Electronic Colloquium on Computational Complexity, Report No. 151 (2014)

Quantum One-Sided Exact Error Algorithms

Debajyoti Bera

November 14, 2014

Abstract

We define a complexity class for randomized algorithms with one-sided error that is exactly equal to a constant (unlike the usual definitions, in which the error is only bounded above or below by a constant). We show that the corresponding quantum classes (one each for a different error probability) are in fact all equivalent to each other and to **EQP**, the quantum analogue of **P**. The technique used is a form of quantum amplitude amplification.

Keywords: quantum computing, randomized algorithm, one-sided error, amplitude amplification

1 Introduction

One of the major, and still open, challenging questions of *Complexity Theory* is the question of how the complexity class **P** compares to **BPP**. One approach towards settling this question is looking at the intermediate classes lying between **P** and **BPP**, e.g., **RP**. However, the current best results (without using oracles) are the obvious inclusions $\mathbf{P} \subseteq \mathbf{RP} \subseteq \mathbf{BPP}$, though there are some evidences, leading to a strong belief, towards equivalence of these classes.

RP is the class of (decision) problems which admit randomized one-sided polynomial-error (worst-case) polynomial-time algorithms. We consider a simplied class that lies between **P** and **RP**. Problems in $\mathbf{RP^E}$ have randomized algorithms similar to those for **RP**, but with an additional requirement that the one-sided error is same for all "no" instances of a certain size. Note that, like **RP**, $\mathbf{RP^E}$ have many similar properties as those of **RP**. For example, $\mathbf{RP^E}$ is closed under union, and intersection. We similarly define its quantum analog, $\mathbf{RQP^E}$. The immediate questions are therefore, the structure of these classes and their relationship with **P** and **RP** (**EQP** and **RQP** for quantum classes)[1].

Rarely, complexity classes are defined in terms of exact error (or, number of accepting paths, for counting classes). The primary reason is the lack of robustness in definition that accompanies this concept. Conceptually, there should not be much difference between complexity of problems that admit randomized algorithms with one-sided error exactly, say, 0.3 to that with error exactly 0.31. However, we show in this paper, that this is not a problem for analogous quantum complexity classes.

Based on what we know, $\mathbf{P} \neq \mathbf{RP^E}$ – but we were able to prove that the quantum analogues of these classes have identical power: $\mathbf{EQP} = \mathbf{RQP^E}$ (**EQP** is the quantum analog of **P**). This was achieved by showing how to completely eliminate the (one-sided) error, using *quantum amplitude amplification* – something which is impossible in general for classical classes without making any complexity theoretic assumptions.

Quantum amplitude amplification[1, 3] is the key ingredient behind the famous quantum unordered search algorithm designed by Lok Grover[4]. The technique shows how to increase the success probability of a quantum circuit, where success probability is defined as the probability that the output state of the circuit lies in a particular subspace. This technique and its variations has underwent a lot of analysis, and has been successfully used to design quantum algorithms that are more efficient compared to classical ones.

In this paper we focus on the effect of amplitude amplification on quantum circuits with one-sided error. We prove our results by adapting a quantum amplitude amplification result from [1] which shows how to

[1] A similar question was asked for **BPP** in `http://cstheory.stackexchange.com/questions/20027/in-what-class-are-randomized-algorithms-that-err-with-exactly-25-chance`

ISSN 1433-8092

remove any probability of error from a quantum algorithm with one-sided error exactly equal to 1/2. This is not possible, in general, for classical randomized algorithms with one-sided error.

Background on quantum computing models and corresponding complexity classes are omitted. Our quantum circuits use arbitrary single qubit gates, whose usage is similar to arbitrary coins (with constant bias) in randomized algorithms.

2 One-sided Error Quantum Polynomial Time

The complexity class $\mathbf{RQP}_\epsilon$ denotes the set of problems decided by a polynomial-time quantum algorithm with one-sided error at most ϵ. It is well known that for all polynomials $p()$, if $\epsilon = \Omega(1/p(n))$, then all $\mathbf{RQP}_\epsilon$ are, in fact, the same class.

