Quantum Interactive Proofs

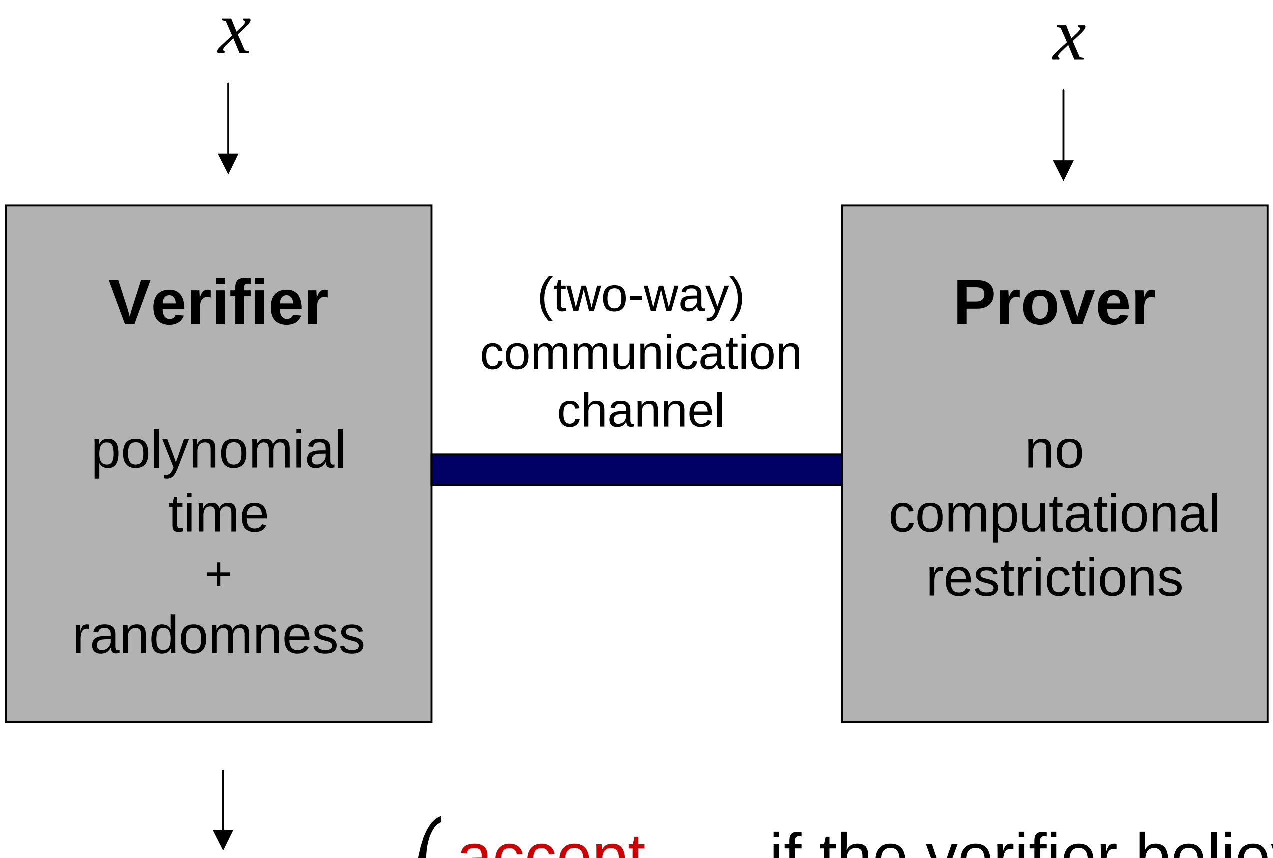
John Watrous
Department of Computer Science
University of Calgary

Interactive Proof Systems

Two parties, the **prover** and the **verifier**, have a conversation based on some common input string x.

- The prover has unlimited computation power.
- The verifier must run in polynomial time (and can flip coins).
- The prover wants the verifier to believe that the input x is in some fixed language L. The verifier wants to verify the validity of this claim.

Interactive Proof Systems



Output: $\begin{cases} \textbf{accept} & \text{if the verifier believes that } x \text{ is in } L \\ \textbf{reject} & \text{otherwise} \end{cases}$

Interactive Proof Systems

A language L has an interactive proof system if:

There exists a verifier V such that the following two conditions are satisfied.

1. (Completeness condition)

   If $x \in L$ then there exists a prover P that can convince V to accept x (with high probability).

2. (Soundness condition)

   If $x \notin L$ then no prover can convince V to accept x (except with small probability).

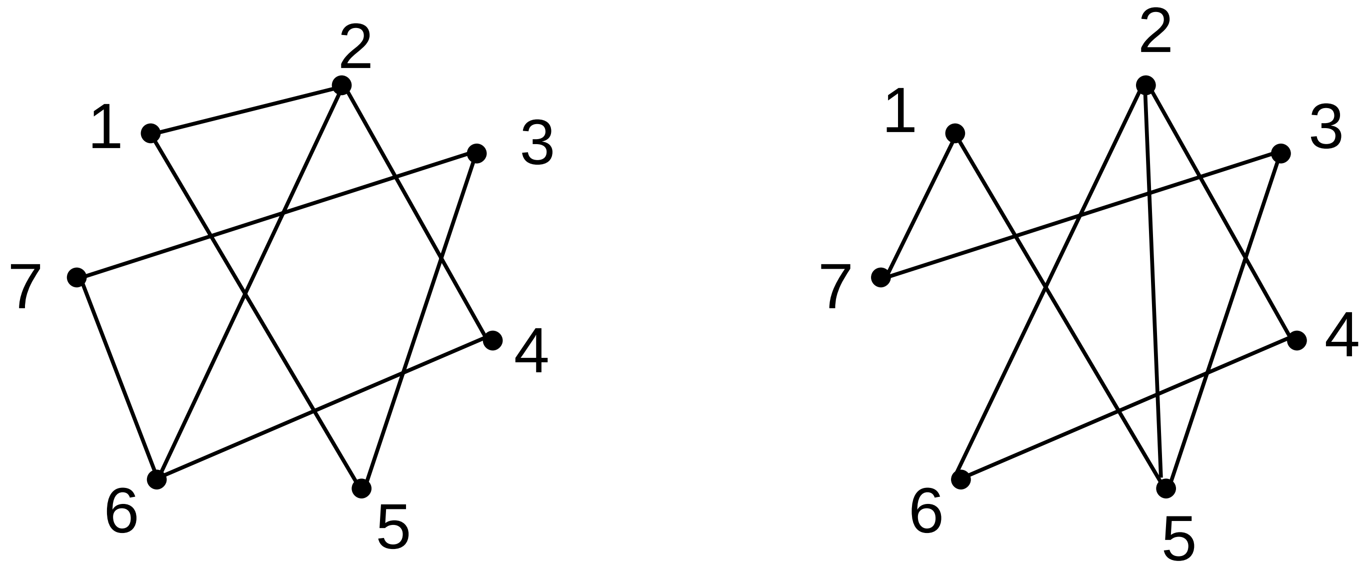
Example: Graph Non-Isomorphism

Suppose the input consists of two graphs:

G_1 and G_2 .

The prover wants to convince the verifier that

$G_1 \not\cong G_2$



G_1 G_2

Example: Graph Non-Isomorphism

The protocol:

1. The verifier randomly chooses one of the two graphs, randomly permutes it, and sends it to the prover.

2. The prover is challenged to identify whether the graph send by the verifier is isomorphic to the first or second input graph.

   The prover sends his guess to the verifier.

3. The verifier **accepts** if the prover correctly guesses the correct graph and **rejects** otherwise.

Which languages have interactive proof systems?

Let IP denote the class of languages that have interactive proof systems.

