Electronic Colloquium on Computational Complexity, Report No. 137 (2025)

Limits to black-box amplification in QMA

Scott Aaronson[1] and Freek Witteveen[2]

[1]University of Texas at Austin. Supported by the Simons Foundation
[2]QuSoft & CWI, Amsterdam

Abstract

We study the limitations of black-box amplification in the quantum complexity class QMA. Amplification is known to boost any inverse-polynomial gap between completeness and soundness to exponentially small error, and a recent result (Jeffery and Witteveen, 2025) shows that completeness can in fact be amplified to be doubly exponentially close to 1. We prove that this is optimal for black-box procedures: we provide a quantum oracle relative to which no QMA verification procedure using polynomial resources can achieve completeness closer to 1 than doubly exponential, or a soundness which is super-exponentially small. This is proven by making the oracle separation from (Aaronson, 2008) between QMA and QMA_1 quantitative, using techniques from complex approximation theory.

1 Introduction

The complexity class QMA (Quantum Merlin–Arthur) is a quantum analogue of NP, where given a problem instance, a prover Merlin sends a quantum witness to a polynomial-time quantum verifier Arthur, in order to convince Arthur whether the problem is a yes-instance or a no-instance. Arthur then performs a polynomial-size quantum computation on the witness, after which he accepts or rejects the witness. Quantum complexity classes typically allow some probability of error. There are two parameters quantifying the allowed error: the *completeness* c, the probability with which Arthur accepts a valid witness in the yes-case, and the *soundness* s, the maximum acceptance probability in the no-case. It is well known that the precise choice of these parameters does not matter as long as there is a non-negligible gap: by amplification techniques [KSV02, MW05], one can boost a polynomially small gap $c - s = 1/\operatorname{poly}$ to completeness $c = 1 - 2^{-\operatorname{poly}}$ and soundness $s = 2^{-\operatorname{poly}}$ exponentially close to 1 and 0 respectively. This motivates the canonical definition, which takes $c = \frac{2}{3}$ and $s = \frac{1}{3}$.

A long-standing open question is whether the completeness can in fact be made *perfect.* We denote by QMA_1 the variant of QMA where we take $c = 1$ (and $s = \frac{1}{3}$, or any other constant). The question whether QMA equals QMA_1 is then: can every QMA protocol be modified so that Arthur always accepts a valid witness in the yes-case, while still rejecting no-instances with bounded probability? There are a number of closely related complexity classes which allow for perfect completeness. This is the case for the variant with only classical randomness MA, the variant with a classical proof and quantum verifier QCMA [JKNN12], the variant with multiple rounds QIP [MW05], and the variant with an exponentially small soundness-completeness gap PreciseQMA [FL18].

For QMA, this question has resisted resolution, and one explanation for this is given by Aaronson [Aar09], who gave a barrier to proving $\mathsf{QMA} = \mathsf{QMA}_1$ using black-box techniques. Here 'black-box' refers to an amplification procedure that does not use any properties of the verification circuit, other than those that define it. Concretely, [Aar09] proved that there exists a quantum oracle relative to which $\mathsf{QMA} \neq \mathsf{QMA}_1$. Any proof showing $\mathsf{QMA} \neq \mathsf{QMA}_1$ would have to break down in the presence of a quantum oracle, i.e. it would have to be quantumly nonrelativizing.

