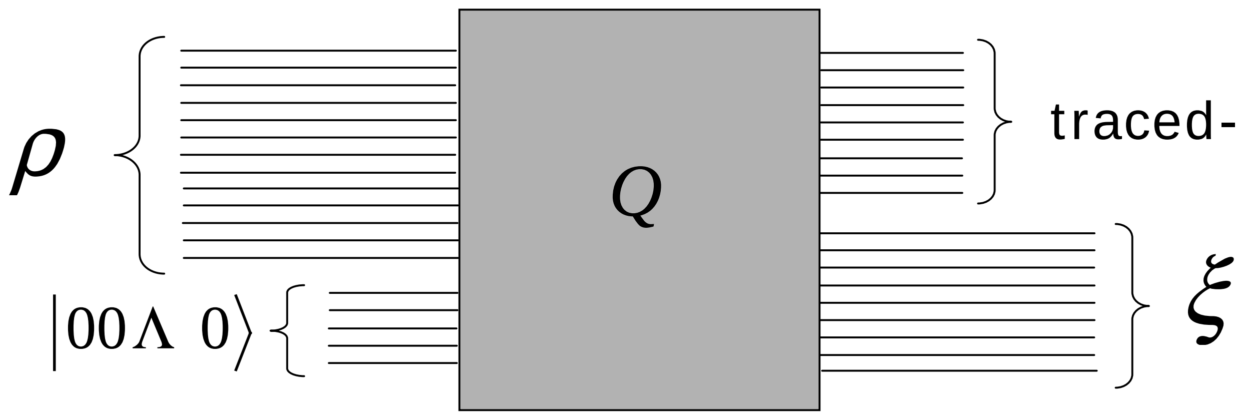
Capturing quantum complexity classes via quantum channels

John Watrous
Department of Computer Science
University of Calgary

Quantum channels

In this talk, a quantum channel is just a trace-preserving, completely positive mapping from n qubits to k qubits.

Described by (unitary) quantum circuits:



$$T(\rho)=\xi$$

General type of problem

We'll be interested in the following general type of computational problem:

Input: classical description of one or more quantum channels

Promise: some guarantee on the properties of the channel or channels.

Output: "yes" or "no"

Example problem #1: can the output be close to totally mixed?

Input: a quantum channel T.

Promise: one of the following holds:

(1) there exists an input ρ such that:

$$\boxed{F(\sigma,\tau) = \mathrm{Tr}\sqrt{\sqrt{\sigma}\,\tau\sqrt{\sigma}}}$$

$$F\left(T(\rho), 2^{-k} I\right) > 1 - \varepsilon$$

(2) for every input ρ:

$$F\left(T(\rho), 2^{-k} I\right) < \varepsilon$$

Output: "yes" if (1) holds, "no" if (2) holds.

Example problem #1: can the output be close to totally mixed?

Shorthand for same problem:

Input: a quantum channel T.

Yes: there exists an input ρ such that:

$$F\left(T(\rho), 2^{-k} I\right) > 1 - \varepsilon$$

No: for every input ρ:

$$F\left(T(\rho), 2^{-k} I\right) < \varepsilon$$

Example problem #2: outputs close together?

Input: two quantum channels T_1 and T_2 .

Yes: there exist states ρ and ξ such that:

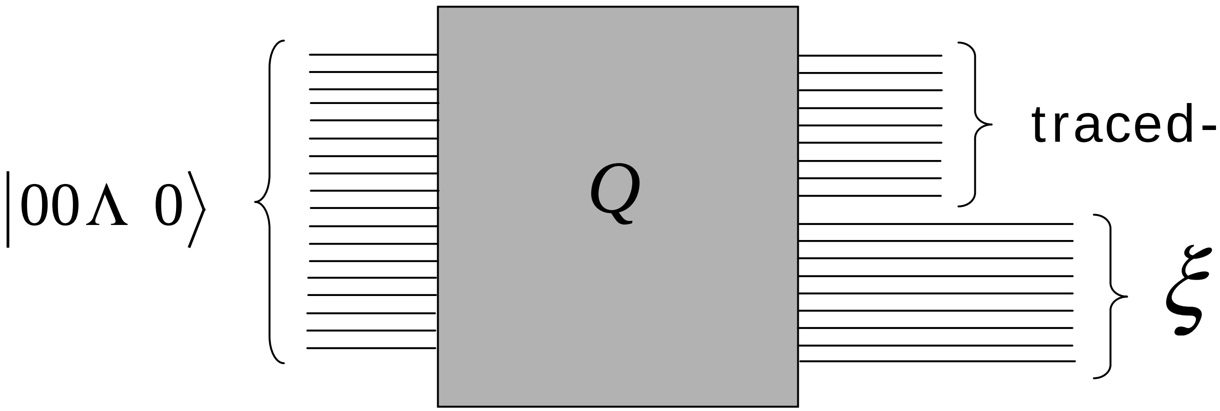
$$F\left(T_1(\rho), T_2\left(\xi\right) \right) > 1 - \varepsilon$$

No: for all states ρ and ξ:

$$F\left(T_1(\rho), T_2\left(\xi\right) \right) < \varepsilon$$

Special case: n=0

It makes sense to consider "channels" with no input:



We won't refer to these as channels...

Convention: when we want to describe **states**, we will describe them in this way.

Example problem #3: output close to a given state?

Input: a quantum channel T and a state ξ.

Yes: there exist a state ρ such that:

$$F\Big(T(\rho), \xi\Big) > 1 - \varepsilon$$

No: for all states ρ:

$$F\Big(T(\rho), \xi\Big) < \varepsilon$$

Example problem #4: states close together?

Input: quantum states ρ and ξ.

Yes: ρ and ξ are close together:

$$F(\rho, \xi) > 1 - \varepsilon$$

No: ρ and ξ are far apart:

$$F(\rho, \xi) < \varepsilon$$

Example problem #5: entanglement breaking channel?

Input: a quantum channel T.

Yes: T is close to entanglement breaking: for all ρ there exists separable ξ s.t.

$$F\big((T \otimes I)(\rho), \xi \big) > 1 - \varepsilon$$

No: T is far from entanglement breaking: there exists ρ s.t. for all separable ξ:

$$F\big((T \otimes I)(\rho), \xi \big) < \varepsilon$$

Complete problems

Let A denote some promise problem. Write

$$A_{\mathrm{yes}}, \; A_{\mathrm{no}}$$

to denote sets of “yes” instances and “no” instances, respectively.

Promise problem A is complete for class C if:

1. $A \in C$
2. for all promise problems B in C there exists a polynomial-time computable f such that

$$x \in B_{\mathrm{yes}} \Rightarrow f(x) \in A_{\mathrm{yes}}, \qquad x \in B_{\mathrm{no}} \Rightarrow f(x) \in A_{\mathrm{no}}$$

Simple example

Consider the following problem A:

Input: a quantum state ρ on <u>one qubit</u>.

Yes: $\langle 1|\rho|1\rangle \geq 2/3$

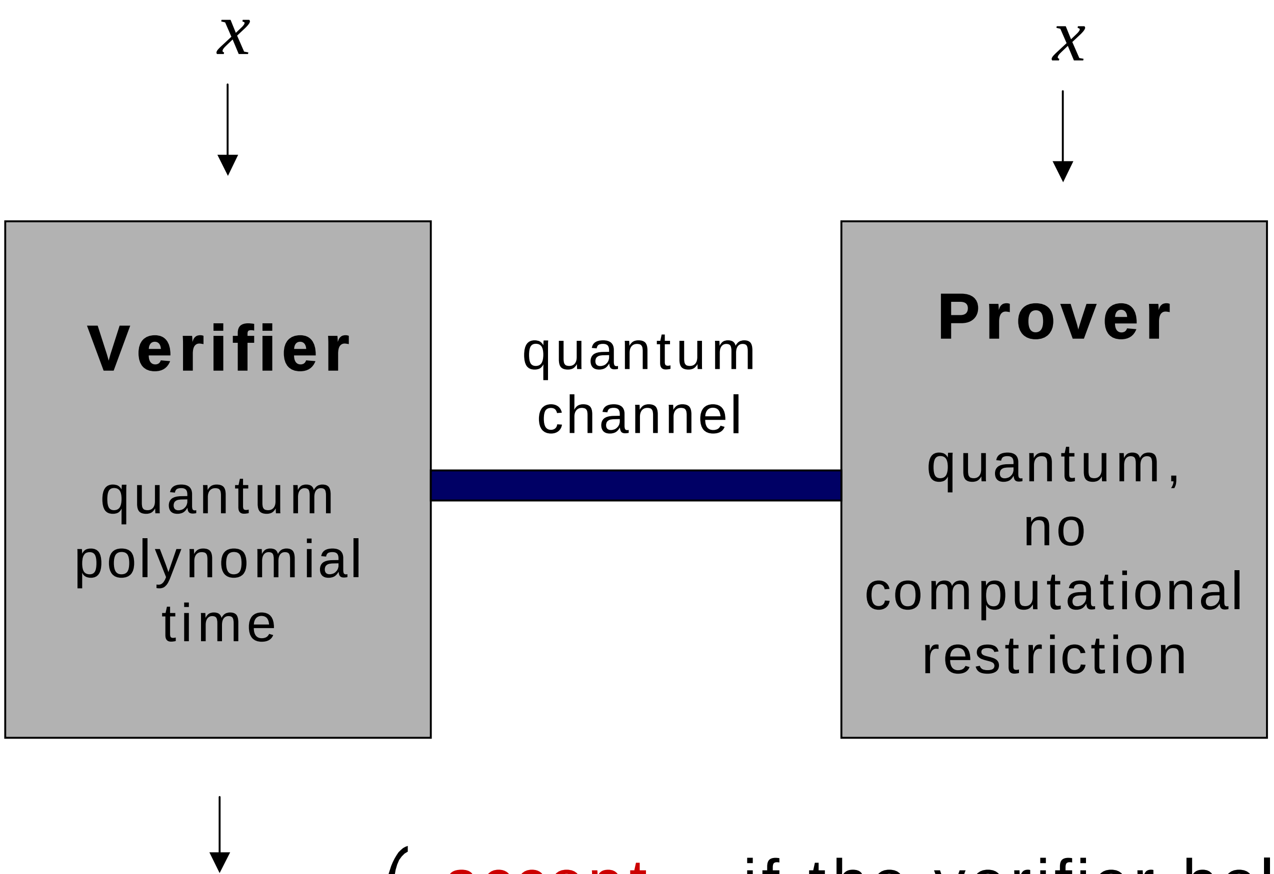
No: $\langle 1|\rho|1\rangle \leq 1/3$

---

1. Easily solved in BQP (by simulating the circuit that describes ρ).
2. Any promise problem B in BQP reduces to A (by virtue of the fact that there exists an efficient quantum algorithm for B).

