

Quantum Polynomial Hierarchies: Karp-Lipton, Error Reduction, and Lower Bounds

Avantika Agarwal¹ Sevag Gharibian² Venkata Koppula³ **Dorian Rudolph²**

¹David R. Cheriton School of Computer Science and Institute for Quantum Computing, University of Waterloo

²Department of Computer Science and Institute for Photonic Quantum Systems (PhoQS), Paderborn University

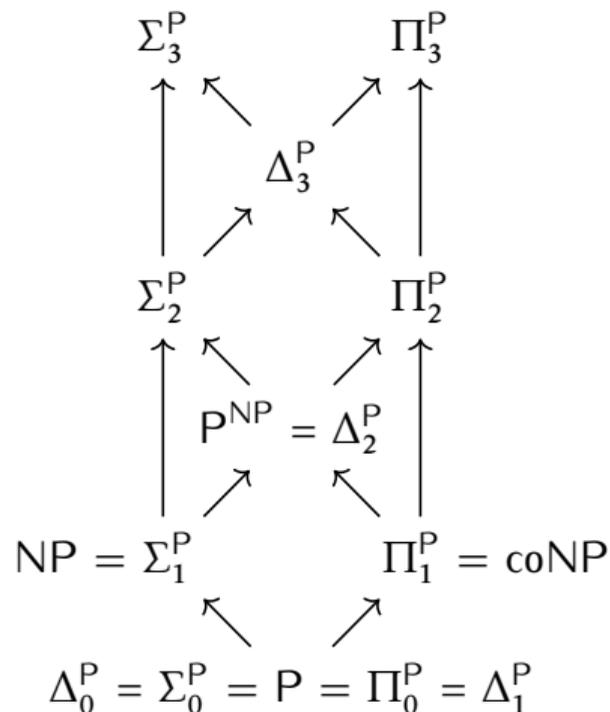
³Department of Computer Science and Engineering, Indian Institute of Technology Delhi



- 1 Introduction
- 2 Results
- 3 Quantum Karp-Lipton
- 4 Error Reduction
- 5 Lower Bounds
- 6 Conclusion

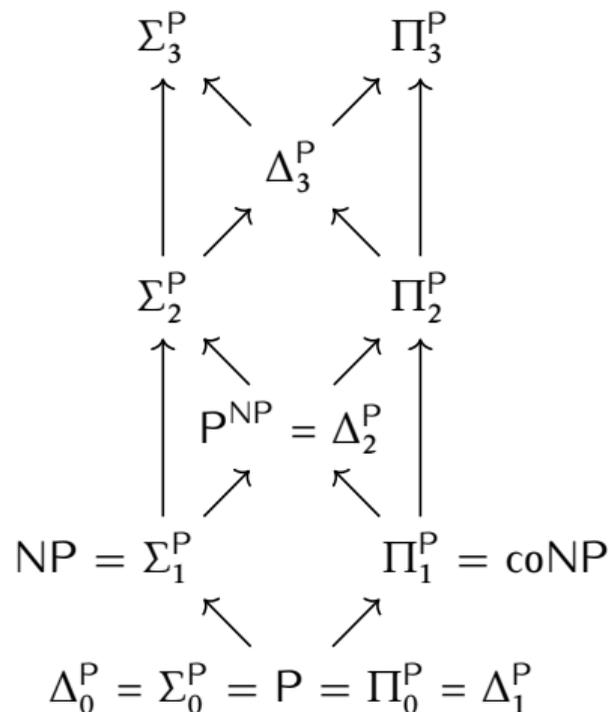
The Polynomial Hierarchy (PH)

- Introduced by Stockmeyer 1976, staple of classical complexity theory.



The Polynomial Hierarchy (PH)

- Introduced by Stockmeyer 1976, staple of classical complexity theory.
- Applications from *randomized computation* to *quantum advantage* analysis for near-term quantum computers.



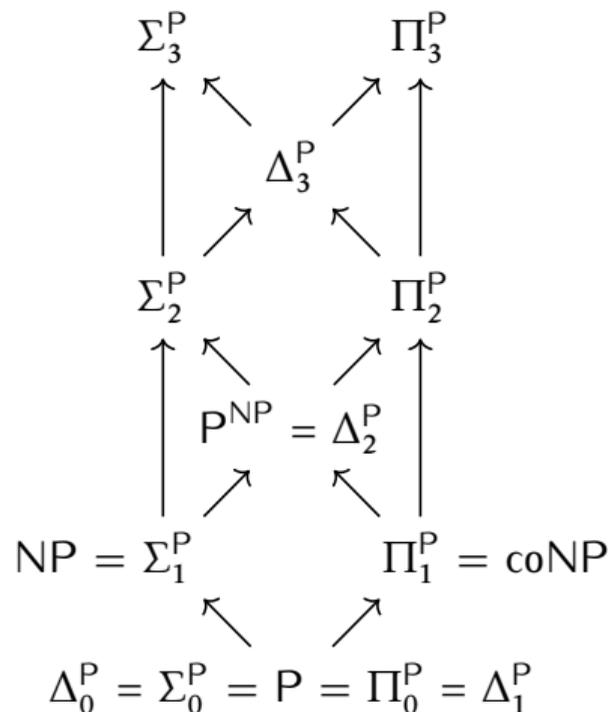
The Polynomial Hierarchy (PH)

- Introduced by Stockmeyer 1976, staple of classical complexity theory.
- Applications from *randomized computation* to *quantum advantage* analysis for near-term quantum computers.

Definition (Σ_i^P)

$L \in \Sigma_i^P$ if there exists a deterministic poly-time Turing machine M s.t.

- $x \in L \Rightarrow \exists y_1 \forall y_2 \exists y_3 \cdots Q_i y_i : M(x, y_1, \dots, y_i) = 1$
- $x \notin L \Rightarrow \forall y_1 \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : M(x, y_1, \dots, y_i) = 0$



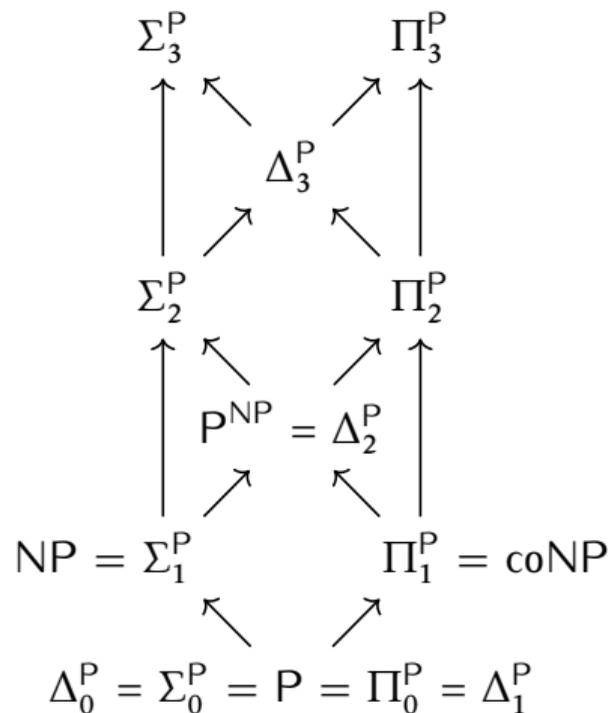
The Polynomial Hierarchy (PH)

- Introduced by Stockmeyer 1976, staple of classical complexity theory.
- Applications from *randomized computation* to *quantum advantage* analysis for near-term quantum computers.

Definition (Π_i^P)

$L \in \Sigma_i^P$ if there exists a deterministic poly-time Turing machine M s.t.

- $x \in L \Rightarrow \forall y_1 \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : M(x, y_1, \dots, y_i) = 1$
- $x \notin L \Rightarrow \exists y_1 \forall y_2 \exists y_3 \cdots Q_i y_i : M(x, y_1, \dots, y_i) = 0$
- Π_i^P : Same as Σ_i^P , but with inverted quantifiers



The *Quantum* Polynomial Hierarchy (QPH)

- Many ways to define a quantum polynomial hierarchy...

The *Quantum* Polynomial Hierarchy (QPH)

Quantum Classical PH (QCPH) [Gharibian, Santha, Sikora, Sundaram, Yirka, 2022]

Promise problem $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Sigma_i$ if there exists a *poly-time uniform* family of quantum circuits $\{V_n\}_{n \in \mathbb{N}}$ and c, s with $c - s \geq 1/\text{poly}(n)$ s.t.

