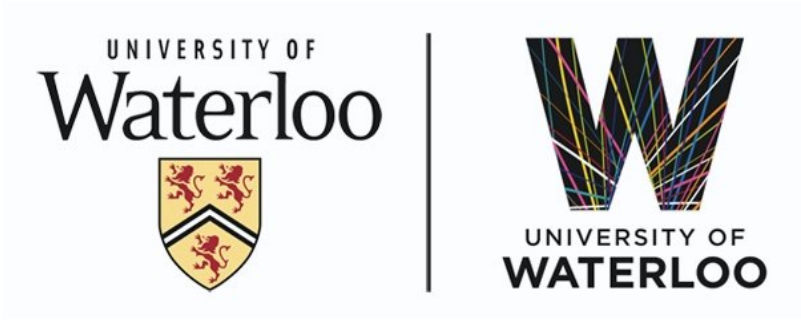
Distinguishability of Quantum Channels

Bill Rosgen

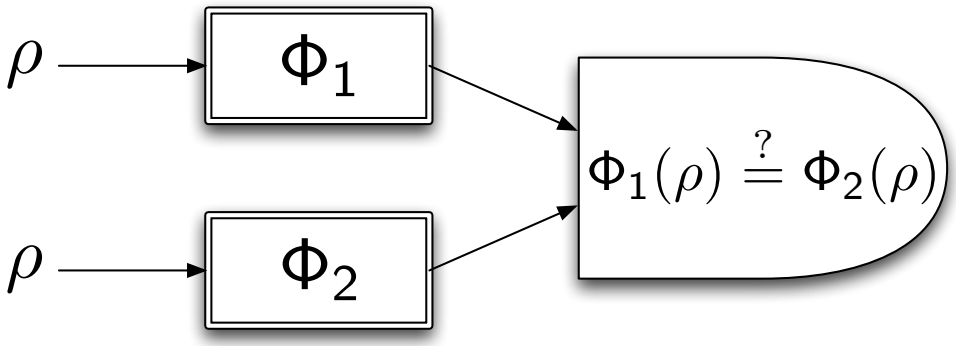
Institute for Quantum Computing
University of Waterloo

July 23, 2009



Distinguishing quantum channels

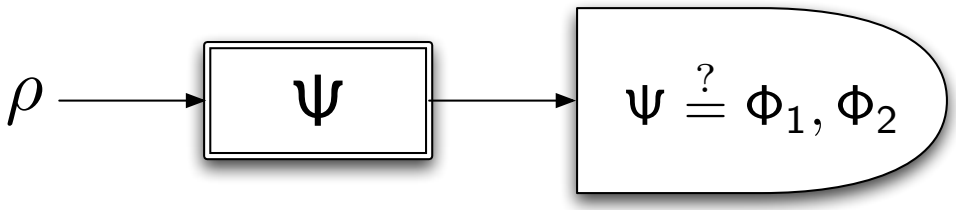
- Given descriptions of two channels: do they behave (nearly) the same on all inputs?



- Is there an input ρ for which $\Phi_1(\rho)$ and $\Phi_2(\rho)$ are almost orthogonal?

An alternate characterization

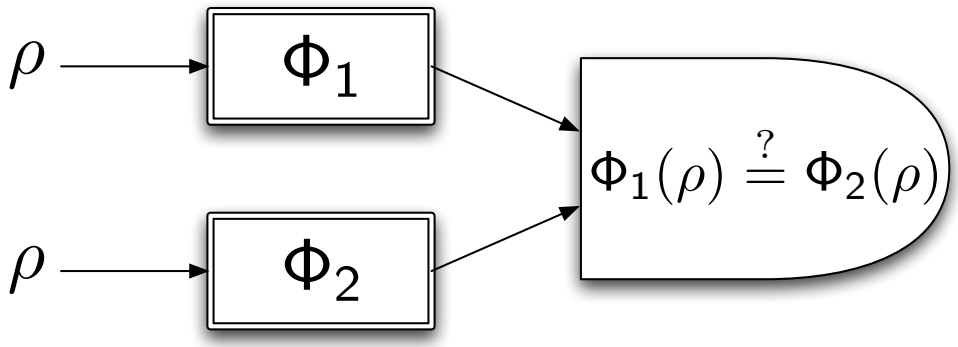
Identifying one of two known channels:



- Given a channel Ψ, one of two known channels Φ_1, Φ_2, with what probability can it be successfully identified with only one use of Ψ?
- This is equivalent to the distinguishability problem.

As a computational problem

- To phrase this in a computational setting, we need to define:
  1. representation of the channels,
  2. notion of distance between them

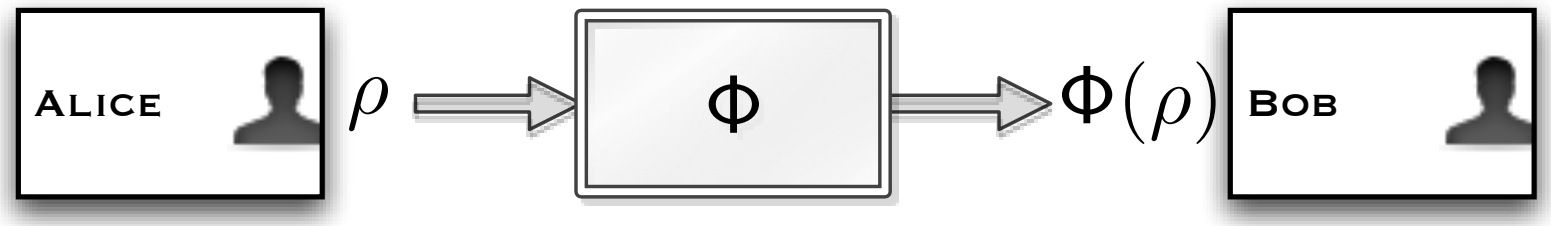


- For suitable choices, this problem is intractable (**QIP**-hard)
- Does simplifying the channels considered make it easier?

Quantum channels

A channel is a completely positive trace preserving linear map.

- $\operatorname{tr} \Phi(X) = \operatorname{tr} X$
- If $X \geq 0$ then $(\Phi \otimes I_{\mathcal{F}})(X) \geq 0$



- Alternately: linear maps on density matrices.

Examples of channels

- Two simple error models are:
  - Completely depolarizing channel

$$N(\rho) = \mathbb{1}/d, \quad N\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} 1/3 & 0 & 0 \\ 0 & 1/3 & 0 \\ 0 & 0 & 1/3 \end{pmatrix}$$

  - Completely dephasing channel

$$D(|i\rangle\langle j|) = \delta_{ij}|i\rangle\langle j|, \quad D\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{pmatrix}$$

Representations of channels

There are two representations of channels that we will need.

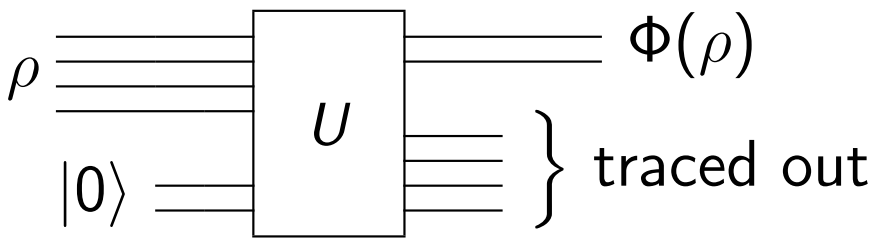
Definition (Kraus representation)

There exist operators A_i such that $\sum_i A_i^* A_i = \mathbb{1}$ and $\Phi(X) = \sum_i A_i X A_i^*$.

