Quantum PCPs: on Adaptivity, Multiple Provers and Reductions to Local Hamiltonians

Gyuhyun Kim
POSTECH

QISCA Quantum Complexity Theory Study
2025. 11. 22

Introduction

What is the Quantum PCP Conjecture?

- The central open problem in quantum complexity theory.
- **Hardness of Approximation Formulation:** It is QMA-hard to distinguish between a k-Local Hamiltonian having zero ground state energy and having energy greater than a fixed constant ϵ (constant promise gap)..
- **Proof-Checking Formulation:** Any problem in QMA can be verified by a polynomial-time quantum verifier performing a **constant number of measurements (a local check)** on a **constant number of qubits** from a quantum proof.

Key Concepts & Connections

Classical PCP	Every problem in NP has a proof verifiable by checking a **constant** number of bits. The foundational result for classical hardness of approximation. NP=PCP(O(logn),O(1))
QPCP	he conjectured quantum analogue of the PCP theorem, asserting that **all QMA problems have a proof that can be locally checked**. This is equivalent to showing that the **Local Hamiltonian problem** is **QMA-hard** even with a constant promise gap.
QMA	**Quantum Merlin-Arthur.** The quantum analogue of NP (verifiable by a quantum verifier using a quantum proof). The **Local Hamiltonian problem** is QMA-complete.

Core Contribution: Framework & Reduction

This work establishes a **General Framework** (Adaptive + Multi-Prover) for QPCPs and provides a detailed, **Efficient Quantum Reduction** (Theorem 1 / Lemma 5) to the Local Hamiltonian problem.

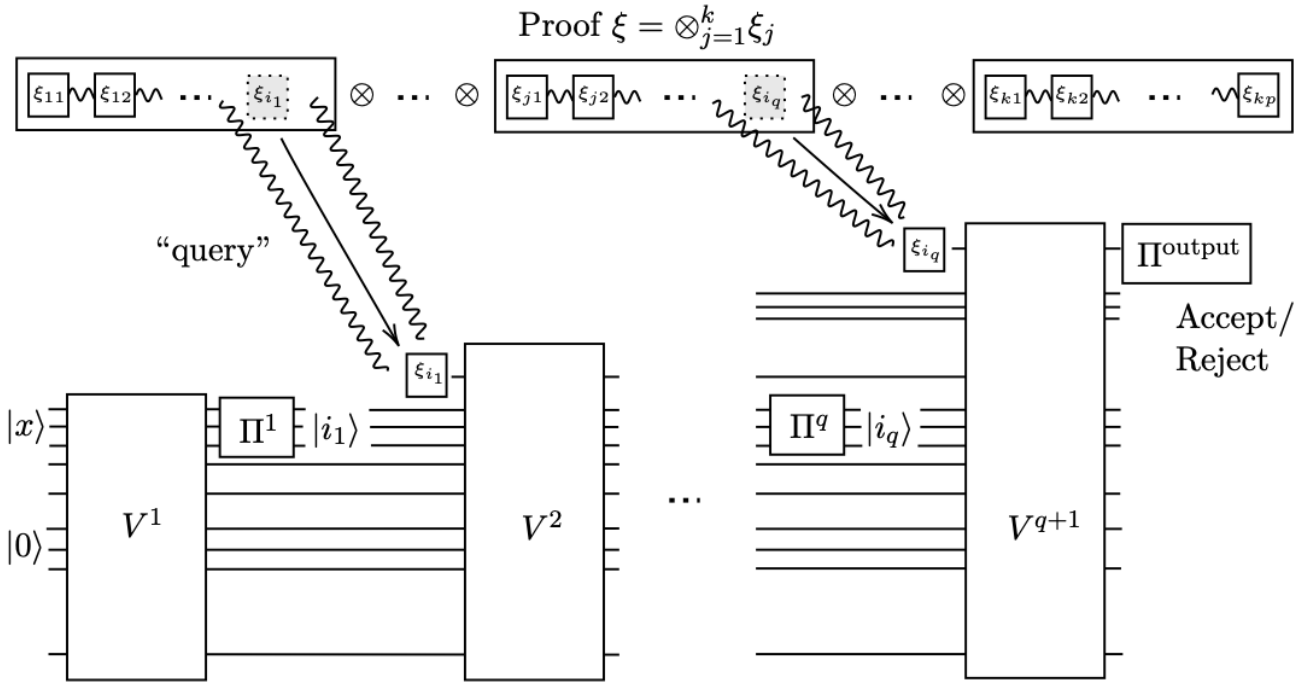
Major Results & Implications

- **Adaptivity Equivalence:** Non-adaptive Quantum PCPs can simulate adaptive Quantum PCPs with a constant number of queries. (Answers an open question from Aharonov et al.)
- **Complexity Class Connection:** Proving the existence of a Quantum PCP for QMA(k) (multi-prover QMA) implies QMA(2)=QMA, connecting two major open problems.
- **Relativization Barrier:** Proves that resolving the QPCP conjecture requires **non-relativizing techniques**, establishing a fundamental barrier similar to the one for the classical PCP theorem.

