On the hardness of distinguishing mixed-state quantum computations

Bill Rosgen
Department of Computing Science
University of Alberta
Edmonton, Alberta, Canada

John Watrous
Department of Computer Science
University of Calgary
Calgary, Alberta, Canada

July 22, 2004

Abstract

This paper considers the following problem. Two mixed-state quantum circuits Q_0 and Q_1 are given, and the goal is to determine which of two possibilities holds: (i) Q_0 and Q_1 act nearly identically on all possible quantum state inputs, or (ii) there exists some input state ρ that Q_0 and Q_1 transform into almost perfectly distinguishable outputs. This problem may be viewed as an abstraction of the following problem: given two physical processes described by sequences of local interactions, are the processes effectively the same or are they different? We prove that this problem is a complete promise problem for the class QIP of problems having quantum interactive proof systems, and is therefore PSPACE-hard. This is in sharp contrast to the fact that the analogous problem for classical (probabilistic) circuits is in AM, and for unitary quantum circuits is in QMA.

1 Introduction

Randomness is a fundamental concept in complexity theory and cryptography that is sometimes under-emphasized in the study quantum computing. For example, the most typically used quantum computational model is the unitary quantum circuit model restricted to pure quantum states; and although this model can simulate randomized computations, in some sense there is really no randomness at all in a unitary circuit computation. Indeed, in the framework of quantum information, pure states and unitary computations may be viewed as being analogous to definite logical states and deterministic computations, with more general types of states and non-unitary operations being possible. In particular, quantum states may be mixed as opposed to pure, arising for example when a probability distribution over pure states is considered, and operations such as measurements and noise may be non-unitary but physically possible.

A variant of the quantum circuit model allowing mixed states and non-unitary operations was introduced by Aharonov, Kitaev, and Nisan [1]. They showed that this more general model is in fact equivalent in power to the unitary quantum circuit model. The principle behind this equivalence is the fact that arbitrary physically realizable quantum operations, including irreversible deterministic computations, random coin-flips, measurements, noise, and so on, can be described by unitary operations acting on larger systems.

However, while the two quantum circuit models are equivalent in computational power, it is a misconception that they are identical, and that there is no loss of generality in restricting ones

attention to fully reversible quantum computational models. Indeed, in some restricted settings the equivalence of the models breaks down. For instance, it is not known if unitary quantum computations can simulate classical randomized computations in bounded space. For quantum finite automata the situation is much more alarming. Here, unitarity imposes a restriction that provably weakens the model over the usual deterministic (but irreversible) model; and while a definition based on mixed-states gives a natural and more satisfying model that generalizes classical (deterministic and probabilistic) finite automata, the weaker and less motivated unitary model has received far more attention.

In this paper we describe a different sense in which the mixed-state quantum circuit model differs significantly from the unitary quantum circuit model. Our interest is with the computational complexity of problems about quantum circuits, and in particular our focus is on the following problem. Assume two mixed-state quantum circuits Q_0 and Q_1, which agree on the number of input qubits and on the number of output qubits, are given. For any input state ρ, let $Q_0(\rho)$ and $Q_1(\rho)$ denote the mixed states obtained by running Q_0 and Q_1, respectively, on input ρ. It is promised that either (i) $Q_0(\rho)$ and $Q_1(\rho)$ are almost identical for all states ρ, or (ii) there exists an input state ρ for which $Q_0(\rho)$ and $Q_1(\rho)$ are very different, and the goal is to determine which of these possibilities holds. (A natural way to formalize the notions of $Q_0(\rho)$ and $Q_1(\rho)$ being "almost identical" and "very different" is discussed in the next section.) This problem is phrased as a promise problem because it would be artificially difficult if it were necessary to distinguish cases when the distances between $Q_0(\rho)$ and $Q_1(\rho)$ are close to some threshold. Even with such a promise, however, we show that this problem is PSPACE-hard. More specifically, we show that this problem is a complete promise problem for the class QIP of problems possessing quantum interactive proof systems. In contrast, the classical analogue of this problem, to distinguish between two probabilistic boolean circuits, is easily shown to be contained in the class AM, while the variant of the problem where Q_0 and Q_1 are unitary quantum circuits is contained in QMA [4]. According to our current state of knowledge this represents a significant difference in hardness, given that AM = PSPACE and QMA = PSPACE both seem unlikely.

It is natural to attribute the apparent difference in hardness of the above problems to the presence of both randomness and quantum computation in the mixed-state quantum circuits variant of the problem—removing either randomness (leaving a unitary model) or quantum computation (leaving a classical probabilistic model) results in a reduction in complexity. This example underscores the distinction between unitary and mixed-state quantum models.

The above problem is also interesting for the much different reason that it abstracts the following natural physical problem: given two physical processes, are they effectively the same or are they different? Under the assumption that the physical processes in question are described in terms of local interactions among particles that can implement qubits and simulate mixed-state quantum computations, it follows that even to solve this problem approximately is PSPACE-hard.

Finally, we are hopeful that the completeness of the problem discussed in this paper may lead to new results on the structural properties of the class QIP. For example, it is currently known that PSPACE $\subseteq$ QIP $\subseteq$ EXP [7], but no strong evidence has yet been provided that suggests either containment should be an equality or a proper containment.

The rest of this paper is organized as follows. In Section 2 we discuss relevant background on mixed-state quantum circuits and other aspects of quantum information, and in Section 3 we state and discuss the definition of the computational problem of distinguishing mixed-state quantum circuits being considered. The main hardness result is proved in Section 4. We conclude with

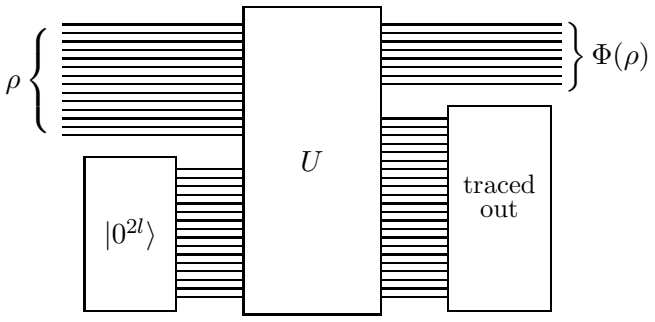


Figure 1: The unitary operation U simulates the admissible operation Φ.

Section 5, which mentions some open questions relating to the topic of the paper.

2 Preliminaries

2.1 Admissible operations and mixed-state quantum circuits

We begin by discussing admissible quantum operations together with the mixed-state quantum circuit model of Aharonov, Kitaev, and Nisan [1].

For positive integers k and l, consider the set of operations mapping k-qubit states to l-qubit states that correspond to physically possible operations (in an idealized sense). Quantum information theory gives a simple description of this set of operations, sometimes called the set of *admissible operations*. Specifically, an operation Φ from k qubits to l qubits is admissible if its action on density matrices is linear, trace-preserving, and completely positive. This means that if ρ is a density matrix on $k+m$ qubits for some arbitrary value of m, and Φ is performed on the first k qubits of ρ, then the result is a valid density matrix on $l+m$ qubits. In symbols, $(\Phi \otimes I_m)(\rho)$ is a density matrix, where I_m denotes the identity mapping on m qubit states. Examples of admissible operations include unitary operations (which require that $k = l$), irreversible classical computations from k bits to l bits, and the operations of adding qubits in some specified state and discarding qubits.

A quantum gate of type (k, l) is a gate that takes k qubits as input and outputs l qubits, and corresponds to some admissible operation. Mixed-state quantum circuits are circuits that consist of some finite collection of such gates along with acyclic input/output relations among these gates. A given mixed-state quantum circuit will have some number n of input qubits and some number m of output qubits. Using the same terminology for circuits as for gates, we may say that a circuit is of type (n, m) when this is the case, and more generally we say that an operation is of type (n, m) if it maps n qubit states to m qubit states. Thus, a circuit Q of type (n, m) specifies some admissible operation of type (n, m), and when convenient we also let Q denote this admissible operation.

