we can obtain a unitary V_σ using $O(\log(1/\varepsilon_\sigma)/\delta_\sigma)$ queries to O_σ that prepares the purification $V_\sigma|0\rangle = |\sigma'\rangle$ of σ', and σ' is a $(4\delta_\sigma^{-1/2}, b, \Theta(\delta_\sigma^{1/2} + \varepsilon_\sigma\delta_\sigma^{-1/2}))$-block-encoding of $\sqrt{\sigma}$, where $b = O(n + n_\sigma)$.

Step 2. By Theorem 2, we can construct a unitary operator W_σ using 1 query to V_σ that is a $(1, O(n + n_\sigma), 0)$-block-encoding of σ', and therefore a $(4\delta_\sigma^{-1/2}, O(n+n_\sigma), \Theta(\delta_\sigma^{1/2} + \varepsilon_\sigma\delta_\sigma^{-1/2}))$-block-encoding of $\sqrt{\sigma}$. By applying W_σ on ρ, we obtain a density operator η that is a $(16\delta_\sigma^{-1}, a, \Theta(\delta_\sigma^{1/2} + \varepsilon_\sigma\delta_\sigma^{-1/2}))$-block-encoding of $\sqrt{\sigma}\rho\sqrt{\sigma}$, where $a = O(n+n_\sigma)$. In other words, $U_\eta = (W_\sigma \otimes I_{n_\rho})(O_\rho \otimes I_a)$ can prepare the purification $U_\eta|0\rangle = |\eta\rangle$ of η. To see this, we note that η is a $(1, a, 0)$-block-encoding of ${}_a\langle 0|\eta|0\rangle_a = \sigma_b'\rho\left(\sigma_b'\right)^\dagger$, where $\sigma_b' = {}_b\langle 0|\sigma'|0\rangle_b$. Here, we note that $\sigma_b'\rho\left(\sigma_b'\right)^\dagger$ is a scaled approximation of $\sqrt{\sigma}\rho\sqrt{\sigma}$ (see Claim 7 for details).

Step 3. Similar to the previous, by Theorem 6 and introducing another two parameters δ_η and ε_η, we find V_η using $O(\log(1/\varepsilon_\eta)/\delta_\eta)$ queries to U_η that prepares η' as a $(4\delta_\eta^{-1/2}, c, \Theta(\delta_\eta^{1/2} + \varepsilon_\eta\delta_\eta^{-1/2}))$-block-encoding of $\sqrt{{}_a\langle 0|\eta|0\rangle_a}$, where $c = O(n + n_\rho + n_\sigma)$. Intuitively, $\sqrt{{}_a\langle 0|\eta|0\rangle_a}$ is approximately proportional to $\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}$ with a scaling factor $16\delta_\sigma^{-1}\delta_\eta^{-1}$.

Step 4. Estimate $\operatorname{tr}\left({}_c\langle 0|\eta'|0\rangle_c\right)$ through V_η by quantum amplitude estimation [43]. More precisely, we can obtain $\tilde{x}$ in $O(M)$ queries to V_η (with high probability) such that

$$|\tilde{x} - x| \le \delta,$$

where

$$\delta = 2\pi\frac{\sqrt{x(1-x)}}{M} + \frac{\pi^2}{M^2}, \quad x = \operatorname{tr}\left({}_c\langle 0|\eta'|0\rangle_c\right).$$

Step 5. Finally, we compute the value of $16\tilde{x}/\sqrt{\delta_\eta\delta_\sigma}$ as our estimation of $F(\rho, \sigma)$. Intuitively, $\tilde{x}$ is an approximation of $\operatorname{tr}\left(\sqrt{{}_a\langle 0|\eta|0\rangle_a}\right) \approx \sqrt{\delta_\eta\delta_\sigma}\operatorname{tr}\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)/16$ as mentioned in step 3.

B. Error Analysis

Now we are going to analyze the error of Algorithm 1. Let $r = \min\{\operatorname{rank}(\rho), \operatorname{rank}(\sigma)\}$. First, we show that $\sigma_b'\rho\left(\sigma_b'\right)^\dagger$ is a scaled approximation of $\sqrt{\sigma}\rho\sqrt{\sigma}$.

