

# EXTREMELY ACCURATE FANTASY QUANTUM COMPUTERS IMPLY THE COLLAPSE OF THE COUNTING HIERARCHY

HENRY YUEN

## 1. INTRODUCTION

Consider a fantasy universe with a non-standard version of quantum mechanics, where the measurement probabilities are not calculated according to the usual Born rule (i.e. square the magnitude of probability amplitudes), but according to the  $p$ -norm, for some integer  $p > 2$ . Aaronson showed that in universes where the probabilities are calculated according to an *even*  $p$ -norm, for  $p > 2$ , quantum computers acquire great power. Let  $\text{BQP}_p$  be the class of problems solvable on a polynomial-time quantum computer in such a universe. Aaronson showed that then  $\text{BQP}_p = \text{PP}$ . The analogous situation for our universe ( $\text{BQP} = \text{PP}$ ) is believed to be false.

One might ask whether there is any use in contemplating these universes with bizarre physics - what consequence do these fantasy complexity classes have for the world we care about? In this note, we prove a statement of the form, “If there’s a fantasy universe where you can do  $X$ , then  $Y$  happens in our universe”. Here,  $X$  is “You can perform *strong error reduction* for quantum computers” (strong error reduction to be defined later) and  $Y$  is “The Counting Hierarchy collapses”. *A priori* one would not expect the integrity of the Counting Hierarchy to be related to the accuracy of quantum computers in a fictitious universe, but here we show such a connection.

We believe that studying fantasy quantum mechanics is useful for the same reason we study other planets: as foreign as Mars or the gas giants or exoplanets may be to us, they yield valuable insight about Earth. Fantasy quantum mechanics may give an absurd caricature of our “real” universe, but it does so in such a way as to illuminate aspects of physics or computation that we wouldn’t have noticed before.

This result is another piece of evidence that quantum information can have applicability beyond quantum computers; the quantum model of computation has very useful mathematical structure that can be exploited to make arguments about classical computation.

## 2. THE MAIN RESULT, IN A NUTSHELL

Originally the author tried to show that  $\text{BQP}_p = \text{PP}$  for *all* integer  $p > 2$ , by modifying Fortnow and Rogers’s alternative proof of  $\text{BQP}_2 \subseteq \text{PP}$ , which was originally proven by Adleman et al [4][8] (by  $\text{BQP}_2$  we mean the class of problems solvable by quantum computers with bounded error, in polynomial time, in *our* beloved 2-norm universe). Unfortunately, this did not work as planned, and the reason appears to be that the proof technique requires extremely accurate simulation of the fantasy quantum machines: the probability of error has to be smaller than the inverse of the dimension of the Hilbert space the quantum machine lives in (we call this *strong error reduction*)! Since the dimension of the Hilbert space is exponential in the number of qubits used by the quantum machine, this is a very small error probability indeed.

It isn’t *a priori* impossible that such accurate simulation could be performed. After all, we know how to amplify the success probabilities of classical randomized machines to be exponentially close

---

*Date:* July 2011.

MIT CSAIL, hyuen@csail.mit.edu. This work was done while the author was a graduate student at the University of Southern California, supported by the USC Provost Graduate Fellowship.

to 1, by using extra randomness and time. A similar amplification can be done with quantum machines (even fantasy ones - see the Appendix), but there seems to be a Catch-22: in order to reduce the error, you could run many copies of the algorithm (either in sequence or in parallel), but that will increase the size of the Hilbert space, meaning you have to do *more* error reduction, which in turn increases the size of the Hilbert space, *ad infinitum*.

