The Acrobatics of BQP

QISCA, Quantum Complexity Theory Study Week 2

Jaehun Han
KAIST, Graduate School of Quantum Science and Technology

2025.10.19

Contents

1. Introduction
2. Raz-Tal Theorem
3. The Acrobatics of BQP
4. Conclusion

Contents

1 Introduction

2 Raz-Tal Theorem

3 The Acrobatics of BQP

4 Conclusion

What is BQP?

Definition: BQP

A language L belongs to **BQP (Bounded-Error Quantum Polynomial-Time)** if there exists a family of polynomial-size quantum circuits $\{C_n\}$ such that for every input $x \in \{0,1\}^n$:

$$x \in L \Rightarrow \Pr[C_n(x) = 1] \geq \tfrac{2}{3}, \qquad x \notin L \Rightarrow \Pr[C_n(x) = 1] \leq \tfrac{1}{3}.$$

That is, the decision can be made by a quantum computer in polynomial time with bounded error.

- **BQP** is the quantum analogue of the classical class **BPP**.
- It captures the set of problems efficiently solvable by a quantum computer.
- The error bound ($\leq 1/3$) can be reduced exponentially by repetition.

Reference: E. Bernstein and U. Vazirani, *"Quantum complexity theory"*, **SIAM Journal on Computing**, 26(5):1411–1473, 1997.

Key Open Questions about BQP

We are still trying to understand how **BQP** relates to classical complexity classes. In particular, there are three central questions that remain unresolved:

1. Is $\mathbf{BPP} = \mathbf{BQP}$?
2. Is $\mathbf{NP} \subseteq \mathbf{BQP}$?
3. Is $\mathbf{BQP} \subseteq \mathbf{NP}$ or $\mathbf{BQP} \subseteq \mathbf{PH}$?

Even after more than **30 years**, none of these questions have been conclusively answered.

Understanding where BQP fits among classical classes remains one of the fundamental goals of quantum complexity theory.

What We Know So Far about BQP

- **Relations with Classical Classes**
  - [BV97] $\mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{P}^{\#\mathbf{P}}$
  - [ADH97] $\mathbf{BQP} \subseteq \mathbf{PP}$

As a result:

$$P \subseteq BPP \subseteq BQP \subseteq PP \subseteq P^{\#P} \subseteq PSPACE \subseteq EXP$$

- **Oracle Results**
  - [FR98] $\mathbf{PP}^{\mathbf{BQP}} = \mathbf{PP}$
  - [BBBV97] $\mathbf{BQP}^{\mathbf{BQP}} = \mathbf{BQP}$ (self-low property)

The Contrast with BPP: Open Questions about BQP

- Researchers have long debated how **BQP** relates to classical complexity classes such as **NP**, **PH**, and **P/poly**.

- Seven key open questions remain unresolved:
  1. Is $\mathbf{NP}^{\mathbf{BQP}} \subseteq \mathbf{BQP}^{\mathbf{NP}}$?
  2. Is $\mathbf{BQP}^{\mathbf{NP}} \subseteq \mathbf{PH}^{\mathbf{BQP}}$?
  3. If $\mathbf{NP} \subseteq \mathbf{BQP}$, does it follow that $\mathbf{PH} \subseteq \mathbf{BQP}$?
  4. If $\mathbf{NP} \subseteq \mathbf{BQP}$, does **PH** collapse?
  5. Is $\mathbf{BQP} \subseteq \mathbf{P/poly}$?
  6. If $\mathbf{P} = \mathbf{NP}$, is **BQP** "small" (e.g., not **EXP**)?
  7. If $\mathbf{P} = \mathbf{NP}$, does $\mathbf{BQP} = \mathbf{QCMA}$?

