

# Quantum Proofs – Part II

## Quantum interactive proofs

John Watrous

Institute for Quantum Information Science and  
Department of Computer Science  
University of Calgary

# Non-interactive vs. interactive proofs

In the previous talk we discussed **non-interactive proofs**; there was no interaction between the verification procedure and the entity that prepared the proof.

In this talk we will discuss **interactive proofs**. Now, the verification procedure may ask questions about the input string and receive answers from the entity that is trying to prove something about it.

# Terminology

An **interactive proof system** involves an interaction between two parties, the **prover** and the **verifier**, concerning an input string  $x$  to a promise problem  $A = (A_{\text{yes}}, A_{\text{no}})$ .

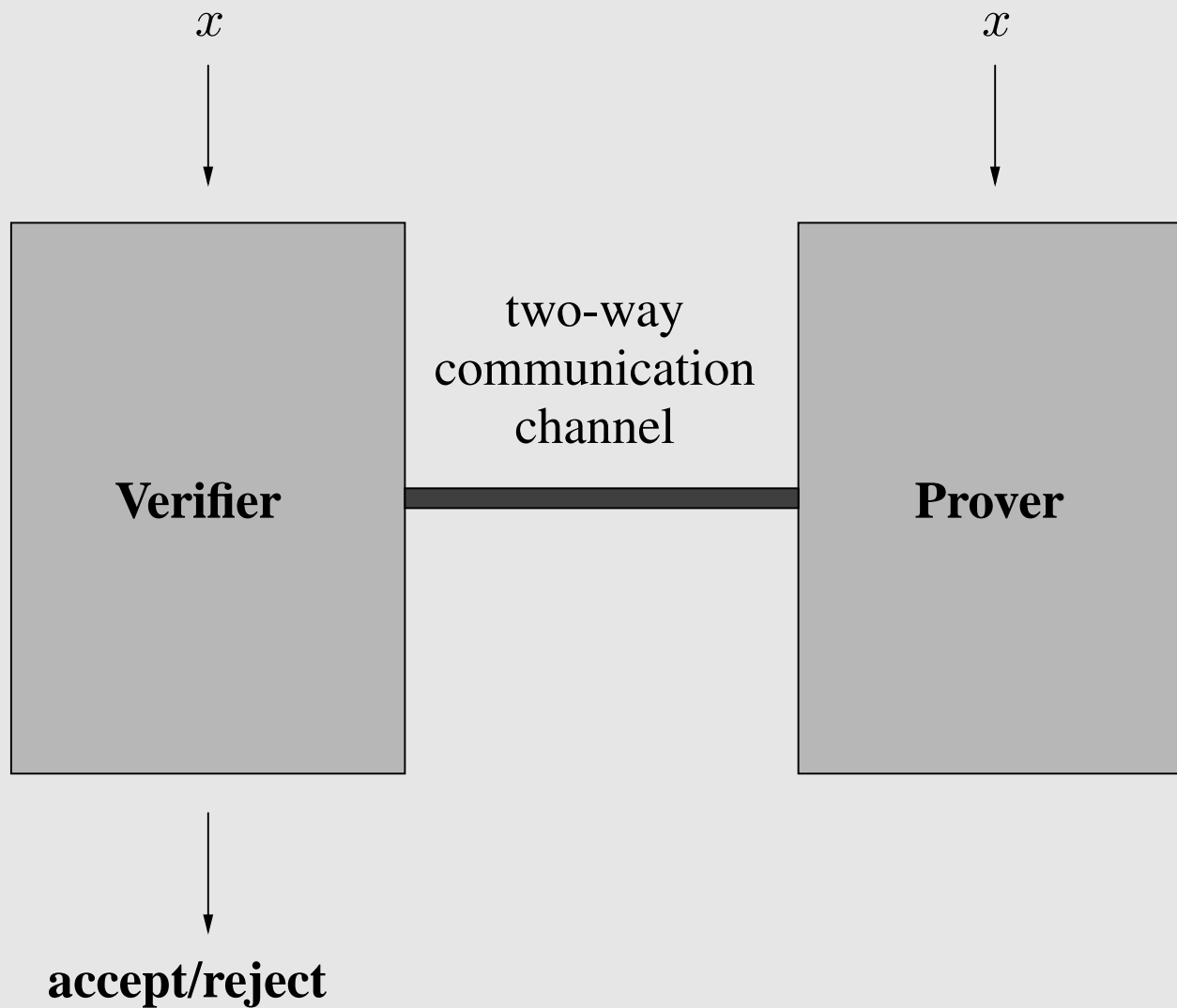
## The Prover

- Goal is to convince the verifier that  $x \in A_{\text{yes}}$ .
- The prover is **not trustworthy**—it will try to prove  $x \in A_{\text{yes}}$  even when this is not the case.
- The prover is **computationally unbounded**.

## The Verifier

- Goal is to check the validity of the prover's argument that  $x \in A_{\text{yes}}$ .
- The verifier is **computationally bounded**. It essentially has the power of BPP (classical) or BQP (quantum).

# Picture of an interactive proof



# Completeness and Soundness

A promise problem  $A = (A_{\text{yes}}, A_{\text{no}})$  **has an interactive proof system** if there exists a verifier  $V$  that satisfies these two conditions:

1. **Completeness.** If  $x \in A_{\text{yes}}$ , then there is a prover  $P$  that convinces  $V$  to accept  $x$  (with high probability).
2. **Soundness.** If  $x \in A_{\text{no}}$ , then no prover  $P$  can convince  $V$  to accept  $x$  (except with small probability).

(No requirements are placed on the system for inputs  $x \notin A_{\text{yes}} \cup A_{\text{no}}$ .)