EQP constitutes the problems with exact polynomial-time quantum algorithms, in other words, $\mathbf{EQP} = \mathbf{RQP}_0$.

We define a new complexity class, named $\mathbf{RQP^E}_\epsilon$ which is like $\mathbf{RQP}_\epsilon$ but with one sided error *exactly equal to* ϵ. Formally,

Definition 2.1. $\mathbf{RQP^E}_\epsilon$ *denotes the class of languages L for which there exists a uniform family of quantum circuits C, and a suitable measurement operator M such that,*

- *if* $x \notin L$, $\Pr[MC(x) = |0\rangle] = 1$
- *if* $x \in L$, $\Pr[MC(x) = |1\rangle] = \epsilon$

Definition 2.2. $\mathbf{RQP^E} = \bigcup_\epsilon \mathbf{RQP^E}_\epsilon$

Now we state and prove the main theorem of this paper. $\imath$ denotes $\sqrt{-1}$.

Theorem 2.3. $\mathbf{RQP^E} = \mathbf{EQP}$.

EQP is trivially contained in $\mathbf{RQP^E}$, in fact $\mathbf{RQP^E}_\epsilon$. For example, for $\epsilon = 1/2$, the **EQP** algorithm can be simply modified to apply a controlled Hadamard gate with target as a qubit initialized to $|0\rangle$, and as control the specified measurement qubit. The target qubit, upon measurement in the computational basis, exhibits a one-sided error of 1/2. For any other constant ϵ, similar controlled gates can be used.

The rest of this section is on the proof of the more difficult direction. We will first show a special case of the other direction (Lemma 2.4), and then generalize it (Corollary 2.5).

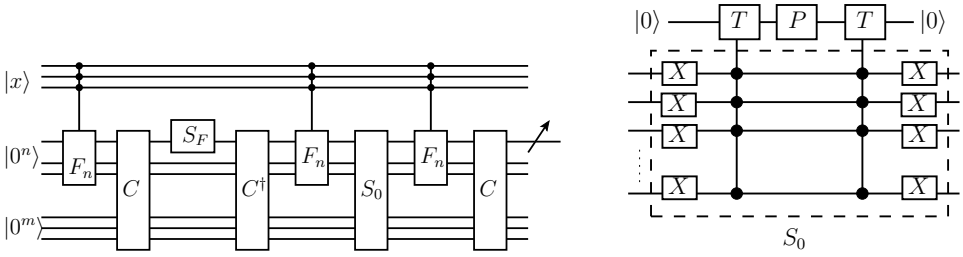

Figure 1: Circuit for $\mathcal{C}'$ (left) and S_0 gate in $\mathcal{C}'$ (right)

Lemma 2.4. *If a language $L \in \mathbf{RQP^E}_{1/2}$, then $L \in \mathbf{EQP}$.*

Proof. We will assume that the algorithms end with a measurement of a specified qubit in the computational basis – this is equivalent most other ways measurement strategies that are commonly applied.

Take any $L \in \mathbf{RQP^E}_{1/2}$, and consider the corresponding circuit C. Suppose m denotes the number of ancillæ qubits used by C, and n denotes the length of any input x, then C acts on $\mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes m}$ and its

output is given by $|\psi\rangle = C|x\rangle|0^m\rangle$. Without loss of generality, suppose that the first qubit is specified for measurement, then the projective measurement operator applied is $|0\rangle\langle 0| \otimes I$.

We will now a construct an **EQP** circuit $\mathcal{C}'$ to decide the same language L. But first note that, $|\psi\rangle = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$ and that, if $x \notin L$, $\langle\psi_1|\psi_1\rangle = 0$, and if $x \in L$, $\langle\psi_1|\psi_1\rangle = 1/2$ $(= \langle\psi_0|\psi_0\rangle)$. The circuit is constructed as $\mathcal{C}' = \mathcal{A}S_0\mathcal{A}^{-1}S_F\mathcal{A}$ and described in Figure 1. $\mathcal{C}'$ acts on $\mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes m}$, and we will denote the space as 3 registers P, Q, R, respectively, of n, n, m qubits. The gates will be labelled with the registers (as superscripts) they are applied on in the following description.

