Optimal Quantum Algorithm for Estimating Fidelity to a Pure State

Wang Fang
School of Informatics, University of Edinburgh, UK

Qisheng Wang
School of Informatics, University of Edinburgh, UK

Abstract

We present an *optimal* quantum algorithm for fidelity estimation between two quantum states when one of them is pure. In particular, the (square root) fidelity of a mixed state to a pure state can be estimated to within additive error ε by using $\Theta(1/\varepsilon)$ queries to their state-preparation circuits, achieving a quadratic speedup over the folklore $O(1/\varepsilon^2)$. Our approach is technically simple, and can moreover estimate the quantity $\sqrt{\mathrm{tr}(\rho\sigma^2)}$ that is not common in the literature. To the best of our knowledge, this is the *first* query-optimal approach to fidelity estimation involving mixed states.

2012 ACM Subject Classification Theory of computation → Quantum query complexity; Theory of computation → Quantum information theory

Keywords and phrases Quantum computing, fidelity estimation, quantum algorithms, quantum query complexity

Digital Object Identifier 10.4230/LIPIcs.ESA.2025.4

Related Version *Full Version*: `https://arxiv.org/abs/2506.23650` [6]

Funding *Wang Fang*: Supported by the Engineering and Physical Sciences Research Council under Grant EP/X025551/1.
Qisheng Wang: Supported by the Engineering and Physical Sciences Research Council under Grant EP/X026167/1.

1 Introduction

The fidelity between quantum states [24, 13] is a closeness measure that is commonly used in quantum physics and quantum computing [20, 34, 12, 33]. Formally, for two (mixed) quantum states ρ and σ, their (square root) fidelity is defined by (see [20, Equation (9.53)])

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

The fidelity is generally bounded by $0 \leq \mathrm{F}(\rho,\sigma) \leq 1$. In particular, when $\mathrm{F}(\rho,\sigma) = 1$, the two states ρ and σ are identical; and when $\mathrm{F}(\rho,\sigma) = 0$, the two states are orthogonal.

The estimation of fidelity turns out to be central in quantum property testing (cf. [18]). The earliest approach is now known as the SWAP test [5], allowing us to estimate to within additive error ε the squared fidelity $\mathrm{F}^2(\rho,\sigma) = \mathrm{tr}(\rho\sigma)$ when ρ and σ are pure states, using $O(1/\varepsilon^2)$ samples of ρ and σ. Moreover, the squared fidelity $\mathrm{F}^2(\rho,\sigma)$ for pure states ρ and σ can be estimated using $O(1/\varepsilon)$ queries to their state-preparation circuits through the SWAP test [5] equipped with quantum amplitude estimation [4]. The approach based on the SWAP test has been found to have various applications [21]. Fidelity estimation for pure states was also considered in some restricted models: a direct fidelity estimation [7] was proposed when only Pauli measurements are allowed and a distributed approach was developed in [1]. Recently, query-optimal and sample-optimal quantum algorithms for estimating the fidelity $\mathrm{F}(\rho,\sigma) = \sqrt{\mathrm{tr}(\rho\sigma)}$ for pure states ρ and σ have been found in [25] and [28], respectively.

Table 1 Complexity of estimating the fidelity $\mathrm{F}(\rho,\sigma)$.

Reference	Condition	Complexity	Notes
[5]	One of ρ and σ is pure	$O(1/\varepsilon^4)$ samples	/
[5, 4]		$O(1/\varepsilon^2)$ queries	/
This Work		$\mathbf{\Theta(1/\varepsilon)}$ **queries**	**Optimal**
[25]	Both ρ and σ are pure	$\Theta(1/\varepsilon)$ queries	Optimal
[28]		$\Theta(1/\varepsilon^2)$ samples	Optimal
[29, 26, 10]	Either ρ or σ is of rank r	$\mathrm{poly}(r,1/\varepsilon)$ queries	/
[10]		$\mathrm{poly}(r,1/\varepsilon)$ samples	/
[15]	$\rho,\sigma \geq I/\kappa$	$\mathrm{poly}(\kappa)\cdot\widetilde{\Theta}(1/\varepsilon)$ queries	Almost optimal in ε
		$\mathrm{poly}(\kappa,1/\varepsilon)$ samples	/

Although fidelity estimation is known to be BQP-complete when one of the quantum states is pure [22], fidelity estimation for mixed states is QSZK-hard in general [31, 32], which means that there is no polynomial-time quantum algorithm for fidelity estimation unless BQP = QSZK. Nevertheless, efficient quantum algorithms for fidelity estimation for low-rank states were recently discovered [29] and later improved [26, 10] with time complexity $\mathrm{poly}(r,1/\varepsilon)$, where r is the rank of the states. Quantum algorithms for fidelity estimation for well-conditioned states was recently proposed with query complexity $\mathrm{poly}(\kappa)\cdot\widetilde{O}(1/\varepsilon)$ [15], achieving almost optimal dependence on the precision ε, where κ is the condition number such that $\rho,\sigma \geq I/\kappa$.

In this paper, we present an optimal quantum algorithm for estimating the fidelity of a mixed state ρ to a pure state $\sigma = |\psi\rangle\langle\psi|$, using queries to the state-preparation circuits of both states. The input model is known as the "*purified quantum query access*" model, where we assume query access to (the controlled version of) a quantum unitary oracle that prepares the purification of the input quantum state, and its inverse. This input model is commonly employed in quantum computational complexity [31] and quantum algorithms [8]. Our main result is stated in the following theorem.

▶ **Theorem 1** (Estimating fidelity to a pure state, Theorem 6 simplified)**.** *Given purified quantum query access to a mixed state ρ and a pure state $\sigma = |\psi\rangle\langle\psi|$, the fidelity $\mathrm{F}(\rho,\sigma) = \sqrt{\langle\psi|\rho|\psi\rangle}$ can be estimated to within additive error ε with query complexity $O(1/\varepsilon)$.*

Prior to the result of Theorem 1, we are only aware of a folklore quantum algorithm based on the SWAP test (which was mentioned above and will be explained in detail in Section 3.1). This folklore approach computes $\mathrm{F}^2(\rho,\sigma) = \langle\psi|\rho|\psi\rangle$ to within additive error ε with query complexity $O(1/\varepsilon)$, thereby resulting in a query complexity of $O(1/\varepsilon^2)$ for estimating $\mathrm{F}(|\psi\rangle,\rho)$ to within additive error ε. By comparison, Theorem 1 exhibits a quadratic improvement.