[Lund, Fortnow, Karloff, and Nisan, 1990] + [Shamir, 1990]:

$$IP = PSPACE$$

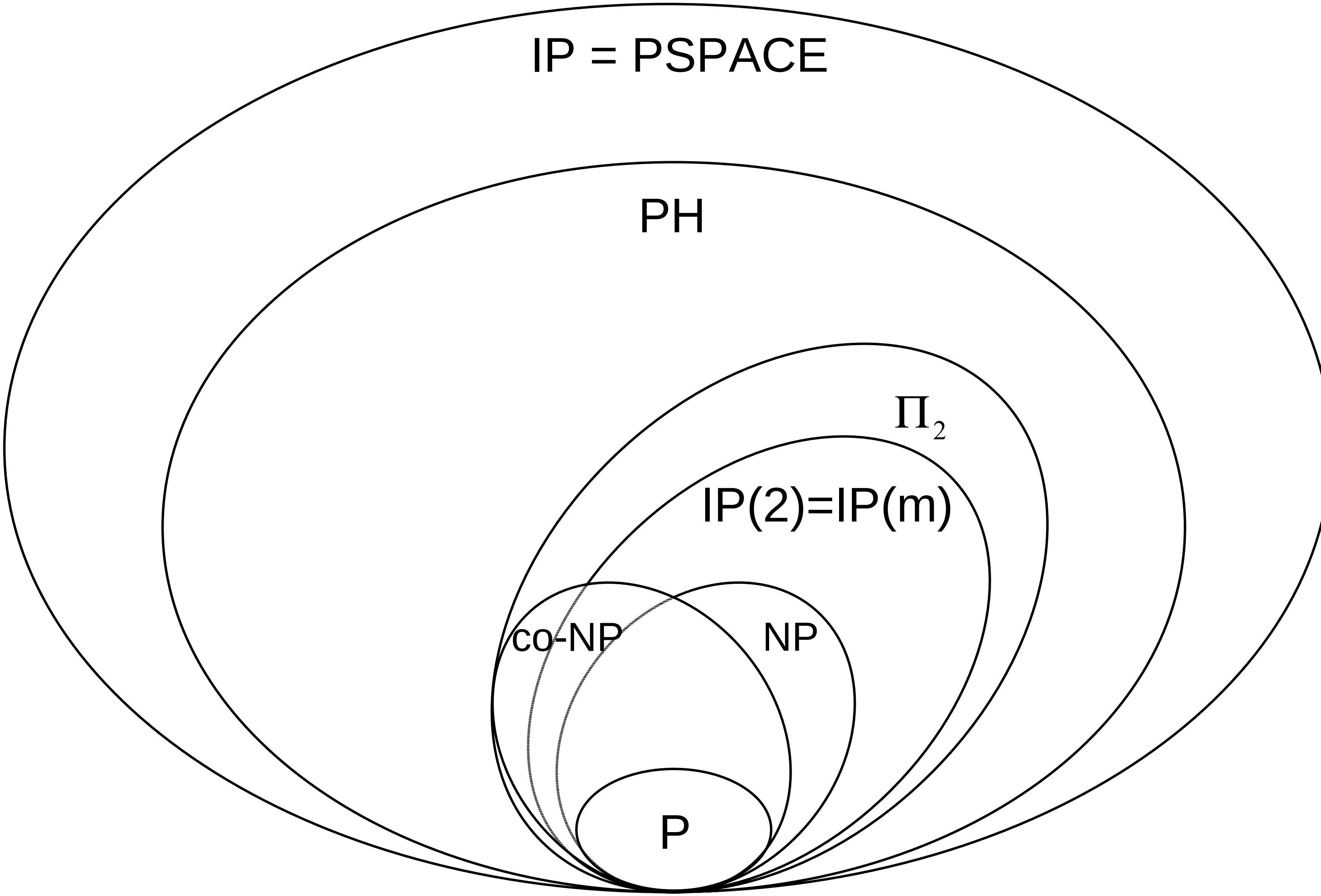
Let $IP(m)$ denote the class of languages having interactive proof systems where the total number of messages sent is at most m.

[Babai, 1985] + [Goldwasser and Sipser, 1989]:

$$IP(m) = IP(2) \subseteq \Pi_2$$

for any <u>constant</u> m.

Diagram of complexity classes

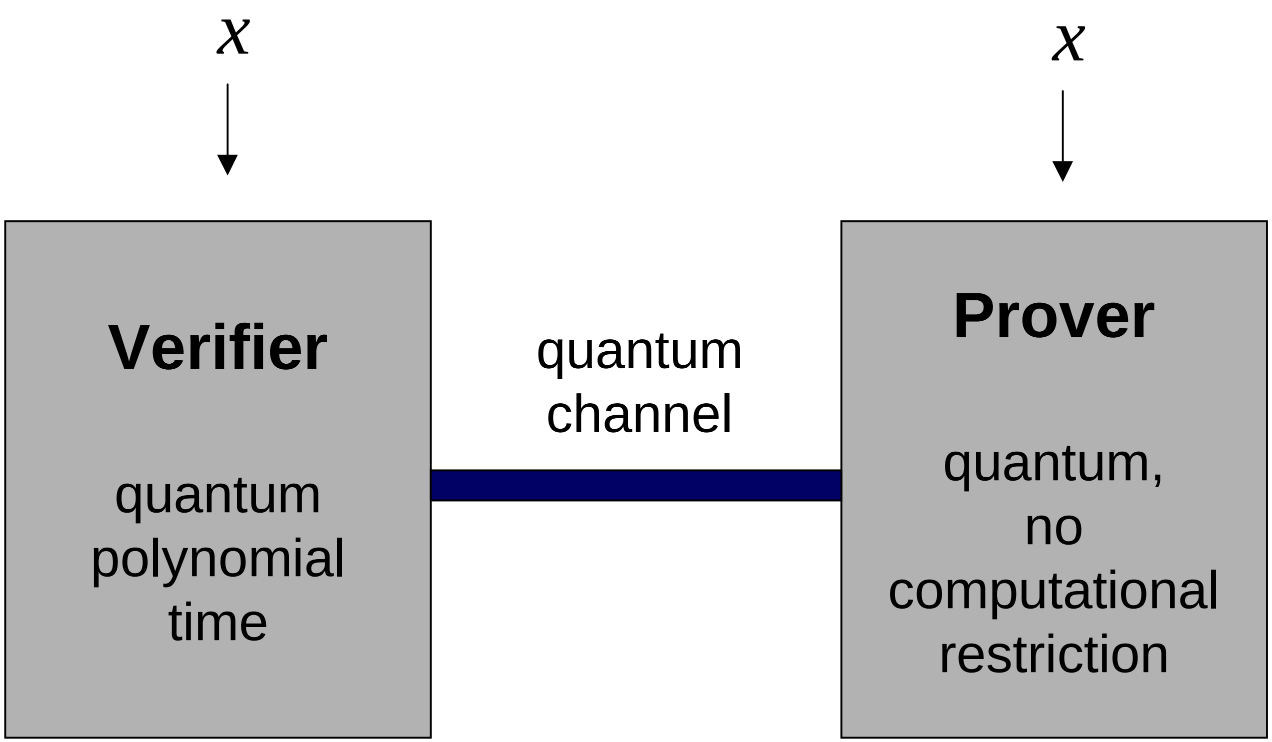


Quantum Interactive Proof Systems

As before, the **prover** and the **verifier** have a conversation based on some common input string x.

- The prover has unlimited quantum computing power.
- The verifier must be quantum polynomial-time.
- The prover and verifier have the same goals as before.

Quantum Interactive Proof Systems

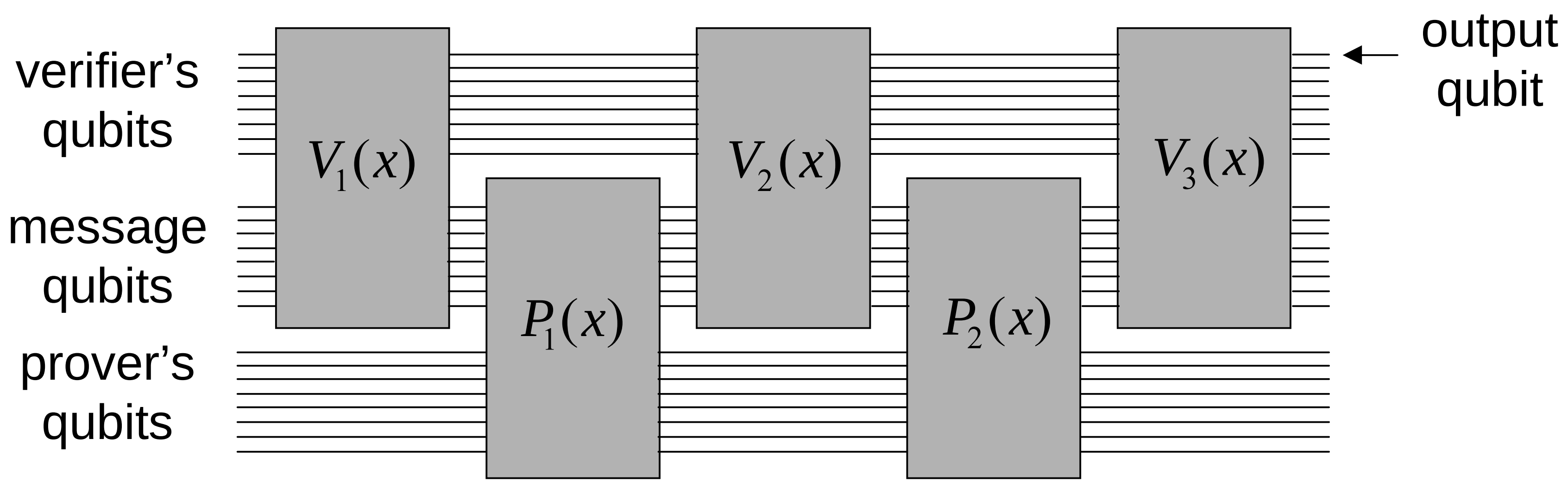


Output:

- accept — if the verifier believes that x is in L
- reject — otherwise

Formalizing the model

We use the quantum circuit model. Example of a circuit for a 4-message quantum interactive proof system:



Complexity Classes

QIP(m) = class of languages having quantum interactive proofs with m messages.