This is not very interesting...

Quantum Interactive Proof Systems



Output:
- accept if the verifier believes x is a "yes" input
- reject otherwise

Problems with quantum interactive proofs

A promise problem A has a quantum interactive proof system if there exists a verifier V such that:

1. (completeness condition)

   If $x \in A_{\text{yes}}$ then there exists some prover P that convinces V to accept (with high probability).

2. (soundness condition)

   If $x \in A_{\text{no}}$ then no prover P can convince V to accept (except with small probability).

Example problem #2: outputs close together?

Input: two quantum channels T_1 and T_2.

Yes: there exist states ρ and ξ such that:

$$F\left(T_1(\rho), T_2(\xi) \right) > 1 - \varepsilon$$

No: for all states ρ and ξ:

$$F\left(T_1(\rho), T_2(\xi) \right) < \varepsilon$$

Complete for *QIP*.

Example problem #3: output close to a given state?

Input: a quantum channel T and a state ξ.

Yes: there exist a state ρ such that:

$$F\left(T(\rho), \xi \right) > 1 - \varepsilon$$

No: for all states ρ:

$$F\left(T(\rho), \xi \right) < \varepsilon$$

Complete* for *QIP(2)*.

Example problem #4: states close together?

Input: quantum states ρ and ξ.

Yes: ρ and ξ are close together:

$$F(\rho, \xi) > 1 - \varepsilon$$

No: ρ and ξ are far apart:

$$F(\rho, \xi) < \varepsilon$$

Complete for $QSZK_{HV}$.

Back to example problem #2: outputs close together?

Input: two quantum channels T_1 and T_2.

Yes: there exist states ρ and ξ such that:

$$F\left(T_1(\rho), T_2(\xi) \right) > 1-\varepsilon$$

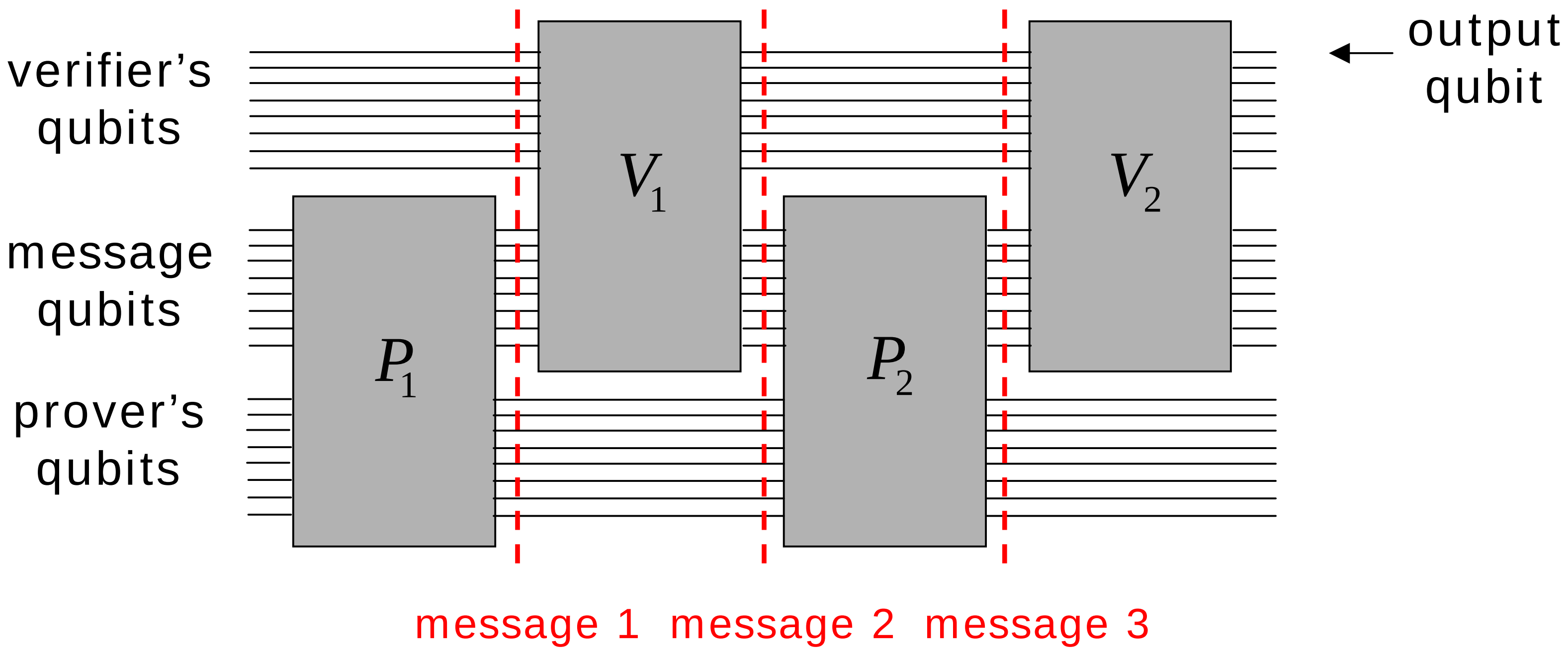
No: for all states ρ and ξ:

$$F\left(T_1(\rho), T_2(\xi) \right) < \varepsilon$$

Complete for *QIP*.

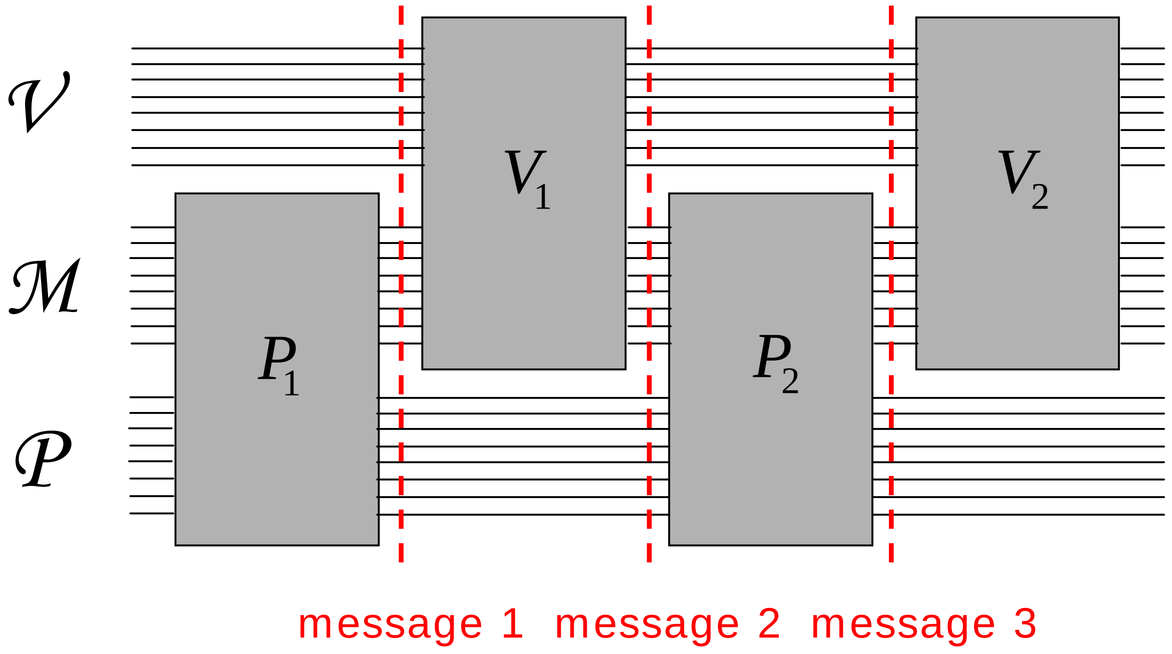
3-Message Quantum Interactive Proofs

We know that $QIP = QIP(3)$, so we just need to show that any problem B with a 3-message quantum interactive proof reduces to our problem.

