Quantum Computing, Postselection, and Probabilistic Polynomial-Time

Scott Aaronson*
Institute for Advanced Study, Princeton, NJ (USA)
aaronson@ias.edu

Abstract

I study the class of problems efficiently solvable by a quantum computer, given the ability to "postselect" on the outcomes of measurements. I prove that this class coincides with a classical complexity class called PP, or Probabilistic Polynomial-Time. Using this result, I show that several simple changes to the axioms of quantum mechanics would let us solve PP-complete problems efficiently. The result also implies, as an easy corollary, a celebrated theorem of Beigel, Reingold, and Spielman that PP is closed under intersection, as well as a generalization of that theorem due to Fortnow and Reingold. This illustrates that quantum computing can yield new and simpler proofs of major results about classical computation.

Keywords: quantum computing, computational complexity, postselection.

1 Introduction

Postselection is the power of discarding all runs of a computation in which a given event does not occur. To illustrate, suppose we are given a Boolean formula in a large number of variables, and we wish to find a setting of the variables that makes the formula true. Provided such a setting exists, this problem is easy to solve using postselection: we simply set the variables randomly, then postselect on the formula being true.

This paper studies the power of postselection in a quantum computing context. I define a new complexity class called PostBQP (Postselected Bounded-Error Quantum Polynomial-Time), which consists of all problems solvable by a quantum computer in polynomial time, given the ability to postselect on a measurement yielding a specific outcome. The main result is that PostBQP equals the well-known classical complexity class PP (Probabilistic Polynomial-Time). Here PP is the class of problems for which there exists a probabilistic polynomial-time Turing machine that accepts with probability greater than $1/2$ if and only if the answer is 'yes.' For example, given a Boolean formula, a PP machine can decide whether the *majority* of settings to the variables make the formula true. Indeed, this problem turns out to be PP-complete (that is, among the hardest problems in PP).[1]

The motivation for the PostBQP = PP result comes from two quite different sources. The original motivation was to analyze the computational power of "fantasy" versions of quantum mechanics, and thereby gain insight into why quantum mechanics is the way it is. In particular, Section 4 will show that if we changed the measurement probability rule from $|\psi|^2$ to $|\psi|^p$ for some $p \neq 2$, or allowed linear but nonunitary evolution, then we could simulate postselection, and thereby solve PP-complete problems in polynomial time. If we consider such an ability extravagant, then we might take these results as helping to explain why quantum mechanics is unitary, and why the measurement rule is $|\psi|^2$.

A related motivation comes from an idea that might be called *anthropic computing*—arranging things so that we are more likely to exist if a computer produces a desired output than if it does not. As a simple example, under the many-worlds interpretation of quantum mechanics, we might kill ourselves in all universes

*Part of this work was done while I was a graduate student at the University of California, Berkeley, CA (USA), supported by an NSF Graduate Fellowship.

[1]See the "Complexity Zoo" (www.complexityzoo.com) for more information about the complexity classes mentioned in this paper.

where a computer fails! My result implies that, using this "technique," we could solve not only NP-complete problems efficiently, but PP-complete problems as well.

However, the PostBQP = PP result also has a more unexpected implication. One reason to study quantum computing is to gain a new, more general perspective on *classical* computer science. By analogy, many famous results in computer science involve only deterministic computation, yet it is hard to imagine how anyone could have proved these results had researchers not long ago "taken aboard" the notion of randomness.[2] Likewise, taking quantum mechanics aboard has already led to some new results about classical computation [4, 9, 25, 29]. What this paper will show is that, even when classical results are already known, quantum computing can sometimes provide new and simpler proofs for them.

When Gill [19, 20] defined PP in 1972, he also asked a notorious question that remained open for eighteen years: is PP closed under intersection?[3] In other words, given two probabilistic polynomial-time Turing machines A and B, does there exist another such machine that accepts with probability greater than $1/2$ if and only if A and B both do? The question was finally answered in the affirmative by Beigel, Reingold, and Spielman [11], who introduced a brilliant technique for representing the logical AND of two majority functions by the sign of a low-degree rational function. Fortnow and Reingold [17] later extended the technique to show that PP is closed under "polynomial-time truth-table reductions." This means that a polynomial-time Turing machine that makes nonadaptive queries to a PP oracle is no more powerful than PP itself. (Note that a query is "nonadaptive" if it does not depend on the answers to previous queries. Beigel [10] has given evidence that the Fortnow-Reingold result does not generalize to adaptive queries.)