- *Completeness*: $x \in L_{\text{yes}} \Rightarrow \exists y_1 \forall y_2 \cdots Q_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \geq c$
- *Soundness*: $x \in L_{\text{no}} \Rightarrow \forall y_1 \exists y_2 \cdots \overline{Q}_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \leq s$

The *Quantum* Polynomial Hierarchy (QPH)

Quantum Classical PH (QCPH) [Gharibian, Santha, Sikora, Sundaram, Yirka, 2022]

Promise problem $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Sigma_i$ if there exists a *poly-time uniform* family of quantum circuits $\{V_n\}_{n \in \mathbb{N}}$ and c, s with $c - s \geq 1/\text{poly}(n)$ s.t.

- *Completeness*: $x \in L_{\text{yes}} \Rightarrow \exists y_1 \forall y_2 \cdots Q_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \geq c$
- *Soundness*: $x \in L_{\text{no}} \Rightarrow \forall y_1 \exists y_2 \cdots \overline{Q}_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \leq s$
- QPH [GSSSY22]: proofs are mixed states
 $x \in L_{\text{yes}} \Rightarrow \exists \rho_1 \forall \rho_2 \cdots Q_i \rho_i: \Pr[V_n \text{ accepts } |x\rangle\langle x| \otimes \rho_1 \otimes \cdots \otimes \rho_i] \geq c.$

The Quantum Polynomial Hierarchy (QPH)

Quantum Classical PH (QCPH) [Gharibian, Santha, Sikora, Sundaram, Yirka, 2022]

Promise problem $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Sigma_i$ if there exists a *poly-time uniform* family of quantum circuits $\{V_n\}_{n \in \mathbb{N}}$ and c, s with $c - s \geq 1/\text{poly}(n)$ s.t.

- *Completeness*: $x \in L_{\text{yes}} \Rightarrow \exists y_1 \forall y_2 \cdots Q_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \geq c$
- *Soundness*: $x \in L_{\text{no}} \Rightarrow \forall y_1 \exists y_2 \cdots \overline{Q}_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \leq s$
- QPH [GSSSY22]: proofs are mixed states
 $x \in L_{\text{yes}} \Rightarrow \exists \rho_1 \forall \rho_2 \cdots Q_i \rho_i: \Pr[V_n \text{ accepts } |x\rangle\langle x| \otimes \rho_1 \otimes \cdots \otimes \rho_i] \geq c.$
- pureQPH (**this work**): proofs are pure states
 $x \in L_{\text{yes}} \Rightarrow \exists |\psi_1\rangle \forall |\psi_2\rangle \cdots Q_i |\psi_i\rangle: \Pr[V_n \text{ accepts } |x\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_i\rangle] \geq c.$

The Quantum Polynomial Hierarchy (QPH)

Quantum Classical PH (QCPH) [Gharibian, Santha, Sikora, Sundaram, Yirka, 2022]

Promise problem $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Sigma_i$ if there exists a *poly-time uniform* family of quantum circuits $\{V_n\}_{n \in \mathbb{N}}$ and c, s with $c - s \geq 1/\text{poly}(n)$ s.t.

- *Completeness*: $x \in L_{\text{yes}} \Rightarrow \exists y_1 \forall y_2 \cdots Q_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \geq c$
- *Soundness*: $x \in L_{\text{no}} \Rightarrow \forall y_1 \exists y_2 \cdots \overline{Q}_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \leq s$

- QPH [GSSSY22]: proofs are mixed states

$$x \in L_{\text{yes}} \Rightarrow \exists \rho_1 \forall \rho_2 \cdots Q_i \rho_i: \Pr[V_n \text{ accepts } |x\rangle\langle x| \otimes \rho_1 \otimes \cdots \otimes \rho_i] \geq c.$$

- pureQPH (**this work**): proofs are pure states

$$x \in L_{\text{yes}} \Rightarrow \exists |\psi_1\rangle \forall |\psi_2\rangle \cdots Q_i |\psi_i\rangle: \Pr[V_n \text{ accepts } |x\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_i\rangle] \geq c.$$

- QCMA $\equiv \text{QC}\Sigma_1$, coQMA $\equiv \text{Q}\Pi_1 = \text{pureQ}\Pi_1$

The Quantum Polynomial Hierarchy (QPH)

Quantum Classical PH (QCPH) [Gharibian, Santha, Sikora, Sundaram, Yirka, 2022]

Promise problem $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Sigma_i$ if there exists a *poly-time uniform* family of quantum circuits $\{V_n\}_{n \in \mathbb{N}}$ and c, s with $c - s \geq 1/\text{poly}(n)$ s.t.

- *Completeness*: $x \in L_{\text{yes}} \Rightarrow \exists y_1 \forall y_2 \cdots Q_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \geq c$
- *Soundness*: $x \in L_{\text{no}} \Rightarrow \forall y_1 \exists y_2 \cdots \overline{Q}_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \leq s$

- QPH [GSSSY22]: proofs are mixed states

$$x \in L_{\text{yes}} \Rightarrow \exists \rho_1 \forall \rho_2 \cdots Q_i \rho_i: \Pr[V_n \text{ accepts } |x\rangle\langle x| \otimes \rho_1 \otimes \cdots \otimes \rho_i] \geq c.$$

- pureQPH (**this work**): proofs are pure states

$$x \in L_{\text{yes}} \Rightarrow \exists |\psi_1\rangle \forall |\psi_2\rangle \cdots Q_i |\psi_i\rangle: \Pr[V_n \text{ accepts } |x\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_i\rangle] \geq c.$$

- QCMA $\equiv \text{QC}\Sigma_1$, coQMA $\equiv \text{Q}\Pi_1 = \text{pureQ}\Pi_1$

- $\text{Q}\Pi_2 = \text{Q}\Sigma_2 \equiv \text{QRG}(1) \subseteq \text{PSPACE}$ [GSSSY22] [Jain, Watrous, 2009]

The Quantum Polynomial Hierarchy (QPH)

Quantum Classical PH (QCPH) [Gharibian, Santha, Sikora, Sundaram, Yirka, 2022]

Promise problem $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Sigma_i$ if there exists a *poly-time uniform* family of quantum circuits $\{V_n\}_{n \in \mathbb{N}}$ and c, s with $c - s \geq 1/\text{poly}(n)$ s.t.

- *Completeness*: $x \in L_{\text{yes}} \Rightarrow \exists y_1 \forall y_2 \cdots Q_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \geq c$
- *Soundness*: $x \in L_{\text{no}} \Rightarrow \forall y_1 \exists y_2 \cdots \overline{Q}_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \leq s$

- QPH [GSSSY22]: proofs are mixed states

$$x \in L_{\text{yes}} \Rightarrow \exists \rho_1 \forall \rho_2 \cdots Q_i \rho_i: \Pr[V_n \text{ accepts } |x\rangle\langle x| \otimes \rho_1 \otimes \cdots \otimes \rho_i] \geq c.$$

- pureQPH (**this work**): proofs are pure states

$$x \in L_{\text{yes}} \Rightarrow \exists |\psi_1\rangle \forall |\psi_2\rangle \cdots Q_i |\psi_i\rangle: \Pr[V_n \text{ accepts } |x\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_i\rangle] \geq c.$$

- QCMA $\equiv \text{QC}\Sigma_1$, coQMA $\equiv \text{Q}\Pi_1 = \text{pureQ}\Pi_1$

- $\text{Q}\Pi_2 = \text{Q}\Sigma_2 \equiv \text{QRG}(1) \subseteq \text{PSPACE}$ [GSSSY22] [Jain, Watrous, 2009]

- Sion's minimax theorem: $\max_{\rho} \min_{\sigma} \text{Tr}(H(\rho \otimes \sigma)) = \min_{\sigma} \max_{\rho} \text{Tr}(H(\rho \otimes \sigma))$

The Quantum Polynomial Hierarchy (QPH)

Quantum Classical PH (QCPH) [Gharibian, Santha, Sikora, Sundaram, Yirka, 2022]

Promise problem $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Sigma_i$ if there exists a *poly-time uniform* family of quantum circuits $\{V_n\}_{n \in \mathbb{N}}$ and c, s with $c - s \geq 1/\text{poly}(n)$ s.t.