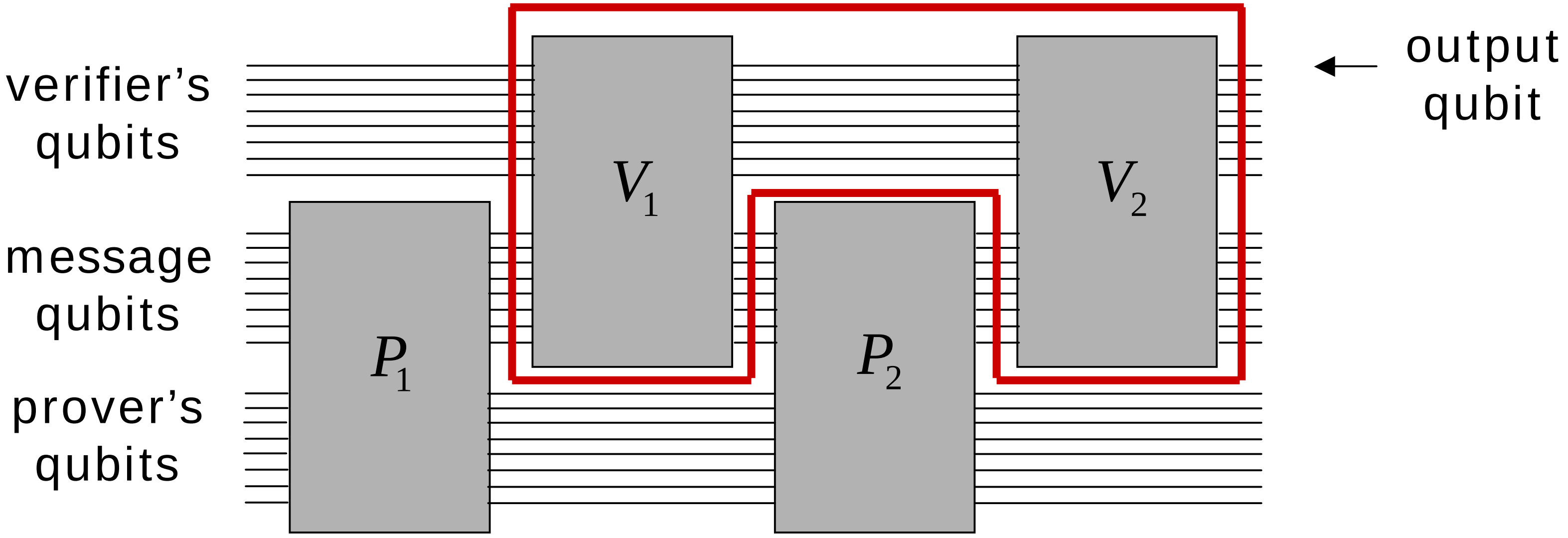


3-Message Quantum Interactive Proofs

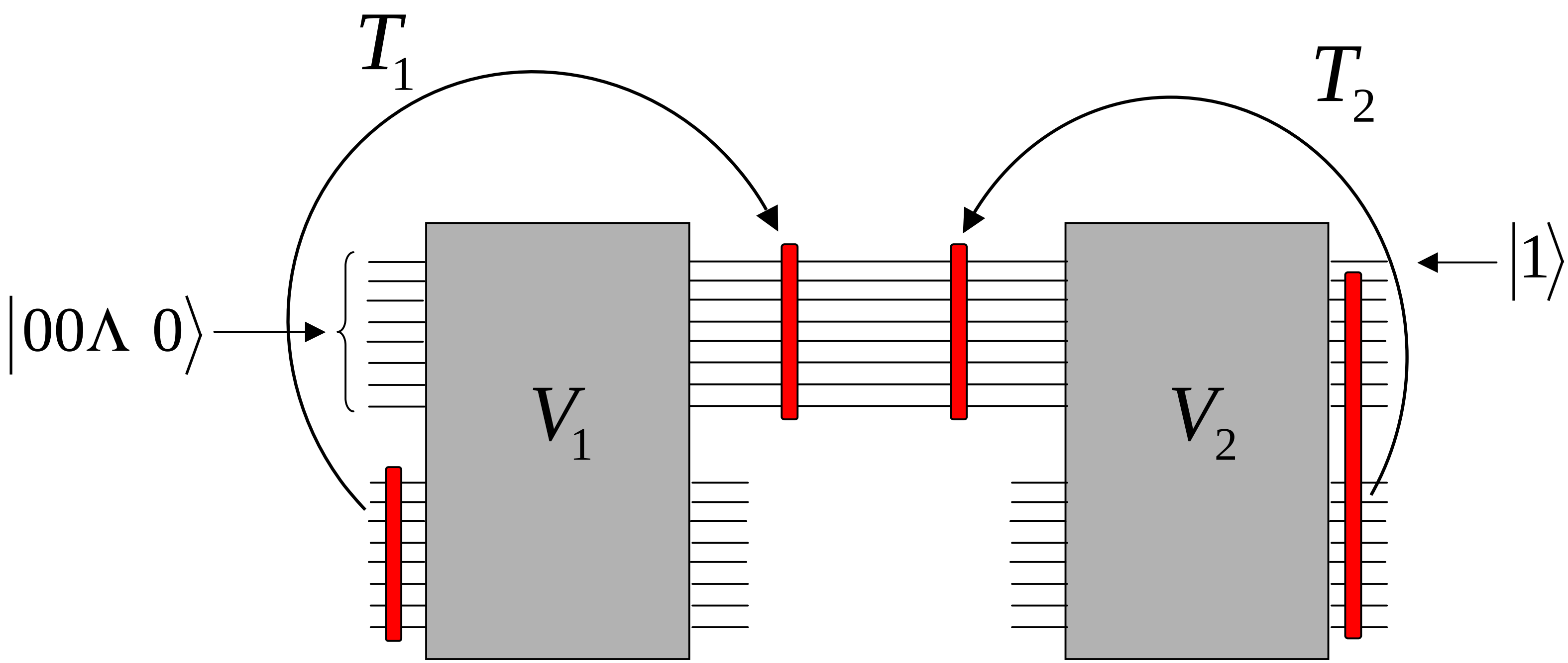
We know that $QIP = QIP(3)$, so we just need to show that any problem B with a 3-message quantum interactive proof reduces to our problem.



Removing prover from the picture



Transformations



Define quantum transformations T_1, T_2 as follows:

$$T_1(\rho) = \mathrm{Tr}_{\mathcal{M}} V_1 \left(|0\Lambda\ 0\rangle\langle 0\Lambda\ 0| \otimes \rho \right) V_1^{\dagger}$$

$$T_2(\xi) = \mathrm{Tr}_{\mathcal{M}} V_2^{\dagger} \left(|1\rangle\langle 1| \otimes \xi \right) V_2$$

Maximum Acceptance Probability

The maximum probability with which the prover can convince the verifier to accept is:

$$\max_{\rho,\xi} \; F\big(T_1(\rho), T_2(\xi)\big)^2$$

where the maximum is over all inputs ρ and ξ.

Bipartite Quantum States

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

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

that satisfy

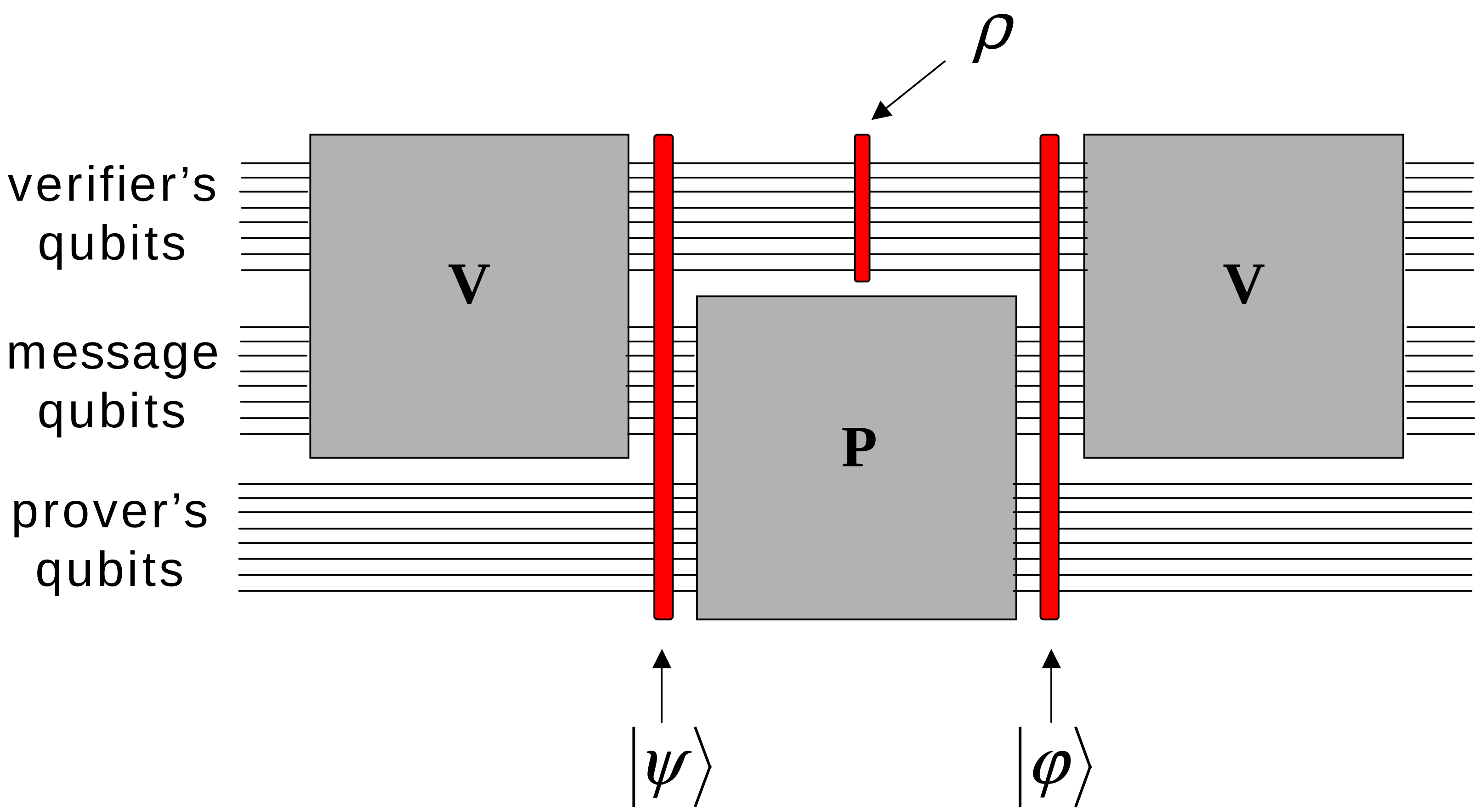
$$\mathrm{Tr}_{\mathcal{H}_2} |\psi\rangle\langle\psi| = \mathrm{Tr}_{\mathcal{H}_2} |\varphi\rangle\langle\varphi|$$

