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

Christopher Bahr [1,3] Eric Hanson [2,3] Prof. Patrick Hayden [1,3,4]

[1]Dept. Computer Science, McGill University

[2]Dept. Math, McGill University

[3]Dept. Physics, McGill University

[4]Dept. of Physics, Stanford University

January 15, 2014

Interactive Proof Systems

- An interactive proof system models computation as the exchange of messages between "provers" and a "verifier".

Interactive Proof Systems

- An interactive proof system models computation as the exchange of messages between "provers" and a "verifier".
- The provers have unlimited computational power but cannot be trusted

Christopher Bahr , Eric Hanson , Prof. Patrick Hayden

Interactive Proof Systems

- An interactive proof system models computation as the exchange of messages between "provers" and a "verifier".
- The provers have unlimited computational power but cannot be trusted
  - so the provers always wants to convince the verifier that the input is a "yes" instance of the problem

Interactive Proof Systems

- An interactive proof system models computation as the exchange of messages between "provers" and a "verifier".
- The provers have unlimited computational power but cannot be trusted
  - so the provers always wants to convince the verifier that the input is a "yes" instance of the problem
- The verifier only has bounded computational power

Interactive Proof Systems

- An interactive proof system models computation as the exchange of messages between "provers" and a "verifier".
- The provers have unlimited computational power but cannot be trusted
  - so the provers always wants to convince the verifier that the input is a "yes" instance of the problem
- The verifier only has bounded computational power
- The verifier and provers exchange messages

Interactive Proof Systems

- An interactive proof system models computation as the exchange of messages between "provers" and a "verifier".
- The provers have unlimited computational power but cannot be trusted
  - so the provers always wants to convince the verifier that the input is a "yes" instance of the problem
- The verifier only has bounded computational power
- The verifier and provers exchange messages
- Require completeness: if the statement is true, the verifier will be convinced by the provers

Interactive Proof Systems

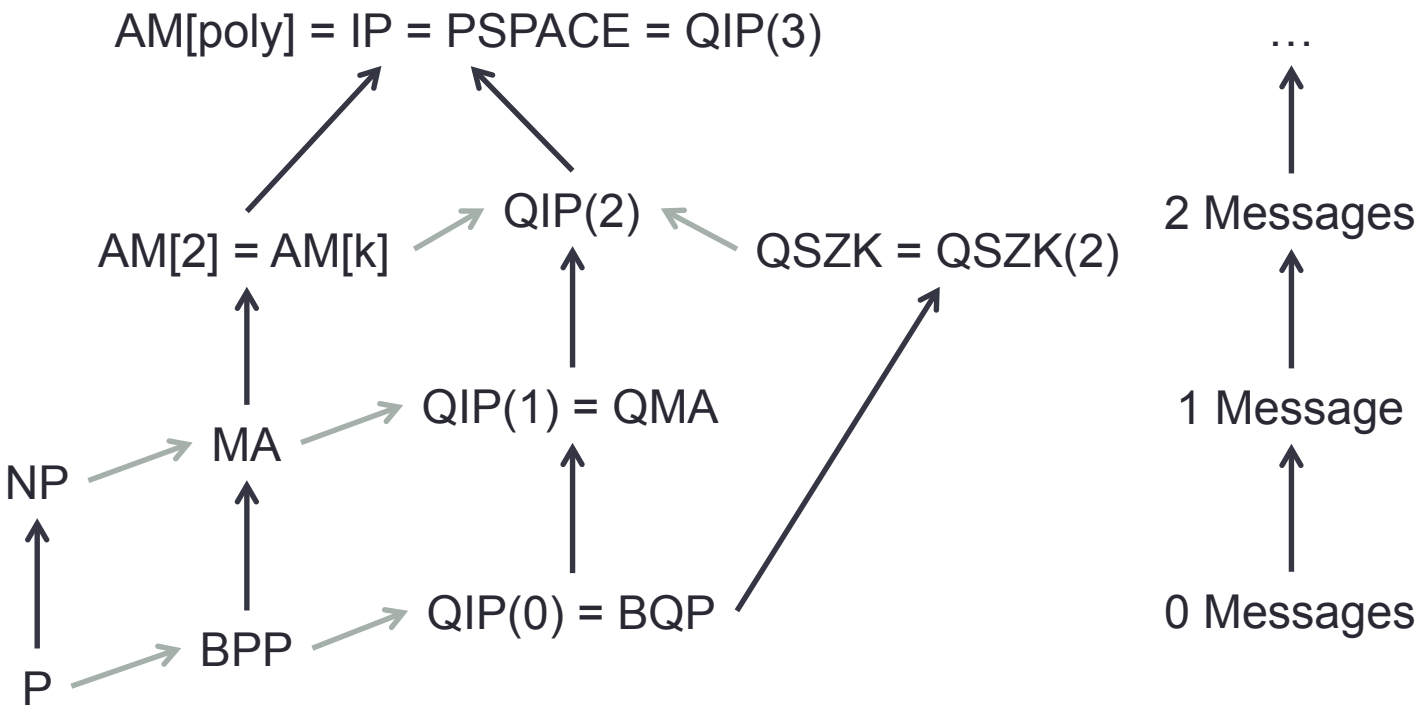
- An interactive proof system models computation as the exchange of messages between "provers" and a "verifier".
- The provers have unlimited computational power but cannot be trusted
  - so the provers always wants to convince the verifier that the input is a "yes" instance of the problem
- The verifier only has bounded computational power
- The verifier and provers exchange messages
- Require completeness: if the statement is true, the verifier will be convinced by the provers
- and soundness: if the statement is false, the provers will only have a small probability of convincing the verifier

Complexity classes

- A complexity class is a set of problems that can be solved subject to different limitations of resources.