# Example: the Pepsi challenge (sort of)

Consider the following claim:

**Coke and Pepsi taste different.**

Suppose you believe this claim, and indeed can taste the difference. (Substitute “salt and sugar” for “Coke and Pepsi” if it helps with the example.)

How do you prove it to a skeptic?

**Non-interactive proof:** hopeless.

**Interactive proof:** easy. Let the skeptic run a **blind taste test**; when you win every time, he should be convinced.

# Similar protocol for GNI

Recall from the previous talk the statement of the graph non-isomorphism problem.

## GRAPH NON-ISOMORPHISM (GNI)

**Input:** Two simple, undirected graphs  $G_0$  and  $G_1$ .

**Yes:**  $G_0$  and  $G_1$  are not isomorphic ( $G_0 \not\cong G_1$ ).

**No:**  $G_0$  and  $G_1$  are isomorphic ( $G_0 \cong G_1$ ).

This problem has a very simple classical interactive proof (requiring just one question and response).

# GNI protocol

1. The verifier randomly chooses a bit  $b \in \{0, 1\}$  and a permutation  $\sigma \in S_n$ , and lets  $H = \sigma(G_b)$ .
2. The verifier sends  $H$  to the prover, and challenges him to guess whether  $b = 0$  or  $b = 1$ . If the prover guesses correctly, the verifier **accepts**, otherwise he **rejects**.

(May be repeated many times in parallel to decrease the error probability.)

Why does it work?

**Completeness.** If  $G_0 \not\cong G_1$ , then  $H$  is isomorphic to  $G_0$  or  $G_1$ , but not both... the prover can determine which and correctly guess  $b$  every time.

**Soundness.** If  $G_0 \cong G_1$ , then knowledge of  $H$  gives no information about  $b$ . Any guess by the prover will be correct with probability  $1/2$ .

# Interactive Proof Complexity Classes

The complexity class containing all promise problems having classical interactive proof systems is denoted  $\text{IP}$ . It is known that  $\text{IP} = \text{PSPACE}$ .

[FELDMAN, 1986; LUND, FORTNOW, KARLOFF, & NISAN, 1990; SHAMIR, 1990]

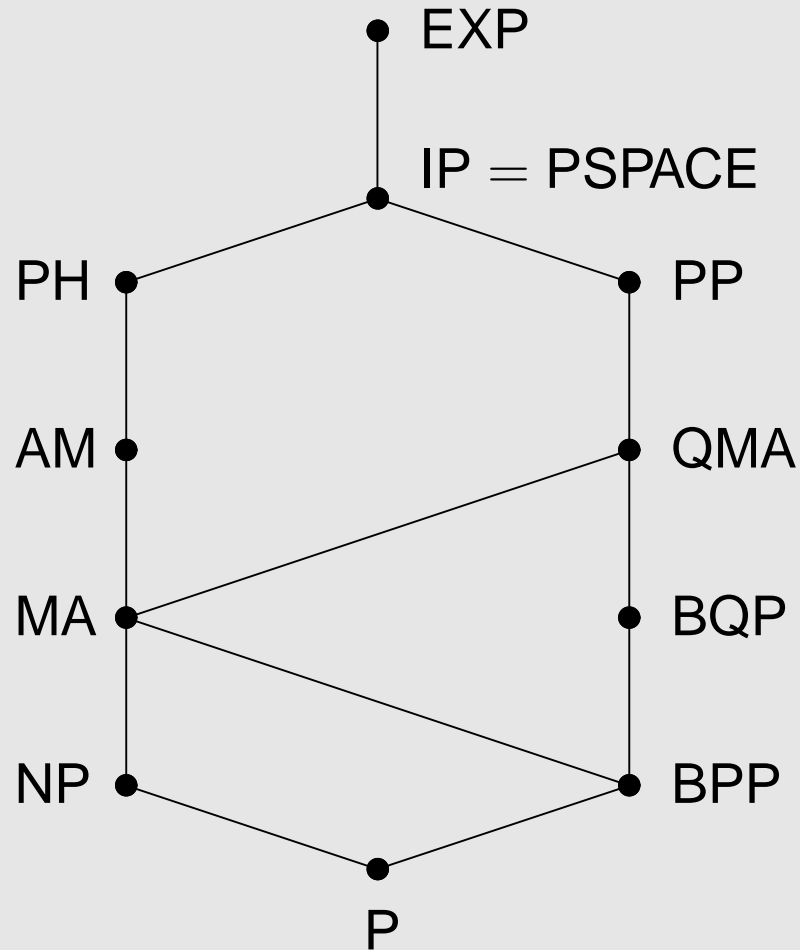
Denote the class of promise problems having classical interactive proofs with at most  $m$  messages by  $\text{IP}(m)$ . For any constant  $c \geq 2$  it holds that

$$\text{IP}(c) = \text{IP}(2) = \text{AM} \subseteq \Pi_2.$$

[BABAI, 1985; GOLDWASSER & SIPSER, 1989]

(Known classical protocols for  $\text{PSPACE}$  require a polynomial number of messages. It is typically conjectured that  $\text{AM} \subsetneq \text{PSPACE}$ .)