The foregoing argument doesn't rule out all possible approaches to such strong error reduction, but we'll see that complexity theory offers compelling evidence that it's impossible. The main result of this note is, informally:

**Theorem 1 (Informal).** *If for even  $p > 2$  all bounded error polynomial-time  $p$ -norm quantum machines admit strong error reduction, then the Counting Hierarchy collapses to the first level ( $\text{PP}^{\text{PP}^{\dots}} = \text{PP}$ ).*

Thus, if one believes in the integrity of the Counting Hierarchy, then strong error reduction for fantasy quantum machines is impossible. There are many results in complexity theory of this form: *If Complexity statement A is true, then Complexity class hierarchy B collapses.* Results like these are used to indicate that Complexity statement A is probably false, because of the strong belief that Complexity class hierarchy B is infinite. The most famous result of this type is the Karp-Lipton theorem, which stated in the contrapositive says unless the Polynomial Hierarchy collapses to the second level, NP cannot be solved by polynomial-sized circuits [9].

### 3. $\text{BQP}_p$

**Notation 1.** *For notational clarity, instead of writing  $\|\Psi\|_p^p$  to denote the  $p$ -norm of a state vector raised to the  $p$ th power, we will write  $N_p(\Psi)^p$ . That is,  $N_p(\Psi) \equiv \|\Psi\|_p$ .*

**Definition 1 ( $\text{BQP}_p$ ).** Let  $p$  be a positive integer greater than 2, and  $\gamma : \mathbb{N} \rightarrow [0, 1/2)$  be functions. Define  $\text{BQP}_p(\gamma)$  to be the set of languages  $L$  such that there exists a positive polynomial  $m(n)$ , and a polynomial-time computable family of unitary quantum circuits  $\{Q_n(x)\}$  with the following properties:

- Each circuit consists of gates drawn from a finite universal set of quantum gates;
- Each circuit has the input  $x \in \{0, 1\}^n$  “hard-coded” in;
- Each circuit  $Q_n(x)$  acts on  $m(n)$  number of scratch qubits, and 1 output qubit;
- For all  $n \in \mathbb{N}$ ,  $x \in \{0, 1\}^n$ ,
  - $x \in L \Rightarrow \Pr[Q_n(x) \text{ accepts on input } |0\rangle^{\otimes m(n)}|0\rangle] \geq 1 - \gamma(n)$
  - $x \notin L \Rightarrow \Pr[Q_n(x) \text{ accepts on input } |0\rangle^{\otimes m(n)}|0\rangle] \leq \gamma(n)$

We define the probability of the event “ $Q_n(x)$  accepts on input  $|0\rangle^{\otimes m(n)}|0\rangle$ ” to be  $\Psi_f/N_p(\Psi)^p$ , where  $|\Psi\rangle = Q_n(x)|0\rangle^{\otimes m(n)}|0\rangle$  (we abuse notation and treat  $Q_n(x)$  as a unitary operator), and  $\Psi_f = \sum_{y \in \{0,1\}^{m(n)}} |\langle y | \langle 1 | \rangle | \Psi \rangle|^p$ .

We say that such a family of quantum circuits  $\{Q_n(x)\}$  *accepts*  $L$ , and has *success probability* of  $1 - \gamma(n)$ , or equivalently has *error* of  $\gamma(n)$ .

We define  $\text{BQP}_p$  as  $\text{BQP}_p(1/3)$ .

### 4. COUNTING CLASSES

Fortnow and Rogers gave an alternative, simpler proof to Adleman, et al.’s result that  $\text{BQP}_2 \subseteq \text{PP}$  [8] (i.e. efficient quantum computation in the standard model of quantum mechanics is computable by PP), through the use of GapP functions and the complexity class AWPP, which they define in [7].

**Definition 2.** A function  $f : \{0, 1\}^* \rightarrow \mathbb{N}$  is in **GapP** (or is a **GapP** function) iff there exists a polynomial-time nondeterministic Turing Machine  $M$  such that for all  $x \in \{0, 1\}^*$ ,  $f(x)$  is the number of accepting states minus the number of rejecting states of  $M$  on input  $x$ .

**Theorem 2** (Fortnow, Fenner, et al.). *A language  $L$  is in **PP** iff there exists a **GapP** function  $f$  where for all  $x \in \{0, 1\}^*$ :*

- $x \in L \Rightarrow f(x) \geq 0$
- $x \notin L \Rightarrow f(x) < 0$ .