Claim 7.

$$\left\|16\delta_\sigma^{-1}\sigma_b'\rho\left(\sigma_b'\right)^\dagger - \sqrt{\sigma}\rho\sqrt{\sigma}\right\| \le \Theta(\delta_\sigma^{1/2} + \varepsilon_\sigma\delta_\sigma^{-1/2}).$$

Proof. Note that

$$\begin{aligned} &16\delta_\sigma^{-1}\sigma_b'\rho\left(\sigma_b'\right)^\dagger - \sqrt{\sigma}\rho\sqrt{\sigma} = \\ &\quad (4\delta_\sigma^{-1/2}\sigma_b' - \sqrt{\sigma})\rho\left(4\delta_\sigma^{-1/2}\sigma_b'\right)^\dagger \\ &\quad + \sqrt{\sigma}\rho\left(\left(4\delta_\sigma^{-1/2}\sigma_b'\right)^\dagger - \sqrt{\sigma}\right). \end{aligned}$$

By the triangle inequality for the operator norm that $\|A+B\| \le \|A\| + \|B\|$ and the sub-multiplicativity that $\|AB\| \le \|A\|\,\|B\|$, we have

$$\begin{aligned} &\left\|16\delta_\sigma^{-1}\sigma_b'\rho\left(\sigma_b'\right)^\dagger - \sqrt{\sigma}\rho\sqrt{\sigma}\right\| \\ &\le \left\|(4\delta_\sigma^{-1/2}\sigma_b' - \sqrt{\sigma})\rho\left(4\delta_\sigma^{-1/2}\sigma_b'\right)^\dagger\right\| \\ &\quad + \left\|\sqrt{\sigma}\rho\left(\left(4\delta_\sigma^{-1/2}\sigma_b'\right)^\dagger - \sqrt{\sigma}\right)\right\| \\ &\le \left\|4\delta_\sigma^{-1/2}\sigma_b' - \sqrt{\sigma}\right\|\|\rho\|\left\|4\delta_\sigma^{-1/2}\sigma_b'\right\| \\ &\quad + \left\|\sqrt{\sigma}\right\|\|\rho\|\left\|\left(4\delta_\sigma^{-1/2}\sigma_b'\right)^\dagger - \sqrt{\sigma}\right\|. \end{aligned}$$

Recall that $\sigma_b' = {}_b\langle 0|\sigma'|0\rangle_b$, where σ' is a $(4\delta_\sigma^{-1/2}, b, \Theta(\delta_\sigma^{1/2} + \varepsilon_\sigma\delta_\sigma^{-1/2}))$-block-encoding of $\sqrt{\sigma}$. That is,

$$\left\|4\delta_\sigma^{-1/2}\sigma_b' - \sqrt{\sigma}\right\| \le \Theta\left(\delta_\sigma^{1/2} + \varepsilon_\sigma\delta_\sigma^{-1/2}\right).$$

This gives that if $\delta_\sigma^{1/2} + \varepsilon_\sigma \delta_\sigma^{-1/2} < 1$, then we have

$$\left\|4\delta_\sigma^{-1/2}\sigma_b'\right\| \leq \left\|4\delta_\sigma^{-1/2}\sigma_b' - \sqrt{\sigma}\right\| + \left\|\sqrt{\sigma}\right\| \leq \Theta(1).$$

Finally, together with $\|\rho\| \leq 1$, $\|\sqrt{\sigma}\| \leq 1$ and $\|A\| = \left\|A^\dagger\right\|$, we have

$$\begin{aligned}
&\left\|16\delta_\sigma^{-1}\sigma_b'\rho\left(\sigma_b'\right)^\dagger - \sqrt{\sigma}\rho\sqrt{\sigma}\right\| \\
&\leq \left\|4\delta_\sigma^{-1/2}\sigma_b' - \sqrt{\sigma}\right\|\left(\left\|4\delta_\sigma^{-1/2}\sigma_b'\right\| + 1\right) \\
&\leq \Theta\left(\delta_\sigma^{1/2} + \varepsilon_\sigma\delta_\sigma^{-1/2}\right).
\end{aligned}$$

□

Next, we show how $\sqrt{{}_a\langle 0|\eta\,|0\rangle_a}$ relates to the fidelity $F(\rho, \sigma)$.

