

# Even quantum advice is unlikely to solve PP

Justin Yirka\*

The University of Texas at Austin

[yirka@utexas.edu](mailto:yirka@utexas.edu)

May 2024

## Abstract

We give a corrected proof that if  $\text{PP} \subseteq \text{BQP}/\text{qpoly}$ , then the Counting Hierarchy collapses, as originally claimed by [Aaronson 2006]. This recovers the related unconditional claim that PP does not have circuits of any fixed size  $n^k$  even with quantum advice. We do so by proving that  $\text{YQP}^*$ , an oblivious version of  $\text{QMA} \cap \text{coQMA}$ , is contained in  $\text{APP}$ , and so is PP-low.

## 1 Introduction

Do reasonably-sized circuits solve hard problems, given that we allow the computation to vary (non-uniformly) as the problem size grows? While directly answering this question for classes such as NP has proven difficult, progress has been made showing conditional results, such as the Karp-Lipton theorem that if  $\text{NP} \subseteq \text{P}/\text{poly}$ , then the polynomial hierarchy collapses [KL80], or showing upper bounds against larger classes, such as PP or NEXP [Vin05, Wil14]. Exploring further, we can consider quantum computation. In this model, circuits are typically uniformly generated but might accept non-uniform *advice* strings as part of their input. Moreover, quantum circuits can not only receive classical advice strings (BQP/poly), but quantum *advice states* (BQP/qpoly).

In [Aar06], Aaronson proved new quantum circuit lower bounds, among other results. In particular, he gave several results characterizing quantum circuits' ability to solve problems in the class PP, the class of problems decidable by probabilistic algorithms with no promise gap, i.e. which accept with probability at least 1/2 or strictly less than 1/2. PP contains both BPP and NP and is contained in PSPACE. Aaronson proved that  $\text{P}^{\text{PP}}$  does not have circuits of size  $n^k$  for any fixed constant  $k$  even if the circuits use quantum advice states. Second, he claimed a quantum analogue of the Karp-Lipton theorem, showing that if  $\text{PP} \subseteq \text{BQP}/\text{qpoly}$ , then the Counting Hierarchy (CH) collapses to QMA, where the Counting Hierarchy is the infinite sequence of classes  $\text{C}_1\text{P} = \text{PP}$  and  $\text{C}_i\text{P} = (\text{C}_{i-1}\text{P})^{\text{PP}}$ , and where QMA is a quantum analogue of NP. Similarly, he showed that under the stronger assumption  $\text{PP} \subseteq \text{BQP}/\text{poly}$ , using classical advice instead of quantum advice, then  $\text{CH} = \text{QCMA}$ . Third, Aaronson combined these results to give the unconditional bound that PP does not have classical or quantum circuits of size  $n^k$  for any fixed constant  $k$  even with quantum advice.<sup>1</sup>

---

\*Supported via Scott Aaronson by a Simons Investigator Award.

<sup>1</sup>Slightly earlier, Vinochandran [Vin05] gave a proof that PP does not have *classical* circuits of fixed polynomial size.

However, Aaronson later noted there was an error in one of the proofs [Aar17]. The first of the above results was unaffected, but the proof of the second result only held under the stronger assumption that  $\text{PP} \subseteq \text{BQP/poly}$ . This also meant the third result only held for quantum circuits with classical, not quantum, advice. Fortunately, no other results in [Aar06] were affected, but no fix for this bug was forthcoming.

Very briefly, the error was a claim that for oracle classes of the form  $\text{C}^{\text{BQP/qpoly}}$ , if a machine for the base class  $\text{C}$  is able to find the quantum advice state that will be used by the oracle machine, then the base machine can “hard-code” the advice state into its oracle queries so that the oracle no longer needs the power to find its own advice, thus reducing  $\text{C}^{\text{BQP/qpoly}}$  to  $\text{C}^{\text{BQP}}$ . This approach works for classes with classical advice, like  $\text{C}^{\text{BQP/poly}}$ . But, because complexity classes and their associated oracles are defined in terms of (classical) strings as input, there is no way to hard-code a general quantum advice state into a query.

In this note, we give a corrected proof of Aaronson’s full claims. We show that if  $\text{PP} \subseteq \text{BQP/qpoly}$ , then the Counting Hierarchy collapses to  $\text{QMA}$  and in fact to  $\text{YQP}^*$ . Given this correction, Aaronson’s proof for the third claim, that  $\text{PP}$  does not have circuits of size  $n^k$  for any fixed constant  $k$  even with quantum advice, now goes through.