- Even after decades of research, **none of these questions are conclusively settled.**

In Contrast: The BPP Case Is Well Understood

- Unlike the quantum case, for **BPP** all analogous questions have clear answers:

  1. $\mathbf{NP}^{\mathbf{BPP}} \subseteq \mathbf{AM} \subseteq \mathbf{BPP}^{\mathbf{NP}}$
  2. $\mathbf{BPP}^{\mathbf{NP}} \subseteq \mathbf{PH} = \mathbf{PH}^{\mathbf{BPP}}$
  3. If $\mathbf{NP} \subseteq \mathbf{BPP}$, then $\mathbf{PH} = \mathbf{BPP}$
  4. If $\mathbf{NP} \subseteq \mathbf{BPP}$, then $\mathbf{PH} = \mathbf{\Sigma_2^P}$ (Sipser–Lautemann)
  5. $\mathbf{BPP} \subset \mathbf{P/poly}$ (Adleman's Theorem)
  6. If $\mathbf{P} = \mathbf{NP}$, then $\mathbf{BPP} \neq \mathbf{EXP}$ (by the time hierarchy theorem)
  7. If $\mathbf{P} = \mathbf{NP}$, then $\mathbf{BPP} = \mathbf{MA}$

- These results illustrate how **BPP** fits neatly within the classical hierarchy — unlike **BQP**, whose relationships remain unsettled.

Randomness vs. Quantumness

- The key difference between **BPP** and **BQP** lies in the source of randomness:
  - **BPP:** classical probabilistic randomness.
  - **BQP:** quantum superposition and interference.
- This distinction underlies the theory of **sampling-based quantum supremacy**.
  - Google Sycamore [AAB+19], USTC [ZWD+20]
  - Aaronson–Arkhipov (BosonSampling, 2011)
  - Bremner–Jozsa–Shepherd (IQP model, 2010)
- Quantum distributions are #**P-hard to approximate** classically.
- If a classical algorithm could efficiently sample from the same distribution, the **Polynomial Hierarchy (PH)** would collapse (by Toda's theorem).

BQP vs. the Classical Hierarchy

- So, BQP behaves fundamentally differently from classical classes.
- Yet, several core questions remain open:
  - Is $\mathbf{NP} \subseteq \mathbf{BQP}$?
  - Is $\mathbf{BQP} \subseteq \mathbf{NP}$?
  - Is $\mathbf{BQP} \subseteq \mathbf{PH}$?
- None of these are known. What we do know: if $\mathbf{NP} \subseteq \mathbf{BQP}$ and $\mathbf{PH}$ is infinite, then at least one of the following must hold:

$$\mathbf{NP} \not\subseteq \mathbf{BQP} \quad \text{or} \quad \mathbf{BQP} \not\subseteq \mathbf{AM}.$$

- Thus, the **quantum world does not fit neatly** inside the classical hierarchy.

Relativization: Classical Perspective

- Since **Baker–Gill–Solovay (1975)** [BGS75], relativization has been a key technique in complexity theory.
  - When direct proofs (e.g., **P** vs. **NP**) are difficult, researchers consider a **relativized world**—attaching an **oracle** to all machines.
  - This allows the study of structural properties of complexity classes, even without resolving the full separation.
- Analogy: like *perturbation theory in physics*—we may not know the exact solution, but can analyze behavior under controlled variations.
- However, relativization is **not a complete proof technique**.
  - Some results are **non-relativizing**, such as **IP** = **PSPACE** [Shamir, 1992] and **MIP** = **NEXP** [BFL, 1991].

Relativization in Quantum Complexity

- In the quantum setting, even **oracle queries can be made in superposition**.
  - This makes quantum relativization far richer and more subtle than its classical counterpart.

- Relativization in quantum complexity is not only formal—it helps us observe how "**free**" quantum computation is within classical hierarchies.

- Early oracle results about **BQP**:
  - [BV97] $\mathbf{BPP} \subsetneq \mathbf{BQP} \subsetneq \mathbf{BPP}^{\#\mathbf{P}}$ — formalized through Simon's (1997) and Shor's (1997) algorithms. $\Rightarrow$ *Factoring* $\in$ **BQP**.
  - [BBBV97] There exists an oracle relative to which $\mathbf{NP} \not\subseteq \mathbf{BQP}$ — Grover's $\sqrt{N}$ search is black-box optimal.

- $\Rightarrow$ Quantum advantage exists, but solving **NP**-complete problems in polynomial time may still be impossible.