Claim 8.

$$\begin{aligned}
&\left|4\delta_\sigma^{-1/2}\mathrm{tr}\left(\sqrt{{}_a\langle 0|\eta\,|0\rangle_a}\right) - F(\rho,\sigma)\right| \\
&\qquad \leq \Theta\left(r\sqrt{\delta_\sigma^{1/2} + \varepsilon_\sigma\delta_\sigma^{-1/2}}\right).
\end{aligned}$$

Proof. Let

$$J = \frac{\delta_\sigma}{16}\sqrt{\sigma}\rho\sqrt{\sigma} - {}_a\langle 0|\eta\,|0\rangle_a\,.$$

In step 2 of the algorithm, it is shown in Claim 7 that $\left\|16\delta_\sigma^{-1}\,{}_a\langle 0|\eta\,|0\rangle_a - \sqrt{\sigma}\rho\sqrt{\sigma}\right\| \leq \Theta(\delta_\sigma^{1/2} + \varepsilon_\sigma\delta_\sigma^{-1/2})$. This leads to

$$\|J\| \leq \Theta(\delta_\sigma^{3/2} + \varepsilon_\sigma\delta_\sigma^{1/2}).$$

We assume that the eigenvalues of $\delta_\sigma\sqrt{\sigma}\rho\sqrt{\sigma}/16$, ${}_a\langle 0|\eta\,|0\rangle_a$ and J are

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

respectively. In our case, note that $\mu_{r+1} = \cdots = \mu_N = 0$ and $\nu_{r+1} = \cdots = \nu_N = 0$. Since the three operators are all Hermitian, by Weyl's inequality, we have

$$\nu_j + \xi_N \leq \mu_j \leq \nu_j + \xi_1$$

for every $1 \leq j \leq N$. Now for each j, let us consider two cases:

Case 1. $\nu_j \leq 2\|J\|$. In this case, $0 \leq \mu_j \leq 3\|J\|$, and then $\left|\sqrt{\mu_j} - \sqrt{\nu_j}\right| \leq \sqrt{3\|J\|}$.

Case 2. $\nu_j > 2\|J\|$. We have

$$\begin{aligned}
\sqrt{\nu_j} - \sqrt{\|J\|} &\leq \sqrt{\nu_j - \|J\|} \leq \sqrt{\mu_j} \\
&\leq \sqrt{\nu_j + \|J\|} \leq \sqrt{\nu_j} + \sqrt{\|J\|}.
\end{aligned}$$

Then it holds that $\left|\sqrt{\mu_j} - \sqrt{\nu_j}\right| \leq \sqrt{\|J\|}$.

The above two cases together yield that

$$\begin{aligned}
&\left|\mathrm{tr}\left(\sqrt{{}_a\langle 0|\eta\,|0\rangle_a}\right) - \mathrm{tr}\left(\sqrt{\frac{\delta_\sigma}{16}\sqrt{\sigma}\rho\sqrt{\sigma}}\right)\right| \\
&\qquad = \left|\sum_{j=1}^{r}\left(\sqrt{\mu_j} - \sqrt{\nu_j}\right)\right| \leq r\sqrt{3\|J\|}.
\end{aligned}$$

These yield the proof. □

Finally, we establish the relationship between ${}_c\langle 0|\eta'\,|0\rangle_c$ and $\sqrt{{}_a\langle 0|\eta\,|0\rangle_a}$.