Fenner proves a useful characterization of **PP**-low classes:

**Theorem 3** (Fenner). *A language  $L$  is low for **PP** if there exists a polynomial-time computable function  $d$ , a **GapP** function  $f$ , such that for all  $x \in \{0, 1\}^n$ , and*

- $x \in L \Rightarrow \frac{2}{3} \leq f(x)/d(|x|) \leq 1$
- $x \notin L \Rightarrow 0 \leq f(x)/d(|x|) \leq \frac{1}{3}$

**Theorem 4** (Fortnow, Rogers).  $\text{PP}^{\text{BQP}_2} = \text{PP}$ .

## 5. THE MAIN RESULT, IN DETAIL

**Definition 3.** For all integer  $p > 2$ ,  $\text{BQP}_p$  admits “strong error reduction” with parameter  $\lambda$  iff for all  $L \in \text{BQP}_p$ , there exists a deterministic polynomial-time generated family of quantum circuits  $Q = \{Q_n(x)\}$  with the following properties:

- (1)  $Q$  accepts  $L$ ;
- (2) Each circuit  $Q_n(x) \in Q$  uses gates drawn only from Adleman’s Universal Set  $S$  (see Appendix);
- (3)  $Q$  has error  $\alpha(n)/3$ , where  $\alpha(n) = d(n)^{-\lambda}$ ,  $d(n)$  being the dimension of the Hilbert space that  $Q_n(x)$  acts upon

**Theorem 5.** *If there exists an even  $p > 2$  such that  $\text{BQP}_p$  admits strong error reduction with parameter  $\lambda = 1 - \frac{2}{p}$ , then the Counting Hierarchy collapses to the first level (i.e.  $\text{PP}^{\text{PP}} = \text{PP}$ ).*

*Proof.* Let  $L \in \text{BQP}_p$ . By assumption, there exists a polynomial-time computable family of quantum circuits  $\{Q_n(x)\}$  with gates only from  $S$ , and the circuit family accepts  $L$  with success probability  $1 - \alpha/3$ , where  $\alpha = d(n)^{-\lambda}$ ,  $d(n)$  being the dimension of the Hilbert space that  $Q_n(x)$  acts upon.

Fix  $x$  and let  $n = |x|$ . Since  $Q_n(x)$  admits strong error reduction,  $Q_n(x)$  only has gates drawn from  $S$ . This implies that, treating  $Q_n(x)$  as a unitary matrix, there exists an integer matrix  $V(x)$  and a polynomial  $t(n)$  such that  $V(x) = 5^{t(n)}Q_n(x)$ . Note that since  $Q_n(x)$  was polynomial-time computable, each of the entries of  $V(x)$  are also polynomial-time computable.

Let  $|\Lambda\rangle$  be the initial state that is fed to  $Q_n(x)$  - i.e.  $|\Lambda\rangle = |0\rangle^{m(n)+1}$ . Let  $\Psi = V_n(x)|\Lambda\rangle$ . Note that  $\Psi$  is not a valid state vector (it doesn’t have unit length). However, each component  $\Psi_i$  is an exponential sum of a polynomial product of polynomial-time computable entries of  $V$ , and thus each component  $\Psi_i$  is a **GapP** function with respect to the input  $x$ .

Let  $f(x) = \sum_{y \in \{0,1\}^{m(n)}} |\langle y | \langle 1 | \Psi \rangle|^p$ , which is an exponential sum of a polynomial product of **GapP** functions, and thus  $f(x)$  is a **GapP** function (due to **GapP** closure properties). Thus the probability of  $Q_n(x)$  accepting is  $f(x)/N_p(\Psi)^p$ .