Now the class PostBQP is trivially closed under intersection, as well as under polynomial-time truth-table reductions. So the fact that PostBQP = PP immediately implies the Beigel et al. [10] and Fortnow-Reingold [17] results. Indeed, it even implies that PP is closed under *quantum* polynomial-time truth-table reductions, which seems to be a new result. In my view, the PostBQP = PP proof is conceptually simpler than Beigel et al.'s original proof, since (for example) it makes no explicit use of rational functions. (Although, as pointed out to me by Richard Beigel, a result on rational functions similar to those in [11] could be *extracted* from the proof of my result.)

This paper is based on chapter 15 of my PhD thesis [3]. Some of the results appeared in preliminary form in [1], before I made the connection to showing PP closed under intersection.

2 Related Work

Besides PostBQP, several other "nondeterministic" versions of BQP have appeared in the literature. Adleman, DeMarrais, and Huang [6] defined NQP to be the class of problems for which there exists a polynomial-time quantum algorithm that accepts with nonzero probability if and only if the answer is 'yes.' Then, in a result reminiscent of this paper's, Fenner et al. [15] showed that NQP equals a classical class called $\mathsf{coC_{=}P}$.[4] Also, Watrous [34] defined QMA as the class of problems for which a polynomial-time quantum verifier can be convinced of a 'yes' answer by a polynomial-size quantum proof. If we require the proof to be classical, then we obtain the apparently weaker class QCMA, defined by Aharonov and Naveh [8]. Note that all of these classes are contained in PP [34], and hence in PostBQP.

The idea of postselection has recurred several times in quantum computing. For example, Terhal and DiVincenzo [33] used postselection to show that constant-depth quantum circuits are probably hard to simulate, and I [2] used it to show that $\mathsf{BQP/qpoly} \subseteq \mathsf{PP/poly}$ (that is, any problem solvable in BQP with polynomial-size quantum advice, is also solvable in PP with polynomial-size classical advice).

If we add postselection to a *classical* probabilistic polynomial-time Turing machine, then we obtain a complexity class known as $\mathsf{BPP_{path}}$, which was defined by Han, Hemaspaandra, and Thierauf [23] and which sits somewhere between MA and PP (MA being a probabilistic generalization of NP).

Fortnow [16] reports that in 1990, he, Fenner, and Kurtz tried to show PP closed under intersection by (1) defining a seemingly weaker class, (2) showing that class closed under intersection, and then (3) showing that it actually equals PP. The attempt failed, and soon thereafter Beigel et al. [10] succeeded with a quite

[2] A few examples are primality testing in deterministic polynomial time [7], undirected graph connectivity in log-space [30], and inapproximability of the 3-SAT problem unless P = NP [32].

[3] It is clear that PP is closed under complement, so this question is equivalent to asking whether PP is closed under union.

[4] Unfortunately, I do not know of any classical result that this helps to prove. That $\mathsf{coC_{=}P}$ is closed under union and intersection is obvious.

different approach. This paper could be seen as a vindication of Fortnow et al.'s original approach—all it was missing was quantum mechanics! Admittedly, Li [27] gave another proof along Fortnow et al.'s lines in 1993. However, Li's proof makes heavy use of rational functions, and seems less intuitive than the one here.

3 The Class PostBQP

In what follows, I assume basic familiarity with quantum computing, and in particular with the class BQP (Bounded-Error Quantum Polynomial Time) defined by Bernstein and Vazirani [12]. It is now time to define PostBQP more formally.

Definition 1 PostBQP *is the class of languages $L \subseteq \{0,1\}^*$ for which there exists a uniform family of polynomial-size quantum circuits $\{C_n\}_{n\geq 1}$ such that for all inputs x,*

(i) After C_n is applied to the state $|0\cdots 0\rangle \otimes |x\rangle$, the first qubit has a nonzero probability of being measured to be $|1\rangle$.

