Quantum Generalizations of the Polynomial Hierarchy with Applications to QMA(2)

Sevag Gharibian
University of Paderborn, Paderborn, North Rhine-Westphalia, Germany, and Virginia Commonwealth University, Richmond, Virginia, USA

Miklos Santha
CNRS, IRIF, Université Paris Diderot, Paris, France and Centre for Quantum Technologies, National University of Singapore, Singapore

Jamie Sikora
Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada

Aarthi Sundaram
Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, Maryland, USA

Justin Yirka
Virginia Commonwealth University, Richmond, Virginia, USA

Abstract

The polynomial-time hierarchy (PH) has proven to be a powerful tool for providing separations in computational complexity theory (modulo standard conjectures such as PH does not collapse). Here, we study whether two quantum generalizations of PH can similarly prove separations in the quantum setting. The first generalization, QCPH, uses classical proofs, and the second, QPH, uses quantum proofs. For the former, we show quantum variants of the Karp-Lipton theorem and Toda's theorem. For the latter, we place its third level, $Q\Sigma_3$, into NEXP using the Ellipsoid Method for efficiently solving semidefinite programs. These results yield two implications for QMA(2), the variant of Quantum Merlin-Arthur (QMA) with two unentangled proofs, a complexity class whose characterization has proven difficult. First, if QCPH = QPH (i.e., alternating quantifiers are sufficiently powerful so as to make classical and quantum proofs "equivalent"), then QMA(2) is in the Counting Hierarchy (specifically, in $\mathrm{P}^{\mathrm{PP}^{\mathrm{PP}}}$). Second, unless $\mathrm{QMA}(2) = Q\Sigma_3$ (i.e., alternating quantifiers do not help in the presence of "unentanglement"), QMA(2) is strictly contained in NEXP.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory, Theory of computation → Complexity classes, Theory of computation → Semidefinite programming

Keywords and phrases Complexity Theory, Quantum Computing, Polynomial Hierarchy, Semidefinite Programming, QMA(2), Quantum Complexity

Digital Object Identifier 10.4230/LIPIcs.MFCS.2018.58

Related Version A full version of this work is available at `https://arxiv.org/abs/1805.11139`.

Acknowledgements SG and AS thank the Center for Quantum Technologies at the National University of Singapore for their support and hospitality, where part of this research was carried out. SG acknowledges support from NSF grants CCF-1526189 and CCF-1617710. AS is supported by the Department of Defense. Research at the Centre for Quantum Technologies is partially funded by the Singapore Ministry of Education and the National Research Foundation under grant R-710-000-012-135. This research was supported in part by the QuantERA ERA-NET

Cofund project QuantAlgo. Research at Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Economic Development Canada and by the Province of Ontario through the Ministry of Research, Innovation and Science.

1 Introduction

The polynomial time hierarchy (PH) [28] is a staple of computational complexity theory, and generalizes P, NP and co-NP with the use of alternating existential ($\exists$) and universal ($\forall$) operators. Roughly, a language $L \subseteq \{0,1\}^*$ is in Σ_i^p, the ith level of PH, if there exists a polynomial-time deterministic Turing machine M that acts as a verifier and accepts i proofs $y_1, \ldots, y_i$ polynomially bounded in size such that:

$$x \in L \quad \Rightarrow \quad \exists y_1 \forall y_2 \exists y_3 \cdots Q_i y_i \text{ such that } M \text{ accepts } (x, y_1, \ldots, y_i),$$
$$x \notin L \quad \Rightarrow \quad \forall y_1 \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i \text{ such that } M \text{ rejects } (x, y_1, \ldots, y_i),$$

where $Q_i = \exists$ if i is odd and $Q_i = \forall$ if i is even, and $\overline{Q}$ denotes the complement of Q. Then, PH is defined as the union over all Σ_i^p for all $i \in \mathbb{N}$. The study of PH has proven remarkably fruitful in the classical setting, from celebrated results such as Toda's Theorem [30], which shows that PH is contained in $\mathrm{P}^{\#\mathrm{P}}$, to the Karp-Lipton Theorem [21], which says that unless PH collapses to its second level, NP does not have polynomial size non-uniform circuits.

As PH has played a role in separating complexity classes (assuming standard conjectures like "PH does not collapse"), it is natural to ask whether *quantum* generalizations of PH can be used to separate *quantum* complexity classes. Here, there is some flexibility in defining "quantum PH", as there is more than one well-defined notion of "quantum NP": The first, Quantum-Classical Merlin Arthur (QCMA) [6], is a quantum analogue of Merlin-Arthur (MA) with a classical proof but quantum verifier. The second, Quantum Merlin Arthur (QMA) [22], is QCMA except with a quantum proof. Generalizing each of these definitions leads to (at least) two possible definitions for "quantum PH", the first using classical proofs (denoted QCPH), and the second using quantum proofs (denoted QPH).

With these definitions in hand, our aim is to separate quantum classes whose complexity characterization has generally been difficult to pin down. A prime example is QMA(2), the variant of QMA with two "unentangled" quantum provers. While the classical analogue of QMA(2) (i.e. an MA proof system with two provers) trivially equals MA, in the quantum regime multiple unentangled provers are conjectured to yield a more powerful proof system (e.g. there exist problems in QMA(2) not known to be in QMA) [24, 10, 9, 1]. For this reason, QMA(2) has received much attention, despite which the strongest bounds known on QMA(2) remain the trivial ones: QMA $\subseteq$ QMA(2) $\subseteq$ NEXP. (Note: QMA $\subseteq$ PP [23, 27].) In this work, we show that, indeed, results about the structure of QCPH or QPH yield implications about the power of QMA(2).

1.1 Results, techniques, and discussion

We begin by informally defining the two quantum generalizations of PH to be studied.

How to define a "quantum PH"? The first definition, QCPH, has its ith level $\mathrm{QC}\Sigma_i$ defined analogously to Σ_i^p, except we replace the Turing machine M with a polynomial-size uniformly generated quantum circuit V such that:

$$x \in A_{\text{yes}} \Rightarrow \exists y_1 \forall y_2 \exists y_3 \cdots Q_i y_i \text{ s.t. } V \text{ accepts } (x, y_1, \ldots, y_i) \text{ with probability } \geq 2/3, \quad (1)$$
$$x \in A_{\text{no}} \Rightarrow \forall y_1 \exists y_2 \forall y_3 \cdots \overline{Q}_i y_i \text{ s.t. } V \text{ accepts } (x, y_1, \ldots, y_i) \text{ with probability } \leq 1/3, \quad (2)$$

where the use of a language L has been replaced with a *promise problem*[1] $A = (A_{\text{yes}}, A_{\text{no}})$ (since $\text{QC}\Sigma_i$ uses a bounded error verifier). The values $2/3$ and $1/3$ are respectively the *completeness* and *soundness* parameters for A and the interval $(1/3, 2/3)$ where no acceptance probabilities are present is termed the *promise gap* for A. Notice that QCPH defined as $\bigcup_{i\in\mathbb{N}} \text{QC}\Sigma_i$, is a generalization of QCMA in that $\text{QC}\Sigma_1 = \text{QCMA}$.

We next define QPH using *quantum* proofs. Here, however, there are various possible definitions one might consider. Can the quantum proofs be *entangled* between alternating quantifiers? (If not, we are enforcing "unentanglement" as in QMA(2). Allowing entanglement, on the other hand, might yield classes similar to QIP; however, note that QIP = QIP(3) (i.e. QIP collapses to a 3-message proof system) [23, 27], and so it is not clear that allowing entanglement leads to an "interesting" hierarchy.) Assuming proofs are unentangled, should the proofs be *pure* or *mixed* quantum states? (For QMA and QMA(2), standard convexity arguments show both classes of proofs are equivalent, but such arguments fail when *alternating* quantifiers are allowed.)

