The efficiency of quantum identity testing of multiple states

2008 J. Phys. A: Math. Theor. 41 395309

(http://iopscience.iop.org/1751-8121/41/39/395309)

IOP PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **41** (2008) 395309 (13pp) doi:10.1088/1751-8113/41/39/395309

The efficiency of quantum identity testing of multiple states

Masaru Kada[1], **Harumichi Nishimura**[1] **and Tomoyuki Yamakami**[2]

[1] School of Science, Osaka Prefecture University, 1-1 Gakuen-cho, Sakai, Osaka 599-8531, Japan
[2] School of Computer Science and Engineering, University of Aizu, 90 Kami-Iawase, Tsuruga, Ikki-machi, Aizu-Wakamatsu, Fukushima 965-8580, Japan

E-mail: kada@mi.s.osakafu-u.ac.jp, hnishimura@mi.s.osakafu-u.ac.jp and yamakami@u-aizu.ac.jp

Received 2 May 2008, in final form 8 August 2008
Published 8 September 2008
Online at stacks.iop.org/JPhysA/41/395309

Abstract

We examine two quantum operations, the permutation test and the circle test, which test the identity of n quantum states. These operations naturally extend the well-studied swap test on two quantum states. We first show the optimality of the permutation test for any input size n as well as the optimality of the circle test for three input states. In particular, when $n = 3$, we present a semi-classical protocol, incorporated with the swap test, which approximates the circle test efficiently. Furthermore, we show that, with the help of classical preprocessing, a single use of the circle test can approximate the permutation test efficiently for an arbitrary input size n.

PACS numbers: 03.67.−a, 03.67.Ac

1. Introduction

When we manipulate quantum information, one of the fundamental operations is to compare two or more pieces of quantum information. In particular, we wish to test whether two quantum states are identical or nearly orthogonal to each other. A standard quantum operation to test the identity of two quantum states is the *(controlled) swap test*, which 'conditionally' swaps the two quantum states and obtains an answer by measuring its controlled qubit. The swap test finds a direct application to, for instance, the *fingerprinting* protocol of Buhrman *et al* [7]. They considered the following three-party communication game (known as the *simultaneous message passing model* in communication complexity [16]). Two parties, Alice and Bob, hold m-bit inputs x and y, respectively, and the referee wishes to calculate a desired value $f(x, y)$ correctly with high probability, based solely on the messages received from Alice and Bob, who are prohibited to communicate with each other.

For instance, the equality function EQ (i.e., $EQ(x, y) = 1$ if $x = y$ and 0 otherwise) requires, by a quantum operation of Buhrman *et al* [7], Alice and Bob to send quantum information of $O(\log m)$ qubits to the referee, who applies the swap test over the received quantum states to test whether $x = y$ (and thus computes $EQ(x, y)$). In Stark comparison, Alice and Bob should send $\Omega(\sqrt{m})$ bits of classical information to referee [4, 17] (this bound turns out to be tight [2]) to compute the equality function. The usefulness of the swap test in the above protocol of Buhrman *et al* stems from the fact that two quantum states received from Alice and Bob are either identical (when $x = y$) or nearly orthogonal (when $x \neq y$).

Besides [7], the swap test has been a key player in various fingerprinting protocols in, e.g., [3, 6, 11, 18, 20]. Moreover, the swap test has been used in various physical and computational settings, which include stabilization of quantum computation [5], quantum estimation [9], quantum Merlin–Arthur games [15] and black-box group problems [10]. Nevertheless, the swap test handles only two quantum states. How can we test the identity of more than two quantum states?

This paper examines two natural generalizations of the swap test, referred to as the *permutation test* and the *circle test*, which turn out to be useful tools in testing the identity of three or more quantum states. Instead of swapping two states in the swap test, the permutation test 'conditionally' permutes n input states by applying, in superposition, all possible permutations over n elements. The circle test is a simpler form of the permutation test using only multiple applications of a single permutation. (For their formal definitions, see section 2.) In a slightly different context, the permutation test can be used to amplify the success probability of the aforementioned quantum protocol for EQ [7]. In this paper, our focal point is the following problem of testing the identity of n quantum states in a state space $\mathcal{H}$, provided that these states are either identical or mutually orthogonal, for simplicity of our argument.

Quantum-state identity problem (QSI_n)
Input: n quantum states $(|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle)$ in a state space $\mathcal{H}$.
Promise: Any pair of the n quantum states is equal or orthogonal.
Output: YES if all n states are identical; NO otherwise.

Over two input states, the swap test can solve the above identity problem QSI_2 by outputting 'EQUAL' on any 'YES' instance with certainty (*completeness error probability* 0) and outputting 'NOT EQUAL' on any 'NO' instance with probability exactly $1/2$ (*soundness error probability* $1/2$). Under the so-called *one-sided error requirement*, in which the completeness error probability should be 0, the swap test is known to be an optimal quantum operation for the identity problem QSI_2. This fact was implicitly proven in 2001 by Kobayashi *et al* [14] (see also [6]). In section 2, we show the optimality of the circle test as well as the permutation test under the same one-sided error requirement; more precisely, the circle test is an optimal operation for the problem QSI_3, and the permutation test is optimal for QSI_n for an arbitrary input size $n \geqslant 2$.

Subsequently, we present efficient approximations of the circle test and the permutation test using 'semi-classical' protocols involving the swap test and the circle test, respectively. As a direct consequence, these approximations help us build a concise quantum circuit that solves the problem QSI_n efficiently, because a quantum circuit that implements the swap test (resp. the circle test) is significantly more concise than any quantum circuit for the circle test (resp. the permutation test). In section 3, we show how a certain sequential application of the swap test efficiently approximates the circle test for QSI_3. Such an operation gives an optimal approximation procedure. In section 4, we show that, with the help of classical preprocessing, a single application of the circle test can approximate the permutation test for

QSI_n with efficiency, which is one-sided error and has optimal soundness error probability up to a multiplicative factor of smaller than 2. We conclude in section 5 with an extension of our results and also a suggestion of future directions.

2. The permutation test and the circle test

Besides the well-studied swap test, we introduce two useful tests, called the *permutation test* and the *circle test*, which are intended to solve our quantum-state identity problem QSI_n on n input states taken from a state space $\mathcal{H}$. We begin with the formal definition of the permutation test on n quantum states $(|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle) \in \mathcal{H}^{\otimes n}$. For our notational convenience, let $\sigma = \{\sigma_0, \sigma_1, \ldots, \sigma_{n!-1}\}$ denote the set of all $n!$ permutations over the integer set $[n] := \{1, 2, \ldots, n\}$; namely, for each $i \in [n]$, σ_i denotes the ith element of the symmetric group S_n (in a certain fixed order). Note that the swap test is in fact the permutation test on two quantum states.