Our primary technical contribution is to show  $\text{YQP}^* \subseteq \text{APP}$ . Here,  $\text{YQP}^*$  is an oblivious version of  $\text{QMA} \cap \text{coQMA}$ , meaning there exists a useful proof state which depends only on the size of the input. Crucially, a  $\text{YQP}^*$  protocol includes a proof-verification circuit that tests if the given quantum state is a “good” proof, before the proof is used to determine whether a particular input is a YES or NO instance. We apply the in-place error reduction technique of Marriott and Watrous [MW05] to this proof-verification circuit. The class  $\text{APP}$  is a subclass of  $\text{PP}$  with an arbitrarily small but nonzero promise gap. It is known to have the nice property that  $\text{PP}^{\text{APP}} = \text{PP}$  [Li93]. Thus,  $\text{YQP}^*$  is also  $\text{PP}$ -low. Our corrected proof combines this result with the known equality  $\text{BQP/qpoly} = \text{YQP}^*/\text{poly}$ , serendipitously proven by Aaronson with Drucker [AD14]. Now, instead of following Aaronson’s original attempt to collapse  $\text{PP}^{\text{PP}}$  to  $\text{PP}^{\text{BQP/qpoly}}$  to  $\text{PP}^{\text{BQP}}$  to  $\text{PP}$ , we can collapse  $\text{PP}^{\text{PP}}$  to  $\text{PP}^{\text{YQP}^*/\text{poly}}$  to  $\text{PP}^{\text{YQP}^*}$  to  $\text{PP}$ .

Our results provide stronger implications and improved bounds for quantum circuits with quantum advice and establish new insights into  $\text{PP}$ -lowness and classes within  $\text{APP}$ . Compared to other quantum Karp-Lipton style bounds, including that if  $\text{QCMA} \subseteq \text{BQP/poly}$ , then  $\text{QCPH}$  collapses [AGKR24] and that if  $\text{NP} \subseteq \text{BQP/qpoly}$ , then  $\Pi_2^P \subseteq \text{QMA}^{\text{PromiseQMA}}$  [AD14], the supposition  $\text{PP} \subseteq \text{BQP/qpoly}$  and the implied collapse of  $\text{CH}$  are both formally stronger. As for unconditional bounds, following Aaronson’s unaffected result that  $\text{P}^{\text{PP}}$  does not have quantum circuits with quantum advice of any fixed polynomial size, our corrected result bound against  $\text{PP}$  is the first improved bound of fixed-size circuits with quantum advice. Regarding  $\text{PP}$ -lowness, our primary lemma establishes  $\text{YQP}^*$  as the largest natural quantum complexity class known to be  $\text{PP}$ -low, improving on the fact that  $\text{BQP}$  is  $\text{PP}$ -low [FR99].<sup>2</sup> Finally, for  $\text{APP}$ , while the largest witness-based class previously known to be contained in  $\text{APP}$  was  $\text{FewP}$  [Li93], our result shows that  $\text{APP}$  in fact contains oblivious-witness classes including  $\text{YQP}^* \supseteq \text{YMA}^* \supseteq \text{YP}^* \supseteq \text{FewP}$ .

---

<sup>2</sup>Morimae and Nishimura [MN16] gave definitions involving quantum postselection constructed to equal  $\text{AWPP}$  and  $\text{APP}$ , which are  $\text{PP}$ -low.

## 2 Preliminaries

In this section, we discuss non-uniform circuits, give definitions for YQP and APP, discuss PP and GapP, and finally state a fact relating quantum circuits to GapP. For a deeper introduction to these classes and other concepts, see [Aar06, AD14] and e.g. [AB09].

The classes of non-uniform circuits we consider, including P/poly, BQP/poly, BQP/qpoly, share the following key characteristics. First, they are defined in terms of circuits or advice that may depend on the size of the problem input (but not on the input itself), with no requirement that the circuit or advice is generated by a uniform algorithm. Second, the circuits are defined with bounded fan-in and fan-out, in contrast to classes such as  $AC_0$  or  $QAC_0$ . Third, the classes consider circuits of polynomial-size, where the size is the number of gates in a circuit.

Advice is typically considered “trusted” in that there is no promised behavior when given the “wrong” advice, so an analysis of correctness can usually assume the “right” advice is provided. In line with this convention, we assume the standard definitions of BQP/poly and BQP/qpoly in which a circuit is only required to accept with high or low probability (outside of the “promise gap”) when the correct advice is provided, although the same notation has sometimes been used to refer to other definitions, see e.g. [Zoo].

The class YQP was first described in [Aar07], but the definition was later corrected by Aaronson and Drucker [AD14]. Informally, it is the oblivious version of  $QMA \cap coQMA$ , so that the witness sent by Merlin depends only on the length of the input. In contrast to the advice of P/poly, this has been described as “untrusted advice” [Aar07]. Oblivious proofs can also be thought of as restricting non-uniform classes, like P/poly or BQP/qpoly, to advice which is verifiable [GM15].