Here, we define QPH to have its ith level, $\text{Q}\Sigma_i$, defined similarly to $\text{QC}\Sigma_i$, except each classical proof y_j is replaced with a mixed quantum state ρ_j on polynomially many qubits. We say a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in $\text{Q}\Sigma_i$ if it satisfies the following conditions:

$$\begin{aligned} x \in A_{\text{yes}} &\Rightarrow \exists \rho_1 \forall \rho_2 \exists \rho_3 \cdots Q_i \rho_i \text{ such that } V \text{ accepts } (x, \rho_1, \ldots, \rho_i) \text{ with probability} \geq 2/3, \\ x \in A_{\text{no}} &\Rightarrow \forall \rho_1 \exists \rho_2 \forall \rho_3 \cdots \overline{Q}_i \rho_i \text{ such that } V \text{ accepts } (x, \rho_1, \ldots, \rho_i) \text{ with probability} \leq 1/3. \end{aligned}$$

Note that $\text{QPH} := \bigcup_{i\in\mathbb{N}} \text{Q}\Sigma_i$, $\text{Q}\Sigma_1 = \text{QMA}$ and $\text{QMA}(2) \subseteq \text{Q}\Sigma_3$ (simply ignore the second proof); where the latter two hold because a lack of alternating quantifiers allows convexity arguments to yield that all proofs can be assumed to be pure. Our results are now stated as follows under three headings.

An analogue of Toda's theorem for QCPH. As previously mentioned, PH is one way to generalize NP using alternations. Another approach is to *count* the number of solutions for an NP-complete problem such as SAT, as captured by #P. Surprisingly, these two notions are related, as shown by the following celebrated theorem of Toda.

▶ **Theorem 1** (Toda's Theorem [30]). $\text{PH} \subseteq \text{P}^{\#\text{P}}$.

In the quantum setting, for QCPH, it can be shown using standard arguments involving enumeration over classical proofs that QCPH $\subseteq$ PSPACE. However, we are able to provide the following stronger result.

▶ **Theorem 2** (A quantum-classical analogue of Toda's theorem). $\text{QCPH} \subseteq \text{P}^{\text{PP}^{\text{PP}}}$.

Thus, we "almost" recover the original bound of Toda's theorem[2], except we require an oracle for the *second* level of the Counting Hierarchy (CH). CH can be defined with its first level as $\mathbf{C}_1^p = \text{PP}$ and its kth level for $k \geq 1$ as $\mathbf{C}_{k+1}^p = \text{PP}^{\mathbf{C}_k^p}$.

Why did we move up to the next level of CH? There are two difficulties in dealing with QCPH (see Section 2 for a detailed discussion). The first can be sketched as follows. Classically, many results involving PH, from basic ones implying the collapse of PH to more

[1] Recall that unlike a decision problem, for a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$, it is not necessarily true that for all inputs $x \in \Sigma^*$, either $x \in A_{\text{yes}}$ or $x \in A_{\text{no}}$. In the case of proof systems such as QCPH, when $x \notin A_{\text{yes}} \cup A_{\text{no}}$, V can output an arbitrary answer.

[2] PP is the set of languages decidable in probabilistic polynomial time with unbounded error. Note $\text{P}^{\text{PP}} = \text{P}^{\#\text{P}}$.

advanced statements such as Toda's theorem, use the following recursive idea (demonstrated with Σ_2 for simplicity): By fixing the existentially quantified proof of Σ_2 the remnant reduces to a co-NP problem, i.e. we can recurse to a lower level of PH. In the quantum setting, however, this does not hold – fixing the existentially quantified proof for $\mathrm{QC}\Sigma_2$ does *not* necessarily yield a co-QCMA problem as some acceptance probabilities may fall in the $(1/3, 2/3)$ promise gap which cannot happen for a problem in co-QCMA! (This is due to the same phenomenon that has been an obstacle to resolving whether $\exists \cdot \mathrm{BPP}$ equals MA (see Remark 17).) Thus, we cannot directly generalize recursive arguments from the classical setting to the quantum setting. The second difficulty is trickier to explain briefly (see Section 2.2 for details). Roughly, Toda's proof that $\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$ crucially uses the Valiant-Vazirani (VV) theorem [31], which has one-sided error (i.e. VV may map YES instances of SAT to NO instances of UNIQUE-SAT, but NO instances of SAT are always mapped to NO instances of UNIQUE-SAT). The VV theorem for QCMA [5] also has this property, but in addition it can output instances which are "invalid". Essentially, they violate the promise of the problem that the QCMA-VV theorem maps to. Combining such *invalid* instances with *alternating* quantifiers, poses problems in extending the parity arguments used in Toda's proof to the QCPH setting.

To circumvent these difficulties, we exploit a high-level idea from [15] where an oracle for SPECTRAL GAP[3] was used to detect "invalid" QMA instances[4]. In our setting, the "correct" choice of oracle turns out to be a Precise-BQP oracle, where Precise-BQP is roughly BQP with an exponentially small promise gap. Using this, we are able to essentially "remove" the promise gap of QCPH altogether, thus recovering a "decision problem" which does not pose the difficulties above. Specifically, this mapping is achieved by Lemma 18 (Cleaning Lemma), which shows that $\forall i \in \mathbb{N},\ \mathrm{QC}\Sigma_i \subseteq \exists \cdot \forall \cdot \cdots \cdot Q_i \cdot \mathrm{P}^{\mathrm{PP}}$.

Notice that although we use a Precise-BQP oracle above, the Cleaning Lemma shows containment using a PP oracle. This is because, Precise-BQP $\subseteq$ PP as shown in Lemma 14 and Corollary 15. One may ask whether our proof technique would also work with an oracle *weaker* than PP. We show, in Theorem 27, that this is unlikely as the problem of detecting proofs in promise gaps of quantum verifiers is PP-complete.

Finally, an immediate corollary of Theorem 2 and the fact that $\mathrm{QMA}(2) \subseteq \mathrm{QPH}$ is:

▶ **Corollary 3.** *If* $\mathrm{QCPH} = \mathrm{QPH}$*, then* $\mathrm{QMA}(2) \subseteq \mathrm{P}^{\mathrm{PP}^{\mathrm{PP}}}$.

In other words, if alternating quantifiers are so powerful so as to make classical and quantum proofs equivalent in power, then it can be shown that QMA(2) is contained in CH (and thus in PSPACE). For comparison, $\mathrm{QMA} \subseteq \mathrm{P}^{\mathrm{QMA[log]}} \subseteq \mathrm{PP}$ [23, 33, 27, 15].

QPH versus NEXP. We next turn to the study of *quantum* proofs, i.e. QPH. As mentioned above, the best known upper bound on QMA(2) is NEXP – a non-deterministic verifier can simply guess an exponential-size description of the proof. When alternating quantifiers are present, however, this strategy seemingly no longer works. In other words, it is not even clear that $\mathrm{QPH} \subseteq \mathrm{NEXP}$! This is in stark contrast to the explicit P^{PP} upper bound for PH [30]. In this section, our goal is to use semidefinite programming to give bounds on some levels of QPH. As we will see, this will yield the existence of a complexity class lying "between" QMA(2) and NEXP.

[3] This problem determines whether the spectral gap of a given local Hamiltonian is "small" or "large".
[4] This was used, in turn, to show in conjunction with [8] that SPECTRAL GAP is $\mathrm{P}^{\mathrm{Unique\text{-}QMA[log]}}$-hard.

▶ **Theorem 4** (Informal Statement). *It holds that* $Q\Sigma_2 \subseteq \mathrm{EXP}$ *and* $Q\Pi_2 \subseteq \mathrm{EXP}$*, even when the completeness-soundness gap is inverse doubly-exponentially small.*

The proof idea is to map alternating quantifiers to an optimization problem with alternating minimizations and maximizations. Namely, to decide if $x \in A_{\text{yes}}$ or $x \in A_{\text{no}}$ for a $Q\Sigma_i$ promise problem $A = (A_{\text{yes}}, A_{\text{no}})$, where i is even, we can solve for α defined as the optimal value of the optimization problem:

$$\alpha := \max_{\rho_1} \min_{\rho_2} \max_{\rho_3} \cdots \min_{\rho_i} \langle C, \rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_i \rangle \tag{3}$$

where C is the POVM operator[5] corresponding to the ACCEPT state of the verifier. This is a non-convex problem, and as such is hard to solve in general. Our approach is to cast the case of $i = 2$ as a semidefinite program (SDP), allowing us to *efficiently* approximate α.

The next natural question is whether a similar SDP reformulation might be used to show whether $Q\Sigma_3$ or $Q\Pi_3$ is contained in EXP. Unfortunately, this is likely to be difficult – indeed, if there existed a "nice" SDP for the optimal success probability of $Q\Sigma_3$ protocols, then it would imply $\mathrm{QMA}(2) \subseteq \mathrm{EXP}$, resolving the longstanding open problem of separating QMA(2) from NEXP (recall $\mathrm{QMA}(2) \subseteq Q\Sigma_3$). Likewise, a "nice" SDP for $Q\Pi_3$ would place $\text{co-QMA}(2) \subseteq \mathrm{EXP}$.

