

On the Hardness of Distinguishing Mixed-State Quantum Computations

Bill Rosgen¹ John Watrous²

¹Department of Computing Science
University of Alberta

²Department of Computer Science
University of Calgary

Conference on Computational Complexity, 2005

Outline

Distinguishing Circuits

- Classical Circuits

- Quantum Circuits

QIP-completeness of QCD

- QCD is in QIP

- The Reduction

Outline

Distinguishing Circuits

Classical Circuits

Quantum Circuits

QIP-completeness of QCD

QCD is in QIP

The Reduction

Distinguishing Classical Circuits

Problem

Given two deterministic boolean circuits, C_0 and C_1 , is there an input x on which $C_0(x) \neq C_1(x)$?

Distinguishing Classical Circuits

Problem

Given two deterministic boolean circuits, C_0 and C_1 , is there an input x on which $C_0(x) \neq C_1(x)$?

- This problem is NP-complete

Distinguishing Probabilistic Circuits

Problem

Given two boolean circuits, C_0 and C_1 , with coin-flip gates, such that the output distributions of the circuits are either close together for all inputs, or far apart for some inputs, is there an input x on which the distributions given by $C_0(x)$ and $C_1(x)$ can be distinguished?

Distinguishing Probabilistic Circuits

Problem

Given two boolean circuits, C_0 and C_1 , with coin-flip gates, such that the output distributions of the circuits are either close together for all inputs, or far apart for some inputs, is there an input x on which the distributions given by $C_0(x)$ and $C_1(x)$ can be distinguished?

- Given only one sample, the probability of distinguishing two distributions is related to the ℓ^1 norm, $\|C_0(x) - C_1(x)\|_1$

Distinguishing Probabilistic Circuits

Problem

Given two boolean circuits, C_0 and C_1 , with coin-flip gates, such that the output distributions of the circuits are either close together for all inputs, or far apart for some inputs, is there an input x on which the distributions given by $C_0(x)$ and $C_1(x)$ can be distinguished?

- Given only one sample, the probability of distinguishing two distributions is related to the ℓ^1 norm, $\|C_0(x) - C_1(x)\|_1$
- This problem is in AM

AM Protocol

Protocol

Input to both P and V are probabilistic circuits C_0 and C_1 .

- 1. V receives an input x from P*
- 2. V chooses $i \in \{0, 1\}$ uniformly, and sends $C_i(x)$ to P*
- 3. V receives from P some $j \in \{0, 1\}$, and accepts if $i = j$*

Outline

Distinguishing Circuits

Classical Circuits

Quantum Circuits

QIP-completeness of QCD

QCD is in QIP

The Reduction

Distinguishing Pure State Computations

Problem

Given two unitary quantum circuits, Q_0 and Q_1 , with the promise that either there is an input on which the outputs are far apart, or that for all inputs, the outputs are close together, is there a state $|\psi\rangle$ on which $Q_0(|\psi\rangle)$ and $Q_1(|\psi\rangle)$ can be distinguished?

Distinguishing Pure State Computations

Problem

Given two unitary quantum circuits, Q_0 and Q_1 , with the promise that either there is an input on which the outputs are far apart, or that for all inputs, the outputs are close together, is there a state $|\psi\rangle$ on which $Q_0(|\psi\rangle)$ and $Q_1(|\psi\rangle)$ can be distinguished?

- This problem is QMA-complete (Janzing, Wocjan, and Beth, quant-ph/0305050), where $\text{QMA} \subseteq \text{PP}$

Distinguishing Mixed-State Circuits

Problem

Given two quantum circuits, Q_0 and Q_1 , such that the circuits are either close together for all inputs, or far apart for some inputs, is there an input state ρ on which the states $Q_0(\rho)$ and $Q_1(\rho)$ can be distinguished?

Distinguishing Mixed-State Circuits

Problem

Given two quantum circuits, Q_0 and Q_1 , such that the circuits are either close together for all inputs, or far apart for some inputs, is there an input state ρ on which the states $Q_0(\rho)$ and $Q_1(\rho)$ can be distinguished?