The quantum query algorithm given in Theorem 1 generalizes the pure-state fidelity estimation in [25] where unitary oracles are required to directly prepare the pure states. In comparison, our result in Theorem 1 allows the unitary oracles to have redundant output qubits (see Section 5 for more details).

Our approach is actually optimal, as it can be used to estimate the fidelity between two pure states and the quantum query lower bound $\Omega(1/\varepsilon)$ is due to [2, 19] (noted in [25]). In Section 6, we further show that the optimality holds even if ρ is of an arbitrary rank.

We compare fidelity estimations for pure states in Table 1.

As a bonus, our approach in Theorem 1 can further estimate the quantity $\sqrt{\mathrm{tr}(\rho\sigma^2)}$ with optimal query complexity (see Section 4.2), which is of independent interest as this quantity is not common in the literature.

Organization of this paper. We give a formal definition of the purified quantum query access model and the problem statement of fidelity estimation in Section 2. Then, we review previous approaches in Section 3 with their subroutines. In Section 4, we present our approach and its generalization. An implication of our results is discussed in Section 5. Lower bounds for fidelity estimation are given in Section 6. Finally, a brief discussion is drawn in Section 7.

2 Problem Settings

In this paper, we assume purified quantum query access to the input quantum states. This input model is widely used in the literature, e.g., [8, 23, 11, 10, 30, 27, 16].

▶ **Definition 2** (Purified quantum query access). *For a mixed quantum state ρ, purified quantum query access to ρ means query access to a unitary oracle U that prepares a purification of ρ. Specifically, suppose U_{AB} acts on two subsystems A and B, then $\rho_{\mathsf{A}} = \mathrm{tr}_{\mathsf{B}}(|\rho\rangle\langle\rho|_{\mathsf{AB}})$, where $|\rho\rangle_{\mathsf{AB}} = U_{\mathsf{AB}}|0\rangle_{\mathsf{AB}}$. Moreover, we are allowed to use queries to (controlled-)U and its inverse.*

We consider the problem of fidelity estimation, formally stated as follows.

▶ **Problem 1** (Fidelity estimation). *Given purified quantum query access to two mixed quantum states ρ and σ, the task is to compute $\mathrm{F}(\rho,\sigma)$ to within additive error ε.*

In particular, this paper focuses on the case of Problem 1 where $\sigma = |\psi\rangle\langle\psi|$ is pure.

3 Warm-Ups

As a warm-up, we review the previous approaches to fidelity estimation involving pure states, together with their useful subroutines.

3.1 SWAP Test

It is well known that the SWAP test [5] can be used to estimate the fidelity $\mathrm{F}(\rho,\sigma)$ when one of ρ and σ is pure. In particular, if $\sigma = |\psi\rangle\langle\psi|$ is pure, the SWAP test on input ρ and σ (see Figure 1) outputs a bit $x \in \{0,1\}$ such that (adapted from [14, Proposition 9])

$$\Pr[x=0] = \frac{1+\mathrm{F}^2(\rho,|\psi\rangle)}{2}. \tag{1}$$

With this, we can estimate $\mathrm{F}(\rho,|\psi\rangle)$. Specifically, suppose that $\tilde{p}$ is an estimate of $\Pr[x=0]$ such that $|\tilde{p}-\Pr[x=0]| \le \delta$. Then, it can be shown that $\sqrt{2\tilde{p}-1}$ is an estimate of $\mathrm{F}(\rho,|\psi\rangle)$ with $|\sqrt{2\tilde{p}-1} - \mathrm{F}(\rho,|\psi\rangle)| \le \Theta(\sqrt{\delta})$. An estimate of $\mathrm{F}(\rho,|\psi\rangle)$ to within additive error ε can be obtained by setting $\delta = \Theta(\varepsilon^2)$.

To estimate $\mathrm{F}(\rho,|\psi\rangle)$ when given purified quantum query access to ρ and $|\psi\rangle$, we need the quantum subroutine for amplitude estimation [4].

▶ **Theorem 3** (Quantum amplitude estimation, [4]). *Suppose that U is a unitary operator such that $U|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}} = \sqrt{p}|0\rangle_{\mathsf{A}}|\varphi_0\rangle_{\mathsf{B}} + \sqrt{1-p}|1\rangle_{\mathsf{A}}|\varphi_1\rangle_{\mathsf{B}}$, where $p \in [0,1]$ and $|\varphi_0\rangle, |\varphi_1\rangle$ are normalized pure states. Then, we can estimate p to within additive error δ using $O(1/\delta)$ queries to (controlled-)U and its inverse.*

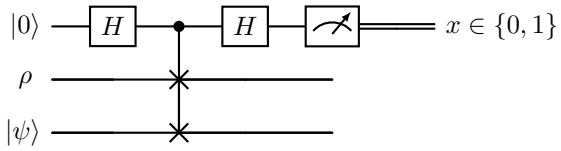

Figure 1 The SWAP test for estimating $\mathrm{F}(\rho, |\psi\rangle)$.

By Theorem 3, we can therefore obtain an estimate of $\mathrm{F}(\rho, |\psi\rangle)$ to within additive error ε using $O(1/\varepsilon^2)$ queries to the state-preparation circuits of ρ and $|\psi\rangle$, based on the SWAP test in Figure 1.

3.2 Pure-State Fidelity Estimation

Recently, a new approach was proposed in [25] for estimating the fidelity $\mathrm{F}(|\varphi\rangle, |\psi\rangle)$ between two pure quantum states $|\varphi\rangle$ and $|\psi\rangle$, improving the folklore approach in Section 3.1. However, the approach in [25] assumes a slightly more restricted input model, where U_φ and U_ψ are two unitary quantum circuits that respectively prepare $|\varphi\rangle$ and $|\psi\rangle$, i.e., $U_\varphi|0\rangle = |\varphi\rangle$ and $U_\psi|0\rangle = |\psi\rangle$.