(ii) If $x \in L$, then conditioned on the first qubit being $|1\rangle$, the second qubit is $|1\rangle$ with probability at least $2/3$.

(iii) If $x \notin L$, then conditioned on the first qubit being $|1\rangle$, the second qubit is $|1\rangle$ with probability at most $1/3$.

Here 'uniform' means that there exists a classical algorithm that outputs a description of C_n in time polynomial in n. Note that, by a result of Shi [31], we can assume without loss of generality that C_n is composed only of Hadamard and Toffoli gates. (This is true even for a postselected quantum circuit, since by the Solovay-Kitaev Theorem [26], we can achieve the needed accuracy in amplitudes at the cost of a polynomial increase in circuit size.)

It is easy to see that NP $\subseteq$ PostBQP. For given a Boolean formula φ with n variables, to decide whether φ has any satisfying assignments we can first generate the state

$$\frac{1}{2^n}|1\rangle|0\rangle|0\rangle + \frac{\sqrt{1-2^{-2n}}}{2^{n/2}} \sum_{x\in\{0,1\}^n} |\varphi(x)\rangle|1\rangle|x\rangle,$$

where $\varphi(x) = 1$ if the assignment x satisfies φ and $\varphi(x) = 0$ otherwise. We then postselect on the first qubit being $|1\rangle$. If φ has no satisfying assignments, then the second qubit will be $|0\rangle$ with certainty; while if φ has one or more satisfying assignments, then the second qubit will be $|1\rangle$ with probability at least $1-2^{-n}$.

To show PostBQP $\subseteq$ PP, we can use the same observations used by Adleman, DeMarrais, and Huang [6] to show that BQP $\subseteq$ PP, but sum only over paths where the first qubit is $|1\rangle$ at the end. In more detail:

Proposition 2 PostBQP $\subseteq$ PP.

Proof. Assume that our quantum circuit is composed of Hadamard and Toffoli gates. Then the final amplitude α_z of each basis state $|z\rangle$ can be written as a sum of exponentially many contributions, call them $a_{z,1},\ldots,a_{z,N}$, each of which is a rational real number computable in classical polynomial time. So the final probability of $|z\rangle$ equals

$$\alpha_z^2 = (a_{z,1} + \cdots + a_{z,n})^2 = \sum_{ij} a_{z,i}a_{z,j}.$$

We need to test which is greater: the sum S_0 of α_z^2 over all z beginning with 10, or the sum S_1 of α_z^2 over all z beginning with 11. We can do this in PP as follows. For $k \in \{0,1\}$, let

$$S_k^+ = \sum_{\substack{z=1k\cdots,\\ ij: a_{z,i}a_{z,j}\geq 0}} a_{z,i}a_{z,j}$$

$$S_k^- = \sum_{\substack{z=1k\cdots,\\ ij: a_{z,i}a_{z,j}< 0}} a_{z,i}a_{z,j}$$

Then $S_0 = S_0^+ + S_0^-$ and $S_1 = S_1^+ + S_1^-$. So to test whether $S_0 > S_1$, it suffices to test whether $S_0^+ - S_1^- > S_1^+ - S_0^-$. Note that $S_0^+ - S_1^-$ and $S_1^+ - S_0^-$ are both sums of nonnegative terms, and thus are representable as the number of accepting and rejecting paths respectively of a PP machine (times some normalizing constant). ■

How robust is PostBQP? Just as Bernstein and Vazirani [12] showed that intermediate measurements do not increase the power of ordinary quantum computers, so it is easily shown that intermediate postselection steps do not increase the power of PostBQP. Whenever we want to postselect on a qubit j being $|1\rangle$, we simply apply a CNOT gate from j into a fresh ancilla qubit that is initialized to $|0\rangle$ and that will never be written to again. Then, at the end, we compute the AND of the ancilla qubits, and swap the result into the first qubit. By a standard Chernoff bound, it follows that we can repeat a PostBQP computation a polynomial number of times, and thereby reduce the error probability from $1/3$ to $1 - 2^{-p(n)}$ for any polynomial p.

A corollary of the above observations is that PostBQP has strong closure properties.

