PAPER Special Section on Foundations of Computer Science — Algorithm, Theory of Computation, and their Applications —

Quantum Query Complexity of Unitary Operator Discrimination

Akinori KAWACHI[†a)], ***Member***, **Kenichi KAWANO**[††], ***Nonmember***, **François LE GALL**[†††], ***Member***, ***and*** **Suguru TAMAKI**[†††], ***Nonmember***

SUMMARY Unitary operator discrimination is a fundamental problem in quantum information theory. The basic version of this problem can be described as follows: Given a black box implementing a unitary operator $U \in S := \{U_1, U_2\}$ under some probability distribution over S, the goal is to decide whether $U = U_1$ or $U = U_2$. In this paper, we consider the query complexity of this problem. We show that there exists a quantum algorithm that solves this problem with bounded error probability using $\left\lceil \sqrt{6}\theta_{\mathrm{cover}}^{-1} \right\rceil$ queries to the black box in the worst case, i.e., under any probability distribution over S, where the parameter θ_{cover}, which is determined by the eigenvalues of $U_1^\dagger U_2$, represents the "closeness" between U_1 and U_2. We also show that this upper bound is essentially tight: we prove that for every $\theta_{\mathrm{cover}} > 0$ there exist operators U_1 and U_2 such that any quantum algorithm solving this problem with bounded error probability requires at least $\left\lceil \frac{2}{3\theta_{\mathrm{cover}}} \right\rceil$ queries under uniform distribution over S.

key words: *quantum algorithms, quantum information theory, query complexity*

1. Introduction

(1) Background

Quantum state discrimination is one of the most fundamental problems in quantum information theory [1]–[4]. In a typical setting, the goal of this problem is to discriminate two quantum states. The success probability of this problem is known to be characterized by the orthogonality of the two states. In particular, non-orthogonal states cannot be discriminated with probability 1, no matter how many independent copies of the input state are given.

A problem closely related to quantum state discrimination is the quantum operator discrimination problem [5]–[15]. Similarly to quantum state discrimination, in a typical setting the goal of quantum operator discrimination is to discriminate two operators: given a black box implementing a quantum operator $O \in \{O_1, O_2\}$ under some distribution over $\{O_1, O_2\}$, the goal is to decide whether $O = O_1$ or $O = O_2$. A specificity of the quantum operator discrimination problem, which is not present in the quantum state discrimination problem, is that we can choose an arbitrary input state on which the operator O is applied. Additionally, the operator O can be applied more than once in various combinations (parallel, sequential, or in any other scheme physically allowed). In contrast to quantum state discrimination, it is known that for several classes of operators discrimination is possible without error [5], [7]–[10], [13]. For example, any two unitary operators can be discriminated without error by applying the operator in parallel on some well-chosen entangled quantum state [5], [8], or by applying the operator sequentially on a non-entangled state [9]. In addition to unitary operators, it is also known that projective measurements can be discriminated without error [13]. Necessary and sufficient conditions for discriminating trace preserving completely positive (TPCP) maps without errors are given in [10] as well.

Many computational problems solved by quantum algorithms can be recasted as discrimination problems. Here the quantum operator given as input typically implements a classical operation on the basis of the corresponding Hilbert space and the goal is to (possibly partially) identify which classical operation it implements. Such problems generalize Grover's original quantum search problem [16] and have been studied under the name of the oracle identification problem [17], [18]. For instance, Grover's algorithm for search solves the following problem: given an oracle U_x corresponding to an unknown string $x \in \{0,1\}^n$ that maps any quantum basis state $|i\rangle|b\rangle$, with $i \in \{1, \ldots, n\}$ and $b \in \{0,1\}$, to the quantum state $|i\rangle|b \oplus x_i\rangle$, determine if x contains at least one non-zero coordinate. These problems have been mainly considered in the query complexity setting, where the complexity is defined as the number of calls of the operator U_x used by the algorithm. Upper and lower bounds on the query complexity of several oracle identification problems have been obtained [17], [18].

Quantum operator discrimination problems relevant to quantum information theory, on the other hand, have not yet been the subject of much study in the framework of quantum query complexity.

(2) Our results

In this paper, we investigate the query complexity of the quantum operator discrimination problem for general quantum unitary operators (i.e., quantum unitary operators not necessarily corresponding to classical operations) in bounded-error settings. More precisely, we consider the following problem: given an unknown unitary operator

Manuscript received March 30, 2018.
Manuscript revised July 27, 2018.
Manuscript publicized November 8, 2018.

[†]The author is with Osaka University, Suita-shi, 565–0871 Japan.
[††]The author is with Tokushima University, Tokushima-shi, 770–8506 Japan.
[†††]The authors are with Kyoto University, Kyoto-shi, 606–8501 Japan.
a) E-mail: kawachi@comm.eng.osaka-u.ac.jp

DOI: 10.1587/transinf.2018FCP0012

$U \in S := \{U_1, U_2\}$ under some probability distribution over a candidate set S, where U is given as a (quantum) black-box and both U_1 and U_2 are known unitary operators, determine whether $U = U_1$ or $U = U_2$ correctly with bounded error probability.

Our main contribution is a characterization of the query complexity of this problem (i.e., the number of times the black-box U has to be applied to solve the problem) in terms of a parameter θ_{cover}, which is defined formally later (Definition 12 in Sect. 3), representing the "closeness" between U_1 and U_2. By showing a tradeoff between the number of queries and success probability, we show the following upper and lower bounds:

- There exists a quantum algorithm that makes $\lceil \sqrt{6}\theta_{\text{cover}}^{-1} \rceil$ non-adaptive queries and can correctly discriminate U_1 from U_2 in the worst case (i.e., under any probability distribution over a candidate set S), for any unitary operators U_1 and U_2, with probability 2/3 (Theorem 14).
- For every distinct unitary operators U_1 and U_2, every quantum algorithm requires at least $\lceil \frac{2}{3\theta_{\text{cover}}} \rceil$ queries to discriminate U_1 from U_2 with probability 2/3 (Theorem 17) under uniform distribution over S.

We thus obtain a tight (up to possible constant factors) characterization of the query complexity of unitary operator discrimination. Our upper bound is actually achieved by a quantum algorithm that makes only non-adaptive queries, i.e., a quantum algorithm in which all queries to the black-box can be made in parallel. On the other hand, our lower bound holds even for adaptive quantum algorithms. Our results thus show that for the quantum unitary operator discrimination problem making adaptive query cannot (significantly) reduce the query complexity of the algorithm. A similar consequence was derived in [19] for unitary discrimination of some continuous candidates. This contrasts with oracle identification problems [20] such as quantum search, where adaptive queries are necessary for achieving the speed-up exhibited by Grover's algorithm [16], and with quantum channel discrimination, where adaptivity is essentially required to discriminate some quantum channels as shown by [21].