Permutation test

Input: n quantum states $(|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle)$ in a state space $\mathcal{H}$.

(i) Start with the quantum state $|0\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$, where $|0\rangle$ (often called the first register) denotes the ground state in the $n!$-dimensional state space.
(ii) Apply the quantum Fourier transform $F_{n!}$ over $n!$ elements to the first register.
(iii) Apply a controlled-σ operation; that is, if the first register contains index $i \in \{0, 1, \ldots, n! - 1\}$, transform $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ to $|\psi_{\sigma_i(1)}\rangle \otimes \cdots \otimes |\psi_{\sigma_i(n)}\rangle$.
(iv) Apply the inverse quantum Fourier transform $(F_{n!})^{-1}$ to the first register.
(v) Measure the first register in the computational basis. If 0 is observed, output EQUAL; otherwise, output NOT EQUAL.

The circle test is a simple form of the permutation test, defined by multiple applications of a single permutation, denoted σ_c, where σ_c is the permutation on $[n]$ of the following form: $\sigma_c(n) = 1$ and $\sigma_c(i) = i + 1$ for any index $i \in [n - 1]$. The notation $\sigma_c^j(i)$ means the result of the j applications of σ_c to i.

Our motivation for introducing the circle test is to provide a tool for building a 'concise' quantum circuit that solves QSI_n efficiently. Consider a quantum circuit that implements the permutation test for the problem QSI_n. Since the permutation test involves the quantum Fourier transform $F_{n!}$ over $n!$ elements, a straightforward decomposition of such a transform gives a large-size quantum circuit for QSI_n. It is therefore better to use a simpler quantum test (than the permutation test) to solve the problem QSI_n with efficiency.

Circle test

Input: n quantum states $(|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle)$ in a state space $\mathcal{H}$.

(i) Start with the quantum state $|0\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ where $|0\rangle$ (often called the first register) denotes the ground state in the n-dimensional state space.
(ii) Apply the quantum Fourier transform F_n to the first register.
(iii) Apply a controlled-σ_c operation; namely, when the first register contains $i \in \{0, 1, \ldots, n-1\}$, transform $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ to $\left|\psi_{\sigma_c^i(1)}\right\rangle \otimes \cdots \otimes \left|\psi_{\sigma_c^i(n)}\right\rangle$.
(iv) Apply the inverse quantum Fourier transform $(F_n)^{-1}$ to the first register.
(v) Measure the first register in the computational basis. If 0 is observed, output EQUAL; otherwise, output NOT EQUAL.

In particular, when $n = 2$, the permutation test as well as the circle test coincides with the swap test. For later analysis, we show how to calculate the probabilities that our new tests on n input states output EQUAL.

Lemma 1. *Given n input states* $(|\psi_1\rangle, \ldots, |\psi_n\rangle) \in \mathcal{H}^{\otimes n}$*, the probabilities that the permutation test and the circle test output EQUAL are, respectively,*

$$\frac{1}{n!}\sum_{k=0}^{n!-1}\prod_{m=1}^{n}\langle\psi_m|\psi_{\sigma_k(m)}\rangle \qquad \text{and} \qquad \frac{1}{n}\sum_{k=0}^{n-1}\prod_{m=1}^{n}\langle\psi_m|\psi_{\sigma_c^k(m)}\rangle. \tag{1}$$

Proof. We show the lemma only for the circle test, because the case of the permutation test can be similarly proven. Let $(|\psi_1\rangle, \ldots, |\psi_n\rangle) \in \mathcal{H}^{\otimes n}$ be our n input states. The circle test outputs EQUAL on these input states with probability exactly $\left\| \sum_{i=0}^{n-1} |\psi_{\sigma_c^i(1)}\rangle \cdots |\psi_{\sigma_c^i(n)}\rangle \right\|^2 / n^2$, which can be further simplified as

$$\frac{1}{n^2}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\langle\psi_{\sigma_c^i(1)}|\psi_{\sigma_c^j(1)}\rangle\cdots\langle\psi_{\sigma_c^i(n)}|\psi_{\sigma_c^j(n)}\rangle$$

$$= \frac{1}{n^2}\sum_{k=0}^{n-1}\sum_{i=0}^{n-1}\prod_{m=1}^{n}\langle\psi_{\sigma_c^i(m)}|\psi_{\sigma_c^{i+k}(m)}\rangle = \frac{1}{n^2}\sum_{k=0}^{n-1}\sum_{i=0}^{n-1}\prod_{m=\sigma_c^{-i}(1)}^{\sigma_c^{-i}(n)}\langle\psi_{\sigma_c^i(m)}|\psi_{\sigma_c^{i+k}(m)}\rangle.$$

Clearly, the last expression equals $\frac{1}{n}\sum_{k=0}^{n-1}\prod_{m=1}^{n}\langle\psi_m|\psi_{\sigma_c^k(m)}\rangle$, as requested. □

From lemma 1, we can obtain the following result for the permutation test.

Proposition 1. *Let n be any number at least 2. The permutation test solves the problem* QSI_n *with completeness error probability 0 and soundness error probability at most* $1/n$.

Proof. Consider a direct application of the permutation test. Obviously, the permutation test has completeness error probability 0 due to expression (1) of lemma 1. Let us fix an arbitrary NO instance $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$. We now argue that in the worst-case scenario, it suffices to consider the case where all indices of our NO instance are divided into two sets I_1 and I_2 satisfying the following 'equivalence' conditions: (i) all states whose indices are in I_1 (resp. I_2) are identical and (ii) any state having an index in I_1 and any state having an index in I_2 are mutually orthogonal. To see that this is sufficient, consider the case where all the indices are divided into three (or more) sets, say, I_1, I_2 and I_3. A key observation is that the soundness error probability on the NO instance is at most the soundness error probability on the same instance whose indices are divided into two sets, I_1 and $I_2 \cup I_3$. Therefore, we need to consider only two sets I_1 and I_2.

Now, assume that we have the aforementioned two sets I_1 and I_2 with $|I_1| = l$ and $|I_2| = n - l$ for a certain number l with $1 \leqslant l \leqslant n-1$. For any permutation σ_k, the value $\prod_{m=1}^{n}\langle\psi_m|\psi_{\sigma_k(m)}\rangle$ becomes 1 if and only if σ_k *setwisely stabilizes* I_1 and I_2; namely, σ_k maps any element with an index in I_1 (resp. I_2) to another element in I_1 (resp. I_2). This property concludes that the soundness error probability of the NO instance equals the ratio between the number of all such permutations and the total number of permutations in S_n. This ratio is clearly $l!(n-l)!/n! \leqslant 1/n$. □

Under the one-sided error requirement, we can show the optimality of the permutation test for QSI_n; namely, any one-sided error quantum operation for QSI_n must have the soundness error probability of at least $1/n$. Earlier, Kobayashi *et al* [14] (see also [6]) implicitly proved the optimality of the permutation test for QSI_2 (equivalently, the swap test).