Proposition 3 PostBQP *is closed under union, intersection, and complement. Indeed, it is closed under* BQP *truth-table reductions. This means that* $\mathsf{PostBQP} = \mathsf{BQP}_{\|,\text{classical}}^{\mathsf{PostBQP}}$*, where* $\mathsf{BQP}_{\|,\text{classical}}^{\mathsf{PostBQP}}$ *is the class of problems solvable by a machine that can make a polynomial number of nonadaptive classical queries to a* PostBQP *oracle, followed by a polynomial-time quantum computation.*

Proof. Clearly PostBQP is closed under complement, since the definition is symmetric with respect to $x \in L$ and $x \notin L$. For closure under intersection, let $L_1, L_2 \in \mathsf{PostBQP}$; then we need to decide whether $x \in L_1 \cap L_2$. Run amplified computations (with error probability at most $1/6$) to decide if $x \in L_1$ and if $x \in L_2$, postselect on both computations succeeding, and accept if and only if both accept. It follows that PostBQP is closed under union as well.

In general, suppose a $\mathsf{BQP}_{\|,\text{classical}}^{\mathsf{PostBQP}}$ machine M submits queries $q_1, \ldots, q_{p(n)}$ to the PostBQP oracle. Then run amplified computations (with error probability at most, say, $\frac{1}{10p(n)}$) to decide the answers to these queries, and postselect on all $p(n)$ of them succeeding. By the union bound, if M had error probability ε with a perfect PostBQP oracle, then its new error probability is at most $\varepsilon + 1/10$, which can easily be reduced through amplification. ■

One might wonder why Proposition 3 does not go through with *adaptive* queries. The reason is subtle: suppose we have two PostBQP computations, the second of which relies on the output of the first. Then even if the first computation is amplified a polynomial number of times, it still has an exponentially small probability of error. But since the second computation uses postselection, *any* nonzero error probability could be magnified arbitrarily, and is therefore too large.

I now prove the main result.

Theorem 4 PostBQP = PP.

Proof. We have already observed that PostBQP $\subseteq$ PP. For the other direction, let $f : \{0,1\}^n \to \{0,1\}$ be an efficiently computable Boolean function, and let $s = |\{x : f(x) = 1\}|$. Then we need to decide in PostBQP whether $s < 2^{n-1}$ or $s \geq 2^{n-1}$. (As a technicality, we can guarantee using padding that $s > 0$.)

The algorithm is as follows: first prepare the state $2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$. Then following Abrams and Lloyd [5], apply Hadamard gates to all n qubits in the first register and postselect[5] on that register being $|0\rangle^{\otimes n}$. This produces the state $|0\rangle^{\otimes n} |\psi\rangle$ where

$$|\psi\rangle = \frac{(2^n - s)|0\rangle + s|1\rangle}{\sqrt{(2^n - s)^2 + s^2}}.$$

Next, for some positive real numbers α, β to be specified later, prepare $\alpha |0\rangle |\psi\rangle + \beta |1\rangle H |\psi\rangle$ where

$$H|\psi\rangle = \frac{\sqrt{1/2}\,(2^n)|0\rangle + \sqrt{1/2}\,(2^n - 2s)|1\rangle}{\sqrt{(2^n - s)^2 + s^2}}$$

[5] Postselection is actually overkill here, since the first register has at least $1/4$ probability of being $|0\rangle^{\otimes n}$.

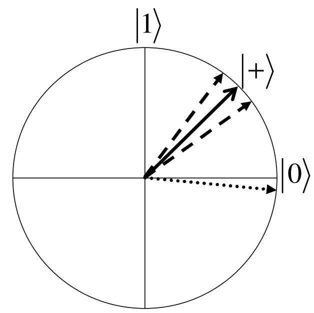

Figure 1: If s and $2^n - 2s$ are both positive, then as we vary the ratio of β to α, we eventually get close to $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ (dashed lines). On the other hand, if $2^n - 2s$ is not positive (dotted line), then we never even get into the first quadrant.

is the result of applying a Hadamard gate to $|\psi\rangle$. Then postselect on the second qubit being $|1\rangle$. This yields the reduced state

$$\left|\varphi_{\beta/\alpha}\right\rangle = \frac{\alpha s\,|0\rangle + \beta\sqrt{1/2}\,(2^n - 2s)\,|1\rangle}{\sqrt{\alpha^2 s^2 + (\beta^2/2)\,(2^n - 2s)^2}}$$

in the first qubit.