Complexity classes

- A complexity class is a set of problems that can be solved subject to different limitations of resources.



Note: black arrows are inclusions; grey arrows are generalizations.

$QMIP_{ne}$

$QMIP_{ne}$ is a quantum complexity class defined as an interactive proof system. A polynomial quantum verifier interacts with multiple unentangled provers by sending an receiving messages. There is no restriction on the number of provers or messages.

A promise problem is in $QMIP_{ne}$ if two conditions hold:

- Completeness: If the answer is "YES," then there exists a protocol such that V accepts with probability at least $2/3$.

$QMIP_{ne}$

$QMIP_{ne}$ is a quantum complexity class defined as an interactive proof system. A polynomial quantum verifier interacts with multiple unentangled provers by sending an receiving messages. There is no restriction on the number of provers or messages.
A promise problem is in $QMIP_{ne}$ if two conditions hold:

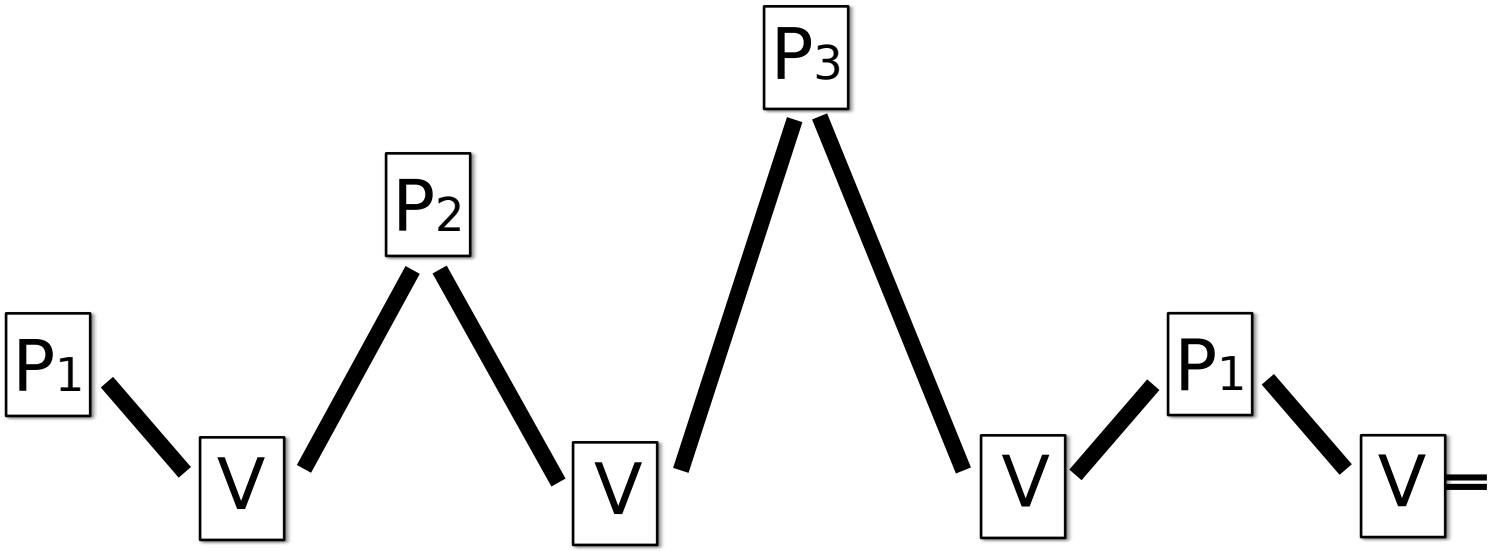
- Completeness: If the answer is "YES," then there exists a protocol such that V accepts with probability at least $2/3$.
- Soundness: If the answer is "NO," then for all protocols, V accepts with probability at most $1/3$.

where by a "protocol" we mean a sequence of messages between the verifier and multiple unentangled provers.

Amplification

The completeness and soundness bounds $2/3$ and $1/3$ 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].

$QMIP_{ne}$



QSEP-STATE

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

QSEP-STATE

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:

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

QSEP-STATE

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:

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

QSEP-STATE

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:

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

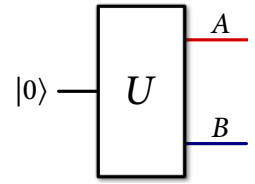
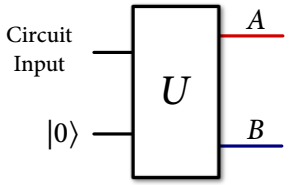
or "NO", every separable state is at least δ_s-far from ρ_{AB} in trace distance:

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

Output: Decide which one is the case.

