Electronic Colloquium on Computational Complexity, Report No. 52 (2024)

Even quantum advice is unlikely to solve PP

Justin Yirka
The University of Texas at Austin
yirka@utexas.edu

March 2024

Abstract

We give a corrected proof that if $\mathsf{PP} \subseteq \mathsf{BQP/qpoly}$, then the Counting Hierarchy collapses, as originally claimed by [Aaronson, CCC 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 YQP^*, an oblivious version of $\mathsf{QMA} \cap \mathsf{coQMA}$, is contained in APP, and so is PP-low.

1 Introduction

In [Aar06], Aaronson proved new quantum circuit lower bounds for PP, among other results. First, Aaronson proved that P^{PP} does not have circuits of size n^k for any fixed constant k even if the circuits use quantum advice states. Second, he gave an analogue of the Karp-Lipton theorem for quantum circuits, showing that if $\mathsf{PP} \subseteq \mathsf{BQP/qpoly}$, then the Counting Hierarchy collapses to QMA, where the Counting Hierarchy is the infinite sequence of classes $\mathsf{C_1P} = \mathsf{PP}$ and $\mathsf{C_iP} = (\mathsf{C_{i-1}P})^{\mathsf{PP}}$. Finally, Aaronson combined these two results to give the unconditional bound that PP does not have circuits of size n^k for any fixed constant k even with quantum advice.[1]

However, Aaronson later noted there was an error in one of the proofs [Aar17]. The first of the above results was unaffected, but the proofs of the second and third results only held for quantum circuits with classical 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 some oracle class $\mathsf{C}^{\mathsf{BQP/qpoly}}$ in which a machine for the base class C is able to find the quantum advice state that will be used by the oracle machine, the base machine could "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 $\mathsf{C}^{\mathsf{BQP/qpoly}}$ to $\mathsf{C}^{\mathsf{BQP}}$. This approach works for classes with classical advice, like $\mathsf{C}^{\mathsf{BQP/poly}}$. But, because complexity classes such as BQP and their associated oracles are defined as maps from $\{0,1\}^*$ to $\{0,1\}$, there is no way to hard-code a quantum advice state into a query.

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

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

ISSN 1433-8092

Our corrected proof relies on the known equality $\mathsf{BQP/qpoly} = \mathsf{YQP}^*\mathsf{/poly}$, serendipitously proven by Aaronson with Drucker [AD14], where YQP^* is an oblivious version of $\mathsf{QMA} \cap \mathsf{coQMA}$. Our primary technical contribution is to show $\mathsf{YQP}^* \subseteq \mathsf{APP}$, which is known to be PP-low, where APP is a subclass of PP with an arbitrarily small but nonzero promise gap.

For comparison, other Karp-Lipton style bounds on quantum complexity classes include that if $\mathsf{QCMA} \subseteq \mathsf{BQP/poly}$, then QCPH collapses [AGKR24] and that if $\mathsf{NP} \subseteq \mathsf{BQP/qpoly}$, then $\Pi_2^{\mathsf{p}} \subseteq \mathsf{QMA}^{\mathsf{PromiseQMA}}$ [AD14]. As for unconditional bounds, following Aaronson's unaffected result that P^{PP} does not have quantum circuits with quantum advice of any fixed polynomial size, our result for PP is the first improved bound on fixed-size circuits with quantum advice. Our primary lemma establishes YQP^* as the largest natural quantum complexity class known to be PP-low, improving on the fact that BQP is PP-low [FR99].[2] Additionally, while the largest witness-based class previously known to be contained in APP was FewP [Li93], our result shows that APP in fact contains oblivious-witness classes including $\mathsf{YQP}^* \supseteq \mathsf{YMA}^* \supseteq \mathsf{YP}^* \supseteq \mathsf{FewP}$.

2 Preliminaries

As this note builds directly on [Aar06] and [AD14], we intentionally give only a concise background. For further background, motivation, and technical details concerning the complexity classes discussed, see these earlier works.

Note that our definitions of $\mathsf{BQP/poly}$ and $\mathsf{BQP/qpoly}$ are the standard ones in which a circuit is only required to satisfy the promise gap when the correct advice is provided. 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 $\mathsf{QMA} \cap \mathsf{coQMA}$, so that the witness sent by Merlin depends only on the length of the input. In contrast to the "advice" of $\mathsf{P/poly}$, this has been described as "untrusted advice". Oblivious proofs can also be thought of as restricting non-uniform classes, like $\mathsf{P/poly}$ or $\mathsf{BQP/qpoly}$, 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 $\mathrm{poly}(n)$ and takes as input $x \in \{0,1\}^n$, a $p(n)$-qubit state ρ for some $p(n) \leq \mathrm{poly}(n)$, 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 $b_{\mathrm{adv}} \in \{0,1\}$.