Facts

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

$$PSPACE \subseteq QIP \subseteq EXP$$

In contrast:

$$IP(poly) = PSPACE$$

$$IP(const) \ = \ IP(2) \ = AM \subseteq \Pi_2$$

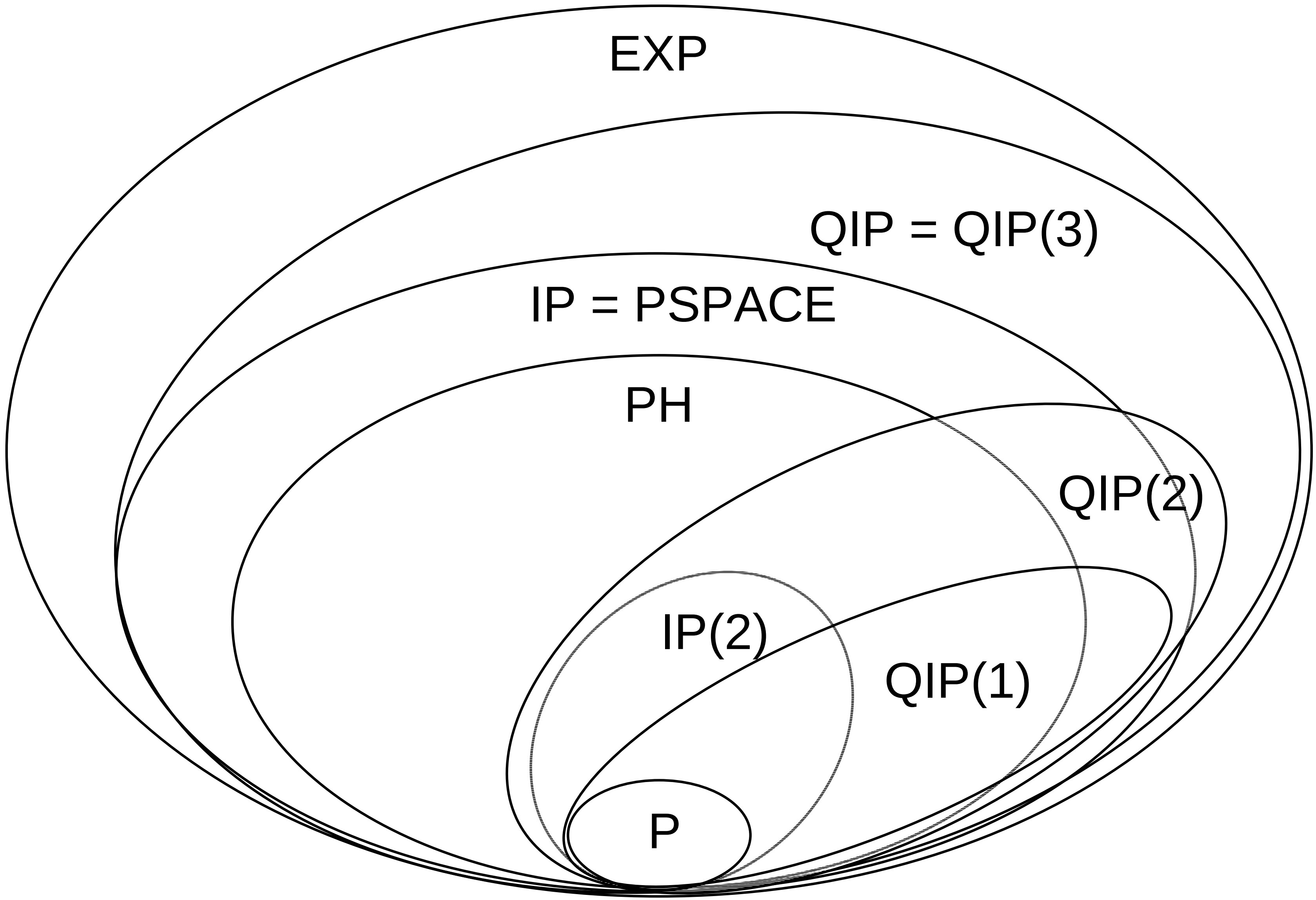
Facts

$$QIP(1) \stackrel{\text{def}}{=} QMA \subseteq PP$$

QMA contains some problems not known to be in MA (i.e., NP with a probabilistic verifier).

$$QIP(2) \quad ???$$

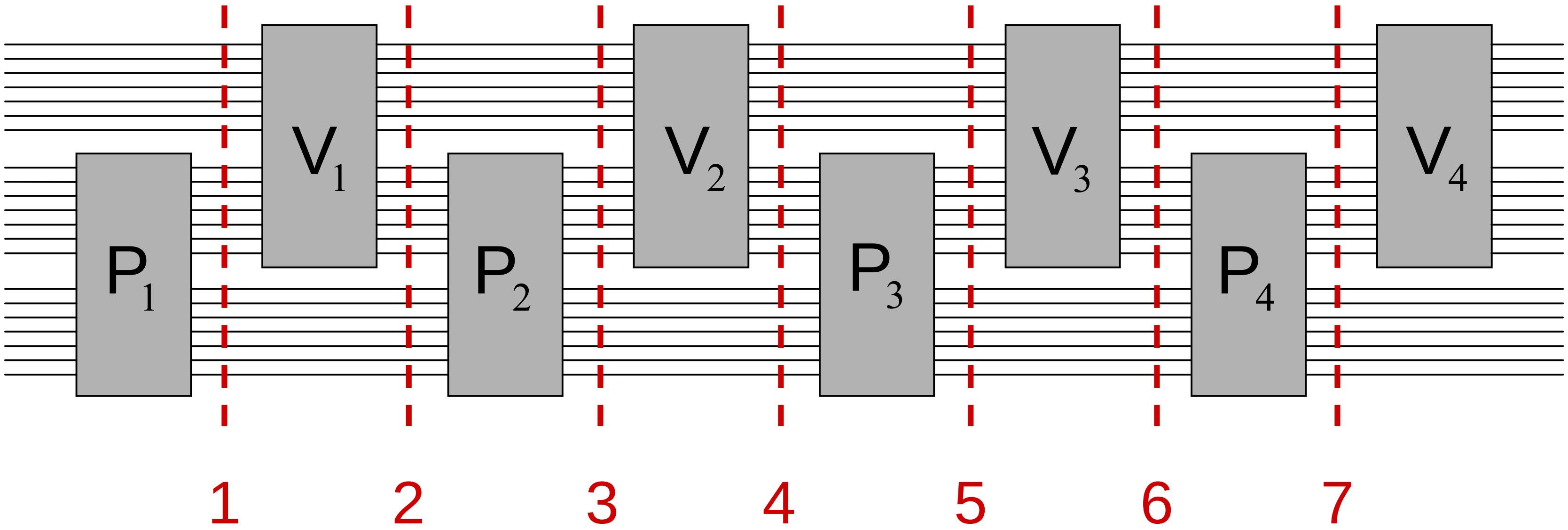
Diagram of complexity classes



Parallelizing quantum interactive proofs

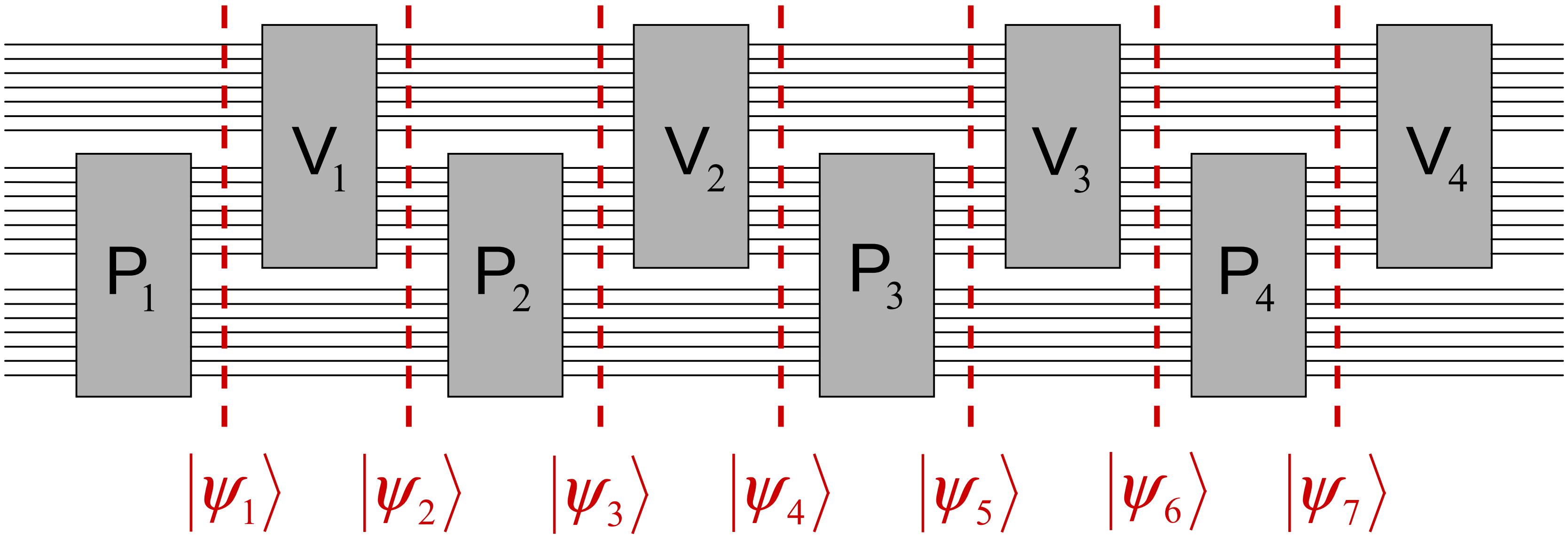
Suppose we have a quantum interactive proof consisting of several rounds:

messages:



Parallelizing quantum interactive proofs

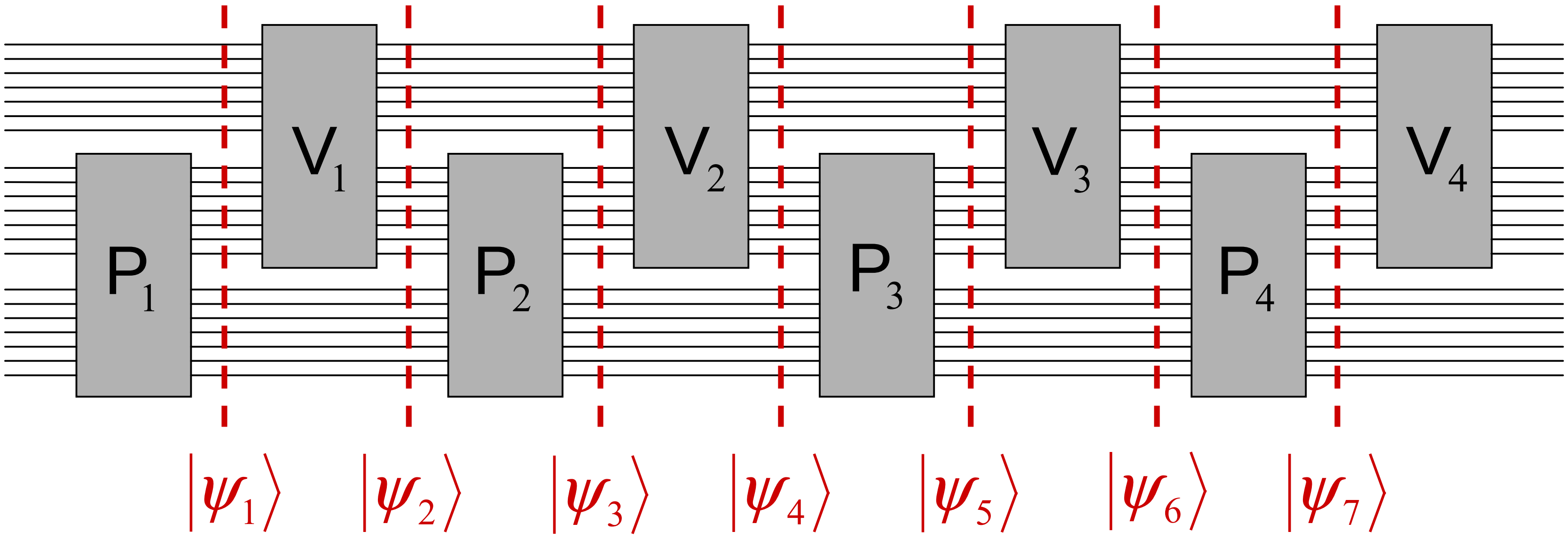
Consider the states of the system during some execution (optimal for the prover):



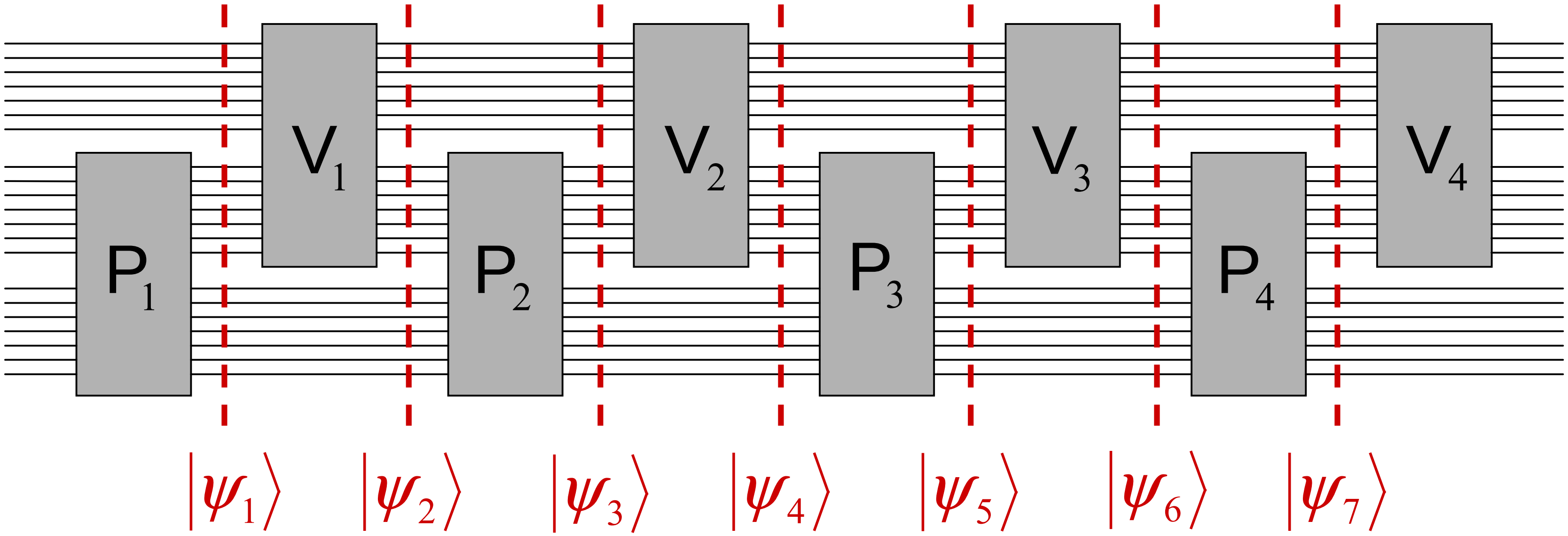
Parallelizing quantum interactive proofs

Message 1 (of parallelized protocol):

The prover sends $|\psi_1\rangle, \ldots, |\psi_m\rangle$ to the verifier.



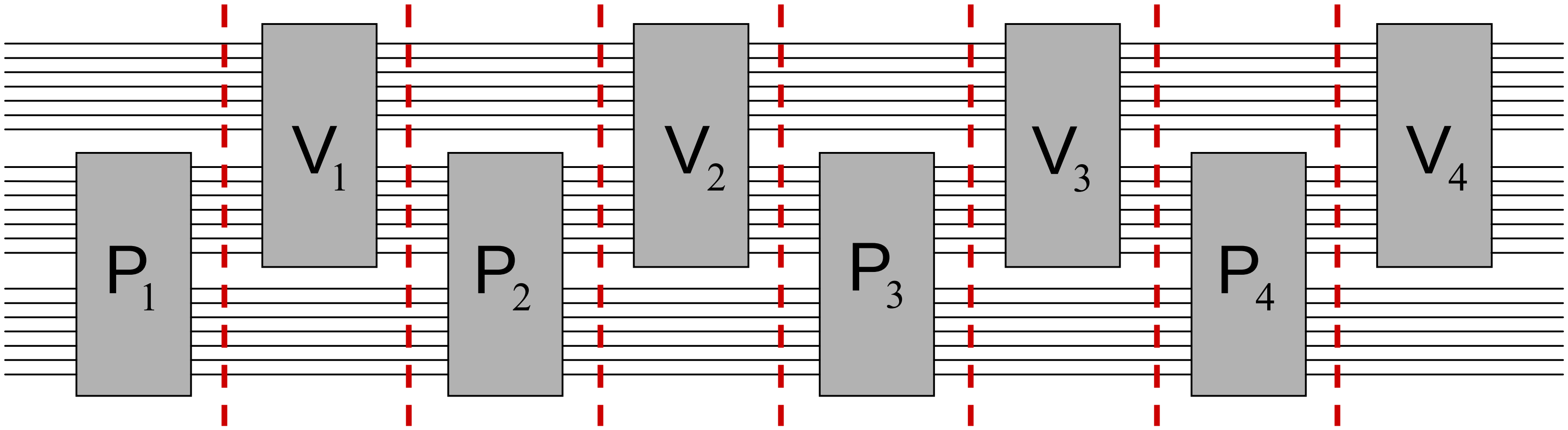
Parallelizing quantum interactive proofs



The verifier now needs to check that these states are consistent with one another…

… this will require 2 additional messages.