Then there exists a unitary operator U acting only on $\mathcal{H}_2$ such that

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

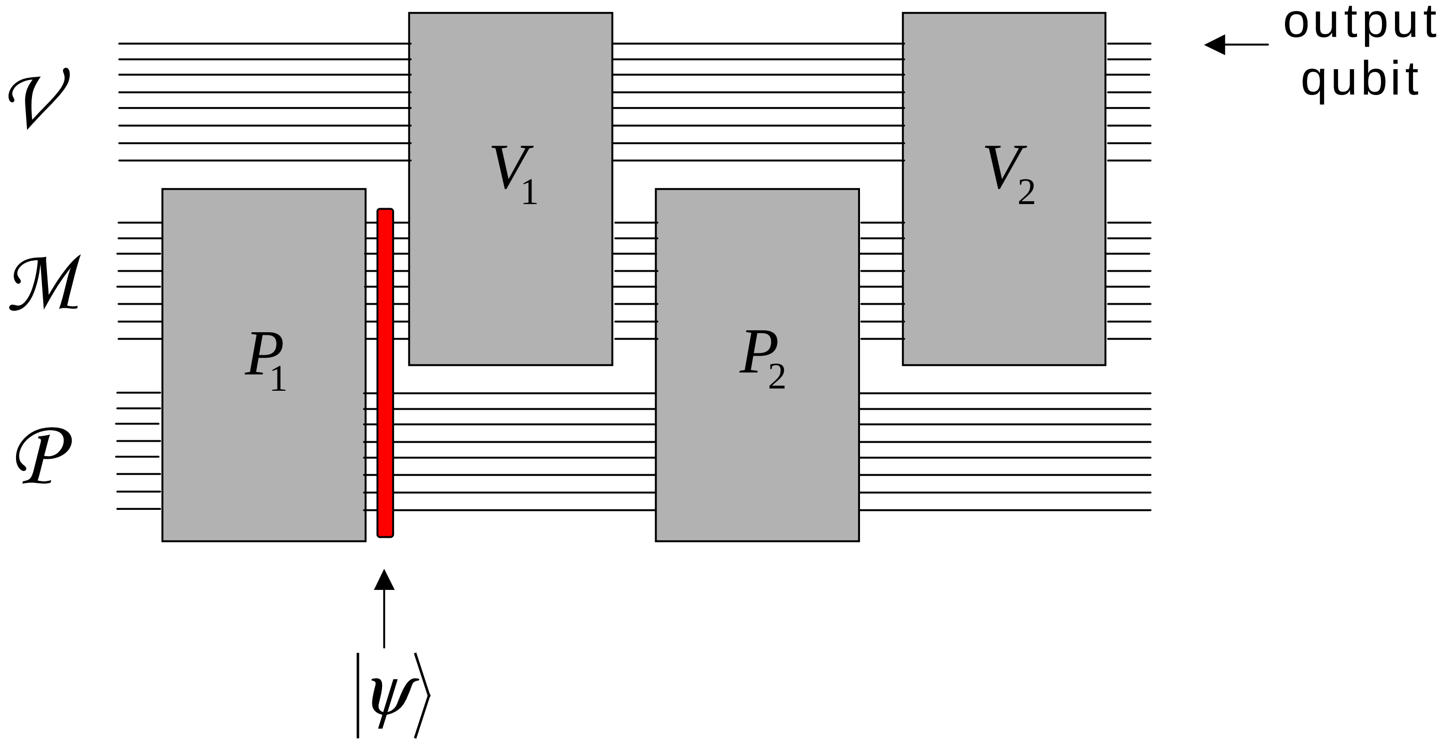
(Approximate version also holds.)

Options for the Prover

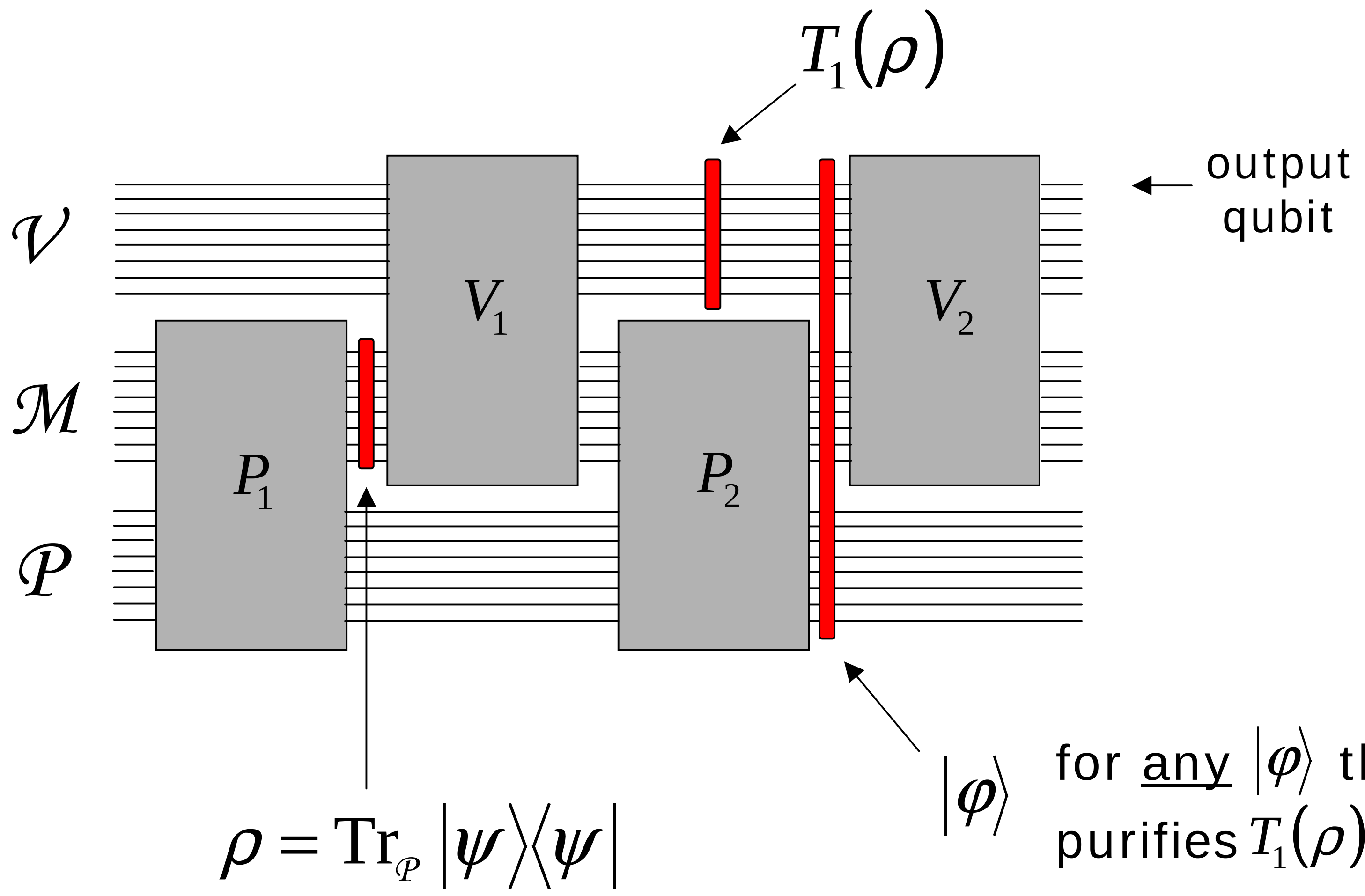


Prover can transform $|\psi\rangle$ to $|\varphi\rangle$ for any $|\varphi\rangle$ that leaves the verifier's qubits in state ρ.

