Quantum Polynomial Hierarchies: Collapses, Karp-Lipton, and More

A merged presentation of:

The Entangled Quantum Polynomial Hierarchy Collapses

Sabee Grewal and Justin Yirka

The University of Texas at Austin

sabee@cs.utexas.edu, yirka@cs.utexas.edu

arXiv: 2401.01453

&

Quantum Polynomial Hierarchies: Karp-Lipton, error reduction, and lower bounds

Avantika Agarwal,[1] Sevag Gharibian,[2] Venkata Koppula,[3] and Dorian Rudolph[2]

[1]University of Waterloo, [2]Paderborn University, [3]IIT Delhi

a243agarwal@uwaterloo.ca, sevag.gharibian@upb.de, kvenkata@iitd.ac.in, dorian.rudolph@upb.de

arXiv: 2401.01633

The University of Texas at Austin
Department of Computer Science
College of Natural Sciences

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

INSTITUTE FOR PHOTONIC QUANTUM SYSTEMS
UNIVERSITÄT PADERBORN

What is the Polynomial Hierarchy (PH)?

PH is a hierarchy of complexity classes generalizing NP. It's *strongly* believed the levels of PH are distinct, just as we believe $\mathrm{P} \neq \mathrm{NP}$. All of PH equals P if and only if $\mathrm{P} = \mathrm{NP}$.

PH has applications in understanding the power of randomness, low-depth circuits, counting classes, interactive proofs, second order logic, and near-term quantum sampling protocols!

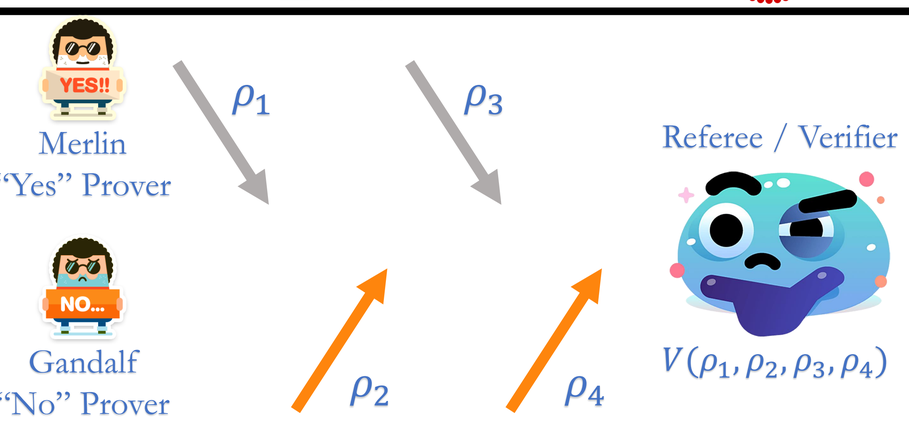
The levels of PH are denoted Σ_k and Π_k for $k \geq 0$. Each level adds a layer of nondeterminism:

$$\Sigma_0 = \Pi_0 = \mathrm{P}, \qquad \Sigma_1 = \mathrm{NP}, \qquad \Pi_1 = \mathrm{coNP}, \qquad \Sigma_2 = \mathrm{NP}^{\mathrm{NP}}, \qquad \Pi_2 = \mathrm{coNP}^{\mathrm{NP}}, \ldots$$