ISSN 1433-8092

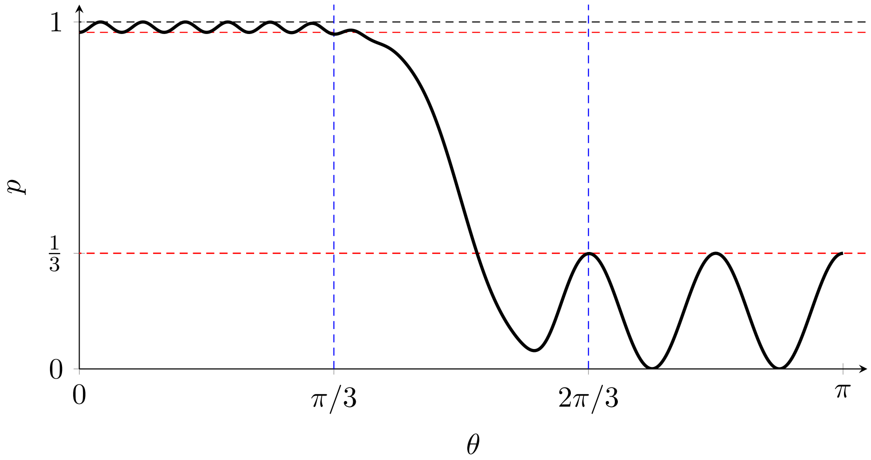

Figure 1: The verifier would like to decide whether $\theta \le \pi/3$ (a yes-instance) or $\theta \ge 2\pi/3$ (a no-instance), given black-box access to the oracle defined in Eq. (1). Here we give a sketch of what the maximal acceptance probability, optimized over all choices of witness, should look like, when we have completeness $c = 1 - \delta$ close to 1, and soundness $s = 1/3$.

All known amplification techniques for QMA are of a black-box nature (so they are quantumly relativizing).

Recently, it was shown in Ref [JW25] that one can reach completeness *doubly exponentially* close to 1

$$c = 1 - 2^{-2^{\text{poly}}},$$

in QMA, improving over the previous best completeness which was exponentially close to 1. The techniques in [JW25] are of a black-box nature. This raises the question: can one get even closer to perfect completeness with black-box amplification procedures?

In this work we show that the doubly-exponential bound is in fact *optimal* in the black-box setting. We prove that there exists a quantum oracle relative to which no QMA protocol using polynomial resources can achieve completeness closer to 1 than doubly exponential.

The key idea in the oracle separation of [Aar09] is that for a simple choice of quantum oracle, the maximal acceptance probability of the verifier is an analytic function in one variable. Perfect completeness would require this function to be constant on an interval, but the analyticity then implies that the maximal acceptance probability is *always* 1, contradicting soundness. We use the same quantum oracle, but give a slightly different analysis and use a result from complex approximation theory, bounding the growth of rational functions, to make this separation quantitative. The key idea of the proof is as follows. The quantum oracle is given by

$$U(z) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \tag{1}$$

for $z = e^{i\theta}$. We then consider the problem where Arthur has to decide whether $z \in E$ (yes-instance) or $z \in F$ (no-instance) for two disjoint arcs of the unit circle, with black-box access to $U(z)$.

Suppose we are given some verifier for this task.

The idea is to consider the accepting measurement operator $P(z)$. The maximal acceptance probability $p(z)$, over all possible witnesses, equals the largest eigenvalue of $P(z)$. If the verifier has completeness close to 1, and soundess $\frac{1}{3}$, the maximal acceptance probability, as a function of the angle θ, must look something like shown in Fig. 1. We now study the following function:[1]

$$r(z) = \operatorname{tr}[(I - P(z))^{-1}]. \tag{2}$$

[1] The idea to use rational function of z in Eq. (2), and apply a bound on the growth of rational functions was suggested to us by GPT-5-Thinking.

If the verifier has completeness close to 1, $p(z)$ is close to 1, and hence $r(z) \geq (1 - p(z))^{-1}$ must be large for $z \in E$. On the other hand, we can use soundness to bound how large $r(z)$ can be for $z \in F$. We can then use the fact that $r(z)$ is a rational function, and a standard result on the growth of rational functions, to bound how close to 1 the completeness can be.

We also investigate the analogous question for the soundness parameter in the definition of QMA. It is known that QMA with perfect soundness equals the complexity class NQP [KMY03], which is hard for the polynomial hierarchy [FGHP99], and thus likely different from QMA. The soundness can be amplified to be exponentially small with standard techniques. Can one do even better? Can one get, analogous to the situation for completeness, to doubly-exponentially small soundness? We show, using the same oracle and rational function approximation techniques, but now using

$$r(z) = \mathrm{tr}[P(z)] \tag{3}$$

that there is no black-box way to do so. This completely settles what completeness and soundness parameters are achievable with black-box amplification techniques in QMA.