Suppose $s < 2^{n-1}$, so that s and $\sqrt{1/2}\,(2^n - 2s)$ are both at least 1. Then we claim there exists an integer $i \in [-n, n]$ such that, if we set $\beta/\alpha = 2^i$, then $|\varphi_{2^i}\rangle$ is close to the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$:

$$|\langle + | \varphi_{2^i}\rangle| \geq \frac{1+\sqrt{2}}{\sqrt{6}} > 0.985.$$

For since $\sqrt{1/2}\,(2^n - 2s)/s$ lies between 2^{-n} and 2^n, there must be an integer $i \in [-n, n-1]$ such that $|\varphi_{2^i}\rangle$ and $|\varphi_{2^{i+1}}\rangle$ fall on opposite sides of $|+\rangle$ in the first quadrant (see Figure 1). So the worst case is that $\langle + | \varphi_{2^i}\rangle = \langle + | \varphi_{2^{i+1}}\rangle$, which occurs when $|\varphi_{2^i}\rangle = \sqrt{2/3}\,|0\rangle + \sqrt{1/3}\,|1\rangle$ and $|\varphi_{2^{i+1}}\rangle = \sqrt{1/3}\,|0\rangle + \sqrt{2/3}\,|1\rangle$. On the other hand, suppose $s \geq 2^{n-1}$, so that $\sqrt{1/2}\,(2^n - 2s) \leq 0$. Then $|\varphi_{2^i}\rangle$ never lies in the first or third quadrants, and therefore $|\langle + | \varphi_{2^i}\rangle| \leq 1/\sqrt{2} < 0.985$.

It follows that, by repeating the whole algorithm $n(2n+1)$ times (as in Proposition 3), with n invocations for each integer $i \in [-n, n]$, we can learn whether $s < 2^{n-1}$ or $s \geq 2^{n-1}$ with exponentially small probability of error. ■

Combining Proposition 3 with Theorem 4 immediately yields that PP is closed under intersection, as well as under BQP truth-table reductions.[6]

4 Fantasy Quantum Mechanics

Is quantum mechanics an island in theoryspace? By "theoryspace," I mean the space of logically conceivable physical theories, with two theories close to each other if they differ in few respects. An "island" in theoryspace is then a natural and interesting theory, whose neighbors are all somehow perverse or degenerate. The Standard Model is not an island, because we do not know of any compelling (non-anthropic) reason why the

[6] Another corollary is a result of Fortnow and Rogers [18] that BQP is "low" for PP; that is, $\mathsf{PP}^{\mathsf{BQP}} = \mathsf{PP}$. For clearly $\mathsf{PostBQP}^{\mathsf{BQP}} = \mathsf{PostBQP}$.

masses and coupling constants should have the values they do. Likewise, general relativity is probably not an island, because of alternatives such as the Brans-Dicke theory.

To many physicists, however, quantum mechanics *does* seem like an island: change any one aspect, and the whole theory becomes inconsistent or nonsensical. There are many mathematical results supporting this opinion: for example, Gleason's Theorem [22] and other "derivations" of the $|\psi|^2$ probability rule [14, 35]; arguments for why amplitudes should be complex numbers, as opposed to (say) real numbers or quaternions [1, 13, 24]; and "absurd" consequences of allowing nonlinear transformations between states [5, 21, 28]. The point of these results is to provide some sort of explanation for why quantum mechanics has the properties it does.

In 1998, Abrams and Lloyd [5] suggested that computational complexity could also be pressed into such an explanatory role. In particular, they showed that under almost any nonlinear variant of quantum mechanics, one could build a "nonlinear quantum computer" able to solve NP-complete and even $\#\mathsf{P}$-complete problems in polynomial time.[7] One interpretation of their result is that we should look very hard for nonlinearities in experiments! But a different interpretation, the one I prefer, is that their result provides independent evidence that quantum mechanics is linear.

This section builds on Theorem 4 to offer similar "evidence" that quantum mechanics is unitary, and that the measurement rule is $|\psi|^2$.