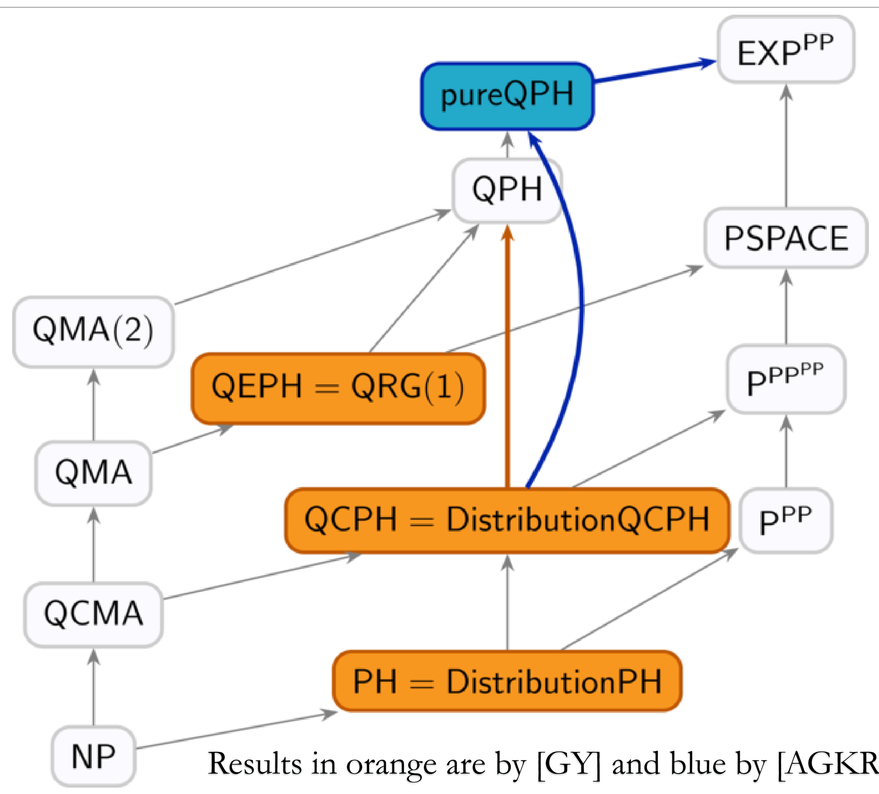
Game theoretic intuition: Σ_k is the set of questions for which the answer can be verified by a k-round debate with a computationally efficient referee.

Merlin argues the answer is YES, Gandalf argues the answer is NO. The two provers alternate sending messages to the referee. The provers can see each other's messages and respond accordingly. The referee is passive, i.e. non-interactive.

PH is a constant-round, competing, non-interactive, public (perfect information) game.



PH	If the correct answer is YES:	$\exists y_1\, \forall y_2\, \exists y_3\, \forall y_4$ such that $\mathrm{M}(y_1, y_2, y_3, y_4) = 1$
	If the correct answer is NO:	$\forall y_1\, \exists y_2\, \forall y_3\, \exists y_4$ such that $\mathrm{M}(y_1, y_2, y_3, y_4) = 0$
QPH	If the correct answer is YES:	$\exists \rho_1\, \forall \rho_2\, \exists \rho_3\, \forall \rho_4$ such that $V(\rho_1, \rho_2, \rho_3, \rho_4) = 1$ w.h.p.
	If the correct answer is NO:	$\forall \rho_1\, \exists \rho_2\, \forall \rho_3\, \exists \rho_4$ such that $V(\rho_1, \rho_2, \rho_3, \rho_4) = 0$ w.h.p.



Results in orange are by [GY] and blue by [AGKR]

Quantum versions of PH

Just like QCMA, QMA, QMA_1, and QMA(2), there are several natural definitions for quantum PH. [GSSSY 2018] defined QCPH and QPH. Both classes generalize $\mathrm{BQP} = \mathrm{QC}\Sigma_0 = \mathrm{Q}\Sigma_0$.

QCPH generalizes $\mathrm{QCMA} = \mathrm{QC}\Sigma_1$. QPH generalizes $\mathrm{QMA} = \mathrm{Q}\Sigma_1$ *and* $\mathrm{QMA}(2) \subseteq \mathrm{Q}\Sigma_3$.

	Proof type	Verifier type	Results
PH	Classical string	Classical	in QPH
QCPH	Classical strings	Quantum	in QPH
QPH	(Unentangled) quantum states	Quantum	
pureQPH	Pure (Unentangled) quantum states	Quantum	in $\mathrm{EXP}^{\mathrm{PP}}$
QEPH	Entangled quantum states	Quantum	equals QRG(1)
DistributionPH	Classical mixed states	Classical	equals PH
DistributionQCPH	Classical mixed states	Quantum	equals QCPH

Entanglement: QEPH collapses to QRG(1)

We define QEPH. Now, the provers are allowed to entangle their proofs: e.g. Merlin's message in round 1 may be entangled with his message in round 3. Here, we have *relaxed* the constraints on the provers, closer to the QIP and QRG models. We prove QEPH collapses to the 2nd level, which equals QRG(1).