Claim 9.

$$\left|\mathrm{tr}\left({}_c\langle 0|\eta'\,|0\rangle_c\right) - \frac{\delta_\eta^{1/2}}{4}\mathrm{tr}\left(\sqrt{{}_a\langle 0|\eta\,|0\rangle_a}\right)\right| \leq \Theta\left(r\left(\delta_\eta + \varepsilon_\eta\right)\right).$$

Proof. In step 3 of the algorithm, we have

$$\left\|4\delta_\eta^{-1/2}\,{}_c\langle 0|\eta'\,|0\rangle_c - \sqrt{{}_a\langle 0|\eta\,|0\rangle_a}\right\| \leq \Theta(\delta_\eta^{1/2} + \varepsilon_\eta\delta_\eta^{-1/2}).$$

We note that ${}_a\langle 0|\eta\,|0\rangle_a = \sigma_b'\rho\left(\sigma_b'\right)^\dagger$, and thus $\mathrm{rank}\left(\sqrt{{}_a\langle 0|\eta\,|0\rangle_a}\right) = \mathrm{rank}({}_a\langle 0|\eta\,|0\rangle_a) \leq \mathrm{rank}(\rho) \leq r$. For the same reason, we have $\mathrm{rank}({}_c\langle 0|\eta'\,|0\rangle_c) \leq r$. Therefore, we have

$$\begin{aligned}
&\left|4\delta_\eta^{-1/2}\mathrm{tr}\left({}_c\langle 0|\eta'\,|0\rangle_c\right) - \mathrm{tr}\left(\sqrt{{}_a\langle 0|\eta\,|0\rangle_a}\right)\right| \\
&\qquad \leq \Theta(r(\delta_\eta^{1/2} + \varepsilon_\eta\delta_\eta^{-1/2})).
\end{aligned}$$

These yield the proof. □

Combining the result of quantum amplitude estimation in step 4 of the algorithm with Claim 7, Claim 8 and Claim 9, we obtain an upper bound of the error of our estimation, which is

$$\begin{aligned}
&\left|\frac{16\tilde{x}}{\sqrt{\delta_\eta\delta_\sigma}} - F(\rho,\sigma)\right| \\
&\qquad \leq \Theta\left(\frac{r(\delta_\eta + \varepsilon_\eta) + \delta}{\sqrt{\delta_\eta\delta_\sigma}} + r\sqrt{\sqrt{\delta_\sigma} + \frac{\varepsilon_\sigma}{\sqrt{\delta_\sigma}}}\right).
\end{aligned} \tag{1}$$

C. Complexity

In Algorithm 1, the number of queries to O_ρ and O_σ is bounded by

$$O\left(\frac{1}{\delta_\sigma}\log\left(\frac{1}{\varepsilon_\sigma}\right) \cdot \frac{1}{\delta_\eta}\log\left(\frac{1}{\varepsilon_\eta}\right) \cdot M\right) = \tilde{O}_{\varepsilon_\sigma,\varepsilon_\eta}\left(\frac{M}{\delta_\sigma\delta_\eta}\right).$$

In order to make the right hand side of Equation (1) $\leq \varepsilon$, we take $\delta_\sigma = \tilde{\Theta}(\varepsilon^4/r^4)$, $\delta_\eta = \tilde{\Theta}(\varepsilon^6/r^6)$, $\delta = \tilde{\Theta}(\varepsilon^6/r^5)$, $\varepsilon_\sigma = \tilde{\Theta}(\varepsilon^4/r^4)$, $\varepsilon_\eta = \tilde{\Theta}(\varepsilon^6/r^6)$ and $M = \tilde{\Theta}(r^{2.5}/\varepsilon^{3.5})$ to minimize the number of queries

$$\tilde{O}_{\varepsilon_\sigma,\varepsilon_\eta}\left(\frac{M}{\delta_\sigma\delta_\eta}\right) = \tilde{O}_{r,\frac{1}{\varepsilon}}\left(\frac{r^{12.5}}{\varepsilon^{13.5}}\right).$$

In addition, the number of elementary quantum gates is $\tilde{O}_{N,r,1/\varepsilon}(r^{12.5}/\varepsilon^{13.5}) = \mathrm{poly}(\log(N), r, 1/\varepsilon)$.

It can be seen that our algorithm exponentially outperforms the best known classical and even quantum algorithms for quantum fidelity estimation when r is small, e.g., $r = \mathrm{polylog}(N)$. In spite of its large exponents of r and ε in the complexity, we believe that our algorithm can be applied on real-world problems, as several quantum-inspired algorithms proposed recently [60], [61] also with large exponents in their complexities are later shown to perform well in practice [62].