**Definition 2.1.** A language  $L$  is in YQP if there exists a polynomial-time uniform family of quantum circuits  $\{Y_n\}_{n \in \mathbb{N}}$  that satisfy the following. Circuit  $Y_n$  is of size  $\text{poly}(n)$  and takes as input  $x \in \{0, 1\}^n$ , a  $p(n)$ -qubit state  $\rho$  for some  $p(n) \leq \text{poly}(n)$ , and an ancilla register initialized to the all-zero state, and has two designated 1-qubit “advice-testing” and “output” qubits.  $Y_n(x, \rho)$  acts as follows:

1. First,  $Y_n$  applies a subcircuit  $A_n$  to all registers, after which the advice-testing qubit is measured, producing a value  $b_{\text{adv}} \in \{0, 1\}$ .
2. Next,  $Y_n$  applies a second subcircuit  $B_n$  to all registers, then measures the output qubit, producing a value  $b_{\text{out}} \in \{0, 1\}$ .

These output bits satisfy the following:

- For all  $n$ , there exists a  $\rho_n$  such that for all  $x$ , the advice bit satisfies  $E[b_{\text{adv}}] \geq 9/10$ .
- For any  $x, \rho$  such that  $E[b_{\text{adv}}] \geq 1/10$ , on input  $x, \rho$  we have

$$\Pr[b_{\text{out}} = L(x) \mid b_{\text{adv}} = 1] \geq 9/10.$$

$L$  is in the subclass YQP\* if the family can be chosen such that  $b_{\text{adv}}$  is independent of  $x$ .

Just as Oblivious-NP is unlikely to contain NP [FSW09], it also seems unlikely that QMA is contained in YQP. On the other hand, it is straightforward to show that any sparse language can be verified obliviously, so  $\text{FewP} \subseteq \text{YP}^*$  and  $\text{FewQMA} \subseteq \text{YQP}^*$ . We also have the trivial bounds  $\text{BQP} \subseteq \text{YQP}^* \subseteq \text{YQP} \subseteq \text{QMA}$  and  $\text{YQP} \subseteq \text{BQP}/\text{qpoly}$ . Studying YQP may be motivated by the use of oblivious complexity classes in constructing circuit lower bounds [FSW09, GLV24], by the fact that  $\text{BQP}/\text{qpoly} = \text{YQP}^*/\text{poly} = \text{YQP}/\text{poly}$  shown by [AD14], or by the results shown in this work.

The class APP was introduced by Li [Li93] in pursuit of a large class of PP-low languages. We use the equivalent definition given by Fenner [Fen03, Corollary 3.7].

**Definition 2.2.**  $L \in \text{APP}$  if and only if there exist functions  $f, g \in \text{GapP}$  and constants  $0 \leq \lambda < \nu \leq 1$  such that for all  $n$  and  $x \in \{0, 1\}^n$ , we have  $g(1^n) > 0$  and

- If  $x \in L$  then  $\nu g(1^n) \leq f(x) \leq g(1^n)$ ;
- If  $x \notin L$  then  $0 \leq f(x) \leq \lambda g(1^n)$ .

In the above definition, recall that  $\text{GapP}$  is the closure of  $\#\text{P}$  under subtraction. In other words, while every function  $f \in \#\text{P}$  corresponds to a nondeterministic polynomial-time Turing Machine  $N$  such that  $f(x)$  equals the number of accepting paths of  $N(x)$ , a  $\text{GapP}$  function equals the number of accepting paths minus the number of rejecting paths.

APP is a subclass of PP and is PP-low, meaning  $\text{PP}^{\text{APP}} = \text{PP}$ . Recall that PP can be thought of as comparing a  $\#\text{P}$  function to a threshold exactly, with no promise gap. The class in fact remains unchanged if it is defined as comparing a  $\text{GapP}$  function to a threshold, and the threshold may be as simple as one-half of the possible paths or as complex as a  $\text{GapP}$  function. In these terms, APP can be thought of as comparing a  $\text{GapP}$  function (here  $f(x)$ ) to some threshold (here  $g(1^n)$ ), where the complexity of the threshold is limited to a  $\text{GapP}$  function which may depend on the input size but not the input, and where there is some arbitrarily small but nonzero promise gap (from  $\lambda g(1^n)$  to  $\nu g(1^n)$ ).

The best known upper bound on APP is PP. Compared with the class  $\text{A}_0\text{PP} = \text{SBQP} \subseteq \text{PP}$  [Kup15],  $\text{A}_0\text{PP}$  contains QMA and is *not* known to be PP-low, while APP is not known to contain even NP but is PP-low.