Motivation

Taken from [MGHW13]:

QPROD-PURE-STATE	Is the state generated by the pure-state quantum circuit close to a product state?	BQP-complete	
QSEP-ISOMETRY$_{1,1\text{-LOCC}}$	Is there an input to the isometry such that the output is close to a separable state in the trace distance, or does every input lead to an output that is far from separable in 1-LOCC distance?	QMA-complete	
QPROD-ISOMETRY QSEP-ISOMETRY	Is there an input to the isometry such that the output is close to a product/separable state?	QMA(2)-complete	

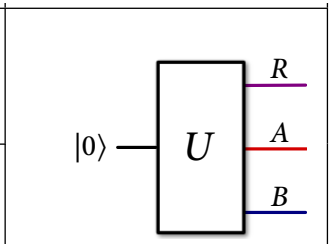
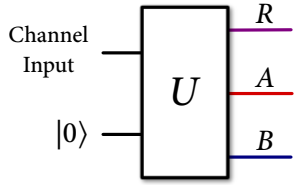
QPROD-STATE	Is the state generated by the mixed-state circuit close to a product state?	QSZK-complete	
QSEP-STATE$_{1,1\text{-LOCC}}$	Is the state generated by the mixed-state circuit close to a separable state?	In QIP(2), QSZK-hard, NP-hard	
QSEP-CHANNEL$_{1,1\text{-LOCC}}$	Is there an input to the channel such that the output is close to a separable state in trace distance or does every input lead to an output that is far from separable in 1-LOCC distance?	QIP-complete	

Figure 1: The collected results of entanglement detection problems and their complexity. The left-most column gives the name of the promise problem. Problem names subscripted with "1, 1-LOCC" indicate that the distance measure for yes-instances is the trace distance while the distance measure for no-instances is the one-way LOCC distance. The second column gives a question to which the problem corresponds. The third column states our complexity-theoretic characterization of the problem. The final column depicts a quantum circuit corresponding to the promise problems.

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:

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 $\frac{1}{\sqrt{2}}(|0\rangle|\varphi\rangle|\psi\rangle + |1\rangle|\psi\rangle|\varphi\rangle)$.

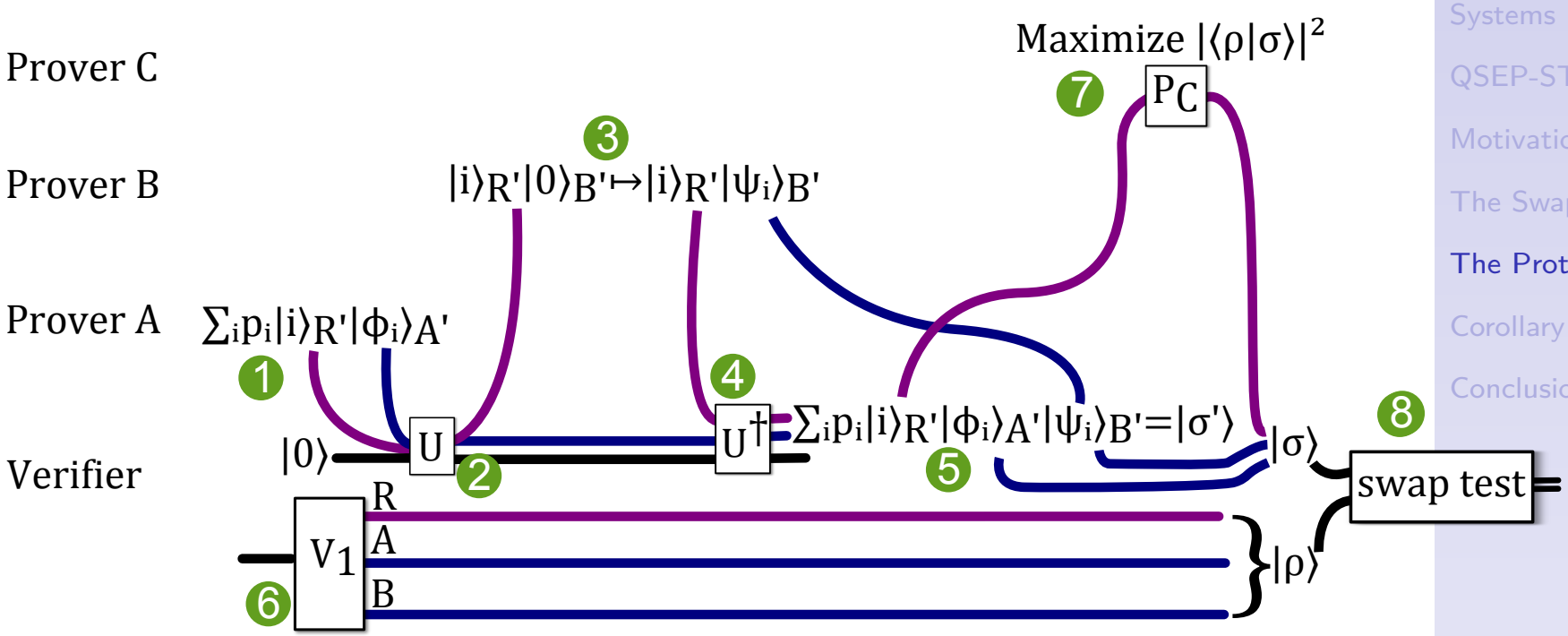
The Swap Test

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.

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 $\frac{1}{2}\left(1 + |\langle\psi|\varphi\rangle|^2\right)$. For example, see [MGHW13].