To overcome this, we resort to non-determinism by stepping up to NEXP. Namely, one can non-deterministically guess the first proof of a $Q\Sigma_3$ protocol, then approximately solve the SDP for the resulting $Q\Pi_2$-flavoured computation. Hence, we have the following as a corollary of Theorem 28.

▶ **Theorem 5** (Informal Statement). *It holds true that* $\mathrm{QMA}(2) \subseteq Q\Sigma_3 \subseteq \mathrm{NEXP}$ *and* $\text{co-QMA}(2) \subseteq Q\Pi_3 \subseteq \text{co-NEXP}$*, even when the completeness-soundness gap is inverse doubly-exponentially small. All the containments hold with equality in the inverse exponentially small completeness-soundness gap setting as* $\mathrm{QMA}(2) = \mathrm{NEXP}$ *in this case* [29].

Three remarks are in order. First, note that our results in this section are independent of the gate set. Second, in principle, it remains plausible that the fourth level of QPH already exceeds NEXP in power. Finally, we have the following implication for QMA(2). Assuming PH does not collapse, alternating quantifiers strictly add power to NP proof systems. If alternating quantifiers similarly add power in the quantum setting, then it would separate QMA(2) from NEXP via the following immediate corollary of Theorem 31.

▶ **Corollary 6.** *If* $\mathrm{QMA}(2) \neq Q\Sigma_3$*, i.e. if the second universally quantified proof of* $Q\Sigma_3$ *adds proving power, then* $\mathrm{QMA}(2) \neq \mathrm{NEXP}$*. Similarly, if* $\text{co-QMA}(2) \neq Q\Pi_3$*, then* $\text{co-QMA}(2) \neq \text{co-NEXP}$*.*

A quantum generalization of the Karp-Lipton Theorem. Finally, our last result studies a topic which is unrelated to QMA(2) – the well-known Karp-Lipton Theorem [21]. The latter shows that if NP-complete problems can be solved by polynomial-size non-uniform Boolean circuits, then $\Sigma_2 = \Pi_2$, which in turn implies that PH collapses to its second level. Here, a "non-uniform" circuit family means that the generation of a circuit for an input depends on the length of the input. The class of decision problems solved by such circuits is $\mathrm{P}_{/\mathrm{poly}}$.

▶ **Theorem 7** (Karp-Lipton [21]). *If* $\mathrm{NP} \subseteq \mathrm{P}_{/\mathrm{poly}}$ *then* $\Pi_2 = \Sigma_2$.

[5] A POVM is a set of Hermitian positive semi-definite operators that sums to the identity. In this case, the POVM has two operators – corresponding to the ACCEPT and REJECT states of the verifier.

In this work, we ask: Does $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$ imply $\text{QC}\Pi_2 = \text{QC}\Sigma_2$? Here, $\text{BQP}_{/\text{mpoly}}$ is the bounded-error analogue of $\text{P}_{/\text{poly}}$ with polynomial-size non-uniform quantum circuits (see Section 4 for formal definition). Unfortunately, generalizing the proof of the Karp-Lipton theorem is problematic for the same "$\exists \cdot \text{BPP}$ versus MA phenomenon" encountered earlier in extending Toda's result. Namely, the proof of Karp-Lipton proceeds by fixing the outer, universally quantified, proof of a Π_2^p machine, and applying the $\text{NP} \subseteq \text{P}_{/\text{poly}}$ hypothesis to the resulting NP computation. However, for $\text{QC}\Pi_2$, it is not clear that fixing the outer, universally quantified, proof yields a QCMA computation; thus, it is not obvious how to use the hypothesis $\text{QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$.

To sidestep this, our approach is to strengthen the hypothesis. Specifically, using the results of [20] on perfect completeness for QCMA, fixing the outer proof of a $\text{QC}\Pi_2$ computation can be seen to yield a Precise-QCMA "decision problem", where by "decision problem", we mean no proofs for the Precise-QCMA verifier are accepted within the promise gap. Here, Precise-QCMA is QCMA with exponentially small promise gap. We hence obtain:

▶ **Theorem 8** (A quantum-classical Karp-Lipton theorem). *If* Precise-QCMA $\subseteq \text{BQP}_{/\text{mpoly}}$*, then* $\text{QC}\Pi_2 = \text{QC}\Sigma_2$*.*

To give this result context, we also show that Precise-QCMA $\subseteq \text{NP}^{\text{PP}}$ (Lemma 38). However, whether $\text{QC}\Pi_2 = \text{QC}\Sigma_2$ collapses QCPH remains open due to the same "$\exists \cdot \text{BPP}$ versus MA phenomenon".

1.2 Related work

The first work we are aware of which considered a quantum version of PH is that of Yamakami [36], which differs from our setting in that it considers quantum Turing machines (we use quantum circuits) and quantum inputs (we use classical inputs, just like QMA). Gharibian and Kempe [14] next introduced and studied cq-Σ_2, defined as our $\text{QC}\Sigma_2$ except with a quantum universally quantified proof. [14] showed completeness and hardness of approximation results for cq-Σ_2 for (roughly) the following problem: What is the smallest number of terms required in a given local Hamiltonian for it to have a frustrated ground space? More recently, Lockhart and González-Guillén [25] considered a hierarchy (denoted QCPH' here) which *a priori* appears identical to our QCPH, but is apparently not so due to the "$\exists \cdot \text{BPP}$ versus MA phenomenon", which we discuss below.

In this work, the "$\exists \cdot \text{BPP}$ versus MA phenomenon", refers to the following discrepancy (see Remark 17 for details) – unlike with MA, *all* proofs in an $\exists \cdot \text{BPP}$ system *must* be accepted with probability at least $2/3$ or at most $1/3$ (i.e. no proof is accepted with probability in the gap $(1/3, 2/3)$). The quantum analogue of this phenomenon yields the open question: Is $\exists \cdot \text{BQP} = \text{NP}^{\text{BQP}}$ equal to QCMA? For this reason, it is not clear whether QCPH equals QCPH'. The latter is defined as $\text{QC}\Sigma_1' = \exists \cdot \text{BQP}$, $\text{QC}\Pi_1' = \forall \cdot \text{BQP}$, and

$$\forall m \geq 1, \text{QC}\Sigma_m' = \exists \cdot \text{QC}\Pi_{m-1}'; \qquad \text{QC}\Pi_m' = \forall \cdot \text{QC}\Sigma_{m-1}'.$$

Clearly, for us $\text{QC}\Sigma_1 = \text{QCMA}$ but in [25] $\text{QC}\Sigma_1' = \exists \cdot \text{BQP}$. The benefit from the latter definition is that one avoids the recursion problems discussed earlier – e.g., fixing the first existential proof in $\text{QC}\Sigma_2'$ *does* reduce the problem to a co-QCMA computation, unlike the case with $\text{QC}\Sigma_2$. Hence, recursive arguments from the context of PH can be easily extended to show that, for instance, QCPH' collapses to $\text{QC}\Sigma_2'$ when $\text{QC}\Sigma_2' = \text{QC}\Pi_2'$. On the other hand, the advantage of our definition of QCPH is that it generalizes a natural quantum complexity class like QCMA.

Let us also remark on Toda's theorem in the context of QCPH′ (for clarity, Toda's theorem is not studied in [25]). The recursive definition of QCPH′ allows one to obtain Toda's P^{PP} upper bound for QCPH′ with a simple argument:

$$\forall i,\ \mathrm{QC}\Sigma_i' = \mathrm{NP}^{\mathrm{NP}^{\cdot^{\cdot^{\cdot^{\mathrm{BQP}}}}}} = \Sigma_i^{\mathrm{BQP}} \quad \Longrightarrow \quad \forall i, \mathrm{QC}\Sigma_i' \subseteq (\mathrm{P}^{\mathrm{PP}})^{\mathrm{BQP}} = \mathrm{P}^{\mathrm{PP}},$$

where the first equality expressly holds due to the recursive definition of $\mathrm{QC}\Sigma_i'$ but is not known to hold for our $\mathrm{QC}\Sigma_i$; the implication arises by relativizing Toda's theorem; and the last equality holds as BQP is low for PP [13]. In contrast, our Theorem 2 yields $\mathrm{QCPH} \subseteq \mathrm{P}^{\mathrm{PP}^{\mathrm{PP}}}$, raising the question: is QCPH′ = QCPH? A positive answer may help shed light on whether $\exists \cdot \mathrm{BQP}$ equals QCMA; we leave this for future work.