- This problem combines both quantum information and randomness

Mixed-State Quantum Circuits

- Mixed states are probability distributions over pure states
- More general representation of quantum information

Mixed-State Quantum Circuits

- Mixed states are probability distributions over pure states
- More general representation of quantum information
- They allow the representation of incomplete knowledge, measurement outcomes, coin flips, . . .

Mixed-State Quantum Circuits

- Mixed states are probability distributions over pure states
- More general representation of quantum information
- They allow the representation of incomplete knowledge, measurement outcomes, coin flips, . . .

Definition

A mixed state is represented by a *density matrix*, which is a trace one positive semidefinite operator.

Trace Norm

- As in the classical probabilistic case, we need to introduce a distance metric between distributions

Trace Norm

- As in the classical probabilistic case, we need to introduce a distance metric between distributions

Definition

The trace norm of a quantum state is a quantum version of the ℓ^1 norm for probability distributions.

Trace Norm

- As in the classical probabilistic case, we need to introduce a distance metric between distributions

Definition

The trace norm of a quantum state is a quantum version of the ℓ^1 norm for probability distributions.

- In particular, $\|\rho_0 - \rho_1\|_{\text{tr}}$ is closely related to the probability that *an optimal* measurement can distinguish ρ_0 and ρ_1

Extending this to Operators

- We need to measure distance between quantum *circuits*

Extending this to Operators

- We need to measure distance between quantum *circuits*
- One standard extension would be

$$\| \| Q_0 - Q_1 \| \| = \max_{\|X\|_{\text{tr}}=1} \| Q_0(X) - Q_1(X) \|_{\text{tr}}$$

Extending this to Operators

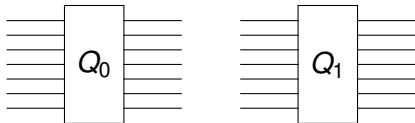
- We need to measure distance between quantum *circuits*
- One standard extension would be

$$\| \| Q_0 - Q_1 \| \| = \max_{\|X\|_{\text{tr}}=1} \| Q_0(X) - Q_1(X) \|_{\text{tr}}$$

- The problem is that the value of this norm can change when extra qubits are added to the system, even though Q_0 and Q_1 do not act on these qubits

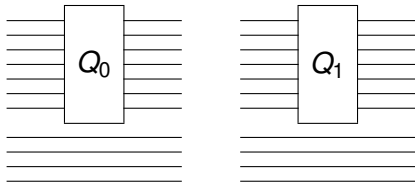
A Better Example

- There are even circuits Q_0 and Q_1 on n qubits with $\|Q_0 - Q_1\| < \frac{4}{n}$,



A Better Example

- There are even circuits Q_0 and Q_1 on n qubits with $\| \| Q_0 - Q_1 \| \| < \frac{4}{n}$,



- but $\| \| Q_0 \otimes I_n - Q_1 \otimes I_n \| \| = 2$, which makes them perfectly distinguishable!

The Diamond Norm

- The change in this norm stabilizes on n qubit circuits when we add n or more extra qubits to the system

The Diamond Norm

- The change in this norm stabilizes on n qubit circuits when we add n or more extra qubits to the system

Definition

If Q_0, Q_1 are quantum operators on n qubits, then the diamond norm of $Q_0 - Q_1$ is

$$\|Q_0 - Q_1\|_{\diamond} = \max_{\|X\|_{\text{tr}}=1} \|(Q_0 \otimes I_n)(X) - (Q_1 \otimes I_n)(X)\|_{\text{tr}}$$

The Diamond Norm

- The change in this norm stabilizes on n qubit circuits when we add n or more extra qubits to the system

Definition

If Q_0, Q_1 are quantum operators on n qubits, then the diamond norm of $Q_0 - Q_1$ is

$$\|Q_0 - Q_1\|_{\diamond} = \max_{\|X\|_{\text{tr}}=1} \|(Q_0 \otimes I_n)(X) - (Q_1 \otimes I_n)(X)\|_{\text{tr}}$$

- This is an analogue of the ℓ^1 norm for quantum circuits

Quantum Circuit Distinguishability

The problem $\text{QCD}_{a,b}$

For $a, b \in [0, 2]$ with $b < a$:

Input: Mixed-state quantum circuits (Q_0, Q_1)

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

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

Quantum Circuit Distinguishability

The problem $QCD_{a,b}$

For $a, b \in [0, 2]$ with $b < a$:

Input: Mixed-state quantum circuits (Q_0, Q_1)

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

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

- Is there an input state ρ such that $Q_0(\rho)$ and $Q_1(\rho)$ are distinguishable?