We will use the following fact shown for uniform circuit families by Watrous [Wat08, Section IV.5], and shown earlier for QTMs by Fortnow and Rogers [FR99].

**Lemma 2.3.** *For any polynomial-time uniformly generated family of quantum circuits  $\{Q_n\}_{n \in \mathbb{N}}$  each of size bounded by a polynomial  $t(n)$ , there is a  $\text{GapP}$  function  $f$  such that for all  $n$ -bit  $x$ ,*

$$\Pr[Q_n(x) \text{ accepts}] = \frac{f(x)}{5^{t(n)}}.$$

### 3 Results

We first prove our main technical result, that  $\text{YQP}^* \subseteq \text{APP}$ , improving on the largest proof-based complexity class known to be contained in APP.

Our approach is as follows. APP evaluates the ratio of two  $\text{GapP}$  functions, where one of the functions is only allowed to depend on the input length. By Lemma 2.3, functions in  $\text{GapP}$  can encode the output probabilities of quantum circuits. So, for a  $\text{YQP}^*$  computation

with circuit  $Y$  and subcircuit  $A$ , we run them both on the maximally-mixed state and ask APP to determine the ratio of their acceptance probabilities. In other words, when  $A$  accepts, however large or small that probability is, does  $Y$  usually accept or usually reject? We require the error reduction technique of Marriott and Watrous [MW05] to make the error in  $A$  negligible.

**Lemma 3.1.**  $YQP^* \subseteq APP$ .

*Proof.* Consider any language  $L \in YQP^*$ . Let  $\{Y_n, A_n, B_n\}_{n \in \mathbb{N}}$  be the associated family of circuits and subcircuits, in which  $Y_n$  takes string  $x$  and a supposed witness or advice state as input, in which subcircuit  $A_n$  validates the advice and produces output bit  $b_{\text{adv}}$ , and in which, given  $A_n$  accepted,  $B_n$  uses the advice to verify whether the particular input  $x$  is in  $L$ , producing the output bit  $b_{\text{out}}$ . Note that because we consider  $YQP^*$ , the circuit  $A_n$  only takes the witness state, not  $x$ , as input. Let  $k$  and  $m$  be polynomials in  $n$  denoting the respective sizes of the ancilla and proof registers.

We use the technique of strong, or in-place, error reduction of Marriott and Watrous [MW05] on the circuits  $A_n$  with a polynomial  $q$  in  $n$  of our choosing to produce a new circuit family  $\{A'\}_{n \in \mathbb{N}}$  such that for any proof  $\rho$ ,

- $\Pr[A_n(\rho)] \geq \frac{9}{10} \Rightarrow \Pr[A'_n(\rho)] \geq 1 - 2^{-q}$ ;
- $\Pr[A_n(\rho)] \leq \frac{1}{10} \Rightarrow \Pr[A'_n(\rho)] \leq 2^{-q}$ .

For later use, we choose  $q > \max\{3m, 10\}$ .

Recall the error reduction algorithm of [MW05] involves, given some quantum input or witness state, applying a circuit  $C$ , recording whether the output is  $|0\rangle$  or  $|1\rangle$  in a variable  $y_i$ , applying  $C^\dagger$ , recording whether the circuit's ancilla register is in the all-zero state or not in a variable  $y_{i+1}$ , and repeating these steps for some number of iterations  $M$ . Call the full, amplified circuit  $C'$ .

Applying the error-reduction procedure, we define  $\{A''_n\}_{n \in \mathbb{N}}$  to be the amplified circuits  $\{A'_n\}_{n \in \mathbb{N}}$  with the additional rule that the circuit accepts iff both  $b_{\text{adv}} = 1$  and the final two recorded variables  $y_{2M} = y_{2M+1} = 1$ . Further, define  $\{A'''_n\}_{n \in \mathbb{N}}$  so that  $A'''_n = A''_n(\frac{\mathbb{I}}{2^m})$ , with the maximally mixed state hard-wired into the proof register. Similarly, we define  $\{Y'_n\}_{n \in \mathbb{N}}$  to apply the amplified subcircuit  $A'_n$  and  $B_n$ , we define  $\{Y''_n\}_{n \in \mathbb{N}}$  to apply  $A''_n$  and  $B_n$  and thus accept iff  $b_{\text{adv}}, b_{\text{out}}, y_{2M}, y_{2M+1}$  all equal 1, and we define  $\{Y'''_n\}_{n \in \mathbb{N}}$  so that  $Y'''_n(x) = Y''_n(x, \frac{\mathbb{I}}{2^m})$  with the maximally mixed state hard-wired into the proof register, meaning that it uses  $A'''_n$  as a subcircuit.

