Two-msg quantum interactive proofs & the quantum separability problem

Mark M. Wilde

School of Computer Science, McGill University

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

arXiv:1211.6120

IEEE? Conference on Computational Complexity,
Palo Alto, California, USA, June 6, 2013

Primer on Quantum Information

Short Primer on Quantum Information

A quantum state is specified mathematically by a **density matrix** (positive semi-definite, trace one):

$$\rho \geq 0 \quad \mathrm{Tr}\{\rho\} = 1$$

Special cases: **pure states** are rank one and **classical states** are all diagonal in some O.N. basis

Rank-1 pure states are in 1-1 correspondence with state vectors:

$$\rho = |\psi\rangle\langle\psi| \Leftrightarrow |\psi\rangle$$

Joint Quantum Systems

Density matrices on multiple systems act on a tensor-product Hilbert space.

For example, if system *A* is specified by ρ, system *B* by σ, and the systems are independent (not having interacted before),
then the joint state is described by

$$\rho \otimes \sigma$$

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**.

Entangled states are responsible for many
of the enhancements in quantum information processing

Purifications

Critical difference between classical and quantum info.:

Any quantum state can be **"purified."**

That is, for every mixed quantum state ρ on system A,
there exists a pure state on systems R and A,
such that we recover the original state ρ
when discarding system R.

Proof by construction:

$$\rho_A = \sum_x \lambda_x |x\rangle\langle x|_A \qquad |\psi_\rho\rangle = \sum_x \sqrt{\lambda_x} |x\rangle_R \otimes |x\rangle_A$$

Important observation: All purifications are related by unitary operations on the purifying system.

Quantum Evolutions

Quantum systems evolve according to **completely-positive, trace-preserving maps** acting on the space of density operators.

(*The two conditions ensure that the map outputs a legitimate quantum state when acting locally on part of a larger quantum system and that it preserves probability.*)

Choi-Kraus theorem Any such map has a representation of the following form:

$$\mathcal{N}(\rho) = \sum_x A_x \rho A_x^\dagger \qquad \text{where} \qquad \sum_x A_x^\dagger A_x = I$$

Special case: Noiseless transformations are **unitary**, and classical stochastic matrices can be embedded

Quantum Separability Problem

Quantum Separability Problem

You are given:

1) A quantum state on systems *A* & *B*

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

Your task: Decide which is the case!

Quantum Separability Problem

The complexity of the quantum separability problem depends on how the state is given and what the complexity parameter is.

Gurvits' version:
the state is specified by a **matrix** and
the complexity parameter is the **dimension**

Promise:

1) $\rho_{AB} \in \mathcal{S}$

2) $\min_{\sigma_{AB} \in \mathcal{S}} \left\| \rho_{AB} - \sigma_{AB} \right\|_2 \geq \varepsilon$

Quantum Sep. Problem (ctd.)

If $\varepsilon \geq \frac{1}{\mathrm{poly}(d)}$

then the q. sep. problem is NP-hard

(Gharibian 2008)

If ε is a constant, then there is a quasi-poly time algorithm to decide it

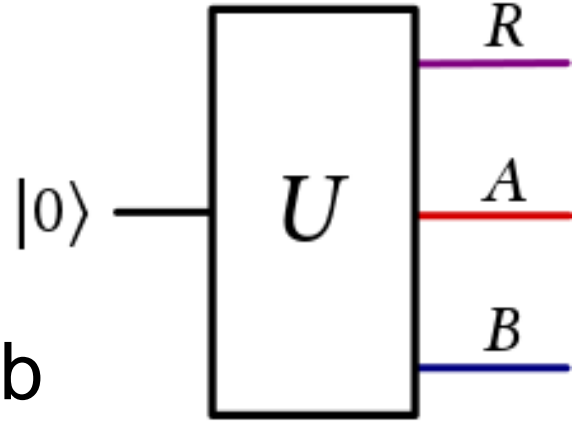
(Brandao, Christandl, and Yard 2010)

Running time is $\exp\{O(\varepsilon^{-2} \log d_A \log d_B)\}$

Our Results

Our Quantum Sep. 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!