Besides the circuit C, which will be used always on registers QR, we will make frequent use of the *fanout* operator[2]. This, and the other components of $\mathcal{C}'$, are listed below.

- The fanout operator effectively copies basis states from a control qubit to a target qubit. On two registers of n qubits each, it works as $F_n|a_1 \dots a_n\rangle|b_1 \dots b_n\rangle = |a_1 \dots a_n\rangle|(b_1 \oplus a_1) \dots (b_n \oplus a_n)\rangle$. Note that, $F_n^\dagger = F_n$.
- $\mathcal{A} = (F_n^{PQ} \otimes I) \otimes (I \otimes C^{QR})$
- $S_F^Q = P$ where the phase gate P is applied on the first qubit of register Q. Notice that, the first qubit of register Q is the measurement qubit with respect to C.
- $S_0^{QR} = I - (1 - \imath)|0^{n+m}\rangle\langle 0^{n+m}|$ which changes the phase of the basis state in which all qubits are in the state $|0\rangle$. Implementation of S_0 is shown in Figure 1 – it requires one additional qubit initialized to $|0\rangle$. However this qubit is in state $|0\rangle$ after application of this operator, so this qubit could be reused if required. This extra qubit has been left out in the description of $\mathcal{C}'$.
- The input to $\mathcal{C}'$ will be $|x\rangle|0^{\otimes n}\rangle|0^{\otimes m}\rangle$.
- We will measure the first qubit of register Q in the standard basis at the end.

Next, we will describe the operation of $\mathcal{C}'$.

$$\begin{aligned}
\mathcal{C}'|x\rangle|0^n\rangle|0^m\rangle =& C^{QR} \cdot F_n^{PQ} \cdot S_0^{QR} \cdot F_n^{PQ} \cdot C^{\dagger QR} \cdot S_F^Q \cdot C^{QR} \cdot F_n^{PQ} \quad |x\rangle|0^n\rangle|0^m\rangle \\
=& C^{QR} \cdot F_n^{PQ} \cdot S_0^{QR} \cdot F_n^{PQ} \cdot C^{\dagger QR} \cdot S_F^Q \cdot C^{QR} \quad |x\rangle|x\rangle|0^n\rangle \\
=& C^{QR} \cdot F_n^{PQ} \cdot S_0^{QR} \cdot F_n^{PQ} \cdot C^{\dagger QR} \cdot S_F^Q \quad |x\rangle\Big(|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle\Big) \\
=& C^{QR} \cdot F_n^{PQ} \cdot S_0^{QR} \cdot F_n^{PQ} \cdot C^{\dagger QR} \quad |x\rangle\Big(|0\rangle|\psi_0\rangle + \imath|1\rangle|\psi_1\rangle\Big) \qquad (*)
\end{aligned}$$

We will now simplify the remaining operator.

$$\begin{aligned}
& C^{QR} \cdot F_n^{PQ} \cdot S_0^{QR} \cdot F_n^{PQ} \cdot C^{\dagger QR} \\
=& C^{QR} \cdot F_n^{PQ} \cdot \Big(I - (1 - \imath)I^P \otimes |0^{n+m}\rangle\langle 0^{n+m}|\Big) \cdot F_n^{PQ} \cdot C^{\dagger QR} \\
=& C^{QR} \cdot F_n^{PQ} \cdot \Big(I - (1 - \imath) \sum_{n\text{-bit } p} |p, 0^{n+m}\rangle\langle p, 0^{n+m}|\Big) \cdot F_n^{PQ} \cdot C^{\dagger QR} \\
=& C^{QR} \cdot \Big(I - (1 - \imath) \sum_{n\text{-bit } p} F_n^{PQ}|p, 0^{n+m}\rangle\langle p, 0^{n+m}|F_n^{PQ}\Big) \cdot C^{\dagger QR} \\
=& C^{QR} \cdot \Big(I - (1 - \imath) \sum_{n\text{-bit } p} |p, p, 0^m\rangle\langle p, p, 0^m|\Big) \cdot C^{\dagger QR} \\
=& I - (1 - \imath) \sum_{n\text{-bit } p} |p\rangle\langle p| \otimes (C^{QR}|p, 0^m\rangle\langle p, 0^m|C^{\dagger QR}
\end{aligned}$$