Definition (Stinespring dilation)

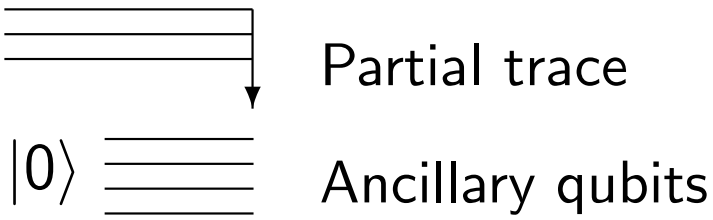
For a channel on states on $\mathcal{A}$, there exists a unitary U on $\mathcal{A} \otimes \mathcal{B}$ such that

$$\Phi(X) = \mathrm{tr}_{\mathcal{B}}\, U(X \otimes |0\rangle\langle 0|)U^*.$$

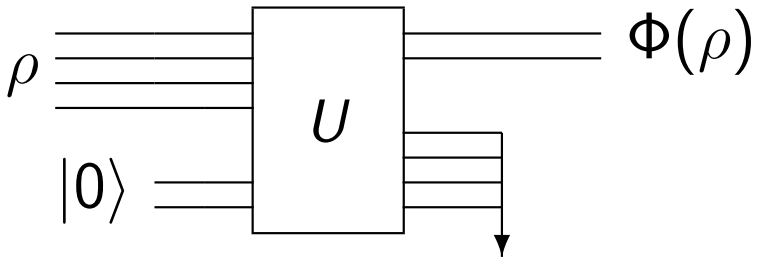


Channels as quantum circuits

- Any quantum channel can be represented with a circuit from some basis of unitary gates, plus two extra gates:

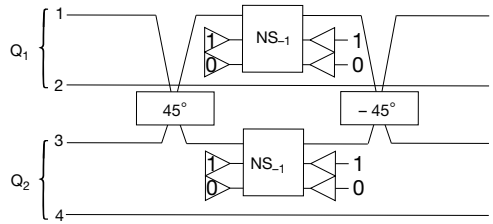


- By pushing these gates to the end/beginning of the circuit, can assume a circuit in Stinespring form.

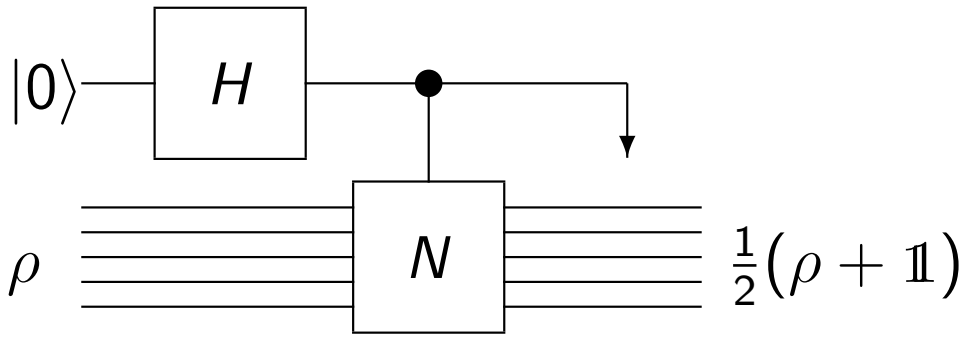


Why use this representation?

- For most of the channels we are interested in, it is logarithmic in the dimension of the system.
  - Quantum algorithms
  - Experimental implementations
  - Realistic noise models?



- Allows a channel to be run backwards, controlled by a different system, etc.

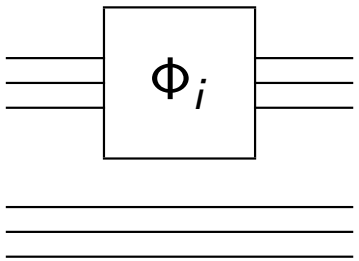


[1] Figure from KLM 01

The diamond norm for channels

- Distance between two channels in terms of the probability of distinguishing them.
- Entanglement with external system can increase this quantity.

$$\begin{aligned}\|\Phi\|_\diamond &= \|\Phi \otimes I_{\mathcal{F}}\|_{\mathrm{tr}} \\ &= \max_\rho \|(\Phi \otimes I_{\mathcal{F}})(\rho)\|_{\mathrm{tr}}\end{aligned}$$



- Given one use of Φ_1 or Φ_2 the optimal probability of identifying the channel is

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

Polarization of the diamond norm

Theorem (R. and Watrous, 05[1])

Given channels Φ_1, Φ_2 as circuits of size n, and $a, b \in [0,1]$ with $2b < a^2$, then channels Ψ_1, Ψ_2 can be constructed in polynomial time (in n, r) such that

$$\|\Phi_1 - \Phi_2\|_\diamond \leq b \implies \|\Psi_1 - \Psi_2\|_\diamond < 2^{-r}$$
$$\|\Phi_1 - \Phi_2\|_\diamond \geq a \implies \|\Psi_1 - \Psi_2\|_\diamond > 2 - 2^{-r}$$

- i.e. distinguishability is no harder if the channels are "close"

[1] Generalizes a similar result for the ℓ_1 norm [SV97]

Fidelity

- A different notion of closeness is given by the fidelity

$$\mathrm{F}(\rho,\sigma) = \mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} = \max_{|\psi\rangle,|\phi\rangle} |\langle\phi|\psi\rangle|,$$

  where the maximum is over purifications of ρ, σ.
- This can be extended to channels:

$$\mathrm{F}_{\max}(\Phi,\Psi) = \max_{\rho,\sigma} \mathrm{F}(\Phi(\rho),\Psi(\sigma)).$$

- $\mathrm{F}_{\max}(\Phi,\Psi)$ and $\|\Phi-\Psi\|_\diamond$ are not directly comparable.
  - $\mathrm{F}_{\max}$ optimizes over two input states, one to each channel
  - $\|\Phi-\Psi\|_\diamond$ applies both channels to the same state

Outline

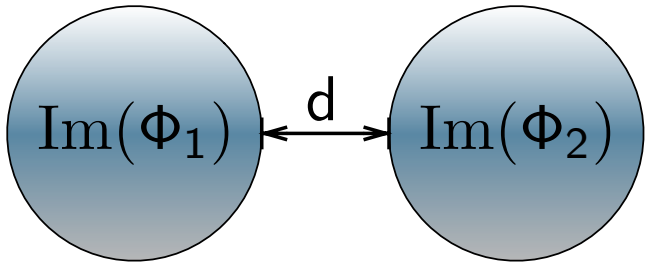
Problem Statement

Close Images

Given two mixed-state circuits Φ_1, Φ_2, decide between

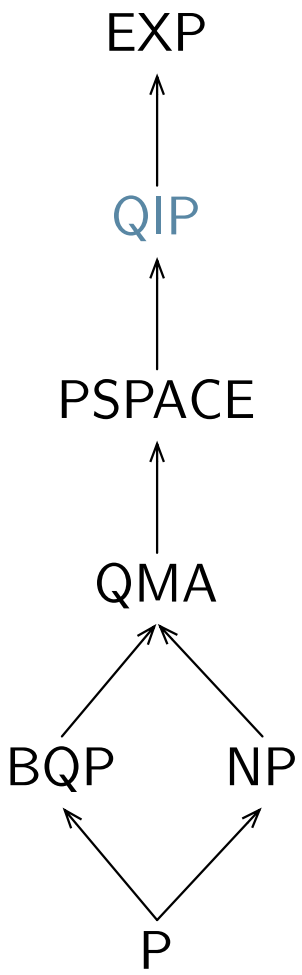
Yes: $\mathsf{F}_{\max}(\Phi_1, \Phi_2) \geq 1 - \varepsilon$.