A caveat is that the proof breaks down if the witness register is allowed to be infinite dimensional, as also observed in [Aar09]. This is not just a quirk of the proof technique: in [JW25] it is proven that (with black-box amplification techniques) one in fact can prove perfect completeness for QMA, provided that one allows computation on an infinite-dimensional Hilbert space with an appropriate gate set. This choice of gate set is such that the infinite-dimensional Hilbert space does not increase the computational power of BQP or QMA.

2 Preliminaries

We first recall the definition of QMA.

Definition 1. For parameters $c, s \in [0, 1]$ with $c > s$, the class $\mathsf{QMA}_{c,s}$ consists of promise problems $L = (L_{\text{yes}}, L_{\text{no}})$ for which there exists a uniform family of polynomial-time quantum circuits $\{V_x\}_{x \in \{0,1\}^n}$, called verifiers, with the following properties:

- (Completeness) If $x \in L_{\text{yes}}$, then there exists a quantum witness state $|\psi\rangle$ such that

$$\Pr[V_x \text{ accepts } |\psi\rangle] \geq c.$$

- (Soundness) If $x \in L_{\text{no}}$, then for all quantum states $|\psi\rangle$,

$$\Pr[V_x \text{ accepts } |\psi\rangle] \leq s.$$

The class QMA is defined as $\mathsf{QMA}_{2/3,1/3}$, since any inverse-polynomial gap between c and s can be amplified to these parameters by standard techniques [MW05]. The subclass QMA_1 is defined as $\mathsf{QMA}_{1,s}$ for some constant $s < 1$, i.e., *QMA with perfect completeness.*

We will also consider QMA with access to a quantum oracle $\mathcal{U}$. Here, there is a collection of possible unitaries, and the verifier get access to a unitary U from this set. The verifier has black-box access to U its inverse, and controlled application of U and its inverse. We then denote by $\mathsf{QMA}^{\mathcal{U}}$ the class of problems which can be solved as in Theorem 1 where Arthur additionally has access to a polynomial number of calls to $\mathcal{U}$.

2.1 Rational functions

A *rational function* of degree d is a quotient

$$r(z) = \frac{p(z)}{q(z)}$$

of two complex polynomials p, q of degree at most d. The study of extremal properties of such functions is a classical subject, with connections to complex analysis.

We will need a particular result concerning the so-called *Zolotarev problem*, which asks how well rational functions can approximate one behavior on a set E and a very different behavior on a disjoint set F. Formally, one considers rational functions r that are large on E and small on F, and asks how large the ratio

$$\frac{\inf_{z\in E}|r(z)|}{\sup_{z\in F}|r(z)|}$$

can be.

Without additional constraints, this ratio can be arbitrarily large: if E is a single point, then one can simply place a pole of r at (or near) that point. A nontrivial bound can be given if E and F each have positive *logarithmic capacity*, a notion from potential theory [Ran95] measuring the "size" of compact subsets of the complex plane.

We use the following theorem, due to Gončar [Gon69].

Theorem 2. *Let $r(z)$ be a rational function of degree d, and let $E, F \subset \mathbb{C}$ be disjoint closed sets with positive logarithmic capacity. Then there exists a constant $C > 0$ (depending only on E and F) such that*

$$\frac{\inf_{z\in E}|r(z)|}{\sup_{z\in F}|r(z)|} \le e^{Cd}.$$

In fact, the optimal constant C is given by the reciprocal of the *capacity* $\mathrm{Cap}(E, F)$ of the condenser (E, F). However, for our purposes, the existence of some positive C suffices.

We also use the fact that the inverse of a matrix is a rational function in the matrix entries, by Cramer's rule. This yields the following simple lemma.