Let $\mathsf{BQP}_{\mathsf{nu}}$ be the class of problems solvable by a uniform family of polynomial-size, bounded-error quantum circuits, where the circuits can consist of arbitrary 1- and 2-qubit *invertible* linear transformations, rather than just unitary transformations. Immediately before a measurement, the amplitude α_x of each basis state $|x\rangle$ is divided by $\sqrt{\sum_y |\alpha_y|^2}$ to normalize it.

Proposition 5 *$\mathsf{BQP}_{nu} = \mathsf{PP}$.*

Proof. The inclusion $\mathsf{BQP}_{\mathsf{nu}} \subseteq \mathsf{PP}$ follows easily from Adleman, DeMarrais, and Huang's proof that $\mathsf{BQP} \subseteq \mathsf{PP}$ [6], which does not depend on unitarity. For the other direction, by Theorem 4 it suffices to show that $\mathsf{PostBQP} \subseteq \mathsf{BQP}_{\mathsf{nu}}$. To postselect on a qubit being $|1\rangle$, simply apply the 1-qubit nonunitary operation

$$\begin{pmatrix} 2^{-q(n)} & 0 \\ 0 & 1 \end{pmatrix}$$

for some sufficiently large polynomial q. ■

Next, for any nonnegative real number p, define BQP_p similarly to BQP, except that when we measure, the probability of obtaining a basis state $|x\rangle$ equals $|\alpha_x|^p / \sum_y |\alpha_y|^p$ rather than $|\alpha_x|^2$. Thus $\mathsf{BQP}_2 = \mathsf{BQP}$. Assume that all gates are unitary and that there are no intermediate measurements, just a single standard-basis measurement at the end.

Theorem 6 *$\mathsf{PP} \subseteq \mathsf{BQP}_p \subseteq \mathsf{PSPACE}$ for all constants $p \neq 2$, with $\mathsf{BQP}_p = \mathsf{PP}$ when $p \in \{4, 6, 8, \ldots\}$.*

Proof. To simulate PP in BQP_p, run the algorithm of Theorem 4, having initialized $O\left(n^2 q(n) / |2-p|\right)$ ancilla qubits to $|0\rangle$ for some sufficiently large polynomial q. Suppose the algorithm's state at some point is $\sum_z \alpha_z |z\rangle$, and we want to postselect on the event $|z\rangle \in \mathcal{S}$, where $\mathcal{S}$ is a subset of basis states. Here is how: if $p < 2$, then apply Hadamard gates to $K = 2q(n) / (2-p)$ fresh ancilla qubits conditioned on $|z\rangle \in \mathcal{S}$. The result is to increase the "probability mass" of each $|z\rangle \in \mathcal{S}$ from $|\alpha_z|^p$ to

$$2^K \cdot \left|2^{-K/2} \alpha_z\right|^p = 2^{(2-p)K/2} |\alpha_z|^p = 2^{q(n)} |\alpha_z|^p,$$

while the probability mass of each $|z\rangle \notin \mathcal{S}$ remains unchanged. Similarly, if $p > 2$, then apply Hadamard gates to $K = 2q(n) / (p-2)$ fresh ancilla qubits conditioned on $|z\rangle \notin \mathcal{S}$. This decreases the probability mass of each $|z\rangle \notin \mathcal{S}$ from $|\alpha_z|^p$ to $2^K \cdot \left|2^{-K/2}\alpha_z\right|^p = 2^{-q(n)} |\alpha_z|^p$, while the probability mass of each $|x\rangle \in \mathcal{S}$ remains unchanged. The final observation is that Theorem 4 still goes through if $p \neq 2$. For it suffices to

[7] A caveat is that it remains an open problem whether this can be done fault-tolerantly. The answer might depend on the allowed types of nonlinear gate. On the other hand, if arbitrary 1-qubit nonlinear gates can be implemented without error, then even PSPACE-complete problems can be solved in polynomial time. This is tight, since nonlinear quantum computers are not hard to simulate in PSPACE.

distinguish the case $|\langle+|\varphi_{2^i}\rangle| > 0.985$ from $|\langle+|\varphi_{2^i}\rangle| \leq 1/\sqrt{2}$ with exponentially small probability of error, using polynomially many copies of the state $|\varphi_{2^i}\rangle$. But we can do this for any p, since all $|\psi|^p$ rules behave well under tensor products (in the sense that $|\alpha\beta|^p = |\alpha|^p |\beta|^p$).