# Diagram of Complexity Classes

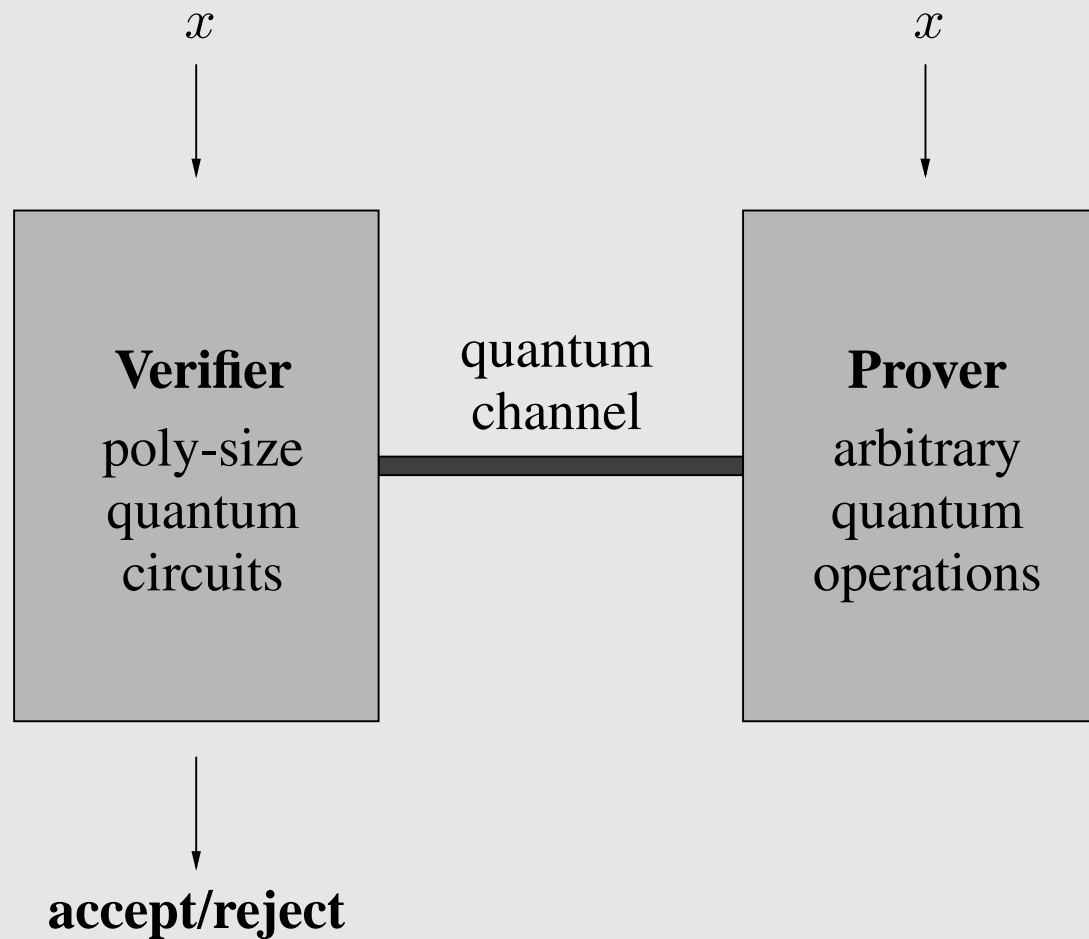


# Quantum Interactive Proofs

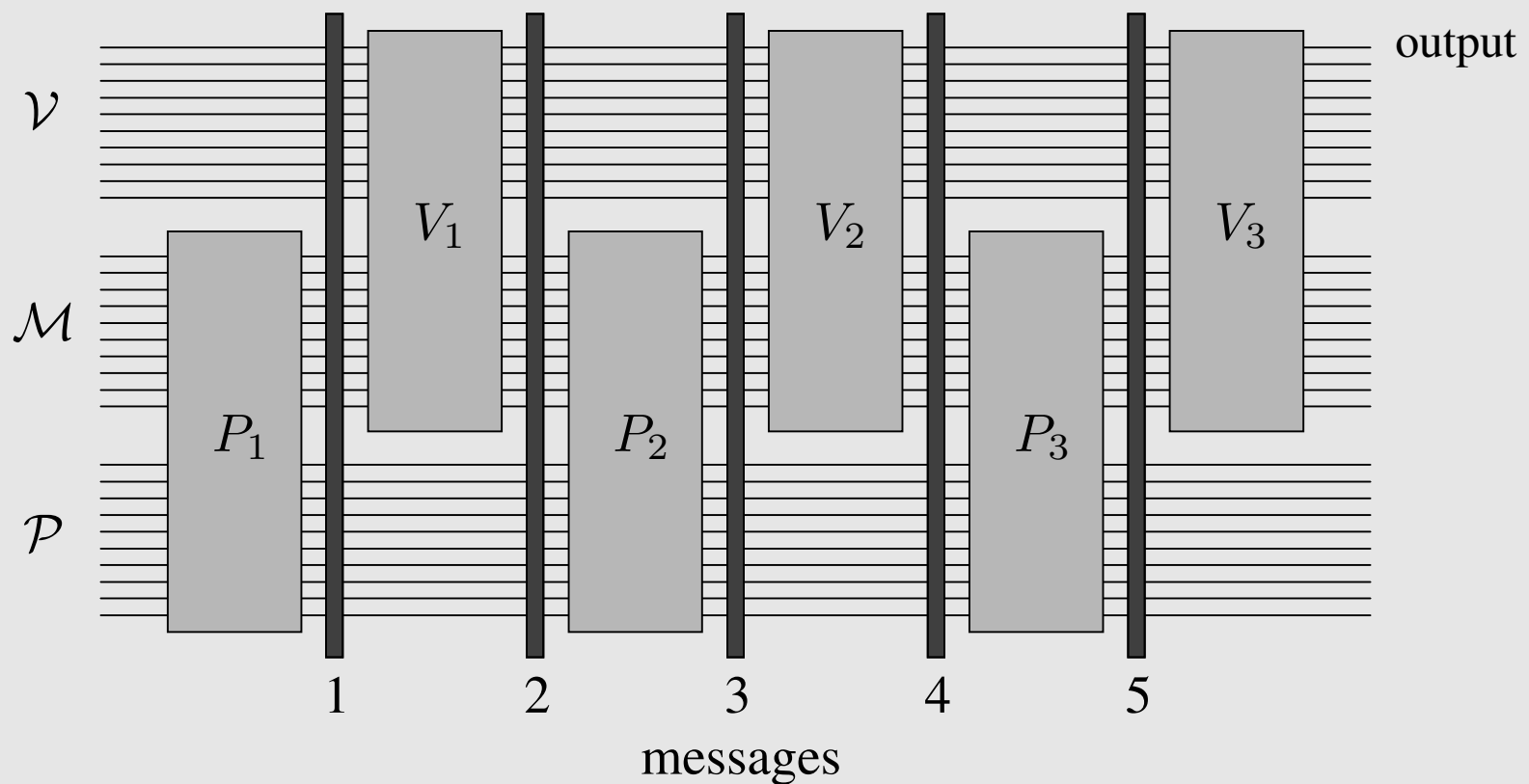
The **quantum interactive proof system** model works exactly the same as the classical model, except that the prover and verifier may **exchange and process quantum information**.