Finally, a quantum version of the Karp-Lipton theorem was covered by Aaronson and Drucker in [3] and further improved by Aaronson, Cojocaru, Gheorghiu, and Kashefi [2], where the consequences of NP-complete problems being solved by small quantum circuits with polynomial sized quantum advice were considered. Their results differ from ours in that different hierarchies are studied, and in their use of quantum advice as opposed to our use of classical advice. Other Karp-Lipton style results for PH involving classes beyond NP show a collapse of PH to MA (usually) if either PP [26, 32], $\mathrm{P}^{\#\mathrm{P}}$ or PSPACE [21] has $\mathrm{P}_{/\mathrm{poly}}$ circuits.

1.3 Open questions

As the study of quantum generalizations of alternating quantifiers is in its infancy, many open questions exist. For example, due to the "$\exists \cdot \mathrm{BPP}$ versus MA phenomenon", we are not able to show "simple" collapse statements such as the following:

▶ **Conjecture 9.** *For $i \geq 1$, if $\mathrm{QC}\Sigma_i = \mathrm{QC}\Pi_i$ for any i, then QCPH collapses to the i^{th} level. Moreover, if QCMA = BQP, then QCPH = BQP.*

Next, can a non-trivial bound on QPH be shown? Here, we have shown that $\mathrm{Q}\Sigma_3 \subseteq \mathrm{NEXP}$; can the complexity of higher levels be bounded? Along these lines, our Theorem 4 shows $\mathrm{Q}\Sigma_2 \subseteq \mathrm{EXP}$; by applying alternative methods for approximating semidefinite programs arising in quantum complexity theory (see, e.g., [19]), we might also conjecture:

▶ **Conjecture 10.** $\mathrm{Q}\Sigma_2 \subseteq \mathrm{PSPACE}$.

Determining where in the complexity zoo QMA(2) lies remains an important open question; assuming alternating quantifiers *do* add proving power to QPH (the analogous assumption for PH is widely believed), our work shows QMA(2) is strictly contained in NEXP. Can this statement be strengthened?

Finally, we remark on defining a hierarchy similar to QCPH, termed MA-PH, where the first level is MA instead of QCMA and the verifier in equations (1) and (2) will be a BPP circuit. Due to the promise nature of the BPP verifier, we conjecture that the same issues faced with QCPH will translate to MA-PH too. Also, as Precise-BPP is equivalent to PP, we can obtain a similar Cleaning Lemma for MA-PH too. Hence, we conjecture that

▶ **Conjecture 11.** $\mathrm{PH} \subseteq \mathrm{MA\text{-}PH} \subseteq \mathrm{QCPH} \subseteq \mathrm{P}^{\mathrm{PP}^{\mathrm{PP}}}$.

Using other techniques that may harness the fact that BPP and MA are contained in PH to obtain a better bound for MA-PH is an interesting open question.

Organization. We begin in Section 2 by showing a quantum-classical analogue of Toda's theorem. Section 3 gives upper bounds on levels of QPH, and Section 4 shows a Karp-Lipton-type theorem. Formal definitions and many proofs are omitted from this version of the paper owing to space constraints.

2 A quantum-classical analogue of Toda's theorem

2.1 Precise-BQP

Our proof of a "quantum-classical Toda's theorem" requires us to define the Precise-BQP class, which we do now. Below, a promise problem is a pair $A = (A_{\text{yes}}, A_{\text{no}})$ such that $A_{\text{yes}}, A_{\text{no}} \subseteq \{0,1\}^*$, $A_{\text{yes}} \cup A_{\text{no}} \subset \{0,1\}^*$ and $A_{\text{yes}} \cap A_{\text{no}} = \emptyset$.

▶ **Definition 12** (Precise-BQP(c,s))**.** A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is contained in Precise-BQP(c,s) for polynomial-time computable functions $c, s : \mathbb{N} \mapsto [0,1]$ if there exists a polynomially bounded function $p : \mathbb{N} \mapsto \mathbb{N}$ such that $\forall \ell \in \mathbb{N},\ c(\ell) - s(\ell) \geq 2^{-p(\ell)}$ and a polynomial-time uniform family of quantum circuits $\{V_n\}_{n\in\mathbb{N}}$ whose input is the all zeroes state and output is a single qubit. Furthermore, for an n-bit input x:

- Completeness: If $x \in A_{\text{yes}}$, then V_n accepts with probability at least c.
- Soundness: If $x \in A_{\text{no}}$, then V_n accepts with probability at most s.

In contrast, BQP is defined such that the completeness and soundness parameters are 2/3 and 1/3, respectively (alternatively, the gap is least an inverse polynomial in n).

▶ **Observation 13** (Rational acceptance probabilities)**.** *By fixing an appropriate universal gate set (e.g. Hadamard and Toffoli [4]) for the description of V_n in Definition 12, we assume henceforth, without loss of generality, that the acceptance probability of V_n is a rational number that can be represented using at most* poly(n) *bits (this observation was used in the proof that* QCMA *has perfect completeness i.e., $c = 1$ [20].).*

The following help to characterize the complexity of Precise-BQP.

▶ **Lemma 14.** *For all $c, s \in [0,1]$ and every n-bit input such that $c - s \in \Omega(1/\exp(n))$,* Precise-BQP$(c,s) \subseteq$ PP.

▶ **Corollary 15.** *Let $\mathbb{P}$ denote the set of all polynomials $p : \mathbb{N} \mapsto \mathbb{N}$. Then,*

$$\bigcup_{p\in\mathbb{P}} \text{Precise-BQP}\left(\frac{1}{2} + \frac{1}{2^{p(n)}}, \frac{1}{2}\right) = \text{PP}.$$

2.2 Bounding the power of QCPH

Classically, PH can be defined in terms of the existential and universal operators; while it is not clear that one can also define QCPH using these operators, they nevertheless prove useful in bounding the power of QCPH.

▶ **Definition 16** (Existential and universal quantifiers [35, 7])**.** For $\mathcal{C}$ a class of languages, $\exists \cdot \mathcal{C}$ is defined as the set of languages L such that there is a polynomial p and set $A \in \mathcal{C}$ such that for input x, $x \in L \Leftrightarrow [\exists y\, (|y| \leq p(|x|))$ and $\langle x, y\rangle \in A]$. The set $\forall \cdot \mathcal{C}$ is defined similarly with $\exists$ replaced with $\forall$.

▶ **Remark 17** (Languages versus promise problems)**.** *Directly extending Definition 16 to promise problems, gives rise to subtle issues. To demonstrate, recall that $\exists \cdot \text{P} = \text{NP}$. Then,* *let* (L, A) *for* $L \in \exists \cdot \mathrm{P} = \mathrm{NP}$ *and* $A \in \mathrm{P}$ *be as in Definition 16, such that* T_A *is a polynomial-time Turing machine deciding* A*. If* $x \in L$*, there exists a bounded length witness* y^* *such that* T_A *accepts* $\langle x, y^* \rangle$ *and, for all* $y' \neq y^*$*,* T_A *by definition either accepts or rejects* $\langle x, y' \rangle$*. Now consider instead* $\exists \cdot \mathrm{BPP}$*, which* a priori *seems equal to Merlin-Arthur (*MA*). Applying the same definition of* $\exists$*, we should obtain a* BPP *machine* T_A *such that if* $x \in L$*, then for all* $y' \neq y^*$*,* T_A either accepts or rejects $\langle x, y' \rangle$*. But this means, by definition of* BPP*, that* $\langle x, y' \rangle$ *is either accepted or rejected with probability at least* $2/3$*, respectively. (Equivalently, for any fixed* y*, the machine* $T_{A,y}$ *must be a* BPP *machine, or more generally a machine with the resources available to class* $\mathcal{C}$*.) Unfortunately, the definition of* MA makes no such promise – *any* $y' \neq y^*$ *can be accepted with arbitrary probability when* x *is a* YES *instance. Indeed, whether* $\exists \cdot \mathrm{BPP} = \mathrm{MA}$ *remains an open question [11].*

The following lemma is the main contribution of this section. To set context, adapting the ideas from Toda's proof of $\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$ to QCPH is problematic for at least two reasons:

1. Remark 17 says that it is not necessarily true that by fixing a proof y to an MA (resp. QCMA) machine, the resulting machine is a BPP (resp. BQP) machine. This prevents the direct extension of recursive arguments, say from [30] to this regime.
2. The "Quantum Valiant Vazirani (QVV)" theorem for QCMA (and MA) [5] is not a many-one reduction, but a *Turing* reduction. Specifically, it produces a set of quantum circuits $\{ Q_i \}$, *at least one of which* is guaranteed to be a YES instance of some Unique-QCMA promise problem Γ if the input Π to the reduction was a YES instance. Unfortunately, some of the Q_i may violate the promise gap of Γ, which implies that when such Q_i are substituted into the Unique-QCMA oracle O, O returns an arbitrary answer. This does not pose a problem in [5], as one-sided error suffices for that reduction – so long as O accepts at least one Q_i, one safely concludes Π was a YES instance. In the setting of Toda's theorem, however, the use of *alternating* quantifiers turns this one-sided error into two-sided error; this renders the output of O useless, as one can no longer determine whether Π was a YES or NO instance.