A necessary and sufficient condition for an operation Φ of type (k, l) to be admissible is that there exists a unitary operation U acting on $k + 2l$ qubits such that the following holds. If the first k qubits are set to state ρ and the remaining $2l$ qubits are initialized to the $|0\rangle$ state, the operation U is applied, and finally the last $k + l$ qubits are discarded (or *traced out*), the resulting state on the remaining l qubits is $\Phi(\rho)$. This situation is illustrated in Figure 1. This fact is generally attributed to Choi [3], and a proof may be found in Kitaev, Shen, and Vyalyi [6]. This process

may be applied to each gate in a given circuit Q, resulting in a unitary circuit P that simulates Q in a sense similar to the situation pictured in Figure 1. Under the assumption that each gate is of constant size, the number of additional qubits required is linear in the number of gates of Q.

For the remainder of this paper it will be assumed that all mixed-state quantum circuits under consideration are composed of gates from some reasonable finite set. In order to avoid a discussion of what exactly is meant by "reasonable", let us for simplicity say that this means that if the gates are expressed as linear mappings, then these mappings can be written as matrices consisting of efficiently approximable numbers. The point is to disallow difficult to compute information from being somehow incorporated into the action of gates acting on a finite number of qubits. Assuming that such a finite set of quantum gates has been fixed, a quantum circuit may easily be described classically. It will not be necessary to discuss a particular method of encoding quantum circuits beyond stating the assumption that the encoding is efficient, reasonable, and disallows compact descriptions of large circuits. Given such a classical description of a circuit Q, it is possible to compute in polynomial time a description of a unitary quantum circuit P that simulates Q in the sense described above.

A few additional requirements on the set of gates of which mixed-state quantum circuits may be composed is required for the hardness results proved in this paper. The requirements are that (i) the set of gates is universal for quantum computation, meaning that any constant-size unitary operation can be efficiently approximated by circuits composed of these gates, (ii) the gates include a gate of type $(0, 1)$ that introduces a qubit initialized to the state $|0\rangle$, and (iii) the gates include the unique gate of type $(1, 0)$ that corresponds to discarding a qubit.

2.2 Distance measures for quantum states and admissible operations

The problem of distinguishing quantum circuits on which this paper focuses requires a notion of distance between admissible operations. The notion we will use, and which we claim is the most natural with respect to the problem, is given by a norm known as the diamond norm.

Before discussing the diamond norm, we need to mention the trace norm, which induces a distance measure between density matrices that is analogous to the distance between probability distributions induced by the 1-norm. For a given square matrix X, the trace norm of X, denoted $\|X\|_{\mathrm{tr}}$, is defined to be the sum of the singular values of X. In case X is Hermitian, $\|X\|_{\mathrm{tr}}$ is also equal to the sum of the absolute value of the eigenvalues of X. Equivalent expressions for the trace norm (for general X) include $\|X\|_{\mathrm{tr}} = \mathrm{tr}\sqrt{X^\dagger X}$ and $\|X\|_{\mathrm{tr}} = \max\{|\,\mathrm{tr}(XU)|\}$, where the maximum is over all unitary U having the same dimensions as X.

The quantity $\|\rho_0 - \rho_1\|_{\mathrm{tr}}$ for given density matrices ρ_0 and ρ_1 has the following operational interpretation. Given any binary-valued measurement, let us say that the measurement is correct in the event that, on input ρ_b, the outcome of the measurement is b, and is incorrect when the outcome is $\neg b$. Assuming ρ_0 and ρ_1 are each given with probability $1/2$, the quantity $\|\rho_0 - \rho_1\|_{\mathrm{tr}}/2$ represents the maximum over all possible measurements that the measurement is correct minus the probability the measurement is incorrect. Thus, $\|\rho_0 - \rho_1\|_{\mathrm{tr}} = 2$ implies that ρ_0 and ρ_1 are perfectly distinguishable by some measurement, while $\|\rho_0 - \rho_1\|_{\mathrm{tr}} = 1$, for example, implies that the maximum probability of correctness for any measurement given ρ_0 and ρ_1 uniformly is $3/4$. Obviously $\|\rho_0 - \rho_1\|_{\mathrm{tr}} = 0$ implies $\rho_0 = \rho_1$, and so no measurement can do better than random guessing in this case.

The trace norm may be extended to differences in admissible operations in the following standard

way: if Φ and Ψ are admissible, then

$$\|\Phi - \Psi\|_{\mathrm{tr}} \stackrel{\mathrm{def}}{=} \max\{\|\Phi(X) - \Psi(X)\|_{\mathrm{tr}} \,:\, \|X\|_{\mathrm{tr}} = 1\}.$$

Unfortunately this norm has some unusual properties that make it unsuitable for describing distances between admissible operations. One problem is that the maximum may not be achieved when X is a density matrix, and another is that the value of the norm may change if Φ and Ψ are tensored with the identity operation on some number of qubits.

With this in mind, one defines the *diamond norm* of the difference $\Phi - \Psi$, for Φ and Ψ admissible operations of type (n, m), as follows:

$$\|\Phi - \Psi\|_{\diamond} \stackrel{\mathrm{def}}{=} \|\Phi \otimes I_n - \Psi \otimes I_n\|_{\mathrm{tr}} = \max\{\|(\Phi \otimes I_n)(X) - (\Psi \otimes I_n)(X)\|_{\mathrm{tr}} \,:\, \|X\|_{\mathrm{tr}} = 1\}.$$

Here, I_n denotes the identity operation on states of n qubits and the maximum is over all $2^{2n} \times 2^{2n}$ matrices X (with $\|X\|_{\mathrm{tr}} = 1$). The diamond norm was first defined and studied by Kitaev [5]. Further information on it may be found in Refs. [6] and [1]. The maximum in the above definition always occurs for X a density matrix (and therefore for $X = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle$ by a simple convexity argument), and the quantity does not grow if the identity is taken on more than n qubits. The second fact was already known but the first is new. A more technical discussion of these facts can be found below in Section 2.4.

The diamond norm gives a similar characterization of the distinguishability of admissible operations that the trace norm gives for states. Specifically, the diamond norm of the difference between two admissible operations characterizes the probability that the output of these two operations can be distinguished, given that an input to the two operations is chosen that maximizes the distinguishability of the outputs. It is important to note that this includes the possibility that the input is a state of a larger system on which the operations act on only part.

Another useful way to measure the similarity between density matrices is given by the fidelity. Specifically, the fidelity between density matrices ρ and ξ is defined as:

$$F(\rho, \xi) \stackrel{\mathrm{def}}{=} \mathrm{tr} \sqrt{\sqrt{\rho}\, \xi \sqrt{\rho}}.$$

The fidelity is a measure of similarity that is related to but different from the trace norm. Generally speaking, when two states are close together they have large fidelity and small trace norm, and when far apart have small fidelity and large trace norm. At first glance the fidelity appears to be an unusual and possibly difficult to use quantity, but in actuality it is often easier to use than the trace norm. (For instance, it is multiplicative with respect to tensor products.) For all density matrices ρ and ξ, it holds that

$$1 - \frac{1}{2}\|\rho - \xi\|_{\mathrm{tr}} \leq F(\rho, \xi) \leq \sqrt{1 - \frac{1}{4}\|\rho - \xi\|_{\mathrm{tr}}^2}.$$

2.3 Quantum interactive proof systems

Quantum interactive proof systems are interactive proof systems in which the prover and verifier may exchange and process quantum information [7, 12]. The class of problems having quantum interactive proof systems is denoted QIP and is known to satisfy PSPACE $\subseteq$ QIP $\subseteq$ EXP.

The main result of this paper, stated more formally in the next section, establishes that the problem of distinguishing mixed-state quantum circuits is QIP-complete. This will be proved by

first noting that a fairly straightforward quantum interactive proof system exists for the problem, and second by reducing a problem that was already known to be complete for QIP to the circuit distinguishing problem. In fact, the problem we will use for the reduction was only implicitly proved to be complete for QIP in Ref. [7], but all of the pieces needed to establish this fact are present in that paper. The problem is as follows.

Problem (Close Images). This problem is parameterized by constants $a, b \in [0, 1]$ with $b < a$. For such constants, define the promise problem $\mathsf{CI}_{a,b}$ as follows:

Input: Mixed state quantum circuits (Q_0, Q_1) of type (n, m).

Yes: There exist n qubit states ρ_0 and ρ_1 such that $F(Q_0(\rho_0), Q_1(\rho_1)) \geq a$.

No: For all n qubit states ρ_0 and ρ_1, $F(Q_0(\rho_0), Q_1(\rho_1)) \leq b$.

