QSEP-STATE $\in$ QMIP$_{ne}$

Christopher Bahr[1], Eric Hanson[2]

Department of Computer Science, McGill University

QMA & QMIP

QMA is the quantum analogue of NP; specifically, QMA is the class of promise problems such that there exists a polynomial quantum verifier V with

- Completeness: If the answer is "YES," then there exists a polynomial size quantum proof such that V accepts with probability at least 2/3.
- Soundness: If the answer is "NO," then for all polynomial size messages, V accepts with probability at most 1/3.

The completeness and soundness bounds 1/3 and 2/3 seem arbitrary, but by running the protocol polynomial times, the error can be reduced exponentially. The completeness and soundness bounds can even be functions of the input size, as long as they are separated by at least an inverse polynomial in the input size [MW05].

Figure 1: An instance of a problem in QMA can be solved by the short protocol where an unbounded prover sends a single message to a polynomial verifier, who processes it and outputs "YES" or "NO".

Quantum Interactive Proof (QIP) defines the class of problems which can be solved by multiple rounds of communication between the prover and the verifier.
Finally QMIP allows multiple rounds of communication with multiple provers who cannot communicate but can share entanglement. We are interested in the related class QMIP$_{ne}$ where entanglement between the provers is prohibited, as defined in [KM01] where it was also shown that QMIP$_{ne}$ = NEXP.

The Problem

Quantum state separability (**QSEP-STATE**(δ_c, δ_s))

Input: 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

Promise: Either "YES", there is a separable state $\sigma_{AB} \in \mathcal{S}$ that is δ_c−close to ρ_{AB} in trace distance:

$$\min_{\sigma_{AB} \in \mathcal{S}} \|\rho_{AB} - \sigma_{AB}\|_1 \leq \delta_c$$

or "NO", every separable state is at least δ_s−far from ρ_{AB} in trace distance:

$$\min_{\sigma_{AB} \in \mathcal{S}} \|\rho_{AB} - \sigma_{AB}\|_1 \geq \delta_s$$

Output: Decide which one is the case.