To sidestep these issues, we adapt a high-level idea from [15]: With the help of an appropriate *oracle*, one can sometimes detect "invalid proofs" (i.e. proofs in promise gaps of bounded error verifiers) and "remove" them. Indeed, we show that using a PP oracle, one can eliminate the promise-gap of QCPH altogether, thus overcoming the limitations given above. This is accomplished by the following "Cleaning Lemma".

▶ **Lemma 18** (Cleaning Lemma). *For all* $i \geq 0$*,* $\mathrm{QC}\Sigma_i \subseteq \exists \cdot \forall \cdot \cdots \cdot Q_i \cdot \mathrm{P}^{\text{Precise-BQP}} \subseteq \exists \cdot \forall \cdot \cdots \cdot Q_i \cdot \mathrm{P}^{\mathrm{PP}}$*, where* $Q_i = \exists$ *(*$Q_i = \forall$*) if* i *is odd (even). An analogous statement holds for* $\mathrm{QC}\Pi_i$*.*

Proof. Let C be a $\mathrm{QC}\Sigma_i$ verification circuit for a promise problem Π. Let $C_{y_1^*,\ldots,y_i^*}$ denote the quantum circuit obtained from C by fixing values $y_1^*, \ldots, y_i^*$ of the i classical proofs. In general, nothing can be said about the acceptance probability $p_{y_1^*,\ldots,y_i^*}$ of $C_{y_1^*,\ldots,y_i^*}$, except that, by Observation 13, $p_{y_1^*,\ldots,y_i^*}$ is a rational number representable using $p(n)$ bits for some fixed polynomial p. Let S denote the set of all rational numbers in $[0, 1]$ representable using $p(n)$ bits of precision. (Note $|S| \in \Theta(2^{p(n)})$.) Then, for any $a, b \in S$ with $a > b$, the triple $(C_{y_1^*,\ldots,y_i^*}, a, b)$ is a valid $\mathrm{QCIRCUIT}(a, b)$ instance, i.e. $C_{y_1^*,\ldots,y_i^*}$ accepts with probability at least a or at most b for $a - b$ an inverse exponential. It follows that using binary search (by varying the values $a, b \in S$ with $a > b$) in conjunction with $\mathrm{poly}(n)$ calls to a $\mathrm{QCIRCUIT}(a, b)$ oracle, we may exactly and deterministically compute $p_{y_1^*,\ldots,y_i^*}$. Moreover, since for all such $a > b$, $\mathrm{QCIRCUIT}(a, b) \in \text{Precise-BQP}(a, b)$, Lemma 14 implies a $\mathrm{QCIRCUIT}(a, b)$ oracle call can be simulated with a PP oracle. Denote the binary search subroutine using the PP oracle as B.

Using C and B, we now construct an oracle Turing machine C' as follows. Given any proofs $y_1^*,\ldots,y_i^*$ as input, C' uses B to compute $p_{y_1^*,\ldots,y_i^*}$ for $C_{y_1^*,\ldots,y_i^*}$. If $p_{y_1^*,\ldots,y_i^*} \geq c$, C' accepts with certainty, and if $p_{y_1^*,\ldots,y_i^*} < c$, C' rejects with certainty. Suppose that the circuits C and C' return 1 when they accept and 0 when they reject. Two observations: (1) Since by construction, for any fixed $y_1^*,\ldots,y_i^*$, B makes only makes "valid" QCIRCUIT(a,b) queries (i.e. satisfying the promise of QCIRCUIT(a,b)), C' is a P^{PP} machine (cf. Observation 20). (2) Since $C'_{y_1^*,\ldots,y_i^*}$ accepts if $C_{y_1^*,\ldots,y_i^*}$ accepts with probability at least c, and since $C'_{y_1^*,\ldots,y_i^*}$ rejects if $C_{y_1^*,\ldots,y_i^*}$ accepts with probability at most s, we conclude that

$$\exists y_1 \forall y_2 \cdots Q_i y_i \,\mathrm{Prob}[C(y_1,\ldots,y_i)=1] \geq c \quad \Leftrightarrow \quad \exists y_1 \forall y_2 \cdots Q_i y_i \; C'(y_1,\ldots,y_i)=1 \tag{4}$$

$$\forall y_1 \exists y_2 \cdots \overline{Q}_i y_i \,\mathrm{Prob}[C(y_1,\ldots,y_i)=1] \leq s \quad \Leftrightarrow \quad \forall y_1 \exists y_2 \cdots \overline{Q}_i y_i \; C'(y_1,\ldots,y_i)=0. \tag{5}$$

(4) and (5) imply that we can simulate Π with a $\exists \cdot \forall \cdot \cdots \cdot Q_i \cdot \mathrm{P}^{\mathrm{PP}}$ computation. The proof for $\mathrm{QC}\Pi_i$ is analogous. ◀

▶ **Remark 19** (Possibility of a stronger containment). *A key question is whether one may replace the* Precise-BQP *oracle in the proof of Lemma 18 with a weaker* BQP *oracle. For example, consider the following alternate definition for oracle Turing machine C': Given proofs $y_1^*,\ldots,y_i^*$, C' plugs $C_{y_1^*,\ldots,y_i^*}$ into a BQP oracle and returns the oracle's answers. It is easy to see that in this case, Equations (4) and (5) hold. However, C' is* not *necessarily a $\mathrm{P}^{\mathrm{BQP}}$ machine, since for some settings of $y_1^*,\ldots,y_i^*$, its input to the* BQP *oracle may violate the BQP promise, hence making the output of C' ill-defined. To further illustrate this subtle point, consider Observation 20. Moreover, in Section 2.3 we show that the task the* Precise-BQP *oracle is used for in Lemma 18 is in fact PP-complete; thus, it is highly unlikely that one can substitute a weaker oracle into the proof above.*

▶ **Observation 20** (When a P machine querying a BQP oracle is not a $\mathrm{P}^{\mathrm{BQP}}$ machine). *The proof of the Cleaning Lemma uses a $\mathrm{P}^{\text{Precise-BQP}}$ machine. Let us highlight a subtle reason why using a weaker* BQP *oracle instead might be difficult (indeed, in Section 2.3 we show that the task we use the* Precise-BQP *oracle for is* PP*-complete). Let M denote the trivially* BQP*-complete problem of determining whether a given polynomial-sized quantum circuit Q accepts with probability at least $2/3$, or accepts with probability at most $1/3$, with the promise that one of the two is the case. Now consider the following polynomial time computation, Π, which is given access to an oracle O_M for M: Π inputs the Hadamard gate H into O_M and outputs O_M's answer. Does it hold that $\Pi \in \mathrm{P}^{\mathrm{BQP}}$? No. Since H violates the promise of BQP, i.e. measuring the output of H yields 0 or 1 with equal probability, the oracle O_M can answer 0 or 1 arbitrarily, and so the output of Π is not well-defined. Having a well-defined output, however, is required for a P^{O_K} computation, where K is any promise class [16].*

▶ **Lemma 21.** *For all $i \geq 0$, the following holds true: $\exists \cdot \forall \cdot \cdots \cdot Q_i \cdot \mathrm{P}^{\mathrm{PP}} \subseteq \Sigma_i^{\mathrm{PP}}$ and $\forall \cdot \exists \cdot \cdots \cdot Q_i \cdot \mathrm{P}^{\mathrm{PP}} \subseteq \Pi_i^{\mathrm{PP}}$ where $Q_i = \exists$ (resp. $Q_i = \forall$) when i is odd (resp. even) in the first containment and vica-versa for the second containment.*

We can now show the main theorem of this section.