VI. HARDNESS

Even though some quantum-inspired algorithms [60], [61] suggest that quantum exponential speedup can disappear in low-rank cases, quantum fidelity estimation still remains hard even under the low-rank assumption as discussed above. To show this, we first formally define LOW-RANK FIDELITY ESTIMATION in the following.

Problem 1 (LOW-RANK FIDELITY ESTIMATION)**.** *Given the description of two quantum circuits O_ρ and O_σ of size* $\operatorname{poly}(n)$ *that prepare purifications of n-qubit (mixed) quantum states ρ and σ, respectively, where the rank of ρ is* $\operatorname{poly}(n)$*, and the additive error $\varepsilon = 1/\operatorname{poly}(n)$, find an estimation of $F(\rho, \sigma)$ within additive error ε.*

Indeed, the description of quantum circuits is not required in our algorithm, but is needed for classical algorithms. It was proved in [34] that a variant of LOW-RANK FIDELITY ESTIMATION is **DQC1**-hard, but the same proof also yields the **DQC1**-hardness of the problem stated here. It is known that **DQC1**-complete problems cannot be efficiently solved by classical computers unless the polynomial hierarchy collapses to the second level [39], [40], which is commonly believed to be false. Therefore, our algorithm could be a candidate that shows the advantage of quantum computers over classical counterparts.

VII. CONCLUSION

In this paper, we proposed a quantum algorithm for quantum fidelity estimation, which yields an exponential speedup over the best known algorithms in the low-rank case. We hope it could be used as a subroutine in developing fidelity-based quantum algorithms [12]. The exponents of some complexity factors in our algorithm are large, but we believe they could be reduced by some more sophisticated techniques (see, for example, [63]). Furthermore, an interesting problem is whether it is possible to keep the advantage of exponential speedup in our algorithm with restricted quantum operations (e.g., Pauli measurements).

One of our main technical results (Theorem 6) can be extended to positive powers (not only square root) of positive semidefinite operator A, and therefore can be used in solving other problems, e.g., computing the sandwiched quantum Rényi relative entropy [64], [65] for $0 < \alpha < 1$:

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

which reduces to the quantum state fidelity $F(\rho, \sigma)$ when $\alpha = 1/2$.

For the topics of future research, it would be interesting to try to adapt our quantum algorithms to computing other quantum information quantities with a similar form to the fidelity $F(\rho, \sigma) = \operatorname{tr}\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)$, such as the von Neumann entropy $S(\rho) = -\operatorname{tr}(\rho \log \rho)$, the quantum relative von Neumann entropy $D(\rho\|\sigma) = \operatorname{tr}\left(\rho(\log\rho - \log\sigma)\right)$, and the quantum relative min-entropy $-\log\left(\operatorname{tr}(\Pi_\rho\sigma)\right)$ [66], where Π_ρ is the projector onto the support of ρ.

ACKNOWLEDGMENT

The authors would like to thank Professor Mark M. Wilde for pointing out the **QSZK**-hardness of fidelity estimation, and Minbo Gao for helpful discussions.

This work has been partly supported by the National Key R&D Program of China (2018YFA0306701) and the National Natural Science Foundation of China (61832015). Z. Zhang was partially supported by the Sydney Quantum Academy, NSW, Australia.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

[2] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Physical Review Letters*, vol. 103, no. 15, p. 150502, 2009.

[3] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467–488, 1982.

[4] D. S. Abrams and S. Lloyd, "Simulation of many-body fermi systems on a universal quantum computer," *Physical Review Letters*, vol. 79, no. 13, pp. 2586–2589, 1997.

[5] M. Freedman, A. Kitaev, and Z. Wang, "Simulation of topological field theories by quantum computers," *Communications in Mathematical Physics*, vol. 227, no. 3, pp. 587–603, 2002.

[6] I. Kassal, S. P. Jordan, P. J. Love, M. Mohseni, and A. Aspuru-Guzik, "Polynomial-time quantum algorithm for the simulation of chemical dynamics," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 105, no. 48, pp. 18 681–86, 2008.

[7] A. Uhlmann, "The "transition probability" in the state space of a *-algebra," *Reports on Mathematical Physics*, vol. 9, no. 2, pp. 273–279, 1976.

