

# Hard Problems in a Quantum World

---

Bill Rosgen

Centre for Quantum Technologies  
National University of Singapore

May 9, 2011



# Overview

- ▶ Computational complexity is the field of computer science where we try to understand which problems we can and cannot solve efficiently in various models of computation.
- ▶ Quantum computation gives us a new (relevant) model of computation to study.
- ▶ In this talk I will survey some of the problems we have evidence are hard to solve (in the worst case) with a quantum computer.

# Outline

## Computational complexity

- Introduction and background

- Circuit model

- QMA-complete problems

- QIP-complete problems

# Computational problems

A *problem* (or *language*)  $P$  is a pair of sets  $P_{\text{yes}}$  and  $P_{\text{no}}$  such that

1.  $P_{\text{yes}} \cap P_{\text{no}} = \emptyset$
2.  $P_{\text{yes}}, P_{\text{no}} \subseteq \{0, 1\}^*$

An *algorithm*  $A$  is some process that takes as input  $x \in \{0, 1\}^*$  and either accepts or rejects.  $A$  solves a problem  $P$  if

1. If  $x \in P_{\text{yes}}$  then  $\Pr[A(x) \text{ accepts}] \geq 1 - \varepsilon$
2. If  $x \in P_{\text{no}}$  then  $\Pr[A(x) \text{ accepts}] \leq \varepsilon$ .

We measure the running time of  $A$  as a function of  $|x|$ .

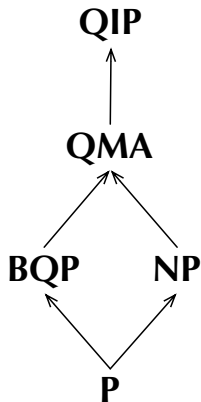
- ▶ This is a *worst-case* definition. We require an algorithm to work correctly for every  $x \in P_{\text{yes}} \cup P_{\text{no}}$

---

<sup>1</sup>strictly: this defines the *promise problems*, but I'll ignore this distinction.

## Complexity classes

A complexity class is the set of all problems solved by algorithms in some model of computation.



**BQP**: Efficient quantum computation

**QMA**: Efficient quantum computation with access to an untrusted quantum proof

**QIP**: Efficient quantum computation with interactive access to untrusted party (equal to **PSPACE** [JJUW10])

(*Efficient* always means polynomial time in the length of  $x$ .)

# Reductions

We need a tool to compare the hardness of different problems.

A problem  $P$  reduces to a problem  $Q$ , written  $P \leq Q$  if there is an efficient transformation  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$  such that

1. If  $x \in P_{\text{yes}}$  then  $f(x) \in Q_{\text{yes}}$ .
2. If  $x \in P_{\text{no}}$  then  $f(x) \in Q_{\text{no}}$ .

Intuitively:  $P$  is no harder than  $Q$ , since we can solve  $P$  using only  $f$  and an algorithm for  $Q$ .

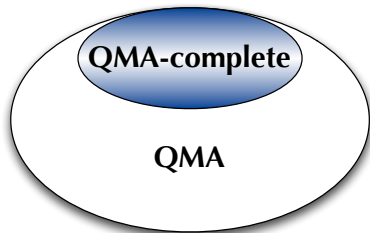
Two problems  $P, Q$  are *equivalent* if  $P \leq Q$  and  $Q \leq P$ .

## Complete problems

Most complexity classes have complete problems.

$P$  is complete for a class  $\mathbf{C}$  if

1.  $Q \leq P$  for all  $Q \in \mathbf{C}$
2.  $P \in \mathbf{C}$ .

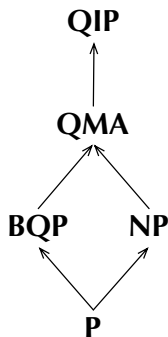


- ▶ A proof of completeness shows that a problem is 'hard'
- ▶ Complete problems give us a different characterization of a computational model
- ▶ Remember: these are *worst-case* results.