The inclusion $\mathsf{BQP}_p \subseteq \mathsf{PSPACE}$ follows easily from the techniques used by Bernstein and Vazirani [12] to show $\mathsf{BQP} \subseteq \mathsf{PSPACE}$. Let $\mathcal{S}$ be the set of accepting states; then simply compute $\sum_{z\in S} |\alpha_z|^p$ and $\sum_{z\notin S} |\alpha_z|^p$ and see which is greater.

To simulate BQP_p in PP when $p \in \{4, 6, 8, \ldots\}$, we generalize the result of Adleman, DeMarrais, and Huang [6], which handled the case $p = 2$. As in Proposition 2, we can write each amplitude α_z as a sum of exponentially many contributions, $a_{z,1} + \cdots + a_{z,N}$, where each $a_{z,i}$ is a rational real number computable in classical polynomial time. Then letting $\mathcal{S}$ be the set of accepting states, it suffices to test whether

$$\begin{aligned}
\sum_{z\in\mathcal{S}} |\alpha_z|^p &= \sum_{z\in\mathcal{S}} \alpha_z^p \\
&= \sum_{z\in\mathcal{S}} \left(\sum_{i\in\{1,\ldots,N\}} a_{z,i} \right)^p \\
&= \sum_{z\in\mathcal{S}} \sum_{B\subseteq\{1,\ldots,N\},|B|=p} \prod_{i\in B} a_{z,i}
\end{aligned}$$

is greater than $\sum_{z\notin\mathcal{S}} |\alpha_z|^p$. We can do this in PP by separating out the positive and negative contributions $\prod_{i\in B} a_{z,i}$, exactly as in Proposition 2. ■

5 Open Problems

What other classical complexity classes can we characterize in quantum terms, and what other questions can we answer by that means? A first step might be to prove even stronger closure properties for PP. For example, let $\mathsf{BQP}_{\parallel}^{\mathsf{PostBQP}}$ be the class of problems solvable by a BQP machine that can make a single *quantum* query, which consists of a list of polynomially many questions for a $\mathsf{PostBQP}$ oracle. Then does $\mathsf{BQP}_{\parallel}^{\mathsf{PostBQP}}$ equal $\mathsf{PostBQP}$? The difficulty in showing this seems to be uncomputing garbage qubits after the $\mathsf{PostBQP}$ oracle is simulated.

As for fantasy quantum mechanics, an interesting open question is whether $\mathsf{BQP}_p = \mathsf{PP}$ for all nonnegative real numbers $p \neq 2$. A natural idea for simulating BQP_p in PP would be to use a Taylor series expansion for the probability masses $|\alpha_x|^p$. Unfortunately, I have no idea how to get fast enough convergence.

6 Acknowledgments

I thank Avi Wigderson for helpful discussions, Richard Beigel and Lance Fortnow for correspondence, and the anonymous reviewers for their comments.

References

[1] S. Aaronson. Is quantum mechanics an island in theoryspace? In A. Khrennikov, editor, *Proceedings of the Växjö Conference "Quantum Theory: Reconsideration of Foundations"*, 2004. quant-ph/0401062.

[2] S. Aaronson. Limitations of quantum advice and one-way communication. *Theory of Computing*, 2004. To appear. Conference version in *Proc. IEEE Complexity 2004*, pp. 320-332. quant-ph/0402095.

[3] S. Aaronson. *Limits on Efficient Computation in the Physical World*. PhD thesis, University of California, Berkeley, 2004.

[4] S. Aaronson. Lower bounds for local search by quantum arguments. In *Proc. ACM STOC*, pages 465–474, 2004. ECCC TR03-057, quant-ph/0307149.

[5] D. S. Abrams and S. Lloyd. Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems. *Phys. Rev. Lett.*, 81:3992–3995, 1998. quant-ph/9801041.