Quantum Circuit Distinguishability

The problem $QCD_{a,b}$

For $a, b \in [0, 2]$ with $b < a$:

Input: Mixed-state quantum circuits (Q_0, Q_1)

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

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

- Is there an input state ρ such that $Q_0(\rho)$ and $Q_1(\rho)$ are distinguishable?
- This abstracts the problem of distinguishing two physical quantum processes defined in terms of local operations

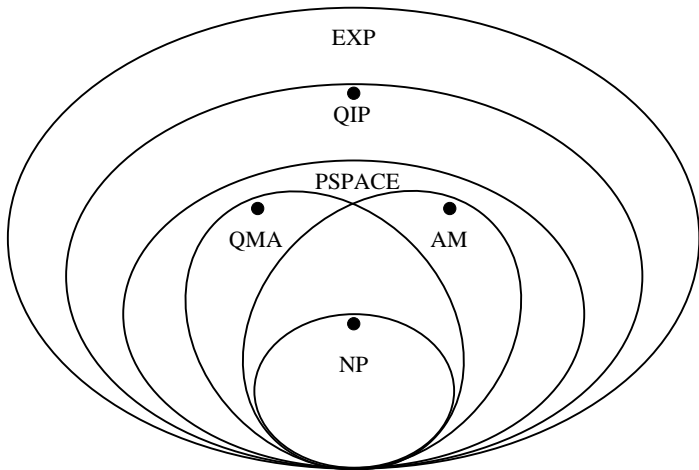
Distinguishing Mixed-State Computations

Theorem

For any $\epsilon > 0$, $\text{QCD}_{2-\epsilon, \epsilon}$ is QIP-complete

- This implies that it is also PSPACE-hard

Complexity Classes



Outline

Distinguishing Circuits
Classical Circuits
Quantum Circuits

QIP-completeness of QCD
QCD is in QIP
The Reduction

QIP Protocol

Protocol (QCD_{2-ε,ε})

Input to both P and V are circuits Q_0 and Q_1 .

- 1. V receives a state ρ from P*
- 2. V chooses $i \in \{0, 1\}$ uniformly, and sends $Q_i(\rho)$ to P*
- 3. V receives from P some $j \in \{0, 1\}$, and accepts if $i = j$*

Outline

Distinguishing Circuits
Classical Circuits
Quantum Circuits

QIP-completeness of QCD
QCD is in QIP
The Reduction

Overview

Theorem

$\text{QCD}_{2-\epsilon, \epsilon}$ is QIP-hard for every $\epsilon > 0$.

Overview

Theorem

$\text{QCD}_{2-\epsilon, \epsilon}$ is QIP-hard for every $\epsilon > 0$.

Overview of Reduction

- *Given a quantum interactive proof system, we build a circuit that implements the Verifier's circuits, we then build circuits R_0, R_1 using this circuit*

Overview

Theorem

$\text{QCD}_{2-\epsilon, \epsilon}$ is QIP-hard for every $\epsilon > 0$.

Overview of Reduction

- *Given a quantum interactive proof system, we build a circuit that implements the Verifier's circuits, we then build circuits R_0, R_1 using this circuit*
- *R_0 and R_1 are distinguishable if and only if the proof system can be made to accept*

Overview

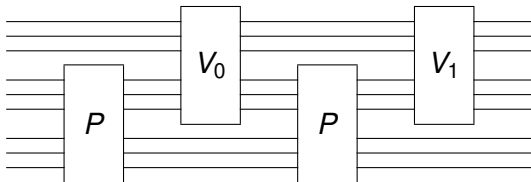
Theorem

$\text{QCD}_{2-\epsilon, \epsilon}$ is QIP-hard for every $\epsilon > 0$.