**Error-reduction properties** We remark on what the bits  $y_i$  tell us about the state of the circuit. Studying the proof of [MW05], if after applying  $C^\dagger$ , a recorded bit  $y_{2i+1} = 1$ , then the state of the ancilla register is projected into the all-zero state. Now, suppose the circuit  $C'$  is applied to an  $m$ -qubit proof state, so there are  $2^m$  eigenstates  $\{|\lambda_i\rangle\}_{i \in [2^m]}$  of  $C'$ . Further studying the proof of [MW05], if the initial state given to  $C'$  was an eigenstate  $|\lambda_i\rangle$ , and after a round of applying  $C^\dagger$  the recorded bit is  $y_{2i+1}$ , then not only is the ancilla register known to be in the all-zero state, but the final state of the proof register is the same as its initial state,  $|\lambda_i\rangle$ .

We are also able to characterize the probabilities of these outcomes. Intuitively, consecutive bits are transitions which depend on whether we expect the circuit beginning with a properly initialized all-zero ancilla register to produce an output qubit close to  $|1\rangle$  or to  $|0\rangle$ , and vice-versa. Suppose an eigenstate  $|\lambda_i\rangle$  is accepted by the original circuit  $C$  with

probability  $p$ . Then when  $C'$  is run on  $|\lambda_i\rangle$ , we have that  $\Pr[y_{2i+1} = 1 \mid y_{2i} = 1] = p$ . Next, we consider  $\Pr[y_{2i} = 1]$ . We may analyze this probability with a two-state Markov chain, such that if  $y_{2i} = 1$ , then  $y_{2i+2} = 1$  with probability  $p^2 + (1-p)^2$  and  $y_{2i+2} = 0$  with probability  $2p(1-p)$ , while if  $y_{2i} = 0$ , then  $y_{2i+2} = 0$  with probability  $p^2 + (1-p)^2$  and  $y_{2i+2} = 1$  with probability  $2p(1-p)$ . If we suppose  $p > 1/2$ , and given  $C'$  begins in the all-zero state ( $y_0 = 1$ ), then it is straightforward to conclude that for any particular  $i$ , we have  $\Pr[y_{2i} = 1] > 1/2$  (see e.g. [LP17, Example 1.1]).

**Analysis** Applying Lemma 2.3, there exist GapP functions  $f, g$  and polynomials  $r, t$  such that for all  $n$ -bit  $x$ ,

$$\Pr[A_n''' \text{ accepts}] = \frac{f(1^n)}{5^{r(n)}} \quad \text{and} \quad \Pr[Y_n'''(x) \text{ accepts}] = \frac{g(x)}{5^{t(n)}}.$$

The function  $f$  depends only on the input length  $n$ , not  $x$ , because the circuit  $A_n'''$  is independent of  $x$ . Next, we define  $F(1^n) = f(1^n)5^{t(n)-r(n)}$ , which is a GapP function since  $5^{t(n)-r(n)} \in \text{FP} \subseteq \text{GapP}$  and GapP is closed under multiplication. Given the definition of YQP\* guarantees there exists a “good” proof for circuit  $A_n$ , we have  $f(1^n), F(1^n) > 0$ . Combining these definitions,

$$\frac{g(x)}{F(1^n)} = \frac{\Pr[Y_n'''(x) \text{ accepts}]}{\Pr[A_n''' \text{ accepts}]}.$$

We will show bounds on the ratio  $g(x)/F(1^n)$  based on whether  $x$  is in  $L$  or not in  $L$  in order to prove  $L$  is in APP. First, note that the ratio is upper-bounded by 1 since  $Y_n'''$  only accepts if the subcircuit  $A_n'''$  accepts, and it is lower-bounded by 0 since probabilities are non-negative. Next, let  $\{|\lambda_i\rangle\}_{i \in [2^m]}$  be the set of eigenvectors  $|\lambda_i\rangle$  of the circuit  $A_n$ . By writing the maximally mixed state, which is hard-wired into the proof register of  $Y_n'''$ , in terms of this eigenbasis, we find

$$\begin{aligned} \frac{\Pr[Y_n'''(x) \text{ accepts}]}{\Pr[A_n''' \text{ accepts}]} &= \frac{\Pr[Y_n''(x, \frac{\mathbb{I}}{2^m}) \text{ accepts}]}{\Pr[A_n''(\frac{\mathbb{I}}{2^m}) \text{ accepts}]} = \frac{\sum_{i=1}^{2^m} \Pr[Y_n''(x, |\lambda_i\rangle) \text{ accepts}]}{\sum_{i=1}^{2^m} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]} \\ &= \frac{\sum_{i=1}^{2^m} \Pr[Y_n''(x, |\lambda_i\rangle) \text{ accepts} \mid A_n''(|\lambda_i\rangle) \text{ accepts}] \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]}{\sum_{i=1}^{2^m} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]} \\ &= \frac{\sum_{i=1}^{2^m} \Pr[B_n(x, |\lambda_i\rangle) \text{ accepts}] \cdot \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]}{\sum_{i=1}^{2^m} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]} \end{aligned}$$