The "yes" instances of the problem are therefore circuits whose images are close with respect to fidelity, while the "no" instances are circuits whose images are far apart. Completeness of this promise problem for QIP holds for any constants a, b with $0 < b < a \leq 1$.

2.4 More notation and technical facts concerning distance measures

The proofs in the sections that follow will require more precise notation than has been necessary thus far, as well as a few key facts about the distance measures discussed previously. It is convenient to include these things at this point, but the reader uninterested in the technical details of the proofs may safely skip the remainder of this section. For the most part our notation is standard and consistent with Kitaev, Shen, and Vyalyi [6], which may be consulted for further background information.

Hilbert spaces will be denoted by scripted letters, such as $\mathcal{H}$, $\mathcal{K}$, etc. It will always be the case in this paper that Hilbert spaces have a standard orthonormal basis that is in correspondence with binary strings of a given length. We write, for instance, $\mathcal{H} = \mathcal{H}(\Sigma^n)$ when the standard basis of $\mathcal{H}$ is in correspondence with Σ^n, for $\Sigma = \{0, 1\}$. For given Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, $\mathbf{L}(\mathcal{H}, \mathcal{K})$ denotes the set of linear operators from $\mathcal{H}$ to $\mathcal{K}$, and $\mathbf{L}(\mathcal{H})$ is shorthand for $\mathbf{L}(\mathcal{H}, \mathcal{H})$. The set $\mathbf{D}(\mathcal{H})$ consists of all positive semidefinite operators on $\mathcal{H}$ having unit trace (i.e., all density matrices over $\mathcal{H}$). The set $\mathbf{U}(\mathcal{H}, \mathcal{K})$ consists of all linear operators from $\mathcal{H}$ to $\mathcal{K}$ that preserve the Euclidean norm. Equivalently, $U^\dagger U = I_{\mathcal{H}}$ (the identity operator on $\mathcal{H}$). In case $\dim(\mathcal{H}) = \dim(\mathcal{K})$, $\mathbf{U}(\mathcal{H}, \mathcal{K})$ consists of those operators that are unitary, and we write $\mathbf{U}(\mathcal{H})$ as a shorthand for $\mathbf{U}(\mathcal{H}, \mathcal{H})$. The set $\mathbf{T}(\mathcal{H}, \mathcal{K})$ consists of the linear operators from $\mathbf{L}(\mathcal{H})$ to $\mathbf{L}(\mathcal{K})$. Admissible operations are examples of such mappings, which in general will be called transformations.

The partial trace is the admissible operation obtained by taking the tensor product of the trace with the identity, and corresponds to discarding part of a quantum system. One writes $\mathrm{tr}_{\mathcal{H}}$ to denote this operation when the trace is on the space $\mathcal{H}$. If $X \in \mathbf{L}(\mathcal{H})$ is positive semidefinite and $|\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ satisfies $\mathrm{tr}_{\mathcal{K}} |\psi\rangle\langle\psi| = X$, then $|\psi\rangle$ is said to be a *purification* of X. Such a purification always exists provided $\dim(\mathcal{K}) \geq \mathrm{rank}(X)$. The fidelity has an alternate characterization in terms of purifications that is important to a proof appearing later.

Lemma 2.1. *Let $\rho, \xi \in \mathbf{D}(\mathcal{H})$. Then for arbitrary purifications $|\psi\rangle, |\phi\rangle \in \mathcal{H} \otimes \mathcal{K}$ of ρ and ξ, respectively, we have $\|\mathrm{tr}_{\mathcal{H}} |\psi\rangle\langle\phi|\|_{\mathrm{tr}} = F(\rho, \xi)$.*

Proof. Using one of the alternate characterizations of the trace-norm together with Uhlmann's Theorem and a well known fact about the unitary equivalence of purifications of a given state, we

have

$$\begin{aligned}\left\| \operatorname{tr}_{\mathcal{H}} |\psi\rangle\langle\phi| \right\|_{\mathrm{tr}} &= \max_{U \in \mathbf{U}(\mathcal{K})} \left| \operatorname{tr} \left(\operatorname{tr}_{\mathcal{H}} |\psi\rangle\langle\phi| \right) U \right| = \max_{U \in \mathbf{U}(\mathcal{K})} \left| \operatorname{tr} |\psi\rangle\langle\phi| (I_{\mathcal{H}} \otimes U) \right| \\ &= \max_{U \in \mathbf{U}(\mathcal{K})} \left| \langle\phi| (I_{\mathcal{H}} \otimes U) |\psi\rangle \right| = F(\rho, \xi)\end{aligned}$$

as claimed. □

We now give a more general definition for the diamond norm, which is consistent with the definition given previously for differences of admissible transformations.

Definition 2.2. If $\Phi \in \mathbf{T}(\mathcal{H}, \mathcal{K})$ then

$$\left\| \Phi \right\|_{\diamond} \stackrel{\text{def}}{=} \left\| \Phi \otimes I_{\mathbf{L}(\mathcal{G})} \right\|_{\mathrm{tr}}$$

where $\mathcal{G}$ is a Hilbert space with $\dim(\mathcal{G}) = \dim(\mathcal{H})$.

It is known (see Ref. [6]) that increasing the dimension of $\mathcal{G}$ gives no increase in $\left\| \Phi \otimes I_{\mathbf{L}(\mathcal{G})} \right\|_{\mathrm{tr}}$.

Theorem 2.3 (Kitaev). *Let $\Phi \in \mathbf{T}(\mathcal{H}, \mathcal{K})$, and let $\mathcal{F}$ be a space of arbitrary finite dimension. Then*

$$\left\| \Phi \otimes I_{\mathbf{L}(\mathcal{F})} \right\|_{\mathrm{tr}} \leq \left\| \Phi \right\|_{\diamond}.$$

The following fact shows that the maximum in Definition 2.2 occurs on a rank-one projection provided Φ is the difference of two completely positive transformations. In particular this holds when Φ is the difference of two admissible operations.

Lemma 2.4. *Let $\Phi \in \mathbf{T}(\mathcal{H}, \mathcal{K})$ satisfy $\Phi = \Phi_0 - \Phi_1$ for Φ_0 and Φ_1 completely positive. Then there exists a Hilbert space $\mathcal{F}$ and a unit vector $|\psi\rangle \in \mathcal{H} \otimes \mathcal{F}$ such that*

$$\left\| \Phi \right\|_{\diamond} = \left\| (\Phi \otimes I_{\mathbf{L}(\mathcal{F})})(|\psi\rangle\langle\psi|) \right\|_{\mathrm{tr}}.$$

Proof. Let $\mathcal{G}$ be a Hilbert space with $\dim \mathcal{G} = \dim \mathcal{H}$. Then

$$\left\| \Phi \right\|_{\diamond} = \left\| \Phi \otimes I_{\mathbf{L}(\mathcal{G})} \right\|_{\mathrm{tr}} = \max\{ \left\| (\Phi \otimes I_{\mathbf{L}(\mathcal{G})})(X) \right\|_{\mathrm{tr}} : \left\| X \right\|_{\mathrm{tr}} = 1 \}.$$

Let $X \in \mathbf{L}(\mathcal{H} \otimes \mathcal{F})$ satisfy this maximum, let $\mathcal{A} = \mathcal{A}(\Sigma)$ be a Hilbert space corresponding to a single qubit, and let $Y \in \mathbf{L}(\mathcal{H} \otimes \mathcal{F} \otimes \mathcal{A})$ be defined as

$$Y = \frac{1}{2} X \otimes |0\rangle\langle 1| + \frac{1}{2} X^{\dagger} \otimes |1\rangle\langle 0|.$$

We have $\left\| Y \right\|_{\mathrm{tr}} = \left\| X \right\|_{\mathrm{tr}} = 1$ and $Y = Y^{\dagger}$.