- *Completeness*: $x \in L_{\text{yes}} \Rightarrow \exists y_1 \forall y_2 \cdots Q_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \geq 1 - \frac{1}{\text{exp}}$
- *Soundness*: $x \in L_{\text{no}} \Rightarrow \forall y_1 \exists y_2 \cdots \overline{Q}_i y_i: \Pr[V_n \text{ accepts } (x, y_1, \dots, y_i)] \leq \frac{1}{\text{exp}}$

- QPH [GSSSY22]: proofs are mixed states

$$x \in L_{\text{yes}} \Rightarrow \exists \rho_1 \forall \rho_2 \cdots Q_i \rho_i: \Pr[V_n \text{ accepts } |x\rangle\langle x| \otimes \rho_1 \otimes \cdots \otimes \rho_i] \geq c.$$

- pureQPH (**this work**): proofs are pure states

$$x \in L_{\text{yes}} \Rightarrow \exists |\psi_1\rangle \forall |\psi_2\rangle \cdots Q_i |\psi_i\rangle: \Pr[V_n \text{ accepts } |x\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_i\rangle] \geq c.$$

- QCMA $\equiv \text{QC}\Sigma_1$, coQMA $\equiv \text{Q}\Pi_1 = \text{pureQ}\Pi_1$

- $\text{Q}\Pi_2 = \text{Q}\Sigma_2 \equiv \text{QRG}(1) \subseteq \text{PSPACE}$ [GSSSY22] [Jain, Watrous, 2009]

- Sion's minimax theorem: $\max_{\rho} \min_{\sigma} \text{Tr}(H(\rho \otimes \sigma)) = \min_{\sigma} \max_{\rho} \text{Tr}(H(\rho \otimes \sigma))$

- Error reduction possible for QCPH but not known for QPH, pureQPH.

- 1 Introduction
- 2 Results
- 3 Quantum Karp-Lipton
- 4 Error Reduction
- 5 Lower Bounds
- 6 Conclusion

Results: Quantum Karp-Lipton

- Karp-Lipton theorem: SAT cannot be solved with poly-size circuits, unless PH collapses to its second level.

Results: Quantum Karp-Lipton

- Karp-Lipton theorem: SAT cannot be solved with poly-size circuits, unless PH collapses to its second level.
 - Generally assumed that $\Sigma_{k+1} \neq \Sigma_k$ for all k .

Results: Quantum Karp-Lipton

- Karp-Lipton theorem: SAT cannot be solved with poly-size circuits, unless PH collapses to its second level.
 - Generally assumed that $\Sigma_{k+1} \neq \Sigma_k$ for all k .
 - Formally: If $\text{NP} \subseteq \text{P}_{/\text{poly}}$, then $\Pi_2 = \Sigma_2$ and therefore $\text{PH} = \Sigma_2$.

Results: Quantum Karp-Lipton

- Karp-Lipton theorem: SAT cannot be solved with poly-size circuits, unless PH collapses to its second level.
 - Generally assumed that $\Sigma_{k+1} \neq \Sigma_k$ for all k .
 - Formally: If $\text{NP} \subseteq \text{P}_{/\text{poly}}$, then $\Pi_2 = \Sigma_2$ and therefore $\text{PH} = \Sigma_2$.
- GSSSY22: If $\text{Precise-QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QC}\Pi_2 = \text{QC}\Sigma_2$.

Results: Quantum Karp-Lipton

- Karp-Lipton theorem: SAT cannot be solved with poly-size circuits, unless PH collapses to its second level.
 - Generally assumed that $\Sigma_{k+1} \neq \Sigma_k$ for all k .
 - Formally: If $\text{NP} \subseteq \text{P}_{/\text{poly}}$, then $\Pi_2 = \Sigma_2$ and therefore $\text{PH} = \Sigma_2$.
- GSSSY22: If $\text{Precise-QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QC}\Pi_2 = \text{QC}\Sigma_2$.

$\text{BQP}_{/\text{mpoly}}$ (BQP with deterministic poly-size Merlin-like advice)

Promise problem $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{BQP}_{/\text{mpoly}}$ if there exists a *poly-time uniform* family of quantum circuits $\{C_n\}_{n \in \mathbb{N}}$ and a collection of advice strings $\{a_n\}_{n \in \mathbb{N}}$ with $|a_n| = \text{poly}(n)$ s.t.

- $x \in L_{\text{yes}} \Rightarrow \Pr[C_n \text{ accepts } |x\rangle|a_n\rangle] \geq 2/3$
- $x \in L_{\text{no}} \Rightarrow \Pr[C_n \text{ accepts } |x\rangle|a_n\rangle] \leq 1/3$

Results: Quantum Karp-Lipton

- Karp-Lipton theorem: SAT cannot be solved with poly-size circuits, unless PH collapses to its second level.
 - Generally assumed that $\Sigma_{k+1} \neq \Sigma_k$ for all k .
 - Formally: If $\text{NP} \subseteq \text{P}_{/\text{poly}}$, then $\Pi_2 = \Sigma_2$ and therefore $\text{PH} = \Sigma_2$.
- GSSSY22: If $\text{Precise-QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QC}\Pi_2 = \text{QC}\Sigma_2$.

$\text{BQP}_{/\text{mpoly}}$ (BQP with deterministic poly-size Merlin-like advice)

Promise problem $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{BQP}_{/\text{mpoly}}$ if there exists a *poly-time uniform* family of quantum circuits $\{C_n\}_{n \in \mathbb{N}}$ and a collection of advice strings $\{a_n\}_{n \in \mathbb{N}}$ with $|a_n| = \text{poly}(n)$ s.t.

- $x \in L_{\text{yes}} \Rightarrow \Pr[C_n \text{ accepts } |x\rangle|a_n\rangle] \geq 2/3$
- $x \in L_{\text{no}} \Rightarrow \Pr[C_n \text{ accepts } |x\rangle|a_n\rangle] \leq 1/3$
- Why? Same problem as $\exists\text{BPP}$ vs. MA : $\text{BQP}_{/\text{poly}}$ has to accept with probability $\leq 1/3$ or $\geq 2/3$ **even for bad advice!**

Results: Quantum Karp-Lipton

- Karp-Lipton theorem: SAT cannot be solved with poly-size circuits, unless PH collapses to its second level.
 - Generally assumed that $\Sigma_{k+1} \neq \Sigma_k$ for all k .
 - Formally: If $\text{NP} \subseteq \text{P}_{/\text{poly}}$, then $\Pi_2 = \Sigma_2$ and therefore $\text{PH} = \Sigma_2$.
- GSSSY22: If $\text{Precise-QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QC}\Pi_2 = \text{QC}\Sigma_2$.

Collapse theorem for QCPH

If for any $k \geq 1$, $\text{QC}\Pi_k = \text{QC}\Sigma_k$, then $\text{QCPH} = \text{QC}\Sigma_k$.

- Also in concurrent work [Falor, Ge, Natarajan, 2023]

Results: Quantum Karp-Lipton

- Karp-Lipton theorem: SAT cannot be solved with poly-size circuits, unless PH collapses to its second level.
 - Generally assumed that $\Sigma_{k+1} \neq \Sigma_k$ for all k .
 - Formally: If $\text{NP} \subseteq \text{P}_{/\text{poly}}$, then $\Pi_2 = \Sigma_2$ and therefore $\text{PH} = \Sigma_2$.
- GSSSY22: If $\text{Precise-QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QC}\Pi_2 = \text{QC}\Sigma_2$.

Collapse theorem for QCPH

If for any $k \geq 1$, $\text{QC}\Pi_k = \text{QC}\Sigma_k$, then $\text{QCPH} = \text{QC}\Sigma_k$.

Karp-Lipton theorem for QCPH

If $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QCPH} = \text{QC}\Sigma_2 = \text{QC}\Pi_2$.

Results: Quantum Karp-Lipton

- Karp-Lipton theorem: SAT cannot be solved with poly-size circuits, unless PH collapses to its second level.
 - Generally assumed that $\Sigma_{k+1} \neq \Sigma_k$ for all k .
 - Formally: If $\text{NP} \subseteq \text{P}_{/\text{poly}}$, then $\Pi_2 = \Sigma_2$ and therefore $\text{PH} = \Sigma_2$.
- GSSSY22: If $\text{Precise-QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QC}\Pi_2 = \text{QC}\Sigma_2$.

Collapse theorem for QCPH

If for any $k \geq 1$, $\text{QC}\Pi_k = \text{QC}\Sigma_k$, then $\text{QCPH} = \text{QC}\Sigma_k$.

Karp-Lipton theorem for QCPH

If $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QCPH} = \text{QC}\Sigma_2 = \text{QC}\Pi_2$.

- QCMA cannot be solved by (non-uniform) poly-size quantum circuits, unless QCPH collapses to its second level.

