Quantum Zero-Knowledge Protocols

Cryptographic Protocols - Final Presentation
Matthew Prest
12/13/2024

Overview

Zero Knowledge Protocols:

- Structure
- Properties
  - Blackbox
  - Round complexity

Quantum Computing Background:

- Bit vs Qubit
  - Superposition, entanglement
- Important Results
  - Algorithms, Limitations

Complexity Classes:

- P - NP, BPP
- BQP - QMA

Focus Paper:

- Post-Quantum vs Fully Quantum
- Non-Programmable EPR Model
- Measure & Reprogram Lemma
- Counter-based ordering

Zero Knowledge (ZK) Protocols

Structure:

- Prover (P), Verifier (V), Simulator (S)
- Transcript of messages between P & V, or V and S
- Completeness, Soundness, Zero-Knowledge

Properties:

- Round complexity
  - Multiple rounds vs Constant Round (Parallel)
- Black-box
  - S interacts with V only depending on Input & Output
- Strict vs Expected Polynomial Time
- Proofs vs Arguments

Examples:

- Graph 3-Colourability
- Quadratic Residues
- Graph Isomorphism

Quantum Computing

Bit vs Qubit:

- Information is physical e.g. transistor voltage, vacuum tube current
- Classical (non-quantum) information is represented as 0s & 1s
- The physical properties of quantum systems necessitate a different representation

Quantum Bits (Qubits):

- We can use normalized complex vectors
- These can be measured (projected) in different bases with different probabilities

$$0 \rightarrow |0\rangle \rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

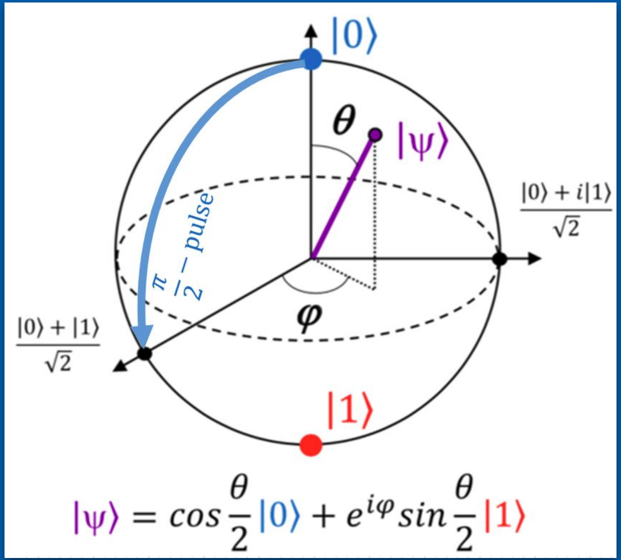
$$1 \rightarrow |1\rangle \rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\begin{aligned} |\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle\,, \\ \text{where } |\alpha|^2 + |\beta|^2 &= 1, \\ Prob(M = 0) &= |\alpha|^2, \\ Prob(M = 1) &= |\beta|^2. \end{aligned}$$

Quantum Computing

Qubits:

- We can represent these states as the north and south pole of a sphere
- Any superposition can be characterized by two angles (Bloch angles)
- States evolve in time unitarily (deterministically) based on their energy



$$|\psi(t)\rangle = U(t)\,|\psi(0)\rangle = e^{-iHt/\hbar}\,|\psi(0)\rangle$$

Quantum Computing

Entanglement:

- More than one qubit is more than the sum of its parts!
- Some states are “tensor factorable” and are reducible to the sum of their parts
- Others are not, in general an N qubit state requires 2^N values to determine!