Substituting this simplification in $(*)$ above,

$$
\begin{aligned}
&\mathcal{C}'|x\rangle|0^n\rangle|0^m\rangle \\
=&\Big(I-(1-\imath)\sum_{n\text{-bit } p}|p\rangle\langle p|\otimes(C^{QR}|p,0^m\rangle\langle p,0^m|C^{\dagger QR}\Big)\ \ |x\rangle\Big(|0\rangle|\psi_0\rangle+\imath|1\rangle|\psi_1\rangle\Big)\\
=&|x\rangle\Big(|0\rangle|\psi_0\rangle+\imath|1\rangle|\psi_1\rangle\Big)-\\
&(1-\imath)\sum_{n\text{-bit } p}|p\rangle\langle p|x\rangle\otimes\Big(C^{QR}|p,0^m\rangle\langle p,0^m|C^{\dagger QR}\Big)\ \ \Big(|0\rangle|\psi_0\rangle+\imath|1\rangle|\psi_1\rangle\Big)\\
=&|x\rangle\Big(|0\rangle|\psi_0\rangle+\imath|1\rangle|\psi_1\rangle\Big)-(1-\imath)|x\rangle\otimes\Big(C^{QR}|x,0^m\rangle\langle x,0^m|C^{\dagger QR}\Big)\ \ \Big(|0\rangle|\psi_0\rangle+\imath|1\rangle|\psi_1\rangle\Big)\\
=&|x\rangle\Big(\big(|0\rangle|\psi_0\rangle+\imath|1\rangle|\psi_1\rangle\big)-(1-\imath)\big(|0\rangle|\psi_0\rangle+|1\rangle|\psi_1\rangle\big)\big(\langle 0|\langle\psi_0|+\langle 1|\langle\psi_1|\big)\ \ \big(|0\rangle|\psi_0\rangle+\imath|1\rangle|\psi_1\rangle\big)\Big)\\
=&|x\rangle\Big(\big(|0\rangle|\psi_0\rangle+\imath|1\rangle|\psi_1\rangle\big)-(1-\imath)\big(|0\rangle|\psi_0\rangle+|1\rangle|\psi_1\rangle\big)\big(\langle\psi_0|\psi_0\rangle+\imath\langle\psi_1|\psi_1\rangle\big)\Big)\\
=&|x\rangle\Big(\big(1-(1-\imath)K\big)|0\rangle|\psi_0\rangle+\big(\imath-(1-\imath)K\big)|1\rangle|\psi_1\rangle\Big)\ \text{ where, } K=\langle\psi_0|\psi_0\rangle+\imath\langle\psi_1|\psi_1\rangle\\
=&\begin{cases}\imath|x\rangle|0\rangle|\psi_0\rangle & \text{if, } x\notin L \text{ i.e., } \langle\psi_1|\psi_1\rangle=0,\ \langle\psi_0|\psi_0\rangle=1\\ (\imath-1)|x\rangle|1\rangle|\psi_1\rangle & \text{if, } x\in L \text{ i.e., } \langle\psi_1|\psi_1\rangle=\langle\psi_0|\psi_0\rangle=1/2\end{cases}
\end{aligned}
$$

Measuring the first qubit of register Q therefore shows $|1\rangle$ if and only if $x \in L$.

□

It can be readily observed that this proof extends to several other quantum classes as well, e.g., $RQAC^k_{1/2} = EQAC^k$ for all $k \geq 0$ and $RQNC^k_{1/2} = EQNC^k$ for $k \geq 1$. We now generalize the 1/2 to any arbitrary small constant $0 < \epsilon < 1$.