No: $\mathsf{F}_{\max}(\Phi_1, \Phi_2) \leq \varepsilon$.



- This is a restatement of the definition of **QIP** [KW 2000]

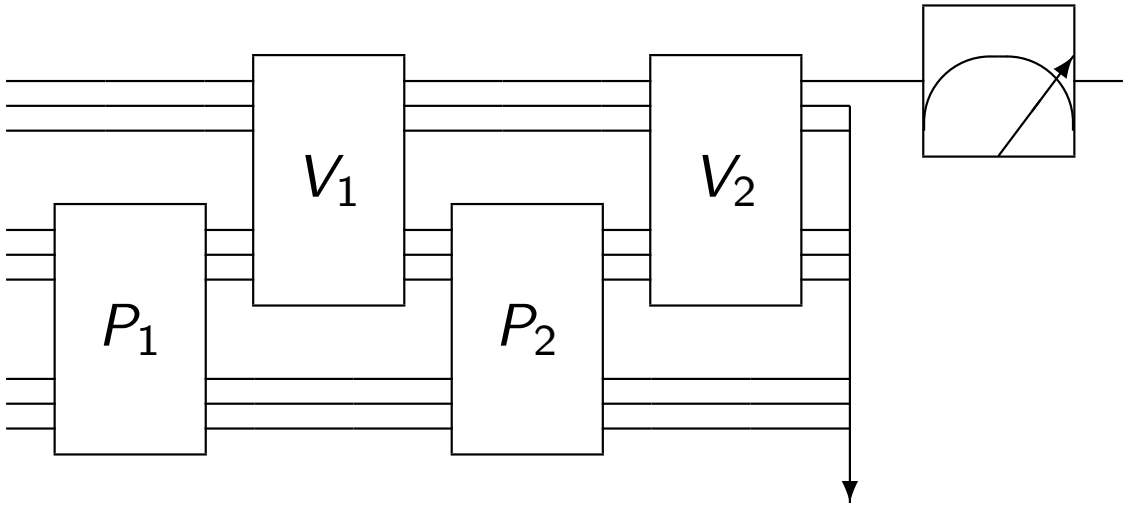
Complexity Classes



P	Classical computation
NP	Classical verifiable computation
BQP	Quantum computation
QMA	Quantum verifiable computation
PSPACE	Classical computation verifiable interactively
QIP	Quantum computation verifiable interactively
EXP	Classical computation in exponential time

Quantum interactive proof systems

- **QIP** is the set of problems that can be verified by interacting with a computationally unbounded prover.

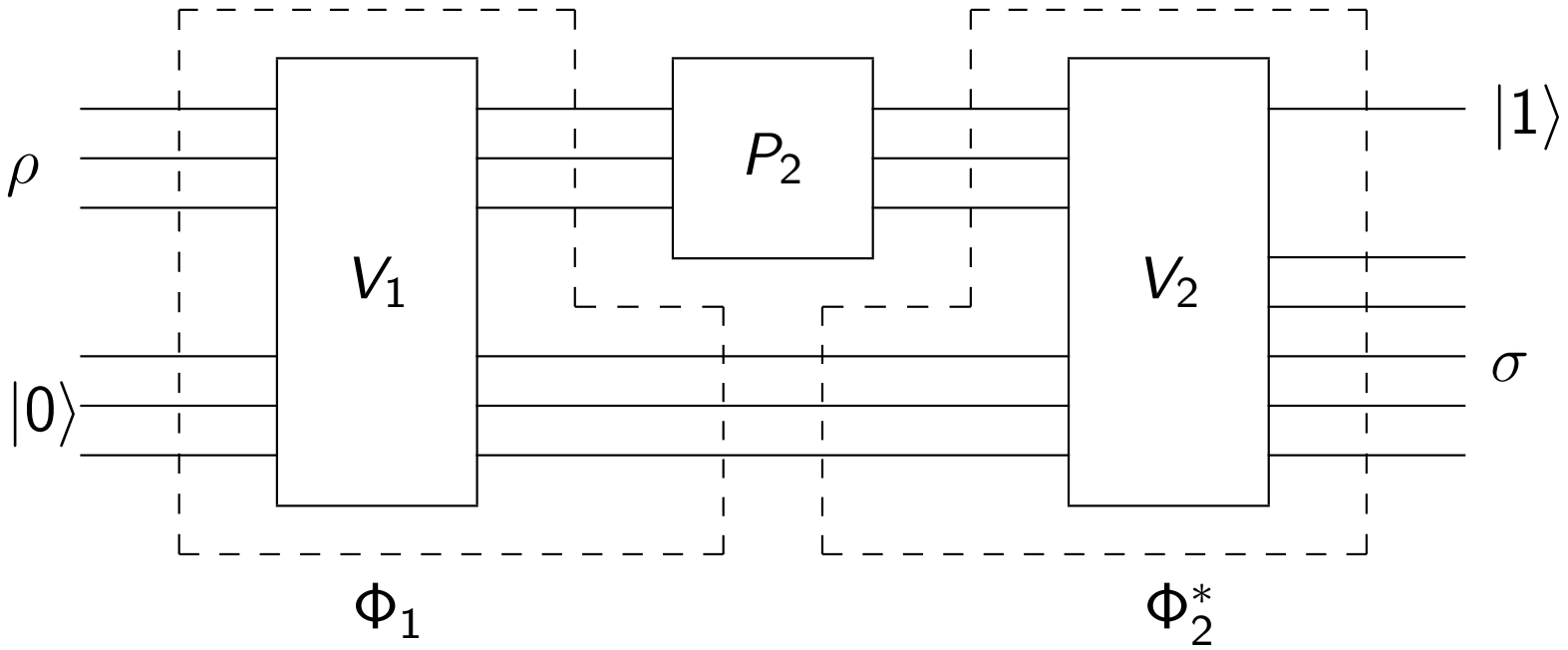


Given a language $L \in \mathbf{QIP}$, there exists a verifier V such that

- If $x \in L$, then there exists P such that $\Pr[V \text{ accepts } P\text{'s proof}] \geq \frac{2}{3}$
- If $x \notin L$, then for any P, $\Pr[V \text{ accepts } P\text{'s proof}] \leq \frac{1}{3}$

QIP-hardness of Close Images

Consider the following two transformations[2]:



The channels are given by: $\Phi_1(\rho) = \mathrm{tr}_{\mathcal{P}}\, V_1(\rho \otimes |0\rangle\langle 0|)V_1^*$