## How is a hardness result useful?

Suppose you want to decide if some local constraints can be satisfied by some global quantum state:

- ▶ In general this is **QMA**-complete [Liu06], and so there is no general algorithm<sup>1</sup>
- ▶ This does *not* mean that every instance is hard, only that there exist hard instances
- ▶ This *does* imply that you will need to use some additional structure or information



---

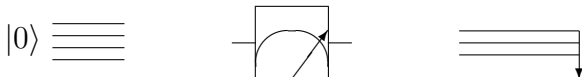
<sup>1</sup>Given the usual complexity-theoretic assumptions ...

## Quantum (mixed-state) circuits

Often the input  $x$  to a problem will be a state or a channel. As a binary representation we will use the circuit model.

- ▶ 'Efficient' states and channels have circuits of size  $\log d$ , but density matrices and Kraus operators are always large.
- ▶ Given a circuit we can run it in quantum polynomial time.

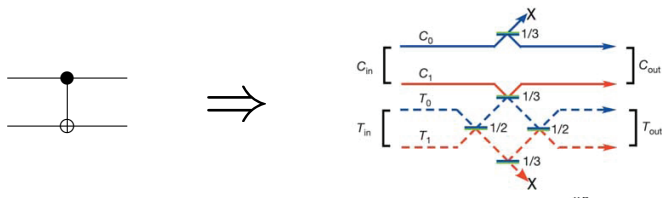
We use any standard set of unitary gates plus three gates:



This model allows us to represent *any* quantum channel.

## Circuits are generic

- ▶ The fact that we use circuits does not limit hardness results
- ▶ Given a problem in the circuit model, we can reduce it to any other model that can simulate circuits:



- ▶ Circuit problems no harder than problems in any model that can simulate circuits.

<sup>1</sup>Gate implementation [O'Brien et al., Nature 2003]

# Circuits are useful

Using circuits to represent states and channels has advantages.

When solving problems:

- ▶ States can be constructed efficiently
- ▶ Channels can be performed efficiently

When proving hardness results:

- ▶ Unitary circuits can be inverted by running them backwards
- ▶ Controlled versions of channels can be constructed

# Outline

Computational complexity

QMA-complete problems

QMA

Local Hamiltonian

Local Consistency

(Non-)Identity Testing

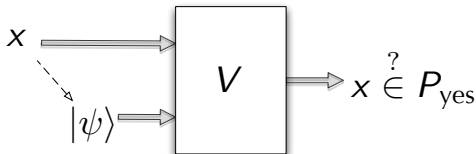
(Non-)Isometry Testing

Detecting Insecure Encryption

QIP-complete problems

# QMA

**QMA:** problems that can be *verified* with a quantum computer.

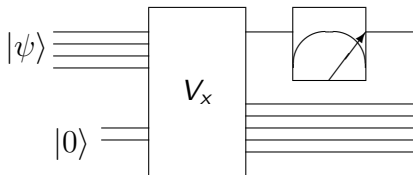


To decide if  $x \in P_{yes}$ , the Verifier (*Arthur*) receives a proof  $|\psi\rangle$  from the Prover (*Merlin*) and runs some efficient circuit  $V$ .

- ▶  $|\psi\rangle$  may depend on  $x$ .
- ▶ Merlin is not computationally bounded.
- ▶ Merlin is not trustworthy.

## QMA (definition)

**QMA** is the set of all problems  $P$  for which there exist polynomial-time unitary circuits  $V$  such that:



- ▶ When  $x \in P_{\text{yes}}$ ,  $\exists |\psi\rangle$  such that outcome is  $|1\rangle$  with  $\text{Pr} \geq 1 - \varepsilon$
- ▶ When  $x \in P_{\text{no}}$ ,  $\forall |\psi\rangle$  the outcome is  $|1\rangle$  with  $\text{Pr} \leq \varepsilon$

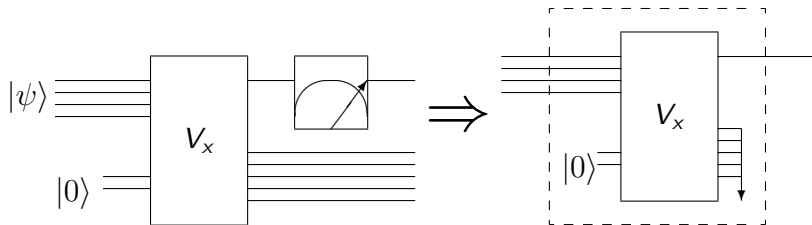
## QMA as a problem

This definition can also be viewed as a complete problem:

### Problem (QMA)

On input  $C$  a circuit with one output qubit, decide between:

- ▶  $C \in \text{QMA}_{\text{yes}}$  if there exists  $|\psi\rangle$  such that  $C(|\psi\rangle)$  is measured to be  $|1\rangle$  with  $\text{Pr} \geq 1 - \epsilon$
- ▶  $C \in \text{QMA}_{\text{no}}$  if for any  $|\psi\rangle$ , of  $C(|\psi\rangle)$  is measured to be  $|1\rangle$  with  $\text{Pr} \leq \epsilon$



## Local Hamiltonians

A Hermitian matrix  $H$  acts on  $k$  qubits if

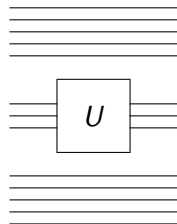
$$H = P(A \otimes \mathbb{1})P^{-1}$$

for  $P$  a permutation matrix and  $A 2^k \times 2^k$ .

A Hermitian matrix  $H$  is  $k$ -local if

$$H = \sum_{i=1}^r H_i$$

where each  $H_i$  acts on at most  $k$  qubits.



# Complexity of Local Hamiltonians

## Problem ( $k$ -local Hamiltonian (KSV02))

On input  $a < b \in \mathbb{R}$  and  $k$ -local  $H = \sum_{i=1}^r H_i$  on  $n$  qubits, with  $r \in \text{poly}(n)$  and  $\|H_i\| \leq \text{poly}(n)$  for each  $i$ , decide between:

- ▶ Yes: smallest eigenvalue of  $H$  is less than  $a$
- ▶ No: smallest eigenvalue of  $H$  is more than  $b$

## Results:

- ▶  $k$ -local Hamiltonian is **QMA**-complete [KSV02]
- ▶ 2-local Hamiltonian is **QMA**-complete [KKR06]
- ▶ 2-local Hamiltonian with only nearest-neighbour interactions on a 2D grid is **QMA**-complete [OT05]
- ▶ Nearest-neighbour interactions on a 1D grid is **QMA**-complete, but uses local dimension 12 [AGIK07]

## Local Consistency

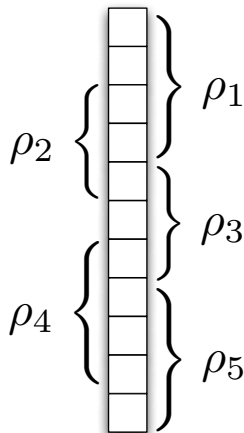
Is a set of (overlapping) local descriptions consistent with some global quantum state?

### Problem (Local Consistency (Liu06))

Given  $\beta \in \mathbb{R}$  and  $\rho_1, \dots, \rho_r$  each on at most  $k$  of the  $n$  qubits, decide between:

- ▶ Yes: there is some  $n$ -qubit  $\sigma$  whose reduced states are exactly the  $\rho_i$ .
- ▶ No: for any  $\sigma$ , there is some  $\rho_i$  such for that the corresponding reduced state  $\sigma_i$

$$\|\rho_i - \sigma_i\|_{\text{tr}} \geq \beta.$$



This is **QMA**-complete\* [Liu06]

## Identity Testing

Given two *unitary* circuits, are they (approximately) the same?

Equivalent to testing if a circuit is close to the identity, since

$$\|U - V\| = \|V^*U - \mathbb{1}\|$$

Problem (Non-identity check [JWB05])

Given unitary  $U$  as a circuit, decide between

- ▶ Yes: there exists  $|\psi\rangle$  such that for any  $\phi$

$$\|U|\psi\rangle - e^{i\phi}|\psi\rangle\| \geq 2 - \varepsilon$$

- ▶ No: for all  $|\psi\rangle$  there exists  $\phi$  such that

$$\|U|\psi\rangle - e^{i\phi}|\psi\rangle\| \leq \varepsilon$$

This is **QMA**-complete [JWB05].

## (Non-)Isometry Testing

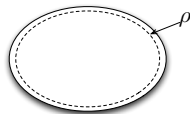
How hard is it to decide if a channel  $\Phi$  is close to unitary?