Lemma 3. *Let $M(z)$ be a $q \times q$ matrix, where each matrix entry is a rational function of degree d. If $M(z)$ is invertible for z in some set $E \subset \mathbb{C}^*$, then the entries of $M(z)^{-1}$ are rational functions of degree $d(2q-1)$ on E.*

Proof. By Cramer's rule,

$$M(z)^{-1} = \frac{\mathrm{adj}(M(z))}{\det(M(z))}.$$

Each entry of $\mathrm{adj}(M(z))$ is a $(q-1)\times(q-1)$ determinant in entries of $M(z)$, hence a rational function of degree at most $d(q-1)$, and $\det(M(z))$ has degree at most dq. Thus every entry of $M(z)^{-1}$ is a rational function with degree at most $d(q-1) + dq = d(2q-1)$. □

3 Limits to black-box QMA amplification

In this section we prove tight black-box lower bounds for amplifying the completeness and soundness parameters of QMA. The following result shows that there is an oracle with respect to which QMA has completeness $c(n)$ which is at most doubly-exponentially close to 1, and soundness which is at most exponentially small. Both bounds follow from the same oracle construction (as in [Aar09]) together with the growth bound for rational functions in Theorem 2.

Theorem 4 (Limits to black-box amplification)**.** *There exists a quantum oracle $\mathcal{U}$ such that the following hold for any* QMA *verification procedure using* $\mathrm{poly}(n)$ *resources:*

1. ***(Completeness barrier).*** *For any black-box* QMA *amplification procedure that achieves completeness $c = 1 - \delta$ and soundness $s = 1/3$, we have*

$$\delta \ge 2^{-2^{\mathrm{poly}(n)}}.$$

More precisely, relative to $\mathcal{U}$,

$$\mathsf{QMA}^{\mathcal{U}} \neq \mathsf{QMA}^{\mathcal{U}}_{c(n),\,1/3} \qquad \textit{for } c(n) = 1 - o\Big(2^{-2^{\mathrm{poly}}}\Big).$$

2. ***(Soundness barrier).*** *For any black-box* QMA *amplification procedure that achieves completeness $c = 2/3$ and soundness $s = \delta$, we have*

$$\delta \geq 2^{-\,\mathrm{poly}(n)}.$$

In particular, relative to $\mathcal{U}$,

$$\mathsf{QMA}^{\mathcal{U}} \neq \mathsf{QMA}^{\mathcal{U}}_{2/3,\,s(n)} \qquad \textit{for } s(n) = o\Big(2^{-\,\mathrm{poly}(n)}\Big).$$

Proof. We use the same quantum oracle as in [Aar09]. Let $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ and, for $z = e^{i\theta} \in S^1$, define

$$U(z) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \frac{1}{2}\begin{pmatrix} z + z^{-1} & i(z^{-1} - z) \\ i(z - z^{-1}) & z + z^{-1} \end{pmatrix}.$$

Fix two closed, disjoint arcs $E, F \subset S^1$ of nonzero length (e.g. $E = \{e^{i\theta} : \theta \in [-\pi/3, \pi/3]\}$ and $F = \{e^{i\theta} : \theta \in [2\pi/3, 4\pi/3]\}$). By Example III.1.2 in [GM05], both E and F have positive logarithmic capacity, so Theorem 2 applies to the pair (E, F).

The promise problem is to decide whether the oracle parameter satisfies $z \in E$ (yes-instances) or $z \in F$ (no-instances). It is obvious that Arthur can do so with constant soundness and completeness (and even with trivial witness), so the problem is in QMA. We will now show, however, that there are limits to how close the completeness and soundness can get to 1 and 0 respectively using polynomial resources.

Consider any QMA verifier V that, on input $x \in \{0,1\}^n$, uses

- $t = t(n) = \mathrm{poly}(n)$ calls to the oracle,
- a witness register of $m = m(n) = \mathrm{poly}(n)$ qubits; let $q = 2^m$ denote its dimension.

Let $P(z)$ denote the POVM element corresponding to acceptance. Write the eigenvalues of $P(z)$ as $1 \geq \lambda_1(z) \geq \cdots \geq \lambda_q(z) \geq 0$. For each fixed z, the optimal acceptance probability, over all choices of witness, equals $\lambda_1(z)$.

