Complete Problem for Perfect Zero-Knowledge Quantum Interactive Proof

Jun Yan
junyan@ios.ac.cn

State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences
Outline

I. Backgrounds
II. Our complete problem
III. Completeness proof
IV. Conclusion
V. Future works
I. Backgrounds(1)

- (Classical) interactive proof system was introduced in 1980’s [GMW89, BM88].
  Two players: prover (unbounded) and verifier (polynomial-time Turing machine), where prover tries to convince verifier to accept some common input by exchanging messages.

- It leads to many interesting and important results in complexity and cryptography:
  IP=PSpace, PCP theorem, zero-knowledge proof/argument, algebrizing barrier…

What verifier learns from the interaction is trivial (polynomial-time computable)
I. Backgrounds(2)

- Quantum interactive proof system was introduced around 2000 [Wat99, KW00, Wat02]. It turns out that
  \[ \text{QIP} = \text{QIP}[3] = \text{QMAM} = \text{IP} = \text{PSPACE} \]
- We can also introduce the notion of zero knowledge for quantum interactive proof system [Wat03, Wat06].
I. Backgrounds (3)

Two generic approaches:

1. **Transformation**
   
   E.g. achieve perfect completeness while preserving statistical zero-knowledge property [Oka96, KW00, Kob08]

2. **Complete problem**
   
   E.g. problem (Q)SD is (Q)SZK-complete [SV97, Wat02]
II. Our Complete Problem(1)

Quantum state of $m$ qubits:

- Described by a trace-one diagonal matrix $\rho = \sum_i p_i x_i x_i^*$ over complex Euclidean space of dimension $2^m$, where $p_i \geq 0$ and $\{x_i\}$ is an orthonormal basis.

- **Trace distance** between two quantum states $\rho$ and $\xi$:
  \[ \delta(\rho, \xi) = \|\rho - \xi\|_1 / 2. \]
II. Our Complete Problem(2)

A representation of quantum state is by a (unitary) quantum circuit $Q$ acting on $n$ qubits initialized in state $|0^n\rangle$, among which $m$ qubits are designated as output; the left are considered as non-output (garbage).
II. Our Complete Problem (3)

Problem **QSI** (Quantum State Identicalness):

- **Input:** a pair of quantum circuits \((Q_0, Q_1)\) encoding two quantum states \((\rho^{Q_0}, \rho^{Q_1})\).
- **Promise:** \(\delta(\rho^{Q_0}, \rho^{Q_1})\) is either \(= 0\) or \(\geq 2/3\).
- **Output:** yes for the former case and no for the latter.
II. Our Complete Problem (4)

The complete problem

QSI ([Wat02, Kob03])
Input: \((Q_0, Q_1)\)
yes: \(\delta(p^{Q_0}, p^{Q_1}) = 0\)
no: \(\delta(p^{Q_0}, p^{Q_1}) \geq 2/3\)

QSI' ([Yan12])
Input: \((Q_0, Q_1, Q_2)\)
yes: \(\delta(p^{Q_0}, p^{Q_1}) = 0\) and \(\text{Tr}(\Pi_1 p^{Q_2}) \geq 2/3\)
No: \(\delta(p^{Q_0}, p^{Q_1}) \geq 2/3\) or \(\text{Tr}(\Pi_1 p^{Q_2}) \leq 1/3\)

QPZK\(_1\) complete

QPZK-complete
III. Completeness Proof(1)

Input: a pair of quantum circuits $(Q_0, Q_1)$ satisfying promise of problem QSI: either $\delta(\rho^{Q_0}, \rho^{Q_1}) = 0$ or $\geq 2/3$.

Apply $Q_1^*$, check if it is all 0’s.
III. Completeness Proof (2)

Verifier’s view

• Quantum state of all qubits other than those at prover’s hands immediately after each message is sent. (Including message qubits and qubits at Verifier’s hands.)

• Denote by view(i) the verifier’s view immediately after the ith message is sent.
(Honest-verifier) zero-knowledge property

- There exist a polynomial-time simulator which can output a collection of quantum states \( \{\sigma_i\} \) such that \( \sigma_i \approx \text{view}(i) \).
- The “\( \approx \)” specifies the “quality” of approximation:
  - Equality: perfect zero-knowledge
  - Close in trace distance: statistical zero-
III. Completeness Proof (4)

Formulate quantum interactive proof system in terms of quantum circuits:

Fig. 1. A 4-message perfect zero-knowledge quantum interactive proof system.
III. Completeness Proof(5)

The computation (seeing from verifier) for yes instance should satisfy

- **Initial** condition: verifier’s view at the beginning is in state $|0\rangle$.
- **Propagation** condition: transition of verifier’s views (at various instants) should be legal.
- **Final** condition: verifier accepts with high
III. Completeness Proof(6)

- Verifier’s views can be approximated by simulator, if we have zero-knowledge property.
- Simplifications ([Wat02]):
  1. Initial condition can be removed.
  2. Half of propagation condition can be removed.
  3. Final condition can be removed if there is no completeness error.
Our Reduction

- $Q_0$: encodes state $\text{Tr}_M(\rho_1) \otimes \text{Tr}_M(\rho_2)$
- $Q_1$: encodes state $\text{Tr}_M(\xi_1) \otimes \text{Tr}_M(\xi_2)$
- $Q_2$: encodes state $\text{Tr}_M \otimes_O (\xi_3)$

Watrous’ construction

Malka proposed using an extra circuit to encode completeness error
Why does it work?

- **yes** instance: by perfect zero-knowledge property.
- **no** instance: by soundness property.

Devise a simulation-based strategy according to a simple fact (unitary equivalence of purifications) in quantum information.
IV. Conclusion

- Completeness error does not make much difference for QPZK.
- We get a complete problem for QPZK which accords with our intuition. (In classical case, we do not know.)
- We can prove several interesting properties of QPZK via our complete problem.
V. Future works

- Study computational zero-knowledge quantum proof (QCZK) via complete problem or similar unconditional characterization (resembling unconditional study of CZK [Vad03].)
- QZK vs Quantum Bit Commitment Scheme: are they equivalent?
- Limitation of “black-box” zero-knowledge quantum proof [GK96, Wat02, JKMR09].
The End