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \otimes \begin{bmatrix}\delta\\ \gamma\end{bmatrix} = \begin{bmatrix}\alpha\delta\\ \alpha\gamma\\ \beta\delta\\ \beta\gamma\end{bmatrix}$$

$$|\Phi_{\pm}\rangle = \frac{1}{\sqrt{2}}\left[\,|00\rangle \pm |11\rangle\,\right]$$
$$|\Psi_{\pm}\rangle = \frac{1}{\sqrt{2}}\left[\,|01\rangle \pm |10\rangle\,\right]$$

$$|\psi\rangle = \alpha_0\,|0...00\rangle + \alpha_1\,|0....01\rangle + ...\alpha_{2N-1}\,|1....11\rangle$$

Quantum Computing

Important Results:

- Algorithm Speed-ups:
  - Unstructured Search $O(N) \longrightarrow O(\sqrt{N})$ (Grover 1996)
  - Prime Factorization $O(e^N) \longrightarrow O(\log(N)^3)$ (Shor 1994)
- Secure Communication
  - Quantum Key Distribution
  - Quantum coin flipping

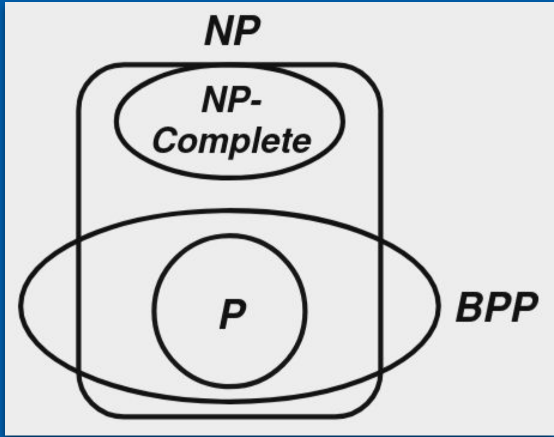
Important Limitations:

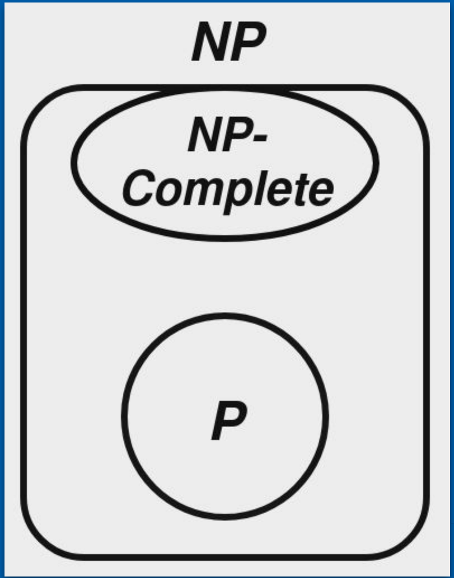
- No-Cloning Theorem
  - Cannot Copy-Paste Quantum states!
  - Cannot be broadcast
- No-Deletion Theorem
- Decoherence
  - Quantum information is easily leaked into the environment
  - Practical challenge to scaling quantum computers

Complexity Classes

Classical:

- P - NP
- Bounded Error, Probabilistic Polynomial Time:
    - L in BPP iff there exists a probabilistic Turing machine that runs in polynomial time for all inputs x in L and outputs 1 when x is in L with $p >= 2/3$
    - For y not in L, it outputs 1 with $p <= 1/3$