[8] R. Jozsa, "Fidelity for mixed quantum states," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2315–2323, 1994.

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[10] B. T. Torosov and N. V. Vitanov, "Smooth composite pulses for high-fidelity quantum information processing," *Physical Review A*, vol. 83, no. 5, p. 053420, 2011.

[11] T. F. Roque, A. A. Clerk, and H. Ribeiro, "Engineering fast high-fidelity quantum operations with constrained interactions," *npj Quantum Information*, vol. 7, no. 1, pp. 1–17, 2021.

[12] F. Shahi and A. T. Rezakhani, "Fidelity-based supervised and unsupervised learning for binary classification of quantum states," *The European Physical Journal Plus*, vol. 136, p. 280, 2021.

[13] J. Watrous, "Limits on the power of quantum statistical zero-knowledge," in *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, 2002, pp. 459–468.

[14] F. G. S. L. Brandão, 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 *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming*, 2019, pp. 27:1–27:14.

[15] J. van Apeldoorn and A. Gilyén, "Improvements in quantum SDP-solving with applications," in *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming*, 2019, pp. 99:1–99:15.

[16] A. Gilyén and T. Li, "Distributional property testing in a quantum world," in *Proceedings of the 11th Innovations in Theoretical Computer Science Conference*, vol. 151, 2020, pp. 25:1–25:19.

[17] A. Gilyén, S. Lloyd, I. Marvian, Y. Quek, and M. M. Wilde, "Quantum algorithm for Petz recovery channels and pretty good measurements," *Physical Review Letters*, vol. 128, no. 22, p. 220502, 2022.

[18] R. Agarwal, S. Rethinasamy, K. Sharma, and M. M. Wilde, "Estimating distinguishability measures on quantum computers," ArXiv e-prints, 2021, arXiv:2108.08406.

[19] T. Gur, M. Hsieh, and S. Subramanian, "Sublinear quantum algorithms for estimating von Neumann entropy," ArXiv e-prints, 2021, arXiv:2111.11139.

[20] S. Subramanian and M. Hsieh, "Quantum algorithm for estimating α-Renyi entropies of quantum states," *Physical Review A*, vol. 104, no. 2, p. 022428, 2021.

[21] J. Watrous, "Quantum computational complexity," ArXiv e-prints, 2008, arXiv:0804.3401.

[22] V. Dodonov and V. Man'ko, "Positive distribution description for spin states," *Physics Letters A*, vol. 229, no. 6, pp. 335–339, 1997.

[23] G. M. d'Ariano, L. Maccone, and M. Paini, "Spin tomography," *Journal of Optics B: Quantum and Semiclassical Optics*, vol. 5, no. 1, p. 77, 2003.

[24] D. Gross, Y. K. Liu, S. T. Flammia, S. Becker, and J. Eisert, "Quantum state tomography via compressed sensing," *Physical Review Letters*, vol. 105, no. 15, p. 150401, 2010.

[25] R. O'Donnell and J. Wright, "Efficient quantum tomography," in *Proceedings of the 48th ACM Symposium on Theory of Computing*, 2016, pp. 899–912.

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

[27] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting," *Physical Review Letters*, vol. 87, no. 16, p. 167902, 2001.

[28] M. Kang, J. Heo, S. Choi, S. Moon, and S. Han, "Implementation of SWAP test for two unknown states in photons via cross-Kerr nonlinearities under decoherence effect," *Scientific Reports*, vol. 9, no. 1, p. 6167, 2019.

[29] Y. Tokunaga, T. Yamamoto, M. Koashi, and N. Imoto, "Fidelity estimation and entanglement verification for experimentally produced four-qubit cluster states," *Physical Review A*, vol. 74, p. 020301(R), 2006.

[30] O. Gühne, C.-Y. Lu, W.-B. Gao, and J.-W. Pan, "Toolbox for entanglement detection and fidelity estimation," *Physical Review A*, vol. 76, p. 030305(R), 2007.

[31] O. Gühne and G. Tóth, "Entanglement detection," *Physics Reports*, vol. 474, no. 1-6, pp. 1–75, 2009.