Results: Error Reduction

One-sided error reduction for pureQPH

For all $i > 0$ and $c - s \geq 1/p(n)$ for some polynomial p ,

- ① For even $i > 0$:

$$\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}} \left(1 - \frac{1}{e^n}, 1 - \frac{1}{np(n)^2} \right)$$

Results: Error Reduction

One-sided error reduction for pureQPH

For all $i > 0$ and $c - s \geq 1/p(n)$ for some polynomial p ,

① For even $i > 0$:

① $\text{pureQ}\Sigma_i(c, s) \subseteq \text{pureQ}\Sigma_i^{\text{SEP}}(1/np(n)^2, 1/e^n)$

② $\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}}(1 - 1/e^n, 1 - 1/np(n)^2)$

② For odd $i > 0$:

① $\text{pureQ}\Sigma_i(c, s) \subseteq \text{pureQ}\Sigma_i^{\text{SEP}}(1 - 1/e^n, 1 - 1/np(n)^2)$

② $\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}}(1/np(n)^2, 1/e^n)$

Results: Error Reduction

One-sided error reduction for pureQPH

For all $i > 0$ and $c - s \geq 1/p(n)$ for some polynomial p ,

① For even $i > 0$:

① $\text{pureQ}\Sigma_i(c, s) \subseteq \text{pureQ}\Sigma_i^{\text{SEP}}(1/np(n)^2, 1/e^n)$

② $\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}}(1 - 1/e^n, 1 - 1/np(n)^2)$

② For odd $i > 0$:

① $\text{pureQ}\Sigma_i(c, s) \subseteq \text{pureQ}\Sigma_i^{\text{SEP}}(1 - 1/e^n, 1 - 1/np(n)^2)$

② $\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}}(1/np(n)^2, 1/e^n)$

- $\text{pureQ}\Sigma_i^{\text{SEP}} \subseteq \text{pureQ}\Sigma_i$ same as $\text{pureQ}\Sigma_i$, but YES-case POVM must be separable across all i proofs: $H = \sum_j H_1^{(j)} \otimes \cdots \otimes H_i^{(j)}$

Results: Error Reduction

One-sided error reduction for pureQPH

For all $i > 0$ and $c - s \geq 1/p(n)$ for some polynomial p ,

① For even $i > 0$:

- ① $\text{pureQ}\Sigma_i(c, s) \subseteq \text{pureQ}\Sigma_i^{\text{SEP}}(1/np(n)^2, 1/e^n)$
- ② $\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}}(1 - 1/e^n, 1 - 1/np(n)^2)$

② For odd $i > 0$:

- ① $\text{pureQ}\Sigma_i(c, s) \subseteq \text{pureQ}\Sigma_i^{\text{SEP}}(1 - 1/e^n, 1 - 1/np(n)^2)$
- ② $\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}}(1/np(n)^2, 1/e^n)$

- **Significance:** One-sided error reduction for QMA(2) [Aaronson, Beigi, Drucker, Fefferman, Shor, 2008] is the first step in the two-sided error reduction [Harrow, Montanaro, 2012], also relying on verifier separability.

Results: Error Reduction

One-sided error reduction for pureQPH

For all $i > 0$ and $c - s \geq 1/p(n)$ for some polynomial p ,

① For even $i > 0$:

① $\text{pureQ}\Sigma_i(c, s) \subseteq \text{pureQ}\Sigma_i^{\text{SEP}}(1/np(n)^2, 1/e^n)$

② $\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}}(1 - 1/e^n, 1 - 1/np(n)^2)$

② For odd $i > 0$:

① $\text{pureQ}\Sigma_i(c, s) \subseteq \text{pureQ}\Sigma_i^{\text{SEP}}(1 - 1/e^n, 1 - 1/np(n)^2)$

② $\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}}(1/np(n)^2, 1/e^n)$

- **Significance:** One-sided error reduction for QMA(2) [Aaronson, Beigi, Drucker, Fefferman, Shor, 2008] is the first step in the two-sided error reduction [Harrow, Montanaro, 2012], also relying on verifier separability.

- Note, $\text{QMA}(2) \subseteq \text{Q}\Sigma_3 \subseteq \text{pureQ}\Sigma_3$.

Results: Upper & Lower Bounds

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

Results: Upper & Lower Bounds

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

Theorem

$\text{QCPH} \subseteq \text{pureQPH} \subseteq \text{EXP}^{\text{PP}}$

Results: Upper & Lower Bounds

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

Theorem

$\text{QCPH} \subseteq \text{pureQPH} \subseteq \text{EXP}^{\text{PP}}$

- Concurrent work: $\text{QCPH} = \text{DistributionQCPH} \subseteq \text{QPH}$, at the cost of constant factor blowup in level [Grewal, Yirka, 2024].

Results: Upper & Lower Bounds

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

Theorem

$\text{QCPH} \subseteq \text{pureQPH} \subseteq \text{EXP}^{\text{PP}}$

- Concurrent work: $\text{QCPH} = \text{DistributionQCPH} \subseteq \text{QPH}$, at the cost of constant factor blowup in level [Grewal, Yirka, 2024].
- Containment in EXP^{PP} follows from Toda's theorem:

$$\text{pureQ}\Sigma_i \subseteq \text{NEXP}^{\text{NP}^{i-1}} \subseteq \text{EXP}^{\text{NP}^i} = \text{EXP}^{\text{P}^{\text{PP}}} = \text{EXP}^{\text{PP}}$$

- 1 Introduction
- 2 Results
- 3 Quantum Karp-Lipton**
- 4 Error Reduction
- 5 Lower Bounds
- 6 Conclusion

Collapse theorem

Collapse theorem for QCPH

If for any $k \geq 1$, $\text{QC}\Pi_k = \text{QC}\Sigma_k$, then $\text{QCPH} = \text{QC}\Sigma_k$.

Collapse theorem

Collapse theorem for QCPH

If for any $k \geq 1$, $\text{QC}\Pi_k = \text{QC}\Sigma_k$, then $\text{QCPH} = \text{QC}\Sigma_k$.

Lemma

If for any $k \geq 1$, $\text{QC}\Sigma_k = \text{QC}\Pi_k$, then for all $i \geq k$, $\text{QC}\Sigma_i = \text{QC}\Pi_i = \text{QC}\Sigma_k$.

Lemma

If for any $k \geq 1$, $QC\Sigma_k = QC\Pi_k$, then for all $i \geq k$, $QC\Sigma_i = QC\Pi_i = QC\Sigma_k$.

Proof.

Proof by induction: Assume $QC\Sigma_j = QC\Pi_j = QC\Sigma_k$ for all $j \in \{k, \dots, i-1\}$.



Lemma

If for any $k \geq 1$, $QC\Sigma_k = QC\Pi_k$, then for all $i \geq k$, $QC\Sigma_i = QC\Pi_i = QC\Sigma_k$.

Proof.

Proof by induction: Assume $QC\Sigma_j = QC\Pi_j = QC\Sigma_k$ for all $j \in \{k, \dots, i-1\}$. Let $L = (L_{\text{yes}}, L_{\text{no}}) \in QC\Sigma_i$ with verifier V_n . Define $L' = (L'_{\text{yes}}, L'_{\text{no}})$:



Lemma

If for any $k \geq 1$, $QC\Sigma_k = QC\Pi_k$, then for all $i \geq k$, $QC\Sigma_i = QC\Pi_i = QC\Sigma_k$.

Proof.

Proof by induction: Assume $QC\Sigma_j = QC\Pi_j = QC\Sigma_k$ for all $j \in \{k, \dots, i-1\}$. Let $L = (L_{\text{yes}}, L_{\text{no}}) \in QC\Sigma_i$ with verifier V_n . Define $L' = (L'_{\text{yes}}, L'_{\text{no}})$:

$$L'_{\text{yes}} = \{(x, y_1) \mid \forall y_2 \exists y_3 \cdots Q_i y_i : \Pr[V_n(x, y_1, \dots, y_i) = 1] \geq 2/3\}$$

$$L'_{\text{no}} = \{(x, y_1) \mid \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : \Pr[V_n(x, y_1, \dots, y_i) = 1] \leq 1/3\}$$



Lemma

If for any $k \geq 1$, $\text{QC}\Sigma_k = \text{QC}\Pi_k$, then for all $i \geq k$, $\text{QC}\Sigma_i = \text{QC}\Pi_i = \text{QC}\Sigma_k$.

Proof.