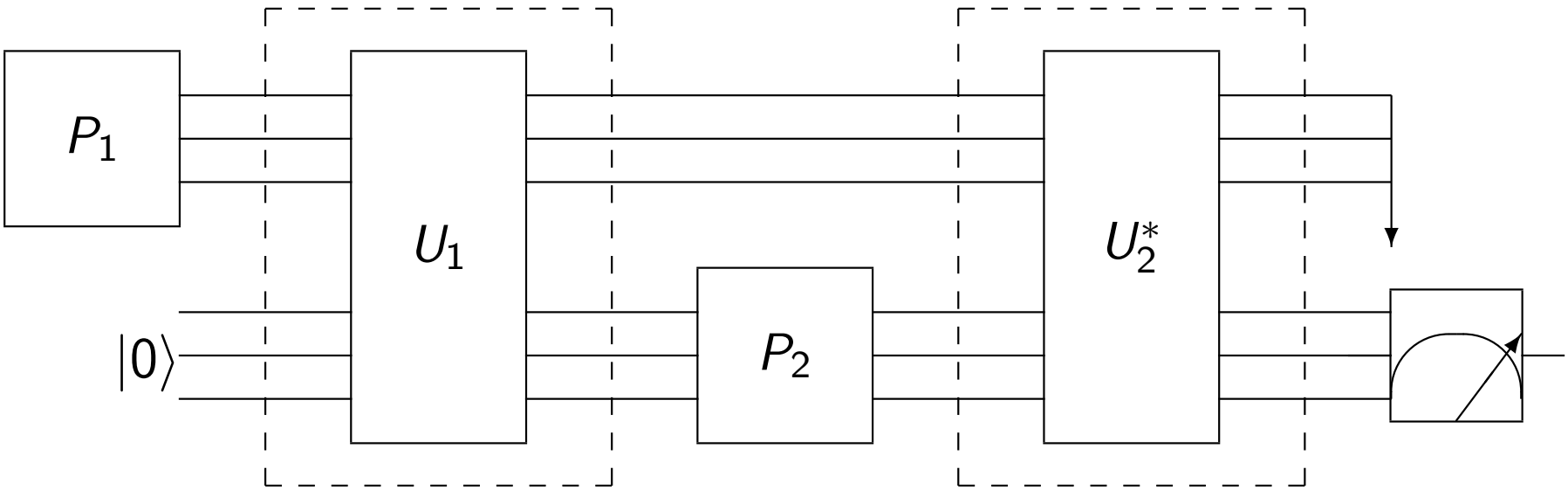
$\Phi_2(\sigma) = \mathrm{tr}_{\mathcal{P}}\, V_2^*(|1\rangle\langle 1| \otimes \sigma)V_2$

- Φ_1 and Φ_2 have close images if and only if V accepts

[2] Kitaev and Watrous 2000

Containment in QIP

The following protocol puts this problem in **QIP**[3]:



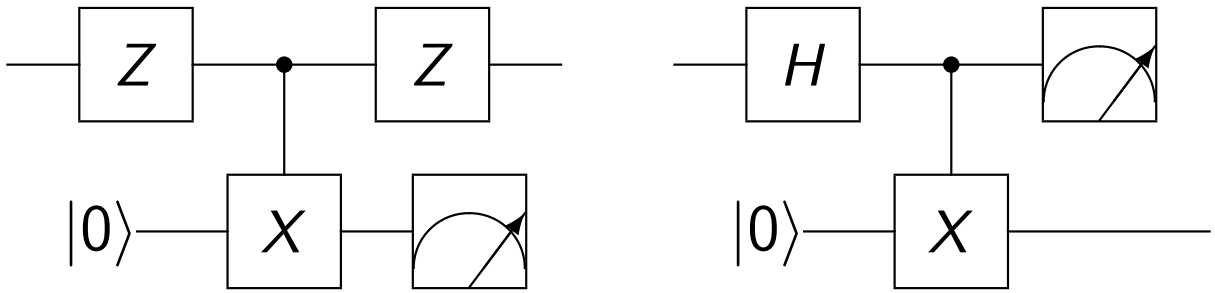
- The transformations have close images if and only if the output qubits are measured in the $|0\rangle$ state.
- This shows that Close Images is **QIP**-complete.

[3] Kitaev and Watrous 2000

Outline

Classical and quantum circuit distinguishability

- What is the compelexity 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 [Janzing, Wocjan, Beth, 03]
- What about general quantum channels?
  - Can be done efficiently in size of matrix representation[4]

[4] Watrous 09; Ben-Aroya and Ta-Shma 09

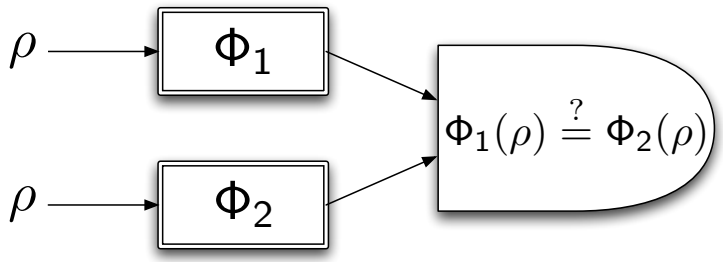
Mixed-state quantum circuit distinguishability

Distinguishability

Given two mixed-state circuits Φ_1, Φ_2, decide between

Yes: $\|\Phi_1 - \Phi_2\|_\diamond \geq 2 - \varepsilon$,

No: $\|\Phi_1 - \Phi_2\|_\diamond \leq \varepsilon$.



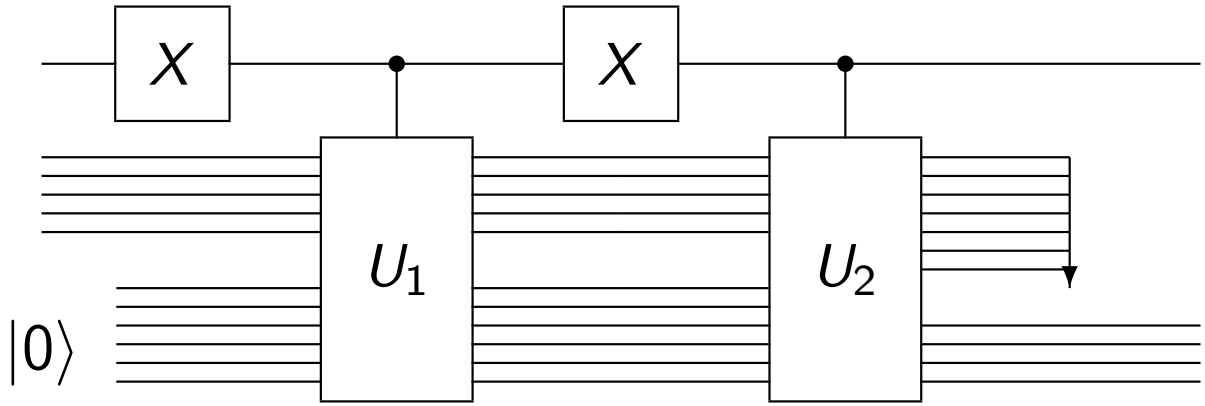
- Less formally: is there and input ρ on which $\Phi_1 \otimes I$ and $\Phi_2 \otimes I$ produce (almost) orthogonal outputs?
- This problem is **QIP**-complete [R. and Watrous, 05].
- This characterizes **QIP** without reference to the model.