▶ **Theorem 22.** $\mathrm{QCPH} \subseteq \mathrm{P}^{\mathrm{PP}^{\mathrm{PP}}}$.

Proof. The claim follows by combining the Cleaning Lemma (Lemma 18), Lemma 21, and Toda's theorem ($\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$), whose proof relativizes (see, e.g., page 4 of [12])). ◀

2.3 Detecting non-empty promise gaps is PP-complete

The technique behind the Cleaning Lemma (Lemma 18) can essentially be viewed as using a PP oracle to determine whether a given quantum circuit accepts some input with probability within the promise gap (s, c), where $c - s$ is an inverse polynomial. One can ask whether this rather powerful PP oracle can be replaced with a weaker oracle (see Remark 19)? We answer this in the negative unless one deviates from our specific proof approach; specifically, we show that the problem of detecting non-empty promise gaps is PP-complete, even if the gap is *constant* in size.

To begin, we define QCIRCUIT(c, s), which is trivially Precise-BQP(c, s)-complete when $c - s$ is an inverse exponential. (Take note that when the $c - s$ gap is larger, say inverse polynomial, QCIRCUIT(c, s) is still contained in Precise-BQP(c, s).)

▶ **Definition 23** (QCIRCUIT(c, s))**.** Parameters $c, s : \mathbb{N} \mapsto [0, 1]$ are polynomial-time computable functions such that $c > s$.

- (Input) A classical description of quantum circuit V_n (acting on n qubits, consisting of poly(n) 1 and 2-qubit gates), taking in the all-zeroes state, and outputting a single qubit.
- (Output) Decide if $\Pr[V_n \text{ accepts }] \geq c$ or $\leq s$, assuming one of the two is the case.

▶ **Definition 24** (NON-EMPTY GAP(c, s))**.** Let V_n be an input for QCIRCUIT(c, s). Then, output YES if $\text{Prob}[V_n \text{ accepts }] \in (s, c)$, and NO otherwise.

We now show that NON-EMPTY GAP is PP-complete.

▶ **Lemma 25.** *For all c, s with the $c - s$ gap at least an inverse exponential in input size,* NON-EMPTY GAP$(c, s) \in$ PP*.*

▶ **Lemma 26.** *There exist $c, s \in \Theta(1)$ such that* NON-EMPTY GAP(c, s) *is* PP*-hard.*

▶ **Theorem 27.** *There exist $c, s \in \Theta(1)$ such that* NON-EMPTY GAP(c, s) *is* PP*-complete.*

3 Bounding the power of $Q\Sigma_2$ and $Q\Sigma_3$

Let $Q\Sigma_2(c, s)$ (resp., $Q\Pi_2(c, s)$) be defined as $Q\Sigma_2$ (resp., $Q\Pi_2$) with completeness and soundness parameters c and s, respectively. We begin by restating Theorem 4 as follows.

▶ **Theorem 28.** *For any polynomial r, if $c - s \geq 1/2^{2^{r(n)}}$, then $Q\Sigma_2(c, s) \subseteq$ EXP and $Q\Pi_2(c, s) \subseteq$ EXP when c and s are computable in exponential time in the size of the input.*

The two containments in Theorem 28 are proven separately in the following two lemmas.

▶ **Lemma 29.** *Let α be the maximum acceptance probability of a $Q\Sigma_2$ protocol (where the optimization is over the first proof ρ_1). Then one can compute γ such that $|\gamma - \alpha| \leq 1/2^{2^r}$, for any polynomial r, in exponential time.*

▶ **Lemma 30.** *Let α be the* minimum *acceptance probability of a $Q\Pi_2$ protocol (where the optimization is again over the first proof ρ_1). Then one can compute γ such that $|\gamma - \alpha| \leq 1/2^{2^r}$, for any polynomial r, in exponential time.*

We now sketch the exponential time protocol that calculates γ in Lemma 29 (we refer the reader to [17] for standard background in convex optimization). The proof of Lemma 30 is similar.

Proof Sketch. Recall from (3) that the maximum acceptance probability of a $\mathrm{QC}\Sigma_2$ protocol can be expressed as $\alpha := \max_{\rho_1}\min_{\rho_2}\langle C, \rho_1 \otimes \rho_2\rangle$, where C is the POVM that corresponds to the quantum verification circuit in the $\mathrm{Q}\Sigma_2$ protocol accepting. We wish to decide in exponential time whether $\alpha \geq c$ or $\alpha \leq s$. Since the promise gap satisfies $c - s \geq 1/2^{2^{r(n)}}$, it suffices to approximate α within additive error (say) $\frac{1}{4}(c-s)$ by computing $\gamma \in \mathbb{R}$, in exponential time, such that $|\gamma - \alpha| \leq 1/(4 \cdot 2^{2^{r(n)}})$.

We begin by constructing C' as a numerical approximation to C such that each entry in C' is correct up to exponentially many bits. This can be done independent of the gate set used to describe the verification circuit, V_n, used for the $\mathrm{Q}\Sigma_2$ instance[6]. Then, for some polynomial r, $|\alpha - \alpha'| \leq \frac{1}{2} \cdot 2^{-2^{r(n)/2}}$ for

$$\alpha' := \max_{\rho_1}\ \min_{\rho_2}\ \{\langle C', \rho_1 \otimes \rho_2\rangle : \mathrm{Tr}(\rho_1) = \mathrm{Tr}(\rho_2) = 1,\ \rho_1, \rho_2 \succeq 0\}. \tag{6}$$

Suppose we fix a feasible ρ_1 and solve the inner optimization problem in (6). Then:

$$\alpha'(\rho_1) := \min_{\rho_2}\ \{\langle C', \rho_1 \otimes \rho_2\rangle : \mathrm{Tr}(\rho_2) = 1,\ \rho_2 \succeq 0\}.$$

We can rewrite $\langle C', \rho_1 \otimes \rho_2\rangle$ as $\langle \mathrm{Tr}_1[(\rho_1 \otimes I)C'], \rho_2\rangle$ where Tr_1 is the partial trace over the register that ρ_1 acts on. Additionally, as $\mathrm{Tr}_1[(\rho_1 \otimes I)C'] = \mathrm{Tr}_1[(\rho_1^{1/2} \otimes I)C(\rho_1^{1/2} \otimes I)]$, this term is Hermitian and positive semidefinite. This implies that the best choice for ρ_2 is a rank-1 projector onto the eigenspace corresponding to least eigenvalue. In other words, $\alpha'(\rho_1) = \lambda_{\min}(\mathrm{Tr}_1[(\rho_1 \otimes I)C'])$ where $\lambda_{\min}(X)$ denotes the least eigenvalue of a Hermitian operator X. For fixed ρ_1, this minimum eigenvalue calculation can be rephrased via the dual optimization program for $\alpha'(\rho_1)$,

$$\alpha'(\rho_1) = \max_{t}\ \{t : tI \preceq \mathrm{Tr}_1[(\rho_1 \otimes I)C']\}.$$

Re-introducing the maximization over ρ_1, we hence obtain

$$\alpha' = \max_{\rho_1, t}\ \{t : tI \preceq \mathrm{Tr}_1[(\rho_1 \otimes I)C'],\ \mathrm{Tr}(\rho_1) = 1,\ \rho_1 \succeq 0\}, \tag{7}$$

which is a semidefinite program. By using the ellpsoid method, we can hence solve this semidefinite program (see [17] for details) to obtain estimate γ of α'. Using an analysis similar to [34], we find a γ such that $|\gamma - \alpha'| \leq \epsilon$ with $\epsilon = 2^{-2^{r(n)}}$. ◀

Using the power of non-determinism, we can also bound the power of $\mathrm{Q}\Sigma_3$ and $\mathrm{Q}\Pi_3$.