The Protocol

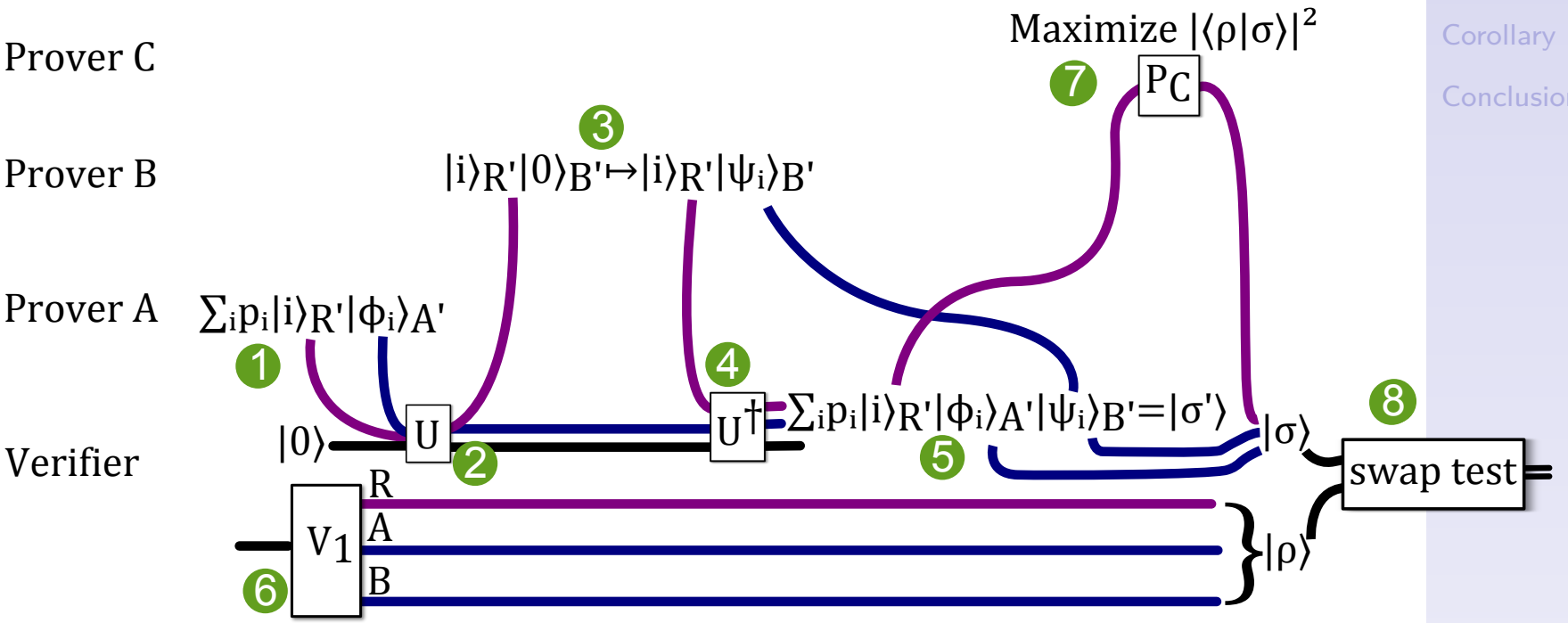


The Steps

1. Prover A constructs half of a separable state:

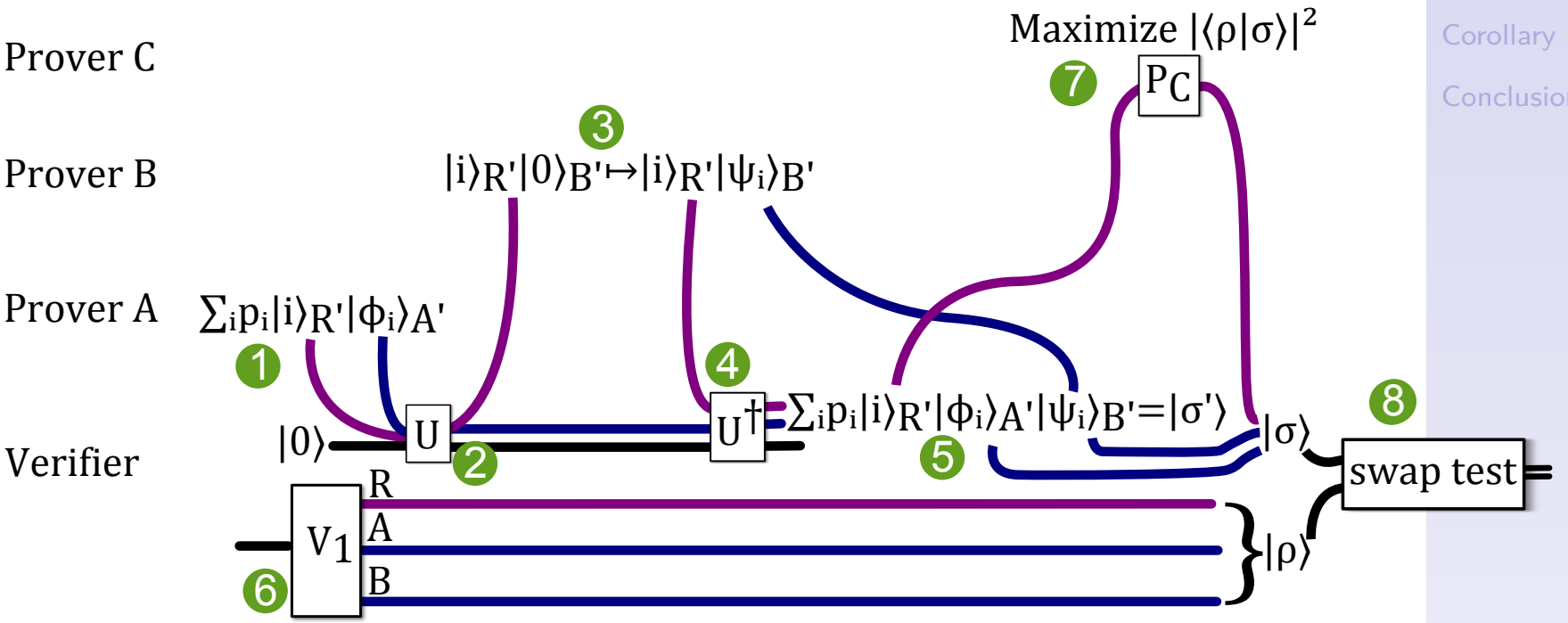
$$\sum_i p_i |i\rangle_{R'} |\varphi_i\rangle_{A'}$$

and sends it to the verifier.