Reduction from Close Images, 1

- Given implementations of Φ_1 and Φ_2 as:

$$\Phi_i(\rho) = \mathrm{tr}_{\mathcal{B}}\, U_i(\rho \otimes |0\rangle\langle 0|)U_i^*,$$

construct the circuit given by:

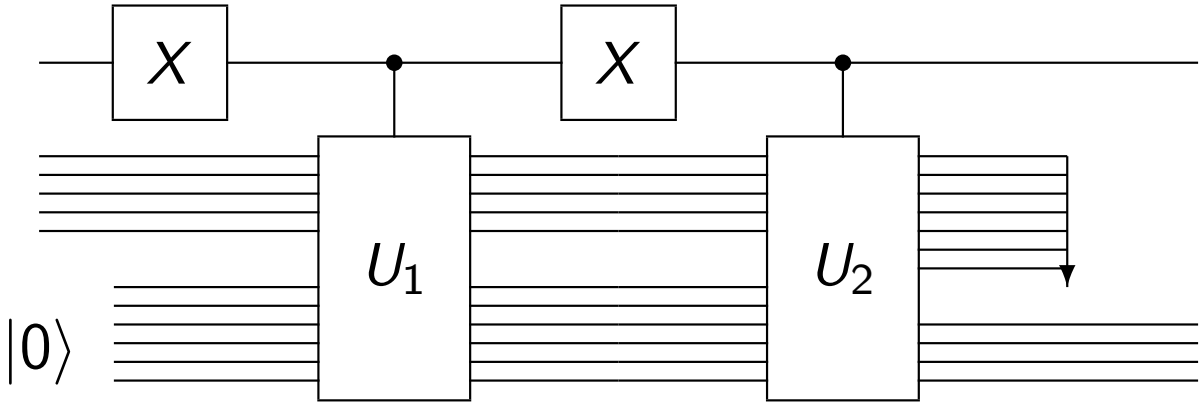


- Consider what happens with the control qubit is $(|0\rangle + |1\rangle)/2$

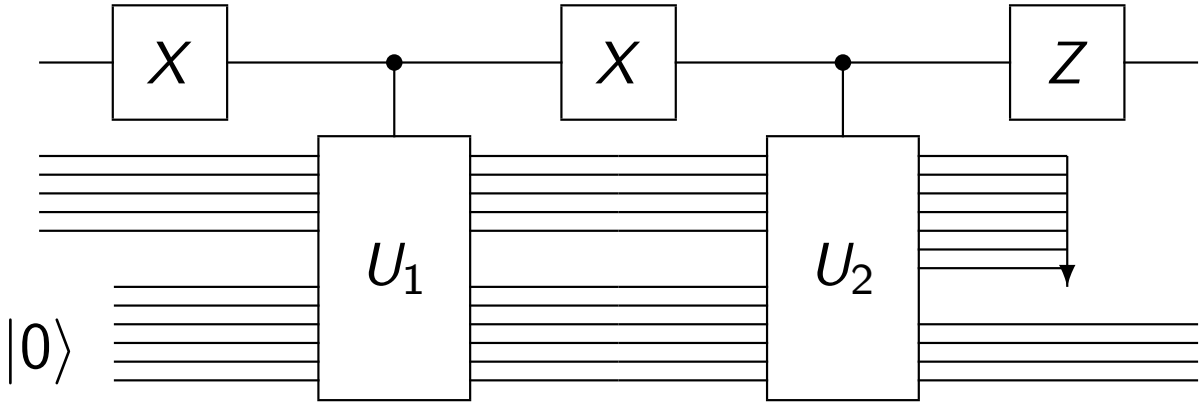
Reduction from Close Images, 2

When the control qubit starts in the $|+\rangle$ state:

- If the original circuits have close images, the output is $|+\rangle$ and $|-\rangle$



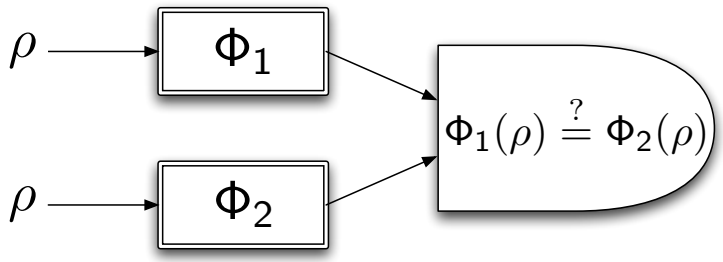
- If the outputs of the originals are far apart, the control qubit is $\mathbb{1}/2$ in both cases



Containment in QIP

Consider the following protocol to solve an instance (Φ_1, Φ_2):

1. V receives input state ρ from prover
2. V chooses $i \in \{1, 2\}$, sends $\Phi_i(\rho)$ to prover
3. V receives $j \in \{1, 2\}$ from prover, accepts iff $i = j$



The prover is being asked to distinguish the two channels, so V accepts with probability $\frac{1}{2} + \frac{1}{4} \left\| \Phi_1 - \Phi_2 \right\|_\diamond$.

Implications

This argument implies that:

- Distinguishing channels (given as circuits) is **QIP**-complete.
- Computing the diamond norm is hard.

Does this have any practical importance?

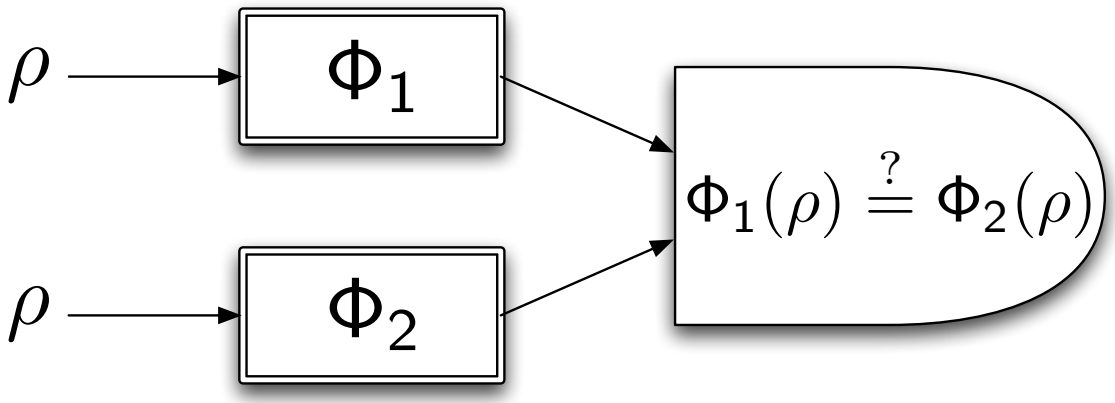
- Even weak process tomography is hard.
- No efficient (general) procedure to check that two implementations are close.

Outline

Classes of channels

How does this problem behave on less general inputs?

- i.e. are the channels seen in practice easy to distinguish?
- can we isolate some property that makes the problem difficult?



- The problem is **QMA**-complete for unitary channels. [JWB 03]

Reductions

We show that a the problem remains **QIP**-complete on:

- channels with log-depth circuits
- mixed-unitary channels
- degradable channels
- anti-degradable channels.