Maximum Acceptance Probability



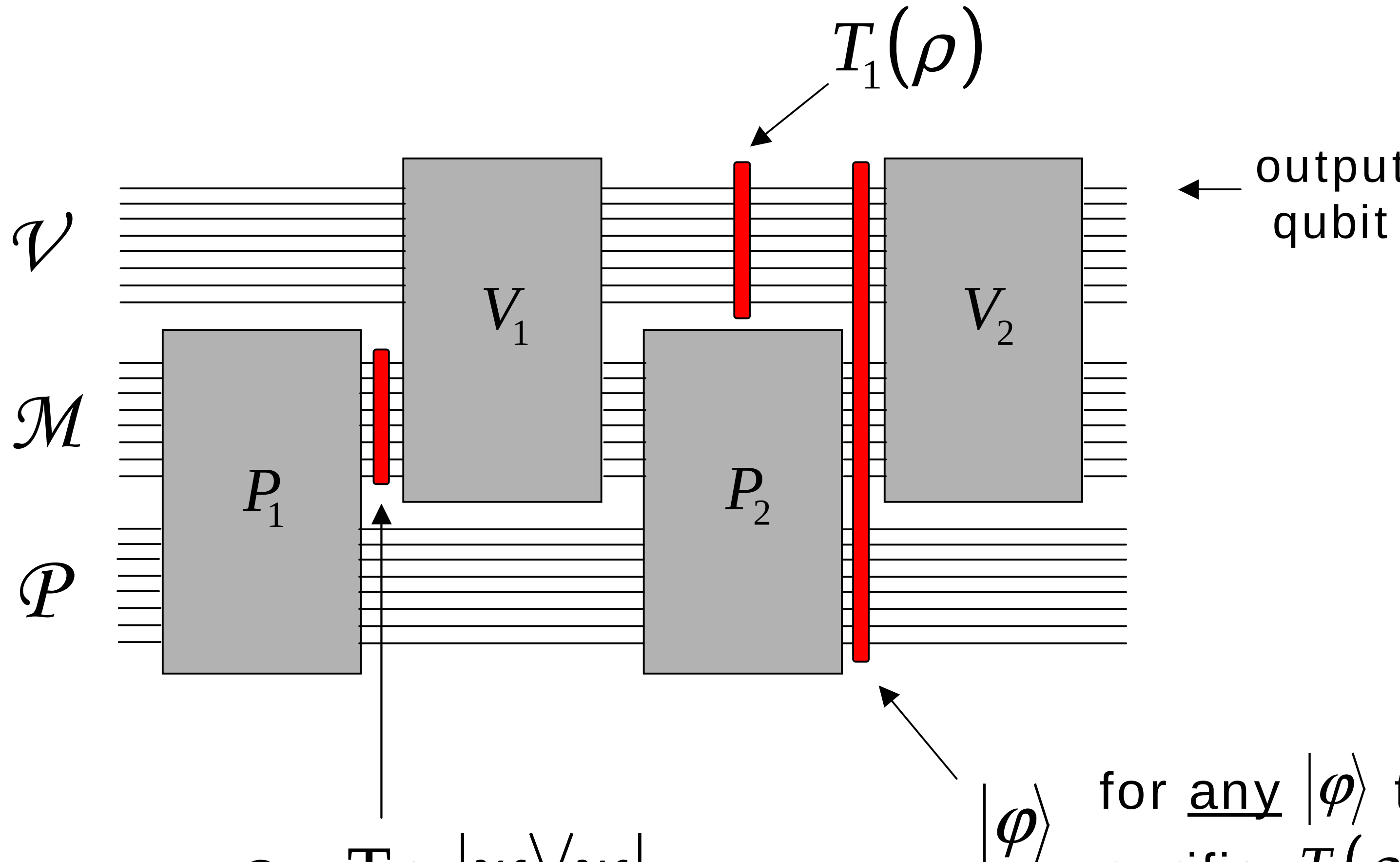
Maximum Acceptance Probability



for any $|\varphi\rangle$ that purifies $T_1(\rho)$.

$$\Pr[\,\text{accept}\,] = \left\| \Pi_{\text{acc}} V_2 |\varphi\rangle \right\|^2$$

Maximum Acceptance Probability

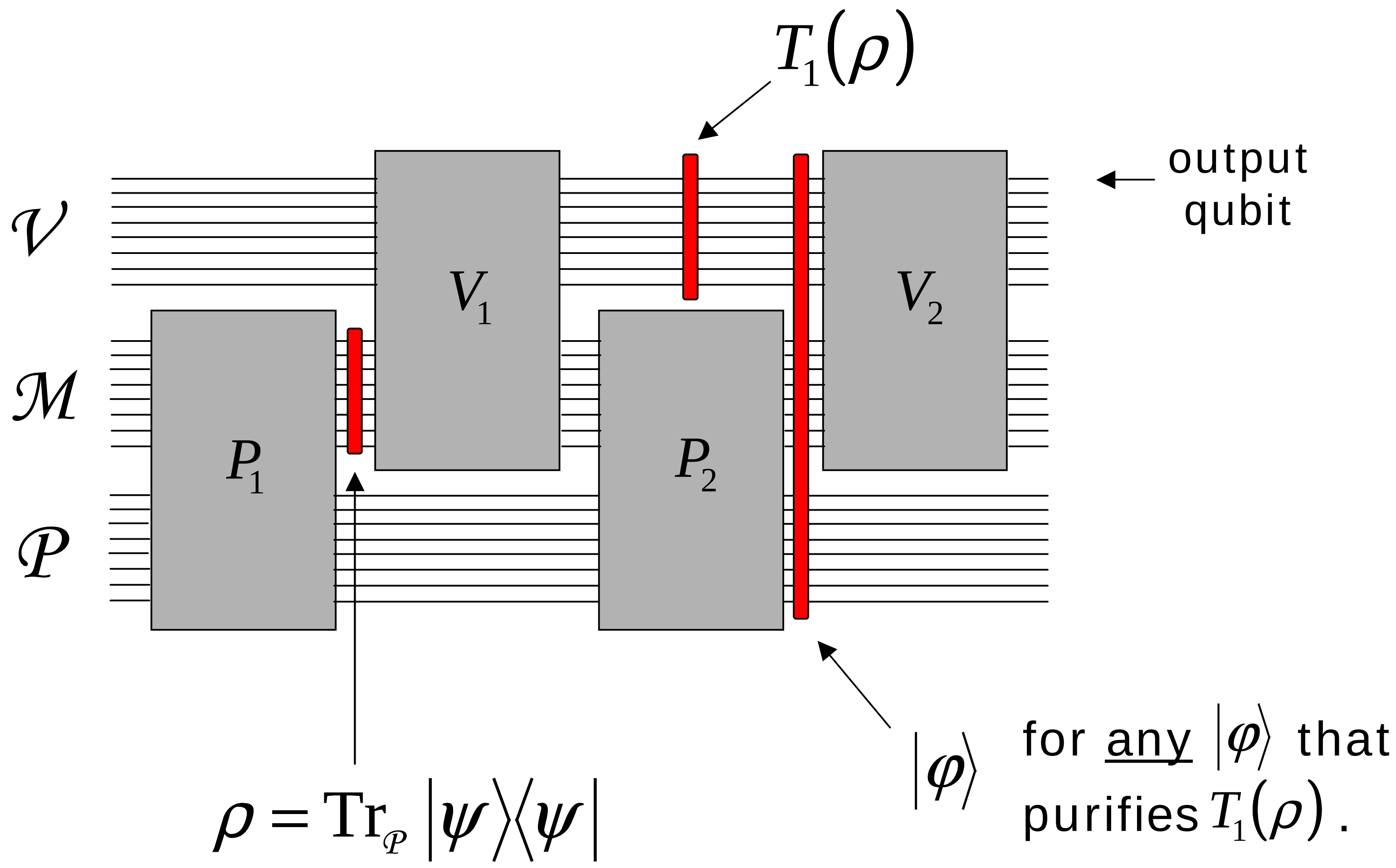


for any $|\varphi\rangle$ that purifies $T_1(\rho)$.

$$\rho = \mathrm{Tr}_{\mathcal{P}} |\psi\rangle\langle\psi|$$

$$\Pr[\text{ accept }] = \max_{|\sigma\rangle} \left| \left(\langle 1| \otimes \langle \sigma| \right) V_2 |\varphi\rangle \right|^2$$

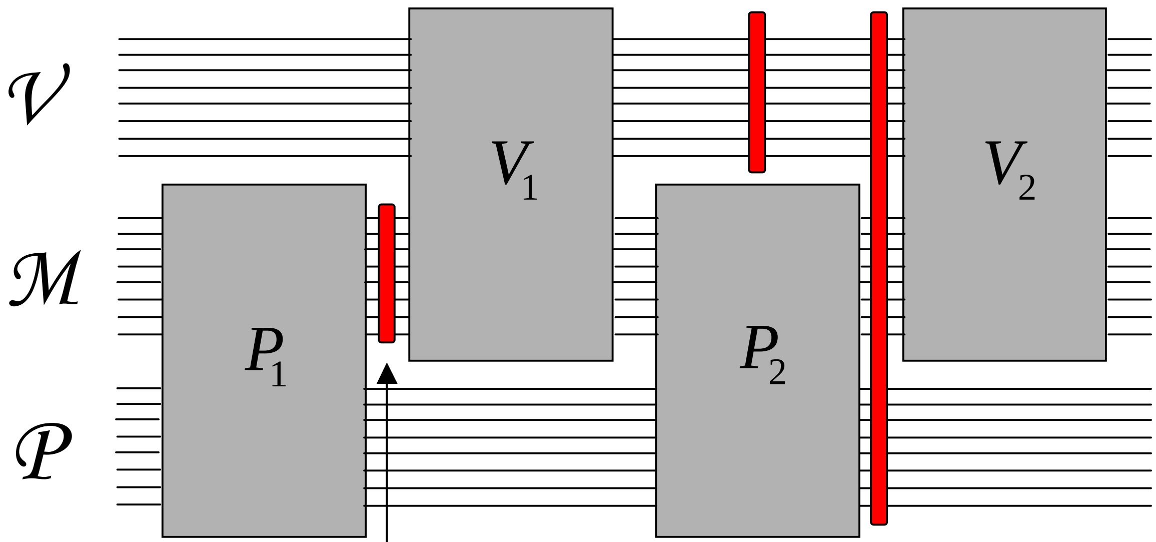
Maximum Acceptance Probability



$$\Pr[\text{ accept }] = \max_{|\sigma\rangle} \left| \langle\varphi| V_2^{\dagger} \left(|1\rangle \otimes |\sigma\rangle \right) \right|^2$$

Maximum Acceptance Probability

$T_1(\rho)$



output qubit

$\rho = \mathrm{Tr}_{\mathcal{P}} |\psi\rangle\langle\psi|$

$|\varphi\rangle$ for any $|\varphi\rangle$ that purifies $T_1(\rho)$.

equality for best $|\varphi\rangle$

$$\Pr[\text{accept}] \leq \max_{\xi} F\big(T_1(\rho), T_2(\xi)\big)^2$$

Maximum Acceptance Probability

The maximum probability with which the prover can convince the verifier to accept is:

$$\max_{\rho,\xi} F\left(T_1(\rho), T_2(\xi)\right)^2$$

where the maximum is over all inputs ρ and ξ.