The key idea of [25] is to *encode* the value of $\mathrm{F}(|\varphi\rangle, |\psi\rangle)$ in the amplitudes of a quantum state, rather than the $\sqrt{(1+\mathrm{F}^2(|\varphi\rangle, |\psi\rangle))/2}$ (in Equation (1)). Specifically, $\mathrm{F}(|\varphi\rangle, |\psi\rangle)$ can be encoded by the unitary operator $W = U_\varphi^\dagger U_\psi$ such that

$$W|0\rangle = \mathrm{F}(|\varphi\rangle, |\psi\rangle)|0\rangle + |\perp\rangle, \tag{2}$$

where $|\perp\rangle$ is an (unnormalized) pure state that is orthogonal to $|0\rangle$. The circuit W is depicted in Figure 2 and it outputs a bit $x \in \{0,1\}$ such that

$$\Pr[x = 0] = \mathrm{F}^2(|\varphi\rangle, |\psi\rangle). \tag{3}$$

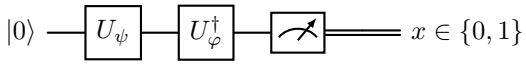

Figure 2 The quantum circuit for estimating $\mathrm{F}(|\varphi\rangle, |\psi\rangle)$.

Finally, the value of $\mathrm{F}(|\varphi\rangle, |\psi\rangle)$ can be estimated by the square root amplitude estimation provided in [25].

▶ **Theorem 4** (Quantum square root amplitude estimation, [25, Theorem I.5]). *Suppose that U is a unitary operator such that $U|0\rangle_\mathsf{A}|0\rangle_\mathsf{B} = \sqrt{p}|0\rangle_\mathsf{A}|\varphi_0\rangle_\mathsf{B} + \sqrt{1-p}|1\rangle_\mathsf{A}|\varphi_1\rangle_\mathsf{B}$, where $p \in [0,1]$ and $|\varphi_0\rangle, |\varphi_1\rangle$ are normalized pure states. Then, we can estimate $\sqrt{p}$ to within additive error δ using $O(1/\delta)$ queries to (controlled-)U and its inverse.*

For convenience, throughout this paper, we use $\mathsf{SqrtAmpEst}(U, \varepsilon)$ *to denote (the returned value of) the square root amplitude estimation process.*

Compared to Theorem 3, Theorem 4 gives an estimate of $\sqrt{p}$ (instead of p), thereby allowing us to skip taking square roots. By Theorem 4, we can therefore obtain an estimate of $\mathrm{F}(|\varphi\rangle, |\psi\rangle)$ to within additive error ε using $O(1/\varepsilon)$ queries to the state-preparation circuits of $|\varphi\rangle$ and $|\psi\rangle$, based on the construction of W in Equation (2).

4 Our Approach

For the task of estimating the fidelity $\mathrm{F}(\rho, |\psi\rangle)$ of a mixed state to a pure state, the approach in Section 3.1 only gives a query complexity of $O(1/\varepsilon^2)$, while the approach in Section 3.2, however, turns out not to be applicable (as a more restricted input model is assumed). In this section, we present a simple quantum algorithm that estimates $\mathrm{F}(\rho, |\psi\rangle)$ to within additive error ε using $O(1/\varepsilon)$ queries to the state-preparation circuits of ρ and $|\psi\rangle$.

Suppose that the purified quantum query access to ρ and $|\psi\rangle$ is given by two quantum circuits U and V, respectively:

$$U_{\mathsf{AB}}|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}} = |\rho\rangle_{\mathsf{AB}}, \tag{4}$$

$$V_{\mathsf{A'B'}}|0\rangle_{\mathsf{A'}}|0\rangle_{\mathsf{B'}} = |\psi\rangle_{\mathsf{A'}}|\psi'\rangle_{\mathsf{B'}}, \tag{5}$$

where $\rho_{\mathsf{A}} = \mathrm{tr}_{\mathsf{B}}(|\rho\rangle\langle\rho|_{\mathsf{AB}})$ and $|\psi'\rangle_{\mathsf{B'}}$ is any pure state. Here, A, B, $\mathsf{A'}$, and $\mathsf{B'}$ are subscripts of subsystems for clarity, where the subsystems A and $\mathsf{A'}$ have the same dimension. Without loss of generality, we can also assume that the subsystems B and $\mathsf{B'}$ have the same dimension.[1]

4.1 Fidelity to a Pure State

Our idea is to encode $\mathrm{F}(\rho, |\psi\rangle)$ in the amplitudes of an efficiently preparable quantum state, and then take use of the square root amplitude estimation in Theorem 4. To this end, we present a quantum circuit

$$W = (V_{\mathsf{AB}}^{\dagger} \otimes I_{\mathsf{A'B'}}) \cdot \mathsf{SWAP}_{\mathsf{BB'}} \cdot (U_{\mathsf{AB}} \otimes V_{\mathsf{A'B'}}). \tag{6}$$

This circuit is depicted in Figure 3 and it outputs two bits $x_{\mathsf{A}}, x_{\mathsf{B}} \in \{0, 1\}$ such that

$$\Pr[x_{\mathsf{A}} = x_{\mathsf{B}} = 0] = \mathrm{F}^2(\rho, |\psi\rangle). \tag{7}$$

Equation (7) is comparable to Equation (1) for the SWAP test and Equation (3) for the pure-state fidelity estimation, and it can be verified by the following proposition.

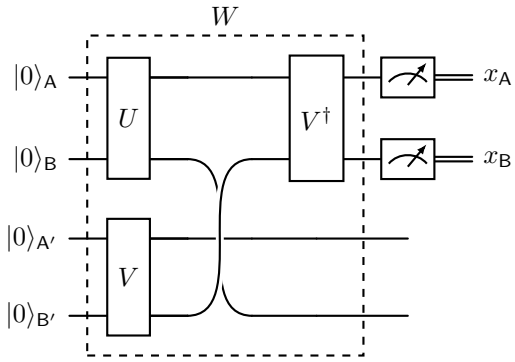

Figure 3 The encoding unitary operator W for $\mathrm{F}(\rho, |\psi\rangle)$.

▶ **Proposition 5.** *$\|(\langle 0|_{\mathsf{A}}\langle 0|_{\mathsf{B}} \otimes I_{\mathsf{A'B'}})W|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|0\rangle_{\mathsf{A'}}|0\rangle_{\mathsf{B'}}\|^2 = \mathrm{F}^2(\rho, |\psi\rangle)$, where W is defined by Equation (6), U_{AB} is defined by Equation (4), and $V_{\mathsf{A'B'}}$ is defined by Equation (5).*

[1] If the subsystem B has a larger dimension than $\mathsf{B'}$, then $V_{\mathsf{A'B'}} \otimes I_{\mathsf{C}}$ (for certain subsystem C) can be a purified quantum query oracle for $|\psi\rangle$ with the ancilla system $\mathsf{B'C}$ having the same dimension as B. A similar construction also applies to the case that the subsystem $\mathsf{B'}$ has a larger dimension than B.