(3) Relation with other works

Note that Acín actually showed upper bounds on the query complexity of the problem by using an entangled input state with non-adaptive queries [5]. Acín provided a geometric interpretation for the statistical distinguishability of unitary operators based on sophisticated metrics of Fubini-Study and Bures. D'Ariano et al. briefly noted a simpler geometric interpretation based on the Euclidean metric on the complex plane for the same result [8]. Duan et al. also showed the same upper bounds with adaptive queries and a non-entangled input state using the parameter θ_{cover} [9]. Our algorithm for the upper bounds uses an entangled input state with non-adaptive queries similarly to Acín's and D'Ariano et al.'s. In addition, we prove a tradeoff between the number of queries and success probability with rigorous analysis. Duan et al. also showed the optimality of their lower bounds to perfectly discriminate two unitary operators [9]. Our proof of the lower bound additionally analyzes the necessary number of queries for imperfect discrimination in details by showing a tradeoff between the number of queries and success probability.

Harrow et al. showed the existence of a quantum state discriminator $\mathcal{M}^*$ which solves the quantum state discrimination problem in the worst case, i.e., independently of a probability distribution over a set of candidate quantum states [22]. Using $\mathcal{M}^*$, we construct the unitary operator discriminator $\mathcal{A}^*$. As with $\mathcal{M}^*$, $\mathcal{A}^*$ solves the unitary operator discrimination problem independently of a probability distribution over a set of candidate unitary operators, which provides the worst-case upper bound of query complexity for unitary operator discrimination problem.

In a more general setting, Aharonov et al. introduced the diamond norm, which can be utilized for quantum channel discrimination [23]. In addition, they pointed out a characterization of success probability for unitary discrimination from eigenvalues of candidate unitary operators, which is similar to the parameter θ_{cover}.

(4) Organization of the paper

The organization of this paper is as follows. In Sect. 2, we define formally the quantum state discrimination problem, the unitary operator discrimination problem, the error probability of a discriminator, and the query complexity. In Sect. 3, we show average-case upper bounds on the query complexity when arbitrary candidate operators U_1 and U_2 are given with probability 1/2 respectively by constructing a discriminator for U_1 and U_2 and analyzing the error probability. In Sect. 4, we show the worst-case upper bounds on the query complexity by combining the discriminator in Sect. 3 with Harrow et al.'s result [22]. In Sect. 5, we show the lower bound on the query complexity of any quantum algorithm solving the quantum unitary operator discrimination problem. Finally, we provide an improved analysis for lower bounds of the query complexity, which is attributed to Mori [27], in Sect. 6.

2. Preliminaries

First, we define the quantum state discrimination problem since the unitary operator discrimination problem can be reduced to the quantum state discrimination problem.

Definition 1 (Quantum state discrimination problem): The *quantum state discrimination problem* is defined as the problem of determining whether an unknown state $|\phi\rangle$ is $|\phi_1\rangle$ or $|\phi_2\rangle$, where $|\phi\rangle$ is given from a candidate set $S = \{|\phi_1\rangle, |\phi_2\rangle\}$ of arbitrary two quantum states. Below, we denote the quantum state discrimination problem of $S = \{|\phi_1\rangle, |\phi_2\rangle\}$ by $\text{QSDP}(\{|\phi_1\rangle, |\phi_2\rangle\})$.

Definition 2 (Error probability of $\text{QSDP}(\{|\phi_1\rangle, |\phi_2\rangle\})$): For a quantum state discriminator $\mathcal{A}$, when $|\phi_1\rangle$ and $|\phi_2\rangle$ are given with probability p_1 and $p_2 := 1 - p_1$ respectively, the

error probability P_{error} of $\mathcal{A}$ is defined as follows:

$$P_{\text{error}} = p_1 \Pr_{\mathcal{A}}[\mathcal{A}(|\phi_1\rangle) = \text{“2”}] + p_2 \Pr_{\mathcal{A}}[\mathcal{A}(|\phi_2\rangle) = \text{“1”}].$$

Namely, the error probability P_{error} is the sum of the probability that $\mathcal{A}$ mistakes $|\phi_1\rangle$ for $|\phi_2\rangle$ and $|\phi_2\rangle$ for $|\phi_1\rangle$, where the probability is taken over randomness of $\{|\phi_1\rangle, |\phi_2\rangle\}$ and $\mathcal{A}$.

The error probability is characterized by the closeness between two quantum states such as the trace distance and the fidelity.

Definition 3 (Trace distance): Let ρ and σ be pure quantum states. The *trace distance* $d(\rho, \sigma)$ is defined as $d(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_{\text{tr}}$, where $\|X\|_{\text{tr}} := \text{Tr}(|X|) = \text{Tr}\left(\sqrt{X^\dagger X}\right)$.

Definition 4 (Fidelity): Let $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$ be pure quantum states. The fidelity $F(\rho, \sigma)$ is defined as $F(\rho, \sigma) = |\langle\psi|\phi\rangle|$. Since it is an absolute value of inner product, it holds that $0 \le F(\rho, \sigma) \le 1$, $F(\rho, \sigma) = 1 \Leftrightarrow |\psi\rangle = |\phi\rangle$, and $F(\rho, \sigma) = 0 \Leftrightarrow |\psi\rangle \perp |\phi\rangle$.

Also, the trace distance and the fidelity satisfy the following relation.

Lemma 5 ([24]): Let ρ and σ be pure quantum states. We then have $d(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_{\text{tr}} = \sqrt{1 - F(\rho, \sigma)^2}$.

A result of Barnum and Knill [25] shows that, assuming a probability distribution $\{p_i\}$ on a candidate set $\{\rho_i\}$ of quantum states, the error probability of a quantum state discriminator $\mathcal{A}$ is bounded as

$$P_{\text{error}} \le \sum_{i \ne j} \sqrt{p_i p_j}\, \sqrt{F\left(\rho_i, \rho_j\right)}.$$

In this paper, we consider the case of two quantum states. Additionally, from $p_1 \ge 0$, $p_2 \ge 0$, and $p_1 + p_2 = 1$, $\sqrt{p_1 p_2} \le \frac{1}{2}$ holds. Therefore, we obtain the following theorem of upper bounds of error probability for quantum state discrimination in the worst case.

Theorem 6: Suppose the quantum states ρ and σ are given from the candidate set $S = \{\rho, \sigma\}$ of pure quantum states with any probability p_1 and p_2 respectively. Then there exists a discriminator $\mathcal{A}$ such that its error probability P_{error} is given as follows:

$$P_{\text{error}} \le \sqrt{p_1 p_2}\, \sqrt{F(\rho, \sigma)} \le \frac{1}{2}\sqrt{F(\rho, \sigma)}.$$

On the other hand, if we choose a uniform probability distribution over two candidate states, the error probability is completely characterized by their fidelity as shown in the following theorem, which is used to prove the lower bounds of query complexity.

Theorem 7 ([15]): Suppose quantum states $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$ are given from $S = \{\rho, \sigma\}$ of pure quantum states with probability $1/2$ respectively. Then there exists a discriminator $\mathcal{A}$ such that its error probability P_{error} is given as follows:

$$\begin{aligned} P_{\text{error}} &= \frac{1}{2}\left(1 - \left\|\frac{1}{2}\rho - \frac{1}{2}\sigma\right\|_{\text{tr}}\right) \\ &= \frac{1}{2}\left(1 - d(\rho, \sigma)\right) \\ &= \frac{1}{2}\left(1 - \sqrt{1 - F(\rho, \sigma)^2}\right). \end{aligned}$$

Next, we define the unitary operator discrimination problem.