Proposition 2. *Let n be any number greater than 1. Any quantum operation to solve* QSI_n *under the one-sided error requirement has soundness probability at least* $1/n$.

Proof. Our proof generalizes the new optimality proof for the swap test of Hotta and Ozawa [13], whose fundamental idea is similar to [6, 14]. Let $\mathcal{H}$ be our state space. Let $\{E_y, E_n\}$ denote any optimal binary positive operator-valued measure (POVM) that meets the one-sided error requirement, from which we have $E_y(|\psi\rangle^{\otimes n}) = |\psi\rangle^{\otimes n}$ for any state $|\psi\rangle \in \mathcal{H}$. Let P_S be the projection onto the *symmetric subspace* [5]

$$\{|S_\mu\rangle\} = \left\{ \sum_{\sigma \in S_n} |m_{\sigma(1)}\rangle \cdots |m_{\sigma(n)}\rangle \,\middle|\, \begin{array}{l} m_1, m_2, \ldots, m_n \text{ are the indices of elements} \\ \text{in the computational basis of } \mathcal{H} \end{array} \right\},$$

which is the subspace of $\mathcal{H}^{\otimes n}$ that is symmetric under the interchange of states for any pair of positions in the tensor product. Here, we claim that P_S satisfies the equation $E_y P_S = P_S$. This claim is shown as follows. Note that the symmetric subspace is also the subspace of $\mathcal{H}^{\otimes n}$ spanned by all states of the form $|\psi\rangle^{\otimes n}$ [5]. Using this fact, for any state $|\phi\rangle \in \mathcal{H}^{\otimes n}$, $P_S|\phi\rangle$ can be expressed as $P_S|\phi\rangle = \sum_\alpha c_\alpha |\varphi_\alpha\rangle^{\otimes n}$. The equality $E_y(|\psi\rangle^{\otimes n}) = |\psi\rangle^{\otimes n}$ implies that $P_S|\phi\rangle$ can be further written as

$$\sum_\alpha c_\alpha |\varphi_\alpha\rangle^{\otimes n} = \sum_\alpha c_\alpha E_y(|\varphi_\alpha\rangle^{\otimes n}) = E_y\left(\sum_\alpha c_\alpha |\varphi_\alpha\rangle^{\otimes n}\right) = E_y P_S|\phi\rangle.$$

It follows from the equality $E_y P_S = P_S$ that $E_y = P_S + \sum_v \lambda_v |A_v\rangle\langle A_v|$, where λ_v is nonnegative (because E_y is positive) and $|A_v\rangle$ lies in the orthogonal complement of the symmetric subspace. Therefore, we conclude that $E_y \geqslant P_S$. Note that the soundness error probability p_e equals

$$p_e = \mathrm{Tr}[E_y(|\psi_1\rangle \cdots |\psi_n\rangle\langle\psi_1| \cdots \langle\psi_n|)]$$

for a certain NO instance $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$. We want to show that $p_e \geqslant 1/n$. Now, let us consider a specific NO instance $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$ satisfying that $|\psi_2\rangle = \cdots = |\psi_n\rangle$ as the worst-case instance. From the inequality $E_y \geqslant P_S$, p_e is lower bounded by

$$p_e \geqslant \mathrm{Tr}[P_S(|\psi_1\rangle \cdots |\psi_n\rangle\langle\psi_1| \cdots \langle\psi_n|)] = \frac{1}{n!} \sum_{\sigma \in S_n} \prod_{i=1}^{n} |\langle\psi_i|\psi_{\sigma(i)}\rangle|^2 = \frac{1}{n}.$$

This completes the proof. □

Propositions 1 and 2 show the optimality of the permutation test for an arbitrary input size n. As for the circle test, when $n = 3$, we can show in the following proposition that the circle test is also optimal under the one-sided error requirement.

Proposition 3. *The problem* QSI_3 *is solved with one-sided error probability by the circle test with soundness error probability exactly* $1/3$.

This proposition follows from a more general statement. For technical reasons, we define the *alternation test* by replacing S_n in the definition of the permutation test with the alternating group A_n, which is the group generated by the even permutations in S_n.

Lemma 2. *For any number* $n \geqslant 2$, *the alternation test solves the problem* QSI_n *with completeness error probability 0 and soundness error probability at most* $1/n$.

Proposition 3 immediately follows from this lemma since A_3 equals the cyclic group C_3, which defines the circle test over three states.

Proof of lemma 2. The alternation test has completeness error probability 0 since, similar to proposition 1, the probability p that the alternation test outputs EQUAL on n input states

$(|\psi_1\rangle, \ldots, |\psi_n\rangle)$ is $p = \frac{2}{n!}\sum_{k=0}^{n!/2-1}\prod_{m=1}^{n}\langle\psi_m|\psi_{\tau_k(m)}\rangle$, where $\tau_1, \ldots, \tau_{n!/2}$ denote all the even permutations over $[n]$ (in a certain fixed order). Hereafter, let us fix a NO instance $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$. Similar to the proof of proposition 1, it suffices to deal with the case where all indices of this NO instance are divided into two sets I_1 and I_2 satisfying: (i) all states having indices in I_1 (resp. I_2) are identical and (ii) any state with an index in I_1 and any state with an index in I_2 are mutually orthogonal. Assume that I_1 and I_2 satisfy $|I_1| = l$ and $|I_2| = n - l$ for a certain number l with $1 \leqslant l \leqslant n - 1$.

Note that, for any even permutation τ_k, the value $\prod_{m=1}^{n}\langle\psi_m|\psi_{\tau_k(m)}\rangle$ equals 1 if and only if τ_k setwisely stabilizes I_1 and I_2. Thus, the soundness error probability of the NO instance equals the ratio between the number L of all even permutations that setwisely stabilize I_1 and I_2, and the total number $|A_n|$. We will show that this ratio $L/|A_n|$ is exactly $l!(n-l)!/n!$, and hence $L/|A_n| = l!(n-l)!/n! \leqslant 1/n$. Since $|A_n| = n!/2$, it is enough to prove that $L = l!(n-l)!/2$. To evaluate L, we consider the following two cases: (i) $l = 1$ or $l = n - 1$ and (ii) $2 \leqslant l \leqslant n - 2$.

