How hard is it to decide if a quantum state is separable or entangled?

Mark M. Wilde

School of Computer Science, McGill University

In collaboration with
Patrick Hayden and **Kevin Milner**

arXiv:1211.6120

APS March Meeting,
Baltimore, Maryland, USA, March 21, 2013

Separability

Separable states can be written as

$$\sigma_{AB} = \sum_{x \in \mathcal{X}} p_X(x) \; |\psi_x\rangle\langle\psi_x|_A \otimes |\phi_x\rangle\langle\phi_x|_B$$

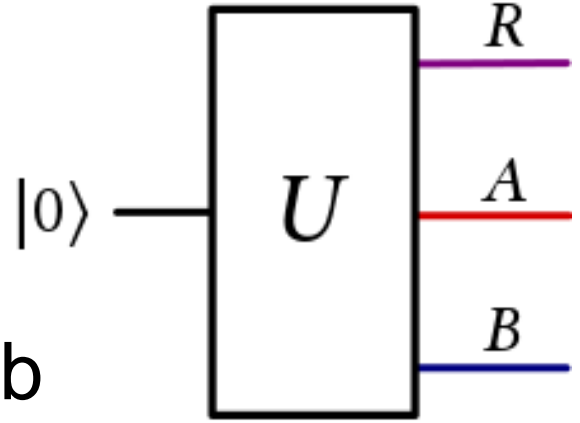
They admit a “local hidden variable theory”

The set of separable states is *convex*.

Any state that is not separable is **entangled**.

A Quantum Separability Problem

You are given:



1) A description of a **quantum circuit**, along with a specification of which qubits are for the "reference", Alice, & Bob

(*trace over the reference qubits*)

2) A **promise** that the state is either close or far from **separable** (in a specific sense)

Your task: Decide which is the case!

The complexity parameter is **circuit size** (number of gates)

Hint: You don't want to think about this classically!

A tool: k-extendibility

A state ρ_{AB} is ***k*-extendible** if there exists a state $\omega_{A\,B1\,\ldots\,Bk}$ such that

1) ω is **invariant under perm's** of the B systems.

2) Tracing over all systems of except A and $B1$ gives ρ_{AB}.

K-extendibility ctd.

Any separable state is trivially *k*-extendible for any *k*. A *k*-extension is just:

$$\sum_{x \in \mathcal{X}} p_X(x) \; |\psi_x\rangle\langle\psi_x|_A \otimes |\phi_x\rangle\langle\phi_x|_{B_1} \otimes \cdots \otimes |\phi_x\rangle\langle\phi_x|_{B_k}$$

For later: Observe that a purification is

$$\sum_{x \in \mathcal{X}} \sqrt{p_X(x)} \; |x\rangle_{R'} \otimes |\psi_x\rangle_A \otimes |\phi_x\rangle_B \otimes |\phi_x\rangle_{B_2} \otimes \cdots \otimes |\phi_x\rangle_{B_k}$$

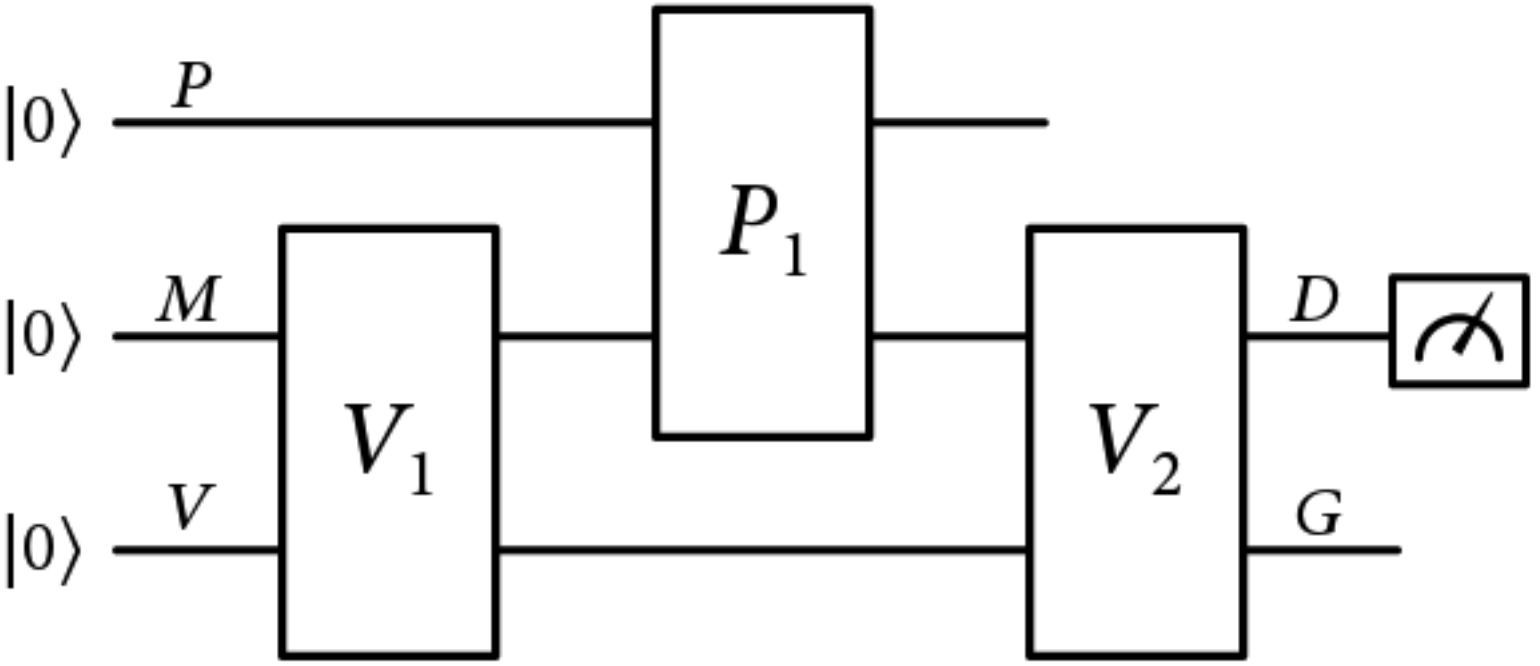
On the other hand, for any entangled state, there exists a *k* such that it is not *k'*-extendible for all $k' \geq k$