Definition 8 (Unitary operator discrimination problem): The *unitary operator discrimination problem* is defined as the problem of determining whether an unknown operator U is U_1 or U_2, where U is given from a candidate set $S = \{U_1, U_2\}$ of arbitrary two unitary operators Below, we denote the unitary operator discrimination problem of $S = \{U_1, U_2\}$ by UODP$(\{U_1, U_2\})$.

Definition 9 (Error probability of UODP$(\{U_1, U_2\})$): For a unitary operator discriminator $\mathcal{A}$, when U_1 and U_2 are given with any probability p_1 and p_2 respectively, the error probability P^U_{error} of $\mathcal{A}$ is defined as follows:

$$P^U_{\text{error}} = p_1 \Pr_{\mathcal{A}}\left[\mathcal{A}^{U_1} = \text{“2”}\right] + p_2 \Pr_{\mathcal{A}}\left[\mathcal{A}^{U_2} = \text{“1”}\right].$$

Namely, the error probability P^U_{error} is the sum of the probability that $\mathcal{A}$ mistakes U_1 for U_2 and U_2 for U_1, where the probability is taken over randomness of $\{U_1, U_2\}$ and $\mathcal{A}$.

Except for Sect. 4, we assume that the given probability distribution is uniform in this paper, i.e., U_1 and U_2 are given with probability $1/2$, respectively.

Generally, the unitary operator discrimination problem can be reduced to the quantum state discrimination problem by applying the unknown unitary operator U to an arbitrary $|\phi\rangle$. An application of U to $|\phi\rangle$ is called a *query*. Then, we denote by $\left|\phi^{U,q}\right\rangle$ the quantum state generated by q queries to U and unitary operators $\{X_i\}_{i=1}^q$, which are independent of U (however, possibly depend on $\{U_1, U_2\}$), specified by $\mathcal{A}$. It is given as follows:

$$\left|\phi^{U,q}\right\rangle = X_q (U \otimes \mathbb{I}) X_{q-1} (U \otimes \mathbb{I}) \cdots X_1 (U \otimes \mathbb{I}) |\phi\rangle.$$

Here, $|\phi\rangle$ and $\left|\phi^{U,q}\right\rangle$ are quantum states of $m+n$ qubits, X_i is a unitary operator over $m+n$ qubits for each i, and U and $\mathbb{I}$ are unitary operators over n qubits and m qubits, respectively. Note that this formulation can represent non-adaptive discrimination. Let $\hat{U}$ be a sequence of unitary operators of $\mathcal{A}$. Then we have $\left|\phi^{U,q}\right\rangle = \hat{U}|\phi\rangle$. Also, we define $\hat{U}_1$ and $\hat{U}_2$ as unitary operators satisfying $\left|\phi^{U_1,q}\right\rangle = \hat{U}_1|\phi\rangle$ and $\left|\phi^{U_2,q}\right\rangle = \hat{U}_2|\phi\rangle$, respectively.

The unitary operator discriminator that makes all the queries at once (regardless of the answers to other queries) is called a *non-adaptive* unitary operator discriminator. Otherwise it is called an *adaptive* unitary operator discriminator. When unitary operators U_1 and U_2 are given from

$S = \{U_1, U_2\}$ with probability p_1 and p_2 respectively, the error probability of any discriminator is bounded for every p_1, p_2 as follows:

$$P^U_{\text{error}} \leq \frac{1}{2}\sqrt{\min_{|\phi\rangle} \left|\langle\phi|\hat{U}_1^\dagger \hat{U}_2 |\phi\rangle\right|} = \frac{1}{2}\sqrt{\min_{|\phi'\rangle} |\langle\phi'|U'|\phi'\rangle|}. \quad (1)$$

For $\hat{U}_1$ and $\hat{U}_2$, let $U' = V^\dagger \hat{U}_1^\dagger \hat{U}_2 V$, where U' is a diagonal matrix, and let $|\phi'\rangle = V^\dagger |\phi\rangle$. This inequality is shown immediately from Theorem 6.

Definition 10: We say a discriminator $\mathcal{A}$ makes q queries if $\mathcal{A}$ applies a unitary operator U q times to the initial state $|\phi\rangle$ in total. We say $\mathcal{A}$ solves UODP$(\{U_1, U_2\})$ with q queries if $\mathcal{A}$ correctly discriminates unitary operators U_1 and U_2 with probability at least $2/3$ with q queries when U_1 and U_2 are given with probability $1/2$ repectively. In addition, we say $\mathcal{A}$ solves UODP$(\{U_1, U_2\})$ with q queries *in the worst case* if $\mathcal{A}$ solves UODP$(\{U_1, U_2\})$ with at most q queries under every probability distribution over $\{U_1, U_2\}$. The query complexity of UODP$(\{U_1, U_2\})$ is the minimum number of queries where $\mathcal{A}$ solves UODP$(\{U_1, U_2\})$.

3. Upper Bounds

Let U_1 and U_2 be unitary operators acting on n qubits. In this section, we suppose that either U_1 or U_2 is given with equal probability, i.e., $1/2$, respectively. Below we give a construction of a non-adaptive q-query discriminator for UODP$(\{U_1, U_2\})$. See Fig. 1 for its schematic description.

Construction 11: (Non-adaptive q-query discriminator $\mathcal{A}$ for UODP$(\{U_1, U_2\})$)

1. Generate an initial qn-qubit quantum state $|\phi\rangle$ that is determined by U_1, U_2 and q as in the proof of Lemma 13.
2. Apply $U^{\otimes q}$ to $|\phi\rangle$, where $U \in \{U_1, U_2\}$ is the unknown unitary operator.
3. Apply the quantum state discriminator for QSDP$\left(\left\{U_1^{\otimes q}|\phi\rangle, U_2^{\otimes q}|\phi\rangle\right\}\right)$, from Theorem 6, to the quantum state $U^{\otimes q}|\phi\rangle$.
4. Output the result of the quantum state discriminator.

To analyze the error probability of the non-adaptive q-query discriminator $\mathcal{A}$, let us introduce a notion of the covering angle.

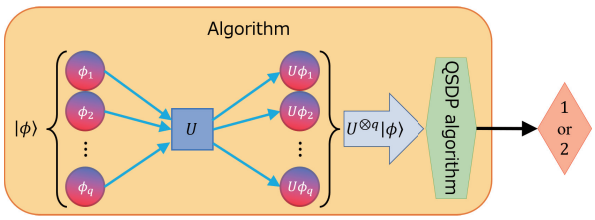

Fig. 1 Non-adaptive unitary operator discriminator $\mathcal{A}$

Definition 12 (Covering angle θ_{cover}): Let $\arg(e^{i\theta}, e^{i\theta'})$ denote the smaller angle between $e^{i\theta}$ and $e^{i\theta'}$ in the complex plane, and let $\text{arc}(e^{i\theta}, e^{i\theta'})$ denote its arc on the complex unit circle. Then, *covering angle* of the set $\left\{e^{i\theta_1}, \ldots, e^{i\theta_n}\right\}$, denoted by θ_{cover}, is defined as $\theta_{\text{cover}} := \min\{\theta : {}^\exists\theta_k, {}^\exists\theta_l \in \{\theta_1, \ldots, \theta_n\}$ s.t. $\theta = \arg(e^{i\theta_k}, e^{i\theta_l}) \wedge \left\{e^{i\theta_1}, \ldots, e^{i\theta_n}\right\} \subseteq \text{arc}(e^{i\theta_k}, e^{i\theta_l})\}$.