From the definition of  $\text{BQP}_p$ , we have that for all  $x \in \{0, 1\}^*$ :

$$\begin{aligned} x \in L &\Rightarrow \Pr[Q_n(x) \text{ accepts}] \geq 1 - \alpha(n)/3 \\ x \notin L &\Rightarrow \Pr[Q_n(x) \text{ accepts}] \leq \alpha(n)/3 \end{aligned}$$

---

When  $x \in L$ :

$$\begin{aligned}
x \in L &\Rightarrow \Pr[Q_n(x) \text{ accepts}] \geq 1 - \alpha/3 \\
&\Rightarrow \frac{f(x)}{N_p(\Psi)^p} \geq 1 - \alpha/3 \\
&\Rightarrow \frac{f(x)}{5^{pt(n)} \cdot \alpha} \geq 1 - \alpha/3 \\
&\Rightarrow \frac{f(x)}{5^{pt(n)} \cdot \alpha} \geq 2/3
\end{aligned}$$

When  $x \notin L$ :

$$\begin{aligned}
x \notin L &\Rightarrow \Pr[Q_n(x) \text{ accepts}] \leq \alpha/3 \\
&\Rightarrow \frac{f(x)}{N_p(\Psi)^p} \leq \alpha/3 \\
&\Rightarrow \frac{f(x)}{5^{pt(n)} \cdot \alpha} \leq 1/3
\end{aligned}$$

Observe that  $5^{pt(n)} \cdot \alpha$  is a polynomial-time computable function. Since  $f(x)$  is a GapP function, this proves that  $\text{BQP}_p$  is low for PP.

In his thesis [2] and in [3], Aaronson proves that for all even  $p > 2$ ,  $\text{PP} = \text{BQP}_p$ . Thus, if  $\text{BQP}_p$  is low for PP, then we have shown  $\text{PP}^{\text{PP}} = \text{PP}$ , which implies the collapse of the Counting Hierarchy to the first level.  $\square$

It is interesting to note that this proof does not relativize, so it avoids conflict with oracle results such as  $\text{P}^{\text{NP}^A} \not\subseteq \text{PP}^A$  for some oracle  $A$ . It does not relativize because we use the fact that we can write a quantum circuit as a matrix consisting only of integer entries. In general, this cannot be done in a relativized world.

## 6. ACKNOWLEDGEMENTS

The author wishes to thank Joseph Bebel, Len Adleman and Scott Aaronson for inspiring discussions and feedback.

## REFERENCES

- [1] Aaronson, S., Is Quantum Mechanics an Island in Theoryspace? *Proceedings of the Växjö Conference “Quantum Theory: Reconsideration of Foundations”*, 2004.
- [2] Aaronson, S., Limits on Efficient Computation in the Physical World. *PhD Thesis, UC Berkeley*, 2004.
- [3] Aaronson, S., Quantum Computing, Postselection, and Probabilistic Polynomial Time. *Proceedings of the Royal Society A*. 461(2063):3473-3482, 2005.
- [4] Adleman, L., DeMarrais, J., Huang, M.-D., Quantum Computability. *SIAM J. Comput.* Vol 26, No. 5, 1997.
- [5] Bernstein, E., Vazirani, U., Quantum Complexity Theory. *SIAM J. Comput.* Vol 26, No. 5, 1997.
- [6] Fenner, S., PP-Lowness and a Simple Definition of AWPP. *Theory Comput. Systems* 2003.
- [7] Fenner, S., Fortnow, L., Kurtz, S., Gap-definable Counting Classes. *Journal of Computer and System Sciences*, 48(1):116-148, 1994.
- [8] Fortnow, L., Rogers, J., Complexity Limitations on Quantum Computation. *13th Conference on Computational Complexity*, 1998.
- [9] Karp, R., Lipton, R., Some connections between nonuniform and uniform complexity classes. *Proceedings of the twelfth annual ACM symposium on Theory of computing*, 1980.
- [10] Li, L. On the Counting Functions. *PhD Thesis, University of Chicago*, 1993.

## 7. APPENDIX

**Lemma 1.** For all  $p > 2$ , for all  $x \in \mathbb{C}^d$ ,  $\|x\|_p^p \leq \|x\|_2^2 \leq (d^{1-2/p})\|x\|_p^p$ .

*Proof.* Let  $x \in \mathbb{C}^d$ . We want to find a tight constant  $c$  such that  $\|x\|_2^2 \leq c\|x\|_p^p$ .