The condition that $\Phi = \Phi_0 - \Phi_1$ for Φ_0 and Φ_1 completely positive implies $\Phi(X)^{\dagger} = \Phi(X^{\dagger})$ for every $X \in \mathbf{L}(\mathcal{H})$. (In fact, the two conditions are equivalent.) Defining $\mathcal{F} = \mathcal{G} \otimes \mathcal{A}$, we therefore have that

$$\begin{aligned}\left\| (\Phi \otimes I_{\mathbf{L}(\mathcal{F})})(Y) \right\|_{\mathrm{tr}} &= \frac{1}{2} \left\| (\Phi \otimes I_{\mathbf{L}(\mathcal{G})})(X) \otimes |0\rangle\langle 1| + (\Phi \otimes I_{\mathbf{L}(\mathcal{G})})(X^{\dagger}) \otimes |1\rangle\langle 0| \right\|_{\mathrm{tr}} \\ &= \frac{1}{2} \left\| (\Phi \otimes I_{\mathbf{L}(\mathcal{G})})(X) \right\|_{\mathrm{tr}} + \frac{1}{2} \left\| (\Phi \otimes I_{\mathbf{L}(\mathcal{G})})(X^{\dagger}) \right\|_{\mathrm{tr}} \\ &= \frac{1}{2} \left\| (\Phi \otimes I_{\mathbf{L}(\mathcal{G})})(X) \right\|_{\mathrm{tr}} + \frac{1}{2} \left\| \left((\Phi \otimes I_{\mathbf{L}(\mathcal{G})})(X) \right)^{\dagger} \right\|_{\mathrm{tr}} \\ &= \left\| (\Phi \otimes I_{\mathbf{L}(\mathcal{G})})(X) \right\|_{\mathrm{tr}} \\ &= \left\| \Phi \right\|_{\diamond}.\end{aligned}$$

As Y is Hermitian, we may write

$$Y = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|,$$

where $\{|\psi_i\rangle\}$ is an orthonormal set of eigenvectors of Y with real eigenvalues $\{\lambda_i\}$. As $\|Y\|_{\mathrm{tr}} = 1$, we have $\sum_i |\lambda_i| = 1$. Now,

$$\left\|(\Phi \otimes I_{\mathbf{L}(\mathcal{F})})(Y)\right\|_{\mathrm{tr}} \leq \sum_i |\lambda_i| \left\|(\Phi \otimes I_{\mathbf{L}(\mathcal{F})})(|\psi_i\rangle\langle\psi_i|)\right\|_{\mathrm{tr}},$$

and because $\sum_i |\lambda_i| = 1$ we have

$$\left\|(\Phi \otimes I_{\mathbf{L}(\mathcal{F})})(|\psi_i\rangle\langle\psi_i|)\right\|_{\mathrm{tr}} \geq \|\Phi\|_\diamond$$

for some i. Let $|\psi\rangle = |\psi_i\rangle$ for some value of i for which this inequality is satisfied. Because $\left\|(\Phi \otimes I_{\mathbf{L}(\mathcal{F})})(|\psi\rangle\langle\psi|)\right\|_{\mathrm{tr}} \leq \|\Phi\|_\diamond$ by Theorem 2.3, we have $\left\|(\Phi \otimes I_{\mathbf{L}(\mathcal{F})})(|\psi\rangle\langle\psi|)\right\|_{\mathrm{tr}} = \|\Phi\|_\diamond$ as required. □

Strangely, this fact does not hold in general for the trace norm $\|\Phi\|_{\mathrm{tr}}$ in place of the diamond norm.

3 The quantum circuit distinguishability problem

The problem of distinguishing the actions of two circuits is an interesting problem from a complexity theoretic standpoint. The problem of distinguishing two classical circuits that do not make use of randomness is in NP, as one can easily verify that two circuits have different outputs given an input on which they differ. If the circuits use randomness they can be distinguished in AM by a fairly straightforward protocol. If we change the model to quantum circuits over pure states, which capture the intuitive notion of deterministic computation using quantum information, the complexity of the circuit distinguishability problem is in QMA (which is essentially a quantum version of NP) as shown by Janzing, Wocjan, and Beth [4]. If we combine these models, moving to mixed state quantum circuits, where non-unitary operations such as measurement can add randomness, we see what appears to be a significant increase in the complexity of the problem. The definition of the problem follows.

Problem (Quantum Circuit Distinguishability). The problem is parameterized by constants $a, b \in [0, 2]$ with $b < a$. For such constants, define a promise problem $\mathsf{QCD}_{a,b}$ as follows:

Input: Mixed-state quantum circuits (Q_0, Q_1), both of the same type (n, m).

Yes: $\|Q_0 - Q_1\|_\diamond \geq a$

No: $\|Q_0 - Q_1\|_\diamond \leq b$

One may also consider the case where a and b are functions depending on the input length, but this paper will focus on the case where a and b are constant.

At first glance this problem appears to be similar to the $\mathsf{CI}_{a,b}$ problem of the previous section, but we claim that the relation is not at all obvious. We feel the QCD problem is a more interesting problem, particularly because it abstracts a natural physical problem and reveals an apparent complexity-theoretic difference between pure and mixed state models as was discussed previously.

In contrast, the CI problem is really just a rephrasing, based on a theorem in quantum information theory known as Uhlmann's Theorem, of the problem that asks whether a given three-message quantum interactive proof system can be made to accept with high probability.

We now observe that $\mathsf{QCD}_{a,b} \in \mathrm{QIP}$ provided a and b are constants with $b < a$. (For variable a and b, this fact holds if a and b are polynomial-time computable and are separated by the reciprocal of some polynomial.) A simple proof system for this problem is based on the "blind taste-test" idea that is frequently used in the study of interactive proofs. Specifically, a prover attempting to prove that circuits Q_0 and Q_1 differ prepares a state ρ on which they differ and sends the part of ρ on which the circuits act to the verifier. The verifier applies either Q_0 or Q_1 randomly, sends the output to the prover, and challenges the prover to identify which circuit was applied.

Theorem 3.1. $\mathsf{QCD}_{a,b} \in \mathrm{QIP}$ *for any constants* a *and* b *with* $0 \leq b < a \leq 2$.

The proof is based on the following protocol.

Protocol 3.2 (Quantum Circuit Distinguishability). Input to both P and V is (Q_0, Q_1), where circuits Q_0 and Q_1 are assumed to both be of type (n, m).

1. V receives from P an n-qubit quantum register X.
2. V selects $i \in \{0, 1\}$ uniformly and applies circuit Q_i to X. The result is an m-qubit register Y, which V sends to P.
3. V receives from P some $j \in \{0, 1\}$, and accepts if $i = j$, rejecting otherwise.

Proof of Theorem 3.1. We will show that the verifier described in Protocol 3.2 admits a quantum interactive proof system for $\mathsf{QCD}_{a,b}$ with acceptance probability at least $\frac{1}{2} + \frac{a}{4}$ on yes instances and acceptance probability at most $\frac{1}{2} + \frac{b}{4}$ on no instances. It suffices to prove that the maximum probability with which a prover can cause the verifier described in Protocol 3.2 to accept is $\frac{1}{2} + \frac{1}{4} \left\| Q_0 - Q_1 \right\|_\diamond$.

Let $\mathcal{H}$ be the Hilbert space corresponding to the input qubits of Q_0 and Q_1, and let $\mathcal{K}$ be the Hilbert space corresponding to the output qubits. By Lemma 2.4 there exists a Hilbert space $\mathcal{G}$ and a unit vector $|\psi\rangle \in \mathcal{H} \otimes \mathcal{G}$ such that $\left\| Q_0 - Q_1 \right\|_\diamond = \left\| (Q_0 \otimes I_{\mathbf{L}(\mathcal{G})})(|\psi\rangle\langle\psi|) - (Q_1 \otimes I_{\mathbf{L}(\mathcal{G})})(|\psi\rangle\langle\psi|) \right\|_{\mathrm{tr}}$. Fix such a $|\psi\rangle$ and define $\rho_0 = (Q_0 \otimes I_{\mathbf{L}(\mathcal{G})})(|\psi\rangle\langle\psi|)$ and $\rho_1 = (Q_1 \otimes I_{\mathbf{L}(\mathcal{G})})(|\psi\rangle\langle\psi|)$. Now, let Π_0 and $\Pi_1 = I - \Pi_0$ be projection operators on $\mathcal{K} \otimes \mathcal{G}$ that specify an optimal projective measurement for distinguishing ρ_0 from ρ_1. Such a measurement satisfies $\operatorname{tr} \Pi_0(\rho_0 - \rho_1) = \operatorname{tr} \Pi_1(\rho_1 - \rho_0) = \frac{1}{2} \left\| \rho_0 - \rho_1 \right\|_{\mathrm{tr}}$. Now, a strategy for the prover that convinces the verifier to accept with probability $\frac{1}{2} + \frac{1}{4} \left\| Q_0 - Q_1 \right\|_\diamond$ is as follows. The prover prepares two registers (X, Z) in state $|\psi\rangle$ and sends X to the verifier. Upon receiving Y from the verifier, the prover measures (Y, Z) with the measurement $\{\Pi_0, \Pi_1\}$ and returns the result to the verifier. It is a simple calculation to show that this measurement correctly determines i with probability $\frac{1}{2} + \frac{1}{4} \left\| \rho_0 - \rho_1 \right\|_{\mathrm{tr}} = \frac{1}{2} + \frac{1}{4} \left\| Q_0 - Q_1 \right\|_\diamond$.