The covering angle θ_{cover} is *formed* by $e^{i\theta_k}$ and $e^{i\theta_l}$ if $\theta_{\text{cover}} = \arg(e^{i\theta_k}, e^{i\theta_l})$. As mentioned in Introduction, the covering angle of $U_1^\dagger U_2$ represents the "closeness" between U_1 and U_2. This notion is also used for characterization of perfect unitary discrimination [9] See Fig. 2 for an illustrated example of a covering angle. Aharonov et al. [23] pointed out that the success probability of unitary discrimination is characterized by the distance from the origin to the polygon whose vertices are the eigenvalues of $U_1^\dagger U_2$ in the complex plane. (Its proof was given, e.g., by Johnston et al. [26].) The parameter θ_{cover} is similar to their characterization, but θ_{cover} is more convenient to characterize the query complexity of the unitary discrimination simply.

Let $\left\{e^{i\theta_1}, \ldots, e^{i\theta_n}\right\}$ be the set of eigenvalues of $U_1^\dagger U_2$ and let θ_{cover} be its covering angle. The following is the main technical lemma of this section.

Lemma 13: The error probability P^U_{error} of the non-adaptive q-query discriminator $\mathcal{A}$ is given as follows:

$$P^U_{\text{error}} \begin{cases} \leq \frac{1}{2}\sqrt{\cos\frac{q\theta_{\text{cover}}}{2}} & (0 \leq q\theta_{\text{cover}} < \pi), \\ = 0 & (\pi \leq q\theta_{\text{cover}}). \end{cases}$$

This lemma immediately implies the following:

Theorem 14: The non-adaptive q-query discriminator $\mathcal{A}$ solves UODP$(\{U_1, U_2\})$ if $q \geq \left\lceil\sqrt{6}\theta_{\text{cover}}^{-1}\right\rceil$. Furthermore, the error probability of $\mathcal{A}$ is zero if $q \geq \left\lceil\frac{\pi}{\theta_{\text{cover}}}\right\rceil$.

Proof of Theorem 14. If $q \geq \left\lceil\frac{\pi}{\theta_{\text{cover}}}\right\rceil$, then $\pi \leq q\theta_{\text{cover}}$ holds and the error probability of $\mathcal{A}$ is zero by Lemma 13. For $0 \leq q\theta_{\text{cover}} < \pi$, again by Lemma 13, it suffices to find q such that

$$P^U_{\text{error}} \leq \frac{1}{2}\sqrt{\cos\frac{q\theta_{\text{cover}}}{2}} \leq \frac{1}{2}\sqrt{1 - \frac{1}{2!}\left(\frac{q\theta_{\text{cover}}}{2}\right)^2 + \frac{1}{4!}\left(\frac{q\theta_{\text{cover}}}{2}\right)^4}$$

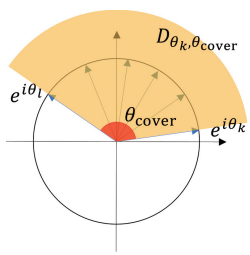

Fig. 2 Covering angle θ_{cover}

$$\leq \frac{1}{2}\sqrt{1-\frac{1}{2}\left(\frac{q\theta_{\mathrm{cover}}}{2}\right)^2\left(1-\frac{\pi^2}{48}\right)} \leq \frac{1}{3}. \quad (2)$$

holds according to Definition 10. From (2), it is easy to see that $P^U_{\mathrm{error}} \leq 1/3$ holds if $q \geq \lceil \sqrt{6}\theta^{-1}_{\mathrm{cover}} \rceil$. □

It remains to prove Lemma 13. It is instructive to first analyze a special case of $q = 1$ as it captures the essence of general cases.

Lemma 15: The error probability of the non-adaptive 1-query discriminator $\mathcal{A}$ is given as follows:

$$P^U_{\mathrm{error}} \begin{cases} \leq \frac{1}{2}\sqrt{\cos\frac{\theta_{\mathrm{cover}}}{2}} & (0 \leq \theta_{\mathrm{cover}} < \pi), \\ = 0 & (\pi \leq \theta_{\mathrm{cover}} \leq 2\pi). \end{cases}$$

Proof of Lemma 15. We consider two cases according to the value of θ_{cover}.

Case (i) $0 \leq \theta_{\mathrm{cover}} < \pi$.

Let $U' = \mathrm{diag}\left(e^{i\theta_1}, \ldots, e^{i\theta_n}\right)$ and $|\phi'\rangle = (\alpha_1, \ldots, \alpha_n)$. By (1) in Sect. 2, the minimum value of the fidelity of $U_1|\phi\rangle$ and $U_2|\phi\rangle$ is represented as follows:

$$\min_{|\phi\rangle} \left|\langle\phi| U_1^\dagger U_2 |\phi\rangle\right| = \min_{|\phi'\rangle} \left|\langle\phi'| U' |\phi'\rangle\right| = \min_{\sum_{j=1}^n |\alpha_j|^2 = 1} \left|\sum_{j=1}^n |\alpha_j|^2 e^{i\theta_j}\right|.$$

The last term above is equal to the square of the shortest distance from the origin of the complex plane to the convex set $C := \left\{\sum_{j=1}^n |\alpha_j|^2 e^{i\theta_j} : \sum_{j=1}^n |\alpha_j|^2 = 1\right\}$. The shortest distance from the origin of the complex plane to C is equal to the shortest distance from the origin of the complex plane to the line segment $C' := \left\{|\alpha_k|^2 e^{i\theta_k} + |\alpha_l|^2 e^{i\theta_l} : |\alpha_k|^2 + |\alpha_l|^2 = 1\right\}$, where $e^{i\theta_k}$ and $e^{i\theta_l}$ form the covering angle θ_{cover}. See Fig. 3 for illustration. Thus, we have

$$\min_{\sum_{j=1}^n |\alpha_j|^2 = 1} \left|\sum_{j=1}^n |\alpha_j|^2 e^{i\theta_j}\right| = \min_{|\alpha_k|^2 + |\alpha_l|^2 = 1} \left||\alpha_k|^2 e^{i\theta_k} + |\alpha_l|^2 e^{i\theta_l}\right|.$$

The minimum of the right hand side above is achieved by setting $|\alpha_k|^2 = \frac{1}{2}$, $|\alpha_l|^2 = \frac{1}{2}$. Hence

$$\min_{|\alpha_k|^2 + |\alpha_l|^2 = 1} \left||\alpha_k|^2 e^{i\theta_k} + |\alpha_l|^2 e^{i\theta_l}\right| = \frac{1}{2}\left|e^{i\theta_k} + e^{i\theta_l}\right| = \cos\frac{\theta_{\mathrm{cover}}}{2}.$$

Thus, P^U_{error} of $\mathcal{A}$ is represented as follows:

$$P^U_{\mathrm{error}} \leq \frac{1}{2}\sqrt{\cos\frac{\theta_{\mathrm{cover}}}{2}} \quad (0 \leq \theta_{\mathrm{cover}} \leq \pi).$$

Case (ii) $\pi \leq \theta_{\mathrm{cover}} \leq 2\pi$.