Body

Generalized QPCP Protocol

This diagram visualizes the most general verification model used: a **multi-prover** system with **adaptive queries**. The verifier performs sequential measurements where the subsequent query location depends on the previous outcome."



Quantifying Verification Failure

Lemma 3. *Let V_x be a (k, q, p_1, p_2, p_3)-QPCP verifier as in Definition 4, with hardcoded input $x \in \{0,1\}^n$. Define $M^{t'}_{i_q,x} = \Pi^{t'}_{i_q} V^{t'}_x$ for all $i_q \in [kp_2(n)]$, $t' \in [q]$. The probability that the quantum PCP rejects a proof ξ, conditioned on taking the query path $(i_1, \ldots, i_q)$, is given by*

$$\Pr[V_x \text{ rejects } \xi | (i_1, \ldots, i_q)] = \frac{\mathrm{tr}\left[P_{x,(i_1,\ldots,i_q)} \rho^0\right]}{\Pr[(i_1, \ldots, i_q)]},$$

where $\Pr[(i_1, \ldots, i_q)]$ is the probability that $i_1, \ldots, i_q$ are queried (and in this order), $\rho^0 = |0\rangle\langle 0|^{\otimes n+p_1(n)} \otimes \xi$, and $P_{x,(i_1,\ldots,i_q)}$ is a $(k+n+p_1(n))$-local operator given by

$$P_{x,(i_1,\ldots,i_q)} = M^{1\dagger}_{i_1,x} \ldots M^{q\dagger}_{i_q,x} V^{q+1\dagger}_x \Pi^{\text{output}}_0 V^{q+1}_x M^q_{i_q,x} \ldots M^1_{i_1,x}. \tag{2}$$

Quantifying Verification Failure

- Lemma 3 provides the **precise mathematical framework** for analyzing the QPCP protocol.
- **Purpose:** It formally defines the **probability that the QPCP verifier rejects a proof** under a specific sequence of adaptive queries.
- **Mechanism:** The calculation uses a complex operator (Px) derived from the product of sequential **measurement operators** and the proof's initial quantum state (ρ0).
- **Role:** This rigorous quantum mechanical formulation of the rejection process is the essential intermediate step necessary before the QPCP problem can be converted into the Local Hamiltonian problem.

Quantum Reduction Bridge

Lemma 5 (Hamiltonians from general quantum PCPs). *Let $q \in \mathbb{N}$ be some constant and let p_1, p_2, and p_3 be polynomials. Let V_x be a (k, q, p_1, p_2, p_3)-*QPCP*-verifier as in Definition 4, with hardcoded input x, $|x| = n$ for some $n \in \mathbb{N}$, and a $kp_2(n)$-qubit quantum proof $\xi = \otimes_{j=1}^{k} \xi_j$, where $\xi_j \in \mathcal{D}\left(\left(\mathbb{C}^2\right)^{\otimes p_2(n)}\right)$. Then there exists a Hamiltonian H_x consisting of q-local PSD terms acting on $kp_2(n)$-qubits such that for all ξ, we have*

$$\Pr[V_x \text{ accepts } \xi] = 1 - \operatorname{tr}[H_x \xi]. \tag{3}$$

Quantum Reduction Bridge

- Lemma 5 presents the **critical identity** that links the QPCP proof-checking concept to the energy minimization inherent in the Local Hamiltonian problem.
- This is the **mathematical bridge** proving that the problem of quantum proof verification can be reduced to the problem of calculating the expected energy of a local quantum system.
- The identity shows that the verifier's **acceptance probability** is precisely related to the expected energy of the newly constructed Local Hamiltonian Hx:
- $\Pr[V_x \text{ accepts } \xi] = 1 - \mathrm{tr}[H_x \xi]$
- This is essential for establishing the QPCP's **Hardness of Approximation** argument, as the complex verification task is now equivalent to finding the ground state energy of a physical system.

