

Distinguishing Short Quantum Computations

Bill Rosgen

wrosgen@iqc.ca

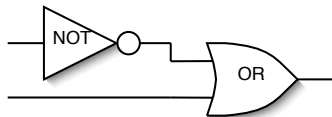
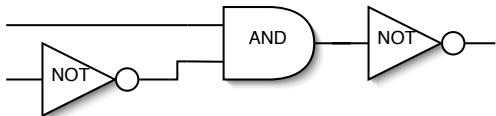
Institute for Quantum Computing
University of Waterloo

22 February, 2008



Distinguishing Classical Circuits

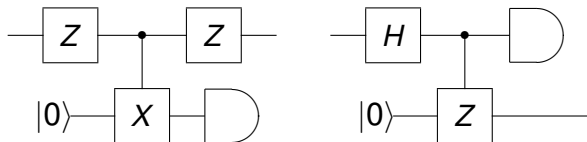
- ▶ Given two classical circuits, what is the complexity of testing if they compute the same function?



- ▶ Deterministic Circuits: **NP**-complete
- ▶ Randomized Circuits: in **AM**

Distinguishing Quantum Circuits

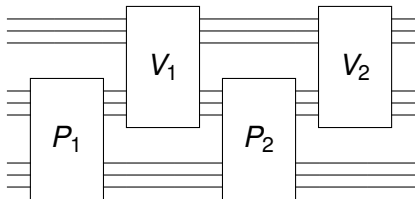
- ▶ What is the complexity of distinguishing quantum circuits?



- ▶ Unitary circuits: **QMA**-complete [DWB03]
- ▶ Mixed state circuits: **QIP**-complete

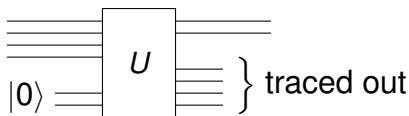
Quantum Interactive Proof Systems

- ▶ **QIP** is the set of languages with *quantum* interactive proofs.
- ▶ **IP = PSPACE** \subseteq **QIP** \subseteq **EXP** [W99, KW00]
- ▶ **QMA** is the set of languages with *one message* quantum interactive proofs.



Circuit Model

- ▶ Unitary gates, as well as measurements and other non-unitary operations are permitted
- ▶ Mixed state circuits can represent any physical process (that is allowed by quantum mechanics).
- ▶ These circuits can be represented in a general form: [AKN98]



Quantum Circuit Distinguishability

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

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

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

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

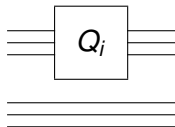
No: $\|Q_0 - Q_1\|_{\diamond} \leq b$

- ▶ i.e. is there an input on which Q_0 and Q_1 act differently?
- ▶ This problem is **QIP**-complete

Kitaev's Diamond Norm

- ▶ This norm seems to be correct for this problem.

$$\begin{aligned}\|Q\|_{\diamond} &= \|Q \otimes I_{\mathcal{F}}\|_{\text{tr}} \\ &= \max_{|\psi\rangle} \|(Q \otimes I_{\mathcal{F}})(|\psi\rangle\langle\psi|)\|_{\text{tr}}\end{aligned}$$



- ▶ $\|Q_1 - Q_2\|_{\diamond}$ corresponds to the probability of correctly identifying Q_i using one application as a black box.

Close Images

 $CI_{a,b}$

For $a, b \in (0, 1]$ with $b < a$:

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

Yes: $F(Q_1(\rho), Q_2(\xi)) \geq a$ for some ρ, ξ

No: $F(Q_1(\rho), Q_2(\xi)) \leq b$ for all ρ, ξ

- ▶ This problem is also **QIP**-complete
- ▶ CI reduces to QCD, with log-depth overhead

Log-depth Close Images

Log-depth $CI_{a,b}$

For $a, b \in (0, 1]$ with $b < a$:

Input: Log-depth mixed-state quantum circuits (Q_0, Q_1)

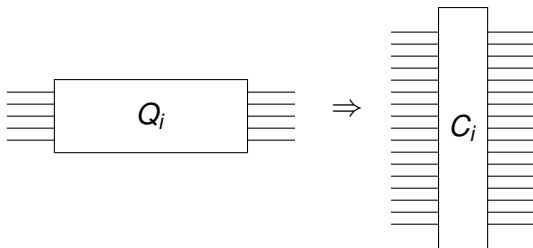
Yes: $F(Q_1(\rho), Q_2(\xi)) \geq a$ for some ρ, ξ

No: $F(Q_1(\rho), Q_2(\xi)) \leq b$ for all ρ, ξ

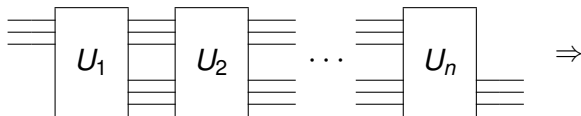
- ▶ This problem remains **QIP**-complete
- ▶ Implies that Log-depth QCD is **QIP**-complete

Overview of the Reduction

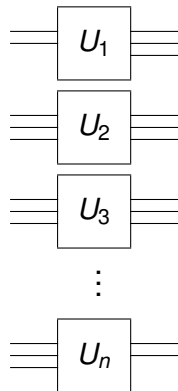
- ▶ Goal: reduce Close Images to Log-depth Close Images.
- ▶ Given circuits (Q_1, Q_2) construct log-depth circuits (C_1, C_2)
- ▶ Either C_i faithfully simulates Q_i ,
or it outputs a state far from the image of C_{2-i} .