The error probability can be calculated in the same way as Case (i). In this case, the convex set C contains the origin of the complex plane, i.e., the shortest distance from the origin to C is zero, hence we have $P^U_{\mathrm{error}} = 0$. □

We are prepared to prove Lemma 13.

Proof of Lemma 13.

Case (i) $0 \leq q\theta_{\mathrm{cover}} \leq \pi$.

Let $U' = \mathrm{diag}\left(e^{i\theta_1}, \ldots, e^{i\theta_n}\right)$. Then the set of eigenvalues of $U'^{\otimes q}$ is

$$\Lambda = \left\{\prod_{j=1}^q e^{i\theta_{k_j}} : 1 \leq k_1, \ldots, k_q \leq n\right\}.$$

Note that if the covering angle θ_{cover} of $\{e^{i\theta_1}, \ldots, e^{i\theta_n}\}$ is formed by $e^{i\theta_k}$ and $e^{i\theta_l}$, then the covering angle of Λ is $q\theta_{\mathrm{cover}}$ and formed by $e^{iq\theta_k}$ and $e^{iq\theta_l}$, as long as q is not too large.

As the proof of Lemma 15, the minimum value of the square of the fidelity of $U_1^{\otimes q}|\phi\rangle$ and $U_2^{\otimes q}|\phi\rangle$ is

$$\min_{|\phi\rangle} \left|\langle\phi| U_1^{\otimes q\dagger} U_2^{\otimes q} |\phi\rangle\right| = \min_{|\phi'\rangle} \left|\langle\phi'| U'^{\otimes q} |\phi'\rangle\right| = \min_{\sum_{j=1}^{qn} |\alpha_j|^2 = 1} \left||\alpha_1|^2 e^{iq\theta_1} + |\alpha_2|^2 e^{i((q-1)\theta_1+\theta_2)} + \cdots + |\alpha_{qn}|^2 e^{iq\theta_n}\right|.$$

This is the square of the shortest distance from the origin of the complex plane to the convex set

$$C_q := \left\{|\alpha_1|^2 e^{iq\theta_1} + |\alpha_2|^2 e^{i((q-1)\theta_1+\theta_2)} + \cdots + |\alpha_{qn}|^2 e^{iq\theta_n} : \sum_{j=1}^{qn} |\alpha_j| = 1\right\}.$$

The shortest distance from the origin of the complex plane to C_q is equal to the line segment

$$C_q' := \left\{|\alpha_x|^2 e^{iq\theta_k} + |\alpha_y|^2 e^{iq\theta_l} : |\alpha_x|^2 + |\alpha_y|^2 = 1\right\}.$$

See Fig. 4 for illustration. Hence, in the same way as the

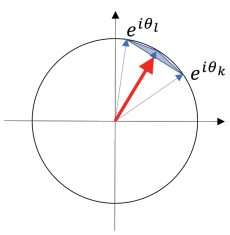

Fig. 3 The shortest distance to the convex set C

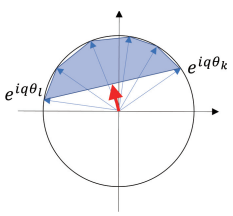

Fig. 4 The shortest distance to the convex set C_q

proof of Lemma 15, we have

$$P^{U}_{\text{error}} \leq \frac{1}{2}\sqrt{\cos\frac{q\theta_{\text{cover}}}{2}} \quad (0 \leq q\theta_{\text{cover}} \leq \pi).$$

Case (ii) $\pi \leq q\theta_{\text{cover}}$.
Since the convex set C_q contains the origin of the complex plane, the error probability of $\mathcal{A}$ can be made zero as the case of $q = 1$. □

4. Worst-Case Upper Bounds

A quantum state discriminator is generally designed to optimize the success probability under a given probability distribution over a set of candidate states. In contrast, Harrow et al. showed the existence of a quantum state discriminator $\mathcal{M}^*$ which solves quantum state discrimination problem independently of the probability distribution over a candidate set by using the min-max theorem [22]. Namely, they showed that some $\mathcal{M}^*$ can solve the quantum state discrimination problem in the worst case.

By applying the argument of Harrow et al. to our setting, we can show the existence of the unitary operator discriminator $\mathcal{A}^*$ in the worst case as in quantum state discrimination problem.

Theorem 16: Let θ_{cover} be the covering angle of $U_1^\dagger U_2$. There exists a non-adaptive $\lceil\sqrt{6}\theta_{\text{cover}}^{-1}\rceil$-query discriminator $\mathcal{A}^*$ that solves UODP$(\{U_1, U_2\})$ in the worst case.

Proof. $\mathcal{A}^*$ is constructed by replacing "QSDP algorithm" in Fig. 1 with $\mathcal{M}^*$. Using $\mathcal{A}^*$, we can show the worst-case upper bound given in the statement by the same analysis with Theorem 14. □

5. Lower Bounds

Every unitary operator discriminator can be represented as an adaptive discriminator given in Fig. 5. We now analyze the necessary number q of queries to solve UODP$(\{U_1, U_2\})$ for every distinct U_1 and U_2. In this section, we suppose that one of U_1 and U_2 is given from a candidate set with probability 1/2.

The unitary operators in Fig. 5 can be described as follows:

$$\hat{U} := X_q(U \otimes \mathbb{I})X_{q-1}(U \otimes \mathbb{I})\cdots X_1(U \otimes \mathbb{I})$$

from a given $U \in \{U_1, U_2\}$ and any fixed unitary operators $X_i\,(i = 1, 2, \ldots, q)$.

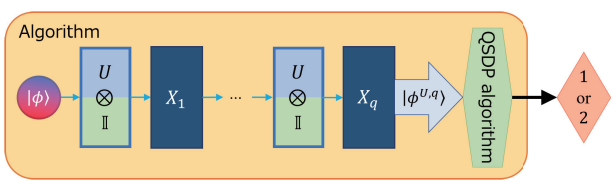

Fig. 5 The arbitrary adaptive discriminator

The following theorem shows the necessary number of queries for every distinct U_1 and U_2.

Theorem 17: Let θ_{cover} be the covering angle of $U_1^\dagger U_2$. If $\mathcal{A}$ solves UODP$(\{U_1, U_2\})$ with q adaptive queries, $q \geq \left\lceil\frac{2}{3\theta_{\text{cover}}}\right\rceil$ holds.