RG and QRG are "Refereed Games" that are *interactive* with *private* communication. The referee sends follow-up questions to the provers, and the provers do not see each other's messages.

$$\mathrm{QMA} \subseteq \mathrm{P}^{\mathrm{QMA}} \subseteq \mathrm{QRG}(1) \overset{?}{\subset} \mathrm{QRG}(2) = \mathrm{PSPACE}$$

Proof sketch: with no un-entanglement, QEPH collapses by convexity and minimax arguments. In fact, this even works for a polynomial number of QEPH rounds.

$$\max_{\rho_1} \min_{\rho_2} \max_{\rho_3} f(\rho_1, \rho_2, \rho_3) = \max_{\rho_1} \max_{\rho_3} \min_{\rho_2} f(\rho_1, \rho_2, \rho_3) = \max_{\rho_{1,3}} \min_{\rho_2} f(\rho_{1,3}, \rho_2)$$

If $\mathrm{QC}\Sigma_k = \mathrm{QC}\Pi_k$ then QCPH collapses

Note that in contrast to PH and QCPH, we know $\mathrm{Q}\Sigma_2 = \mathrm{Q}\Pi_2 = \mathrm{QRG}(1)$ are equal.

This collapse theorem was left open by [GSSSY18] because of subtle issues dealing with promise gaps. We give a careful proof handling these issues, showing QCPH behaves similarly to PH.

Karp-Lipton: If $\mathrm{QCMA} \subseteq \mathrm{BQP}_{/\mathrm{mpoly}}$ then $\mathrm{QC}\Sigma_2$

In words, there do not exist small circuits solving QCMA unless QCPH collapses.

Using our new collapse theorem above, we want to show $\mathrm{QCMA} \subseteq \mathrm{BQP}_{/\mathrm{mpoly}}$ implies $\mathrm{QC}\Sigma_2 = \mathrm{QC}\Pi_2$. The classical Karp-Lipton theorem uses search-to-decision reduction for SAT. However, this does not easily work with quantum promise problems. We use the QCMA Valiant-Vazirani filter of [ABBS08] to make any accepting proofs unique. Then we use the single-query quantum search-to-decision reduction for UQCMA from [INNRY22]. From here, the proof follows as for Karp-Lipton.

Classical mixed states: DistributionPH = PH

QPH alters proofs in two ways: (1) they are quantum not classical states (2) the states may be mixed. Convexity arguments often let us restrict our attention to pure states, but here the competitive setup breaks this. For example: is it true that for all x there exists a y such that $x = y$? If x, y are bits then YES. But if x, y are qubits – or even single-bit classical mixed states – then NO.

We define DistributionPH and DistributionQCPH to allow classical mixed states / distributions / random variables as proofs (and the referee gets one sample). These proofs are an intermediate between classical and quantum states.

This presents a new game theory model: proofs are public, but they are undetermined (random).

We find that in fact, PH = DistributionPH and QCPH = DistributionQCPH.

Our proof generalizes a result of [Lipton and Young 1994] that provers can send distributions with at most polynomial support.

QPH is at least as powerful as PH: PH, QCPH ⊆ QPH

[GSSSY18] defined QPH but left it an open problem whether QPH contained QCPH or even PH! QPH trivially contains QMA(2), QMA, and BQP, but containment of PH is non-trivial. Provers might cheat by sending mixtures of strings instead of a fixed string.

We show PH ⊆ QCPH ⊆ QPH. Our proof is a careful parallel repetition protocol which increases the number of rounds by a constant multiple.

PH, QCPH ⊆ pureQPH

Error-reduction: We introduce pureQPH and show one-sided error reduction for it. While error reduction for QCPH follows from parallel repetition, it is non-trivial for QPH or pureQPH just like for QMA(2) - the tensor product structure is not necessarily preserved during repetition.

To overcome this, we give an asymmetric version of the Product Test [Harrow, Montanaro 13] dubbed the APT. The APT takes in an n-system state $|\psi\rangle$ in register A, and (ideally) m copies of $|\psi\rangle$ in register B. The APT accepts if B is the correct form and $|\psi\rangle$ is a product state.