Parallelizing quantum interactive proofs

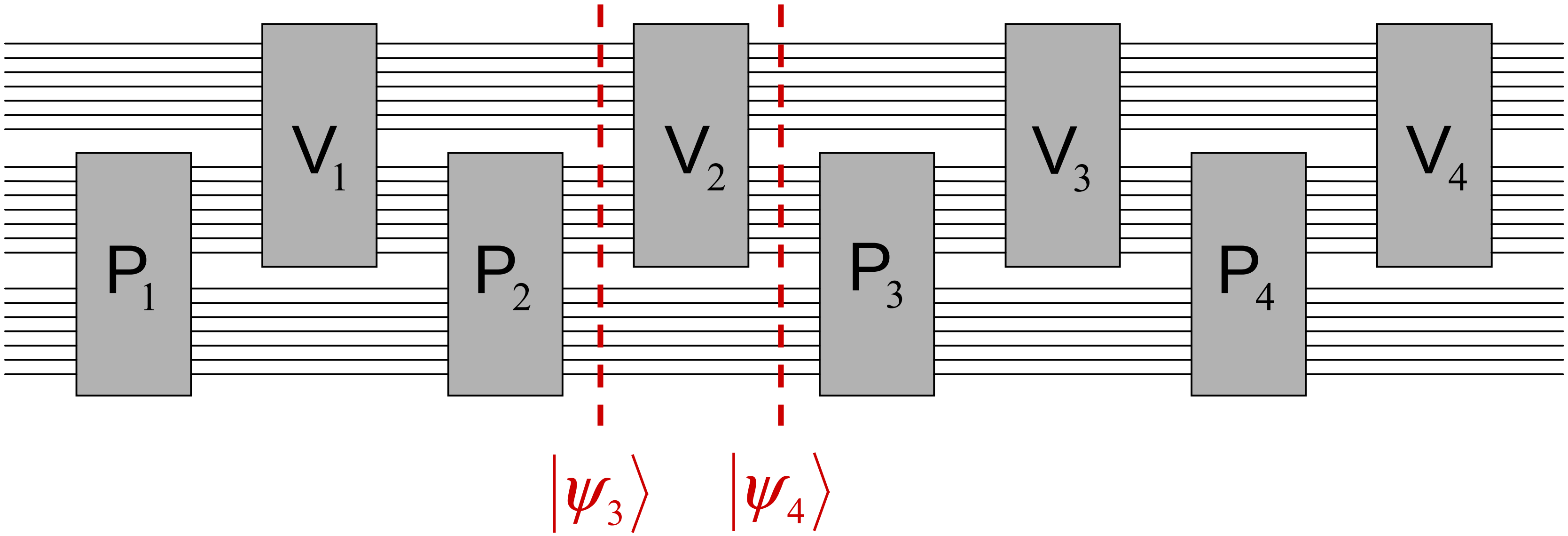


$|\psi_1\rangle$ $|\psi_2\rangle$ $|\psi_3\rangle$ $|\psi_4\rangle$ $|\psi_5\rangle$ $|\psi_6\rangle$ $|\psi_7\rangle$

The verifier randomly chooses 2 consecutive states to test for consistency.

Case 1: states are separated by a verifier transformation.

Parallelizing quantum interactive proofs



The verifier randomly chooses 2 consecutive states to test for consistency.

Case 1: states are separated by a verifier transformation.

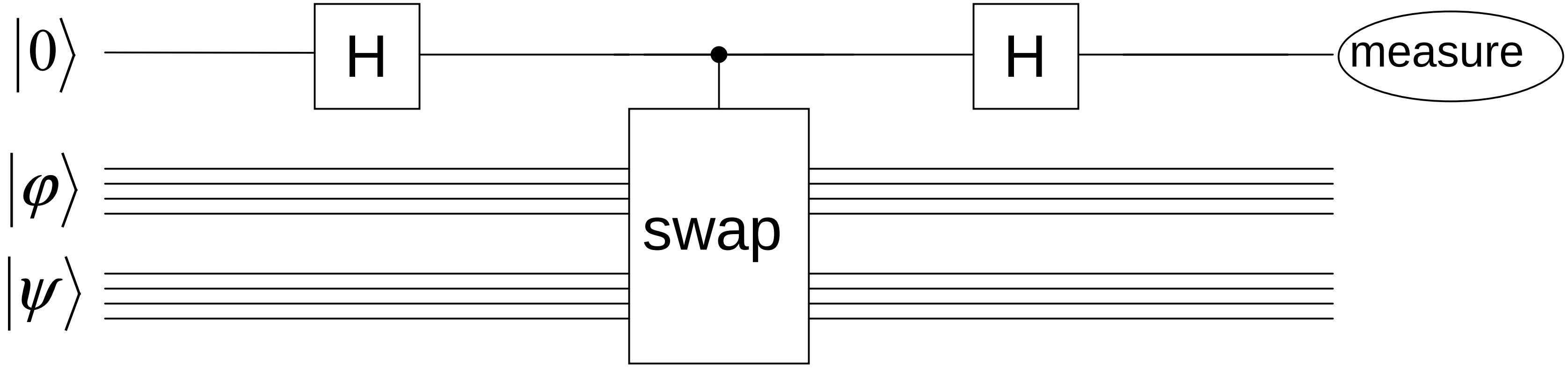
Easy

Swap test

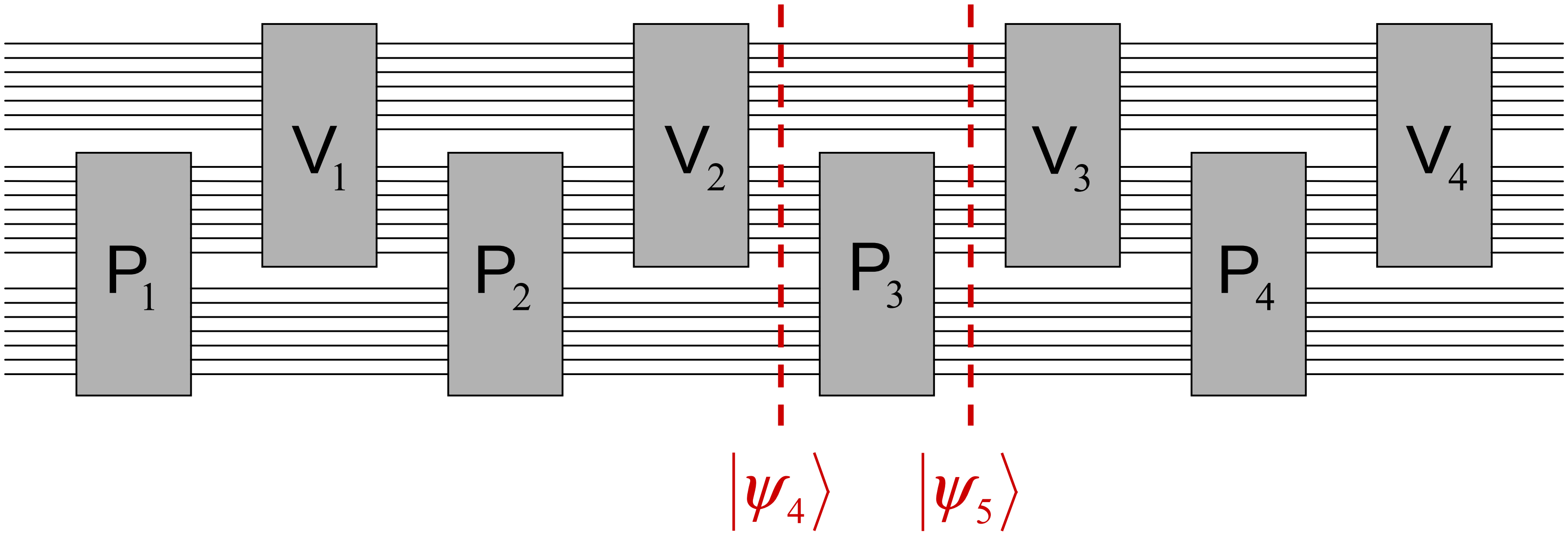
Suppose we have two (pure) quantum states:

$$|\varphi\rangle \quad \text{and} \quad |\psi\rangle$$

Want to know if they are close together or far apart.