Proof. This can be shown by direct calculations.

$$
\begin{aligned}
&\|(\langle 0|_{\mathsf{A}}\langle 0|_{\mathsf{B}} \otimes I_{\mathsf{A}'\mathsf{B}'})W|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|0\rangle_{\mathsf{A}'}|0\rangle_{\mathsf{B}'}\|^2 \\
&= \left\|(\langle 0|_{\mathsf{A}}\langle 0|_{\mathsf{B}} \otimes I_{\mathsf{A}'\mathsf{B}'})(V_{\mathsf{AB}}^{\dagger} \otimes I_{\mathsf{A}'\mathsf{B}'}) \cdot \mathsf{SWAP}_{\mathsf{BB}'} \cdot (U_{\mathsf{AB}} \otimes V_{\mathsf{A}'\mathsf{B}'})|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|0\rangle_{\mathsf{A}'}|0\rangle_{\mathsf{B}'}\right\|^2 \\
&= \|(\langle \psi|_{\mathsf{A}}\langle \psi'|_{\mathsf{B}} \otimes I_{\mathsf{A}'\mathsf{B}'}) \cdot \mathsf{SWAP}_{\mathsf{BB}'} \cdot |\rho\rangle_{\mathsf{AB}}|\psi\rangle_{\mathsf{A}'}|\psi'\rangle_{\mathsf{B}'}\|^2 \\
&= \|(\langle \psi|_{\mathsf{A}} \otimes I_{\mathsf{BA}'} \otimes \langle \psi'|_{\mathsf{B}'}) \cdot |\rho\rangle_{\mathsf{AB}}|\psi\rangle_{\mathsf{A}'}|\psi'\rangle_{\mathsf{B}'}\|^2 \\
&= \|(\langle \psi|_{\mathsf{A}} \otimes I_{\mathsf{BA}'}) \cdot |\rho\rangle_{\mathsf{AB}}|\psi\rangle_{\mathsf{A}'}\|^2 \\
&= \langle \rho|_{\mathsf{AB}}\langle \psi|_{\mathsf{A}'} \cdot (|\psi\rangle\langle\psi|_{\mathsf{A}} \otimes I_{\mathsf{BA}'}) \cdot |\rho\rangle_{\mathsf{AB}}|\psi\rangle_{\mathsf{A}'} \\
&= \langle \rho|_{\mathsf{AB}} \cdot (|\psi\rangle\langle\psi|_{\mathsf{A}} \otimes I_{\mathsf{B}}) \cdot |\rho\rangle_{\mathsf{AB}} \\
&= \operatorname{tr}\big((|\psi\rangle\langle\psi|_{\mathsf{A}} \otimes I_{\mathsf{B}}) \cdot |\rho\rangle\langle\rho|_{\mathsf{AB}}\big) \\
&= \operatorname{tr}\Big(\operatorname{tr}_{\mathsf{B}}\big((|\psi\rangle\langle\psi|_{\mathsf{A}} \otimes I_{\mathsf{B}}) \cdot |\rho\rangle\langle\rho|_{\mathsf{AB}}\big)\Big) \\
&= \operatorname{tr}\big(|\psi\rangle\langle\psi|_{\mathsf{A}} \cdot \operatorname{tr}_{\mathsf{B}}(|\rho\rangle\langle\rho|_{\mathsf{AB}})\big) \\
&= \operatorname{tr}(|\psi\rangle\langle\psi|_{\mathsf{A}} \cdot \rho_{\mathsf{A}}) \\
&= \mathrm{F}^2(\rho, |\psi\rangle).
\end{aligned}
$$

◀

According to Proposition 5, we can write

$$
W|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|0\rangle_{\mathsf{A}'}|0\rangle_{\mathsf{B}'} = \mathrm{F}(\rho, |\psi\rangle)|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\phi\rangle_{\mathsf{A}'\mathsf{B}'} + \sqrt{1 - \mathrm{F}^2(\rho, |\psi\rangle)}|\phi^{\perp}\rangle_{\mathsf{ABA}'\mathsf{B}'} \tag{8}
$$

for some normalized pure states $|\phi\rangle$ and $|\phi^{\perp}\rangle$ such that $(|0\rangle\langle 0|_{\mathsf{A}} \otimes |0\rangle\langle 0|_{\mathsf{B}} \otimes I_{\mathsf{A}'\mathsf{B}'})|\phi^{\perp}\rangle = 0$. With this, we can therefore estimate $\mathrm{F}(\rho, |\psi\rangle)$ using the square root amplitude estimation (Theorem 4). We formally state the result and give its rigorous proof as follows.

Algorithm 1 Quantum query algorithm for estimating fidelity to a pure state.

Input: Quantum oracles U and V that prepare n-qubit purifications of a k-qubit mixed state ρ and a k-qubit pure state $|\psi\rangle\langle\psi|$, respectively (as well as $U^{\dagger}$, $V^{\dagger}$, and their controlled versions); the desired additive error $\varepsilon \in (0, 1)$.

Output: An estimate of $\mathrm{F}(|\psi\rangle, \rho)$ to within additive error ε with probability at least $2/3$.

1: Let unitary operator

$$
\begin{aligned}
W' = (I_{\mathsf{C}} \otimes |0\rangle\langle 0|_{\mathsf{A}} \otimes |0\rangle\langle 0|_{\mathsf{B}} \otimes I_{\mathsf{A}'\mathsf{B}'} + X_{\mathsf{C}} \otimes (I_{\mathsf{AB}} - |0\rangle\langle 0|_{\mathsf{A}} \otimes |0\rangle\langle 0|_{\mathsf{B}}) \otimes I_{\mathsf{A}'\mathsf{B}'}) \\
\cdot (V_{\mathsf{AB}}^{\dagger} \otimes I_{\mathsf{A}'\mathsf{B}'}) \cdot \mathsf{SWAP}_{\mathsf{BB}'} \cdot (U_{\mathsf{AB}} \otimes V_{\mathsf{A}'\mathsf{B}'}).
\end{aligned}
$$

2: **return** $\mathsf{SqrtAmpEst}(W', \varepsilon)$ by Theorem 4.