We consider case (i) when $l = 1$. In this case, any even permutation that setwisely stabilizes I_1 and I_2 must fix a unique element in I_1, and thus it is also an even permutation on I_2. This implies that $L = |A_{n-1}|$, which is $(n-1)!/2$, as desired. In case (ii), any even permutation that setwisely stabilizes I_1 and I_2 is either (a) the product of an even permutation over I_1 and an even permutation over I_2 or (b) the product of an odd permutation over I_1 and an odd permutation over I_2. First, we consider case (a). Let us consider the total number of products of even permutations over I_1 and even permutations over I_2. This number clearly equals $(l!/2)((n-l)!/2) = l!(n-l)!/4$, which implies that $L = l!(n-l)!/2$. Case (b) is similar. □

Unfortunately, the circle test cannot be optimal for certain input sizes n. For instance, if $n = 4$, the circle test can achieve an optimal soundness error probability of $1/4$ for a NO instance $(|\psi\rangle, |\psi\rangle, |\psi\rangle, |\psi^{\perp}\rangle)$, where $|\psi\rangle$ is an arbitrary state in $\mathcal{H}$ and $|\psi^{\perp}\rangle$ denotes a state orthogonal to $|\psi\rangle$, whereas another NO instance $(|\psi\rangle, |\psi^{\perp}\rangle, |\psi\rangle, |\psi^{\perp}\rangle)$ makes the circle test produce a soundness error probability of $1/2$ (which is far greater than $1/4$).

In section 4, we show that the circle test for QSI_n works asymptotically as good as the permutation test, if we incorporate additional classical preprocessing with the circle test.

3. Approximation of the circle test by the swap test

We have shown in the previous section that the permutation test and the circle test are optimal quantum operations to solve the identity problem QSI_3 with one-sided error probability. From a practical viewpoint, it would be ideal to build an identity test for QSI_3 only with the swap test as a main quantum ingredient. This is mainly because the swap test is much simpler than the other two operations, and, more importantly, the swap test has been well studied for its theoretical applications as well as its physical implementations (e.g., see [8, 12, 19]). How can we develop such a test? A simple and natural approach is a sequential application of the swap test (which we refer to as a *Swap protocol*). More precisely, a Swap protocol 'classically' chooses two quantum states for the swap test (out of three or more states) and applies the swap test to them as its only true 'quantum' operation. In the following theorem, we present a certain Swap protocol for QSI_3, which asymptotically achieves the same soundness error probability as the circle test does.

Theorem 1. *Let m be any positive number at least 2. There exists a Swap protocol for* QSI_3*, which achieves the soundness error probability of at most* $1/3 + 1/4^{m-1}$ *by applying the swap test m times sequentially.*

Proof. Let $m \geqslant 2$ be fixed throughout this proof. Our desired Swap protocol for QSI_3, referred to as SRS (sequential random swap), is given as follows.

Protocol SRS(m)

Input: three quantum states $(|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle) \in \mathcal{H}^{\otimes 3}$

(i) Randomly choose two of the three states $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_3\rangle$.
(ii) Repeat the following two steps m times as long as the protocol does not halt.
(ii-1) Perform the swap test on the chosen two states. If the test outputs NOT EQUAL, output NO and halt.
(ii-2) Choose the leftover state as well as one of the two resulting states at random.
(iii) Output YES.

If three input states are identical, then SRS(m) obviously outputs YES with certainty. Consider the case where all the three input states are mutually orthogonal. Hereafter, we deal only with an arbitrary NO instance $(|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle) \in \mathcal{H}^{\otimes 3}$. We first analyze the soundness error probability for $m = 2$. In the protocol SRS(2), the first swap test at step (ii-1) outputs NO with probability exactly $1/2$, regardless of which states are chosen at step (i). Without the loss of generality, we assume that $|\psi_1\rangle$ and $|\psi_2\rangle$ are the chosen states at step (i). After the first swap test outputs EQUAL at step (ii-1), the resulting state is of the form $\frac{1}{\sqrt{2}}(|\psi_1\rangle|\psi_2\rangle + |\psi_2\rangle|\psi_1\rangle)$ since $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal. At step (ii-2), we obtain two input states: the pure state $|\psi_3\rangle$ and the mixed state $\boldsymbol{\rho} = \frac{1}{2}(|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2|)$. These input states can be evaluated as EQUAL by the second swap test at step (ii-1) with probability exactly $\frac{1}{2} + \frac{1}{2}\,\mathrm{Tr}(\boldsymbol{\rho}|\psi_3\rangle\langle\psi_3|) = \frac{1}{2}$. Therefore, we obtain the correct answer NO at step (ii-1) with probability exactly $\frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$. This gives the soundness error probability of $1/4$, which is smaller than $1/3$. Since the soundness error probability of SRS(m) decreases as m becomes larger, we conclude that SRS(m) has soundness error probability smaller than $1/3$.

The more complex case is that two input states are identical and the remainder is orthogonal to them. Because of the symmetry of our protocol, we can assume that $|\psi_1\rangle = |\psi_3\rangle$ and $|\psi_2\rangle = |\psi_1^{\perp}\rangle$. We need to consider the following two cases:

(a) $|\psi_1\rangle$ and $|\psi_2\rangle$ (or alternatively $|\psi_2\rangle$ and $|\psi_3\rangle$) are chosen at step (i).
(b) $|\psi_1\rangle$ and $|\psi_3\rangle$ are chosen at step (i).

We begin with case (a). For notational convenience, we use the following abbreviations: $|1\rangle := |\psi_1^{\perp}\rangle|\psi_1\rangle|\psi_1\rangle$, $|2\rangle := |\psi_1\rangle|\psi_1^{\perp}\rangle|\psi_1\rangle$ and $|3\rangle := |\psi_1\rangle|\psi_1\rangle|\psi_1^{\perp}\rangle$. It is not important for us to choose, at step (ii-2), which of the two resulting states to apply the swap test, since if the protocol does not halt, after step (ii-1), on, say, the first and the second states, the obtained state is in the form: $\alpha(|1\rangle + |2\rangle) + \beta|3\rangle$. For simplicity, we assume that the second state is always chosen at step (ii-2). For our further analysis, we need the following lemma. For readability, we ignore normalization factors of quantum states in the lemma.