2. Next, Y_n applies a second subcircuit B_n to all registers, then measures the output qubit, producing a value $b_{\mathrm{out}} \in \{0,1\}$.

These output bits satisfy the following:

- For all n, there exists a ρ_n such that for all x, the advice bit satisfies $\mathrm{E}[b_{\mathrm{adv}}] \geq 9/10$.

[2] Morimae and Nishimura [MN16] gave definitions involving quantum postselection chosen to equal AWPP and APP.

- If for any x, ρ we have $\mathrm{E}[b_{\text{adv}}] \geq 1/10$, then on input x, ρ 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_{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 $\mathsf{FewP} \subseteq \mathsf{YP}^*$ and $\mathsf{FewQMA} \subseteq \mathsf{YQP}^*$. We also have the trivial bounds $\mathsf{BQP} \subseteq \mathsf{YQP}^* \subseteq \mathsf{YQP} \subseteq \mathsf{QMA}$ and $\mathsf{YQP} \subseteq \mathsf{BQP/qpoly}$. Studying YQP may be motivated by the use of oblivious complexity classes in constructing circuit lower bounds [FSW09, GLV24], by the fact that $\mathsf{BQP/qpoly} = \mathsf{YQP}^*\mathsf{/poly} = \mathsf{YQP/poly}$ 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. $L \in \mathsf{APP}$ if and only if there exist functions $f, g \in \mathsf{GapP}$ and constants $0 \leq \lambda < \upsilon \leq 1$ such that for all n and $x \in \{0,1\}^n$, we have $g(1^n) > 0$ and

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

In the above definition, recall that GapP is the closure of #P under subtraction. In other words, while every function $f \in \#\mathsf{P}$ corresponds to a nondeterministic polynomial-time Turing Machine N such that $f(x)$ equals the number of accepting paths of $N(x)$, a 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 $\mathsf{PP}^{\mathsf{APP}} = \mathsf{PP}$. Recall that PP can be thought of as comparing a #P function to a threshold exactly, with no promise gap. The class in fact remains unchanged if it is defined as comparing a GapP function to a threshold as simple as one-half of the possible paths or as complex as a GapP function. Then, APP can be thought of as comparing a GapP function (here $f(x)$) to some threshold (here $g(1^n)$), where the complexity of the threshold is limited to a 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 $\upsilon g(1^n)$).

The best known upper bound on APP is PP. Compared with the class $\mathsf{A_0PP} = \mathsf{SBQP} \subseteq \mathsf{PP}$ [Kup15], $\mathsf{A_0PP}$ 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* 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 which will later allow us to prove Theorems 3.4 and 3.5.

Lemma 3.1. $\mathsf{YQP}^* \subseteq \mathsf{APP}$.

Proof. Consider any language $L \in \mathsf{YQP}^*$. 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_{adv}, and in which, given A_n accepted, B_n uses the advice to verify the particular input x and outputs bit b_{adv}. 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 ρ,

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

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'.

Remark 3.2. Studying the proof of [MW05], if the final recorded bit $y_{2M+1} = 1$, then the final state of the ancilla register was projected into the all-zero state. Additionally, suppose the circuit C' is applied to an m-qubit proof state, so there are 2^m eigenstate $\{|\lambda_i\rangle\}_{i\in[2^n]}$ of C'. Further studying the proof of [MW05], if the initial state given to C' was an eigenstate $|\lambda_i\rangle$ and after applying C' the final two recorded bits were $y_{2M} = y_{2M+1} = 1$, then the final state of the proof register is the same as the initial state, $|\lambda_i\rangle$. If an eigenstate $|\lambda_i\rangle$ was accepted by the original circuit C with probability p, then when C' is run on $|\lambda_i\rangle$, the probability that of $y_{2M} = y_{2M+1} = 1$ is at least $p \times \min\{p, 1-p\}$.

Combining all of the above, 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.

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

$$\Pr\left[A'''_n \text{ accepts}\right] = \frac{f(1^n)}{5^{r(n)}} \quad \text{and} \quad \Pr\left[Y'''_n(x) \text{ accepts}\right] = \frac{g(x)}{5^{t(n)}}.$$

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 $5^{t(n)-r(n)} \in \mathsf{FP} \subseteq \mathsf{GapP}$ and GapP is closed under multiplication. We have

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

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

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

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

$$\mathcal{B} = \left\{ i \in [2^m] \mid \Pr\left[A_n(|\lambda_i\rangle)\right] \le 0.1 \right\}.$$

Then we can rewrite both the numerator and denominator in the above ratio to give