▶ **Theorem 6** (Estimating fidelity to a pure state)**.** *Suppose that U and V are quantum unitary operators that prepare n-qubit purifications of a k-qubit mixed state $\rho = \operatorname{tr}_{\mathsf{B}}(|\rho\rangle\langle\rho|_{\mathsf{AB}})$ and a k-qubit pure state $|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|_{\mathsf{A}'}$, respectively, as in Equations (4) and (5). For $\varepsilon \in (0, 1)$, there is a quantum query algorithm that estimates $\mathrm{F}(\rho, |\psi\rangle)$ to within additive error ε with probability at least $2/3$ using $O(1/\varepsilon)$ queries to (controlled-)U, (controlled-)V, and their inverses.*

Proof. The formal algorithm is given in Algorithm 1. To make the proof rigorous, we introduce an auxiliary system C that consists of one qubit. Let

$$
W' = \big((I_{\mathsf{C}} \otimes |0\rangle\langle 0|_{\mathsf{A}} \otimes |0\rangle\langle 0|_{\mathsf{B}} + X_{\mathsf{C}} \otimes (I_{\mathsf{AB}} - |0\rangle\langle 0|_{\mathsf{A}} \otimes |0\rangle\langle 0|_{\mathsf{B}})) \otimes I_{\mathsf{A}'\mathsf{B}'}\big)W, \tag{9}
$$

where W is defined by Equation (6). According to Equation (8), we have

$$W'|0\rangle_{\mathsf{C}}|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|0\rangle_{\mathsf{A}'}|0\rangle_{\mathsf{B}'} = \mathrm{F}(|\psi\rangle,\rho)|0\rangle_{\mathsf{C}}|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|\phi\rangle_{\mathsf{A}'\mathsf{B}'} + \sqrt{1-\mathrm{F}(|\psi\rangle,\rho)^2}|1\rangle_{\mathsf{C}}|\phi^{\perp}\rangle_{\mathsf{ABA}'\mathsf{B}'}.$$

Finally, we can obtain an estimate $\tilde{x} = \mathsf{SqrtAmpEst}(W',\varepsilon)$ of $\mathrm{F}(|\psi\rangle,\rho)$ to within additive error ε (i.e., $|\tilde{x} - \mathrm{F}(|\psi\rangle,\rho)| < \varepsilon$) with probability at least $2/3$ using $O(1/\varepsilon)$ queries to W'. According to Equations (6) and (9), one query to W' consists of one query to U and two queries to V. Therefore, the way we obtain $\tilde{x}$ uses $O(1/\varepsilon)$ queries to both U and V. ◀

4.2 Generalization to Two Mixed States

In this subsection, we naturally extend the unitary operator in Figure 3 to the scenario where V prepares a purification of an arbitrary mixed state σ. That is, we replace Equation (5) with

$$V_{\mathsf{A}'\mathsf{B}'}|0\rangle_{\mathsf{A}'}|0\rangle_{\mathsf{B}'} = |\sigma\rangle_{\mathsf{A}'\mathsf{B}'}, \tag{10}$$

where $\sigma_{\mathsf{A}'} = \mathrm{tr}_{\mathsf{B}'}(|\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})$. In this case, it turns out that $\sqrt{\mathrm{tr}(\rho\sigma^2)}$ is encoded in the amplitude. Note that when σ is pure, $\sigma^2 = \sigma$, the quantity $\sqrt{\mathrm{tr}(\rho\sigma^2)}$ equals the fidelity $\mathrm{F}(\rho,\sigma)$. Specifically, the circuit in Figure 3 outputs two bits $x_{\mathsf{A}}, x_{\mathsf{B}} \in \{0,1\}$ such that

$$\Pr[x_{\mathsf{A}} = x_{\mathsf{B}} = 0] = \mathrm{tr}(\rho\sigma^2), \tag{11}$$

which generalizes Equation (7). This can be verified by the following proposition.

▶ **Proposition 7.** *$\|(\langle 0|_{\mathsf{A}}\langle 0|_{\mathsf{B}} \otimes I_{\mathsf{A}'\mathsf{B}'})W|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|0\rangle_{\mathsf{A}'}|0\rangle_{\mathsf{B}'}\|^2 = \mathrm{tr}(\rho\sigma^2)$, where W is defined by Equation (6), U_{AB} is defined by Equation (4), and $V_{\mathsf{A}'\mathsf{B}'}$ is defined by Equation (10).*

Proof. This can be shown by direct calculations generalizing the proof of Proposition 5.

$$\begin{aligned}
&\|(\langle 0|_{\mathsf{A}}\langle 0|_{\mathsf{B}} \otimes I_{\mathsf{A}'\mathsf{B}'})W|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}|0\rangle_{\mathsf{A}'}|0\rangle_{\mathsf{B}'}\|^2 \\
&= \|(\langle\sigma|_{\mathsf{AB}} \otimes I_{\mathsf{A}'\mathsf{B}'}) \cdot \mathsf{SWAP}_{\mathsf{BB}'} \cdot |\rho\rangle_{\mathsf{AB}}|\sigma\rangle_{\mathsf{A}'\mathsf{B}'}\|^2 \\
&= \langle\rho|_{\mathsf{AB}}\langle\sigma|_{\mathsf{A}'\mathsf{B}'} \cdot \mathsf{SWAP}_{\mathsf{BB}'} \cdot (|\sigma\rangle\langle\sigma|_{\mathsf{AB}} \otimes I_{\mathsf{A}'\mathsf{B}'}) \cdot \mathsf{SWAP}_{\mathsf{BB}'} \cdot |\rho\rangle_{\mathsf{AB}}|\sigma\rangle_{\mathsf{A}'\mathsf{B}'} \\
&= \mathrm{tr}\big(\mathsf{SWAP}_{\mathsf{BB}'}(|\sigma\rangle\langle\sigma|_{\mathsf{AB}} \otimes I_{\mathsf{A}'\mathsf{B}'})\mathsf{SWAP}_{\mathsf{BB}'} \cdot (|\rho\rangle\langle\rho|_{\mathsf{AB}} \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\big) \\
&= \mathrm{tr}\big(\mathsf{SWAP}_{\mathsf{AA}'}(I_{\mathsf{AB}} \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\mathsf{SWAP}_{\mathsf{AA}'} \cdot (|\rho\rangle\langle\rho|_{\mathsf{AB}} \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\big) \\
&= \mathrm{tr}\Big(\mathrm{tr}_{\mathsf{B}}\big(\mathsf{SWAP}_{\mathsf{AA}'}(I_{\mathsf{AB}} \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\mathsf{SWAP}_{\mathsf{AA}'} \cdot (|\rho\rangle\langle\rho|_{\mathsf{AB}} \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\big)\Big) \\
&= \mathrm{tr}\big(\mathsf{SWAP}_{\mathsf{AA}'}(I_{\mathsf{A}} \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\mathsf{SWAP}_{\mathsf{AA}'} \cdot (\mathrm{tr}_{\mathsf{B}}(|\rho\rangle\langle\rho|_{\mathsf{AB}}) \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\big) \\
&= \mathrm{tr}\big(\mathsf{SWAP}_{\mathsf{AA}'}(I_{\mathsf{A}} \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\mathsf{SWAP}_{\mathsf{AA}'} \cdot (\rho_{\mathsf{A}} \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\big) \\
&= \mathrm{tr}\big((I_{\mathsf{A}} \otimes \langle\sigma|_{\mathsf{A}'\mathsf{B}'}) \cdot \mathsf{SWAP}_{\mathsf{AA}'}(I_{\mathsf{A}} \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\mathsf{SWAP}_{\mathsf{AA}'} \cdot (\rho_{\mathsf{A}} \otimes |\sigma\rangle_{\mathsf{A}'\mathsf{B}'})\big) \\
&= \mathrm{tr}\Big(\big((I_{\mathsf{A}} \otimes \langle\sigma|_{\mathsf{A}'\mathsf{B}'})\mathsf{SWAP}_{\mathsf{AA}'}(I_{\mathsf{A}} \otimes |\sigma\rangle_{\mathsf{A}'\mathsf{B}'})\big)^2 \cdot \rho_{\mathsf{A}}\Big).
\end{aligned}$$