where we have used the fact that  $Y_n''$  accepting requires that  $A_n''$  accepts and our observation that  $A_n''$  accepting guarantees the initial eigenstate  $|\lambda_i\rangle$  is sent on to the subcircuit  $B_n$  within  $Y_n''$ . Define

$$\mathcal{B} = \{i \in [2^m] \mid \Pr[A_n''(|\lambda_i\rangle)] \leq 0.1\},$$

which are intuitively the “bad” proofs, such that states in  $\mathcal{B}$  will be rejected by  $A_n''$  with high probability while the “not bad” states in  $\overline{\mathcal{B}}$  cause  $B_n$  to output the correct answer with high probability. Then we can rewrite both the numerator and denominator in the above ratio to give

$$\frac{\sum_{i \in \mathcal{B}} \Pr[B_n(x, |\lambda_i\rangle) \text{ accepts}] \cdot \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}] + \sum_{i \in \overline{\mathcal{B}}} \Pr[B_n(x, |\lambda_i\rangle) \text{ accepts}] \cdot \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]}{\sum_{i \in \mathcal{B}} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}] + \sum_{i \in \overline{\mathcal{B}}} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]}$$



We will use this expression as the starting point for our analysis of the YES and NO cases.

Now, suppose we have a YES instance with  $x \in L$ . We are guaranteed at least one proof is accepted by  $A$  with high probability, and denote it by  $|\lambda^*\rangle$ . Then, we may calculate that  $g(x)/F(1^n)$  is at least

$$\begin{aligned} \frac{\sum_{i \in \mathcal{B}} 0 + \sum_{i \in \bar{\mathcal{B}}} \frac{9}{10} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]}{\sum_{i \in \mathcal{B}} 2^{-q} + \sum_{i \in \bar{\mathcal{B}}} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]} &= \frac{\sum_{i \in \bar{\mathcal{B}}} \frac{9}{10} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]}{|\mathcal{B}| 2^{-q} + \sum_{i \in \bar{\mathcal{B}}} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]} \\ &\geq \frac{\frac{9}{10} \Pr[A_n''(|\lambda^*\rangle) \text{ accepts}]}{|\mathcal{B}| 2^{-q} + \Pr[A_n''(|\lambda^*\rangle) \text{ accepts}]}, \end{aligned}$$

where the second line follows by the fact that  $x/(c+x)$  decreases as  $x$  decreases. Next, we use the same fact, the earlier bound on the probability that the error-reduction variables  $y_{2M}, y_{2M+1}$  equal 1, and our choice  $q > \max\{3m, 10\}$  to find that the above is at least

$$\begin{aligned} \frac{\frac{9}{10}(1-2^{-q})(0.9)(0.5)}{|\mathcal{B}| 2^{-q} + (1-2^{-q})(0.9)(0.5)} &\geq \frac{0.405(1-2^{-q})}{2^{m-q} + 0.45(1-2^{-q})} \\ &\geq \frac{0.405(1-2^{-q})}{2^{-q/3} + 0.45(1-2^{-q})} \\ &\geq \frac{0.405(1-2^{-10})}{2^{-10/3} + 0.45(1-2^{-10})} > 0.73. \end{aligned}$$

On the other hand, consider a NO instance. We have that  $g(x)/F(1^n)$  is at most

$$\begin{aligned} \frac{|\mathcal{B}| 2^{-q} + \sum_{i \in \bar{\mathcal{B}}} \frac{1}{10} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]}{\sum_{i \in \mathcal{B}} 0 + \sum_{i \in \bar{\mathcal{B}}} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]} &\leq \frac{2^{m-q}}{\sum_{i \in \bar{\mathcal{B}}} \Pr[A_n''(|\lambda_i\rangle) \text{ accepts}]} + \frac{1}{10} \\ &\leq \frac{2^{m-q}}{2^{-m}(1-2^{-q})} + \frac{1}{10} \\ &< \frac{2^{-q/3}}{1-2^{-q}} + \frac{1}{10} < 0.2, \end{aligned}$$

where the second line follows by the existence of  $|\lambda^*\rangle$  and the final line uses our choice of  $q > \max\{3m, 10\}$ .

We have shown a constant separation of  $g(x)/F(1^n)$  in YES and NO instances. This satisfies the definition of APP in [Definition 2.2](#) of APP, so we conclude  $\text{YQP}^* \subseteq \text{APP}$ .  $\square$

Next, the fact APP is known to be PP-low [[Li93](#), Theorem 6.4.14] gives us the following corollary.