▶ **Theorem 31.** *For any polynomial r and input size n, if $c - s \geq 1/r(n)$, then*

$$\mathrm{QMA}(2) \subseteq \mathrm{Q}\Sigma_3 \subseteq \mathrm{NEXP} \quad \textit{and} \quad \text{co-QMA}(2) \subseteq \mathrm{Q}\Pi_3 \subseteq \text{co-NEXP}, \tag{8}$$

where all classes have completeness and soundness c and s, respectively. Moreover, if we allow smaller gaps (in principle, gaps which are at most inverse singly exponential in n suffice for the first claim below), such as $c - s \geq 1/2^{2^{r(n)}}$, then

$$\mathrm{QMA}(2)(c,s) = \mathrm{Q}\Sigma_3(c,s) = \mathrm{NEXP} \quad \textit{and} \quad \text{co-QMA}(2)(c,s) = \mathrm{Q}\Pi_3(c,s) = \text{co-NEXP}. \tag{9}$$

Here, we assume c and s are computable in exponential time in the size of the input.

---

[6] This can be accomplished in exponential time as follows: Replace gate set G with G' by approximating each entry of each gate in G using $2^{s(n)}$ bits of precision, for some sufficiently large, fixed polynomial s. Define C' as C, except each use of a gate $U \in G$ is replaced with its approximation $U' \in G'$. Then, via the well-known bound $\|U_m \cdots U_1 - V_m \cdots V_1\|_\infty \leq \sum_{i=1}^m \|U_i - V_i\|_\infty$ (for unitary U_i, V_i), it follows that $\left\|C' - C\right\|_\infty \in O(\mathrm{poly}(n)/(2^{2^{s(n)}}))$, since V_n contains $\mathrm{poly}(n)$ gates. Here, $\|A\|_\infty = \max_{|\psi\rangle} \|A\,|\psi\rangle\|_2$ for unit vectors $|\psi\rangle$ denotes the spectral or operator norm. Finally, apply the fact that $\max_{i,j}|A(i,j)| \leq \|A\|_\infty$ (p. 314 of [18]).

4 Karp-Lipton type theorems

The Karp-Lipton [21] theorem showed that if $\mathrm{NP} \subseteq \mathrm{P}_{/\mathrm{poly}}$ (i.e. if NP can be solved by polynomial-size non-uniform circuits), then $\Sigma_2 = \Pi_2$ (which in turn collapses PH collapses to its second level). Then, building on the conjecture that the polynomial hierarchy is infinite, this result implies that $\mathrm{NP} \not\subseteq \mathrm{P}_{/\mathrm{poly}}$ (a stronger claim than $\mathrm{P} \neq \mathrm{NP}$ as $\mathrm{P} \subseteq \mathrm{P}_{/\mathrm{poly}}$). Some attempts to separate NP from P use this as a basis to try and prove the stronger claim instead. For instance, this has lead to the approach of proving super-polynomial circuit lower bounds for circuits of NP-complete problems. Here, we show that the proof technique of Karp and Lipton carries over easily to the quantum setting, *provided* one uses the stronger hypothesis Precise-QCMA $\subseteq \mathrm{BQP}_{/\mathrm{mpoly}}$ (as opposed to QCMA $\subseteq \mathrm{BQP}_{/\mathrm{mpoly}}$). Whether this causes QCPH to collapse to its second level, however, remains open (see Remark 37 below). We begin by formally defining the classes $\mathrm{BQP}_{/\mathrm{mpoly}}$ and Precise-QCMA.

▶ **Definition 32** ($\mathrm{BQP}_{/\mathrm{mpoly}}$)**.** A promise problem $\Pi = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ is in $\mathrm{BQP}_{/\mathrm{mpoly}}$ if there exists a polynomial-sized family of quantum circuits $\{C_n\}_{n\in\mathbb{N}}$ and a collection of binary advice strings $\{a_n\}_{n\in\mathbb{N}}$ with $|a_n| = \mathrm{poly}(n)$, such that for all n and all strings x where $|x| = n$, $\Pr[C_n(|x\rangle, |a_n\rangle) = 1] \geq 2/3$ if $x \in A_{\mathrm{yes}}$ and $\Pr[C_n(|x\rangle, |a_n\rangle) = 1] \leq 1/3$ if $x \in A_{\mathrm{no}}$.

Equivalently, $\mathrm{BQP}_{/\mathrm{mpoly}}$ is the set of promise problems solvable by a *non-uniform* family of polynomial-sized bounded error quantum circuits. It is used as a quantum analogue for $\mathrm{P}_{/\mathrm{poly}}$ in this scenario. Here, we remark on the use of mpoly instead of poly in Definition 32. Note that $\mathrm{BQP}_{/\mathrm{poly}}$ accepts Karp-Lipton style advice i.e. it is a BQP circuit that accepts a poly-sized advice string to provide *some answer* with probability at least 2/3 even if the "advice is bad". On the other hand, $\mathrm{BQP}_{/\mathrm{mpoly}}$ accepts Merlin style advice i.e. it is a BQP circuit accepting poly-sized classical advice such that the output is correct with probability at least 2/3 if the "advice is good". Note $\mathrm{BQP}_{/\mathrm{poly}}$ versus $\mathrm{BQP}_{/\mathrm{mpoly}}$ is analogous to the "$\exists \cdot$BPP versus MA" phenomenon. Moreover, as we are concerned with variations of QCMA, and not $\exists \cdot$BQP, $\mathrm{BQP}_{/\mathrm{mpoly}}$ is the right candidate for us.

▶ **Definition 33** (Precise-QCMA)**.** A promise problem $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ is said to be in Precise-QCMA(c, s) for polynomial-time computable functions $c, s : \mathbb{N} \mapsto [0, 1]$ if there exists polynomially bounded functions $p, q : \mathbb{N} \mapsto \mathbb{N}$ such that $\forall \ell \in \mathbb{N}$, $c(\ell) - s(\ell) \geq 2^{-q(\ell)}$, and there exists a polynomial-time uniform family of quantum circuits $\{V_n\}_{n\in\mathbb{N}}$ that takes a classical proof $y \in \{0, 1\}^{p(n)}$ and outputs a single qubit. Moreover, for an n-bit input x:

- Completeness: If $x \in A_{\mathrm{yes}}$, then $\exists\, y$ such that V_n accepts y with probability at least c.
- Soundness: If $x \in A_{\mathrm{no}}$, then $\forall\, y$, V_x accepts y with probability at most s.

Define Precise-QCMA $= \bigcup_{c,s}$ Precise-QCMA(c, s).

As an aside, note that QCMA is defined with $c - s \in \Omega(1/\mathrm{poly}(n))$. Recall from the discussion in Section 1.1 that the main obstacle to the recursive arguments that work well for NP in [21] is the "promise problem" nature of $\mathrm{QC}\Pi_2$ and QCMA. However, exploiting the perfect completeness of Precise-QCMA[7] and the fact that $\forall c < s' \leq s$, Precise-QCMA$(c, s) \subseteq$ Precise-QCMA(c, s'), we "recover" the notion of a decision problem in a rigorous sense by working with Precise-QCMA as demonstrated below.

[7] The perfect completeness proof for QCMA also works in the inverse exponentially small gap setting [20].

▶ **Claim 34.** *For every promise problem* $\Pi' = (A_{\text{yes}}, A_{\text{no}}) \in \text{Precise-QCMA}(c, s)$ *with verifier* V'*, there exists a verifier* V *(a poly-time uniform quantum circuit family), a polynomial* q *and a decision problem* $\Pi = (A_{\text{yes}}, \{0,1\}^* \setminus A_{\text{yes}})$ *such that* $\Pi \in \text{Precise-QCMA}(1, 1 - 2^{-q(n)})$ *with verifier* V*. Moreover, for all proofs* y*,* V *accepts* y *with probability either* 1 *or at most* $1 - 2^{-q(n)}$*.*

Building on this "decision problem" flavour of Precise-QCMA, we first show:

▶ **Lemma 35.** *Suppose* $\text{Precise-QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$*. Then, for every promise problem* $\Pi = (A_{\text{yes}}, A_{\text{no}})$ *in* Precise-QCMA *and every* n*-bit input* x*, there exists a polynomially bounded function* $p : \mathbb{N} \mapsto \mathbb{N}$ *and a bounded error polynomial time non-uniform quantum circuit family* $\{C_n\}_{n \in \mathbb{N}}$ *such that:*

- *if* $x \in A_{\text{yes}}$*, then* C_n *outputs valid proof* $y \in \{0,1\}^{p(n)}$ *such that* (x, y) *is accepted by the corresponding* Precise-QCMA *verifier with probability* 1*;*
- *if* $x \in A_{\text{no}}$*, then* C_n *outputs a symbol* $\perp$ *with probability exponentially close to* 1 *signifying that there is no* $y \in \{0,1\}^{p(n)}$*, such that* (x, y) *is accepted by the corresponding* Precise-QCMA *verifier with probability* 1*.*

We next give a quantum-classical analogue of the Karp-Lipton theorem, whose proof is in the appendix.