Every matrix element of $U(z)$ and $U(z)^\dagger$ (and hence also of their controlled versions) is an affine combination of z and z^{-1}. Hence, by expanding the verifier circuit and projecting on the accept outcome, each entry of $P(z)$ is a polynomial of degree $2t$ in z and z^{-1}, and hence a rational function of degree $4t$.

Completeness barrier Assume the verifier achieves completeness $1 - \delta$ on E and soundness $1/3$ on F:

$$\lambda_1(z) \geq 1 - \delta \quad (z \in E), \qquad \lambda_1(z) \leq \tfrac{1}{3} \quad (z \in F).$$

We consider the following function:

$$r(z) = \mathrm{tr}\big[(I - P(z))^{-1}\big] = \sum_{i=1}^{q} \frac{1}{1 - \lambda_i(z)}.$$

By Theorem 3, $r(z)$ is a rational function of degree $d = O(qt)$.

We now bound r on E and F. On E, $1 - \lambda_1(z) \leq \delta$, so

$$r(z) = \sum_{i=1}^{q} \frac{1}{1 - \lambda_i(z)} \geq \frac{1}{1 - \lambda_1(z)} \geq \frac{1}{\delta}.$$

On F, since $\lambda_1(z) \leq \frac{1}{3}$ and $\lambda_i(z) \leq \lambda_1(z)$, we have

$$r(z) = \sum_{i=1}^{q} \frac{1}{1-\lambda_i(z)} \leq q \cdot \frac{1}{1-\lambda_1(z)} \leq \frac{3q}{2}.$$

Therefore

$$\frac{\inf_{z\in E} r(z)}{\sup_{z\in F} r(z)} \geq \frac{2}{3q\delta}.$$

Applying Theorem 2 gives a constant $C > 0$ such that

$$\frac{\inf_{z\in E} r(z)}{\sup_{z\in F} r(z)} \leq e^{Cd}.$$

Combining, we conclude that

$$\frac{2}{3q\delta} \leq e^{Cd} \quad\Longrightarrow\quad \delta \geq \frac{2}{3q}\, e^{-Cd}.$$

Now, $d = O(qt)$, $q = 2^{\mathrm{poly}(n)}$, and $t = \mathrm{poly}(n)$, which proves 1.

Soundness barrier Assume the verifier achieves completeness $2/3$ on E and soundness δ on F:

$$\lambda_1(z) \geq \tfrac{2}{3} \quad (z \in E), \qquad \lambda_1(z) \leq \delta \quad (z \in F).$$

Consider

$$r(z) = \mathrm{tr}\big[P(z)\big] = \sum_{i=1}^{q} \lambda_i(z),$$

then $r(z)$ is a rational function of degree $d = 4t$. We again bound r on E and F. On E, $r(z) \geq \lambda_1(z) \geq \frac{2}{3}$. On F, $r(z) = \sum_i \lambda_i(z) \leq q\lambda_1(z) \leq q\delta$. Therefore

$$\frac{\inf_{z\in E} r(z)}{\sup_{z\in F} r(z)} \geq \frac{2}{3q\delta}.$$

Applying Theorem 2 yields a constant $C > 0$ such that

$$\frac{\inf_{z\in E} r(z)}{\sup_{z\in F} r(z)} \leq e^{Cd}$$

and hence

$$\frac{2}{3q\delta} \leq e^{Cd} \quad\Longrightarrow\quad \delta \geq \frac{2}{3q}\, e^{-Cd}.$$

With degree $d = O(t) = \mathrm{poly}(n)$ and $q = 2^{\mathrm{poly}(n)}$, we have

$$\delta \geq 2^{-\,\mathrm{poly}(n)}$$

which proves 2. □

Note that in the proof of Theorem 4, the crucial difference between the completeness and the soundness cases is that the function $r(z)$ does not depend on the witness dimension q.