**Corollary 3.2.** *YQP\* is PP-low, i.e.  $\text{PP}^{\text{YQP}^*} = \text{PP}$ .*

For intuition, an alternative proof of [Corollary 3.2](#) might have relied on the equality  $\text{PP} = \text{postBQP}$  [[Aar05](#)], where  $\text{postBQP}$  has the ability to post-select, i.e. it is guaranteed to output the correct answer with high probability *conditioned on* some other event which may occur with very small probability. So, instead of  $\text{PP}^{\text{YQP}^*}$ , we might have considered  $\text{postBQP}^{\text{YQP}^*}$ . Whenever the  $\text{postBQP}$  machine would make a query, it instead could run the  $\text{YQP}^*$  proof-validation circuit on the maximally mixed state, post-select on it accepting, then simulate the rest of the  $\text{YQP}^*$  computation.

We are now able to give a corrected proof of the result originally claimed for  $\text{BQP}/\text{qpoly}$  but only proved for  $\text{BQP}/\text{poly}$  by Aaronson [[Aar06](#)]. We mostly repeat Aaronson's proof, but substitute  $\text{YQP}^*$  where he relied on  $\text{QMA}$ .

**Theorem 3.3.** *If  $\text{PP} \subseteq \text{BQP}/\text{qpoly}$ , then the Counting Hierarchy collapses to  $\text{CH} = \text{QMA} = \text{YQP}^*$ .*

*Proof.* Suppose  $\text{PP} \subseteq \text{BQP}/\text{qpoly}$ . From [AD14], we know that  $\text{BQP}/\text{qpoly} = \text{YQP}^*/\text{poly}$ . Then in  $\text{YQP}^*$ , without any trusted advice, Arthur can request Merlin sends many copies of the quantum advice  $|\psi\rangle$  and a description of the circuit  $C$  such that  $C, |\psi\rangle$  compute PERMANENT, a PP-complete problem. Of course, this advice is now untrusted. Arthur verifies that  $C, |\psi\rangle$  in fact work on a large fraction of inputs by simulating the interactive protocol for  $\#P$  due to [LFKN92], which also works for PP, using  $C, |\psi\rangle$  in place of the prover. If the protocol accepts (meaning the “prover” worked), then Arthur can use the random self-reducibility of PERMANENT to generate a circuit  $C'$  which is correct on *all* inputs (see e.g. [AB09, Sec. 8.6.2]). Thus, we have  $\text{PP} = \text{YQP}^*$ .

In this way, any level of the Counting Hierarchy  $\text{C}_i\text{P} = (\text{C}_{i-1}\text{P})^{\text{PP}}$  with  $i > 1$  is reducible to  $(\text{C}_{i-1}\text{P})^{\text{YQP}^*}$  which by Corollary 3.2 equals  $\text{C}_{i-1}\text{P}$ . This works recursively for all levels, collapsing  $\text{C}_i\text{P}$  to  $\text{C}_1\text{P} = \text{PP}$ , so that all of  $\text{CH} = \text{PP} = \text{YQP}^*$ .  $\square$

Given the above result, we can also fully recover the following result originally claimed by Aaronson [Aar06], giving an improved unconditional upper bound on fixed-size quantum circuits with quantum advice.

**Theorem 3.4.** *PP does not have quantum circuits of size  $n^k$  for any fixed  $k$ . Furthermore, this holds even if the circuits can use quantum advice.*

*Proof.* Suppose PP does have circuits of size  $n^k$ . This implies  $\text{PP} \subseteq \text{BQP}/\text{qpoly}$ , which by Theorem 3.3 implies  $\text{CH} = \text{YQP}^*$ , which includes  $\text{P}^{\text{PP}} = \text{PP} = \text{YQP}^*$ . Together, there are circuits of size  $n^k$  for  $\text{P}^{\text{PP}}$ , which contradicts the result of [Aar06, Theorem 4] (unaffected by the bug) that  $\text{P}^{\text{PP}}$  does not have such circuits even with quantum advice.  $\square$

In fact, [Aar06] noted that the proof showing  $\text{P}^{\text{PP}}$  does not have circuits of size  $n^k$  for fixed  $k$  even with quantum advice can be strengthened. Substituting this stronger result into the above proof, we have that Theorem 3.4 can be strengthened to show for all functions  $f(n) \leq 2^n$ , the class  $\text{PTIME}(f(f(n)))$ , which is like PP but for machines of running time  $f(f(n))$ , requires quantum circuits using quantum advice of size at least  $f(n)/n^2$ . In particular, this implies PEXP, the exponential-time version of PP, requires quantum circuits with quantum advice of “half-exponential” size (meaning a function that becomes exponential when composed with itself [MVW99]).