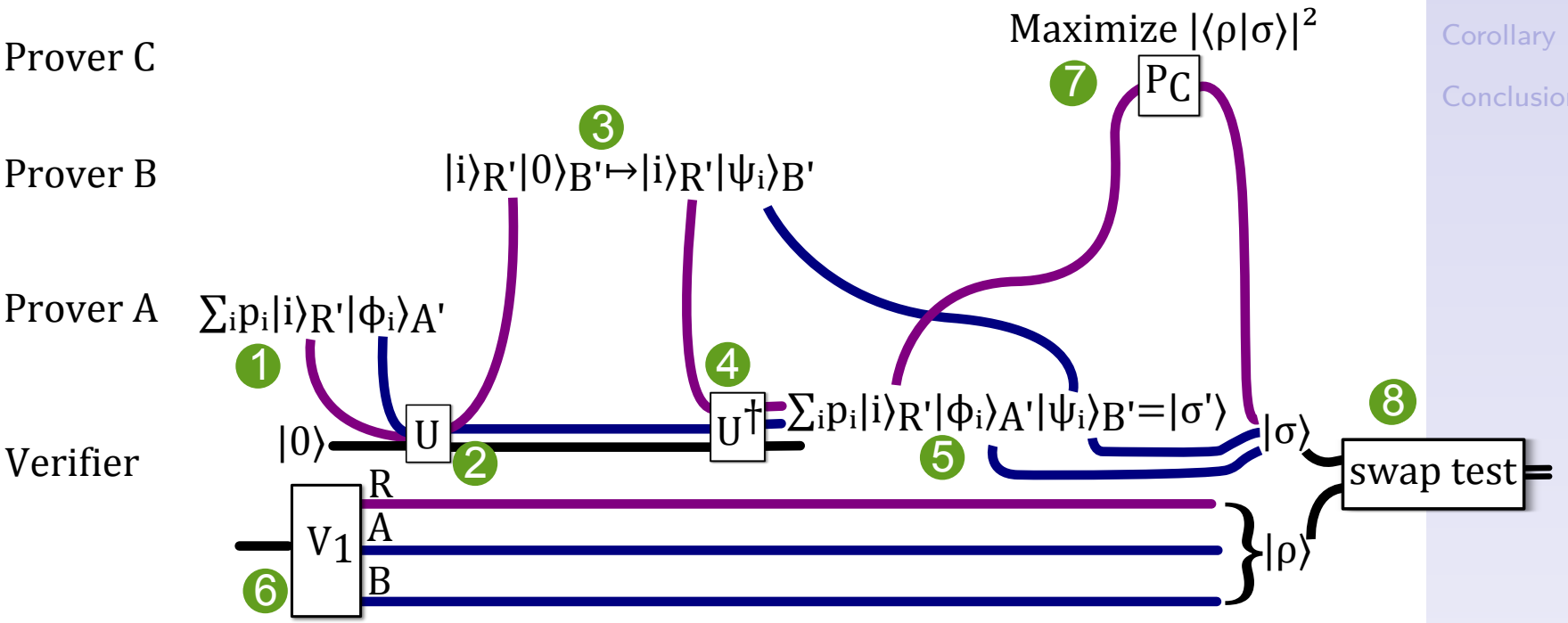
The Steps

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



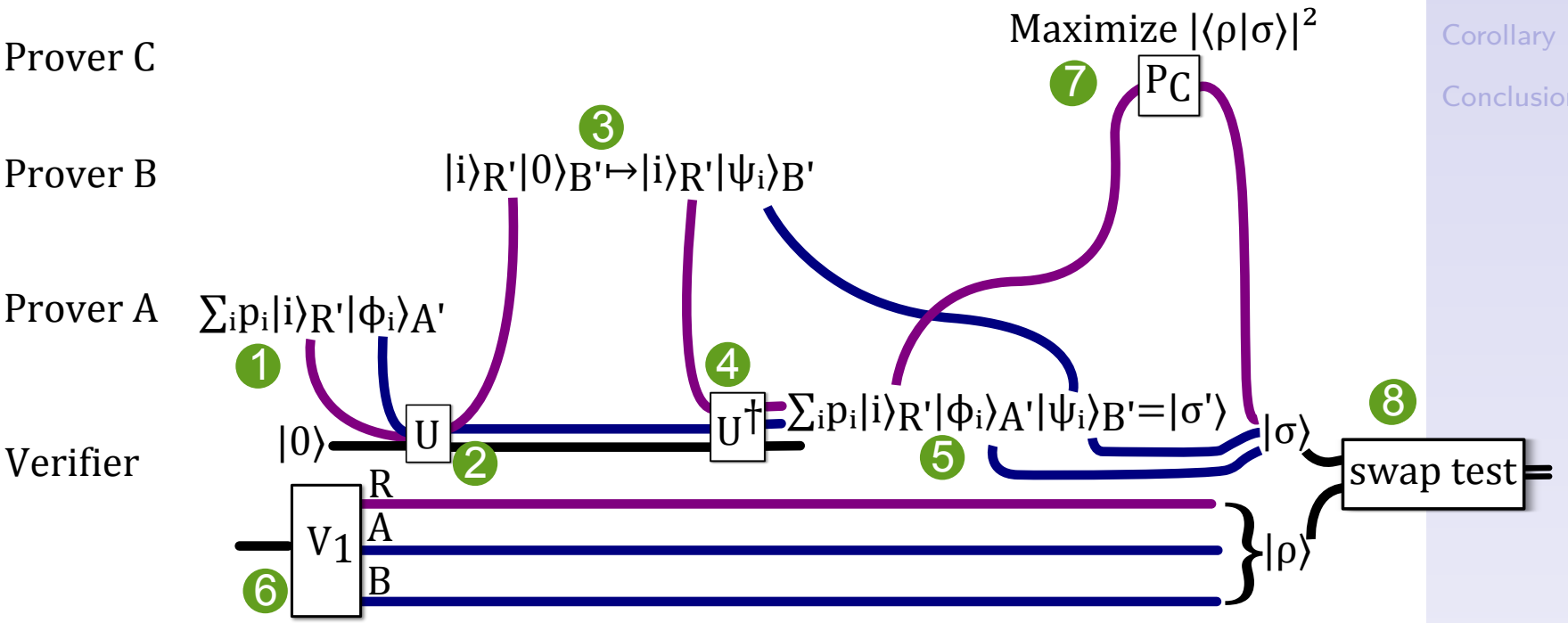
The Steps