General assumptions and notions of completeness and soundness are unchanged. . .

# Quantum Interactive Proofs



# Circuit for Quantum Interactive Proof



# Complexity classes and known relations

Let  $\text{QIP}(m)$  denote the class of promise problems having  $m$  message quantum interactive proof systems. (Always assume the last message is from the prover to the verifier.)

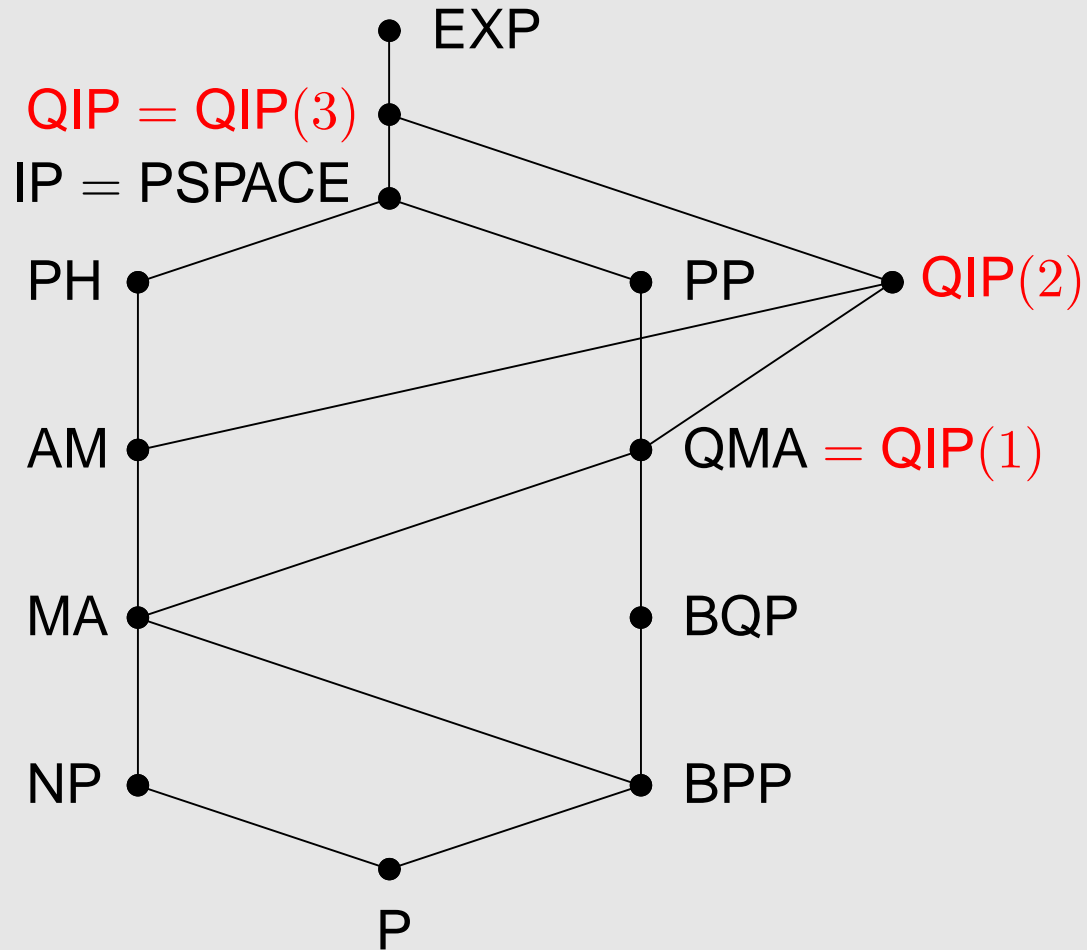
- For any  $m \geq 3$  it holds that

$$\text{QIP} \stackrel{\text{def}}{=} \text{QIP}(3) = \text{QIP}(m).$$

(This includes  $m = \text{poly.}$ )