Lemma 3. *Let k be any number in $[m]$. Under the condition that the protocol does not halt after the $(k-1)$th swap test in case (a), the (conditional) probability p_k that the protocol does not halt after the kth swap test is $p_k = 1 - \frac{6}{4^k+8}$. The obtained (non-normalized) state can be represented as $(a_k + 1)|1\rangle + (a_k + 1)|2\rangle + a_k|3\rangle$, where $a_k = \frac{2}{3}(4^{(k-1)/2} - 1)$, if k is odd, and $a_k|1\rangle + (a_k + 1)|2\rangle + (a_k + 1)|3\rangle$, where $a_k = \frac{1}{3}(4^{k/2} - 1)$, if k is even.*

Meanwhile, we postpone the proof of this lemma. Let q_k be the (accumulative) probability that the protocol does not halt after the kth swap test in case (a). Since $q_1 = p_1$ and $q_k = p_k q_{k-1}$ for any $k \geqslant 2$, lemma 3 implies that $q_1 = 1/2$ and $q_k = \left(1 - \frac{6}{4^k+8}\right) q_{k-1}$. These recurrence equations have a unique solution $q_k = \frac{1}{3} + \frac{2}{3 \cdot 4^k}$ for any number $k \geqslant 1$.

Next, let us consider case (b). Let r_k be the (accumulative) probability that the protocol does not halt after the kth swap test in case (b). Under our assumption, case (b) can be analyzed in the same way as case (a) if we replace k in case (a) by $k+1$, because the first swap test makes no effect on its subsequent computation. We then obtain that $r_1 = 1$ and $r_k = q_{k-1}$ for any number $k \geqslant 2$.

Note that case (a) holds with probability $2/3$ and case (b) holds with probability $1/3$. Therefore, if the given input is a NO instance, where two of the three states are identical and the other is orthogonal to them, the protocol SRS(m) outputs YES at step (iii) with probability $(2/3)q_m + (1/3)r_m = 1/3 + 1/4^{m-1}$, as requested.

Proof of lemma 3. The proof is done by induction on $k \geqslant 1$. Let p_k denote the probability that the protocol does not halt after kth swap test in case (a). Consider the basis case $k = 1$. After the first swap test, since we obtain the state $|1\rangle + |2\rangle$ with probability $1/2$, the protocol outputs NO with probability exactly $1/2$. Hence, we have $p_1 = 1/2$ and $a_1 = 0$. In the case of $k = 2$, note that the swap test is applied to the second and third states. The total state including the first register (used by the quantum Fourier transform) evolves by the swap test as follows:

$$\begin{aligned}(|0\rangle + |1\rangle)(|1\rangle + |2\rangle) &\mapsto |0\rangle(|1\rangle + |2\rangle) + |1\rangle(|1\rangle + |3\rangle)\\ &\mapsto (|0\rangle + |1\rangle)(|1\rangle + |2\rangle) + (|0\rangle - |1\rangle)(|1\rangle + |3\rangle)\\ &= |0\rangle(2|1\rangle + |2\rangle + |3\rangle) + |1\rangle(|2\rangle - |3\rangle).\end{aligned}$$

Provided that the protocol does not halt, we obtain the state $2|1\rangle + |2\rangle + |3\rangle$, which yields $a_2 = 1$. The desired probability p_2 is thus calculated as

$$p_2 = 1 - \frac{1^2 + (-1)^2}{2^2 + 1^2 + 1^2 + 1^2 + (-1)^2} = 3/4.$$

This yields the lemma for the case $k = 2$.

Next, let k be any integer greater than 2. First, we deal with the case where k is odd. Assuming that the lemma holds for k, we want to show that the lemma also holds for $k+1$. By our induction hypothesis, we have the state $|\psi_k\rangle = (a_k + 1)|1\rangle + (a_k + 1)|2\rangle + a_k|3\rangle$ after the kth swap test, where $a_k = \frac{2}{3}(4^{(k-1)/2} - 1)$. Note that the $(k+1)$th swap test is applied to the second and third states in $|\psi_k\rangle$. The swap test makes the total state evolve as follows:

$$\begin{aligned}&(|0\rangle + |1\rangle)((a_k + 1)|1\rangle + (a_k + 1)|2\rangle + a_k|3\rangle)\\ &\quad\mapsto |0\rangle((a_k + 1)|1\rangle + (a_k + 1)|2\rangle + a_k|3\rangle)\\ &\qquad + |1\rangle((a_k + 1)|1\rangle + (a_k + 1)|3\rangle + a_k|2\rangle)\\ &\quad\mapsto (|0\rangle + |1\rangle)((a_k + 1)|1\rangle + (a_k + 1)|2\rangle + a_k|3\rangle)\\ &\qquad + (|0\rangle - |1\rangle)((a_k + 1)|1\rangle + a_k|2\rangle + (a_k + 1)|3\rangle)\\ &\quad= |0\rangle((2a_k + 2)|1\rangle + (2a_k + 1)|2\rangle + (2a_k + 1)|3\rangle) + |1\rangle(|2\rangle - |3\rangle).\end{aligned}$$

We then obtain the state $(2a_k + 2)|1\rangle + (2a_k + 1)|2\rangle + (2a_k + 1)|3\rangle$ if the protocol does not halt. From this state, it immediately follows that $a_{k+1} = 2a_k + 1$. Therefore, p_{k+1} has the value

$$\begin{aligned}p_{k+1} &= 1 - \frac{1^2 + (-1)^2}{(2a_k + 2)^2 + 2(2a_k + 1)^2 + 1^2 + (-1)^2}\\ &= 1 - \frac{2}{(a_{k+1} + 1)^2 + 2a_{k+1}^2 + 2}.\end{aligned}$$

Since $a_{k+1} = 2a_k + 1 = \frac{1}{3}(4^{(k+1)/2} - 1)$, we finally obtain $p_{k+1} = 1 - \frac{6}{4^{k+1}+8}$. We thus conclude, from the induction hypothesis for k, that the lemma holds for $k+1$. A similar analysis

verifies that the induction step also holds for any even number k. Therefore, the mathematical induction guarantees the correctness of the lemma. □

This completes the proof of the theorem. □

As a direct consequence of theorem 1, we conclude that SRS is one of the best choices among all Swap protocols solving the problem QSI_3.

4. Approximation of the permutation test by the circle test

This section compares the performances of the circle test and of the permutation test. First, we focus our attention on the circle test for QSI_n, where n is a prime number. For such a number n, we can show that the circle test has the same performance for QSI_n as the permutation test does. This indicates that the circle test is a best quantum test for any 'prime' input size n among all one-sided error quantum operations for QSI_n.

Proposition 4. *Let n be a prime number. The circle test for QSI_n achieves the soundness error probability of at most $1/n$.*

Proof. Let n be any prime number and let $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$ be any instance of the identity problem QSI_n. Lemma 1 implies that the circle test outputs EQUAL on the instance with the probability $p = \frac{1}{n}\sum_{k=0}^{n-1}\prod_{m=1}^{n}\left\langle\psi_m\middle|\psi_{\sigma_c^k(m)}\right\rangle$. If $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$ is a YES instance, then it is straightforward to show that $p = 1$. Next, we consider the case where $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$ is a NO instance. Now, we claim the following.