This is equivalent to testing how mixed the output of  $\Phi \otimes I$  can be when the input is a pure state.

### Definition

A state  $\rho$  is  $\varepsilon$ -pure if  $\min_{|\psi\rangle} \|\rho - |\psi\rangle\langle\psi|\|_{\text{tr}} \leq \varepsilon$ .

- ▶ Equivalent definitions (up to constants):
  - ▶  $\text{tr}(\rho^2) \geq 1 - \varepsilon$ ,
  - ▶  $\|\rho\|_{\infty} \geq 1 - \varepsilon$ .



# Computational problem

## Problem (Non-isometry)

Given a circuit  $\Phi$ , decide between:

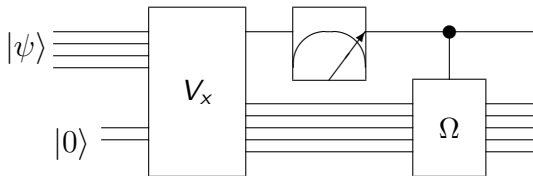
- ▶ Yes: For some  $|\psi\rangle$ ,  $(\Phi \otimes I)(|\psi\rangle\langle\psi|)$  is  $(1 - \varepsilon)$  far from pure,
- ▶ No: All pure-state inputs to  $\Phi \otimes I$  result in  $\varepsilon$ -pure outputs.



Is there pure input  $|\psi\rangle$  on which  $\Phi \otimes I$  outputs a highly mixed state, or is the output of  $\Phi \otimes I$  always close to pure?

## Hardness of Non-isometry Testing

- ▶ Argue by reduction from an arbitrary problem in **QMA**
- ▶ Add to the verifier a controlled depolarizing channel:

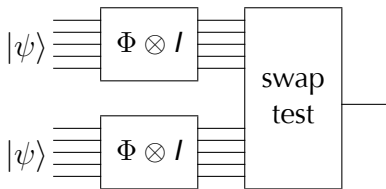


- ▶ if  $x \in QMA_{\text{yes}}$ , there is  $|\psi\rangle$  with output  $(1 - 2\epsilon)$ -far from pure
- ▶ if  $x \in QMA_{\text{no}}$ , output state is  $2\epsilon$ -pure for any  $|\psi\rangle$

## Non-isometry Testing in QMA

How to put the problem into **QMA**?

Given two *unentangled* copies of the same state  $|\psi\rangle$ :



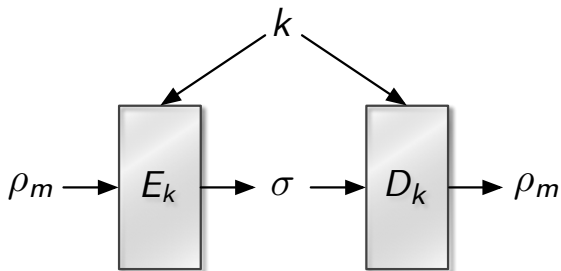
The output is 'antisymmetric' with probability

$$\frac{1}{2} - \frac{1}{2} \text{tr} [(\Phi \otimes I)(|\psi\rangle\langle\psi|)^2]$$

Proof requires a more complicated technique to deal with entangled states, but the argument is quite technical.

## Detecting Insecure Encryption

How hard is it to check that an encryption system is secure?



Given  $E_k$  we want to check that for any  $\rho_m$  and a random key  $k \in \{0, 1\}^r$ ,  $\sigma$  has almost no information about  $\rho_m$ .

## More notation ...

Formalizing this requires the *diamond norm* on channels:

$$\|\Phi\|_{\diamond} = \|\Phi \otimes I\|_{\text{tr}} = \max_{\rho} \|(\Phi \otimes I)(\rho)\|_{\text{tr}}$$

Given one of  $\Phi_1$  and  $\Phi_2$  as a black box, the probability of identifying the channel with a single use is:

$$\frac{1}{2} + \frac{\|\Phi_1 - \Phi_2\|_{\diamond}}{4}.$$



# Detecting Insecure Encryption

## Problem (Detecting Insecure Encryption)

Given a circuit  $E$  that takes a quantum input (of dimension  $d$ ) and a secret key  $k \in \{1, \dots, 2^r\}$ , decide between