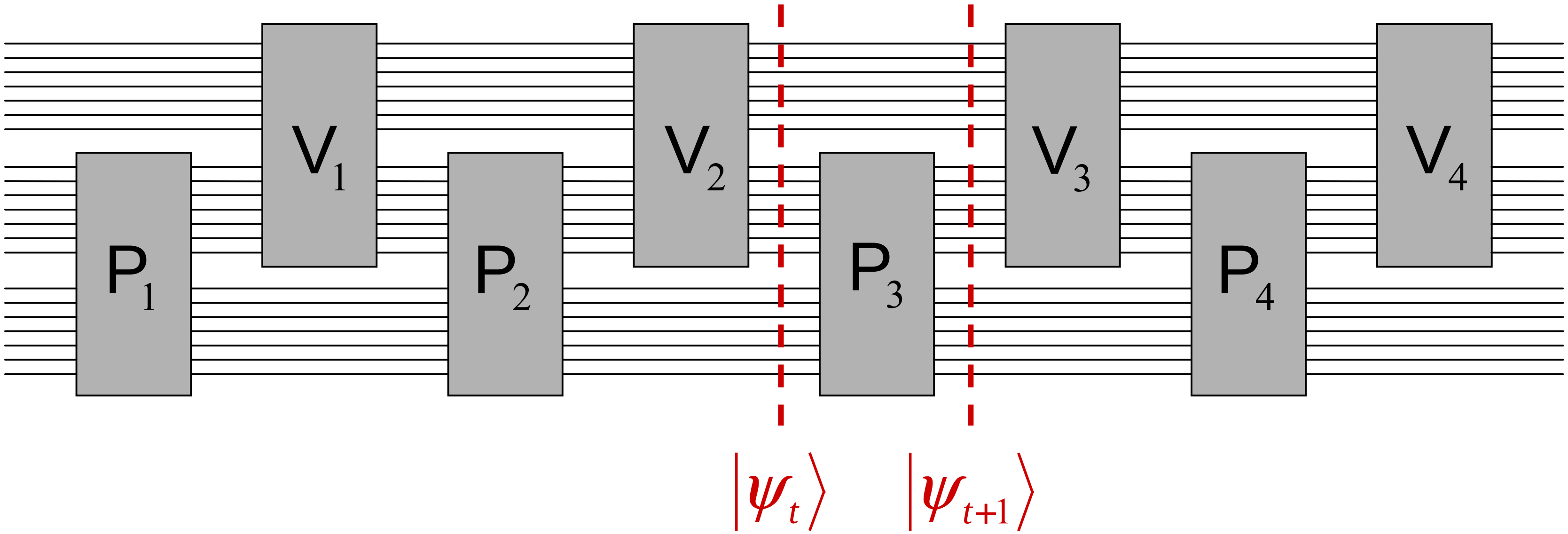


Parallelizing quantum interactive proofs



Case 2: states are separated by a <u>prover</u> transformation.

Parallelizing quantum interactive proofs



Messages 2 and 3 (of parallelized protocol):

Verifier sends the message and private prover qubits of $|\psi_t\rangle$ to the prover… the prover is challenged to convert $|\psi_t\rangle$ to $|\psi_{t+1}\rangle$.

Parallelizing quantum interactive proofs

It turns out that this works. (Proof is not hard, but relies heavily on the quantum formalism.)

A cheating prover will be caught with probability at least

$$\frac{c}{m^2}$$

for some constant c.

Parallel repetition can be used to reduce soundness error to be exponentially small… still only use 3 messages.

Bipartite Quantum States

Suppose $|\psi\rangle$ and $|\varphi\rangle$ are bipartite quantum states

$$|\psi\rangle, |\varphi\rangle \in \mathrm{H}_1 \otimes \mathrm{H}_2$$

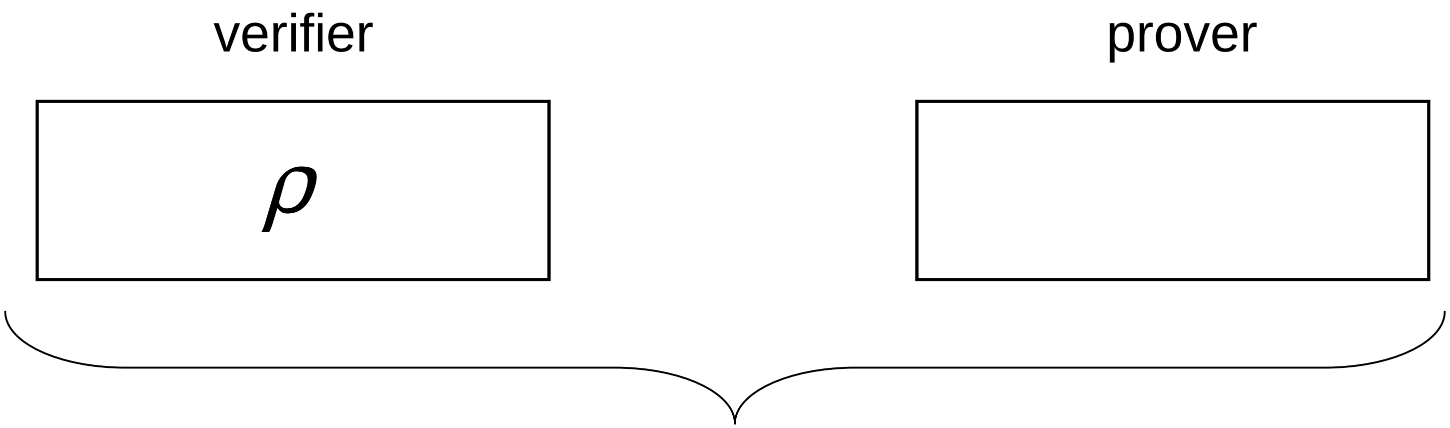
that would "look the same" if H_2 were discarded:

$$\mathrm{tr}_{\mathrm{H}_2} |\psi\rangle\langle\psi| = \mathrm{tr}_{\mathrm{H}_2} |\varphi\rangle\langle\varphi|$$

Then there exists a unitary operator U acting only on H_2 such that

$$(I \otimes U)|\psi\rangle = |\varphi\rangle$$

Options for the Prover



$$|\psi\rangle \quad \alpha \quad |\varphi\rangle$$

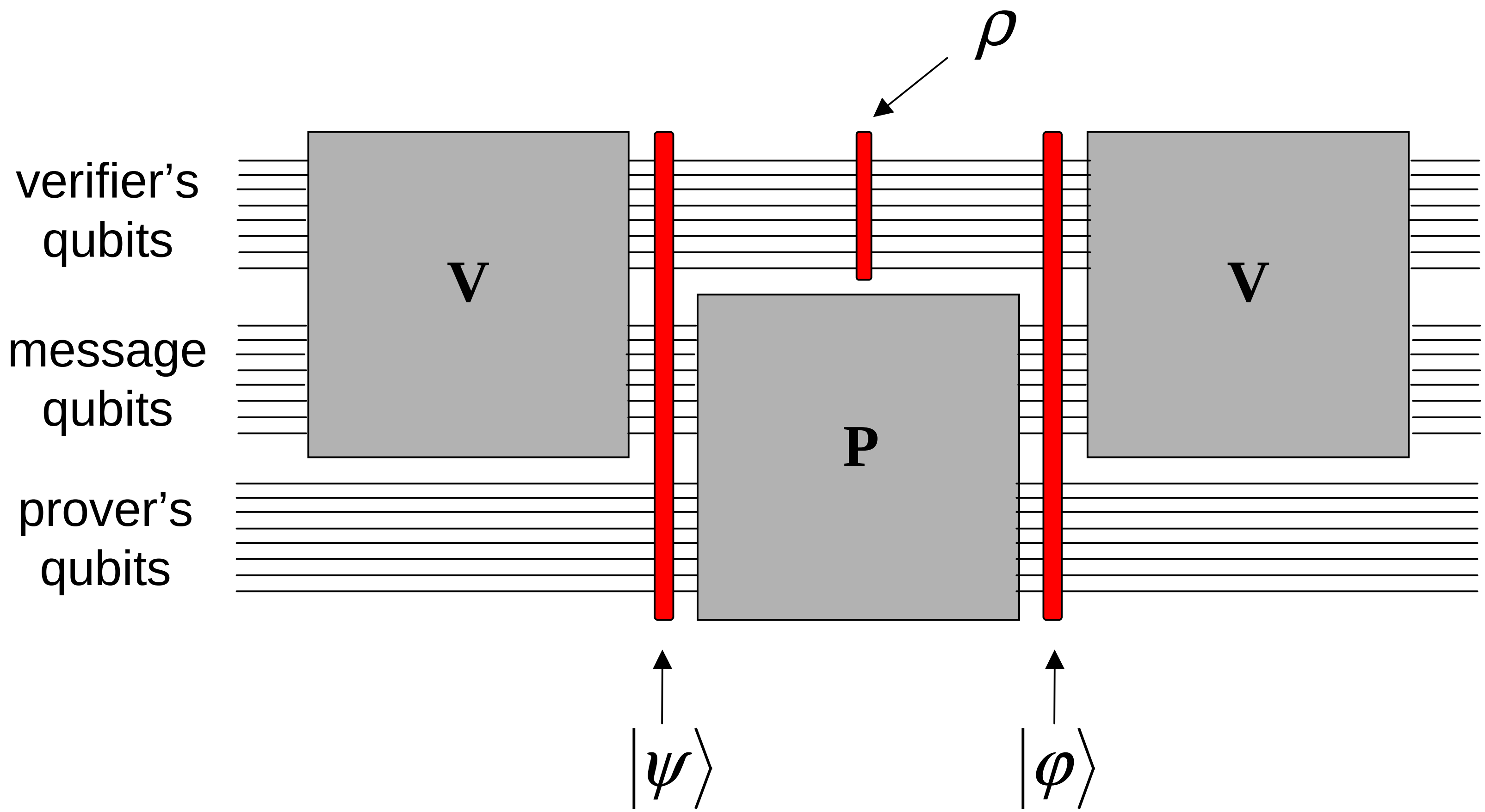
Mixed state of the verifier's qubits:

$$\rho = \mathrm{tr}_{\mathrm{prover}} |\psi\rangle\langle\psi| \;\; = \mathrm{tr}_{\mathrm{prover}} |\varphi\rangle\langle\varphi|$$

Question: what freedom does the prover have in changing the state of the system?