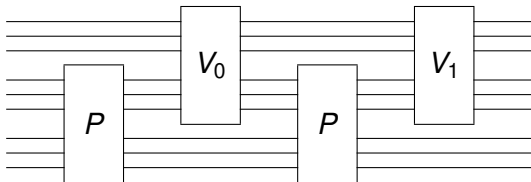
Overview of Reduction

- Given a quantum interactive proof system, we build a circuit that implements the Verifier's circuits, we then build circuits R_0, R_1 using this circuit
- R_0 and R_1 are distinguishable if and only if the proof system can be made to accept
- Via an amplification theorem, $\text{QCD}_{2-\epsilon, \epsilon}$ is QIP-hard

Quantum Interactive Proofs

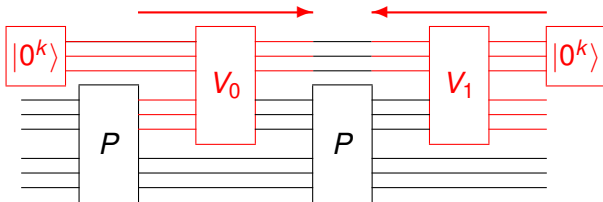


Quantum Interactive Proofs



The Verifier in a three-message quantum interactive proof system can be made to accept if and only if there are inputs on which V_0 and V_1^\dagger act almost identically.

Quantum Interactive Proofs



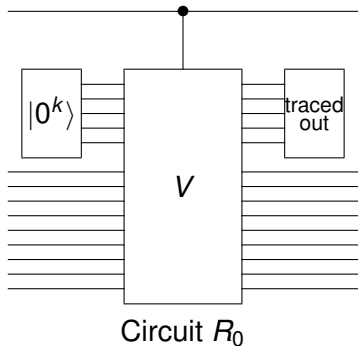
The Verifier in a three-message quantum interactive proof system can be made to accept if and only if there are inputs on which V_0 and V_1^\dagger act almost identically.

Construction

- Given V_0, V_1 from a quantum interactive proof system, we construct a unitary circuit V that, depending on a control qubit, simulates either V_0 or V_1^\dagger on the input

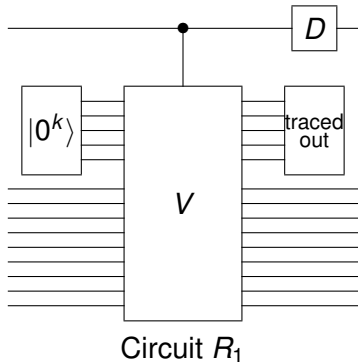
Construction

- Given V_0, V_1 from a quantum interactive proof system, we construct a unitary circuit V that, depending on a control qubit, simulates either V_0 or V_1^\dagger on the input
- Using this, we build circuits R_0 and R_1



Construction

- Given V_0, V_1 from a quantum interactive proof system, we construct a unitary circuit V that, depending on a control qubit, simulates either V_0 or V_1^\dagger on the input
- Using this, we build circuits R_0 and R_1



The Idea

- If R_0 and R_1 are given input with the control qubit in superposition with the input to the circuits, then in effect both V_0 and V_1^\dagger are run

The Idea

- If R_0 and R_1 are given input with the control qubit in superposition with the input to the circuits, then in effect both V_0 and V_1^\dagger are run
- The only difference is the decoherence gate, which has the same effect as measuring the control qubit and then forgetting the result

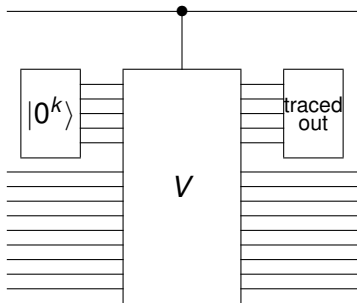
The Idea

- If R_0 and R_1 are given input with the control qubit in superposition with the input to the circuits, then in effect both V_0 and V_1^\dagger are run
- The only difference is the decoherence gate, which has the same effect as measuring the control qubit and then forgetting the result
- The private qubits of the Verifier in V_i are traced out, which is equivalent to measuring and then discarding them