This is done by reducing an instance of the general problem to an instance of the restricted problem, i.e. finding a mapping

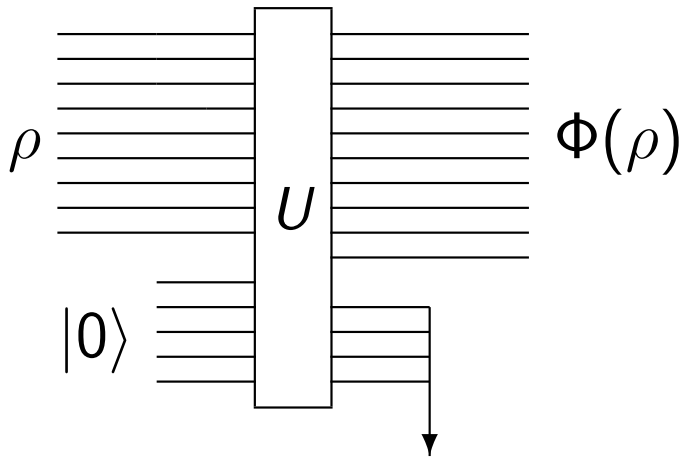
$$(\Phi_1, \Phi_2) \longmapsto (\Psi_1, \Psi_2) \text{ such that } \|\Psi_1 - \Psi_2\|_\diamond \approx \|\Phi_1 - \Phi_2\|_\diamond$$

where Ψ_1 and Ψ_2 are the in the restricted class.

Log-depth Close Images

Is Close Images hard on log-depth circuits?

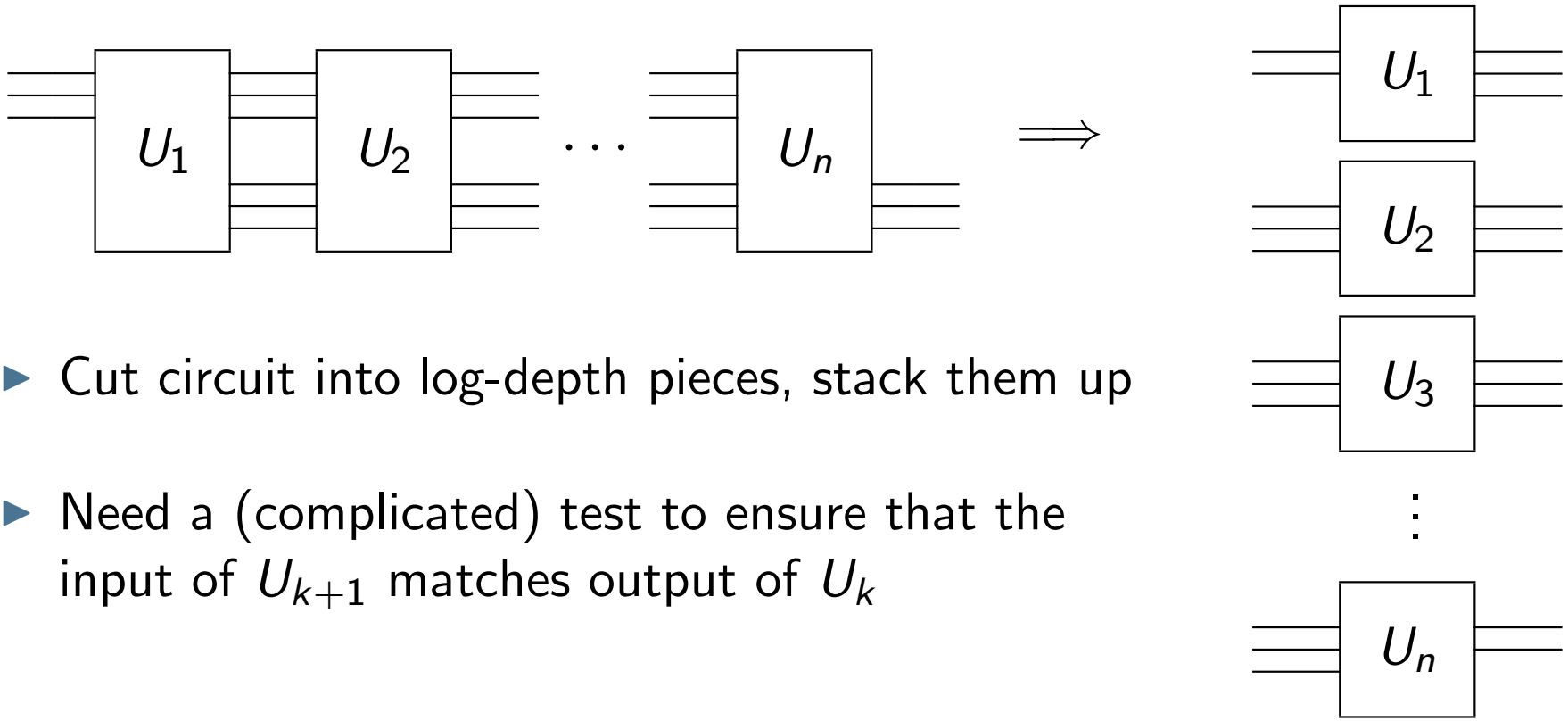
- Many important problems have such circuits, such as the quantum Fourier transform [Cleve and Watrous, 00].



- Close Images remains **QIP**-complete on channels with log-depth circuits.

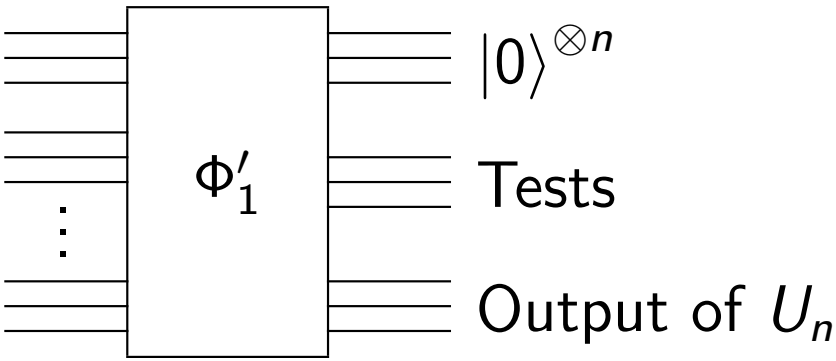
Reduction to log-depth

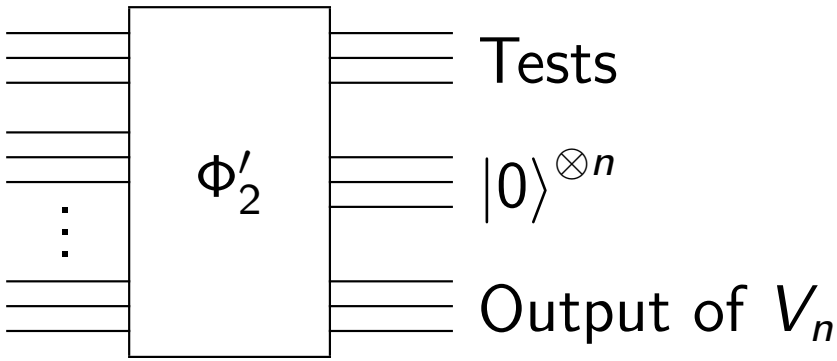
Simple-minded approach:



- Cut circuit into log-depth pieces, stack them up
- Need a (complicated) test to ensure that the input of U_{k+1} matches output of U_k