Lemma 4. *Let $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$ be any NO instance. For any number $k \in [n-1]$, there exists an index $m \in [n]$ such that $\left\langle\psi_m\middle|\psi_{\sigma_c^k(m)}\right\rangle = 0$.*

From this lemma, it follows that the probability p equals $\frac{1}{n}\prod_{m=1}^{n}\left\langle\psi_m\middle|\psi_{\sigma_c^0(m)}\right\rangle$. Therefore, the circle test outputs EQUAL on $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$ with probability $\frac{1}{n}\prod_{m=1}^{n}\left\langle\psi_m\middle|\psi_{\sigma_c^0(m)}\right\rangle$, which is clearly upper bounded by $1/n$.

To complete the proof of the proposition, we need to prove lemma 4. Let us assume, toward a contradiction, that the lemma fails. By the promise of QSI_n, there exists a number $k \in [n-1]$ such that, for any number $m \in [n]$, $|\psi_m\rangle = |\psi_{\sigma_c^k(m)}\rangle$. Since $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$ is a NO instance, there exist two indices μ and μ' for which $\langle\psi_\mu|\psi_{\mu'}\rangle = 0$. This yields the existence of a proper subset $I = \{\mu_1, \mu_2, \ldots\}$ of $[n]$ satisfying that $|\psi_\mu\rangle = |\psi_\nu\rangle$ for any pair $\mu, \nu \in I$, and $\langle\psi_\mu|\psi_\nu\rangle = 0$ for any $\mu \in I$ and $\nu \in [n]\backslash I$. Choose μ_1 in I. Since $|\psi_m\rangle = |\psi_{\sigma_c^k(m)}\rangle$ for any $m \in [n]$, we obtain $\left|\psi_{\mu_1}\right\rangle = \left|\psi_{\sigma_c^k(\mu_1)}\right\rangle = \left|\psi_{\sigma_c^{2k}(\mu_1)}\right\rangle = \cdots$. Let $S = \left\{\mu_1, \sigma_c^k(\mu_1), \sigma_c^{2k}(\mu_1), \ldots\right\}$. It follows from the definition of I that $S \subseteq I$. Since the set S is the $\mathbb{Z}_n$-orbit with respect to μ_1, its cardinality is a divisor of n. The 'prime' condition of n concludes that $[n] = S$. Since $S \subseteq I$, we have $I = [n]$, which contradicts our assumption that I is a proper subset of $[n]$. This completes the proof of the lemma and thus completes the proof of the proposition. □

For an arbitrary input size n, how good is the performance of the circle test for QSI_n, compared to the permutation test? Under the one-sided error requirement, as seen in section 2, the circle test, in general, cannot be optimal for QSI_n. Nevertheless, it is possible to give a simple and almost optimal protocol, called RCIR (randomized circle test), which uses the circle test only once after the classical processing of permuting n quantum states randomly.

Protocol RCIR

Input: n quantum states $(|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle) \in \mathcal{H}^{\otimes n}$

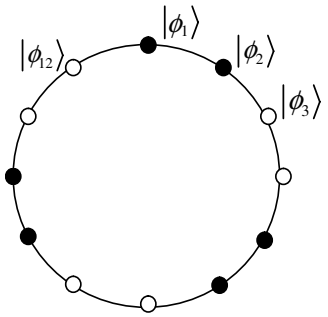

Figure 1. An example of cyclic alignment of all I_1 states with $n = 12$ and $|I_1| = 6$.

(i) Permute the input quantum states by a randomly chosen permutation $\tau \in S_n$. Let $(|\phi_1\rangle, \ldots, |\phi_n\rangle)$, where $|\phi_j\rangle = |\psi_{\tau(j)}\rangle$, be the resulting quantum states.
(ii) Apply the circle test to $(|\phi_1\rangle, \ldots, |\phi_n\rangle)$.

We show that the protocol RCIR is an 'asymptotically' optimal quantum operation for QSI_n up to a constant multiplicative factor of nearly $\pi^2/6$.

Theorem 2. *The protocol RCIR meets the one-sided error requirement and achieves the soundness error probability of at most* $\pi^2/6n + O(1/n^2) \leqslant 1.7/n + O(1/n^2)$.

Proof. With the same reasoning given in the proof of proposition 1, it suffices to analyze only NO instances $(|\psi_1\rangle, \ldots, |\psi_n\rangle)$ whose indices are divided into two sets I_1 and I_2 such that any two states with indices in I_1 (also, I_2) are identical and any pair of states, one of which has an index in I_1 and the other has an index in I_2, is orthogonal. In what follows, we call a state whose index is in I_1 (resp. I_2) an I_1 *state* (resp. I_2 *state*). Let I_1 and I_2 be such sets of indices of the permuted states $\{|\phi_1\rangle, \ldots, |\phi_n\rangle\}$ obtained at step (i) of the protocol RCIR. For convenience, let $I_1 = \{\mu_1, \mu_2, \ldots, \mu_r\}$ with $\mu_1 < \mu_2 < \cdots < \mu_r$ and $I_2 = [n]\backslash I_1$, where $r \in [n-1]$. Without the loss of generality, we assume that $|I_1| \leqslant |I_2|$; namely, $r \leqslant n/2$. Let us also assume that there are exactly s elements $k_1 = 0, k_2, \ldots, k_s \in \{0, 1, \ldots, n-1\}$ such that each number $k \in \{k_1, \ldots, k_s\}$ satisfies $\langle\phi_m|\phi_{\sigma_c^k(m)}\rangle = 1$ for any number $m \in [n]$. Lemma 1 concludes that the soundness error probability of the protocol equals s/n. The following lemma is easily proven.

Lemma 5. *Let* $K = \{k_1, k_2, \ldots, k_s\}$.
(i) For any $m \geqslant 1$*, if* $k' \in K$ *then so is* mk'.
(ii) If $k', k'' \in K$ *then so is* $\mathrm{GCD}(k', k'')$.

By lemma 5, the set $K = \{k_1, k_2, k_3, \ldots, k_s\}$ can be of the form $k_1 = 0, k_2 = k, k_3 = 2k, \ldots, k_s = (s-1)k$ for the divisor $k(= n/s)$ of n. For convenience, we call s and k the *repetition number* and the *cycle size*, respectively.