The Idea

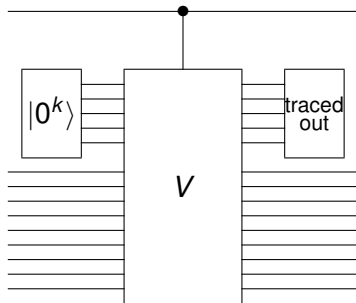
- If R_0 and R_1 are given input with the control qubit in superposition with the input to the circuits, then in effect both V_0 and V_1^\dagger are run
- The only difference is the decoherence gate, which has the same effect as measuring the control qubit and then forgetting the result
- The private qubits of the Verifier in V_i are traced out, which is equivalent to measuring and then discarding them
- The maximum acceptance probability for the proof system is directly related to minimum distance between any output to V_0 and V_1^\dagger

If the Verifier Accepts



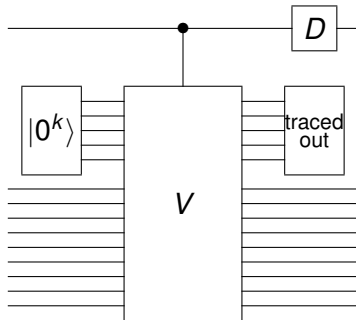
- Take as input to V_0 the initial state of the proof system, after the first message from the prover, and taking as input to V_1^\dagger the output of the system

If the Verifier Accepts



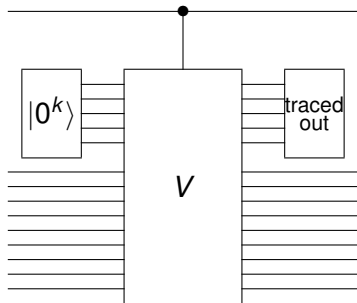
- Since the Verifier accepts, the state of the private qubits will be identical after each circuit

If the Verifier Accepts



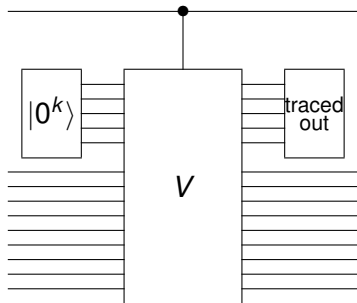
- There is no information in the private qubits, and so tracing them out will have no effect on the coherence of the control qubit

If the Verifier Rejects



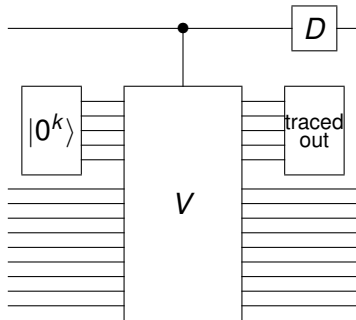
- There are no inputs to V_0 and V_1^\dagger that can make the state of the private qubits closer than a threshold

If the Verifier Rejects



- This leaves information in the private bits that can determine which of V_0 or V_1^\dagger has been performed

If the Verifier Rejects



- Thus, tracing these qubits out will destroy the coherence of the control qubit, and so the decoherence gate has no effect

Almost There

- A more formal treatment of the previous argument proves that $\text{QCD}_{1,1/4}$ is QIP-hard

Almost There

- A more formal treatment of the previous argument proves that $\text{QCD}_{1,1/4}$ is QIP-hard
- To prove that $\text{QCD}_{1,1/4}$ reduces to $\text{QCD}_{2-\epsilon,\epsilon}$, we generalize to admissible quantum operators a polarization theorem of Sahai and Vadhan

Amplification

Theorem

Let $a, b \in (0, 2)$ with $2b < a^2$. When given input $(R_0, R_1, 1^n)$, for R_0, R_1 mixed-state quantum circuits, there is a deterministic polynomial-time procedure that outputs quantum circuits (S_0, S_1) such that

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

Amplification

Theorem

Let $a, b \in (0, 2)$ with $2b < a^2$. When given input $(R_0, R_1, 1^n)$, for R_0, R_1 mixed-state quantum circuits, there is a deterministic polynomial-time procedure that outputs quantum circuits (S_0, S_1) such that

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

- This immediately shows that $\text{QCD}_{2-\epsilon, \epsilon}$ is QIP-hard

Summary

- Distinguishing mixed-state quantum computations is QIP-complete
- This seems to be significantly harder than either the classical case, or the pure-state case
- Outlook
 - Does this shed any light on QIP?
 - is QIP closed under complementation?
 - can this problem be solved in PSPACE?
 - Any non-trivial problem candidates for $\text{QIP} \setminus \text{PSPACE}$?