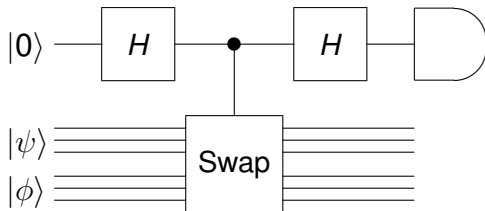
Breaking C into Log-depth Pieces



- ▶ Cut Q_i into log-depth pieces
- ▶ Stacking produces a circuit that is not faithful
- ▶ Need a test to ensure that the input of U_{k+1} matches output of U_k

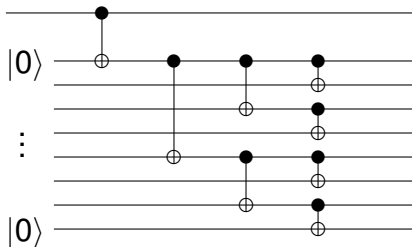


The Swap Test



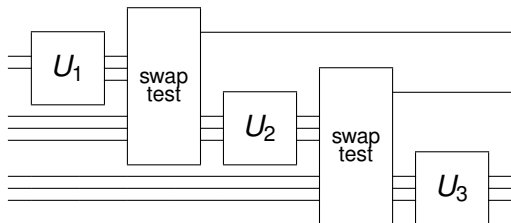
- ▶ On pure states, output is $|1\rangle$ with prob. $(1 - |\langle\psi|\phi\rangle|^2)/2$
- ▶ Can be implemented in log-depth

Log-depth Controlled Operations



- ▶ Log-depth circuits for controlled ops. using a binary tree [MN02]
- ▶ Requires operation to act individually on qubits
- ▶ Adds logarithmic overhead

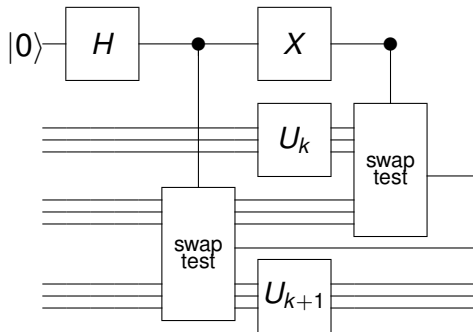
Straightforward Implementation



- ▶ This circuit will be faithful, but requires logarithmic depth

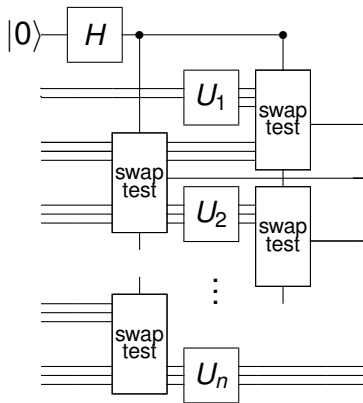
Reducing the Depth

- ▶ Add intermediate inputs to reduce the depth
- ▶ Randomly perform one or the other of the swap tests (simplifies the analysis)

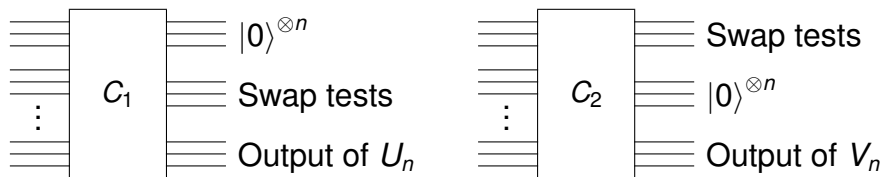


The (Almost) Final Construction

- ▶ Apply this between each piece
- ▶ This circuit will either faithfully simulate Q_i , or at least one swap test outputs $|1\rangle$



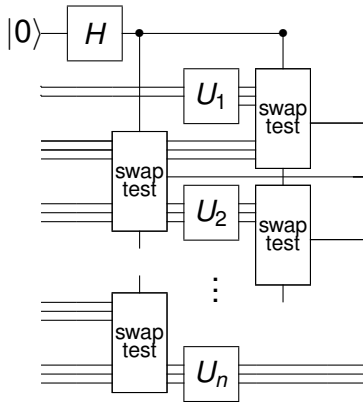
The Final Construction



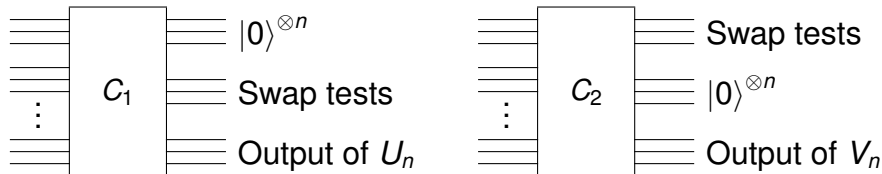
- ▶ Add dummy qubits so that if a swap test outputs $|1\rangle$, then the outputs of the two circuits will be far apart.
- ▶ This completes the reduction.

C_i can Simulate Q_i

- ▶ For pure states, if each input is set correctly, all of the swap tests will output 0
- ▶ In this case, the output of the circuit is $Q_i(|\psi\rangle\langle\psi|) \otimes |0\rangle\langle 0|$



If the C_i are close, then the Q_i are



If the outputs of C_1 and C_2 are close:

1. C_1 faithfully simulates Q_1
2. C_2 faithfully simulates Q_2
3. The outputs of Q_1 and Q_2 are close

Conclusions and Open Problems

- ▶ This can be used to show that the Log-depth Close Images problem is complete for **QIP**.
- ▶ This implies that distinguishing log-depth quantum circuits is also complete for **QIP**.

Open Problems

- ▶ Properties of **QIP**:
 - ▶ Closure under complement?
 - ▶ Better upper or lower bounds?
- ▶ What further restrictions can be placed on the circuits?