Applications

The completeness of these problems allows us to prove various things about the corresponding classes, such as:

- $QIP \subseteq EXP$: the complete problem can be solved in EXP via semidefinite programming.
- $QSZK$ closed under complement and parallelizable to 2 messages: there exists a 2-message $QSZK$-protocol for the corresponding complete problem and its complement
- $QSZK \subseteq PSPACE$: the complete problem can be solved in $PSPACE$.

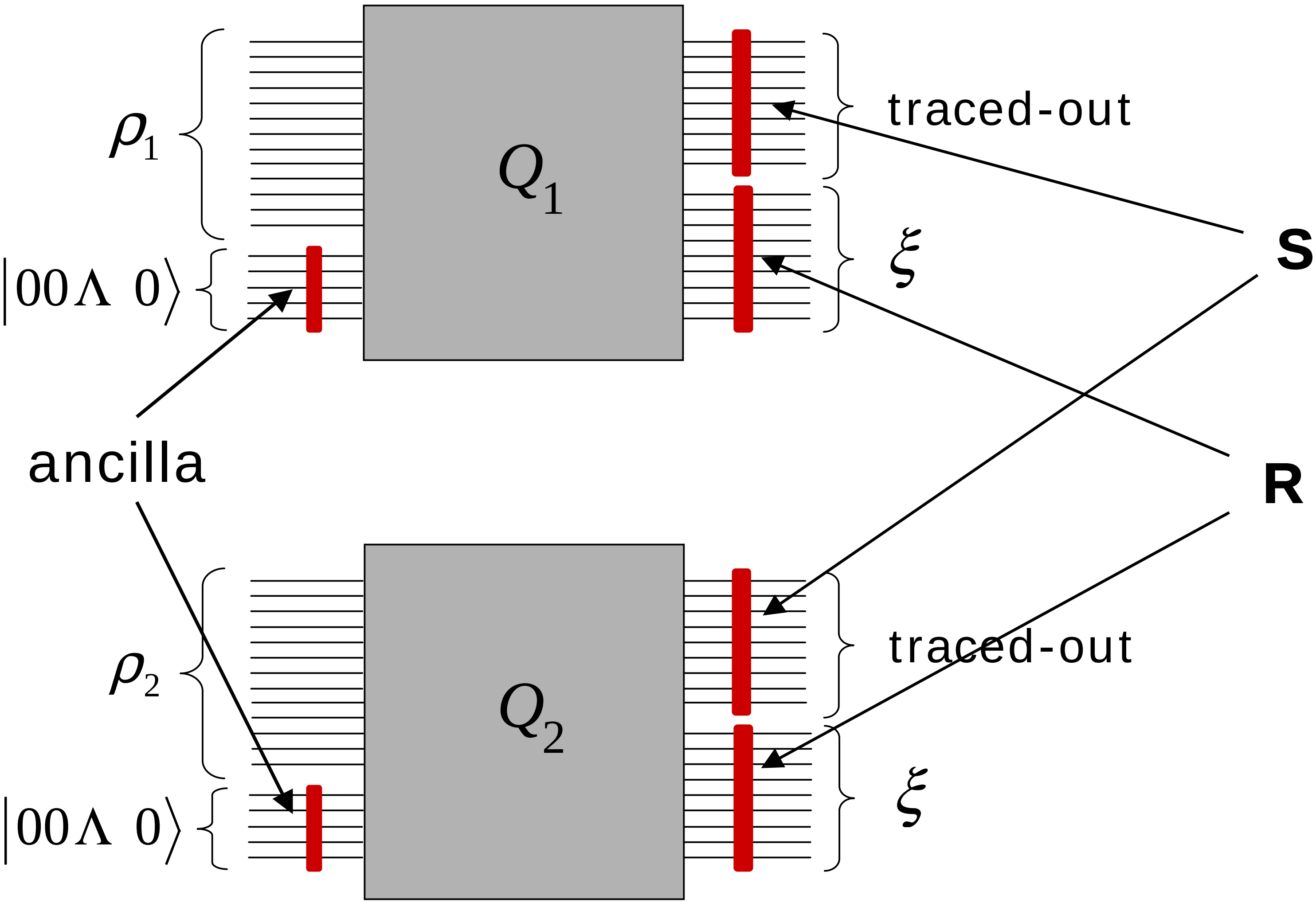
Applications

- $QIP \subseteq QMAM$: any problem having a quantum interactive proof system also has a 3-message **quantum Arthur-Merlin game**.

A quantum Arthur-Merlin game is a restricted type of quantum interactive proof:

- the verifier's (Arthur's) messages consist only of fair coin-flips (classical).
- all of Arthur's computation takes place after all messages have been sent.

Quantum Arthur-Merlin protocol



Quantum Arthur-Merlin protocol

Message 1 (from Merlin to Arthur):

Merlin sends some register **R** (supposedly corresponding to the common output of the channels).

Message 2 (from Arthur to Merlin):

Arthur flips a coin: call the result b. Send b to Merlin.

Message 3 (from Merlin to Arthur):

Merlin sends some register **S** (corresponds to traced-out qubits).

Quantum Arthur-Merlin protocol

Arthur's verification procedure (after messages are sent):

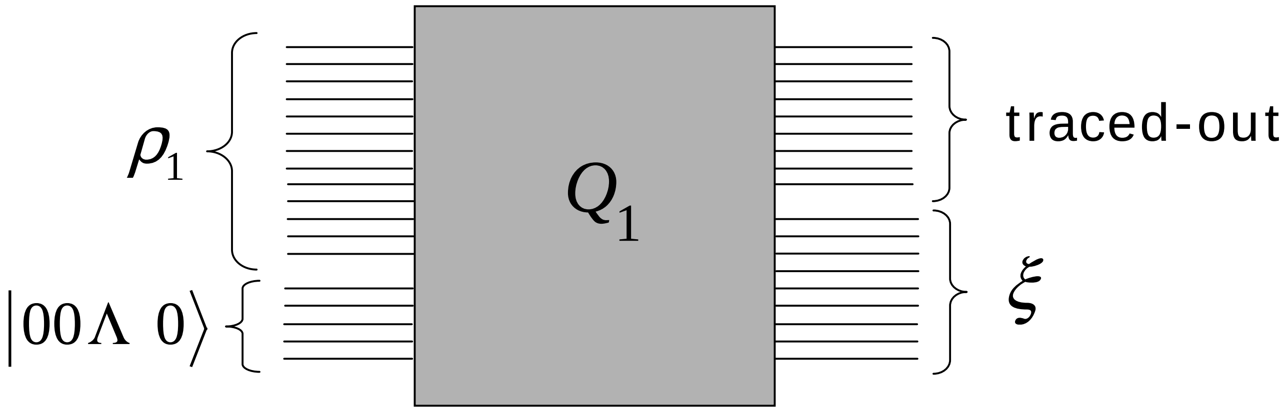
If the coin-flip was $b = 0$:

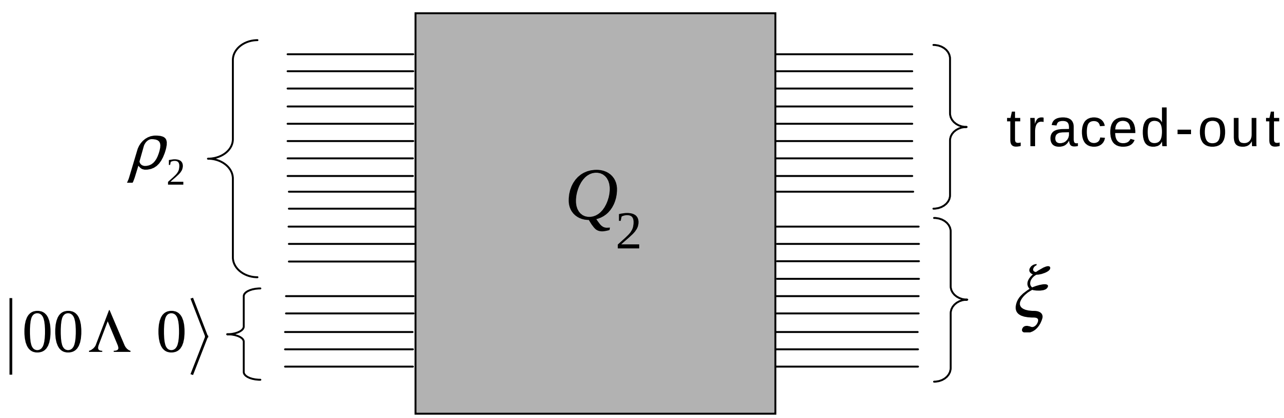
Apply Q_2^{-1} to (**R**,**S**).
Accept if all ancilla qubits are set to 0, reject otherwise.