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

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 $x \in L$. As this is YQP^*, 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

$$\frac{\sum_{i\in\mathcal{B}} 0 + \sum_{i\in\overline{\mathcal{B}}} \frac{9}{10} \Pr\left[A_n''(|\lambda_i\rangle) \text{ accepts}\right]}{\sum_{i\in\mathcal{B}} 2^{-q} + \sum_{i\in\overline{\mathcal{B}}} \Pr\left[A_n''(|\lambda_i\rangle) \text{ accepts}\right]} \ge \frac{\frac{9}{10} \Pr\left[A_n''(|\lambda^*\rangle) \text{ accepts}\right]}{|\mathcal{B}|\, 2^{-q} + \Pr\left[A_n''(|\lambda^*\rangle) \text{ accepts}\right]}$$

which, using the fact that $x/(c+x)$ decreases as x decreases as well as the bound stated in Remark 3.2 on the probability the error-reduction variables y_{2M}, y_{2M+1} are 1, is at least

$$\frac{\frac{9}{10}(1-2^{-q})(0.9)(0.1)}{|\mathcal{B}|\, 2^{-q} + (1-2^{-q})(0.9)(0.1)} = \frac{0.081(1-2^{-q})}{2^{m-q} + 0.09(1-2^{-q})}$$
$$\ge \frac{0.081(1-2^{-q})}{2^{-q/2} + 0.09(1-2^{-q})} \ge \frac{0.081(1-2^{-10})}{2^{-5} + 0.09(1-2^{-10})} > 0.66,$$

where in the last line we used our freedom to choose the polynomial q.

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

$$\frac{|\mathcal{B}| \times 1 \times 2^{-q} + |\overline{\mathcal{B}}| \times \frac{1}{10} \times 1}{2^m \Pr[A_n''' \text{ accepts}]} \leq \frac{2^m 2^{-q} + 2^m \frac{1}{10}}{2^m} = 2^{-q} + \frac{1}{10} \leq 0.2.$$

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 $\mathsf{YQP}^* \subseteq \mathsf{APP}$. □

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

Corollary 3.3. YQP^* *is* PP*-low, i.e.* $\mathsf{PP}^{\mathsf{YQP}^*} = \mathsf{PP}$.

We are now able to give a corrected proof of the result originally claimed for $\mathsf{BQP/qpoly}$ but only proved for $\mathsf{BQP/poly}$ by Aaronson [Aar06].

Theorem 3.4. *If* $\mathsf{PP} \subseteq \mathsf{BQP/qpoly}$*, then the Counting Hierarchy collapses to* $\mathsf{CH} = \mathsf{QMA} = \mathsf{YQP}^*$*.*

Proof. We repeat Aaronson's original claimed proof [Aar06], but substitute YQP^* where he relied on QMA.

Suppose $\mathsf{PP} \subseteq \mathsf{BQP/qpoly}$. From [AD14], we know that $\mathsf{BQP/qpoly} = \mathsf{YQP}^*\mathsf{/poly}$. Then in YQP^*, without trusted classical 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 $\#\mathsf{P}$ due to [LFKN92], which also works for PP, using $C, |\psi\rangle$ in place of the prover. If the protocol accepts, 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 $\mathsf{PP} = \mathsf{YQP}^*$.

In this way, any level of the Counting Hierarchy $\mathsf{C_iP} = (\mathsf{C_{i-1}P})^{\mathsf{PP}}$ with $i > 1$ is reducible to $(\mathsf{C_{i-1}P})^{\mathsf{YQP}^*}$ which by Corollary 3.3 equals $\mathsf{C_{i-1}P}$. This works recursively for all levels, collapsing $\mathsf{C_iP}$ to $\mathsf{C_1P} = \mathsf{PP}$, so that all of $\mathsf{CH} = \mathsf{PP} = \mathsf{YQP}^*$. □

Given the above result, we can also fully recover the following result originally claimed by Aaronson [Aar06].

Theorem 3.5. 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 $\mathsf{PP} \subseteq \mathsf{BQP/qpoly}$, which by Theorem 3.4 implies $\mathsf{CH} = \mathsf{YQP}^*$, which includes $\mathsf{P}^{\mathsf{PP}} = \mathsf{PP} = \mathsf{YQP}^*$. Together, there are circuits of size n^k for P^{PP}, which contradicts the result of [Aar06] (unaffected by the bug) that P^{PP} does not have such circuits even with quantum advice. □

In fact, as [Aar06] observes, because his proof that P^{PP} does not have circuits of size n^k for fixed k can be strengthened, we have that Theorem 3.5 can be strengthened to show for all functions $f(n) \leq 2^n$, the class $\mathsf{PTIME(f(f(n)))}$, 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

[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.

[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.

[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.

[Zoo] Complexity Zoo: BQP/poly, BQP/mpoly, BQP/qpoly, BQP. Accessed 13 Mar. 2024. URL: https://complexityzoo.net/Complexity_Zoo:B.

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il