The probability of acceptance attained by the above prover strategy is optimal, which may be argued as follows. Let ξ denote the mixed state of the register X together with any private qubits of the prover, which we represent as a register Z, immediately after the first message is sent. As before, we let $\mathcal{G}$ denote the Hilbert space corresponding to the prover's private qubit register Z. The verifier applies either Q_0 or Q_1, which causes the pair (Y, Z) to be in state $(Q_0 \otimes I_{\mathbf{L}(\mathcal{G})})(\xi)$ with probability $1/2$ and $(Q_1 \otimes I_{\mathbf{L}(\mathcal{G})})(\xi)$ with probability $1/2$. The register Y is sent to the prover. The prover's final message to the verifier is measured by the verifier, resulting in a single bit. This

process may be viewed as a binary valued measurement of registers (Y, Z). The probability that this measurement is correct is bounded above by

$$\frac{1}{2} + \frac{1}{4} \left\| (Q_0 \otimes I_{\mathbf{L}(\mathcal{G})})(\xi) - (Q_1 \otimes I_{\mathbf{L}(\mathcal{G})})(\xi) \right\|_{\mathrm{tr}} \leq \frac{1}{2} + \frac{1}{4} \left\| Q_0 - Q_1 \right\|_{\diamond}$$

as required. □

Note that a simple variant of the protocol described above gives an ordinary interactive proof system for the classical probabilistic version of the Circuit Distinguishability problem. As the proof system uses a constant number of messages, this demonstrates that the classical variant of the problem is contained in AM.

4 QIP-hardness of distinguishing quantum circuits

In this section we prove that $\mathsf{QCD}_{a,b}$ is hard, with respect to Karp reductions, for the class QIP for any choice of constants a and b with $0 < b < a < 2$.

Theorem 4.1. $\mathsf{QCD}_{2-\varepsilon,\varepsilon}$ *is* QIP*-complete for every* $\varepsilon > 0$.

This theorem is proved in two stages. First, the Close Images problem (for some appropriate choice of parameters) is reduced to $\mathsf{QCD}_{1,1/4}$, implying QIP-hardness of $\mathsf{QCD}_{1,1/4}$. Then, it is argued that $\mathsf{QCD}_{1,1/4}$ reduces to $\mathsf{QCD}_{2-\varepsilon,\varepsilon}$ for any constant $\varepsilon > 0$, which is sufficient to establish the main result. In fact, $\mathsf{QCD}_{2-\varepsilon,\varepsilon}$ remains QIP-hard even when ε is not constant, but rather is an exponentially small function of the input size.

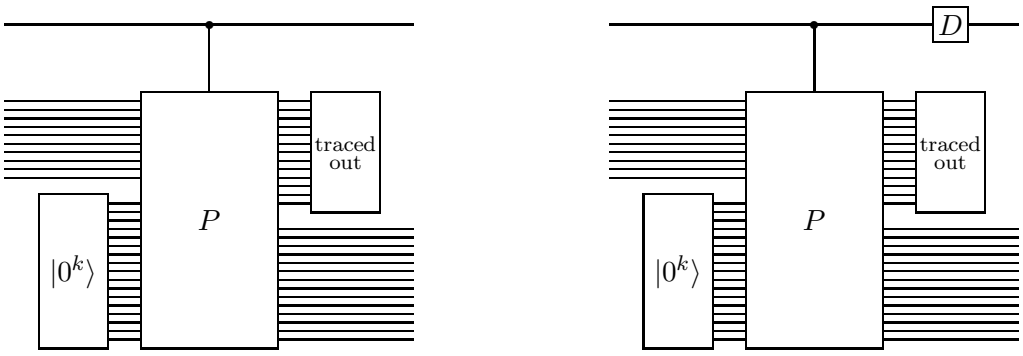
4.1 Overview of proof

The input to the CI problem is a description of two circuits Q_0 and Q_1, both of type (n, m) for nonnegative integers n and m. The reduction will transform the description of these two circuits into a description of two circuits (R_0, R_1) that form an input to the QCD problem.

As discussed in Section 2.1 we may convert Q_0 and Q_1 into unitary circuits P_0 and P_1, acting on $n + k = m + l$ qubits, that simulate Q_0 and Q_1. Here, k is the number of initialized qubits introduced into the circuit and l is the number of "garbage" qubits that are discarded at the end of the simulation. The assumption that P_0 and P_1 act on the same number of qubits can be made without loss of generality, as additional dummy qubits could be added to either circuit as necessary. Given descriptions of P_0 and P_1 it is possible to efficiently construct a unitary circuit P that acts on one more qubit than P_0 and P_1, and uses this additional qubit as a control to determine which of the two circuits P_0 or P_1 to perform. In other words, $P(|0\rangle|\psi\rangle) = |0\rangle P_0|\psi\rangle$ and $P(|1\rangle|\psi\rangle) = |1\rangle P_1|\psi\rangle$ for any $|\psi\rangle$.

Next, define $D(\sigma) = |0\rangle\langle 0|\sigma|0\rangle\langle 0| + |1\rangle\langle 1|\sigma|1\rangle\langle 1|$. This is an admissible operation on a single qubit that represents the process known as decoherence. Informally, the qubit is measured in the standard basis and the result is forgotten. If this gate is not included in the choice of basis gates, it can easily be constructed from gates in any basis satisfying the requirements discussed in Section 2.1.

Finally, let R_0 and R_1 be circuits constructed from P and D as described in Figure 2. Here, the input qubits to R_0 and R_1 correspond to the input qubits of Q_0 or Q_1, which P simulates, as well as the control qubit of P. The remaining k qubits are initialized to the zero state, which is required



Circuit R_0. Circuit R_1.

Figure 2: Circuits output by the reduction.

for the correct functioning of P. The qubits that are output by P include the control qubit, the m qubits representing the output of Q_0 or Q_1, and the l "garbage" qubits that are traced out when simulating Q_0 or Q_1. The circuits R_0 and R_1, however, reverse the roles of the output qubits and garbage qubits of P. Specifically, the garbage qubits of P together with the control qubit are the output qubits of R_0 and R_1, while the qubits of P corresponding to the output of Q_0 or Q_1 are traced out by R_0 and R_1. It is this reversal that is the key to the reduction. The circuits R_0 and R_1 differ only in that R_1 includes the decoherence gate on the control qubit after P is performed while R_0 does not.

When either of the circuits R_0 and R_1 is given an input in which the control qubit is in a superposition of state 0 and 1, possibly entangled with the other input qubits, in effect both of the circuits Q_0 and Q_1 are run. The idea of the reduction is that if the outputs of Q_0 and Q_1 are close on their respective inputs, then when run in superposition discarding these outputs will not destroy the coherence of the control qubit, and thus the outputs of R_0 and R_1 will differ significantly because of the action of the decoherence gate. If the outputs of Q_0 and Q_1 are distinguishable, however, discarding the output qubits of Q_0 or Q_1 is tantamount to decoherence of the control qubit, and so there is no significant difference between R_0 and R_1 in this case as the decoherence gate is effectively redundant.

Formalizing this argument and using suitable parameters allows us to conclude that $\mathsf{QCD}_{1,1/4}$ is QIP-hard. Extending hardness to $\mathsf{QCD}_{2-\varepsilon,\varepsilon}$ can be accomplished by using a variant of Sahai and Vadhan's method of "polarizing" samplable distributions [10] applied to admissible transformations.

4.2 Proof of Theorem 4.1

This section contains a more formal proof that $\mathsf{QCD}_{2-\varepsilon,\varepsilon}$ is QIP-hard for any constant $\varepsilon > 0$, as described in the previous subsection. As $\mathsf{QCD}_{2-\varepsilon,\varepsilon} \in \mathrm{QIP}$, this will imply Theorem 4.1.