To help the reader, let us see an example. Figure 1 renders a cyclic alignment of all I_1 states with parameters $n = 12$ and $r = 6$, where the repetition number s is 3 and the cycle size k is 4. A black node (resp. white node) indicates an I_1 state (resp. I_2 state). Each cyclic alignment of I_1 states induces an I_1 *pattern*, which is a bit string $(b_1, \ldots, b_k)$ defined by $b_i = 1$ if $i \in I_1$ and 0 otherwise. In figure 1, this I_1 pattern is $(1, 1, 0, 0)$. By the definition of cycle size k, such an I_1 pattern uniquely characterizes a cyclic alignment of I_1 states as follows: for any $j \in \{0, 1, \ldots, s-1\}$ and $i \in [k]$, the index $jk + i \in [n]$ is in I_1 if $i \in I_1$, and in I_2 if

$i \in I_2$. Note that the Hamming weight of $(b_1, \ldots, b_k)$, which indicates the number of indices in $[k] \cap I_1$, is exactly $|I_1|/s = r/s$.

Now, we return to our proof. We wish to show that the soundness error probability for any fixed r is at most $\pi^2/6n + O(1/n^2)$. Let p_s be the probability that a cyclic alignment of I_1 states with repetition number s is chosen by the protocol RCIR. Note that, as far as $\mathrm{GCD}(n, r) = 1, s$ equals 1; hence, we have $p_1 = 1$. This implies that the soundness error probability equals $1/n$. Since a cyclic alignment of all I_1 states is randomly chosen, it follows that, for $s \geqslant 2$, $p_s \leqslant \frac{\binom{k}{r/s}}{\binom{n}{r}} = \frac{\binom{n/s}{r/s}}{\binom{n}{r}}$. Recall that any cyclic alignment of I_1 states with repetition number s produces the soundness error probability of s/n. Therefore, the total soundness error probability is at most

$$p_1 \cdot \frac{1}{n} + \sum_{s:s|n} \frac{\binom{n/s}{r/s}}{\binom{n}{r}} \cdot \frac{s}{n} \leqslant \frac{1}{n} + \sum_{s:s|n} \frac{\binom{n/s}{r/s}}{\binom{n}{r}} \cdot \frac{s}{n}. \tag{2}$$

To upper bound equation (2) further, we need the following technical lemma. Recall that s is a divisor of r. For convenience, let $q(n, r, s) = \frac{\binom{n/s}{r/s}}{\binom{n}{r}} \cdot \frac{s}{n}$.

Lemma 6. *The value $q(n, r, s)$ is at most $\frac{1}{ns^2}$ if $s \leqslant r/3$, $\frac{6}{(n-1)(n-2)(n-3)}$ if $s = r/2$ and $\frac{2}{n(n-1)}$ if $s = r$.*

We continue our argument. Lemma 6 helps us upper bound the right-hand expression of equation (2) as

$$\begin{aligned}
&\frac{1}{n} + \sum_{s:s|n} \left(\frac{1}{ns^2} \right) + O(1/n^2) \\
&\qquad \leqslant \frac{1}{n} + \sum_{s=2}^{\infty} \left(\frac{1}{ns^2} \right) + O(1/n^2) = \frac{1}{n} + \frac{\pi^2/6 - 1}{n} + O(1/n^2).
\end{aligned}$$

The last expression is clearly equal to $\pi^2/6n + O(1/n^2)$, as requested.

What remains is to prove lemma 6. Consider the first case $s = r$. In this case, we have $q(n, r, s) = \frac{\binom{n/s}{1}}{\binom{n}{s}} \cdot \frac{s}{n} = \frac{1}{\binom{n}{s}}$, which is bounded from above by $\frac{1}{\binom{n}{2}} = \frac{2}{n(n-1)}$ because $s \geqslant 2$. Let us consider the second case $s = r/2$. The expression $q(n, r, s)$ is further calculated as

$$q(n, r, s) = \frac{\binom{n/s}{2}}{\binom{n}{2s}} \cdot \frac{s}{n} = \frac{2s(2s-1)\cdots 1}{n(n-1)\cdots(n-2s+1)} \cdot \frac{n/s - 1}{2}. \tag{3}$$

Noting that $2s \geqslant 4$, $2s = r \leqslant n/2$ and $n - 2s + 1 \geqslant n/2 + 1$, it follows from equation (3) that $q(n, r, s)$ is at most

$$\begin{aligned}
&\frac{1 \cdot 2 \cdot 3 \cdot 4 \cdots 2s}{n(n-1)(n-2)(n-3)\cdots(n-2s+1)} \cdot \frac{n}{2s} \\
&\qquad \leqslant \frac{1 \cdot 2 \cdot 3 \cdot 4}{n(n-1)(n-2)(n-3)} \cdot \frac{n}{4} = \frac{6}{(n-1)(n-2)(n-3)}.
\end{aligned}$$

In the final case $s \leqslant r/3$, the expression $q(n, r, s)$ equals

$$\begin{aligned}
q(n, r, s) &= \frac{\binom{n/s}{r/s}}{\binom{n}{r}} \cdot \frac{s}{n} = \frac{\frac{(n/s)(n/s-1)\cdots(n/s-r/s+1)}{(r/s)(r/s-1)\cdots 1}}{\frac{n(n-1)\cdots(n-r+1)}{r(r-1)\cdots 1}} \cdot \frac{s}{n} \\
&= \frac{s \cdot \frac{n}{s} \cdots \left(\frac{n}{s} - \frac{r}{s} + 1\right) \cdot r \cdots 1}{n \cdot n \cdots (n-r+1)\,(\frac{r}{s} \cdots 1)},
\end{aligned}$$

which is clearly at most

$$\frac{s}{n}\left(\frac{n/s}{n}\right)^{r/s}\frac{r\cdots\left(\frac{r}{s}+1\right)}{\left(n-\frac{r}{s}\right)\cdots(n-r+1)}.$$

This expression is further upper bounded by $\frac{s}{n}\left(\frac{1}{s}\right)^{r/s}$, since $2\leqslant s\leqslant r\leqslant n/2$ implies $\frac{r}{n-\frac{r}{s}}\leqslant 2/3$. From our assumption $s\leqslant r/3$, it therefore follows that

$$q(n,r,s)\leqslant\frac{s}{n}\left(\frac{1}{s}\right)^{r/s}\leqslant\frac{s}{n}\left(\frac{1}{s}\right)^{3}=\frac{1}{ns^2}.$$

This ends the proof of the lemma and thus the proof of theorem 2. □

5. Closing discussion

The swap test has been widely used in the literature to test the identity of two quantum states. In this paper, we have studied two additional tests, the permutation test and the circle test, which generalize the swap test. We have analyzed the performances of these two tests for the quantum-state identity problem, QSI_n, under the one-sided error requirement. Throughout this paper, we have restricted our attention to the identity problem's *promise* (in the definition of QSI_n) and also the *one-sided error requirement*. These restrictions make our analysis easier; nevertheless, the restrictions can be relaxed. We briefly discuss how our result can be applied to less-constrained situations.