If the coin-flip was $b = 1$:

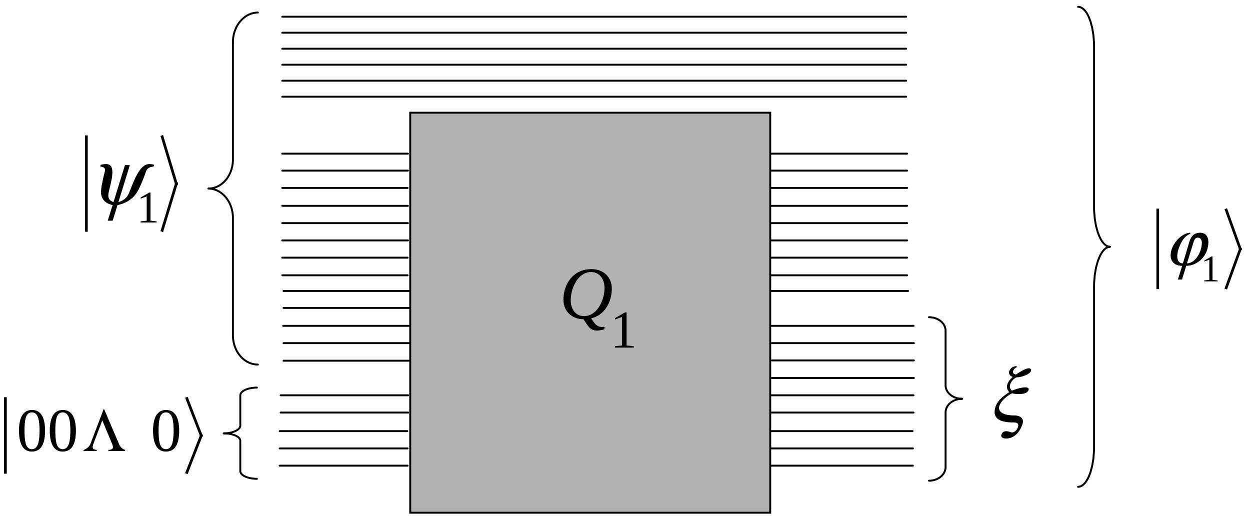
Apply Q_1^{-1} to (**R**,**S**).
Accept if all ancilla qubits are set to 0, reject otherwise.