Let Q_0 and Q_1 be mixed-state circuits of type (n, m), and consider the circuit construction described in Section 4.1. To be more precise, let $\mathcal{H} = \mathcal{H}(\Sigma^n)$ denote the space corresponding to the input qubits of Q_0 and Q_1 and let $\mathcal{K} = \mathcal{K}(\Sigma^m)$ denote the space corresponding to the output qubits of Q_0 and Q_1. As discussed in Section 2.1, it is possible to efficiently construct unitary circuits P_0 and P_1, acting on $n + k = m + l$ qubits for some choice of k and l, that simulate Q_0 and Q_1. Specifically, if $\mathcal{E} = \mathcal{E}(\Sigma^k)$ and $\mathcal{F} = \mathcal{F}(\Sigma^l)$, then P_0 and P_1 induce unitary transformations

$U_0, U_1 \in \mathbf{U}(\mathcal{H} \otimes \mathcal{E}, \mathcal{K} \otimes \mathcal{F})$ satisfying $Q_i(\rho) = \mathrm{tr}_{\mathcal{F}} U_i(\rho \otimes |0^k\rangle\langle 0^k|)U_i^\dagger$ for $i = 0, 1$.

Next, let $\mathcal{A} = \mathcal{A}(\Sigma)$ be the space corresponding to a single qubit, and define a unitary operator $U \in \mathbf{U}(\mathcal{A} \otimes \mathcal{H} \otimes \mathcal{E}, \mathcal{A} \otimes \mathcal{K} \otimes \mathcal{F})$ by the the equations $U(|0\rangle|\psi\rangle) = |0\rangle\, U_0|\psi\rangle$ and $U(|1\rangle|\psi\rangle) = |1\rangle\, U_1|\psi\rangle$ for every $|\psi\rangle \in \mathcal{H} \otimes \mathcal{E}$. It is possible to construct a unitary circuit P whose operation is described by U that has size polynomial in the sizes of P_0 and P_1. Specifically, this may be done by replacing each gate of P_0 and P_1 by a similar gate that is appropriately controlled by the qubit corresponding to the space $\mathcal{A}$ and running the two circuits one after the other. The controlled gates are of constant size and may either be implemented directly or approximated with very high accuracy depending on the basis gates being considered. See Nielsen and Chuang [9, section 4.3] for further information on such constructions. We can assume without loss of generality that P acts on exactly those qubits P_0 and P_1 act on plus the control qubit; any ancilla required by P can be included in P_0 and P_1.

Finally, the circuits R_0 and R_1 described in Figure 2 correspond to admissible operations in the set $\mathbf{T}(\mathcal{A} \otimes \mathcal{H}, \mathcal{A} \otimes \mathcal{F})$, and can be described more precisely by

$$R_0(X) = \mathrm{tr}_{\mathcal{K}} \left(P \left(X \otimes |0^k\rangle\langle 0^k| \right) \right), \qquad R_1(X) = (D \otimes I_{\mathbf{L}(\mathcal{F})}) \left(\mathrm{tr}_{\mathcal{K}} \left(P \left(X \otimes |0^k\rangle\langle 0^k| \right) \right) \right)$$

for every $X \in \mathbf{L}(\mathcal{A} \otimes \mathcal{H})$. Here, the decoherence operation D is acting on $\mathcal{A}$, i.e., $D \in \mathbf{T}(\mathcal{A}, \mathcal{A})$. The space $\mathcal{K}$, which corresponds to the output qubits of Q_0 and Q_1, is the space that is traced out by R_0 and R_1, while the output qubits of R_0 and R_1 consist of the control qubit and the "garbage" qubits of P_0 and P_1, which correspond to $\mathcal{F}$. Descriptions of these two new circuits can be computed in polynomial time given descriptions of Q_0 and Q_1.

The following lemma formalizes the intuition discussed previously that R_0 and R_1 act very differently if Q_0 and Q_1 can be made to have outputs that have high fidelity with one another.

Lemma 4.2. $\|R_0 - R_1\|_\diamond = \max\{F(Q_0(\rho_0), Q_1(\rho_1)) \,:\, \rho_0, \rho_1 \in \mathbf{D}(\mathcal{H})\}$.

Proof. Let $\rho_0, \rho_1 \in \mathbf{D}(\mathcal{H})$ be any two states. We will show that $\|R_0 - R_1\|_\diamond \geq F(Q_0(\rho_0), Q_1(\rho_1))$. Define $W_0, W_1 \in \mathbf{L}(\mathcal{H}, \mathcal{K} \otimes \mathcal{F})$ as $W_i = U_i(I_{\mathcal{H}} \otimes |0^k\rangle)$ for $i = 0, 1$, where U_i is the unitary operator corresponding to circuit P_i. Each W_i is a unitary embedding that effectively concatenates k ancilla qubits to a vector in $\mathcal{H}$, and then performs U_i on the resulting vector. Let $|\psi_0\rangle, |\psi_1\rangle \in \mathcal{H} \otimes \mathcal{G}$ be any purifications of ρ_0, ρ_1, respectively, where $\mathcal{G}$ is any Hilbert space large enough to admit such purifications. Let $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|\psi_0\rangle + \frac{1}{\sqrt{2}}|1\rangle|\psi_1\rangle$ and consider the action of R_0 and R_1 on $|\psi\rangle\langle\psi|$ (where the circuits act trivially on the space $\mathcal{G}$). The circuits are identical aside from the decoherence gate. Immediately after the circuit P is performed but before the qubits corresponding to the space $\mathcal{K}$ are traced out, the state obtained for both circuits will be $|\phi\rangle\langle\phi|$, for $|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle|\phi_0\rangle + \frac{1}{\sqrt{2}}|1\rangle|\phi_1\rangle$, where $|\phi_0\rangle = (W_0 \otimes I_{\mathcal{G}})|\psi_0\rangle$ and $|\phi_1\rangle = (W_1 \otimes I_{\mathcal{G}})|\psi_1\rangle$. The output of circuit R_0 can therefore be written as

$$\frac{1}{2}\,\mathrm{tr}_{\mathcal{K}} \left(|0\rangle\langle 0| \otimes |\phi_0\rangle\langle\phi_0| \,+\, |0\rangle\langle 1| \otimes |\phi_0\rangle\langle\phi_1| \,+\, |1\rangle\langle 0| \otimes |\phi_1\rangle\langle\phi_0| \,+\, |1\rangle\langle 1| \otimes |\phi_1\rangle\langle\phi_1| \right)$$

while the output of circuit R_1 is

$$\frac{1}{2}\,\mathrm{tr}_{\mathcal{K}} \left(|0\rangle\langle 0| \otimes |\phi_0\rangle\langle\phi_0| \,+\, |1\rangle\langle 1| \otimes |\phi_1\rangle\langle\phi_1| \right).$$

This is because the effect of the decoherence gate is to eliminate the cross-terms $|0\rangle\langle 1| \otimes |\phi_0\rangle\langle\phi_1|$ and $|1\rangle\langle 0| \otimes |\phi_1\rangle\langle\phi_0|$. As $|\phi_0\rangle, |\phi_1\rangle \in \mathcal{K} \otimes \mathcal{F} \otimes \mathcal{G}$ are purifications of $Q_0(\rho_0)$ and $Q_1(\rho_1)$, respectively,

we may conclude by Theorem 2.3 and Lemma 2.1 that

$$\begin{aligned}\|R_0 - R_1\|_\diamond &\geq \big\|(R_0 \otimes I_{\mathbf{L}(\mathcal{G})})(|\phi\rangle\langle\phi|) - (R_1 \otimes I_{\mathbf{L}(\mathcal{G})})(|\phi\rangle\langle\phi|)\big\|_{\mathrm{tr}} \\ &= \frac{1}{2}\,\big\||0\rangle\langle 1| \otimes \mathrm{tr}_{\mathcal{K}}\,|\phi_0\rangle\langle\phi_1| + |1\rangle\langle 0| \otimes \mathrm{tr}_{\mathcal{K}}\,|\phi_1\rangle\langle\phi_0|\big\|_{\mathrm{tr}} = \|\mathrm{tr}_{\mathcal{K}}\,|\phi_0\rangle\langle\phi_1|\|_{\mathrm{tr}} = F(Q_0(\rho_0), Q_1(\rho_1)).\end{aligned}$$