Lemma 2.5. *If a language $L \in \mathbf{RQP}^{\mathbf{E}}{}_{\epsilon}$, then $L \in \mathbf{EQP}$.*

Proof. We will essentially use the same proof as in Lemma 2.4 with a modification of the S_0 operator. We will therefore, only discuss the changes from the main Lemma. In the same framework as used by the proof of that lemma, $L \in \mathbf{RQP}^{\mathbf{E}}{}_{\epsilon}$ implies that there is a circuit $\mathcal{C}$ which either rejects all strings not in L, or accepts the other strings with probability 1/2.

Notice that, for our question K (defined in the proof of the above lemma) is $(1 - \epsilon + \imath\epsilon)$. Choose ϕ so that, $1 - (1 - e^{\imath\phi})(1 - \epsilon + \imath\epsilon) = 0$. Referring to the proof above, for the current lemma we have: if $x \notin L$, $\langle\psi_1|\psi_1\rangle = 0$, and if $x \in L$, $\langle\psi_1|\psi_1\rangle = \epsilon$. Say, we choose operator $S_0^{QR} = I - (1 - e^{\imath\phi})|0^{n+m}\rangle\langle 0^{n+m}|$. It changes the phase of the basis state in which all qubits are in the state $|0\rangle$, by $e^{\imath\phi}$; S_0 can be implemented using similar construction as in Figure 1 – specifically, using a different single qubit gate instead of phase (P) gate[2]. Now, recalculating the steps of the above lemma proves that $\mathcal{C}'$ now accepts or rejects a string with zero probability of error. □

3 Conclusion

Consider the language $EQ = \{\langle x, y\rangle \mid x \text{ and } y \text{ are identical } n\text{-bit strings}\}$. Suppose, the only operations allowed on the input are inner product between two n-bit strings. Classically, this requires $\Omega(n)$ operations to determine with certainty, and $\Omega(\log n)$ queries to get an one-sided error randomized algorithm with

[2]The proof requires using a customized single qubit gate for every ϵ appearing in $\mathbf{RQP}^{\mathbf{E}}{}_{\epsilon}$, which we feel is okay since usual quantum circuit models allow use of arbitrary single qubit gates.

polynomially small error. However, the results proved in this paper can be used to obtain a quantum algorithm with $O(1)$ queries without *any* probability of error.

Complexity classes for problems allowing error are never defined in terms of an exact error, but upper or lower bounds of error probability. In this paper, we took the unusual route of defining an one-sided exact-error complexity class $\mathbf{RP^E}_\epsilon$ and its quantum analogue $\mathbf{RQP^E}_\epsilon$ (ϵ denotes the one-sided error). For the classical class, it is not clear whether $\mathbf{RP^E}_\epsilon$ is robust enough (like $\mathbf{RP}$) so that $\mathbf{RP^E}_{\epsilon_1} = \mathbf{RP^E}_{\epsilon_2}$ for $\epsilon_1 \neq \epsilon_2$, and furthermore, the relationship among these classes with each other and with $\mathbf{P}$ is unknown. However, we were able to resolve this question for the corresponding quantum classes. We showed that $\mathbf{RQP^E}_\epsilon = \mathbf{EQP}$ for all constant ϵ. We showed this by employing the technique of quantum amplitude amplification, and were able to reduce the (one-sided) error probability to 0 – something that is not currently possible for arbitrary one-sided classical randomized algorithms.

References

[1] G. Brassard and P. Hoyer. An exact quantum polynomial-time algorithm for Simon's problem. In *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems*, pages 12–23. IEEE Comput. Soc, 1997.

[2] Christoph Durr. Quantum circuits: Fanout, parity, and counting. *arXiv preprint quant-ph/9903046*, 1999.

[3] Lov Grover. Quantum Computers Can Search Rapidly by Using Almost Any Transformation. *Physical Review Letters*, 80(19):4329–4332, May 1998.

[4] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, New York, New York, USA, July 1996. ACM Press.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de