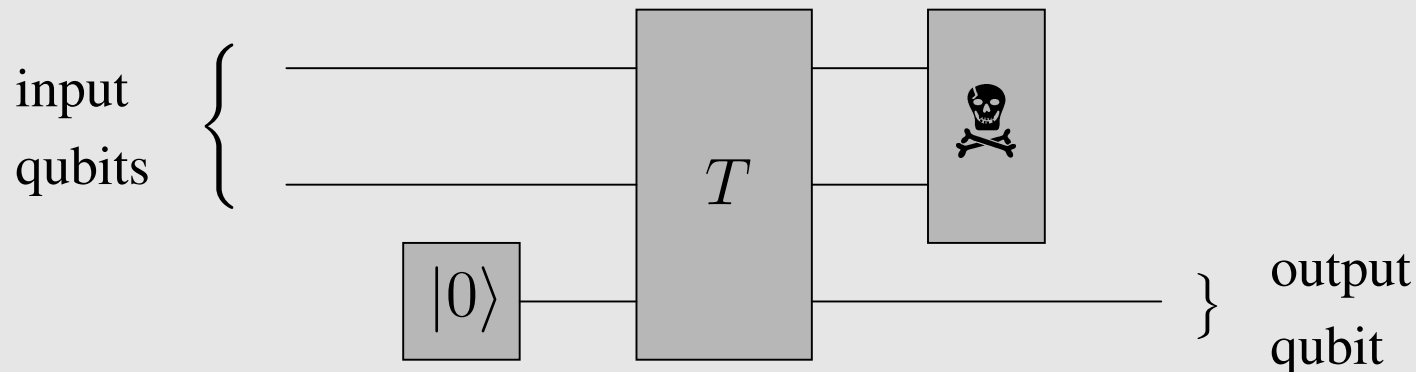
- It holds that  $\text{PSPACE} \subseteq \text{QIP} \subseteq \text{EXP}$ .
- We have already discussed  $\text{QIP}(1)$ ; it is better known as  $\text{QMA}$ ...
- Not too much is known about  $\text{QIP}(2)$  except trivialities...

# Diagram of Complexity Classes



# Connection to Admissible Maps

In the previous talk, we briefly discussed general (non-unitary) quantum circuits. Our example of a circuit of type  $(2, 1)$  was the following:



This circuit (call it  $Q$ ) induces a completely positive trace-preserving mapping (sometimes called an **admissible** mapping); if  $\rho$  is a density matrix on two qubits, then the output  $Q(\rho)$  is a density matrix on one qubit.

# A Simple Complete Problem for QIP

Given two admissible maps  $Q$  and  $R$  (with the same output dimension), define their **max-fidelity** as

$$F_{\max}(Q, R) = \max_{\rho, \xi} F(Q(\rho), R(\xi))$$

(maximum is over density matrices  $\rho$  and  $\xi$  of appropriate dimensions).

## CLOSE IMAGES

**Input:** Quantum circuits  $Q$  and  $R$  (of the same type).

**Yes:**  $F_{\max}(Q, R) = 1$ .

**No:**  $F_{\max}(Q, R) \leq 1/10$ .

# Complete Promise Problems

A promise problem  $A = (A_{\text{yes}}, A_{\text{no}})$  is **complete** for QIP if:

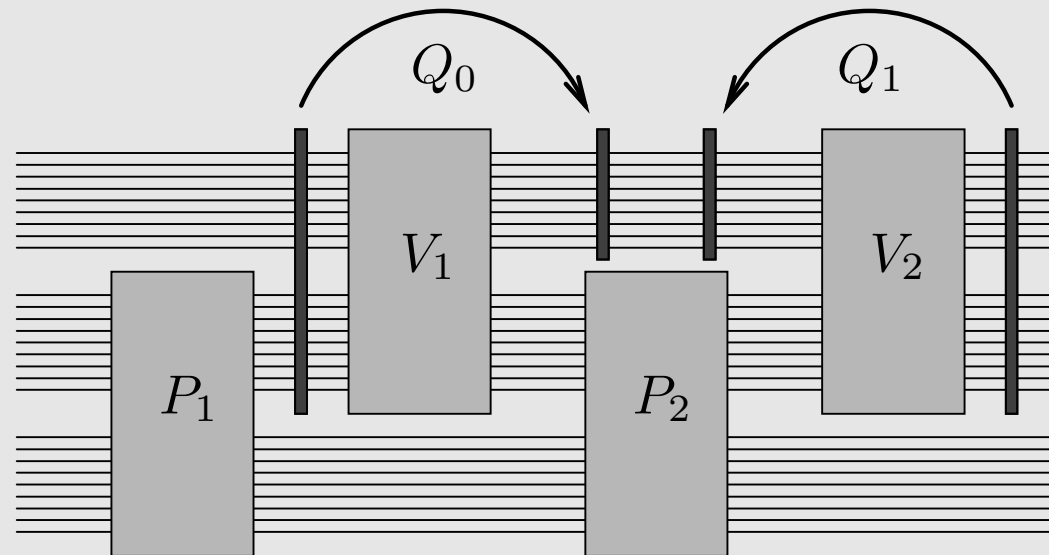
1.  $A$  is in QIP.
2. For every other promise problem  $B = (B_{\text{yes}}, B_{\text{no}})$  in QIP, there exists a polynomial-time computable function  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$  such that

$$x \in B_{\text{yes}} \Rightarrow f(x) \in A_{\text{yes}},$$

$$x \in B_{\text{no}} \Rightarrow f(x) \in A_{\text{no}}.$$

# Completeness of Close Images

Given a 3-message quantum interactive proof for some promise problem:



Circuits implementing  $Q_0$  and  $Q_1$  are easy to obtain given a description of  $V_1$  and  $V_2$ , and contain all the information we need:

$$\max_{P_1, P_2} \text{Prob}[V \text{ accepts}] = F_{\max}(Q_0, Q_1)^2$$

# Trace norm and distinguishability

The **trace norm** of a matrix  $X$  is the sum of the singular values of  $X$ . Equivalently,

$$\|X\|_{\text{tr}} = \text{tr} \sqrt{X^\dagger X}.$$

This norm relates closely to the probability with which two mixed states  $\rho_0$  and  $\rho_1$  can be distinguished:

Suppose  $\{E_0, E_1\}$  is any binary-valued measurement and  $\xi \in \{\rho_0, \rho_1\}$  is chosen uniformly. The probability the measurement correctly identifies  $\xi$  is at most

$$\frac{1}{2} + \frac{1}{4} \|\rho_0 - \rho_1\|_{\text{tr}}.$$

This bound is achieved for an optimal measurement.