Next, by Lemma 2.4 we have $\|R_0 - R_1\|_\diamond = \big\|(R_0 \otimes I_{\mathbf{L}(\mathcal{G})})(|\psi\rangle\langle\psi|) - (R_1 \otimes I_{\mathbf{L}(\mathcal{G})})(|\psi\rangle\langle\psi|)\big\|_{\mathrm{tr}}$ for some Hilbert space $\mathcal{G}$ and unit vector $|\psi\rangle \in \mathcal{A} \otimes \mathcal{H} \otimes \mathcal{G}$. As $|\psi\rangle$ is a unit vector we may write $|\psi\rangle = \sqrt{p}\,|0\rangle|\psi_0\rangle + \sqrt{1-p}\,|1\rangle|\psi_1\rangle$ for $|\psi_0\rangle, |\psi_1\rangle \in \mathcal{H} \otimes \mathcal{G}$ unit vectors and $p \in [0,1]$. Let $|\phi_i\rangle = (W_i \otimes I_{\mathcal{G}})|\psi_i\rangle$ and $\rho_i = \mathrm{tr}_{\mathcal{G}}\,|\psi_i\rangle\langle\psi_i|$, for $i = 0, 1$. We have

$$\begin{aligned}&\big\|(R_0 \otimes I_{\mathbf{L}(\mathcal{G})})(|\psi\rangle\langle\psi|) - (R_1 \otimes I_{\mathbf{L}(\mathcal{G})})(|\psi\rangle\langle\psi|)\big\|_{\mathrm{tr}} \\ &\qquad = \sqrt{p(1-p)}\,\big\||0\rangle\langle 1| \otimes \mathrm{tr}_{\mathcal{K}}\,|\phi_0\rangle\langle\phi_1| + |1\rangle\langle 0| \otimes \mathrm{tr}_{\mathcal{K}}\,|\phi_1\rangle\langle\phi_0|\big\|_{\mathrm{tr}} \\ &\qquad = 2\sqrt{p(1-p)}\,\|\mathrm{tr}_{\mathcal{K}}\,|\phi_0\rangle\langle\phi_1|\|_{\mathrm{tr}} \\ &\qquad \leq F(Q_0(\rho_0), Q_1(\rho_1)).\end{aligned}$$

This completes the proof of the lemma. □

This lemma and the above construction imply that $\mathsf{CI}_{a,b} \leq_m^p \mathsf{QCD}_{a,b}$ for all $a, b \in [0,1]$ with $b < a$. As $\mathsf{CI}_{1,1/4}$ is a complete promise problem for QIP and $\mathsf{QCD}_{1,1/4}$ is in QIP, we have that $\mathsf{QCD}_{1,1/4}$ is QIP-complete.

Finally, we can extend the QIP-hardness of $\mathsf{QCD}_{1,1/4}$ to instances of the Quantum Circuit Distinguishability problem with a much stronger promise. This fact is based on a generalization of the "polarization" method developed by Sahai and Vadhan [10] in the context of statistical zero-knowledge.

Theorem 4.3. *Let $a, b \in (0,2)$ satisfy $2b < a^2$. There exists a deterministic, polynomial-time procedure that, when given as input $(R_0, R_1, 1^n)$, where R_0 and R_1 are mixed-state quantum circuits, outputs quantum circuits (S_0, S_1) such that*

1. *$\|R_0 - R_1\|_\diamond \leq b \;\Rightarrow\; \|S_0 - S_1\|_\diamond < 2^{-n}$, and*
2. *$\|R_0 - R_1\|_\diamond \geq a \;\Rightarrow\; \|S_0 - S_1\|_\diamond > 2 - 2^{-n}$.*

Sahai and Vadhan proved this theorem for polynomial-time samplable distributions, and it was observed in Ref. [11] that the theorem carries over to polynomial-time preparable quantum states. In the present case, the theorem must be extended to admissible operations.

Lemma 4.4. *If $\Phi_1, \Phi_2 \in \mathbf{T}(\mathcal{H}, \mathcal{K})$ satisfy $\|\Phi_1 - \Phi_2\|_\diamond = \varepsilon$, then*

$$2 - 2e^{\frac{-k\varepsilon^2}{8}} < \left\|\Phi_1^{\otimes k} - \Phi_2^{\otimes k}\right\|_\diamond \leq k\varepsilon.$$

Proof. Let $\mathcal{F}$ be a Hilbert space of dimension equal to that of $\mathcal{H}$, and let $Y \in \mathbf{L}(\mathcal{H} \otimes \mathcal{F})$ satisfy $\|Y\|_{\mathrm{tr}} = 1$ and

$$\big\|(\Phi_1 \otimes I_{\mathbf{L}(\mathcal{F})})(Y) - (\Phi_2 \otimes I_{\mathbf{L}(\mathcal{F})})(Y)\big\|_{\mathrm{tr}} = \|\Phi_1 - \Phi_2\|_\diamond = \varepsilon.$$

Then because $\left\|Y^{\otimes k}\right\|_{\mathrm{tr}} = 1$ we have

$$\begin{aligned}
&\left\|\Phi_1^{\otimes k} - \Phi_2^{\otimes k}\right\|_\diamond \\
&\quad = \max\left\{\left\|(\Phi_1 \otimes I_{\mathbf{L}(\mathcal{F})})^{\otimes k}(X) - (\Phi_2 \otimes I_{\mathbf{L}(\mathcal{F})})^{\otimes k}(X)\right\|_{\mathrm{tr}} : X \in \mathbf{L}((\mathcal{H}\otimes\mathcal{F})^{\otimes k}),\, \|X\|_{\mathrm{tr}} = 1\right\} \\
&\quad \geq \left\|\left((\Phi_1 \otimes I_{\mathbf{L}(\mathcal{F})})(Y)\right)^{\otimes k} - \left((\Phi_1 \otimes I_{\mathbf{L}(\mathcal{F})})(Y)\right)^{\otimes k}\right\|_{\mathrm{tr}} \\
&\quad \geq 2 - 2e^{\frac{-k\varepsilon^2}{8}}.
\end{aligned}$$

The last inequality follows from the result for states analogous to what is here being proved [11].

The second inequality will be proved by induction. The base case $k = 1$ is trivial:

$$\left\|\Phi_1^{\otimes 1} - \Phi_2^{\otimes 1}\right\|_\diamond = \|\Phi_1 - \Phi_2\|_\diamond = \varepsilon.$$

Assume then that $k > 1$, and define $\Psi_i = \Phi_i^{\otimes(k-1)}$ for $i \in \{1, 2\}$. We have

$$\begin{aligned}
\left\|\Phi_1^{\otimes k} - \Phi_2^{\otimes k}\right\|_\diamond &= \|\Psi_1 \otimes \Phi_1 - \Psi_2 \otimes \Phi_2\|_\diamond \\
&= \|\Psi_1 \otimes \Phi_1 - \Psi_2 \otimes \Phi_1 + \Psi_2 \otimes \Phi_1 - \Psi_2 \otimes \Phi_2\|_\diamond \\
&\leq \|(\Psi_1 - \Psi_2) \otimes \Phi_1\|_\diamond + \|\Psi_2 \otimes (\Phi_1 - \Phi_2)\|_\diamond \\
&= \|\Psi_1 - \Psi_2\|_\diamond \|\Phi_1\|_\diamond + \|\Psi_2\|_\diamond \|\Phi_1 - \Phi_2\|_\diamond .
\end{aligned}$$

Because the diamond norm of any admissible transformation is one (see [1] for a proof), we obtain

$$\|\Psi_1 - \Psi_2\|_\diamond \|\Phi_1\|_\diamond + \|\Psi_2\|_\diamond \|\Phi_1 - \Phi_2\|_\diamond \leq (k-1)\varepsilon + \varepsilon = k\varepsilon$$

as required. □

Lemma 4.5. *There is a deterministic polynomial-time procedure that, on input $(Q_0, Q_1, 1^r)$, where Q_0, Q_1 are descriptions of mixed-state quantum circuits, produces as output descriptions of two quantum circuits, (R_0, R_1) satisfying*

$$2 - 2\exp\left(-\frac{r}{8}\|Q_0 - Q_1\|_\diamond^2\right) \leq \|R_0 - R_1\|_\diamond \leq r\,\|Q_0 - Q_1\|_\diamond .$$

Proof. For $i = 0, 1$, construct R_i by placing r copies of the circuit Q_i in parallel. Then $R_i = Q_i^{\otimes r}$, and the bounds on $\|R_0 - R_1\|_\diamond$ follow from Lemma 4.4. □

Proposition 4.6. *Let $\Phi_0, \Phi_1 \in \mathbf{T}(\mathcal{H}, \mathcal{K})$ and $\Psi_0, \Psi_1 \in \mathbf{T}(\mathcal{F}, \mathcal{G})$. Define*

$$\begin{aligned}
\Xi_0 &= \frac{1}{2}\Phi_0 \otimes \Psi_0 + \frac{1}{2}\Phi_1 \otimes \Psi_1, \\
\Xi_1 &= \frac{1}{2}\Phi_0 \otimes \Psi_1 + \frac{1}{2}\Phi_0 \otimes \Psi_1.
\end{aligned}$$

Then $\|\Xi_0 - \Xi_1\|_\diamond = \frac{1}{2}\|\Phi_0 - \Phi_1\|_\diamond \cdot \|\Psi_0 - \Psi_1\|_\diamond$.