Proving the Reduction's Success

Theorem 1. *Let $q \in \mathbb{N}$ be some constant and p_1, p_2, p_3 be polynomials. Let V_x be a $[k, q, p_1, p_2, p_3]$-*QPCP*-verifier as in Definition 4, taking input x, $|x| = n$ for some $n \in \mathbb{N}$, and a kp_2-qubit quantum proof ξ. For all $\epsilon > 0$, there exists a quantum reduction from V_x to a q-local Hamiltonian $\hat{H}_x = \sum_{i \in [m]} \hat{H}_{x,i}$, with $m = \mathrm{poly}(n)$, $\hat{H}_{x,i}$ PSD for each $i \in [m]$, and $\left\|\hat{H}_x\right\| \leq 1$, such that, given a proof ξ,*

$$\left|\Pr[V_x \text{ accepts } \xi] - \left(1 - \mathrm{tr}\left[\hat{H}_x \xi\right]\right)\right| \leq \epsilon. \tag{9}$$

The quantum reduction succeeds with probability $1-\delta$ and runs in time $\mathrm{poly}(n, 1/\epsilon, \log(1/\delta))$.

Proving the Reduction’s Success

Theorem 1 confirms the main technical success: an **efficient quantum reduction** to the q-local Hamiltonian H^x. The key finding is that the transformation **preserves the constant promise gap** (ϵ).

The small error bound:

$$\Pr[V_x \text{ accepts } \xi] - (1 - \mathrm{tr}[\hat{H}^x \xi]) \leq \epsilon$$

This guarantees the accuracy needed to maintain the QMA-hard status in the approximate setting."

Conclusion

Adaptive Query No Extra Power

Theorem 3 (Adaptive versus non-adaptive)**.** *For any* $c - s = \Omega(1)$ *and* $q = \mathcal{O}(1)$*, we have that*

$$\mathsf{QPCP}_{c,s}[q] \subseteq \mathsf{QPCP}_{\mathrm{NA}}[q']$$

with

$$q' = \mathcal{O}\left(q\left(\frac{4^q}{c-s}\right)^2\right).$$

Proof. We verify the correctness of Protocol 3, which defines a (q')-$\mathsf{QPCP}_{\mathrm{NA}}$ verifier for some q', which we will show to be $\mathcal{O}(q)$. Let $A = (A_{\mathrm{YES}}, A_{\mathrm{NO}})$ be a promise problem in $\mathsf{QPCP}_{\mathrm{A}}[q]$ for an arbitrary constant q, and let $x \in \{0,1\}^n$ be an input.

Adaptive Query No Extra Power

- **Non-Adaptive Can Simulate Adaptive:** For a constant number of queries ($q=O(1)$) and a constant promise gap ($c-s=\Omega(1)$), the power of **Adaptive QPCP** ($QPCP_{c,s}[q]$) is equivalent to that of **Non-Adaptive QPCP** ($QPCPNA[q']$).
- **The Identity:**
- $QPCP_{c,s}[q] \subseteq QPCPNA[q']$
- **Minimal Overhead:** The simulation is efficient, requiring only a constant factor increase in the total number of queries (q' is proportional to q).

Adaptive Query No Extra Power

- **The Significance**
- **Failure to Boost Power:** The high flexibility of choosing the next proof location **adaptively** provides **no additional computational advantage** over simply pre-determining all query locations.
- **Robustness of the Rules:** This result establishes that the definition of QPCP is **robust** under the choice of query method.
- **Conclusion:** Like the classical PCP theorem, adaptive queries are **superfluous** for constant-query Quantum PCP.

Multi-Prover Success Implies Collapse

Theorem 5 (PCPs for QMA[2]). *If there exists a* $2 \leq k' \leq \mathrm{poly}(n)$ *and* $q = \mathcal{O}(1)$ *such that* $\mathsf{QMA}[2] \subseteq \mathsf{QPCP}[k', q]$*, then* $\mathsf{QMA}[2] = \mathsf{QMA}$.

Proof. Suppose that such a k' and q indeed exist. Let $A = (A_{\mathrm{YES}}, A_{\mathrm{NO}})$ be any problem in $\mathsf{QPCP}[k', q]$, with verifier V and input x. We have already verified in the proof of Theorem 3 that Step 2 of Protocol 6 can be made to with probability at least $1-\delta' \geq \sqrt{2/3}$, producing a fixed Hamiltonian when succeeding, and Step 3 can be made to succeed with probability at least $1 - \delta \geq \sqrt{2/3}$ by standard error reduction for QMA (the arguments holds for any $1 \leq k \leq \mathrm{poly}(n)$). Thus, we have:

- If $x \in A_{\mathrm{YES}}$, then $\Pr[\text{Protocol 6 accepts}] \geq 2/3$,
- If $x \in A_{\mathrm{NO}}$, then $\Pr[\text{Protocol 6 accepts}] \leq 1/3$,

which implies $A \in \mathsf{QMA}$, and hence $\mathsf{QPCP}[k', q] \subseteq \mathsf{QMA}$. Hence, since the assumption implies $\mathsf{QMA}[2] \subseteq \mathsf{QPCP}[k', q] \subseteq \mathsf{QMA}$ and $\mathsf{QMA} \subseteq \mathsf{QMA}[2]$ holds trivially, the result follows. □