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

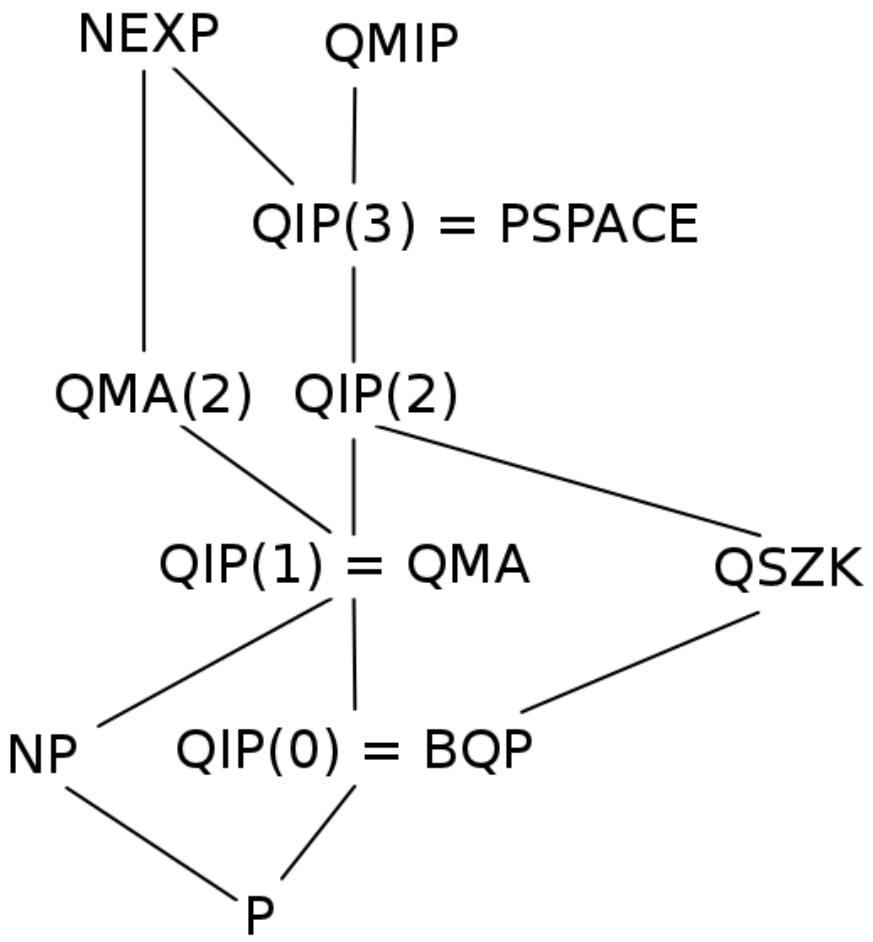
1. Yes: There is a separable state $\sigma_{AB} \in \mathcal{S}$ that is δ_c-close to ρ_{AB} in trace distance:
$$\min_{\sigma_{AB} \in \mathcal{S}} \|\rho_{AB} - \sigma_{AB}\|_1 \leq \delta_c.$$

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

Main Results

QSEP-CIRCUIT is in QIP(2)

QSEP-CIRCUIT is hard for QSZK and NP



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

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

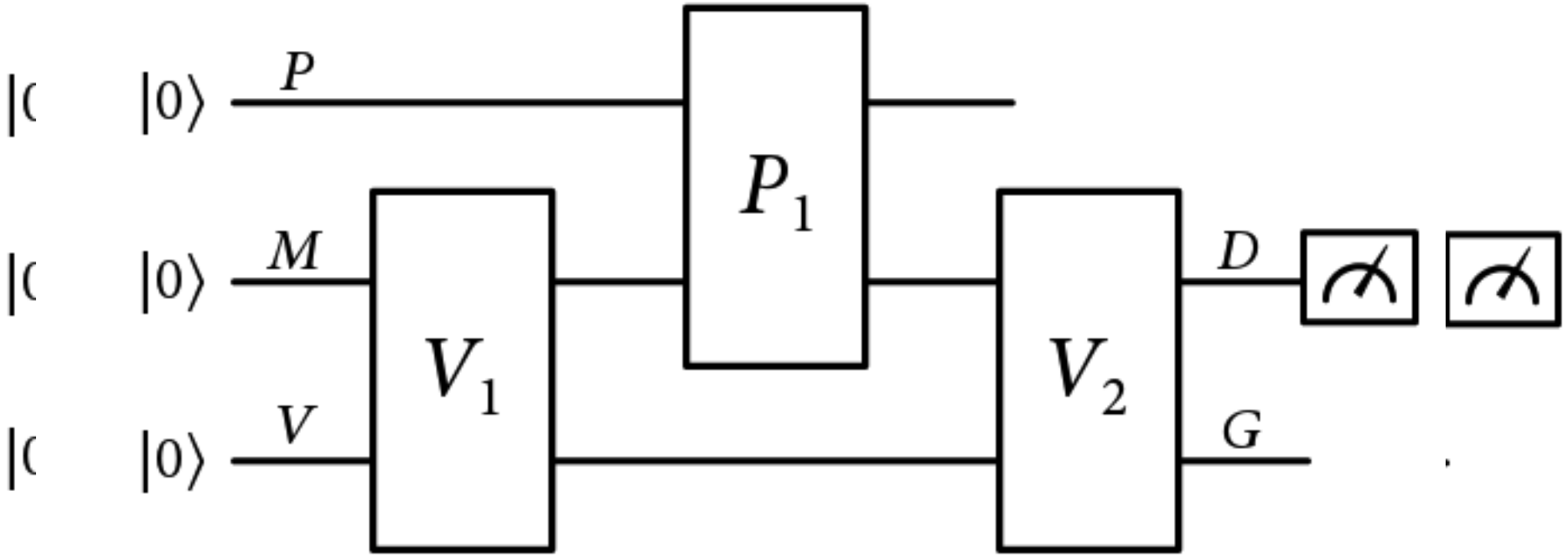
On the other hand, for any entangled state, there exists a *k* such that it is not *k′*-extendible for all $k' \geq k$

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)



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....

Maximum Acceptance Probability

An upper bound on the
maximum acceptance probability
of this proof system is given by
the **maximum *k*-extendible fidelity**

$$\max_{\sigma_{AB} \in \mathcal{E}_k} F(\rho_{AB}, \sigma_{AB})$$

where

$$F(\rho_{AB}, \sigma_{AB}) \equiv \| \sqrt{\rho_{AB}} \sqrt{\sigma_{AB}} \|_1^2$$

In the limit as *k* becomes large,
we obtain an entanglement measure
by taking the negative logarithm.

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"*)