# Circuit Distinguishability

Suppose we have two admissible maps  $Q_0$  and  $Q_1$ , both of type  $(n, m)$ .

Is there a similar notion of distance between  $Q_0$  and  $Q_1$  to the trace distance between mixed states  $\rho_1$  and  $\rho_2$ ?

One possibility: let the trace distance induce a norm on super-operators:

$$\|Q_0 - Q_1\|_{\text{tr}} = \max_{\xi} \|Q_0(\xi) - Q_1(\xi)\|_{\text{tr}}.$$

(Maximum over density matrices on  $n$  qubits.)

**Bad choice...**

## So close and yet so far...

Let  $Q_0$  and  $Q_1$  be mappings of type  $(n, n)$  defined as follows:

$$Q_0(X) = \frac{1}{2^n + 1} ((\text{tr } X)I + X^\top), \quad Q_1(X) = \frac{1}{2^n - 1} ((\text{tr } X)I - X^\top).$$

These are both admissible maps (and could be implemented by circuits).

For every mixed state  $\xi$  it holds that  $\|Q_0(\xi) - Q_1(\xi)\|_{\text{tr}} \leq \frac{4}{2^n + 1}$ .

Let

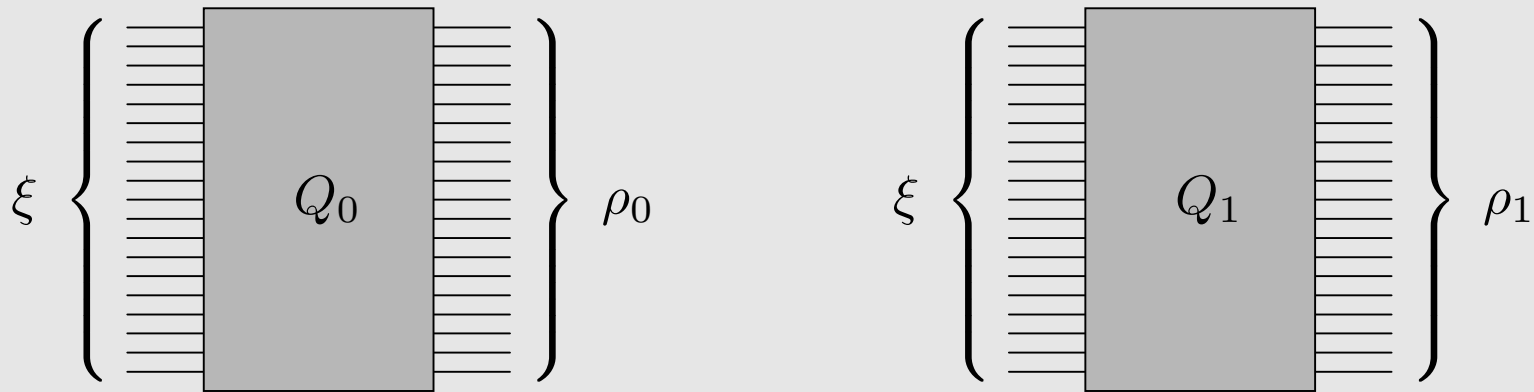
$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n - 1} |i\rangle |i\rangle.$$

Then

$$\|(Q_0 \otimes I)(|\psi\rangle \langle \psi|) - (Q_1 \otimes I)(|\psi\rangle \langle \psi|)\|_{\text{tr}} = 2;$$