- ▶ Yes: There exists a subspace  $S$  of dimension  $\sqrt{d}$  such that for all  $|\psi\rangle \in S$  and all  $k$

$$\|E_k(|\psi\rangle\langle\psi|) - |\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|\|_{\text{tr}} \leq \varepsilon$$

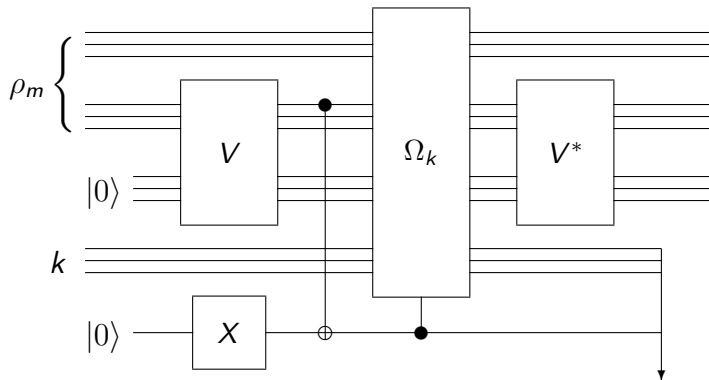
- ▶ No:

$$\left\| \frac{1}{2^r} \sum_k E_k - \Omega \right\|_{\diamond} \leq \varepsilon$$

Either the encryption is almost perfect, or it fails completely on a large subspace. This problem is **QMA**-complete.

## Reduction from QMA

Let  $V$  be a **QMA** verifier and let  $\Omega_k$  be the channel that applies Pauli operators indexed by  $k$ .



The output is encrypted only when  $V$  would have rejected.

# Outline

Computational complexity

QMA-complete problems

QIP-complete problems

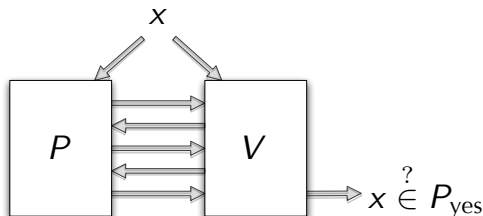
QIP

Close Images

Channel Distinguishability

# Quantum interactive proof systems

**QIP:** problems that can be *interactively verified*.

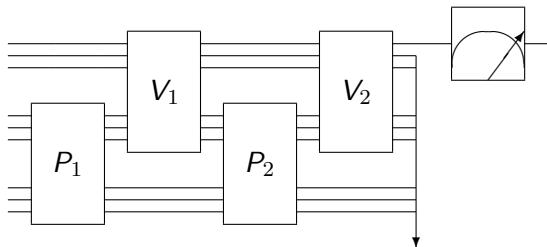


To decide if  $x \in P_{\text{yes}}$ , the Verifier communicates with a Prover while performing some efficient quantum computation.

- ▶ Both parties know  $x$ .
- ▶ Prover is not computationally bounded (or trustworthy).
- ▶ Both parties have private memory.

## QIP (definition)

Formally the Verifier is specified by quantum circuits  $V_1, \dots, V_k$



Given a problem  $\Pi \in \mathbf{QIP}$ , there exists a verifier  $V$  such that

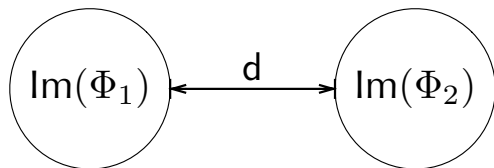
- ▶ If  $x \in \Pi_{\text{yes}}$ , then there exists  $P$  such that  $\Pr[V \text{ accepts } P\text{'s proof}] \geq 1 - \varepsilon$
- ▶ If  $x \in \Pi_{\text{no}}$ , then for any  $P$ ,  $\Pr[V \text{ accepts } P\text{'s proof}] \leq \varepsilon$

## Close Images

### Problem (Close Images (KW00))

Given two circuits  $\Phi_1, \Phi_2$ , decide between

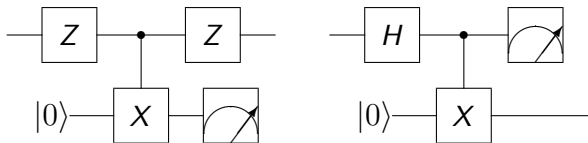
- ▶ Yes: There exist  $\rho, \sigma$  such that  $F(\Phi_1(\rho), \Phi_2(\sigma)) \geq 1 - \epsilon$ .
- ▶ No: For all  $\rho, \sigma$ ,  $F(\Phi_1(\rho), \Phi_2(\sigma)) \leq \epsilon$ .