Proof. Using Ξ_0, Ξ_1 as in the proposition, we have

$$\begin{aligned}
\|\Xi_0 - \Xi_1\|_\diamond &= \left\| \frac{1}{2}\Phi_0 \otimes \Psi_0 + \frac{1}{2}\Phi_1 \otimes \Psi_1 - \frac{1}{2}\Phi_0 \otimes \Psi_1 - \frac{1}{2}\Phi_0 \otimes \Psi_1 \right\|_\diamond \\
&= \left\| \frac{1}{2}(\Phi_0 - \Phi_1) \otimes (\Psi_0 - \Psi_1) \right\|_\diamond \\
&= \frac{1}{2} \|\Phi_0 - \Phi_1\|_\diamond \cdot \|\Psi_0 - \Psi_1\|_\diamond .
\end{aligned}$$

as desired. □

Lemma 4.7. *There is a deterministic polynomial-time procedure that, on input $(Q_0, Q_1, 1^r)$, where Q_0, Q_1 are descriptions of mixed-state quantum circuits, produces as output descriptions of two quantum circuits (R_0, R_1) satisfying*

$$\|R_0 - R_1\|_\diamond = 2 \left(\frac{\|Q_0 - Q_1\|_\diamond}{2} \right)^r .$$

Proof. The circuit R_0 performs a transformation defined as

$$R_0 = \frac{1}{2^{r-1}} \sum_{\substack{x_1,\ldots,x_r \in \{0,1\} \\ x_1 + \cdots + x_r \equiv 0 \,(\mathrm{mod}\, 2)}} Q_{x_1} \otimes \cdots \otimes Q_{x_r}$$

while R_1 performs a similar transformation defined as

$$R_1 = \frac{1}{2^{r-1}} \sum_{\substack{x_1,\ldots,x_r \in \{0,1\} \\ x_1 + \cdots + x_r \equiv 1 \,(\mathrm{mod}\, 2)}} Q_{x_1} \otimes \cdots \otimes Q_{x_r}.$$

These circuits are effectively running r copies of Q_0 and/or Q_1 in parallel, with the choice of Q_0 or Q_1 determined uniformly at random subject to the constraint that R_0 applies an even number of copies of Q_1 while R_1 applies an odd number. Such circuits may be constructed in time polynomial in the sizes of Q_0 and Q_1. A proof by induction based on Proposition 4.6 establishes that R_0 and R_1 have the required property. □

Proof of Theorem 4.3. First, we apply the procedure given by Lemma 4.5 to $(Q_0, Q_1, 1^r)$, with

$$r = \left\lceil \log(16n) / \log(a^2/(2b)) \right\rceil ,$$

obtaining circuits (Q_0', Q_1') satisfying

$$\begin{aligned}
\|Q_0 - Q_1\|_\diamond < b \quad &\Rightarrow \quad \left\|Q_0' - Q_1'\right\|_\diamond < 2(b/2)^r \\
\|Q_0 - Q_1\|_\diamond > a \quad &\Rightarrow \quad \left\|Q_0' - Q_1'\right\|_\diamond > 2(a/2)^r
\end{aligned}$$

Next, we apply the procedure given by Lemma 4.7 to $(Q_0', Q_1', 1^s)$, where $s = \lfloor (b/2)^{-r}/4 \rfloor$, obtaining circuits (Q_0'', Q_1'') satisfying

$$\begin{aligned}
\|Q_0 - Q_1\|_\diamond < b \quad &\Rightarrow \quad \left\|Q_0'' - Q_1''\right\|_\diamond < 2(b/2)^r (b/2)^{-r}/4 = 1/2 \\
\|Q_0 - Q_1\|_\diamond > a \quad &\Rightarrow \quad \left\|Q_0'' - Q_1''\right\|_\diamond > 2 - 2\exp(-\frac{s}{2}(a/2)^{2r}) \geq 2 - 2e^{-2n+1}.
\end{aligned}$$

Finally, we apply the construction of Lemma 4.5 once more, to $(Q_0'', Q_1'', 1^t)$, where $t = \lceil (n+1)/2 \rceil$, obtaining circuits (R_0, R_1) satisfying

$$\begin{aligned} \|Q_0 - Q_1\|_\diamond < b \quad &\Rightarrow \quad \|R_0 - R_1\|_\diamond < (1/2)^{(n+1)/2}(1/2)^{(n-1)/2} = 2^{-n} \\ \|Q_0 - Q_1\|_\diamond > a \quad &\Rightarrow \quad \|R_0 - R_1\|_\diamond > (2 - 2e^{-2n+1})^{\lceil (n+1)/2 \rceil}(1/2)^{\lceil (n+1)/2 \rceil - 1} \geq 2 - 2^{-n}. \end{aligned}$$

The circuits (R_0, R_1) have size polynomial in r, s, t and the size of the original circuits (Q_0, Q_1). Because r, s, t are bounded by polynomials in n, the size of the constructed circuits is polynomial in the size of the input. □

Theorem 4.3 implies that $\mathsf{QCD}_{1,1/4} \leq_m^p \mathsf{QCD}_{2-\varepsilon,\varepsilon}$ for every $\varepsilon > 0$, which proves Theorem 4.1.

5 Conclusion

We have demonstrated that the problem of distinguishing mixed-state quantum circuits is a complete promise problem for the class QIP. Because QIP contains PSPACE, we conclude that this problem is PSPACE-hard, whereas its classical analogue is contained in the class AM and its unitary quantum circuit analogue is in QMA.

Some open questions relating to this paper follow.

- Does the QIP-completeness of the QCD problem shed any light on properties of QIP? For instance, is QIP is closed under complementation? Is QCD $\in$ PSPACE, which would imply QIP = PSPACE?
- There are interesting questions and results relating to implementations of quantum computers that deal with unitary circuits with mixed-state inputs. (See, e.g., [2, 8].) Analogues of the QCD problem can be defined for this setting. For example, one might consider unitary circuits that act on some collection of inputs together with a collection of qubits in the totally mixed state. How hard is the QCD problem in this context?
- Because it is not known whether QIP = PSPACE, the QCD problem is a candidate problem for QIP\PSPACE. Are there any reasonable non-promise problem candidates for problems in QIP but not in PSPACE?

Acknowledgments

This research was supported by Canada's NSERC, the Canadian Institute for Advanced Research (CIAR), and the Canada Research Chairs Program.

References

[1] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998.

[2] A. Ambainis, L. Schulman, and U. Vazirani. Computing with highly mixed states. In *Proceedings of the 32nd Annual Symposium on the Theory of Computing*, 2000.

[3] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975.

[4] D. Janzing, P. Wocjan, and T. Beth. "Identity check" is QMA-complete. Available as arXiv.org e-Print quant-ph/0305050, 2003.

[5] A. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[6] A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[7] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof system. In *Proceedings of the 32nd ACM Symposium on Theory of Computing*, pages 608–617, 2000.

[8] E. Knill and R. Laflamme. On the power of one bit of quantum information. *Physical Review Letters*, 81:5672–5675, 1998.

[9] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[10] A. Sahai and S. Vadhan. A complete promise problem for statistical zero-knowledge. *Journal of the ACM*, 50(2):196–249, 2003.

[11] J. Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science*, pages 459–468, 2002. Full version available at http://www.cpsc.ucalgary.ca/~jwatrous/papers.html.

[12] J. Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.