Resulting circuits

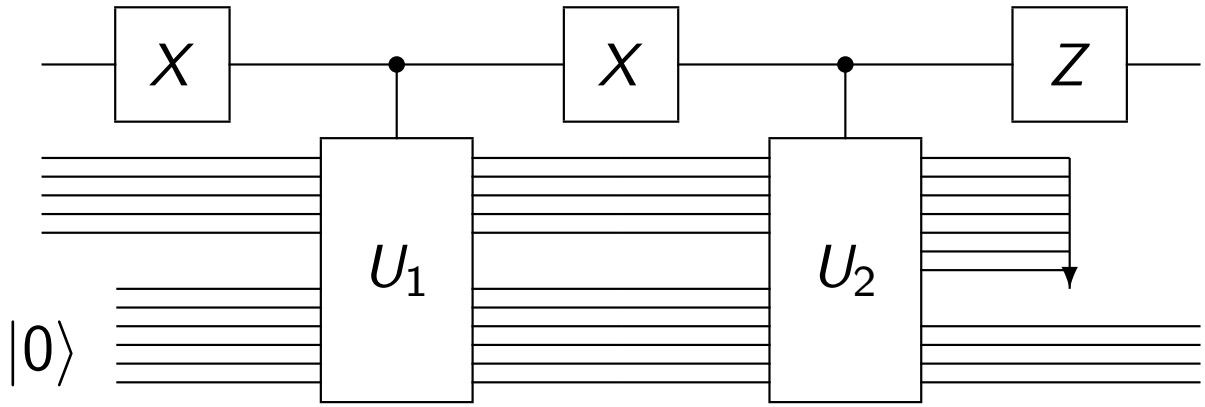




- Add dummy qubits so that if a test fails (outputs $|1\rangle$) then the outputs of the two circuits will be far apart.
- If the circuits have similar outputs, the tests have all passed, so the circuits Φ'_1 and Φ'_2 simulate the original instance.
- Log-depth Close Images is **QIP**-complete.

Log-depth distinguishability

- The reduction to distinguishability preserves log-depth circuits:



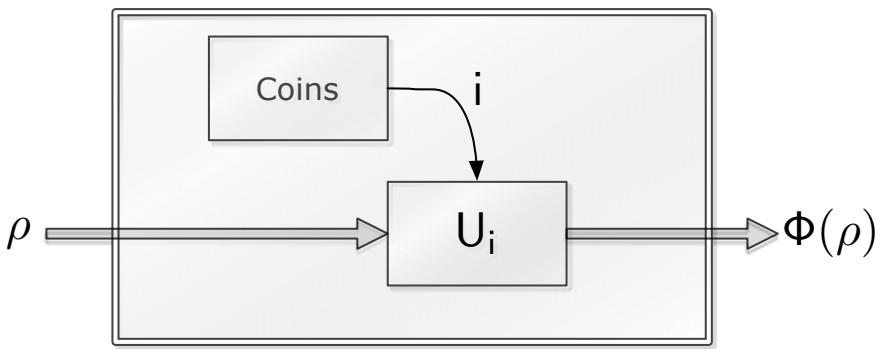
- Log-depth Distinguishability is also **QIP**-complete.

Mixed-unitary channels

Definition

A channel Φ is *mixed-unitary* if there exists a probability distribution p_i and unitaries U_i such that

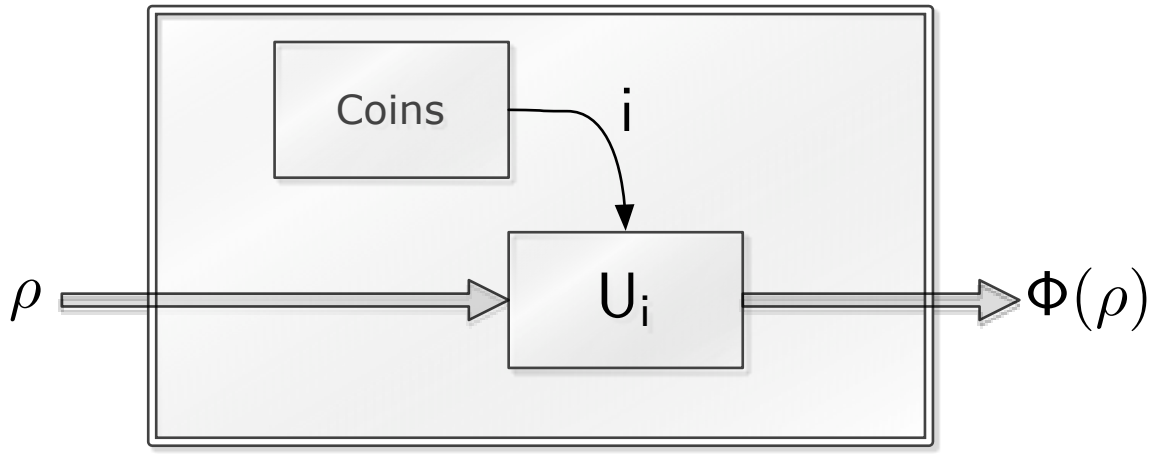
$$\Phi(X) = \sum_i p_i U_i X U_i^*.$$



Examples:

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

Why you should care about mixed-unitary channels



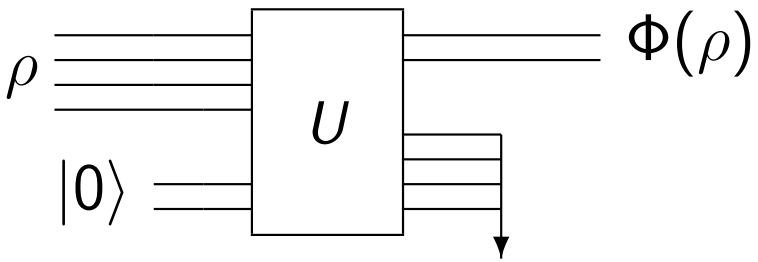
- Exactly reversible by measuring environment, correcting[5]
- Non-contractive with respect to entropy
- Classical capacity is additive for qubit mixed unitary channels[6], not additive for large enough channels[7]

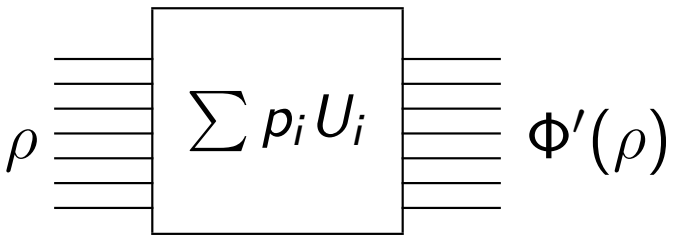
[5] Gregoratti and Werner 03
[6] Tregub 86, King 02
[7] Hastings 09

Simulating a circuit with a mixed-unitary circuit

Strategy:

- Given Φ, find approximation Φ' that is mixed-unitary



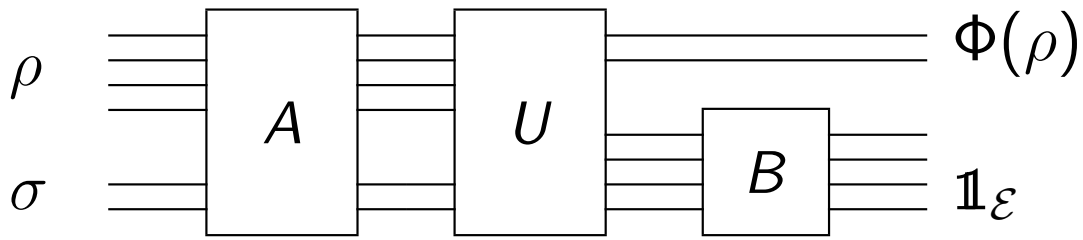


Only two operations that are not mixed-unitary:

1. Partial trace
2. Ancillary qubits in $|0\rangle$ state

The simulation

- Given input $\rho \otimes |0\rangle\langle 0|$ the output is $\Phi(\rho) \otimes \mathbb{1}_{\mathcal{E}}$
- If the input is not in $\mathcal{H} \otimes \{|0\rangle\}$, the output is highly mixed



- The result is random unitary, since all of the components are.