Contents

1 Introduction

2 Raz-Tal Theorem

3 The Acrobatics of BQP

4 Conclusion

From Fortnow & Rogers (1998)

- **Fortnow & Rogers (1998)** showed that there exists an oracle where $\mathbf{P} = \mathbf{BQP}$ while $\mathbf{PH}$ is infinite. $\Rightarrow$ Quantum power does not necessarily collapse classical hierarchies.

- Since then, key question emerged:

$$\text{Is } \mathbf{BQP} \subseteq \mathbf{PH} \text{ ?}$$

  How far apart are quantum and classical worlds under oracles?

- **Aaronson & Chen (2017)** further showed that if quantum sampling can be classically approximated, then **PH collapses**. $\Rightarrow$ To prove quantum advantage, **non-relativizing techniques are required.**

The Forrelation Problem (Aaronson, 2010)

Problem: Forrelation

Given Boolean functions $f, g : \{0,1\}^n \to \{-1,+1\}$, decide whether

1. f and g are independent random functions, or
2. g is correlated with the Fourier transform of f.

- **Quantum algorithm:** solves with a single quantum query (time $O(n)$).
- **Classical algorithm:** requires $\Omega(2^{n/2})$ queries.
- $\Rightarrow$ **Forrelation** proposed as an indicator of quantum supremacy.
- Aaronson conjectured: **Forrelation** $\notin$ **PH**.

The Raz–Tal Theorem (2018)

- **Raz & Tal (2018)** proved Aaronson's conjecture:

$$\mathbf{BQP} \not\subseteq \mathbf{PH} \quad \text{(relative to an oracle).}$$

- **Technique:**
  - Strengthened $\mathbf{AC}^0$ **lower bound** techniques.
  - Analyzed low-order Fourier coefficients of the Forrelation function.
  - Introduced a probabilistic view via **Brownian motion**.

- **Main Theorem (Raz–Tal):** Any **PH** machine distinguishes random (f, g) from forrelated pairs only with bias $2^{-\Omega(n)}$.

  $\Rightarrow$ PH cannot distinguish them at all; the first oracle separation $\mathbf{BQP} \not\subseteq \mathbf{PH}$.

Contents

1 Introduction

2 Raz-Tal Theorem

3 The Acrobatics of BQP

4 Conclusion

Overview of Main Results

The following results extend the Raz–Tal framework, exploring how BQP behaves under various relativized worlds.

No.	**Result**	**Implication**
Thm 3	$\exists$ oracle: $NP^{BQP} \not\subseteq BQP^{PH}$, $NP^{BQP} \not\subseteq BQP^{NP}$	Quantum–classical nondeterminism non-interchangeable.
Thm 4	$\exists$ oracle: $P = NP$, but $BQP \neq QCMA$	Even if $P = NP$, BQP remains distinct.
Conj 5	$\exists$ oracle: $NP \subseteq BQP$, but $PH \not\subseteq BQP$	BQP cannot swallow PH.
Thm 6	$\exists$ oracle: $BQP^{NP} \not\subseteq PH^{BQP}$	Asymmetry between PH and BQP.
Thm 7	(random oracle) $PP = PostBQP \not\subseteq QMA^{hier}$	QMA hierarchy cannot express PostBQP.
Thm 8	(random oracle) $\Sigma_{k+1}^{P} \not\subseteq BQP^{\Sigma_k^P}$	PH levels remain distinct.
Thm 9	$\exists$ oracle: $BQP = P^{\#P}$, PH infinite	Quantum power classical collapse.
Thm 10	$\exists$ oracle: $P = NP \neq BQP = P^{\#P}$	BQP can still be much stronger.

Together, these theorems reveal how BQP diverges fundamentally from classical hierarchies.

Theorem 3 — Fortnow Problem

Theorem 3

$\exists$ oracle such that $NP^{BQP} \not\subseteq BQP^{PH}, \quad NP^{BQP} \not\subseteq BQP^{NP}$.