Proof by induction: Assume $\text{QC}\Sigma_j = \text{QC}\Pi_j = \text{QC}\Sigma_k$ for all $j \in \{k, \dots, i-1\}$. Let $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Sigma_i$ with verifier V_n . Define $L' = (L'_{\text{yes}}, L'_{\text{no}})$:

$$L'_{\text{yes}} = \{(x, y_1) \mid \forall y_2 \exists y_3 \cdots Q_i y_i : \Pr[V_n(x, y_1, \dots, y_i) = 1] \geq 2/3\}$$

$$L'_{\text{no}} = \{(x, y_1) \mid \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : \Pr[V_n(x, y_1, \dots, y_i) = 1] \leq 1/3\}$$

$L' \in \text{QC}\Pi_{i-1} = \text{QC}\Sigma_{i-1}$. Thus there exists V'_n s.t.

$$(x, y_1) \in L'_{\text{yes}} \Rightarrow \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : \Pr[V'_n(x, y_1, \dots, y_i) = 1] \geq 2/3$$

$$(x, y_1) \in L'_{\text{no}} \Rightarrow \forall y_2 \exists y_3 \cdots Q_i y_i : \Pr[V'_n(x, y_1, \dots, y_i) = 1] \leq 1/3$$



Lemma

If for any $k \geq 1$, $QC\Sigma_k = QC\Pi_k$, then for all $i \geq k$, $QC\Sigma_i = QC\Pi_i = QC\Sigma_k$.

Proof.

Proof by induction: Assume $QC\Sigma_j = QC\Pi_j = QC\Sigma_k$ for all $j \in \{k, \dots, i-1\}$. Let $L = (L_{\text{yes}}, L_{\text{no}}) \in QC\Sigma_i$ with verifier V_n . Define $L' = (L'_{\text{yes}}, L'_{\text{no}})$:

$$L'_{\text{yes}} = \{(x, y_1) \mid \forall y_2 \exists y_3 \cdots Q_i y_i : \Pr[V_n(x, y_1, \dots, y_i) = 1] \geq 2/3\}$$

$$L'_{\text{no}} = \{(x, y_1) \mid \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : \Pr[V_n(x, y_1, \dots, y_i) = 1] \leq 1/3\}$$

$L' \in QC\Pi_{i-1} = QC\Sigma_{i-1}$. Thus there exists V'_n s.t.

$$(x, y_1) \in L'_{\text{yes}} \Rightarrow \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : \Pr[V'_n(x, y_1, \dots, y_i) = 1] \geq 2/3$$

$$(x, y_1) \in L'_{\text{no}} \Rightarrow \forall y_2 \exists y_3 \cdots Q_i y_i : \Pr[V'_n(x, y_1, \dots, y_i) = 1] \leq 1/3$$

$$x \in L_{\text{yes}} \Rightarrow \exists y_1 : (x, y_1) \in L'_{\text{yes}} \Rightarrow \exists y_1 \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : \Pr[V'_n(x, y_1, \dots, y_i) = 1] \geq 2/3$$

$$x \in L_{\text{no}} \Rightarrow \forall y_1 : (x, y_1) \in L'_{\text{no}} \Rightarrow \forall y_1 \forall y_2 \exists y_3 \cdots Q_i y_i : \Pr[V'_n(x, y_1, \dots, y_i) = 1] \leq 1/3$$

□

Lemma

If for any $k \geq 1$, $QC\Sigma_k = QC\Pi_k$, then for all $i \geq k$, $QC\Sigma_i = QC\Pi_i = QC\Sigma_k$.

Proof.

Proof by induction: Assume $QC\Sigma_j = QC\Pi_j = QC\Sigma_k$ for all $j \in \{k, \dots, i-1\}$. Let $L = (L_{\text{yes}}, L_{\text{no}}) \in QC\Sigma_i$ with verifier V_n . Define $L' = (L'_{\text{yes}}, L'_{\text{no}})$:

$$L'_{\text{yes}} = \{(x, y_1) \mid \forall y_2 \exists y_3 \cdots Q_i y_i : \Pr[V_n(x, y_1, \dots, y_i) = 1] \geq 2/3\}$$

$$L'_{\text{no}} = \{(x, y_1) \mid \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : \Pr[V_n(x, y_1, \dots, y_i) = 1] \leq 1/3\}$$

$L' \in QC\Pi_{i-1} = QC\Sigma_{i-1}$. Thus there exists V'_n s.t.

$$(x, y_1) \in L'_{\text{yes}} \Rightarrow \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : \Pr[V'_n(x, y_1, \dots, y_i) = 1] \geq 2/3$$

$$(x, y_1) \in L'_{\text{no}} \Rightarrow \forall y_2 \exists y_3 \cdots Q_i y_i : \Pr[V'_n(x, y_1, \dots, y_i) = 1] \leq 1/3$$

$$x \in L_{\text{yes}} \Rightarrow \exists y_1 : (x, y_1) \in L'_{\text{yes}} \Rightarrow \exists y_1 \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i : \Pr[V'_n(x, y_1, \dots, y_i) = 1] \geq 2/3$$

$$x \in L_{\text{no}} \Rightarrow \forall y_1 : (x, y_1) \in L'_{\text{no}} \Rightarrow \forall y_1 \forall y_2 \exists y_3 \cdots Q_i y_i : \Pr[V'_n(x, y_1, \dots, y_i) = 1] \leq 1/3$$

Hence, $L \in QC\Sigma_{i-1}$. □

Karp-Lipton theorem for QCPH

If $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QCPH} = \text{QC}\Sigma_2 = \text{QC}\Pi_2$.

Proof sketch.

- Let $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Pi_2$ with verifier V_n and negligible error ϵ .

Karp-Lipton theorem for QCPH

If $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QCPH} = \text{QC}\Sigma_2 = \text{QC}\Pi_2$.

Proof sketch.

- Let $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Pi_2$ with verifier V_n and negligible error ϵ .
- Need to show $L \in \text{QC}\Sigma_2$. Define verifier $V'_n(x, C, y_1) := V_n(x, y_1, C(x, y_1))$:
 - V'_n takes in quantum circuit C , computes $y_2 = C(x, y_1)$, and runs $V_n(x, y_1, y_2)$.

Karp-Lipton theorem for QCPH

If $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QCPH} = \text{QC}\Sigma_2 = \text{QC}\Pi_2$.

Proof sketch.

- Let $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Pi_2$ with verifier V_n and negligible error ϵ .
- Need to show $L \in \text{QC}\Sigma_2$. Define verifier $V'_n(x, C, y_1) := V_n(x, y_1, C(x, y_1))$:
- If $x \in L_{\text{no}}$, then $\exists y_1 \forall y_2 : \Pr[V_n(x, y_1, y_2) = 1] \leq \epsilon$. Thus,
 $\forall C \exists y_1 : \Pr[V'_n(x, C, y_1) = 1] \leq \epsilon$.

Karp-Lipton theorem for QCPH

If $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QCPH} = \text{QC}\Sigma_2 = \text{QC}\Pi_2$.

Proof sketch.

- Let $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Pi_2$ with verifier V_n and negligible error ϵ .
- Need to show $L \in \text{QC}\Sigma_2$. Define verifier $V'_n(x, C, y_1) := V_n(x, y_1, C(x, y_1))$:
- If $x \in L_{\text{no}}$, then $\exists y_1 \forall y_2 : \Pr[V_n(x, y_1, y_2) = 1] \leq \epsilon$. Thus,
 $\forall C \exists y_1 : \Pr[V'_n(x, C, y_1) = 1] \leq \epsilon$.
- If $x \in L_{\text{yes}}$, given y_1 , the problem of finding y_2 s.t. $V_n(x, y_1, y_2)$ accepts, is in QCMA.

Karp-Lipton theorem for QCPH

If $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QCPH} = \text{QC}\Sigma_2 = \text{QC}\Pi_2$.

Proof sketch.

- Let $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Pi_2$ with verifier V_n and negligible error ϵ .
- Need to show $L \in \text{QC}\Sigma_2$. Define verifier $V'_n(x, C, y_1) := V_n(x, y_1, C(x, y_1))$:
- If $x \in L_{\text{no}}$, then $\exists y_1 \forall y_2: \Pr[V_n(x, y_1, y_2) = 1] \leq \epsilon$. Thus, $\forall C \exists y_1: \Pr[V'_n(x, C, y_1) = 1] \leq \epsilon$.
- If $x \in L_{\text{yes}}$, given y_1 , the problem of finding y_2 s.t. $V_n(x, y_1, y_2)$ accepts, is in QCMA.
- Use randomized reduction from QCMA to UQCMA [Aharonov, Ben-Or, Brandão, Sattah, 2022] to compute instance $\phi_{(x, y_1)}$ with unique witness. By $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, \exists circuit \tilde{C} deciding $\phi_{(x, y_1)}$.

Karp-Lipton theorem for QCPH

If $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QCPH} = \text{QC}\Sigma_2 = \text{QC}\Pi_2$.

Proof sketch.