▶ **Theorem 36** (A Quantum-Classical Karp-Lipton Theorem)**.** *If* $\text{Precise-QCMA} \subseteq \text{BQP}_{/\text{mpoly}}$ *then* $\text{QC}\Pi_2 = \text{QC}\Sigma_2$*.*

▶ **Remark 37** (Collapse of QCPH?)**.** *An appeal of the classical Karp-Lipton theorem is that it implies that if* $\text{NP} \subseteq \text{P}_{/\text{poly}}$*, then PH collapses to its second level; this is because if* $\Pi_2^p = \Sigma_2^p$*, then* PH *collapses to* Σ_2^p*. Does an analogous statement hold for* QCPH *as a result of Theorem 8? Unfortunately, the answer is not clear. The problem is similar to that outlined in Remark 17. Namely, classically* $\Pi_2^p = \Sigma_2^p$ *collapses* PH *since for any* Π_3^p *decision problem, fixing the first (universally) quantified proof yields a* Σ_2^p *computation. But this can be replaced with a* Π_2^p *computation by assumption, yielding a computation with quantifiers* $\forall\forall\exists$*, which trivially collapses to* $\forall\exists$*, i.e.* $\Pi_3^p \subseteq \Pi_2^p$*. In contrast, for (say)* $\text{QC}\Pi_3$*, similar to the phenomenon in Remark 17, fixing the first (universally) quantified proof does* not *necessarily yield a* $\text{QC}\Sigma_2^p$ *computation. Thus, a recursive application of the assumption* $\text{QC}\Sigma_2^p = \text{QC}\Pi_2^p$ *cannot straightforwardly be applied.*

Since Precise-QCMA plays an important role in Theorem 8, we close with an upper bound on Precise-QCMA.

▶ **Lemma 38.** $\text{Precise-QCMA} \subseteq \text{NP}^{\text{PP}}$.

Proof. Let V be a Precise-QCMA verifier. Using Claim 34, we may assume that for any proof y, V either accepts y with probability 1 or rejects with probability at most $1 - 2^{-q(n)}$. Thus, for any fixed y, the resulting computation V_y is a Precise-BQP computation. This implies $\text{Precise-QCMA} \subseteq \exists \cdot \text{Precise-BQP}$ (see also Remark 17). But by Definition 16, $\exists \cdot \text{Precise-BQP} \subseteq \text{NP}^{\text{Precise-BQP}}$. Combining this with Lemma 14, which says that $\text{Precise-BQP} \subseteq \text{PP}$, yields the claim. ◀

References

1 S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor. The power of unentanglement. *Theory of Computing*, 5:1–42, 2009. `doi:10.4086/toc.2009.v005a001`.

2 S. Aaronson, A. Cojocaru, A. Gheorghiu, and E. Kashefi. On the implausibility of classical client blind quantum computing. Available at arXiv.org e-Print quant-ph/1704.08482, 2017.

3 S. Aaronson and A. Drucker. A full characterization of quantum advice. *SIAM Journal on Computing*, 43(3):1131–1183, 2014.

4 D. Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. Available at arXiv.org e-Print quant-ph/0301040, jan 2003. `arXiv:quant-ph/0301040`.

5 D. Aharonov, M. Ben-Or, F. Brandão, and O. Sattath. The pursuit for uniqueness: Extending Valiant-Vazirani theorem to the probabilistic and quantum settings. Available at arXiv.org e-Print quant-ph/0810.4840v1, 2008.

6 D. Aharonov and T. Naveh. Quantum NP - A survey. Available at arXiv.org e-Print quant-ph/0210077v1, 2002.

7 E. W. Allender and K. W. Wagner. *Counting hierarchies: Polynomial time and constant depth circuits*, pages 469–483. World Scientific, 1993. `doi:10.1142/9789812794499_0035`.

8 A. Ambainis. On physical problems that are slightly more difficult than QMA. In *Proceedings of 29th IEEE Conference on Computational Complexity (CCC 2014)*, pages 32–43, 2014.

9 S. Beigi. NP vs $\mathrm{QMA}_{\log}(2)$. *Quantum Information and Computation*, 10:0141–0151, 2010.

10 H. Blier and A. Tapp. All languages in NP have very short quantum proofs. In *Proceedings of the 3rd International Conference on Quantum, Nano and Micro Technologies*, pages 34–37, 2009.

11 S. Fenner, L. Fortnow, S. A. Kurtz, and L. Li. An oracle builder's toolkit. *Information and Computation*, 182(2):95–136, 2003. `doi:10.1016/S0890-5401(03)00018-X`.

12 L. Fortnow. The role of relativization in complexity theory. *Bulletin of the European Association for Theoretical Computer Science*, 52:52–229, 1994.

13 L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999.

14 S. Gharibian and J. Kempe. Hardness of approximation for quantum problems. In *Proceedings of 39th International Colloquium on Automata, Languages and Programming (ICALP 2012)*, pages 387–398, 2012.

15 S. Gharibian and J. Yirka. The complexity of simulating local measurements on quantum systems. In Mark M. Wilde, editor, *12th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2017)*, volume 73 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:17, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. `doi:10.4230/LIPIcs.TQC.2017.2`.

16 O. Goldreich. On promise problems: A survey. *Theoretical Computer Science*, 3895:254–290, 2006.

17 M. Grötschel, L. Lovász, and A. Schrijver. *Geometric Algorithms and Combinatorial Optimization*. Springer-Verlag, 1993.

18 R. A. Horn and C. H. Johnson. *Matrix Analysis*. Cambridge University Press, 1990.

19 R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. QIP = PSPACE. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing*, pages 573–581, 2010.

20 S. P. Jordan, H. Kobayashi, D. Nagaj, and H. Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information & Computation*, 12(5 & 6):461–471, 2012.

21 R. M. Karp and R. J. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proceedings of the Twelfth Annual ACM Symposium on Theory of Computing*, STOC '80, pages 302–309, New York, NY, USA, 1980. ACM. `doi:10.1145/800141.804678`.

22 A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.

23 A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the 32nd ACM Symposium on Theory of Computing (STOC 2000)*, pages 608–617, 2000.

24 Y.-K. Liu, M. Christandl, and F. Verstraete. Quantum computational complexity of the N-representability problem: QMA complete. *Physical Review Letters*, 98:110503, 2007.

25 J. Lockhart and C. E. González-Guillén. Quantum state isomorphism. *arXiv preprint arXiv:1709.09622*, 2017.

26 C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992. `doi:10.1145/146585.146605`.

27 C. Marriott and J. Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

28 A. Meyer and L. Stockmeyer. The equivalence problem for regular expressions with squaring requires exponential time. In *Proceedings of the 13th Symposium on Foundations of Computer Science*, pages 125–129, 1972.

29 A. Pereszlényi. Multi-prover quantum Merlin-Arthur proof systems with small gap. Available at arXiv.org e-Print quant-ph/1205.2761, 2012.

30 S. Toda. PP is as hard as the Polynomial-Time Hierarchy. *SIAM Journal on Computing*, 20:865–877, 1991.

31 L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47:85–93, 1986.

32 N. V. Vinodchandran. A note on the circuit complexity of pp. *TCS*, 347(1-2):415–418, 2005. `doi:10.1016/j.tcs.2005.07.032`.

33 M. Vyalyi. QMA=PP implies that PP contains PH. *Electronic Colloquium on Computational Complexity*, 2003.

34 J. Watrous. Semidefinite programs for completely bounded norms. *Theory of Computing*, 5:217–238, 2009.

35 C. Wrathall. Complete sets and the Polynomial-Time Hierarchy. *Theoretical Computer Science*, 3(1):23–33, 1976. `doi:10.1016/0304-3975(76)90062-1`.

36 T. Yamakami. Quantum NP and a quantum hierarchy. In *Proceedings of the 2nd IFIP International Conference on Theoretical Computer Science*, pages 323–336. Kluwer Academic Publishers, 2002.