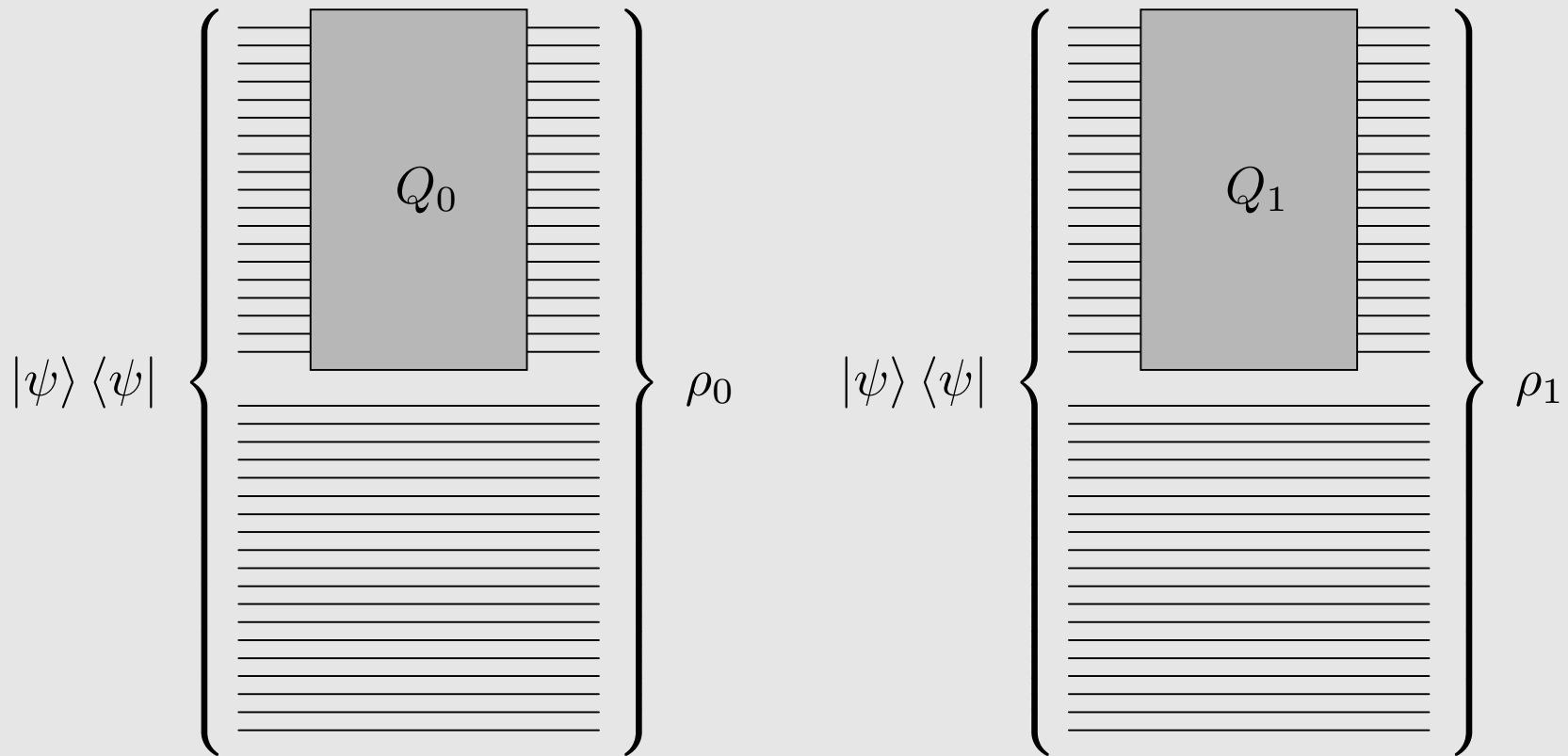
$(Q_0 \otimes I)(|\psi\rangle \langle \psi|)$  and  $(Q_1 \otimes I)(|\psi\rangle \langle \psi|)$  are **perfectly distinguishable!**

## So close and yet so far...



$$\rho_0 \approx \rho_1 \quad (\text{for any choice of } \xi)$$

# So close and yet so far...



$\rho_0 \perp \rho_1$  (i.e., they are perfectly distinguishable)

# Kitaev's "Diamond" Norm

Given two admissible maps  $Q_0$  and  $Q_1$ , both of type  $(n, m)$ , define

$$\begin{aligned}\|Q_0 - Q_1\|_{\diamond} &= \|Q_0 \otimes I_n - Q_1 \otimes I_n\|_{\text{tr}} \\ &= \max_{\xi} \|(Q_0 \otimes I_n)(\xi) - (Q_1 \otimes I_n)(\xi)\|_{\text{tr}}\end{aligned}$$

where  $I_n$  is the identity super-operator on  $n$  qubits, and the maximum is over all density operators  $\xi$  on  $2n$  qubits.

This norm is called the **diamond norm**, and it has several remarkable properties...

The **diamond-distance** between admissible maps may be viewed as the sensible analogue of the trace-distance between density operators.

# Quantum Circuit Distinguishability

Consider the following problem (where  $\varepsilon$  is a small positive constant).

## QUANTUM CIRCUIT DISTINGUISHABILITY

**Input:** Quantum circuits  $Q_0$  and  $Q_1$  (of the same type).

**Yes:**  $\|Q_0 - Q_1\|_{\diamond} \geq 2 - \varepsilon$ .

**No:**  $\|Q_0 - Q_1\|_{\diamond} \leq \varepsilon$ .

Informally, this problem asks whether two physical processes (described by quantum circuits) act nearly identically or not.

**Fact:** QUANTUM CIRCUIT DISTINGUISHABILITY is QIP-complete.

# Quantum Circuit Distinguishability

It is easy to show that QUANTUM CIRCUIT DISTINGUISHABILITY has a quantum interactive proof—we can use a blind taste-test:

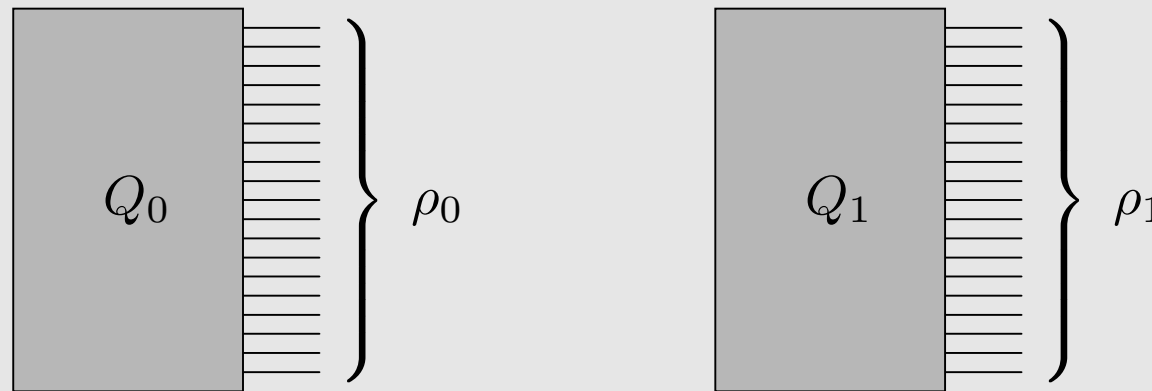
1. The prover prepares a state on which  $Q_0$  and  $Q_1$  (supposedly) differ, and sends the input qubits to the verifier.
2. The verifier randomly selects  $b \in \{0, 1\}$ , applies  $Q_b$  to the input qubits sent by the prover, and sends the prover the output qubits.
3. The prover is challenged to guess  $b$ ; the verifier accepts if the prover is correct and rejects if the prover is wrong.