[6] L. Adleman, J. DeMarrais, and M.-D. Huang. Quantum computability. *SIAM J. Comput.*, 26(5):1524–1540, 1997.

[7] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. www.cse.iitk.ac.in/users/manindra/primality.ps, 2002.

[8] D. Aharonov and T. Naveh. Quantum NP - a survey. quant-ph/0210077, 2002.

[9] D. Aharonov and O. Regev. Lattice problems in NP intersect coNP. In *Proc. IEEE FOCS*, pages 362–371, 2004.

[10] R. Beigel. Perceptrons, PP, and the polynomial hierarchy. *Computational Complexity*, 4:339–349, 1994.

[11] R. Beigel, N. Reingold, and D. Spielman. PP is closed under intersection. *J. Comput. Sys. Sci.*, 50(2):191–202, 1995.

[12] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26(5):1411–1473, 1997. First appeared in ACM STOC 1993.

[13] C. M. Caves, C. A. Fuchs, and R. Schack. Unknown quantum states: the quantum de Finetti representation. *J. Math. Phys.*, 45(9):4537–4559, 2002. quant-ph/0104088.

[14] D. Deutsch. Quantum theory of probability and decisions. *Proc. Roy. Soc. London*, A455:3129–3137, 1999. quant-ph/9906015.

[15] S. Fenner, F. Green, S. Homer, and R. Pruim. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy. *Proc. Roy. Soc. London*, A455:3953–3966, 1999. quant-ph/9812056.

[16] L. Fortnow. My Computational Complexity Web Log. Wednesday, October 30, 2002 entry. fortnow.com/lance/complog.

[17] L. Fortnow and N. Reingold. PP is closed under truth-table reductions. *Information and Computation*, 124(1):1–6, 1996.

[18] L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *J. Comput. Sys. Sci.*, 59(2):240–252, 1999. cs.CC/9811023.

[19] J. Gill. *Probabilistic Turing Machines and Complexity of Computation.* PhD thesis, University of California, Berkeley, 1972.

[20] J. Gill. Computational complexity of probabilistic Turing machines. *SIAM J. Comput.*, 6:675–695, 1977.

[21] N. Gisin. Weinberg's non-linear quantum mechanics and superluminal communications. *Phys. Lett. A*, 143:1–2, 1990.

[22] A. M. Gleason. Measures on the closed subspaces of a Hilbert space. *J. Math. Mech.*, 6:885–893, 1957.

[23] Y. Han, L. Hemaspaandra, and T. Thierauf. Threshold computation and cryptographic security. *SIAM J. Comput.*, 26(1):59–78, 1997.

[24] L. Hardy. Quantum theory from five reasonable axioms. quant-ph/0101012, 2003.

[25] I. Kerenidis and R. de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. In *Proc. ACM STOC*, pages 106–115, 2003. quant-ph/0208062.

[26] A. Kitaev. Quantum computation: algorithms and error correction. *Russian Math. Surveys*, 52(6):1191–1249, 1997.

[27] L. Li. *On the Counting Functions.* PhD thesis, University of Chicago, 1993. At www.cs.uchicago.edu/files/tr_authentic/TR-93-12.ps.

[28] J. Polchinski. Weinberg's nonlinear quantum mechanics and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.*, 66:397–400, 1991.

[29] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. Submitted, 2004.

[30] O. Reingold. Undirected ST-connectivity in log-space. 2004.

[31] Y. Shi. Both Toffoli and controlled-NOT need little help to do universal quantum computation. *Quantum Information and Computation*, 3(1):84–92, 2002. quant-ph/0205115.

[32] J. Håstad. Some optimal inapproximability results. *J. ACM*, 48:798–859, 2001.

[33] B. M. Terhal and D. P. DiVincenzo. Adaptive quantum computation, constant-depth circuits and Arthur-Merlin games. *Quantum Information and Computation*, 4(2):134–145, 2004. quant-ph/0205133.

[34] J. Watrous. Succinct quantum proofs for properties of finite groups. In *Proc. IEEE FOCS*, pages 537–546, 2000. cs.CC/0009002.

[35] W. H. Zurek. Environment-assisted invariance, causality, and probabilities in quantum physics. *Phys. Rev. Lett.*, 90, 2003. quant-ph/0211037.