Denote  $\alpha_i = |x_i|$ . So we want to minimize  $f(\vec{\alpha}) = \sum_i \alpha_i^p$ , subject to  $g(\vec{\alpha}) = \sum_i \alpha_i^2 = 1$  (changing 1 to some other constant does not change our bound). By the method of Lagrange multipliers, we set the partial derivatives of  $f$  equal to the partial derivatives of  $g$  times the Lagrange multiplier  $\lambda$ . We have  $p\alpha_i^{p-1} = \lambda \cdot 2\alpha_i$ . Since all the  $\alpha_i$  are non-negative, we have that  $\alpha_i = \alpha_j$ , for all  $i, j$ . This turns out to be the minimum of  $f$  subject to  $g = 1$ . At this optimum point,  $f(d^{-1/2}, \dots, d^{-1/2}) = d^{1-p/2}$ . Thus,  $\|x\|_p^p \leq d^{1-p/2}\|x\|_2^2$ . By setting  $c = d^{1-2/p}$ , we obtain our bound.  $\square$

Adleman, et al. effectively showed that there exists a universal finite set of quantum gates with transition amplitudes are drawn from  $\{0, \pm 1, \pm 3/5, \pm 4/5\}$  [4]. Denote that universal gate set as  $S$ .

We claim that the results of Adleman, et al. extends to our setting:  $\text{BQP}_p$  does not change when you restrict your gates to  $S$ .

**Lemma 2.** Given a polynomial-time computable family of circuits  $\{Q_n\}$  that accepts a  $\text{BQP}_p$  problem  $L$ , there is a polynomial-time computable family of circuits  $\{\hat{Q}_n\}$  that also accepts  $L$ , but where each  $\hat{Q}_n$  uses gates only from  $S$ , and  $\|Q_n - \hat{Q}_n\| \leq \epsilon$  for some  $\epsilon = 2^{-n^c}$ .

*Proof.* This follows from the Solovay-Kitaev theorem.  $\square$

The following theorem isn't used anywhere in the above proofs, but it shows that "normal" error reduction can be done with  $\text{BQP}_p$ , in the same way that error reduction can be done with BPP. We believe this is the limit of error reduction one can do for  $\text{BQP}_p$ .

**Theorem 6** (Error reduction for  $\text{BQP}_p$ ). Let  $p$  be an integer greater than 2. Let  $q(n)$  be a polynomial satisfying  $q(n) > 2$ . Then  $\text{BQP}_p(2^{-q(n)}) = \text{BQP}_p$ .

*Proof.* It is clear that  $\text{BQP}_p(2^{-q(n)}) \subseteq \text{BQP}_p$ . We now prove  $\text{BQP}_p \subseteq \text{BQP}_p(2^{-q(n)})$ .

Let  $L \in \text{BQP}_p(1/3)$ . Let  $\{Q_n(x)\}$  be the associated family of quantum circuits that solves  $L$ . Consider the following circuit family construction  $\{\hat{Q}_n(x)\}$ : for each  $n$ , for all  $x \in \{0, 1\}^n$ , we run  $Q_n(x)$   $k$  times in parallel, for some  $k$  to be specified later. We take the  $k$  output bits of each  $Q_n(x)$  circuit and then compute the majority answer.

For convenience, for all  $y \in \{0, 1\}^*$ , define  $H(y)$  to be the Hamming weight of  $y$ .

The unitary of the first stage of the computation (running  $Q_n(x)$   $k$  times in parallel) is  $S_1 = Q_n(x)^{\otimes k} \otimes I$ . Denote the unitary computing the second stage (computing majority) as  $S_2 = M$ , where  $M$  has the following action:

For all  $y \in \{0, 1\}^k$ ,  $a_1, \dots, a_k \in \{0, 1\}^{m(n)}$ ,  $b \in \{0, 1\}$ :

$$M \left( \bigotimes_{1 \leq i \leq k} |a_i\rangle |y_i\rangle |b\rangle \right) = \bigotimes_{1 \leq i \leq k} |a_i\rangle |y_i\rangle |b \oplus I(y)\rangle$$

where  $I(y) = 1$  if and only if  $H(y) \geq k/2$ , 0 otherwise, and  $\oplus$  is addition modulo 2.  $M$  is clearly unitary, and polynomial-time constructible.