Answer: the prover can change the state to **any** $|\varphi\rangle$ that leaves the verifier with mixed state ρ .

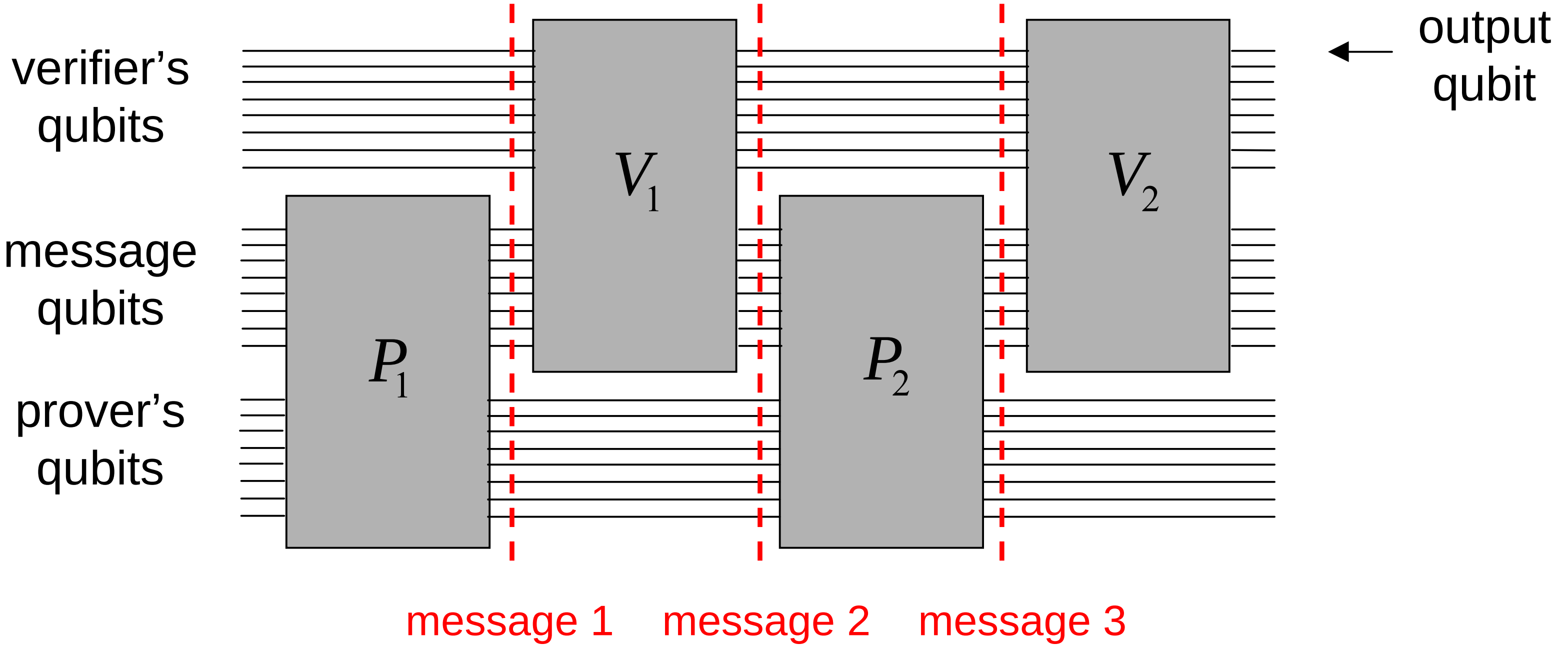
Options for the Prover



Prover can transform $|\psi\rangle$ to $|\varphi\rangle$ for any $|\varphi\rangle$ that leaves the verifier's qubits in state ρ .

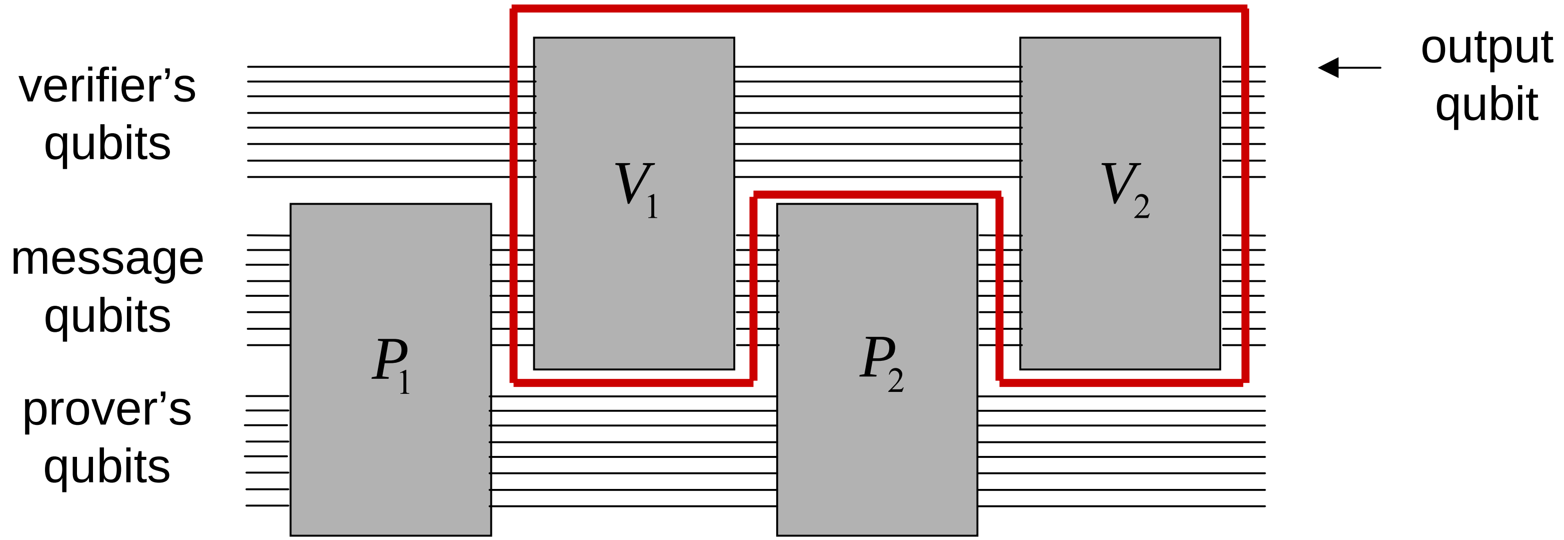
Simulating QIP in EXP

We know *QIP* = *QIP(3)*, so we can focus on 3-message proof systems:



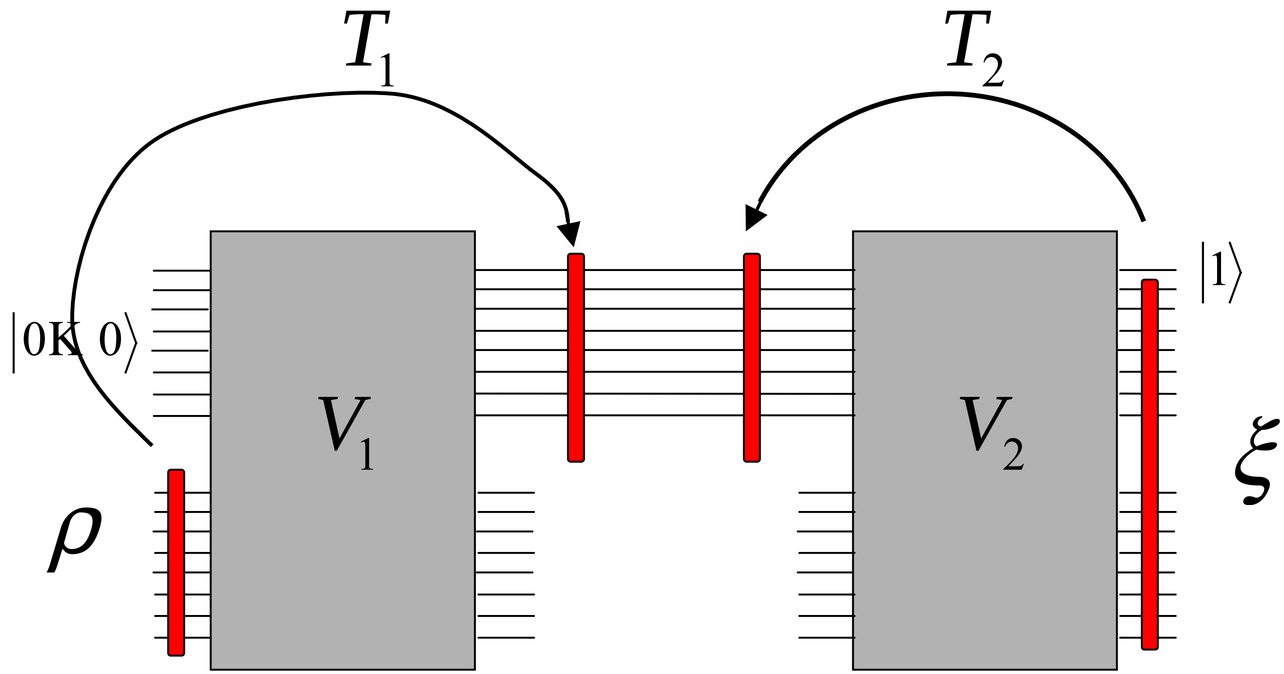
We want to approximate the **maximum probability** with which a prover can convince the verifier to accept.

Simulating QIP in EXP



Based on what we know about bipartite quantum states, we can focus on just this part of the system, and completely remove the prover from the picture.

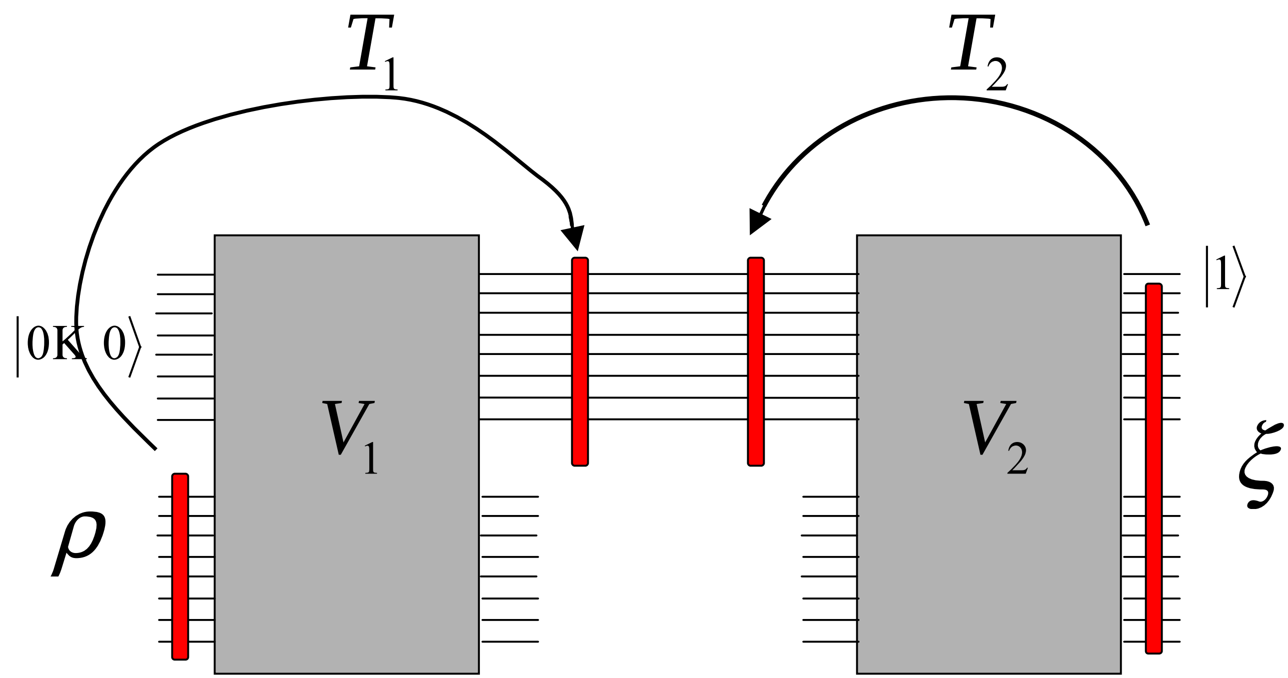
Simulating QIP in EXP



maximum probability of acceptance $= \max_{\rho,\xi} F(T_1(\rho), T_2(\xi))^2$

$$F(\sigma,\tau) = \mathrm{Tr}\sqrt{\sqrt{\sigma}\,\tau\,\sqrt{\sigma}} = \mathrm{Tr}\left|\sqrt{\sigma}\sqrt{\tau}\right|$$

Simulating QIP in EXP



maximum probability of acceptance $= \max_{\rho,\xi} F(T_1(\rho), T_2(\xi))^2$

This can be approximated by an exponential-size semidefinite programming problem.

One-message quantum proof systems

We may also consider quantum interactive proofs where there is no interaction:

"Quantum NP"

Are there properties having succinct quantum proofs but not succinct classical proofs?

The Group Non-Membership Problem

Given elements in some finite group:

$$g_1, \ldots, g_k \quad \text{and} \quad h$$

The property we will be interested in:

"h <u>cannot</u> be generated from $g_1, \ldots, g_k$"

Concrete Example

Invertible matrices mod 7:

$$g_1 = \begin{pmatrix} 1 & 4 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix} \qquad g_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \qquad g_3 = \begin{pmatrix} 1 & 6 & 3 \\ 1 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}$$

$$h = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 0 \\ 5 & 0 & 1 \end{pmatrix}$$

Interested in whether h can be generated from $g_1, g_2, \text{and } g_3$.

Succinct Proofs for Non-Membership?

- In the case of **matrix groups**, it is not known if non-membership has succinct (classical) proofs.

- For **black-box groups**, non-membership provably does <u>not</u> have succinct (classical) proofs.

- For **all groups**, non-membership <u>does</u> have succinct quantum proofs.

Quantum Proofs for Non-Membership

Let

$$G = \langle g_1, \ldots, g_k \rangle.$$

Write

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle$$

$|G\rangle$ is a quantum proof that $h \notin G$ (for <u>any</u> $h \notin G$).

Note: it may be very difficult to construct $|G\rangle$.

Quantum Proofs for Non-Membership

Suppose we have $|G\rangle$ (in some register **R**).
Then we can test membership in G as follows:

- Prepare a new qubit **B** in state

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

State of the entire system:

$$\frac{1}{\sqrt{2}}|0\rangle|G\rangle + \frac{1}{\sqrt{2}}|1\rangle|G\rangle$$

Quantum Proofs for Non-Membership

2. Perform a "controlled-multiply-by-h" operation on **R** (using **B** as the control).

State of system:

$$\frac{1}{\sqrt{2}}|0\rangle|G\rangle + \frac{1}{\sqrt{2}}|1\rangle|hG\rangle$$

Quantum Proofs for Non-Membership

3. Perform a Hadamard transform on **B**.

$$H : |0\rangle \;\alpha\; \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \qquad H : |1\rangle \;\alpha\; \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

State of system:

$$\frac{1}{2}|0\rangle\big(|G\rangle + |hG\rangle\big) + \frac{1}{2}|1\rangle\big(|G\rangle - |hG\rangle\big)$$

4. Measure **B**.

$$\Pr[\text{result is } 1] = \begin{cases} 0 & \text{if} \quad h \in G \\ 1/2 & \text{if} \quad h \notin G \end{cases}$$

(Can repeat to reduce probability of error.)

Quantum Proofs for Non-Membership

Problem: we cannot trust that **R** really is in state $|G\rangle$.

Before performing the membership test on h, do the following (several times):

- Choose a random element g in G.
- Run the membership test on g.
- If the result is "not a member", then output "invalid proof".

(If the result is "is a member", then proceed with the next iteration.)

Open Questions

There are many variants of (classical) interactive proof systems:

- interactive proofs with stronger restrictions on the verifier (or on the prover).
- multi-prover interactive proof systems
- multiple competing provers
- probabilistically checkable proofs
- zero-knowledge

General problem:

How do quantum versions of these proof systems compare to the classical case?

(Quantum versions of some of these have been studied.)

Open Questions

What else can be said about relations between quantum interactive proof system classes and other complexity classes?

What can be said about $QIP(2)$?

Does graph non-isomorphism have succinct quantum proofs?