- Let $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Pi_2$ with verifier V_n and negligible error ϵ .
- Need to show $L \in \text{QC}\Sigma_2$. Define verifier $V'_n(x, C, y_1) := V_n(x, y_1, C(x, y_1))$:
- If $x \in L_{\text{no}}$, then $\exists y_1 \forall y_2: \Pr[V_n(x, y_1, y_2) = 1] \leq \epsilon$. Thus, $\forall C \exists y_1: \Pr[V'_n(x, C, y_1) = 1] \leq \epsilon$.
- If $x \in L_{\text{yes}}$, given y_1 , the problem of finding y_2 s.t. $V_n(x, y_1, y_2)$ accepts, is in QCMA.
- Use randomized reduction from QCMA to UQCMA [ABBS22] to compute instance $\phi_{(x, y_1)}$ with unique witness. By $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, \exists circuit \tilde{C} deciding $\phi_{(x, y_1)}$.
- Apply search-to-decision reduction of [Irani, Natarajan, Nirkhe, Rao, Yuen, 2022] to construct circuit C that finds the unique witness for $\phi_{(x, y_1)}$:
 $\Pr_{y_2 \leftarrow C(x, y_1)}[V_n(x, y_1, y_2) = 1] \geq 1/\text{poly}$.

Karp-Lipton theorem for QCPH

If $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, then $\text{QCPH} = \text{QC}\Sigma_2 = \text{QC}\Pi_2$.

Proof sketch.

- Let $L = (L_{\text{yes}}, L_{\text{no}}) \in \text{QC}\Pi_2$ with verifier V_n and negligible error ϵ .
- Need to show $L \in \text{QC}\Sigma_2$. Define verifier $V'_n(x, C, y_1) := V_n(x, y_1, C(x, y_1))$:
- If $x \in L_{\text{no}}$, then $\exists y_1 \forall y_2: \Pr[V_n(x, y_1, y_2) = 1] \leq \epsilon$. Thus,
 $\forall C \exists y_1: \Pr[V'_n(x, C, y_1) = 1] \leq \epsilon$.
- If $x \in L_{\text{yes}}$, given y_1 , the problem of finding y_2 s.t. $V_n(x, y_1, y_2)$ accepts, is in QCMA.
- Use randomized reduction from QCMA to UQCMA [ABBS22] to compute instance $\phi_{(x, y_1)}$ with unique witness. By $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$, \exists circuit \tilde{C} deciding $\phi_{(x, y_1)}$.
- Apply search-to-decision reduction of [INNRY22] to construct circuit C that finds the unique witness for $\phi_{(x, y_1)}$: $\Pr_{y_2 \leftarrow C(x, y_1)}[V_n(x, y_1, y_2) = 1] \geq 1/\text{poly}$.
- $\exists C \forall y_1: \Pr[V'_n(x, C, y_1) = 1] \geq 1/\text{poly}$. □

- 1 Introduction
- 2 Results
- 3 Quantum Karp-Lipton
- 4 Error Reduction**
- 5 Lower Bounds
- 6 Conclusion

Asymmetric Product Test (APT)

Recall, for $L \in \text{pureQ}\Pi_i$ (i even), there exist c, s with $c - s \geq 1/\text{poly}$ s.t.

Asymmetric Product Test (APT)

Recall, for $L \in \text{pureQ}\Pi_i$ (i even), there exist c, s with $c - s \geq 1/\text{poly}$ s.t.

- $x \in L_{\text{yes}} \Rightarrow \forall |\psi_1\rangle \exists |\psi_2\rangle \cdots \exists |\psi_i\rangle: \Pr[V(|x, \psi_1, \dots, \psi_i\rangle) = 1] \geq c$
- $x \in L_{\text{no}} \Rightarrow \exists |\psi_1\rangle \forall |\psi_2\rangle \cdots \forall |\psi_i\rangle: \Pr[V(|x, \psi_1, \dots, \psi_i\rangle) = 1] \leq s$

Asymmetric Product Test (APT)

Recall, for $L \in \text{pureQ}\Pi_i$ (i even), there exist c, s with $c - s \geq 1/\text{poly}$ s.t.

- $x \in L_{\text{yes}} \Rightarrow \forall |\psi_1\rangle \exists |\psi_2\rangle \cdots \exists |\psi_i\rangle: \Pr[V(|x, \psi_1, \dots, \psi_i\rangle) = 1] \geq 1 - 1/\text{exp}$
- $x \in L_{\text{no}} \Rightarrow \exists |\psi_1\rangle \forall |\psi_2\rangle \cdots \forall |\psi_i\rangle: \Pr[V(|x, \psi_1, \dots, \psi_i\rangle) = 1] \leq 1/\text{exp}$
- Could do “majority voting” if we get $\text{poly}(n)$ copies of each state.

Asymmetric Product Test (APT)

Recall, for $L \in \text{pureQ}\Pi_i$ (i even), there exist c, s with $c - s \geq 1/\text{poly}$ s.t.

- $x \in L_{\text{yes}} \Rightarrow \forall |\psi_1\rangle \exists |\psi_2\rangle \cdots \exists |\psi_i\rangle: \Pr[V(|x, \psi_1, \dots, \psi_i\rangle) = 1] \geq 1 - 1/\text{exp}$
- $x \in L_{\text{no}} \Rightarrow \exists |\psi_1\rangle \forall |\psi_2\rangle \cdots \forall |\psi_i\rangle: \Pr[V(|x, \psi_1, \dots, \psi_i\rangle) = 1] \leq 1 - 1/\text{poly}$
- Could do “majority voting” if we get $\text{poly}(n)$ copies of each state.
- If the last proof $|\psi_i\rangle$ contains copies of all previous states, then we can still do majority voting. Verify this with the APT!

Asymmetric Product Test (APT)

Recall, for $L \in \text{pureQ}\Pi_i$ (i even), there exist c, s with $c - s \geq 1/\text{poly}$ s.t.

- $x \in L_{\text{yes}} \Rightarrow \forall |\psi_1\rangle \exists |\psi_2\rangle \cdots \exists |\psi_i\rangle: \Pr[V(|x, \psi_1, \dots, \psi_i\rangle) = 1] \geq 1 - 1/\text{exp}$
- $x \in L_{\text{no}} \Rightarrow \exists |\psi_1\rangle \forall |\psi_2\rangle \cdots \forall |\psi_i\rangle: \Pr[V(|x, \psi_1, \dots, \psi_i\rangle) = 1] \leq 1 - 1/\text{poly}$
- Could do “majority voting” if we get $\text{poly}(n)$ copies of each state.
- If the last proof $|\psi_i\rangle$ contains copies of all previous states, then we can still do majority voting. Verify this with the APT!
- We construct new “asymmetric version” of the product test [Mintert, Kuś, Buchleitner, 2005] [Harrow, Montanaro, 2012]

APT

① Input:

- Register A : $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ with $|\psi_i\rangle \in \mathbb{C}^{d_i}$
- Register B : $|\phi\rangle \in \mathbb{C}^{(d:=d_1 \cdots d_n)^m}$ (m copies of $|\psi\rangle$)

APT

① Input:

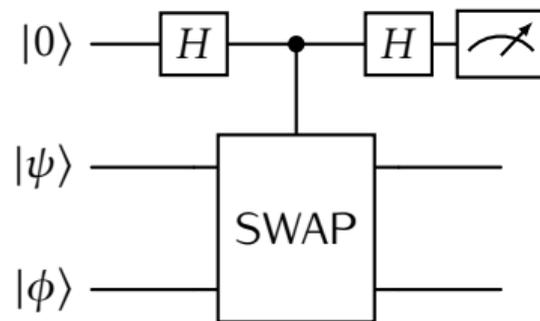
- Register A : $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ with $|\psi_i\rangle \in \mathbb{C}^{d_i}$
- Register B : $|\phi\rangle \in \mathbb{C}^{(d:=d_1 \cdots d_n)^m}$ (m copies of $|\psi\rangle$)

② Choose $(i, j) \in [n] \times [m]$ uniformly at random.

APT

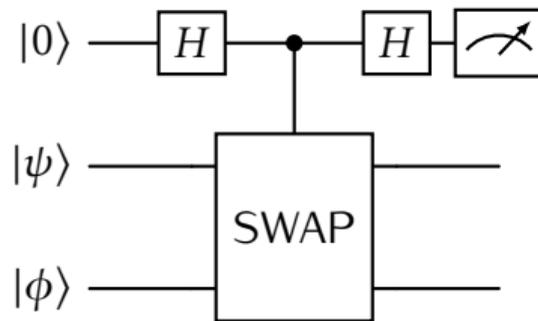
① Input:

- Register A : $|\psi\rangle = |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$ with $|\psi_i\rangle \in \mathbb{C}^{d_i}$
- Register B : $|\phi\rangle \in \mathbb{C}^{(d:=d_1 \dots d_n)^m}$ (m copies of $|\psi\rangle$)

② Choose $(i, j) \in [n] \times [m]$ uniformly at random.③ Run SWAP test between i -th register of A and its j -th copy in B .