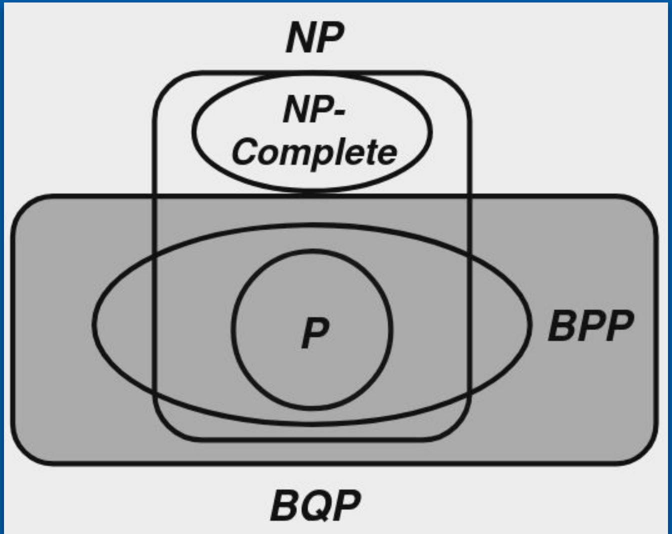


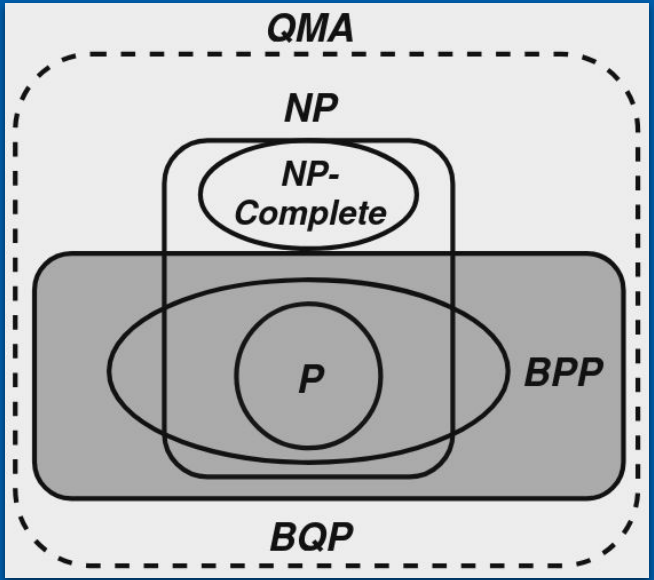


Complexity Classes

Quantum:

- BQP
  - Quantum analogue of BPP
- QMA
  - Quantum analogue of NP





Focus Paper

The Black-Box Simulation Barrier Persists in a Fully Quantum World:

- Chia et al (Sept 2024)

Post-Quantum (PQ) vs Fully Quantum (FQ):

- PQ: A malicious verifier has access to a quantum computer, prover and communication channels are classical
- FQ: All actors and channels are permitted quantum resources

Focus Paper

The Black-Box Simulation Barrier Persists in a Fully Quantum World:

- Chia et al (Sept 2024)

Key Results:

- For any language L, if there exists a constant-round FQ BBZK protocol with expected QPT simulation, then it holds that $L \in BQP$.
- There does not exist any constant-round FQ BBZK protocol for QMA unless $QMA \subseteq BQP$.

Implications:

- $QMA \subseteq BQP$ is assumed to not be true, so FQ ZK protocols must require relaxed constraints

Non-Programmable EPR Model

NPE Model:

- Trusted dealer provides a supply of maximally entangled (EPR/Bell) pairs, with Prover (or Simulator) and Verifier each receiving one half

Bell (EPR) Pairs:

- Maximally entangled 2-qubit states (perfectly correlated)
- These act as a quantum resource
- These are powerful enough that we can equivalently consider purely classical Verifiers/Provers but with this being the only quantum component
- “Any K-round FQ BBZK protocol can be converted to an equivalent protocol in the NPE model, where the prover sends only classical messages while still allowing the verifier to retain quantum capabilities”

$$|\Phi_\pm\rangle = \frac{1}{\sqrt{2}}\left[\,|00\rangle \pm |11\rangle\,\right]$$

$$|\Psi_\pm\rangle = \frac{1}{\sqrt{2}}\left[\,|01\rangle \pm |10\rangle\,\right]$$

Measure-and-Reprogram

Recall Graph 3-Colourability:

Prover

1. P Randomly shuffles known 3 colouring.
2. P commits to each vertex colour using envelopes

Verifier

3. V Challenges P to open 2 envelopes connected by an edge

Prover

4. P opens envelopes and shows they are different colours

Simulator

Measure-and-Reprogram

Recall Graph 3-Colourability:

Prover	Verifier	Simulator
		1. S guesses V's challenge and and commits to a random 3-colouring valid for that guess
	2. V Challenges S to open 2 envelopes connected by an edge →	
		3. S opens envelopes, if the colours match, abort, rewind and start again with new guess

Measure-and-Reprogram

Breakdown in the Quantum Case:

Challenge can be a superposition of multiple edges:

$$C = \sum_{(u,v)\in G} p_{u,v} \left| u, v \right\rangle$$

S could measure C but this would alter C and rewinding would not guarantee the same outcome.

Verifier	Simulator
	1. S guesses V's challenge and and commits to a random 3-colouring valid for that guess
2. V Challenges S to open 2 envelopes connected by an edge →	
	3. S opens envelopes, if the colours match, abort, rewind and start again with new guess

Measure-and-Reprogram

Solution:

- In graph 3-colourability, we think of S rewinding and guessing different envelopes.
- We can equivalently think of S rewinding and reprogramming V to make V guess differently.
- In this construction, V makes calls to a random oracle H that determines the challenge. We start with a null oracle (always returns 0).
- A random subset k of q total queries are chosen prior to be measured.
- Each measured query, reprograms H to return 1 for the measurement outcome for subsequent rounds.

Proof Overview

For a language L, assume there exists a constant-round FQ BBZK protocol. The goal is to construct a decider B for L that runs in BQP.

1. Using NPE model, assume WLOG that all messages to/from P are classical.
2. Define a malicious verifier V* as a random-aborting verifier with a local and global counter.
3. Define the desired decider B so that it executes a measure-and-reprogram technique with V*.
4. Demonstrate completeness and soundness.

Counter Structure

The malicious Verifier V* maintains two additional registers:

- A global counter register gc
  - Initialized to 0
  - Records the number of times V* has been called
- A local counter register lc
  - Initialized to 0
  - Records at which round the current execution is located
- Example:
  - At some round k, V* receives a message p_k where gc = k-1, and lc = j-1
  - First set gc = gc + 1 = k
  - if j-1 ≠k-1, V* does nothing
  - if j-1 = k-1, V* behaves as V with random aborting querying $H(p_1, \ldots, p_j)$, and if H returns 1 then set lc = lc + 1 = j
- The global counter always increases, the local counter only increases if the round is 'successful'

Rewinding Queries

Rewinding the interaction in the FQ setting with measurement is tricky:

- Rewinding without measurement simply needs the unitary inverse matrix
- After each query of S we can express the state as a superposition of ‘good’ and ‘bad’ branches
    - The ‘good’ branch will mirror the state of the honest V in a real execution at that round
    - The ‘bad’ branch consists of error terms
- When rewinding the ‘bad’ branch S can use a dummy operator that only adjusts gc and lc
- Regardless of how many rounds S rewinds, once it returns to round k the transcript will be essentially identical

Questions from Audience?

Citations:

- Chia, Nai-Hui, et al. "The Black-Box Simulation Barrier Persists in a Fully Quantum World." *arXiv preprint arXiv:2409.06317* (2024).
- Chia, Nai-Hui, et al. "On the impossibility of post-quantum black-box zero-knowledge in constant round." *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2022.
- Goldreich, Oded, Silvio Micali, and Avi Wigderson. "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems." *Journal of the ACM (JACM)* 38.3 (1991): 690-728.
- Goldwasser, Shafi, Silvio Micali, and Chales Rackoff. "The knowledge complexity of interactive proof-systems." *Providing sound foundations for cryptography: On the work of shafi goldwasser and silvio micali*. 2019. 203-225.
- Don, Jelle, et al. "Security of the Fiat-Shamir transformation in the quantum random-oracle model." *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39*. Springer International Publishing, 2019.
- Nielsen, Michael A., and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.