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



The Steps

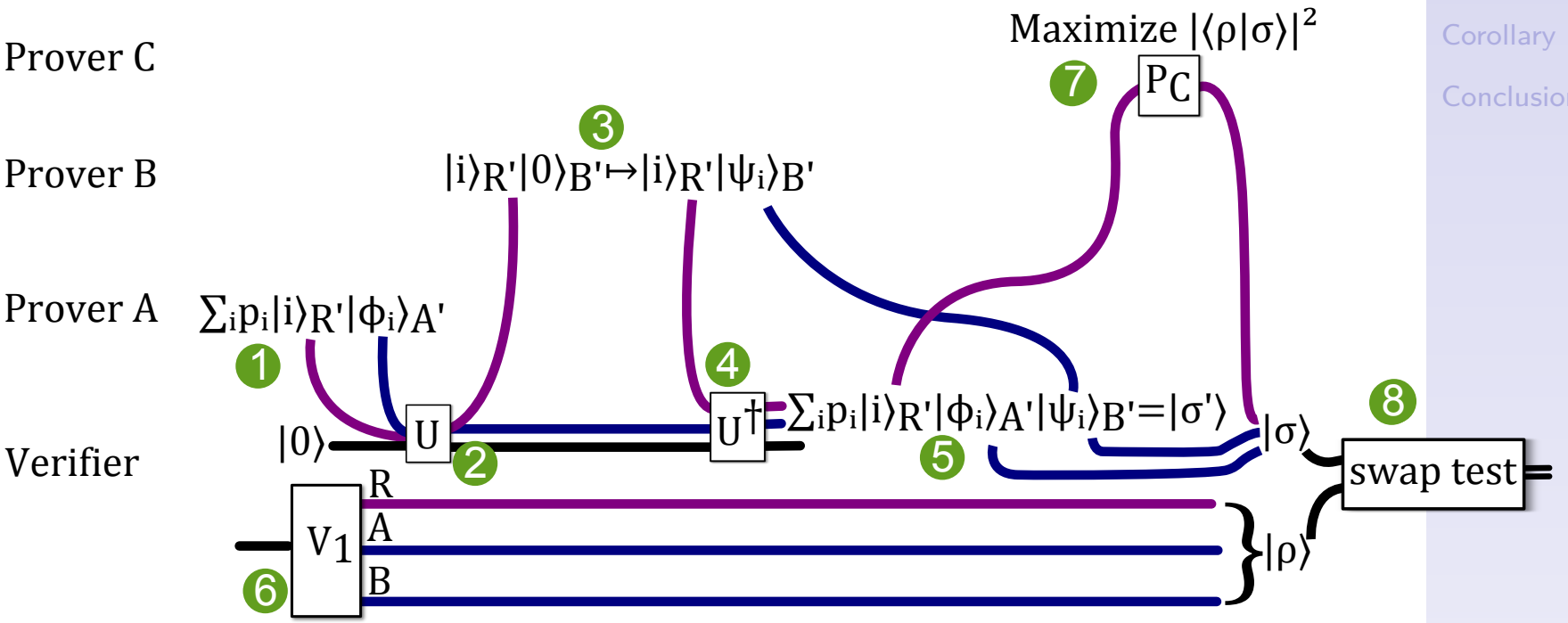
4. The verifier performs $U^\dagger$ on his private qubits and the R' system to add the phases back