Mixed-unitary distinguishability

Theorem

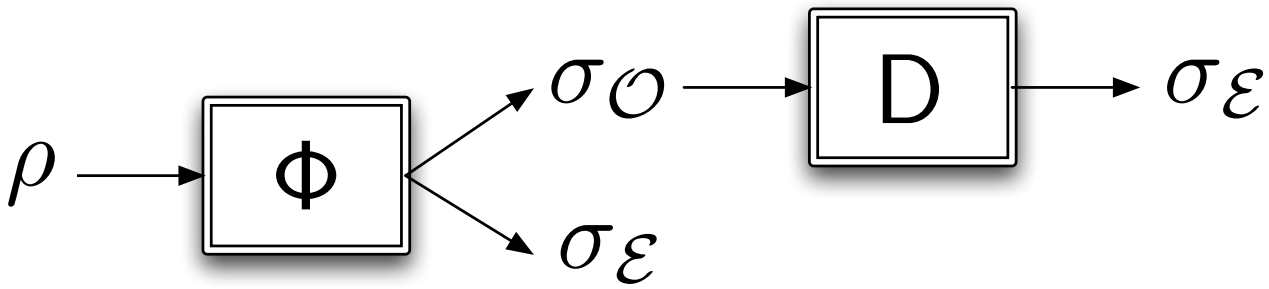
Let Φ_1, Φ_2 be channels with input plus ancillary dimension d, and let Φ_1', Φ_2' be the mixed-unitary approximations of them. Then

$$\|\Phi_1 - \Phi_2\|_\diamond \leq \left\|\Phi_1' - \Phi_2'\right\|_\diamond \leq \|\Phi_1 - \Phi_2\|_\diamond + O(1/d).$$

- The error is exponentially small in the number of qubits.
- Mixed-unitary Distinguishability is **QIP**-complete.

Degradable and antidegradable channels

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



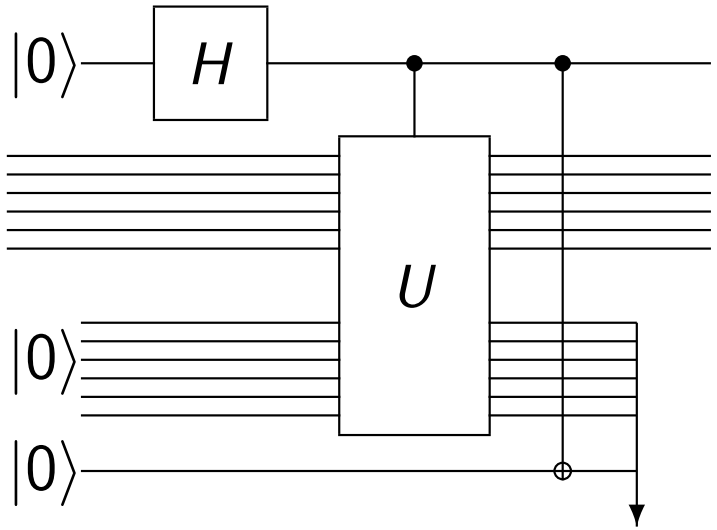
- These channels are not additive.[8]
- DISTINGUISHABILITY remains **QIP**-complete on this class.

[8] Cubitt, Ruskai, Smith 08; Hastings 09

Reduction to the degradable case

- For any channel Φ, construct the degradable channel[9]

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



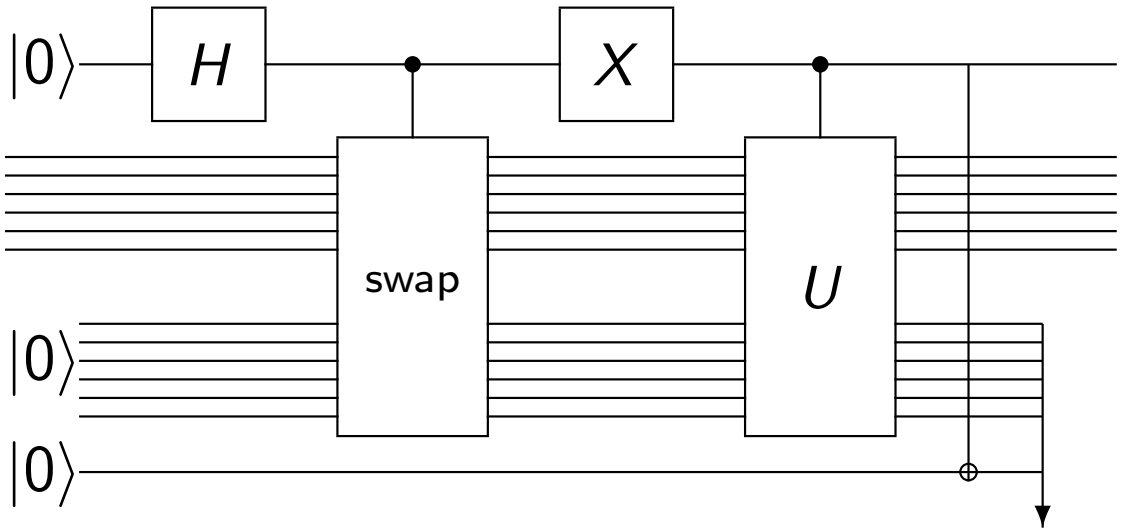
- The diamond norm satisfies $\|\Phi'\|_\diamond = \|\Phi\|_\diamond / 2$

[9] Cubitt, Ruskai, Smith 08

Reduction to the antidegradable case

- For any channel Φ, construct the antidegradable channel

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



- The diamond norm satisfies $\|\Phi'\|_\diamond = \|\Phi\|_\diamond / 2$

Reduction to degradable/antidegradable channels

- Reduction from DISTINGUISHABILITY with error (a, b) to degradable (or antidegradable) case with error $(a/2, b/2)$.

Lemma (R. and Watrous 05)

If $\|\Psi_1 - \Psi_2\|_\diamond = \delta$, *then*

$$2 - 2e^{\frac{-k\delta^2}{8}} < \left\|\Phi_1^{\otimes k} - \Phi_2^{\otimes k}\right\|_\diamond \leq k\delta.$$

- This implies that DISTINGUISHABILITY is **QIP**-complete on the degradable and the antidegradable channels.

Outline

Summary of results

- Approximating $\|\Phi - \Psi\|_\diamond$ is hard (Φ, Ψ given as circuits).
- This is true even if Φ, Ψ have log-depth circuits.
- This is true even if Φ, Ψ are mixed-unitary.
- This is true even if Φ, Ψ are degradable or antidegradable.

Open problems

- How to decide if a black-box channel is unitary?
- Extend hardness to entanglement-breaking or Pauli channels?
- Can these reductions tell us anything about other problems?