Proof. Let $|\phi\rangle$ be any initial state and let $\left|\phi^{U,q}\right\rangle$ be the state after applying $\hat{U}$ to the initial state $|\phi\rangle$. Then, we obtain the following states for U_1 and U_2 respectively:

$$\begin{aligned}\hat{U}_1|\phi\rangle &:= \left|\phi^{U_1,q}\right\rangle \\ &= X_q(U_1 \otimes \mathbb{I})X_{q-1}(U_1 \otimes \mathbb{I})\cdots X_1(U_1 \otimes \mathbb{I})|\phi\rangle, \\ \hat{U}_2|\phi\rangle &:= \left|\phi^{U_2,q}\right\rangle \\ &= X_q(U_2 \otimes \mathbb{I})X_{q-1}(U_2 \otimes \mathbb{I})\cdots X_1(U_2 \otimes \mathbb{I})|\phi\rangle.\end{aligned}$$

We represent their states as $\rho_q := \left|\phi^{U_1,q}\right\rangle\!\left\langle\phi^{U_1,q}\right|$ and $\sigma_q := \left|\phi^{U_2,q}\right\rangle\!\left\langle\phi^{U_2,q}\right|$ respectively. Then, the trace norm is $\left\|\rho_q - \sigma_q\right\|_{\text{tr}}$, and we obtain the equation as follows:

$$\begin{aligned}\left\|\rho_q - \sigma_q\right\|_{\text{tr}} = \Big\| & X_q(U_1 \otimes \mathbb{I})\rho_{q-1}(U_1 \otimes \mathbb{I})^\dagger X_q^\dagger \\ & - X_q(U_2 \otimes \mathbb{I})\sigma_{q-1}(U_2 \otimes \mathbb{I})^\dagger X_q^\dagger \Big\|_{\text{tr}}.\end{aligned}$$

Since unitary operators do not change the trace distance, we have

$$\begin{aligned}&\Big\| X_q(U_1 \otimes \mathbb{I})\rho_{q-1}(U_1 \otimes \mathbb{I})^\dagger X_q^\dagger \\ &\qquad - X_q(U_2 \otimes \mathbb{I})\sigma_{q-1}(U_2 \otimes \mathbb{I})^\dagger X_q^\dagger \Big\|_{\text{tr}} \\ &= \Big\| (U_1 \otimes \mathbb{I})\rho_{q-1}(U_1 \otimes \mathbb{I})^\dagger \\ &\qquad - (U_2 \otimes \mathbb{I})\sigma_{q-1}(U_2 \otimes \mathbb{I})^\dagger \Big\|_{\text{tr}}.\end{aligned}$$

By the triangle inequality,

$$\begin{aligned}&\Big\| (U_1 \otimes \mathbb{I})\rho_{q-1}(U_1 \otimes \mathbb{I})^\dagger - (U_2 \otimes \mathbb{I})\sigma_{q-1}(U_2 \otimes \mathbb{I})^\dagger \Big\|_{\text{tr}} \\ &= \Big\| (U_1 \otimes \mathbb{I})\rho_{q-1}(U_1 \otimes \mathbb{I})^\dagger - (U_1 \otimes \mathbb{I})\sigma_{q-1}(U_1 \otimes \mathbb{I})^\dagger \\ &+ (U_1 \otimes \mathbb{I})\sigma_{q-1}(U_1 \otimes \mathbb{I})^\dagger - (U_2 \otimes \mathbb{I})\sigma_{q-1}(U_2 \otimes \mathbb{I})^\dagger \Big\|_{\text{tr}} \\ &\leq \left\|\rho_{q-1} - \sigma_{q-1}\right\|_{\text{tr}} \\ &+ \Big\| (U_1 \otimes \mathbb{I})\sigma_{q-1}(U_1 \otimes \mathbb{I})^\dagger - (U_2 \otimes \mathbb{I})\sigma_{q-1}(U_2 \otimes \mathbb{I})^\dagger \Big\|_{\text{tr}}.\end{aligned}$$

By Definition 3, 4 and Lemma 5, $\Big\| (U_1 \otimes \mathbb{I})\sigma_{q-1}(U_1 \otimes \mathbb{I})^\dagger - (U_2 \otimes \mathbb{I})\sigma_{q-1}(U_2 \otimes \mathbb{I})^\dagger \Big\|_{\text{tr}}$ is:

$$\begin{aligned}&\Big\| (U_1 \otimes \mathbb{I})\sigma_{q-1}(U_1 \otimes \mathbb{I})^\dagger - (U_2 \otimes \mathbb{I})\sigma_{q-1}(U_2 \otimes \mathbb{I})^\dagger \Big\|_{\text{tr}} \\ &= 2d\Big((U_1 \otimes \mathbb{I})\sigma_{q-1}(U_1 \otimes \mathbb{I})^\dagger, (U_2 \otimes \mathbb{I})\sigma_{q-1}(U_2 \otimes \mathbb{I})^\dagger\Big) \\ &= 2\sqrt{1 - F\Big((U_1 \otimes \mathbb{I})\sigma_{q-1}(U_1 \otimes \mathbb{I})^\dagger, (U_2 \otimes \mathbb{I})\sigma_{q-1}(U_2 \otimes \mathbb{I})^\dagger\Big)^2} \\ &= 2\sqrt{1 - \left|\left\langle\phi^{U_2,q-1}\right|(U_1 \otimes \mathbb{I})^\dagger(U_2 \otimes \mathbb{I})\left|\phi^{U_2,q-1}\right\rangle\right|^2} \\ &= 2\sqrt{1 - \left|\left\langle\phi^{U_2,q-1}\right|\Big(U_1^\dagger U_2 \otimes \mathbb{I}\Big)\left|\phi^{U_2,q-1}\right\rangle\right|^2}\end{aligned}$$

$$\leq 2\sqrt{1-\min_{|\psi\rangle}\left|\langle\psi|\left(U_1^\dagger U_2\otimes\mathbb{I}\right)|\psi\rangle\right|^2}.$$

Since $U_1^\dagger U_2$ is diagonalizable, there is always the unitary operator V for generating the diagonal operator D from the $U_1^\dagger U_2$. Therefore, we obtain $U_1^\dagger U_2 = VDV^\dagger$. By using it,

$$\begin{aligned}
&\min_{|\psi\rangle}\left|\langle\psi|\left(U_1^\dagger U_2\otimes\mathbb{I}\right)|\psi\rangle\right|^2\\
&=\min_{|\psi\rangle}\left|\langle\psi|\left(VDV^\dagger\otimes\mathbb{I}\right)|\psi\rangle\right|^2\\
&=\min_{|\psi\rangle}\left|\langle\psi|\left(V\otimes\mathbb{I}\right)\left(D\otimes\mathbb{I}\right)\left(V^\dagger\otimes\mathbb{I}\right)|\psi\rangle\right|^2.
\end{aligned}$$

Here, using the state $|\psi'\rangle$ satisfying $|\psi'\rangle = \left(V^\dagger\otimes\mathbb{I}\right)|\psi\rangle$, we obtain:

$$\begin{aligned}
&\min_{|\psi\rangle}\left|\langle\psi|\left(V\otimes\mathbb{I}\right)\left(D\otimes\mathbb{I}\right)\left(V^\dagger\otimes\mathbb{I}\right)|\psi\rangle\right|^2\\
&\qquad=\min_{|\psi'\rangle}\left|\langle\psi'|\left(D\otimes\mathbb{I}\right)|\psi'\rangle\right|^2.
\end{aligned}$$

Let $D = \mathrm{diag}\left(e^{i\theta_1},\ldots,e^{i\theta_n}\right)$ and let $\left(e^{i\theta_k}, e^{i\theta_l}\right)$ be the pair making the covering angle θ_{cover}. Then $\min_{|\psi'\rangle}|\langle\psi'|(D\otimes\mathbb{I})|\psi'\rangle|^2$ becomes as follows:

$$\begin{aligned}
&\min_{|\psi'\rangle}\left|\langle\psi'|\left(D\otimes\mathbb{I}\right)|\psi'\rangle\right|^2 = \left|\frac{1}{2}e^{i\theta_k}+\frac{1}{2}e^{i\theta_l}\right|^2\\
&=\frac{1}{2}\left(1+\cos\left(\theta_k-\theta_l\right)\right)=\frac{1}{2}\left(1+\cos\theta_{\mathrm{cover}}\right)\\
&\qquad=\cos^2\frac{\theta_{\mathrm{cover}}}{2}.
\end{aligned}$$