- ▶ The **QIP**-completeness of this problem follows from the fact that **QIP** can be reduced to 3 messages [KW00].
- ▶ Problem is still hard for log-depth circuits.

# Classical and quantum circuit distinguishability

- ▶ What is the complexity of distinguishing two circuits?
  - ▶ i.e. deciding if they have inputs on which they disagree.
  - ▶ i.e. determining if  $\|\Phi_1 - \Phi_2\|_\diamond$  is large or small.



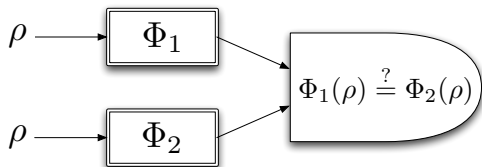
- ▶ Classical circuits: **NP**-complete
- ▶ Unitary circuits: **QMA**-complete [JWB05]
- ▶ For general channels this is **QIP**-complete [RW05]

# Distinguishing quantum circuits

## Problem (Quantum Circuit Distinguishability)

Given two circuits  $\Phi_1, \Phi_2$ , decide between

- ▶ Yes:  $\|\Phi_1 - \Phi_2\|_{\diamond} \geq 2 - \epsilon$ ,
- ▶ No:  $\|\Phi_1 - \Phi_2\|_{\diamond} \leq \epsilon$ .

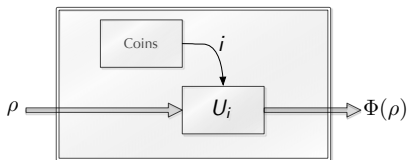


- ▶ Less formally: is there an input  $\rho$  on which  $\Phi_1 \otimes I$  and  $\Phi_2 \otimes I$  produce (almost) orthogonal outputs?

# Mixed-unitary channels

Distinguishability remains **QIP**-complete when restricted to convex mixtures of unitary channels.

- ▶  $\Phi$  is mixed-unitary if  $\Phi(\rho) = \sum_i p_i U_i \rho U_i^*$ , where the  $p_i$  form a probability distribution.

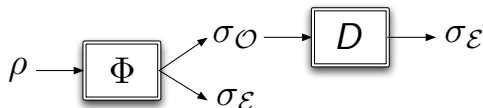


Examples:

- ▶ Depolarizing channel:  
 $\frac{1}{4}(\rho + X\rho X + Z\rho Z + XZ\rho ZX)$
- ▶ Dephasing channel:  
 $\frac{1}{2}(\rho + Z\rho Z)$

## Degradable channels

- ▶ A channel is degradable if there is a channel that takes the output state to environment state.



- ▶ For any channel  $\Phi$ , construct the degradable channel<sup>1</sup>

$$\Phi'(\rho) = \frac{1}{2}|0\rangle\langle 0| \otimes \rho + \frac{1}{2}|1\rangle\langle 1| \otimes \Phi(\rho)$$

- ▶ This satisfies  $\|\Phi' - \Psi'\|_{\diamond} = \frac{1}{2} \|\Phi - \Psi\|_{\diamond}$
- ▶ After some amplification, this shows that distinguishing degradable channels is **QIP**-complete.

---

<sup>1</sup>This construction can be found in [CRS08]

## Open problems / discussion

- ▶ This talk has listed many of the problems that we know to be hard in a world with large-scale quantum computers.
  - ▶ Classically we know *thousands* of **NP**-complete problems.
  - ▶ Much more interesting is understanding interesting or practical problems, i.e. what is the simplest form of tomography that is hard?
- ▶ Classically we have approximation algorithms for many of the problems known to be hard. This is still largely open in the quantum case.
- ▶ Do decision problems even make sense in a quantum world? The classical tricks for turning function problems into decision problems do not work for quantum states.