APT

- 1 Input:
 - Register A : $|\psi\rangle = |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$ with $|\psi_i\rangle \in \mathbb{C}^{d_i}$
 - Register B : $|\phi\rangle \in \mathbb{C}^{(d:=d_1 \dots d_n)^m}$ (m copies of $|\psi\rangle$)
- 2 Choose $(i, j) \in [n] \times [m]$ uniformly at random.
- 3 Run SWAP test between i -th register of A and its j -th copy in B .



Lemma

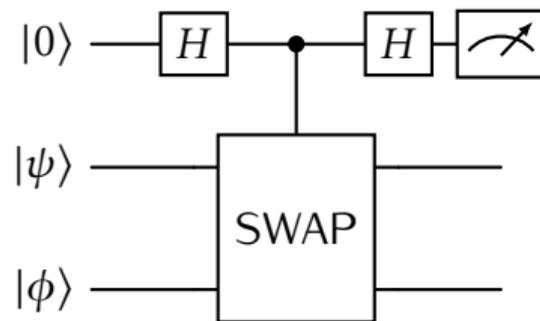
Let $|\phi\rangle_{BC} \in \mathbb{C}^{d^m} \otimes \mathbb{C}^{d'}$ for some $d' > 0$ s.t.

$$\max_{|\psi\rangle := |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle \in \mathbb{C}^d} \langle \phi |_{BC} [(|\psi\rangle \langle \psi|^{\otimes m})_B \otimes I_C] | \phi \rangle_{BC} = 1 - \epsilon$$

for $\epsilon \geq 0$.

APT

- 1 Input:
 - Register A : $|\psi\rangle = |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle$ with $|\psi_i\rangle \in \mathbb{C}^{d_i}$
 - Register B : $|\phi\rangle \in \mathbb{C}^{(d:=d_1 \dots d_n)^m}$ (m copies of $|\psi\rangle$)
- 2 Choose $(i, j) \in [n] \times [m]$ uniformly at random.
- 3 Run SWAP test between i -th register of A and its j -th copy in B .



Lemma

Let $|\phi\rangle_{BC} \in \mathbb{C}^{d^m} \otimes \mathbb{C}^{d'}$ for some $d' > 0$ s.t.

$$\max_{|\psi\rangle := |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle \in \mathbb{C}^d} \langle \phi |_{BC} [(|\psi\rangle\langle\psi|^{\otimes m})_B \otimes I_C] | \phi \rangle_{BC} = 1 - \epsilon$$

for $\epsilon \geq 0$. Then, APT accepts $|\eta\rangle_{ABC} := |\psi\rangle_A \otimes |\phi\rangle_{BC}$ w.p. $\leq 1 - \epsilon/2mn$ for all $|\psi\rangle$.

One-sided Error Reduction

Lemma

Let i be even, $c - s \geq 1/p(n)$. Then

$$\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}} \left(1 - \frac{1}{e^n}, 1 - \frac{1}{np(n)^2} \right).$$

One-sided Error Reduction

Lemma

Let i be even, $c - s \geq 1/p(n)$. Then

$$\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}} \left(1 - \frac{1}{e^n}, 1 - \frac{1}{np(n)^2} \right).$$

- Let V be a verifier for $L \in \text{pureQ}\Pi_i(c, s)$ s.t.

One-sided Error Reduction

Lemma

Let i be even, $c - s \geq 1/p(n)$. Then

$$\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}} \left(1 - \frac{1}{e^n}, 1 - \frac{1}{np(n)^2} \right).$$

- Let V be a verifier for $L \in \text{pureQ}\Pi_i(c, s)$ s.t.
- Verifier $V'((|\psi_1\rangle \otimes \cdots \otimes |\psi_{i-1}\rangle)_A \otimes |\psi_i\rangle_{BC})$ with $|\psi_i'\rangle = (|\psi_1\rangle \otimes \cdots \otimes |\psi_{i-1}\rangle)_B^{\otimes m} \otimes |\psi_i\rangle_C^{\otimes m}$ (for honest last prover). Do with probability $1/2$:

One-sided Error Reduction

Lemma

Let i be even, $c - s \geq 1/p(n)$. Then

$$\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}} \left(1 - \frac{1}{e^n}, 1 - \frac{1}{np(n)^2} \right).$$

- Let V be a verifier for $L \in \text{pureQ}\Pi_i(c, s)$ s.t.
- Verifier $V'(|\psi_1\rangle \otimes \cdots \otimes |\psi_{i-1}\rangle\rangle_A \otimes |\psi_i\rangle\rangle_{BC})$ with $|\psi_i'\rangle = (|\psi_1\rangle \otimes \cdots \otimes |\psi_{i-1}\rangle\rangle_B^{\otimes m} \otimes |\psi_i\rangle\rangle_C^{\otimes m}$ (for honest last prover). Do with probability $1/2$:
 - ① Apply APT between A and B .

One-sided Error Reduction

Lemma

Let i be even, $c - s \geq 1/p(n)$. Then

$$\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}} \left(1 - \frac{1}{e^n}, 1 - \frac{1}{np(n)^2} \right).$$

- Let V be a verifier for $L \in \text{pureQ}\Pi_i(c, s)$ s.t.
- Verifier $V'((|\psi_1\rangle \otimes \cdots \otimes |\psi_{i-1}\rangle)_A \otimes |\psi_i\rangle_{BC})$ with $|\psi_i'\rangle = (|\psi_1\rangle \otimes \cdots \otimes |\psi_{i-1}\rangle)_B^{\otimes m} \otimes |\psi_i\rangle_C^{\otimes m}$ (for honest last prover). Do with probability $1/2$:
 - ① Apply APT between A and B .
 - ② Run original verifier V verifier on all m copies of $|\psi_1\rangle, \dots, |\psi_i\rangle$ inside B, C and accept if at least $(c + s)/2$ runs accept.

One-sided Error Reduction

Lemma

Let i be even, $c - s \geq 1/p(n)$. Then

$$\text{pureQ}\Pi_i(c, s) \subseteq \text{pureQ}\Pi_i^{\text{SEP}} \left(1 - \frac{1}{e^n}, 1 - \frac{1}{np(n)^2} \right).$$

- Let V be a verifier for $L \in \text{pureQ}\Pi_i(c, s)$ s.t.
- Verifier $V'((|\psi_1\rangle \otimes \cdots \otimes |\psi_{i-1}\rangle)_A \otimes |\psi_i\rangle_{BC})$ with $|\psi_i\rangle = (|\psi_1\rangle \otimes \cdots \otimes |\psi_{i-1}\rangle)_B^{\otimes m} \otimes |\psi_i\rangle_C^{\otimes m}$ (for honest last prover). Do with probability $1/2$:
 - 1 Apply APT between A and B .
 - 2 Run original verifier V verifier on all m copies of $|\psi_1\rangle, \dots, |\psi_i\rangle$ inside B, C and accept if at least $(c + s)/2$ runs accept.
- Note that APT also bounds entanglement between B, C .

- 1 Introduction
- 2 Results
- 3 Quantum Karp-Lipton
- 4 Error Reduction
- 5 Lower Bounds**
- 6 Conclusion

QCPH \subseteq pureQPH

Lemma

For all even $k \geq 2$, $\text{Q}\Pi_k \subseteq \text{pureQ}\Pi_k$.

QCPH \subseteq pureQPH

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

- Let V be a verifier for $L \in \text{QC}\Pi_k$ s.t.

QCPH \subseteq pureQPH

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

- Let V be a verifier for $L \in \text{QC}\Pi_k$ s.t.
 - $x \in L_{\text{yes}} \Rightarrow \forall y_1 \dots \exists y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \geq 1 - 1/\exp$
 - $x \in L_{\text{no}} \Rightarrow \exists y_1 \dots \forall y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \leq 1/\exp$

QCPH \subseteq pureQPH

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

- Let V be a verifier for $L \in \text{QC}\Pi_k$ s.t.
 - $x \in L_{\text{yes}} \Rightarrow \forall y_1 \dots \exists y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \geq 1 - 1/\text{exp}$
 - $x \in L_{\text{no}} \Rightarrow \exists y_1 \dots \forall y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \leq 1/\text{exp}$
- Define pureQ Π_k verifier $V'(|x\rangle \otimes |\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle \otimes |\psi'_k\rangle)$. Last proof $|\psi'_k\rangle = (|\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle)_B^{\otimes m} \otimes |\psi_k\rangle_C$ (honest prover).