- **Background:** Fortnow (2005) raised the question whether $NP^{BQP} \subseteq BQP^{NP}$ or not.
- **Main Result:** The paper shows a negative answer — quantum and classical nondeterminism are non-interchangeable.
- **Intuition:** When a quantum oracle is combined with classical nondeterminism, the order of composition matters.
- **Insight:** "Quantum randomness cannot be fixed." Classical nondeterministic queries cannot control superposed quantum states.

Contrast: In the classical world, $NP^{BPP} = BPP^{NP}$*, showing how quantum composition breaks this symmetry.*

Theorem 4 — Classical Collapse, Yet Quantum Distinct

Theorem 4

$$\exists \text{ oracle such that } P = NP, \quad \text{but } BQP \neq QCMA.$$

- **Background:** In classical complexity, if $P = NP$, most major separations collapse. One might expect quantum complexity classes to collapse as well.
- **Main Result:** Even under $P = NP$, the class BQP remains *strictly distinct* from $QCMA$ (Quantum Classical Merlin–Arthur).
- **Intuition:** Classical certificates (Merlin–Arthur with classical witness) cannot simulate the full expressive power of quantum verification.
- **Insight:** This separation is *relativizing*, showing that quantum verification retains a unique structure even when deterministic and nondeterministic computation coincide.

Implication: The existence of efficient classical proofs ($P = NP$) does not eliminate the need for quantum proofs.

Conjecture 5 — BQP Cannot Swallow PH

Conjecture 5

$$\exists \text{ oracle such that } NP \subseteq BQP \quad \text{but} \quad PH \not\subseteq BQP.$$

- **Meaning:** Even if quantum algorithms can efficiently solve all NP problems, they may still fail to capture the full power of the polynomial hierarchy.
- **Intuition:** Quantum computation may efficiently solve search problems, yet higher–order alternations of quantifiers ($\exists\forall\exists\cdots$) remain beyond its reach.
- **Relation to Raz–Tal:** Extends the idea that $BQP \not\subseteq PH$ (relativized). Now the conjecture goes further—assuming $NP \subseteq BQP$, PH would still *not* collapse into the quantum world.
- **Interpretation:** Suggests a strict structural separation between quantum computation and the classical logical hierarchy.

In short: Quantum advantage does not necessarily imply domination over classical hierarchies.

Theorem 6 — Asymmetry between BQP and PH

Theorem 6

$\exists$ oracle such that $BQP^{NP} \not\subseteq PH^{BQP}$.

- **Background:** After Raz–Tal's separation ($BQP \not\subseteq PH$), a natural question arises: does the reverse inclusion $PH^{BQP} \supseteq BQP^{NP}$ hold?
- **Main Result:** No — the inclusion fails even in the opposite direction. Quantum and classical hierarchies are fundamentally asymmetric.
- **Intuition:** Quantum queries can exploit superpositions over nondeterministic paths, whereas PH^{BQP} machines can only make classical adaptive queries to quantum oracles.
- **Implication:** There is no "universal" direction of inclusion between the two; quantum and classical hierarchies are structurally incomparable.

This deepens the Raz–Tal separation: BQP and PH not only differ, but their oracle-extended versions fail to simulate one another.

Theorem 7 — Limits of the QMA Hierarchy

Theorem 7

$$\text{(Random oracle)} \quad PP = \text{PostBQP} \not\subseteq QMA^{QMA^{QMA^{\cdots}}}.$$

- **Background:** In classical complexity, we know that PostBPP $\subseteq PH$ (Stockmeyer, 1985). A natural question is whether its quantum analogue also lies within a quantum hierarchy.
- **Main Result:** Even an unbounded tower of quantum-Merlin–Arthur verifiers cannot simulate PostBQP.
- **Intuition:** Postselection boosts quantum computational power up to PP. The QMA hierarchy, however, relies on polynomial-size quantum proofs, which cannot encode postselected amplitudes.
- **Insight:** No "quantum Stockmeyer theorem" exists — the hierarchy of quantum verifiers is strictly weaker than postselection.

Implication: Quantum proofs cannot reproduce the full counting power of PP, highlighting structural limits of QMA hierarchies.