Therefore, we obtain the following equation:

$$\begin{aligned}
&2\sqrt{1-\min_{|\psi\rangle}\left|\langle\psi|\left(U_1^\dagger U_2\otimes\mathbb{I}\right)|\psi\rangle\right|^2}\\
&=2\sqrt{1-\cos^2\frac{\theta_{\mathrm{cover}}}{2}}=2\sin\frac{\theta_{\mathrm{cover}}}{2}.
\end{aligned}$$

Since $\sin\theta\leq\theta$, we obtain $2\sin\frac{\theta_{\mathrm{cover}}}{2}\leq\theta_{\mathrm{cover}}$. Therefore, we obtain:

$$\begin{aligned}
\left\|\rho_q-\sigma_q\right\|_{\mathrm{tr}} &\leq \left\|\rho_{q-1}-\sigma_{q-1}\right\|_{\mathrm{tr}}\\
&\quad+2\sqrt{1-\min_{|\psi\rangle}\left|\langle\psi|\left(U_1^\dagger U_2\otimes\mathbb{I}\right)|\psi\rangle\right|^2}\\
&\leq \left\|\rho_{q-1}-\sigma_{q-1}\right\|_{\mathrm{tr}}+\theta_{\mathrm{cover}}.
\end{aligned}$$

This means that the trace distance only increases at most θ_{cover} per once query. Therefore, we obtain $\left\|\rho_q-\sigma_q\right\|_{\mathrm{tr}}\leq q\theta_{\mathrm{cover}}$. Since the discrimination error probability P_{error}^U after q queries is represented with $\frac{1}{2}\left(1-\frac{1}{2}\left\|\rho_q-\sigma_q\right\|_{\mathrm{tr}}\right)$ from Theorem 7, P_{error}^U becomes as follows:

$$P_{\mathrm{error}}^U\geq\frac{1}{2}\left(1-\frac{1}{2}q\theta_{\mathrm{cover}}\right).$$

Thus, from $\frac{1}{2}\left(1-\frac{1}{2}q\theta_{\mathrm{cover}}\right)\leq\frac{1}{3}$, we have $q\geq\frac{2}{3\theta_{\mathrm{cover}}}$. Since the number of queries q is integer, using the ceiling function, $q\geq\left\lceil\frac{2}{3\theta_{\mathrm{cover}}}\right\rceil$ holds. □

6. Improved Analysis for Lower Bounds of Fidelity

The observation and analysis in this section are attributed to Mori [27].

In Sects. 3 and 5, we proved upper and lower bounds of the query complexity from the fidelity of quantum states. Actually, the upper bound of the fidelity $F\left(\left|\phi^{U_1,q}\right\rangle\!\left\langle\phi^{U_1,q}\right|,\left|\phi^{U_2,q}\right\rangle\!\left\langle\phi^{U_2,q}\right|\right)\leq\cos\frac{q\theta_{\mathrm{cover}}}{2}$ obtained in Sect. 3 is exactly optimal, since we can show the following tight lower bound:

Lemma 18: [Mori [27]] Let θ_{cover} be the covering angle of $U_1^\dagger U_2$. For every $X_1,\ldots,X_{q-1}$ and every $|\phi\rangle$, we have

$$F\left(\left|\phi^{U_1,q}\right\rangle\!\left\langle\phi^{U_1,q}\right|,\left|\phi^{U_2,q}\right\rangle\!\left\langle\phi^{U_2,q}\right|\right)\geq\cos\frac{q\theta_{\mathrm{cover}}}{2}$$

if $0\leq q\theta_{\mathrm{cover}}<\pi$.

Proof. The idea for improving the lower bound is the same as Zalka's proof of the exact optimality of Grover's quantum search [28]. Let

$$\begin{aligned}
\left|\phi^{i,q}\right\rangle = X_q\left(U_2\otimes\mathbb{I}\right)X_{q-1}\left(U_2\otimes\mathbb{I}\right)\cdots X_{i+1}\left(U_2\otimes\mathbb{I}\right)\\
X_i\left(U_1\otimes\mathbb{I}\right)X_{i-1}\cdots X_1\left(U_1\otimes\mathbb{I}\right)|\phi\rangle
\end{aligned}$$

for $i\in\{0,1,\ldots,q-1\}$. Note that $\left|\phi^{0,q}\right\rangle=\left|\phi^{U_2,q}\right\rangle$ and $|\phi^{q,q}\rangle=\left|\phi^{U_1,q}\right\rangle$.

Let $\cos\theta_{0,1}=\left|\left\langle\phi^{0,q}\middle|\phi^{1,q}\right\rangle\right|$ and $\cos\theta_{1,q}=\left|\left\langle\phi^{1,q}\middle|\phi^{q,q}\right\rangle\right|$ for $0\leq\theta_{0,1},\theta_{1,q}\leq\pi/2$. We now show that

$$\left|\left\langle\psi^{0,q}\middle|\psi^{q,q}\right\rangle\right|\geq\cos(\theta_{0,1}+\theta_{1,q}). \tag{3}$$

Define $x=\left\langle\phi^{0,q}\middle|\phi^{q,q}\right\rangle$, $y_{0,1}=\left\langle\phi^{0,q}\middle|\phi^{1,q}\right\rangle$, and $y_{1,q}=\left\langle\phi^{1,q}\middle|\phi^{q,q}\right\rangle$. The Gram matrix

$$\begin{aligned}
G&=\begin{bmatrix}\left\langle\phi^{0,q}\right|\\ \left\langle\phi^{1,q}\right|\\ \left\langle\phi^{q,q}\right|\end{bmatrix}\begin{bmatrix}\left|\phi^{0,q}\right\rangle & \left|\phi^{1,q}\right\rangle & |\phi^{q,q}\rangle\end{bmatrix}\\
&=\begin{bmatrix}1 & y_{0,1} & x\\ y_{0,1}^* & 1 & y_{1,q}\\ x^* & y_{1,q}^* & 1\end{bmatrix}
\end{aligned}$$

is positive semidefinite, and thus, its determinant

$$\det(G)=1+2\mathrm{Re}(y_{0,1}y_{1,q}x^*)-\left|y_{0,1}\right|^2-\left|y_{0,1}\right|^2-|x|^2$$

is non-negative. Since $\left|y_{0,1}\right|\left|y_{1,q}\right||x|\geq\mathrm{Re}(y_{0,1}y_{1,q}x^*)$ and $\left|y_{0,1}\right|=\cos\theta_{0,1},\left|y_{1,q}\right|=\cos\theta_{1,q}$, we obtain

$$1+2\cos\theta_{0,1}\cos\theta_{1,q}|x|-\cos\theta_{0,1}^2-\cos\theta_{1,q}^2-|x|^2\geq 0.$$

Therefore, we obtain $|x|\geq\cos(\theta_{0,1}+\theta_{1,q})$, which implies (3).