The proof is completed by showing that $(I_{\mathsf{A}} \otimes \langle\sigma|_{\mathsf{A}'\mathsf{B}'})\mathsf{SWAP}_{\mathsf{AA}'}(I_{\mathsf{A}} \otimes |\sigma\rangle_{\mathsf{A}'\mathsf{B}'}) = \sigma_{\mathsf{A}}$. To see this, note that

$$
\begin{aligned}
&(I_{\mathsf{A}} \otimes \langle\sigma|_{\mathsf{A}'\mathsf{B}'})\mathsf{SWAP}_{\mathsf{A}\mathsf{A}'}(I_{\mathsf{A}} \otimes |\sigma\rangle_{\mathsf{A}'\mathsf{B}'}) \\
=\ & \mathrm{tr}_{\mathsf{A}'\mathsf{B}'}\big(\mathsf{SWAP}_{\mathsf{A}\mathsf{A}'} \cdot (I_{\mathsf{A}} \otimes |\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\big) \\
=\ & \mathrm{tr}_{\mathsf{A}'}\Big(\mathsf{SWAP}_{\mathsf{A}\mathsf{A}'} \cdot \big(I_{\mathsf{A}} \otimes \mathrm{tr}_{\mathsf{B}'}(|\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})\big)\Big) \\
=\ & \mathrm{tr}_{\mathsf{A}'}\big(\mathsf{SWAP}_{\mathsf{A}\mathsf{A}'} \cdot (I_{\mathsf{A}} \otimes \sigma_{\mathsf{A}'})\big) \\
=\ & \mathrm{tr}_{\mathsf{A}'}\big((\sigma_{\mathsf{A}} \otimes I_{\mathsf{A}'}) \cdot \mathsf{SWAP}_{\mathsf{A}\mathsf{A}'}\big) \\
=\ & \sigma_{\mathsf{A}} \cdot \mathrm{tr}_{\mathsf{A}'}(\mathsf{SWAP}_{\mathsf{A}\mathsf{A}'}) \\
=\ & \sigma_{\mathsf{A}} \cdot I_{\mathsf{A}} \\
=\ & \sigma_{\mathsf{A}}. \qquad \blacktriangleleft
\end{aligned}
$$

Therefore, with a similar analysis, we can estimate the quantity $\sqrt{\mathrm{tr}(\rho\sigma^2)}$ by Proposition 7 with the same complexity as Theorem 6, stated as follows.

▶ **Theorem 8.** *Suppose that U and V are quantum unitary operators that prepare n-qubit purifications of a k-qubit mixed states $\rho = \mathrm{tr}_{\mathsf{B}}(|\rho\rangle\langle\rho|_{\mathsf{A}\mathsf{B}})$ and $\sigma = \mathrm{tr}_{\mathsf{B}'}(|\sigma\rangle\langle\sigma|_{\mathsf{A}'\mathsf{B}'})$, respectively, as in Equations (4) and (10). For $\varepsilon \in (0,1)$, there is a quantum query algorithm that estimates $\sqrt{\mathrm{tr}(\rho\sigma^2)}$ to within additive error ε with probability at least $2/3$ using $O(1/\varepsilon)$ queries to (controlled-)U, (controlled-)V, and their inverses.*

To provide an intuitive understanding of our encoding scheme, we restructure the circuit in Figure 3 into the form shown in Figure 4. This revised visualization explicitly reveals the

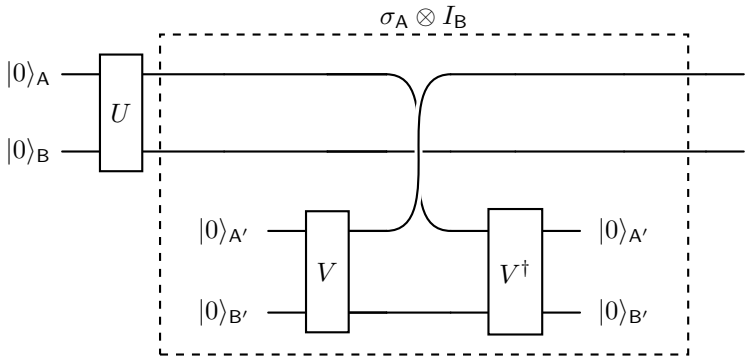

Figure 4 Restructured circuit of Figure 3, illustrating the operator $\sigma_{\mathsf{A}} \otimes I_{\mathsf{B}}$ and its action on the purification $|\rho\rangle_{\mathsf{A}\mathsf{B}}$.

construction of an operator $\sigma_{\mathsf{A}} \otimes I_{\mathsf{B}}$ acting on the purification $|\rho\rangle_{\mathsf{A}\mathsf{B}}$ of ρ_{A}. Since

$$\|(\sigma_{\mathsf{A}} \otimes I_{\mathsf{B}})|\rho\rangle_{\mathsf{A}\mathsf{B}}\|^2 = \mathrm{tr}\big(\rho\sigma^2\big),$$

we clearly see that $\sqrt{\mathrm{tr}(\rho\sigma^2)}$ is encoded into the amplitude of an efficiently preparable quantum state. While the encoding pattern for σ in Figure 4 had previously appeared in [17], people mainly focused on operator properties without explicitly deriving the amplitude structure of the resulting pure state.