Theorem 8 — Persistence of the PH Gap

Theorem 8

$$\text{(Random oracle)} \quad \Sigma_{k+1}^P \not\subseteq BQP^{\Sigma_k^P}, \quad \forall k.$$

- **Background:** Raz–Tal (2019) proved that $BQP \not\subseteq PH$. This theorem generalizes that result to every level of the polynomial hierarchy.
- **Main Result:** Even when a quantum oracle is given access to lower levels of PH, the hierarchy does *not* collapse — each Σ_{k+1}^P remains strictly stronger than $BQP^{\Sigma_k^P}$.
- **Technique:** Extends the Raz–Tal "randomness obfuscation" argument using a *quantum projection lemma* (a quantum analogue of Håstad et al., 2017 random restriction).
- **Intuition:** Under random oracle relativization, quantum algorithms cannot exploit higher quantifier alternations. Thus PH retains its infinite depth even in a quantum context.

Implication: The polynomial hierarchy resists collapse under quantum oracles — demonstrating the enduring separation between logical quantifier depth and quantum power.

Theorem 9 — BQP $= P^{\#P}$ but PH Infinite

Theorem 9

$\exists$ oracle such that $BQP = P^{\#P}$, and PH is infinite.

- **Background:** In the classical world, if a class gains $\#P$ power, the polynomial hierarchy often collapses. This theorem shows that in the quantum world, such collapse does *not* necessarily occur.
- **Main Idea:** Extend Raz–Tal's oracle framework to encode $\#P$ computation within BQP queries, while ensuring that to PH machines, the oracle still appears pseudorandom.
- **Technique:** Construct a random oracle augmented with *Forrelation instances* that are visible to BQP but indistinguishable to PH. Each $\#P$ computation is embedded via structured quantum correlations.
- **Result:** BQP becomes as powerful as $P^{\#P}$, yet the PH remains infinite.
- **Insight:** Quantum power (counting through amplitude interference) does not imply classical hierarchy collapse.

Implication: Even when BQP reaches counting-class power, the polynomial hierarchy can still stretch infinitely—quantum $\neq$ collapse.

Theorem 10 — $P = NP$ but $BQP \neq P$

Theorem 10

$$\exists \text{ oracle such that } P = NP \neq BQP = P^{\#P}.$$

- **Background:** Classically, if $P = NP$, then nondeterminism adds no power — the entire PH collapses to P. The natural question: would quantum power also collapse in this world?
- **Result:** There exists an oracle where $P = NP$, yet BQP remains as strong as $P^{\#P}$. Hence, even when classical nondeterminism vanishes, quantum interference preserves superior power.
- **Technique:** Start from the oracle of Theorem 9 (where $BQP = P^{\#P}$, PH infinite), then augment it to collapse PH to P, keeping the Forrelation parts intact. PH sees randomness; BQP still exploits hidden quantum correlations.
- **Implication:** "Even if $P = NP$, quantum advantage persists." The collapse of classical hierarchies does not erase quantum superiority.

Conclusion: Quantum computation remains fundamentally distinct from classical computation, even in a world where nondeterminism is free.

Contents

1. Introduction
2. Raz-Tal Theorem
3. The Acrobatics of BQP
4. Conclusion

Conclusion

Summary of Main Results

- The paper extends the **Raz–Tal framework**, constructing various oracles that separate BQP from classical hierarchies (NP, PH, QMA, etc.).
- Demonstrates that:
  - Quantum and classical nondeterminism are **non-interchangeable**.
  - The **polynomial hierarchy remains infinite**, even with quantum power.
  - Even if $P = NP$, **quantum computation stays fundamentally stronger.**
- Together, these results reveal that **BQP cannot be neatly placed within classical hierarchies**.

Open Problems and Future Directions

- **Oracles where BQP = EXP**
- **Finer Control over BQP and PH**
- **Stronger Random Restriction Lemmas**
- **Collapsing QMAH to P**

Quantum complexity remains a frontier where new principles, beyond relativization, are essential.

Thanks for Listening

The Acrobatics of BQP

Jaehun Han, KAIST
pjhhan@kaist.ac.kr

Quantum Complexity Theory Study, QISCA