In addition, we have

$$\left|\left\langle \phi^{0,q} \middle| \phi^{1,q} \right\rangle\right| = \cos\theta_{0,1} \geq \cos\frac{\theta_{\text{cover}}}{2},$$

as done in the proof of Lemma 15. By induction, we can obtain

$$\left|\left\langle \phi^{0,q} \middle| \phi^{q,q} \right\rangle\right| \geq \cos\frac{q\theta_{\text{cover}}}{2}$$

for $0 \leq q\theta_{\text{cover}} < \pi$. □

By Theorem 7, the error probability is completely characterized by the fidelity if the distribution on $\{U_1, U_2\}$ is uniform. Therefore, we obtain the optimal lower bound of the error probability

$$P^{U}_{\text{error}} \geq \frac{1}{2}\left(1 - \sin\left(\frac{q\theta_{\text{cover}}}{2}\right)\right)$$

from Lemma 18 for $0 \leq q < \pi/\theta_{\text{cover}}$. Then, we can reprove the lower bound $\lceil \pi/\theta_{\text{cover}} \rceil$ of query complexity for perfect unitary discrimination, which was shown in [9].

Acknowledgments

The preliminary version of this paper was published in COCOON 2017. AK was partially supported by MEXT KAKENHI (24106009) and JSPS KAKENHI (16H01705, 17K12640). ST was supported in part by MEXT KAKENHI (24106003) and JSPS KAKENHI (26330011, 16H02782). FLG was partially supported by MEXT KAKENHI (24106009) and JSPS KAKENHI (16H01705, 16H05853). The authors are grateful to Akihito Soeda for helpful discussions and to Ryuhei Mori for his observation and analysis described in Sect. 6 for improvements of the lower bounds. The authors also appreciate the editor and reviewers for valuable comments to earlier versions of this paper.

References

[1] K.M.R. Audenaert, J. Calsamiglia, L. Masanes, R. Muñoz-Tapia, A. Acín, E. Bagan, and F. Verstraete, "The quantum Chernoff2 bound," Physical Review Letters, vol.98, no.160501, 2007.
[2] A. Chefles, "Unambiguous discrimination between linearly independent quantum states," Physics Letters A, vol.239, no.6, pp.339–347, March 1998.
[3] Y. Feng, R. Duan, and M. Ying, "Unambiguous discrimination between quantum mixed states," Physical Review A, vol.70, no.012308, July 2004.
[4] C. Mochon, "Family of generalized "pretty good" measurements and the minimal-error pure-state discrimination problems for which they are optimal," Physical Review A, vol.73, no.012308, March 2006.
[5] A. Acín, "Statistical distinguishability between unitary operations," Physical Review Letters, vol.87, no.177901, 2001.
[6] A. Chefles, A. Kitagawa, M. Takeoka, M. Sasaki, and J. Twamley, "Unambiguous discrimination among oracle operators," Journal of Physics A: Mathematical and Theoretical, vol.40, no.10183, 2007.
[7] A.M. Childs, J. Preskill, and J. Renes, "Quantum information and precision measurement," Journal of Modern Optics, vol.47, no.2-3, pp.155–176, 2000.
[8] G.M. D'Ariano, P.L. Presti, and M.G.A. Paris, "Using entanglement improves the precision of quantum measurements," Physical Review Letters, vol.87, no.270404, 2001.
[9] R. Duan, Y. Feng, and M. Ying, "Entanglement is not necessary for perfect discrimination between unitary operations," Physical Review Letters, vol.98, no.100503, 2007.
[10] R. Duan, Y. Feng, and M. Ying, "The perfect distinguishability of quantum operations," Physical Review Letters, vol.103, no.210501, 2009.
[11] M. Piani and J. Watrous, "All entangled states are useful for channel discrimination," Physical Review Letters, vol.102, no.250501, 2009.
[12] G. Wang and M. Ying, "Unambiguous discrimination among quantum operations," Physical Review A, vol.73, no.042301, 2006.
[13] Z. Ji, Y. Feng, R. Duan, and M. Ying, "Identification and distance measures of measurement apparatus," Physical Review Letters, vol.96, no.200401, 2006.
[14] M.F. Sacchi, "Optimal discrimination of quantum operations," Physical Review A, vol.71, no.062340, 2005.
[15] M. Ziman and M. Sedlák, "Single-shot discrimination of quantum unitary processes," Journal of Modern Optics, vol.57, no.3, pp.253–259, 2010.
[16] L.K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," Physical Review Letters, vol.79, no.325, July 1997.
[17] A. Ambainis, K. Iwama, A. Kawachi, R. Raymond, and S. Yamashita, "Improved algorithms for quantum identification of boolean oracles," Theoretical Computer Science, vol.378, no.1, pp.41–53, 2007.
[18] R. Kothari, "An optimal quantum algorithm for the oracle identification problem," Proceedings of the 31st International Symposium on Theoretical Aspects of Computer Science (STACS 2014), Leibniz International Proceedings in Informatics, vol.25, pp.482–493, 2014.
[19] G. Chiribella, G.M. D'Ariano, and P. Perinotti, "Memory effects in quantum channel discrimination," Physical Review Letters, vol.101, no.180501, 2008.
[20] A. Ambainis, K. Iwama, A. Kawachi, H. Masuda, R.H. Putra, and S. Yamashita, "Quantum identification of boolean oracles," Proceedings of the 21st Annual Symposium on Theoretical Aspects of Computer Science, LNCS 2996, pp.105–116, 2004.
[21] A.W. Harrow, A. Hassidim, D.W. Leung, and J. Watrous, "Adaptive versus non-adaptive strategies for quantum channel discrimination," Physical Review A, vol.81, no.032339, 2010.
[22] A.W. Harrow and A. Winter, "How many copies are needed for state discrimination?," IEEE Trans. Inf. Theory, vol.58, no.1, pp.1–2, Jan. 2012.
[23] D. Aharanov, A. Kitaev, and N. Nisan, "Quantum circuits with mixed states," Proceedings of the 30th annual ACM Symposium on Theory of Computing, pp.20–30, 1998.
[24] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[25] H. Barnum and E. Knill, "Reversing quantum dynamics with near-optimal quantum and classical fidelity," Journal of Mathematical Physics, vol.43, no.5, pp.2097–2106, 2002.
[26] N. Johnston, D.W. Kribs, and V.I. Paulsen, "Computing stabilized norms for quantum operations via the theory of completely bounded maps," Quantum Information and Computation, vol.9, no.1, pp.16–35, 2009.
[27] R. Mori, personal communication, 2018.
[28] C. Zalka, "Grover's quantum searching algorithm is optimal," Physical Review A, vol.60, no.4, pp.2746–2751, 1999.

Akinori Kawachi is an associate professor of Department of Information and Communications Technology, Osaka University. Received B.E., M.Info., and Ph.D. degrees from Kyoto University in 2000, 2002, and 2004, respectively. His research interests are computational complexity, quantum computing, and foundations of cryptography.

Kenichi Kawano has received B.E. and M.E. from Tokushima University in 2016, and 2018. He currently works at Sun-M System.

François Le Gall is an associate professor at the Graduate School of Informatics, Kyoto University. He received his Ph.D. from the University of Tokyo in 2006 under the supervision of Hiroshi Imai. His research interests include quantum computation and algorithms.

Suguru Tamaki is an assistant professor of Informatics at Kyoto University. He received his Ph.D. from Kyoto University in 2006 under the supervision of Kazuo Iwama. His research interests include algorithms and theory of computation.