The Steps

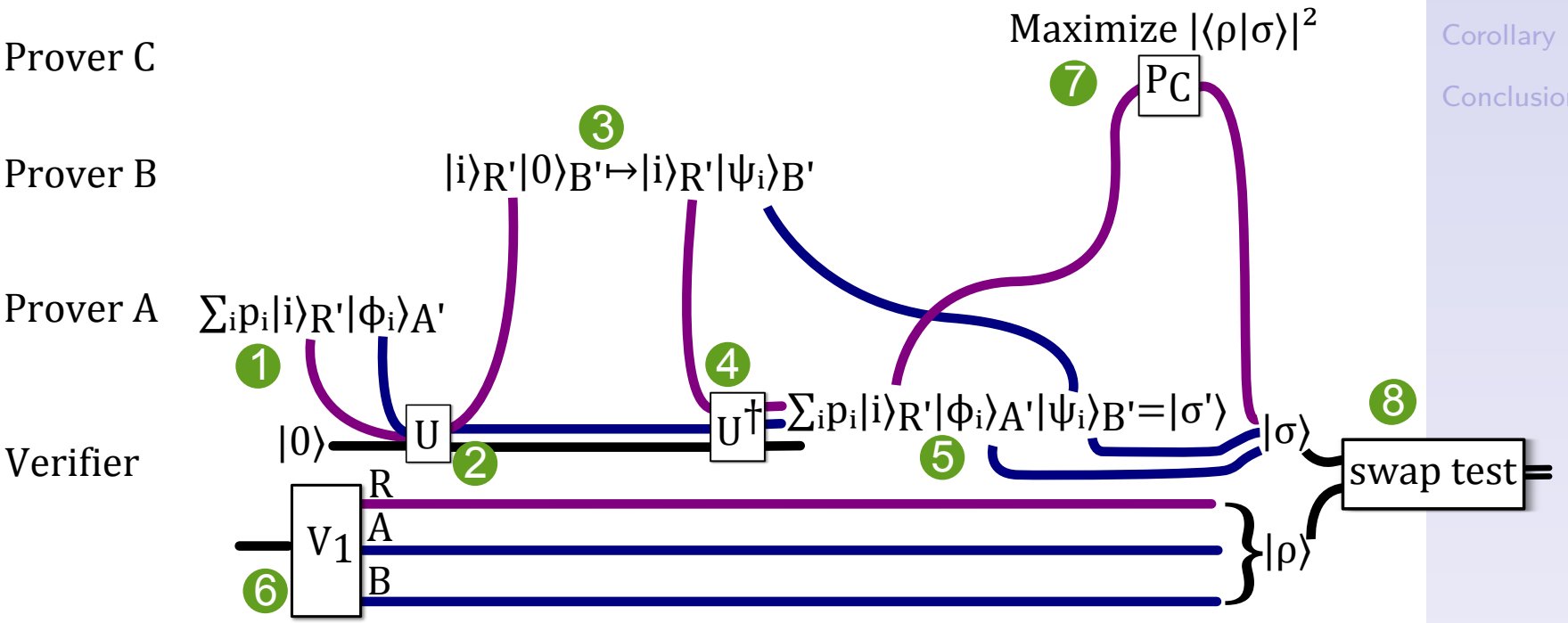
5. The verifier now has the state

$$|\sigma'\rangle = \sum_i \sqrt{p_i}|i\rangle_{R'}|\varphi_i\rangle_{A'}|\psi_i\rangle_{B'}$$