## References

- [Aar05] Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2063):3473–3482, 2005. doi:10.1098/rspa.2005.1546.
- [Aar06] Scott Aaronson. Oracles are subtle but not malicious. In *Proceedings of the 21st Annual IEEE Conference on Computational Complexity*, pages 340–354. IEEE Computer Society, 2006. doi:10.1109/CCC.2006.32.
- [Aar07] Scott Aaronson. The learnability of quantum states. *Proc. R. Soc. A.*, 463(2088):3089–3114, 2007. doi:10.1098/rspa.2007.0113.



- [Aar17] Scott Aaronson. Yet more errors in papers, May 2017. Accessed 14 Jan. 2024. URL: <https://scottaaronson.blog/?p=3256>.
- [AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: a Modern Approach*. Cambridge University Press, 2009.
- [AD14] Scott Aaronson and Andrew Drucker. A full characterization of quantum advice. *SIAM Journal on Computing*, 43(3):1131–1183, 2014. doi:10.1137/110856939.
- [AGKR24] Avantika Agarwal, Sevag Gharibian, Venkata Koppula, and Dorian Rudolph. Quantum polynomial hierarchies: Karp-Lipton, error reduction, and lower bounds, 2024. arXiv:2401.01633.
- [Fen03] Stephen A. Fenner. PP-lowness and a simple definition of AWPP. *Theory of Computing Systems*, 36:199–212, 2003. doi:10.1007/s00224-002-1089-8.
- [FR99] Lance Fortnow and John Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999. doi:10.1006/jcss.1999.1651.
- [FSW09] Lance Fortnow, Rahul Santhanam, and Ryan Williams. Fixed-polynomial size circuit bounds. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity*, pages 19–26. IEEE, 2009. doi:10.1109/CCC.2009.21.
- [GLV24] Karthik Gajulapalli, Zeyong Li, and Ilya Volkovich. Oblivious classes revisited: Lower bounds and hierarchies. ECCC: TR24-049, 2024. URL: <https://eccc.weizmann.ac.il/report/2024/049/>.
- [GM15] Oded Goldreich and Or Meir. Input-oblivious proof systems and a uniform complexity perspective on P/poly. *ACM Transactions on Computation Theory*, 7(4):1–13, 2015. doi:10.1145/2799645.
- [KL80] Richard M. Karp and Richard J. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proceedings of the 12th annual ACM Symposium on Theory of Computing*, pages 302–309, 1980. doi:10.1145/800141.804678.
- [Kup15] Greg Kuperberg. How hard is it to approximate the Jones polynomial? *Theory of Computing*, 11(1):183–219, 2015.
- [LFKN92] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM (JACM)*, 39(4):859–868, 1992. doi:10.1145/146585.146605.
- [Li93] Lide Li. *On the counting functions*. PhD thesis, The University of Chicago, 1993. URL: <https://www.proquest.com/dissertations-theses/on-counting-functions/docview/304080357/se-2>.
- [LP17] David A. Levin and Yuval Peres. *Markov chains and mixing times*, volume 107. American Mathematical Soc., 2017.
- [MN16] Tomoyuk Morimae and Harumichi Nishimura. Quantum interpretations of AWPP and APP. *Quantum Info. Comput.*, 16(5–6):498–514, 2016. doi:10.26421/QIC16.5-6-6.

- [MVW99] Peter Bro Miltersen, N. V. Vinodchandran, and Osamu Watanabe. Super-polynomial versus half-exponential circuit size in the Exponential Hierarchy. In *International Computing and Combinatorics Conference*, pages 210–220. Springer, 1999. doi:10.1007/3-540-48686-0\_21.
- [MW05] Chris Marriott and John Watrous. Quantum Arthur–Merlin games. *Computational Complexity*, 14:122–152, 2005. doi:10.1007/s00037-005-0194-x.
- [Vin05] N. V. Vinodchandran. A note on the circuit complexity of PP. *Theoretical Computer Science*, 347(1):415–418, 2005. doi:10.1016/j.tcs.2005.07.032.
- [Wat08] John Watrous. Quantum computational complexity, 2008. arXiv:0804.3401v1.
- [Wil14] Ryan Williams. Nonuniform ACC circuit lower bounds. *Journal of the ACM (JACM)*, 61(1):1–32, 2014. doi:10.1145/2559903.
- [Zoo] Complexity Zoo: BQP/poly, BQP/mpoly, BQP/qpoly, BQP. Accessed 13 Mar. 2024. URL: [https://complexityzoo.net/Complexity\\_Zoo:B](https://complexityzoo.net/Complexity_Zoo:B).