The promise of our identity problem QSI_n demands that any pair of quantum states is identical or orthogonal. By relaxing the latter orthogonality, we can consider the following weak form of an identity problem, denoted $\mathrm{QSI}_n^{\varepsilon}$, in which we want to determine either (a) all n quantum states are identical or (b) there are two states whose inner product is less than or equal to ε, provided that either (a) or (b) holds. This problem $\mathrm{QSI}_n^{\varepsilon}$ was dealt with in a fingerprinting protocol in [7]. Our results in this paper still provide a good proximity of the three tests to the problem $\mathrm{QSI}_n^{\varepsilon}$ since QSI_n coincides with $\mathrm{QSI}_n^{\varepsilon}$ when $\varepsilon=0$.

Our one-sided error requirement requests that the completeness error probability should be 0. This requirement naturally occurs in the literature regarding the swap test (e.g., [6, 7, 18]). As a natural relaxation of this requirement, when we allow non-zero completeness error probability, we obtain the *two-sided error requirement*. Even with this relaxed requirement, we can claim that the swap test is 'optimal' in the sense that the swap test achieves the largest gap between the probabilities that EQUAL is outputted on YES instances and on NO instances. This claim can be shown by a *trace-norm distance argument* as follows.

Consider the two YES instances $(|0\rangle,|0\rangle)$ and $(|1\rangle,|1\rangle)$, where each input is a single qubit. For simplicity, let us denote them by $|00\rangle$ and $|11\rangle$, respectively. Similarly, consider two NO instances $|+-\rangle$ and $|-+\rangle$, where $|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$ and $|-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$. Now, let $\boldsymbol{\rho}_y=\frac{1}{2}(|00\rangle\langle 00|+|11\rangle\langle 11|)$ and $\boldsymbol{\rho}_n=\frac{1}{2}(|+-\rangle\langle +-|+|-+\rangle\langle -+|)$. Write p_c and p_s for the completeness and soundness error probabilities, respectively, of the test. There is a POVM M such that the l_1-norm gap GAP between two probability distributions obtained by M on $\boldsymbol{\rho}_y$ and $\boldsymbol{\rho}_n$ is at least $|(1-p_c)-p_s|+|(1-p_s)-p_c|=2-2p_c-2p_s$. In contrast, since the trace-norm distance between $\boldsymbol{\rho}_y$ and $\boldsymbol{\rho}_n$ is $1/2$, the value GAP should be at most 1 [1] (see also [15]). This yields the inequality $p_c+p_s\geqslant 1/2$. Note that the swap test achieves the equality $p_c+p_s=1/2$. Therefore, the swap test is optimal even in the two-sided error requirement.

With a similar argument for the circle test for QSI_3, we can prove that the circle test is also 'optimal' with two-sided error probability. In contrast, the optimality of the permutation

test under the two-sided error requirement is currently open. We expect the optimality of the permutation test; however, it is likely that the trace-norm distance argument for the permutation test is insufficient to prove the optimality under the two-sided error requirement.

Another interesting open question in line of our work is to seek an efficient approximation of the permutation test for QSI_n by use of a certain Swap protocol that runs the swap test $O(n)$ times. Such a Swap protocol provides an ideal construction of a quantum circuit that implements the permutation test since it is much more concise than the direct construction of the permutation test based on the decomposition of the Fourier transform $F_{n!}$ over $n!$ elements.

Acknowledgments

We are grateful to Masahiro Hotta and Masanao Ozawa for sending us their unpublished manuscript that became a basis of our proof of proposition 2. HN was supported in part by Scientific Research Grant, Ministry of Japan, 19700011. TY was supported in part by grants from the Mazda Foundation and from the Grant-in-Aid for Scientific Research of Japan.

References

[1] Aharonov D, Kitaev A and Nisan N 1998 *Proc. 30th ACM Symp. on Theory of Computing* (New York: ACM) p20
[2] Ambainis A 1996 *Algorithmica* **16** 298
[3] Ambainis A and Shi Y 2004 *Quantum Inf. Comput.* **4** 146
[4] Babai L and Kimmel P G 1997 *Proc. 12th IEEE Conf. on Computational Complexity* (Los Alamitos, CA: IEEE) p239
[5] Barenco A, Berthiaume A, Deutsch D, Ekert A, Jozsa R and Macchiavello C 1997 *SIAM J. Comput.* **26** 1541
[6] de Beaudrap J N 2004 *Phys. Rev.* A **69** 022307
[7] Buhrman H, Cleve R, Watrous J and de Wolf R 2001 *Phys. Rev. Lett.* **87** 167902
[8] Du J, Zou P, Peng X, Oi D K L, Kwek L C, Oh C H and Ekert A 2006 *Phys. Rev.* A **74** 042319
[9] Ekert A K, Alves C M, Oi D K L, Horodecki M, Horodecki P and Kwek L C 2002 *Phys. Rev. Lett.* **88** 217901
[10] Friedl K, Ivanyos G, Magniez F, Santha M and Sen P 2003 *Proc. 35th ACM Symp. on Theory of Computing* (New York: ACM) p1
[11] Gavinsky D, Kempe J and de Wolf R 2006 *Proc. 21st IEEE Conf. on Computational Complexity* (Los Alamitos, CA: IEEE) p288
[12] Horn R T, Babichev S A, Marzlin K P, Lvovsky A I and Sanders B C 2005 *Phys. Rev. Lett.* **95** 150502
[13] Hotta M and Ozawa M 2007 private communication
[14] Kobayashi H, Matsumoto K and Yamakami T 2001 arXiv:quant-ph/0110006
[15] Kobayashi H, Matsumoto K and Yamakami T 2003 *Proc. 14th Int. Symp. on Algorithms and Computation (Lecture Notes in Computer Science* vol 2906*)* (New York: Springer) p189
[16] Kushilevitz E and Nisan N 1997 *Communication Complexity* (Cambridge: Cambridge University Press)
[17] Nisan N and Szegedy M 1996 *Proc. 28th ACM Symp. on Theory of Computing* (New York: ACM) p561
[18] Scott A J, Walgate J and Sanders B C 2007 *Quantum Inf. Comput.* **7** 243
[19] Wang B and Duan L M 2007 *Phys. Rev.* A **75** 050304
[20] Yao A C-C 2003 *Proc. 35th ACM Symp. on Theory of Computing* (New York: ACM) p77