[32] S. T. Flammia and Y.-K. Liu, "Direct fidelity estimation from few pauli measurements," *Physical Review Letters*, vol. 106, p. 230501, 2011.

[33] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, "Practical characterization of quantum devices without tomography," *Physical Review Letters*, vol. 107, p. 210404, 2011.

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

[35] R. Chen, Z. Song, X. Zhao, and X. Wang, "Variational quantum algorithms for trace distance and fidelity estimation," *Quantum Science and Technology*, vol. 7, no. 1, p. 015019, 2022.

[36] K. C. Tan and T. Volkoff, "Variational quantum algorithms to estimate rank, quantum entropies, fidelity, and fisher information via purity minimization," *Physical Review Research*, vol. 3, no. 3, p. 033251, 2021.

[37] L. Bittel and M. Kliesch, "Training variational quantum algorithms is NP-hard," *Physical Review Letters*, vol. 127, no. 12, p. 120502, 2021.

[38] E. Knill and R. Laflamme, "Power of one bit of quantum information," *Physical Review Letters*, vol. 81, p. 5672, 1998.

[39] T. Morimae, "Hardness of classically sampling the one-clean-qubit model with constant total variation distance error," *Physical Review A*, vol. 96, p. 040302(R), 2017.

[40] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, "Impossibility of classically simulating one-clean-qubit model with multiplicative error," *Physical Review Letters*, vol. 120, p. 200502, 2018.

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

[42] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe, "Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, 2019, pp. 193–204.

[43] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *Quantum Computation and Information*, vol. 305, pp. 53–74, 2002.

[44] H. Li and F. D. M. Haldane, "Entanglement spectrum as a generalization of entanglement entropy: Identification of topological order in non-Abelian fractional quantum hall effect states," *Physical Review Letters*, vol. 101, no. 1, p. 010504, 2008.

[45] A. Montanaro and R. de Wolf, "A survey of quantum property testing," *Theory of Computing Library, Graduate Surveys*, vol. 7, pp. 1–81, 2016.

[46] C. Bădescu, R. O'Donnell, and J. Wright, "Quantum state certification," in *Proceedings of the 51st ACM Symposium on Theory of Computing*, 2019, pp. 503–514.

[47] R. O'Donnell and J. Wright, "Quantum spectrum testing," in *Proceedings of the 47th ACM Symposium on Theory of Computing*, 2015, pp. 529–538.

[48] ——, "Efficient quantum tomography II," in *Proceedings of the 49th ACM Symposium on Theory of Computing*, 2017, pp. 962–974.

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

[50] J. Acharya, I. Issa, N. V. Shende, and A. B. Wagne, "Measuring quantum entropy," in *2019 IEEE International Symposium on Information Theory*, 2019, pp. 3012–3016.

[51] S. Bravyi, A. W. Harrow, and A. Hassidim, "Quantum algorithms for testing properties of distributions," *IEEE Transactions on Information Theory*, vol. 57, no. 6, pp. 3971–3981, 2011.

[52] A. Montanaro, "Quantum speedup of Monte Carlo methods," *Proceedings of the Royal Society A*, vol. 471, no. 2181, p. 20150301, 2015.

[53] S. Chakraborty, E. Fischer, A. Matsliah, and R. de Wolf, "New results on quantum property testing," in *Proceedings of the 30th International Conference on Foundations of Software Technology and Theoretical Computer Science*, vol. 8, 2010, pp. 145–156.

[54] T. Li and X. Wu, "Quantum query complexity of entropy estimation," *IEEE Transactions on Information Theory*, vol. 65, no. 5, pp. 2899–2921, 2019.

[55] Q. Wang, J. Guan, J. Liu, Z. Zhang, and M. Ying, "New quantum algorithms for computing quantum entropies and distances," ArXiv e-prints, 2022, arXiv:2203.13522.

[56] A. Gilyén and A. Poremba, "Improved quantum algorithms for fidelity estimation," ArXiv e-prints, 2022, arXiv:2203.15993.

[57] S. Lloyd, M. Mohseni, and P. Rebentrost, "Quantum principal component analysis," *Nature Physics*, vol. 10, pp. 631–633, 2014.