Intuitively, related to **monogamy of entanglement**

Quantum Interactive Proofs

1) A model of computation in which you are allowed to interact with an all-powerful, yet untrustworthy prover

2) A way for characterizing complexity (for example, it is known that QIP = PSPACE)



Formal Statement

QSEP-CIRCUIT(δ_c, δ_s) Given is a mixed-state quantum circuit to generate the n-qubit state ρ_{AB}, along with a labeling of the qubits in the reference system R and the output qubits for A and B. Decide whether

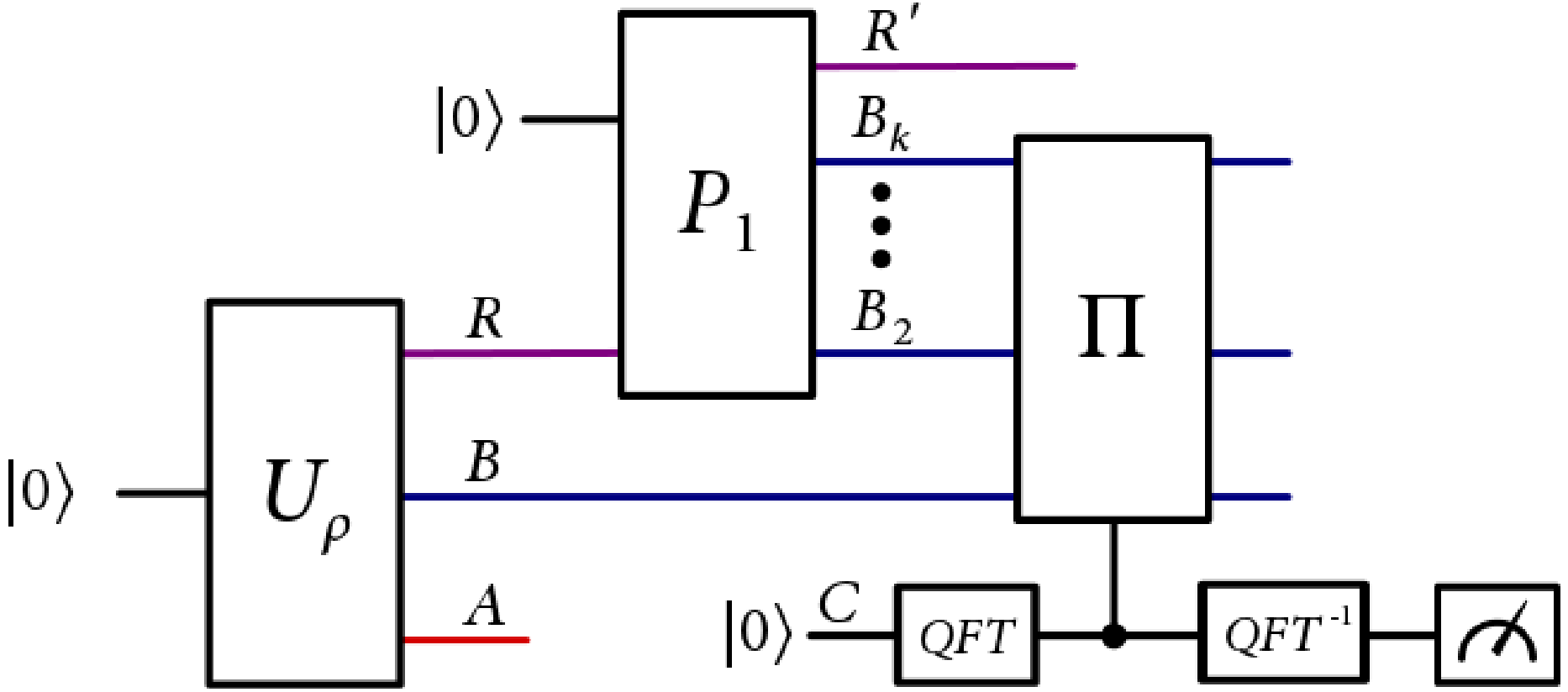
1. Yes: There is a separable state $\sigma_{AB} \in \mathcal{S}$ that is δ_c-close to ρ_{AB} in trace distance:
$$\min_{\sigma_{AB} \in \mathcal{S}} \|\rho_{AB} - \sigma_{AB}\|_1 \leq \delta_c.$$

2. No: Every separable state is at least δ_s-far from ρ_{AB} in 1-LOCC distance:
$$\min_{\sigma_{AB} \in \mathcal{S}} \|\rho_{AB} - \sigma_{AB}\|_{1-\mathrm{LOCC}} \geq \delta_s.$$

Two-message QIP system

Idea for a proof system:

Prover should try to convince you that
the state is separable, but you have to make sure
he's not trying to cheat....



Conclusion and Unmentioned Results

- This variant of the quantum separability problem is

In QIP(2), Hard for QSZK, Hard for NP

- We know that the complement is in PSPACE

Follows from QIP(3) being closed under complement or by giving a Short Quantum Game for it...

- We have established that other variants are

BQP-complete, QMA-complete, and QIP-complete

(*the one I presented is thus the "odd man out"*)