5 An Implication: Generalized Pure-State Fidelity Estimation

Our quantum algorithm provided in Theorem 1 suggests a new approach to estimating the fidelity between pure states, where the pure states are given through purified quantum query access, or equivalently prepared by (purified) quantum channels. The purified quantum query

access to a (mixed) quantum state can be understood as a purified version of the quantum channel that prepares the quantum state (cf. [9]). Formally, a quantum channel $\mathcal{E}$ is said to prepare a quantum state ρ, if $\rho = \mathcal{E}(|0\rangle\langle 0|)$. A purified version of $\mathcal{E}$ is a unitary operator U acting on two subsystems A and B such that $\mathcal{E}(\sigma) = \mathrm{tr}_{\mathsf{B}}(U(\sigma_{\mathsf{A}} \otimes |0\rangle\langle 0|_{\mathsf{B}})U^{\dagger})$ for every mixed quantum state σ. Then, ρ can be prepared by the unitary operator U in the way that its purification is prepared by $|\rho\rangle_{\mathsf{AB}} = U|0\rangle_{\mathsf{A}}|0\rangle_{\mathsf{B}}$ and ρ is obtained by tracing out the subsystem B, i.e., $\rho = \mathrm{tr}_{\mathsf{B}}(|\rho\rangle\langle\rho|_{\mathsf{AB}})$. In the following, we state the special case of Theorem 1 for pure-state fidelity estimation.

▶ **Corollary 9** (Pure-state fidelity estimation). *Given purified quantum query access to two pure states $|\varphi\rangle$ and $|\psi\rangle$, the fidelity $\mathrm{F}(|\varphi\rangle, |\psi\rangle) = |\langle\varphi|\psi\rangle|$ can be estimated to within additive error ε with query complexity $O(1/\varepsilon)$.*

Corollary 9 generalizes the pure-state fidelity estimation in [25, Theorem IV.2] to a more general input model. By comparison, the prior approach for pure-state fidelity estimation [25] requires that the pure states should be prepared by a unitary quantum channel. Specifically, Ref. [25] assumes two unitary oracles U_{φ} and U_{ψ} such that $U_{\varphi}|0\rangle = |\varphi\rangle$ and $U_{\psi}|0\rangle = |\psi\rangle$ (see Section 3.2 for details). The input model employed in [25] is more restricted than the purified quantum query access model. For example, $U_{\varphi} \otimes I$ always provides purified quantum query access to $|\varphi\rangle$, where I is the identity operator; however, it is unlikely that U_{φ} could be implemented by purified quantum query access to $|\varphi\rangle$.

In addition to adopting a more general input model than [25], Corollary 9 attains the same optimal query complexity of $O(1/\varepsilon)$, where the lower bound (noted in [25]) is implied in [2, 19] (see Theorem 10).

6 Lower Bounds

For completeness, we discuss the lower bounds for estimating the fidelity. In fact, a lower bound of $\Omega(1/\varepsilon)$ is implied in [2, 19] when both quantum states are pure (as noted in [25]).

▶ **Theorem 10** (Adapted from [2, 19]). *Given purified quantum query access to quantum states ρ and $|\psi\rangle$, any quantum query algorithm that estimates $\mathrm{F}(\rho, |\psi\rangle)$ to within additive error ε requires query complexity $\Omega(1/\varepsilon)$, even if ρ is pure.*

We strengthen this lower bound so that it applies to the case where ρ is a mixed quantum state of an arbitrary rank.

▶ **Theorem 11.** *Given purified quantum query access to quantum states ρ and $|\psi\rangle$, any quantum query algorithm that estimates $\mathrm{F}(\rho, |\psi\rangle)$ to within additive error ε requires query complexity $\Omega(1/\varepsilon)$, even if ρ is of an arbitrary rank.*

To prove Theorem 11, we need the following tool.

▶ **Theorem 12** ([3, Theorem 4]). *Let p and q be probability distributions over n elements. Then, any quantum algorithm that determines whether an unknown unitary oracle U is*

$$U_p = \sum_{j=1}^{n} \sqrt{p_j}|j\rangle \text{ or } U_q = \sum_{j=1}^{n} \sqrt{q_j}|j\rangle$$

requires $\Omega(1/d_{\mathrm{H}}(p,q))$ queries to U, where

$$d_{\mathrm{H}}(p,q) = \sqrt{\frac{1}{2}\sum_{j=1}^{n}\left(\sqrt{p_j} - \sqrt{q_j}\right)^2}$$

is the Hellinger distance.

Now we are ready to prove the lower bounds.

Proof of Theorem 11. Let $r = \mathrm{rank}(\rho) \geq 2$ be an arbitrary rank parameter. Now we reduce the distinguishing problem in Theorem 12 to the estimation of $\mathrm{F}(\rho, |\psi\rangle)$. Consider the two probability distributions $p^{\pm}$ such that

$$p_1^{\pm} = p \pm \varepsilon,\ p_j^{\pm} = \frac{1 - p \mp \varepsilon}{r - 1} \text{ for } 2 \leq j \leq r, \text{ and } p_j^{\pm} = 0 \text{ for } r < j \leq n,$$

where $p \in (0, 1)$ is an arbitrary constant. It can be verified that

$$d_{\mathrm{H}}(p^+, p^-) = \sqrt{1 - \sqrt{p^2 - \varepsilon^2} - \sqrt{(1-p)^2 - \varepsilon^2}} \leq O(\varepsilon).$$

To distinguish whether an unknown unitary oracle U is U_{p^+} or U_{p^-}, we can prepare a mixed state ρ that is either of the following two mixed states

$$\rho_{\pm} = (p \pm \varepsilon)|0\rangle\langle 0| + \sum_{j=2}^{r} \frac{1 - p \mp \varepsilon}{r - 1} |j\rangle\langle j|,$$

using one query to U. By taking $|\psi\rangle = |0\rangle$, we can distinguish which the case is by noting that the fidelity $\mathrm{F}(\rho_{\pm}, |0\rangle) = \sqrt{p \pm \varepsilon} = \sqrt{p} \pm \Theta(\varepsilon)$. Therefore, any quantum algorithm for estimating $\mathrm{F}(\rho, |\psi\rangle)$ to within additive error $\Theta(\varepsilon)$ requires query complexity $\Omega(1/d_{\mathrm{H}}(p^+, p^-)) = \Omega(1/\varepsilon)$, even if ρ is of rank r. ◀

7 Discussion

In this paper, we present an optimal quantum algorithm for estimating the fidelity of a mixed state to a pure state, given purified quantum query access. Our approach is simple, which moreover estimates the quantity $\sqrt{\mathrm{tr}(\rho\sigma^2)}$ that has not been commonly considered in the literature. Here, we raise some questions for future research.