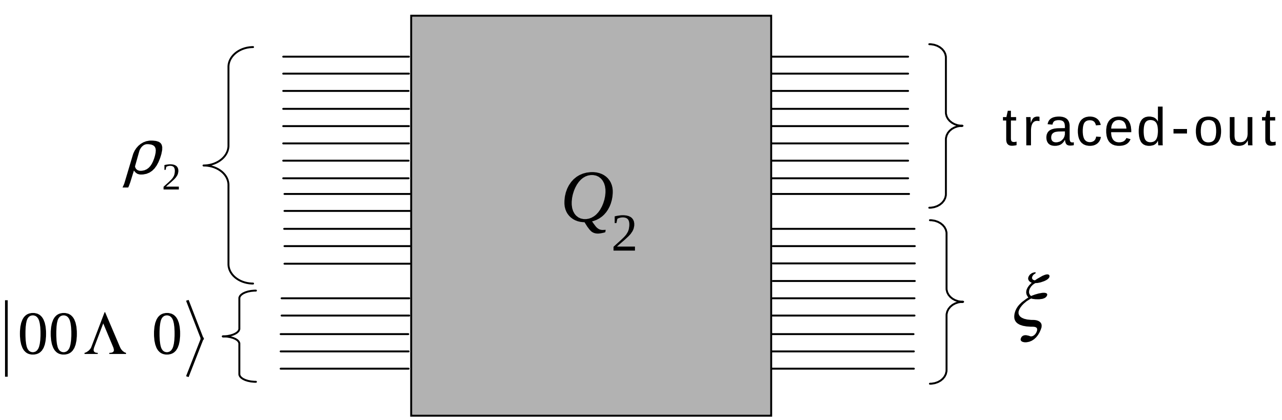
“Honest” Merlin strategy



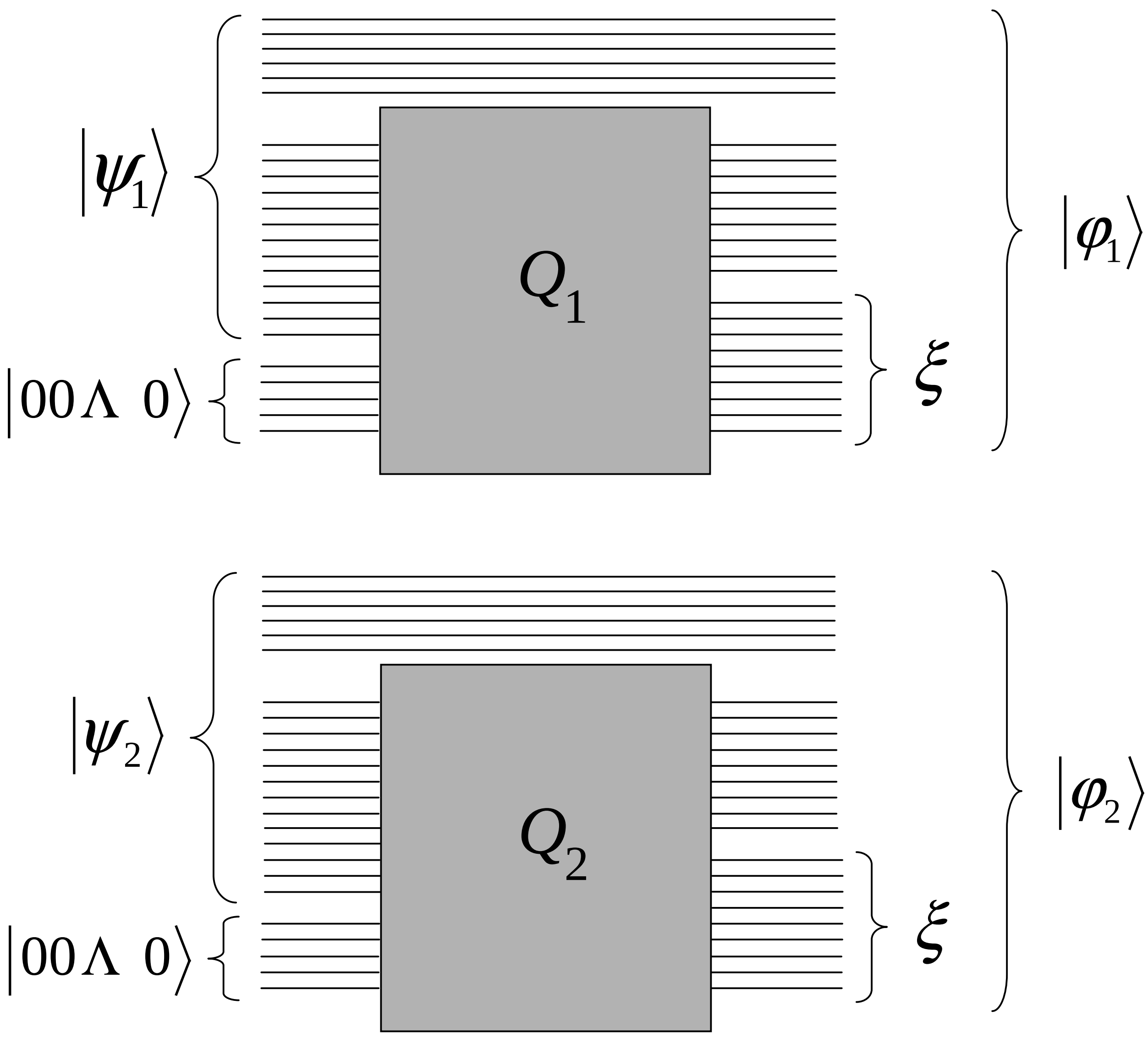


“Honest” Merlin strategy

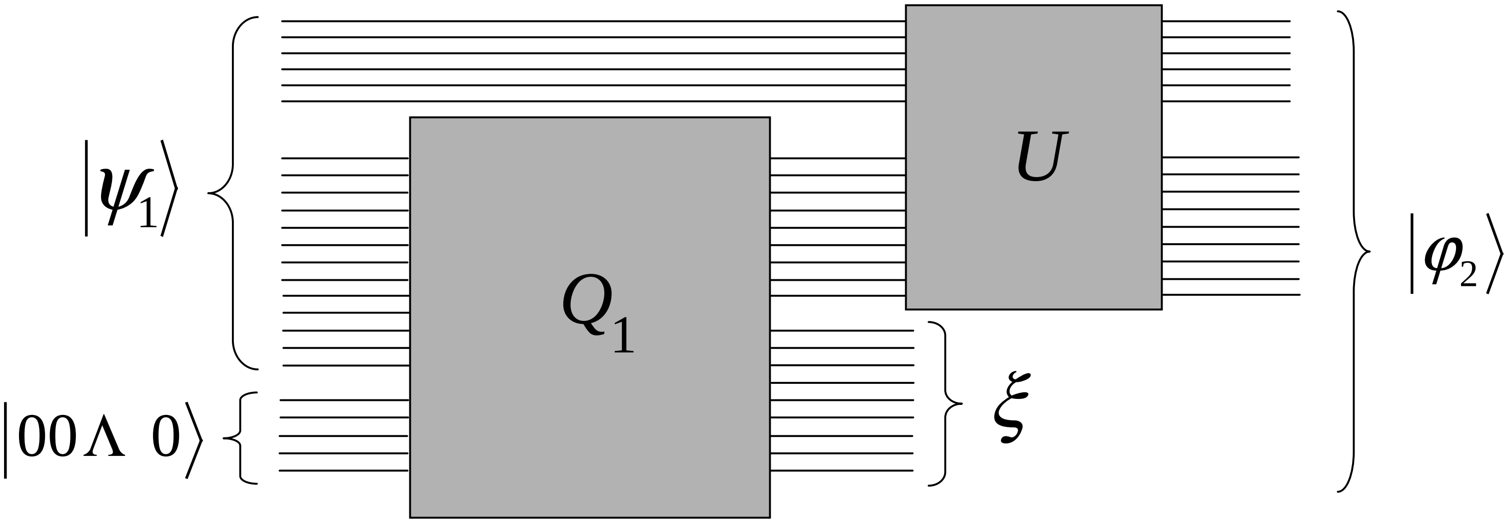


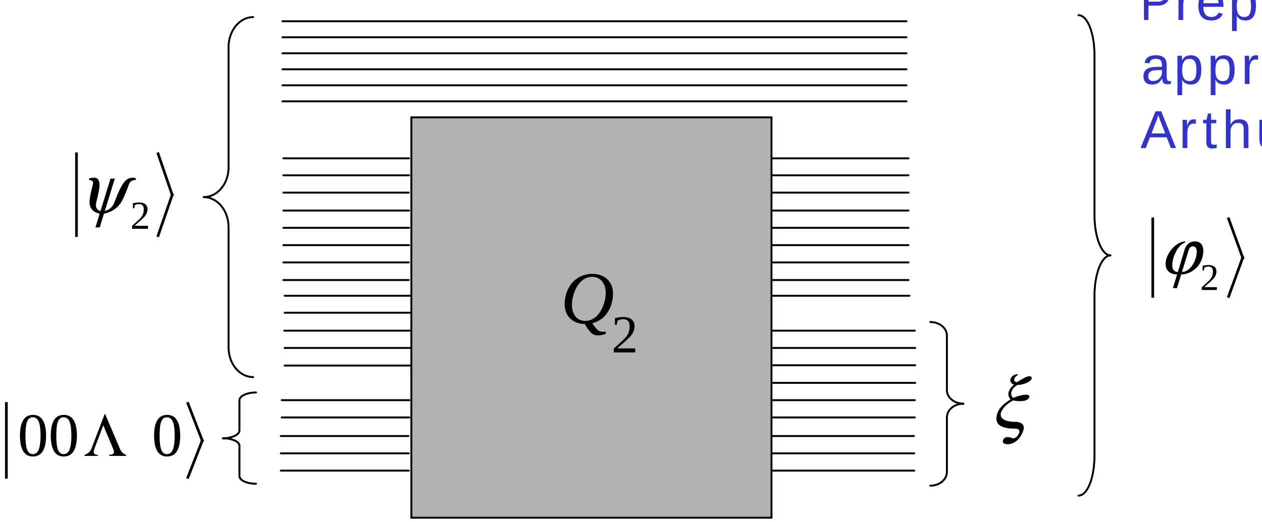


“Honest” Merlin strategy



"Honest" Merlin strategy



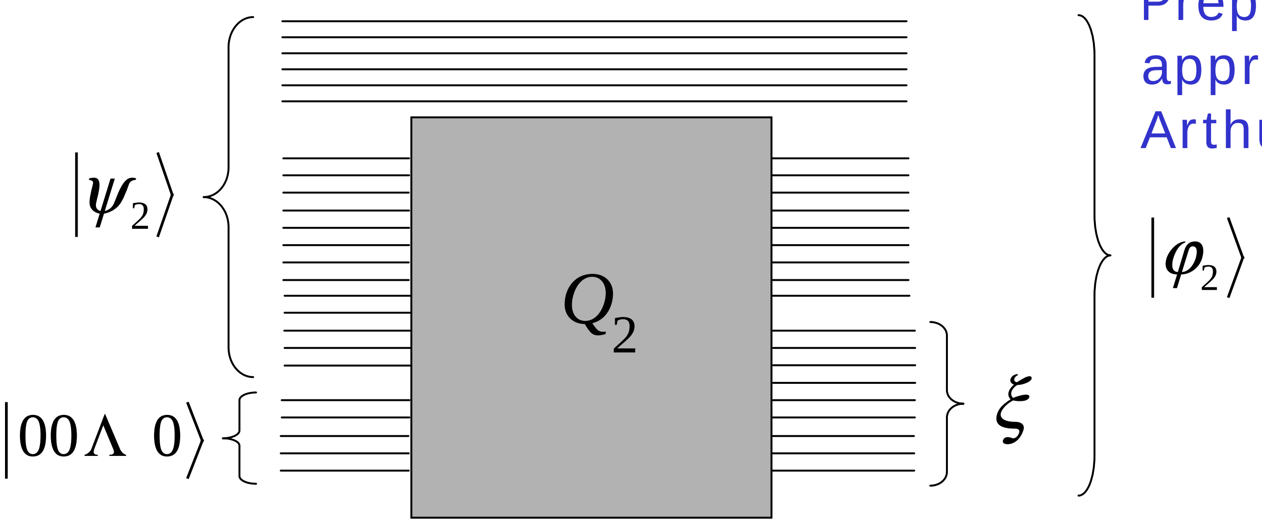


<u>Step 1:</u>
Prepare $|\varphi_2\rangle$, send appropriate part to Arthur.

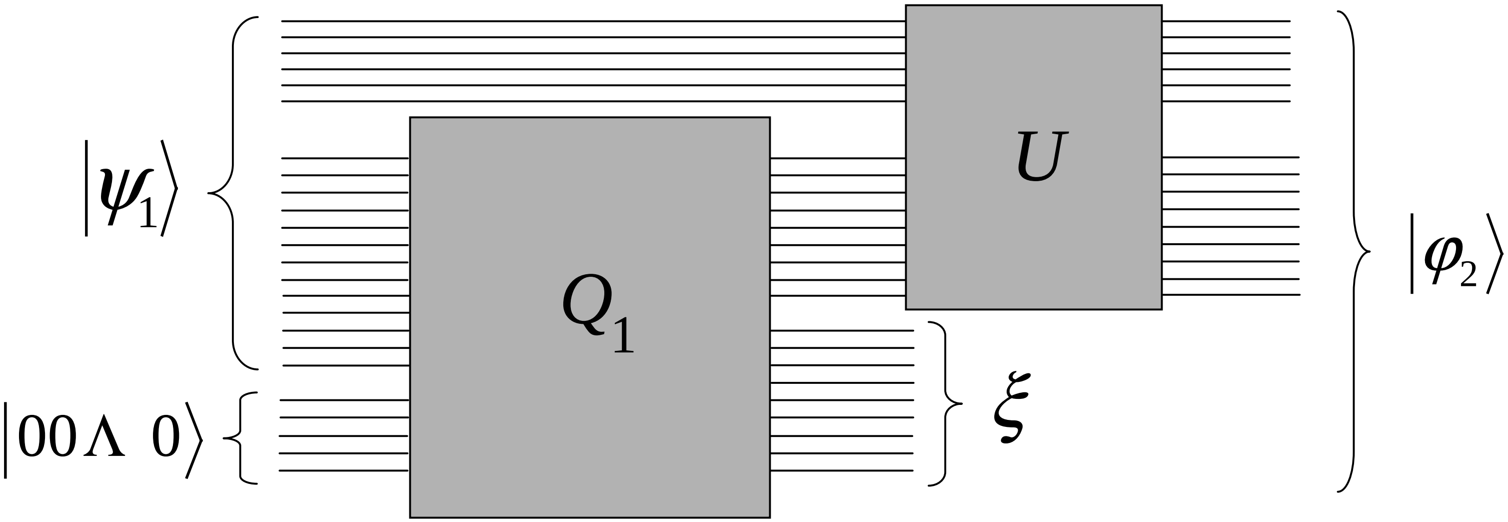
“Honest” Merlin strategy

Step 2 (if b=0)
Send the rest of $|\varphi_2\rangle$ to Arthur.

Step 1:
Prepare $|\varphi_2\rangle$, send appropriate part to Arthur.



"Honest" Merlin strategy



<u>Step 1:</u>
Prepare $|\varphi_2\rangle$, send appropriate part to Arthur.

<u>Step 2</u> (if b=1)
Apply U^{-1} to the rest of $|\varphi_2\rangle$,
rest of to Arthur.

QMAM protocol: soundness

Suppose Merlin is cheating...

Let the reduced state of register **R** (sent on the first message from Merlin to Arthur) be σ.

Claim: maximum acceptance probability is

$$\max_{\rho,\xi}\left\{\frac{1}{2}F\left(T_1(\rho),\sigma\right)^2+\frac{1}{2}F\left(\sigma,T_2(\xi)\right)^2\right\}$$

$$\leq\frac{1}{2}+\frac{1}{2}\max_{\rho,\xi}F\left(T_1(\rho),T_2(\xi)\right)$$

Open questions

- Find other complete problems for quantum classes.
- Develop relations among complexity of various problems about channels (e.g., problems concerning entanglement, channel capacity,...).
- There are still many interesting questions about quantum interactive proof systems that are unanswered. (E.g., just about everything about $QIP(2)$.)