Multi-Prover Success Implies Collapse

- **The Claim (Theorem 5)**
- **Multi-Prover Success Implies Collapse:** If **QMA[2]** (two unentangled provers) is contained within any constant-query Multi-Prover QPCP, then the class **QMA[2] must equal QMA** (the single-prover class).
- If $QMA[2] \subseteq QPCP[k',q]$, then $QMA[2] = QMA$

Multi-Prover Success Implies Collapse

- **The Dilemma's Significance**
- **Conflict with Core Belief:** This result conflicts with the widely accepted belief that QMA[2] is **strictly harder** than QMA.
- **No Easy Path:** The generalization (Multi Prover) does **not** provide a clear path to prove QPCP=QMA. Instead, its success would imply a **collapse of complexity classes** (QMA[2]=QMA).
- **Conclusion:** The pursuit of QPCP=QMA must focus on the challenging **single-prover scenario**, avoiding this generalization.

Oracle Separation: Non-Relativizing Hardness

Theorem 6. *There exists a quantum oracle U relative to which* $\mathsf{QCMA}^U \neq \mathsf{QMA}^U$ *and* $\mathsf{QPCP}[k,q]^U \neq \mathsf{QMA}^U$*, for all* $q \in \mathcal{O}(\log n)$*,* $1 \leq k \leq \mathrm{poly}(n)$*.*

Proof. This follows from using the same proof as [34], Theorem 1.1, using the lower bound of Lemma 18 to show that $\mathsf{QPCP}_{P_\epsilon^{k'}}[q]^U \neq \mathsf{QMA}^U$ for all constant $q \in \mathcal{O}(\log n)$, from which the separation $\mathsf{QPCP}[q]^U \neq \mathsf{QMA}^U$ follows by Lemma 16. □

We remark that our proof technique should work for any oracle separation between QCMA and QMA that uses counting arguments exploiting the doubly exponentially large number of quantum states and the fact that QCMA has only access to an exponential number of proofs. This shows that any proof of the quantum PCP conjecture (via the proof verification formulation) requires (as expected) quantumly non-relativising techniques.

The previous quantum oracle separations crucially exploit the doubly exponentially large number of quantum states that have low mutual fidelities. However, one may wonder whether a similar idea might be used to also show that for low-complexity states a similar separation holds? It turns out that this is surprisingly easy, by simply using a similar oracle to the one that separates BQP from NP [48]. Observe this oracle is classical, and can alternatively be viewed as a state 1-design over the set of all quantum states used in the previous separation. We state the following result, for which the proof is given in Appendix D.

Corollary 4. *There exists a classical oracle* $\mathcal{O}$ *relative to which* $\mathsf{QPCP}[k,q]^{\mathcal{O}} \neq \mathsf{QMA}^{\mathcal{O}}$ *(in fact* $\neq \mathsf{NP}^{\mathcal{O}}$*) for all* $q \in \mathcal{O}(1)$*.*

Note that a much stronger statement also holds, we can even combine QCMA and QPCP (so a classical proof and quantum proof which can be accessed locally) and the same separation would still hold.

Oracle Separation: Non-Relativizing Hardness

- **The Claim (Theorem 6)**
- **Oracle Failure:** The paper proves that there exists a **Quantum Oracle U** under which the complexity classes **QMA and QPCP are not equal** ($QMA^U \neq QPCP^U$)
- **The Problem:** This means the proof for the equality QMA=QPCP **cannot be Relativized** (it fails under the oracle test)

Oracle Separation: Non-Relativizing Hardness

- **Non-Relativizing Proof Required:** Since the proof fails the oracle test, conventional, general methods of proof (relativizing techniques) are insufficient
- **Need for New Physics:** Solving QMA=QPCP requires **non-relativizing techniques**—a new, deep theory that fundamentally relies on the unique properties of **Quantum Information** (like entanglement and state complexity)
- **Conclusion:** The conjecture is categorized as a **fundamental difficulty** in complexity theory, similar to the original classical PCP theorem.

Summary

1. Generalized QPCP Defined

Introduces multi-prover and adaptive-query extensions.

Still equivalent to the Local Hamiltonian problem.

2. Limits of These Extensions

Adaptive queries add no power (simulated by non-adaptive QPCP).

Multi-prover strengthening would collapse QMA[2] to QMA.

3. Need for Non-Relativizing Techniques

QMA = QPCP fails under a quantum oracle.

Resolving QPCP requires fundamentally new, non-relativizing methods.

Thank you!