1. Can we encode $\sqrt{\mathrm{tr}(\rho\sigma)}$ rather than $\sqrt{\mathrm{tr}(\rho\sigma^2)}$ in the amplitudes? In addition to its relationship with fidelity estimation, this may also estimate the *Frobenius norm* of a quantum state, $\|\rho\|_F = \sqrt{\mathrm{tr}(\rho^2)}$, which is also the square root of purity.
2. Can we estimate the fidelity $\mathrm{F}(\rho, |\psi\rangle)$ with *optimal* sample complexity, generalizing the result of [28]?

References

1 Anurag Anshu, Zeph Landau, and Yunchao Liu. Distributed quantum inner product estimation. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 44–51, 2022. doi:10.1145/3519935.3519974.

2 Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001. doi:10.1145/502090.502097.

3 Aleksandrs Belovs. Quantum algorithms for classical probability distributions. In *Proceedings of the 27th Annual European Symposium on Algorithms*, pages 16:1–16:11, 2019. doi:10.4230/LIPIcs.ESA.2019.16.

4 Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. In Samuel J. Lomonaco, Jr. and Howard E. Brandt, editors, *Quantum Computation and Information*, volume 305 of *Contemporary Mathematics*, pages 53–74. AMS, 2002. doi:10.1090/conm/305/05215.

5 Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001. doi:10.1103/PhysRevLett.87.167902.

6 Wang Fang and Qisheng Wang. Optimal quantum algorithm for estimating fidelity to a pure state. ArXiv e-prints, 2025. doi:10.48550/arXiv.2506.23650.

7 Steven T. Flammia and Yi-Kai Liu. Direct fidelity estimation from few Pauli measurements. *Physical Review Letters*, 106(23):230501, 2011. doi:10.1103/PhysRevLett.106.230501.

8 András Gilyén and Tongyang Li. Distributional property testing in a quantum world. In *Proceedings of the 11th Innovations in Theoretical Computer Science Conference*, pages 25:1–25:19, 2020. doi:10.4230/LIPIcs.ITCS.2020.25.

9 András Gilyén, Seth Lloyd, Iman Marvian, Yihui Quek, and Mark M. Wilde. Quantum algorithm for Petz recovery channels and pretty good measurements. *Physical Review Letters*, 128(22):220502, 2022. doi:10.1103/PhysRevLett.128.220502.

10 András Gilyén and Alexander Poremba. Improved quantum algorithms for fidelity estimation. ArXiv e-prints, 2022. arXiv:2203.15993.

11 Tom Gur, Min-Hsiu Hsieh, and Sathyawageeswar Subramanian. Sublinear quantum algorithms for estimating von Neumann entropy. ArXiv e-prints, 2021. arXiv:2111.11139.

12 Masahito Hayashi. *Quantum Information Theory: Mathematical Foundation*. Springer, 2017. doi:10.1007/978-3-662-49725-8.

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

14 Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: are multiple Merlins more helpful to Arthur? *Chicago Journal of Theoretical Computer Science*, 2009:3, 2009. doi:10.4086/cjtcs.2009.003.

15 Nana Liu, Qisheng Wang, Mark M. Wilde, and Zhicheng Zhang. Quantum algorithm for matrix geometric means. *npj Quantum Information*, 11:101, 2025. doi:10.1038/s41534-025-00973-7.

16 Yupan Liu and Qisheng Wang. On estimating the trace of quantum state powers. In *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 947–993, 2025. doi:10.1137/1.9781611978322.28.

17 Guang Hao Low and Isaac L. Chuang. Hamiltonian Simulation by Qubitization. *Quantum*, 3:163, 2019. doi:10.22331/q-2019-07-12-163.

18 Ashley Montanaro and Ronald de Wolf. A survey of quantum property testing. In *Theory of Computing Library*, number 7 in Graduate Surveys, pages 1–81. University of Chicago, 2016. doi:10.4086/toc.gs.2016.007.

19 Ashwin Nayak and Felix Wu. The quantum query complexity of approximating the median and related statistics. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, pages 384–393, 1999. doi:10.1145/301250.301349.

20 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

21 Harumichi Nishimura. A survey: SWAP test and its applications to quantum complexity theory. In Shin-ichi Minato, Takeaki Uno, Norihito Yasuda, Takashi Horiyama, Ken-ichi Kawarabayashi, Shigeru Yamashita, and Hirotaka Ono, editors, *Algorithmic Foundations for Social Advancement: Recent Progress on Theory and Practice*, pages 243–261. Springer, 2025. doi:10.1007/978-981-96-0668-9_16.

22 Soorya Rethinasamy, Rochisha Agarwal, Kunal Sharma, and Mark M. Wilde. Estimating distinguishability measures on quantum computers. *Physical Review A*, 108(1):012409, 2023. doi:10.1103/PhysRevA.108.012409.

23 Sathyawageeswar Subramanian and Min-Hsiu Hsieh. Quantum algorithm for estimating α-renyi entropies of quantum states. *Physical Review A*, 104(2):022428, 2021. doi:10.1103/PhysRevA.104.022428.

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

25 Qisheng Wang. Optimal trace distance and fidelity estimations for pure quantum states. *IEEE Transactions on Information Theory*, 70(12):8791–8805, 2024. doi:10.1109/TIT.2024.3447915.

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

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

28 Qisheng Wang and Zhicheng Zhang. Sample-optimal quantum estimators for pure-state trace distance and fidelity via samplizer. ArXiv e-prints, 2024. doi:10.48550/arXiv.2410.21201.

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

30 Xinzhao Wang, Shengyu Zhang, and Tongyang Li. A quantum algorithm framework for discrete probability distributions with applications to Rényi entropy estimation. *IEEE Transactions on Information Theory*, 70(5):3399–3426, 2024. doi:10.1109/TIT.2024.3382037.

31 John Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 459–468, 2002. doi:10.1109/SFCS.2002.1181970.

32 John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009. doi:10.1137/060670997.

33 John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. doi:10.1017/9781316848142.

34 Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013. doi:10.1017/9781316809976.