Since black-box amplification procedures can also *achieve* completeness $c = 1 - 2^{-2^{\mathrm{poly}}}$ and soundness $s = 2^{-\,\mathrm{poly}}$, this gives the optimal completeness and soundness parameters for QMA which can be achieved through black-box reductions.

4 Discussion

While previously it was known how to achieve completeness and soundness exponentially close to 1 and 0 respectively, this work, together with [JW25], shows that with black-box reductions one can achieve completeness doubly exponentially close to 1, and soundness exponentially small, and that this is optimal. The asymmetry between soundness and completeness is natural from the definition: completeness only requires a single eigenvalue of the accepting measurement operator to be very close to 1, while soundness is a condition on all possible witness states and requires *all* eigenvalues of the accepting mesurement operator to be close to 0.

Let us call attention to something conceptually strange about our result. Recall that $\mathsf{QMA} \subseteq \mathsf{PP} = \mathsf{PostBQP}$, with the containment believed to be strict. Nevertheless, we saw in this paper that "the approximation theory object corresponding to QMA," namely the largest eigenvalue of an $\exp(n) \times \exp(n)$ Hermitian matrix of low-degree polynomials, is in some respects *more* powerful than "the approximation theory object corresponding to PP," namely a low-degree rational function. In particular, the former allows amplification to doubly exponentially small completeness error, while the latter does not.

How is this possible? In our view, the resolution is simply that, to prove $\mathsf{QMA} \subseteq \mathsf{PP}$, it suffices to calculate only a crude estimate of the largest eigenvalue in question—something that *is* possible using low-degree rational functions. Indeed, if we ask for more precise information about the largest eigenvalue, we get the class $\mathsf{PreciseQMA}$, which equals PSPACE [FL18] and hence is presumably more powerful than $\mathsf{PostBQP} = \mathsf{PP}$.

Of course, the central open question we leave is whether $\mathsf{QMA} = \mathsf{QMA}_1$ for some, or all, finite-dimensional gate sets.

A more minor open question is whether, in our oracle separation, we can take the angle θ to have some fixed value, say $\theta = \pi$, in the no-case, rather than belonging to an interval of values. We conjecture that the answer is yes but a new argument seems needed.

Acknowledgments

We thank Stacey Jeffery for helpful discussions.

References

[Aar09] Scott Aaronson. On perfect completeness for QMA. *Quantum Information and Computation*, 9:81–89, 2009. arXiv: 0806.0450.

[FGHP99] Stephen Fenner, Frederic Green, Steven Homer, and Randall Pruim. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 455(1991):3953–3966, 1999. arXiv: quant-ph/9812056.

[FL18] Bill Fefferman and Cedric Yen-Yu Lin. A complete characterization of unitary quantum space. In *9th Innovations in Theoretical Computer Science Conference (ITCS 2018)*, pages 4–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2018. arXiv: 1604.01384.

[GM05] John B Garnett and Donald E Marshall. *Harmonic measure*. Number 2 in New Mathematical Monographs. Cambridge University Press, 2005.

[Gon69] AA Gončar. Zolotarev problems connected with rational functions. *Mathematics of the USSR-Sbornik*, 7(4):623, 1969.

[JKNN12] Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information and Computation*, 12(5-6):461–471, 2012. arXiv: 1111.5306.

[JW25] Stacey Jeffery and Freek Witteveen. $\mathsf{QMA} = \mathsf{QMA}_1$ with an infinite counter. *arXiv: 2506.15551*, 2025.

[KMY03] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In *International Symposium on Algorithms and Computation*, pages 189–198. Springer, 2003. arXiv: quant-ph/0306051.

[KSV02] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. *Classical and quantum computation*. Number 47 in Graduate Studies in Mathematics. American Mathematical Society, 2002.

[MW05] Chris Marriott and John Watrous. Quantum Arthur–Merlin games. *computational complexity*, 14(2):122–152, 2005. arXiv: cs/0506068.

[Ran95] Thomas Ransford. *Potential theory in the complex plane*. Number 28 in London Mathematical Society Student Texts. Cambridge University Press, 1995.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il