QCPH \subseteq pureQPH

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

- Let V be a verifier for $L \in \text{QC}\Pi_k$ s.t.
 - $x \in L_{\text{yes}} \Rightarrow \forall y_1 \dots \exists y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \geq 1 - 1/\text{exp}$
 - $x \in L_{\text{no}} \Rightarrow \exists y_1 \dots \forall y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \leq 1/\text{exp}$
- Define pureQ Π_k verifier $V'(|x\rangle \otimes |\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle \otimes |\psi'_k\rangle)$. Last proof $|\psi'_k\rangle = (|\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle)_B^{\otimes m} \otimes |\psi_k\rangle_C$ (honest prover). Do with probability 1/2:
 - 1 Run APT between A (i.e. $|\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle$) and B .

QCPH \subseteq pureQPH

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

- Let V be a verifier for $L \in \text{QC}\Pi_k$ s.t.
 - $x \in L_{\text{yes}} \Rightarrow \forall y_1 \cdots \exists y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \geq 1 - 1/\exp$
 - $x \in L_{\text{no}} \Rightarrow \exists y_1 \cdots \forall y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \leq 1/\exp$
- Define pureQ Π_k verifier $V'(|x\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_{k-1}\rangle \otimes |\psi'_k\rangle)$. Last proof $|\psi'_k\rangle = (|\psi_1\rangle \otimes \cdots \otimes |\psi_{k-1}\rangle)_B^{\otimes m} \otimes |\psi_k\rangle_C$ (honest prover). Do with probability 1/2:
 - 1 Run APT between A (i.e. $|\psi_1\rangle \otimes \cdots \otimes |\psi_{k-1}\rangle$) and B .
 - 2 Measure all proofs in standard basis and denote the outcomes by y_1, \dots, y_k and $y_{i,j}$ for the j -th copy of i .

QCPH \subseteq pureQPH

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

- Let V be a verifier for $L \in \text{QC}\Pi_k$ s.t.
 - $x \in L_{\text{yes}} \Rightarrow \forall y_1 \dots \exists y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \geq 1 - 1/\exp$
 - $x \in L_{\text{no}} \Rightarrow \exists y_1 \dots \forall y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \leq 1/\exp$
- Define pureQ Π_k verifier $V'(|x\rangle \otimes |\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle \otimes |\psi'_k\rangle)$. Last proof $|\psi'_k\rangle = (|\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle)_B^{\otimes m} \otimes |\psi_k\rangle_C$ (honest prover). Do with probability 1/2:
 - 1 Run APT between A (i.e. $|\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle$) and B .
 - 2 Measure all proofs in standard basis and denote the outcomes by y_1, \dots, y_k and $y_{i,j}$ for the j -th copy of i .
 - If there exists i, j s.t. $y_i \neq y_{i,j}$, reject if i is even (\exists), accept if i is odd (\forall).

QCPH \subseteq pureQPH

Lemma

For all even $k \geq 2$, $\text{QC}\Pi_k \subseteq \text{pureQ}\Pi_k$.

- Let V be a verifier for $L \in \text{QC}\Pi_k$ s.t.
 - $x \in L_{\text{yes}} \Rightarrow \forall y_1 \dots \exists y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \geq 1 - 1/\exp$
 - $x \in L_{\text{no}} \Rightarrow \exists y_1 \dots \forall y_k: \Pr[V(x, y_1, \dots, y_k) = 1] \leq 1/\exp$
- Define pureQ Π_k verifier $V'(|x\rangle \otimes |\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle \otimes |\psi'_k\rangle)$. Last proof $|\psi'_k\rangle = (|\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle)_B^{\otimes m} \otimes |\psi_k\rangle_C$ (honest prover). Do with probability 1/2:
 - 1 Run APT between A (i.e. $|\psi_1\rangle \otimes \dots \otimes |\psi_{k-1}\rangle$) and B .
 - 2 Measure all proofs in standard basis and denote the outcomes by y_1, \dots, y_k and $y_{i,j}$ for the j -th copy of i .
 - If there exists i, j s.t. $y_i \neq y_{i,j}$, reject if i is even (\exists), accept if i is odd (\forall).
 - Otherwise, run $V(x, y_1, \dots, y_k)$.

- 1 Introduction
- 2 Results
- 3 Quantum Karp-Lipton
- 4 Error Reduction
- 5 Lower Bounds
- 6 Conclusion**

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.
 - Otherwise, oracle separation?

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.
 - Otherwise, oracle separation?
- Is $\text{pureQPH} \subseteq \text{QPH}$?

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.
 - Otherwise, oracle separation?
- Is $\text{pureQPH} \subseteq \text{QPH}$?
- Error reduction for QPH?

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.
 - Otherwise, oracle separation?
- Is $\text{pureQPH} \subseteq \text{QPH}$?
- Error reduction for QPH?
- Two-sided error reduction for pureQPH ?

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.
 - Otherwise, oracle separation?
- Is $\text{pureQPH} \subseteq \text{QPH}$?
- Error reduction for QPH?
- Two-sided error reduction for pureQPH ?
- Collapse theorem for QPH/ pureQPH ?

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.
 - Otherwise, oracle separation?
- Is $\text{pureQPH} \subseteq \text{QPH}$?
- Error reduction for QPH?
- Two-sided error reduction for pureQPH ?
- Collapse theorem for QPH/ pureQPH ?
- Evidence that QCPH/QPH/ pureQPH *don't* collapse?

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.
 - Otherwise, oracle separation?
- Is $\text{pureQPH} \subseteq \text{QPH}$?
- Error reduction for QPH?
- Two-sided error reduction for pureQPH?
- Collapse theorem for QPH/pureQPH?
- Evidence that QCPH/QPH/pureQPH *don't* collapse?
- Improve $\text{pureQPH} \subseteq \text{EXP}^{\text{PP}}$. Is $\text{pureQ}\Sigma_3 \subseteq \text{NEXP}$?

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.
 - Otherwise, oracle separation?
- Is $\text{pureQPH} \subseteq \text{QPH}$?
- Error reduction for QPH?
- Two-sided error reduction for pureQPH?
- Collapse theorem for QPH/pureQPH?
- Evidence that QCPH/QPH/pureQPH *don't* collapse?
- Improve $\text{pureQPH} \subseteq \text{EXP}^{\text{PP}}$. Is $\text{pureQ}\Sigma_3 \subseteq \text{NEXP}$?
 - [GSSSY22] shows $\text{Q}\Sigma_3 \subseteq \text{NEXP}$: Guess $|\psi_1\rangle$ and use $\text{Q}\Pi_2 \subseteq \text{EXP}$.

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.
 - Otherwise, oracle separation?
- Is $\text{pureQPH} \subseteq \text{QPH}$?
- Error reduction for QPH?
- Two-sided error reduction for pureQPH?
- Collapse theorem for QPH/pureQPH?
- Evidence that QCPH/QPH/pureQPH *don't* collapse?
- Improve $\text{pureQPH} \subseteq \text{EXP}^{\text{PP}}$. Is $\text{pureQ}\Sigma_3 \subseteq \text{NEXP}$?
 - [GSSSY22] shows $\text{Q}\Sigma_3 \subseteq \text{NEXP}$: Guess $|\psi_1\rangle$ and use $\text{Q}\Pi_2 \subseteq \text{EXP}$.
 - Even $\text{pureQ}\Pi_2 \in \text{NEXP}$ remains open.

Open Questions

- Toda's theorem for QCPH, i.e., $\text{QCPH} \subseteq \text{P}^{\text{PP}}$?
 - [GSSSY22] shows $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.
 - Otherwise, oracle separation?
- Is $\text{pureQPH} \subseteq \text{QPH}$?
- Error reduction for QPH?
- Two-sided error reduction for pureQPH?
- Collapse theorem for QPH/pureQPH?
- Evidence that QCPH/QPH/pureQPH *don't* collapse?
- Improve $\text{pureQPH} \subseteq \text{EXP}^{\text{PP}}$. Is $\text{pureQ}\Sigma_3 \subseteq \text{NEXP}$?
 - [GSSSY22] shows $\text{Q}\Sigma_3 \subseteq \text{NEXP}$: Guess $|\psi_1\rangle$ and use $\text{Q}\Pi_2 \subseteq \text{EXP}$.
 - Even $\text{pureQ}\Pi_2 \in \text{NEXP}$ remains open.

Thanks.