[58] S. Chakraborty, A. Gilyén, and S. Jeffery, "The power of block-encoded matrix powers: improved regression techniques via faster hamiltonian simulation," in *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming*, 2019, pp. 33:1–33:14.

[59] A. Gilyén, "Quantum singular value transformation & its algorithmic applications," Ph.D. dissertation, University of Amsterdam, Amsterdam: Institute for Logic, Language and Computation, 2019.

[60] A. Gilyén, S. Lloyd, and E. Tang, "Quantum-inspired low-rank stochastic regression with logarithmic dependence on the dimension," ArXiv e-prints, 2018, arXiv:1811.04909.

[61] E. Tang, "A quantum-inspired classical algorithm for recommendation systems," in *Proceedings of the 51st Annual Symposium on Theory of Computing*, 2019, pp. 219–228.

[62] J. M. Arrazola, A. Delgado, B. R. Bardhan, and S. Lloyd, "Quantum-inspired algorithms in practice," *Quantum*, vol. 4, p. 307, 2020.

[63] A. Ambainis, "Variable time amplitude amplification and quantum algorithms for linear algebra problems," in *Proceedings of the 29th Symposium on Theoretical Aspects of Computer Science*, 2012, pp. 636–647.

[64] 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," *Communications in Mathematical Physics*, vol. 331, no. 2, pp. 593–622, 2014.

[65] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," *Journal of Mathematical Physics*, vol. 54, no. 12, p. 122203, 2013.

[66] N. Datta, "Min- and max-relative entropies and a new entanglement monotone," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2816–2826, 2009.

PLACE
PHOTO
HERE

Qisheng Wang received the B.Sc. degree and Ph.D. degree from the Department of Computer Science and Technology, Tsinghua University, China, in 2017 and 2022, respectively. His research interests include quantum algorithms, quantum circuits, and formal models of quantum computing.

This article has been accepted for publication in IEEE Transactions on Information Theory. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIT.2022.3203985

PLACE
PHOTO
HERE

Zhicheng Zhang received his B.E. degree from University of Chinese Academy of Sciences, China, in 2021. He is currently working toward the PhD degree at Centre for Quantum Software and Information, University of Technology Sydney, Australia. His research interests include quantum computing and quantum algorithms.

PLACE
PHOTO
HERE

Kean Chen received the B.E. and M.E. degrees from the Department of Electronic Engineering, Shanghai Jiao Tong University, China, in 2017 and 2020, respectively. He is currently working toward the PhD degree at the Institute of Software, Chinese Academy of Sciences, China. His current research interests include quantum computing and quantum information.

PLACE
PHOTO
HERE

Ji Guan received his bachelor's degree in mathematics from Sichuan University, China, in 2014, and then obtained his Ph.D. degree in computer science from University of Technology Sydney, Australia, in 2018. He is currently a faculty researcher at the Institute of Software, Chinese Academy of Sciences. His primary research interests are trustworthy quantum machine learning and model checking quantum systems.

PLACE
PHOTO
HERE

Wang Fang received his B.Sc. degree from the Department of Mathematics, Nanjing University, China, in 2018. He is currently working toward the Ph.D. degree at the Institute of Software, Chinese Academy of Sciences, China. His current research interests include quantum computing and quantum information.

PLACE
PHOTO
HERE

Junyi Liu received his B.E. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China, in 2017. He is currently working toward the Ph.D. degree at the Institute of Software, Chinese Academy of Sciences, China. His current research interests include quantum programming and quantum algorithms.

PLACE
PHOTO
HERE

Mingsheng Ying received the graduation degree from Fuzhou Teachers College, Jiangxi, China, in 1981. He had been a Distinguished Professor and Research Director of the Centre for Quantum Software and Information, University of Technology Sydney, Australia. He is currently a Research Professor and Deputy Director for Research of the Institute of Software, Chinese Academy of Sciences; and Cheung Kong Professor in the Department of Computer Science and Technology, Tsinghua University, China. His research interests are quantum computing, programming theory, and logics in artificial intelligence. 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). Currently, he serves as (Co-)Editor-in-Chief of *ACM Transactions on Quantum Computing*.