Lower-bound: We use the APT to force the final pureQPH prover to send many copies of *all* previous proofs, forcing the provers to send classical strings instead of superpositions.

This avoid the multiplicative blowup of [GY], but gives QCPH ⊆ pureQPH not ⊆ QPH.

New upper bound: QPH ⊆ $\mathrm{EXP}^{\mathrm{PP}}$

QPH ⊆ pureQPH: This follows by purification of mixed states. Just double the number of qubits.

pureQPH ⊆ $\mathrm{EXP}^{\mathrm{PP}}$: The only previous bound on QPH is the trivial $\mathrm{QPH} \subseteq \mathrm{EXPH} = \mathrm{NEXP}^{\mathrm{NP}^{\mathrm{NP}^{\cdots}}}$. We upper bound both QPH and pureQPH by $\mathrm{EXP}^{\mathrm{PP}}$, an exponential analogue to Today's theorem.

Proof: $\mathrm{pureQ}\Sigma_k \subseteq \mathrm{NEXP}^{\mathrm{NP}^{k-1}}$, and $\mathrm{NEXP}^{\mathrm{O}} \subseteq \mathrm{EXP}^{\mathrm{NP}^{\mathrm{O}}}$ for any O, so $\mathrm{pureQ}\Sigma_k \subseteq \mathrm{EXP}^{\mathrm{NP}^{k-1}}$. Then, $\mathrm{NP}^k \subseteq \mathrm{P}^{\mathrm{PP}}$ (Toda's theorem), so $\mathrm{pureQ}\Sigma_k \subseteq \mathrm{EXP}^{\mathrm{P}^{\mathrm{PP}}}$. Finally, EXP can simulate the P computation so that $\mathrm{EXP}^{\mathrm{P}^{\mathrm{PP}}} \subseteq \mathrm{EXP}^{\mathrm{PP}}$.

Open Questions

Can $\mathrm{QEPH} = \mathrm{QRG}(1)$ help resolve $\mathrm{QRG}(1)$ vs. $\mathrm{QRG}(2) = \mathrm{PSPACE}$?

Can QPH help attack QMA(2)? Know $\mathrm{QMA}(2) \subseteq \mathrm{Q}\Sigma_3 \subseteq \mathrm{NEXP}$. Is $\mathrm{pureQ}\Sigma_3 \subseteq \mathrm{NEXP}$?

Compare quantifier definitions with oracle definitions: $\mathrm{QMAH} = \mathrm{QMA}^{\mathrm{QMA}^{\cdots}}$, which is in the counting hierarchy and PSPACE, while $\mathrm{QMA}(2) \subseteq \mathrm{QPH} \subseteq \mathrm{EXP}^{\mathrm{PP}}$.

References

Gharibian, Santha, Sikora, Sundaram, Yirka. Quantum generalizations of the polynomial hierarchy with applications to QMA(2). 2018. – Aharonov, Ben-Or, Brandao, Sattath. The Pursuit of Uniqueness: Extending Valiant-Vazirani Theorem to the Probabilistic and Quantum Settings. 2008. – Irani, Natarajan, Nirkhe, Rao, Yuen. Quantum search-to-decision reductions and the state synthesis problem. 2022. – Lipton, Young. Simple Strategies for Large Zero-Sum Games with Applications to Complexity Theory. 1994.

Acknowledgments

SG and JY were supported via Scott Aaronson by a Vannevar Bush Fellowship from the US Department of Defense, the Berkeley NSF-QLCI CIQC Center, a Simons Investigator Award, and the Simons "It from Qubit" collaboration. This work was completed in part while AA was a student at IIT Delhi and while visiting Paderborn University. SG was supported by the DFG under grant numbers 450041824 and 432788384, the BMBF within the funding program "Quantum Technologies - from Basic Research to Market" via project PhoQuant (grant number 13N16103), and the project "PhoQC" from the programme "Profilbildung 2020", an initiative of the Ministry of Culture and Science of the State of Northrhine Westphalia. VK was supported by the Pankaj Gupta Fellowship at IIT Delhi.