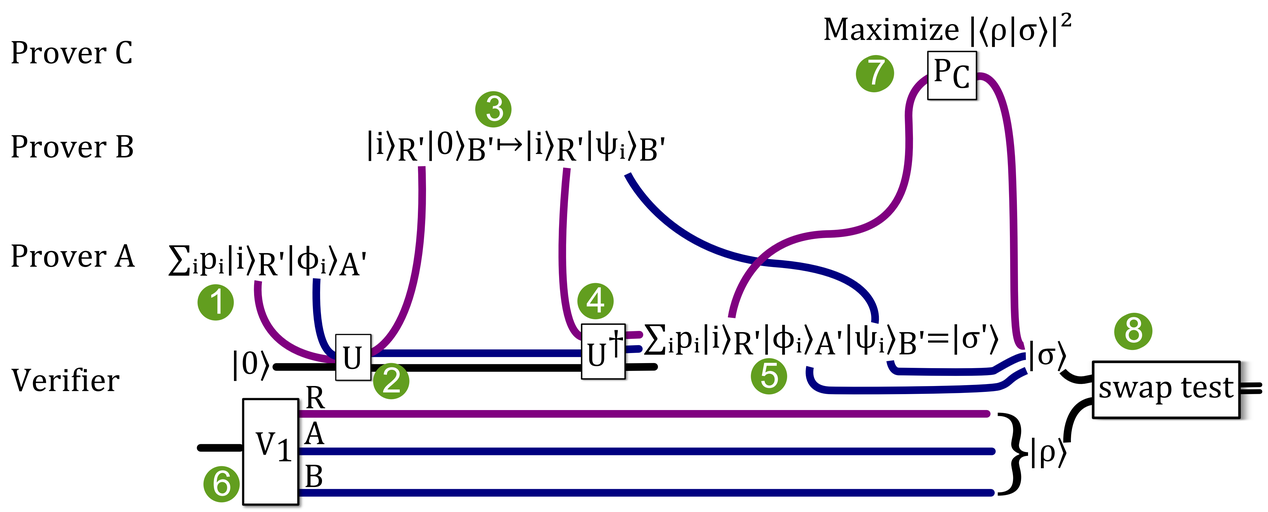
The Swap Test

The swap operation S simply swaps two states ($S|\varphi\rangle|\psi\rangle = |\psi\rangle|\varphi\rangle$). The swap test between $|\varphi\rangle$ and $|\psi\rangle$ is the following: A control state is initialized to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and the states are swapped conditioned on the control qubit being $|1\rangle$; this yields the state $\frac{1}{\sqrt{2}}(|0\rangle|\varphi\rangle|\psi\rangle + |1\rangle|\psi\rangle|\varphi\rangle)$. Then the Hadamard gate is applied and the control qubit measured in the standard basis; if the result is $|0\rangle$, the swap test passes. It can be shown that this happens with probability $\frac{1}{2}(1 + |\langle\psi|\varphi\rangle|^2)$. For example, see [MGHW13].

The Protocol

1. Prover A constructs half of a separable state:
$$\sum_i \sqrt{p_i}|i\rangle_{R'}|\varphi_i\rangle_{A'}$$
and sends it to the verifier.
2. The verifier dephases by performing the operation $U : |0\rangle_V|i\rangle_{R'} \mapsto |i\rangle_V|i\rangle_{R'}$ (where V indicates the verifier's private qubits) and sends the R' system to Prover B
3. Prover B performs the operation $|i\rangle_{R'}|0\rangle_{B'} \mapsto |i\rangle_{R'}|\psi_i\rangle_{B'}$ and sends R' and B' to the verifier
4. The verifier performs $U^\dagger$ on his private qubits and the R' system to add the phases back
5. The verifier now has the state
$$|\sigma'\rangle = \sum_i \sqrt{p_i}|i\rangle_{R'}|\varphi_i\rangle_{A'}|\psi_i\rangle_{B'}$$
6. The verifier uses the input circuit to construct a purification of ρ, $|\rho\rangle$.
7. The verifier sends the reference system of $|\sigma'\rangle$ to Prover C, who applies a unitary P_C. The system of R', A', B' after the unitary is applied is $|\sigma\rangle$. Prover C chooses P_C in order to maximize $|\langle\rho|\sigma\rangle|^2$ (which maximizes the probability of the swap test passing).
8. Prover C returns the reference system to the verifier, who performs the swap test with $|\rho\rangle$ and $|\sigma\rangle$. The verifier accepts if and only if the swap test does.

Diagram of the Protocol



A Simple Corollary

In the channel version of this problem, QSEP-CHANNEL, the circuit is replaced by a channel. The promise is that either there exists an input to the channel such that the output is close to separable or for any input to the channel the output is far from separable.
The channel version can also be shown to be in QMIP$_{ne}$ by simply having another prover send the ideal input state to the verifier and then running the protocol featured here.

Future Work

We are currently working with a similar problem, QPROD-CHANNEL. Here we test whether the output state of the channel is product across some cut, rather than separable. It can easily be placed in QMIP$_{ne}$ using a somewhat simpler version of this protocol. We are working to place a tighter upper bound on the problem.

References

[KM01] H. Kobayashi and K. Matsumoto, *Quantum Multi-Prover Interactive Proof Systems with Limited Prior Entanglement*, eprint arXiv:cs/0102013 (2001).

[MGHW13] K. Milner, G. Gutoski, P. Hayden, and M. M. Wilde, *Quantum interactive proofs and the complexity of entanglement detection*, ArXiv e-prints (2013).

[MW05] C. Marriott and J. Watrous, *Quantum Arthur-Merlin Games*, eprint arXiv:cs/0506068 (2005).

Acknowledgements

We would like to thank Patrick Hayden for supervising this project and Kevin Milner for his help throughout.