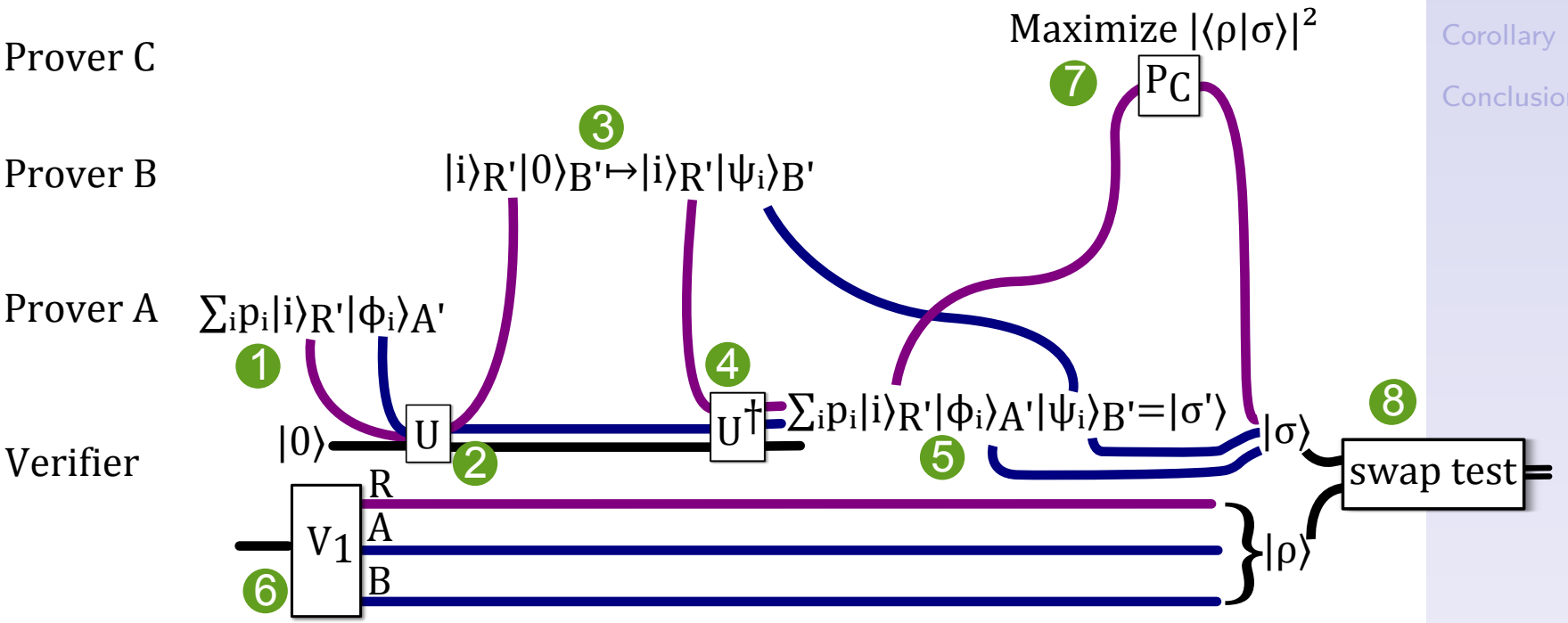
The Steps

6. The verifier uses the input circuit to construct a purification of ρ, $|\rho\rangle$.



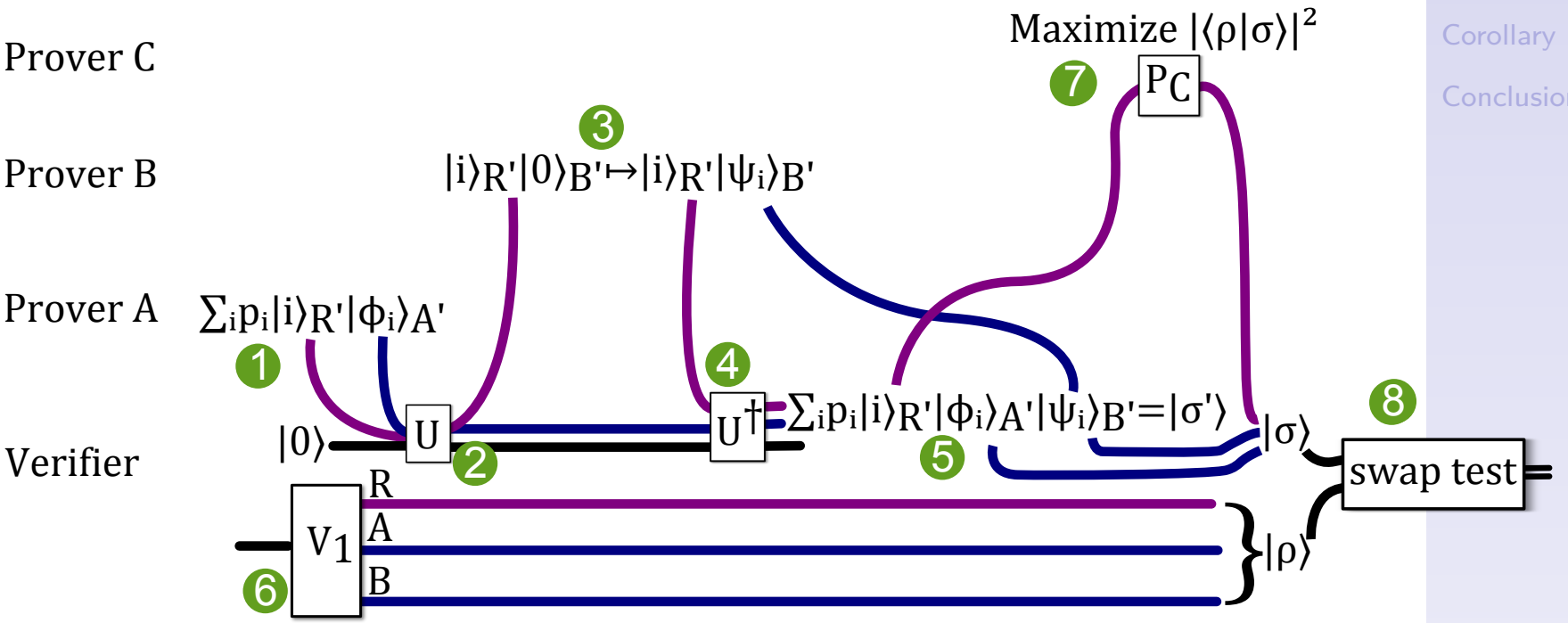
The Steps

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).



The Steps

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.



Why this protocol works

We need to show that we achieve an inverse polynomial gap between the completeness and soundness bounds.
We know the probability of the swap test passing is

$$\frac{1}{2}(1 + |\langle\rho|\sigma\rangle|^2)$$

because Prover C maximized this inner product squared, by Uhlmann's theorem, $|\langle\rho|\sigma\rangle|^2 = F(\rho, \sigma)$, the fidelity between the states. We can then use Fuchs and van de Graaf inqualities to relate the fidelity to the trace distance, and use the promise of our problem to show the difference between the probability of accepting and rejecting is at least $\frac{1}{8}\delta_s^2 - \frac{1}{2}\delta_c$.

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.

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 $\mathsf{QMIP}_{\mathsf{ne}}$ by simply having another prover send the ideal input state to the verifier and then running the protocol featured here.

Christopher Bahr , Eric Hanson , Prof. Patrick Hayden

Conclusion

- QSEP-STATE is a natural problem to consider in the context of Kevin Milner's classification of quantum complexity classes in terms of seperability problems

Conclusion

- QSEP-STATE is a natural problem to consider in the context of Kevin Milner's classification of quantum complexity classes in terms of seperability problems
- Further work could include a lower bound for the problem, or possibly a tighter upper bound

References


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


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


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

Acknowledgements

We would like to thank Kevin Milner for his help and suggestions.