Let's analyze this circuit:

- (1) We begin with state  $|\Psi_0\rangle = |0\rangle^{\otimes (m(n)+1)k} |0\rangle$  (the last qubit is the output qubit).
- (2) After passing  $|\Psi_0\rangle$  through  $S_1$ , we have:

$$|\Psi_1\rangle = S_1|\Psi_0\rangle = (\alpha(x)|w_0(x)\rangle|0\rangle + \beta(x)|w_1(x)\rangle|1\rangle)^{\otimes k} |0\rangle$$

where  $|w_0(x)\rangle$  and  $|w_1(x)\rangle$  are the states of the workspace qubits corresponding to the “YES” and “NO” answers, respectively, and  $\alpha(x)$  and  $\beta(x)$  are complex amplitudes.

(3) After computing majority on  $|\Psi_1\rangle$ , we have:

$$|\Psi_2\rangle = M|\Psi_1\rangle = \sum_{y \in \{0,1\}^k} \alpha(x)^{k-H(y)} \beta(x)^{H(y)} \left( \bigotimes_{1 \leq i \leq k} |w_{y_i}(x)\rangle |y_i\rangle \right) |I(y)\rangle$$

(4) Let us compute the probability of acceptance. Suppose  $x \in L$ . Then, by definition of  $\text{BQP}_p(1/3)$ , we know that:

$$\frac{|\beta(x)|^p \sum_z |w_{1,z}(x)|^p}{|\alpha(x)|^p \sum_z |w_{0,z}(x)|^p + |\beta(x)|^p \sum_z |w_{1,z}(x)|^p} \geq \frac{2}{3}$$

where for  $b \in \{0, 1\}$ ,

$$|w_b(x)\rangle = \sum_{z \in \{0,1\}^{m(n)}} w_{b,z}(x) |z\rangle$$

with complex amplitudes  $w_{b,z}$ . For convenience, let

$$A = |\alpha(x)|^p \sum_z |w_{0,z}(x)|^p$$

$$B = |\beta(x)|^p \sum_z |w_{1,z}(x)|^p$$

Hence,  $B \geq 2A$ . The probability that the output state  $|\Psi_2\rangle$  is measured in an accepting state is:

$$\begin{aligned} & \frac{\sum_{H(y) \geq k/2} A^{k-H(y)} B^{H(y)}}{\sum_{y \in \{0,1\}^k} A^{k-H(y)} B^{H(y)}} \\ &= \frac{\sum_{H(y) \geq k/2} A^{k-H(y)} B^{H(y)}}{(A+B)^k} \\ &= \sum_{H(y) \geq k/2} \left( \frac{A}{A+B} \right)^{k-H(y)} \left( \frac{B}{A+B} \right)^{H(y)} \\ &= \sum_{j \geq k/2} \binom{k}{j} \left( \frac{A}{A+B} \right)^{k-j} \left( \frac{B}{A+B} \right)^j \end{aligned}$$

Since  $r = B/(A+B) \geq 2/3$ , by the Chernoff bound, this sum is greater than  $1 - \exp(-2k(r - \frac{1}{2})^2)$ , i.e., exponentially close to 1. A similar analysis holds for  $x \notin L$ .

Setting  $k \geq \frac{q(n)}{(r-1/2)^2}$  allows us to achieve a success probability greater than  $1 - 2^{-q(n)}$ . Hence the circuit family  $\{\hat{Q}_n(x)\}$  is still polynomially sized in  $n$ , and can be generated in deterministic polynomial time. This completes the proof that  $\text{BQP}_p \subseteq \text{BQP}_p(2^{-q(n)})$ .  $\square$