The proof that this problem is as hard as every other problem in QIP will have to wait for another talk...

# State Distinguishability

We may also consider a restricted version of the QUANTUM CIRCUIT DISTINGUISHABILITY problem where there are no input qubits ...

**Input:** Quantum circuits  $Q_0$  and  $Q_1$  of type  $(0, n)$  for some  $n$ .

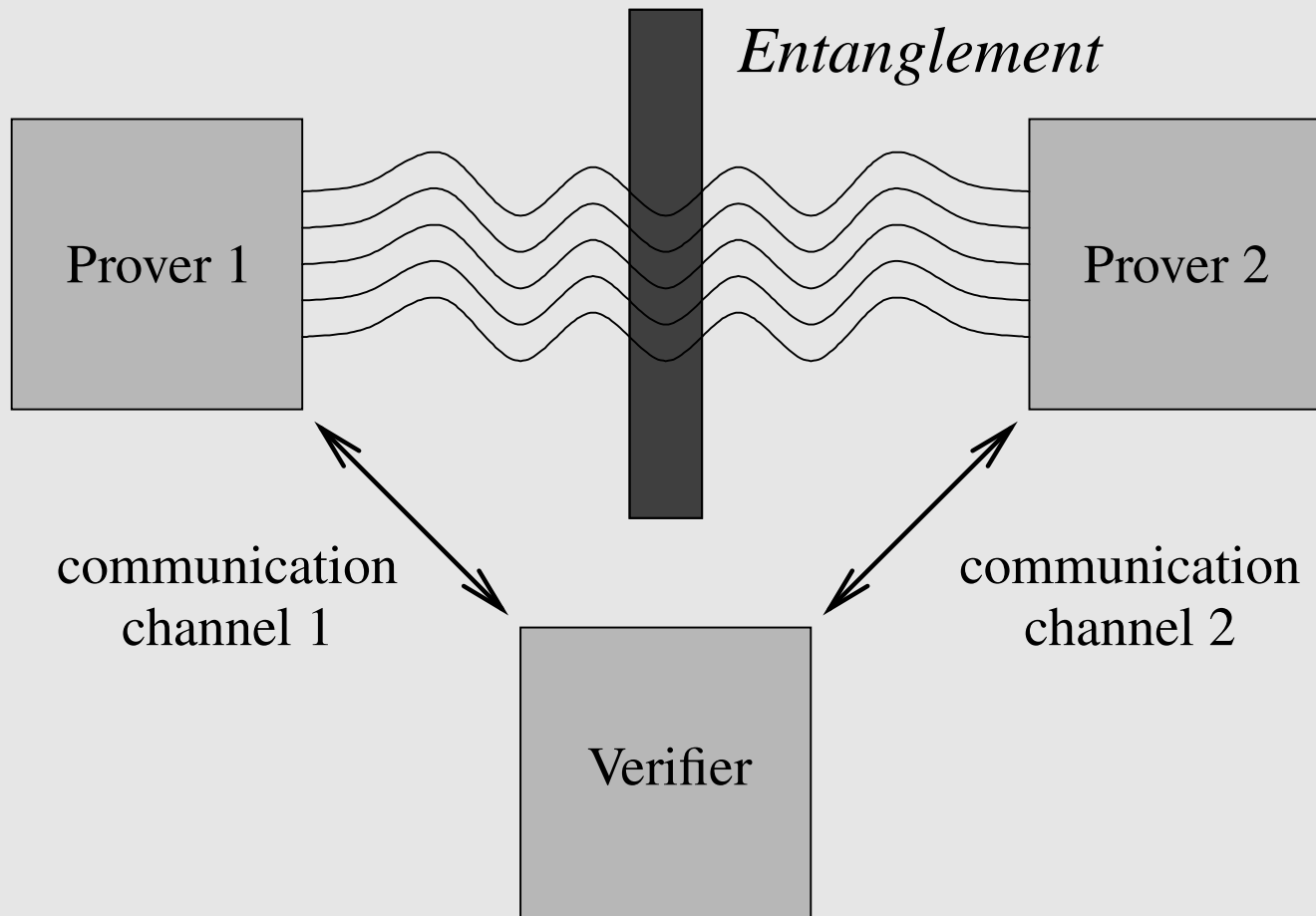


**Yes:**  $\|\rho_0 - \rho_1\|_{\text{tr}} \geq 2 - \varepsilon.$

**No:**  $\|\rho_0 - \rho_1\|_{\text{tr}} \leq \varepsilon.$

**Complete for (honest verifier) quantum statistical zero-knowledge.**

# Multiple Provers



# Multiple Provers

**Classical case:** multiple provers give a great deal of power;

$$\text{MIP} = \text{NEXP}$$

(where **MIP** is the class of problems having two-prover interactive proofs and **NEXP** is the class of problems solvable in nondeterministic exponential time). [BABAI, FORTNOW, & LUND, 1991]

**Quantum case:** We have no idea—**QMIP** could be more powerful, less powerful, or incomparable to **NEXP**.

# General Open Problems

1. Understand the power of multiple prover quantum interactive proofs.
2. Most questions about zero-knowledge remain unanswered—even known classical zero-knowledge protocols may not be zero-knowledge in a quantum world.
3. Give interesting relationships between quantum interactive proof system complexity classes and other complexity classes. What can be said about  $\text{QIP}(2)$ ?