Exercise Set 12
Quantum Computation

Exercise 1 (From a decision version of factoring to actual factoring)

Complexity classes such as BQP are usually defined for decision problems, whose output is one bit. Factoring, however, is usually presented as a search problem: given an integer N, find its prime factors. This exercise explains why this distinction is not a serious issue for factoring.

Consider the following decision problem:

$$\text{LargePrimeFactor} = \{\langle N, k\rangle : N \text{ has a prime factor } p \text{ with } k \leq p \leq N-1\}.$$

Inputs are written in binary, and $n = \lceil \log_2 N \rceil$ denotes the input length of N up to constant factors. Assume you are given an algorithm A that solves LargePrimeFactor in time $\text{poly}(n)$. Give an algorithm that takes an integer N as input, and uses calls to A in order to return a complete factorization of N. What is the maximum number of calls to A that your algorithm will make, as a function of n?

Exercise 2 (Local gates and path-sums)

The proof that BQP $\subseteq$ PSPACE is based on a simple idea: one can compute a single amplitude of a quantum circuit by summing over all possible computational paths. This is usually much too slow, but it can be done while reusing memory.

Let S be the number of qubits, and identify basis states with bit strings in $\{0,1\}^S$. For a unitary U, write

$$U_{i,j} = \langle i| U |j\rangle, \qquad i,j \in \{0,1\}^S.$$

1. Let U apply a Hadamard gate to qubit k and the identity to all other qubits. Give an efficient rule for computing $U_{i,j}$ from the two strings i, j.

2. Let U apply a CNOT with control qubit k and target qubit ℓ, and the identity elsewhere. Give an efficient rule for computing $U_{i,j}$.

3. Repeat part (b) for a Toffoli gate with control qubits k, ℓ and target qubit r. Again, specify exactly when $U_{i,j} = 1$.

Exercise 3 (Using a BQP algorithm as a subroutine)

A classical polynomial-time algorithm can use another classical polynomial-time algorithm as a subroutine. For BQP *this is slightly more delicate, because a bounded-error quantum algorithm does not implement an exact oracle. This exercise shows why the difficulty can be overcome.*

Let $L \in \mathsf{BQP}$, and let $f : \{0,1\}^n \to \{0,1\}$ be its characteristic function: $f(x) = 1$ iff $x \in L$. Assume, after error reduction, that there is a polynomial-size quantum circuit U with the following property. It keeps the input register x unchanged and maps

$$|x\rangle\,|0\rangle\,|0^w\rangle \longmapsto \sqrt{p_x}\,|x\rangle\,|f(x)\rangle\,|\phi_x\rangle + \sqrt{1-p_x}\,|x\rangle\,|1-f(x)\rangle\,|\psi_x\rangle\,,$$

where $w \le \mathrm{poly}(n)$ and $p_x \ge 1-\varepsilon$ for every x. Here the middle qubit is the output qubit and the last register is the workspace.

1. *Explain why we may assume the error ε is exponentially small, for example $\varepsilon \le 2^{-10n}$, while keeping the circuit size polynomial.*

2. *We would like to approximate the ideal bit oracle*

   $$O_f : |x\rangle\,|b\rangle \longmapsto |x\rangle\,|b \oplus f(x)\rangle\,.$$

   Construct a circuit V using U, $U^\dagger$, and one CNOT gate, such that on inputs of the form

   $$|x\rangle\,|b\rangle\,|0\rangle\,|0^w\rangle$$

   it approximately implements

   $$|x\rangle\,|b\rangle\,|0\rangle\,|0^w\rangle \longmapsto |x\rangle\,|b \oplus f(x)\rangle\,|0\rangle\,|0^w\rangle\,.$$

3. *Show that for each basis input $|x\rangle\,|b\rangle\,|0\rangle\,|0^w\rangle$, the state produced by V has distance $O(\sqrt{\varepsilon})$ from the ideal state.*

4. *The previous part bounds the error on each basis state. Explain why choosing ε exponentially small makes the operator-norm error of V on the whole subspace with clean workspace exponentially small.*

5. *Suppose a polynomial-size quantum circuit for another language L' makes $q(n)$ queries to the ideal oracle O_f, where $q(n) \le \mathrm{poly}(n)$. Replace each query by the approximate circuit V. Use a hybrid argument or triangle inequality to show that the total error introduced is still negligible.*

6. *Conclude that a BQP computation may use a BQP language as a subroutine without leaving BQP. In other words, BQP is closed under polynomially many BQP subroutine calls.*

Exercise 4 (A stronger upper bound, $\mathsf{BQP} \subseteq \mathsf{PP}$) *(optional)*

This exercise proves a stronger classical upper bound than $\mathsf{BQP} \subseteq \mathsf{PSPACE}$. The class PP consists of decision problems solvable by a polynomial-time randomized classical algorithm whose acceptance probability is strictly larger than $1/2$ on yes-instances and strictly smaller than $1/2$ on no-instances. Unlike BPP, the gap above or below $1/2$ may be exponentially small.

For this exercise, assume that the BQP computation is given by a polynomial-size circuit C over Hadamard, Toffoli, and Z gates, acting on $S = \mathrm{poly}(n)$ qubits. The input is $\big|x, 0^{S-n}\big\rangle$. Measuring the first qubit at the end gives $f(x)$ with probability at least $2/3$. You may take for granted that restricting to such a gate set does not change BQP, up to efficient approximation.

1. Let
$$|\theta_x\rangle = C\left|x, 0^{S-n}\right\rangle$$
and define
$$a_x = \left\langle x, 0^{S-n}\right| C^\dagger Z_1 C \left|x, 0^{S-n}\right\rangle,$$
where Z_1 applies a Z gate to the first qubit. Show that
$$a_x = 1 - 2p_{\text{acc}}(x),$$
where $p_{\text{acc}}(x)$ is the probability that the first qubit is measured as 1. Conclude that
$$f(x) = 0 \Rightarrow a_x \geq \frac{1}{3}, \qquad f(x) = 1 \Rightarrow a_x \leq -\frac{1}{3}.$$

2. Apply the path-sum formula to the circuit $D = C^\dagger Z_1 C$ and the amplitude a_x. Explain why every nonzero computational path contributes either $+2^{-h/2}$ or $-2^{-h/2}$, where h is the total number of Hadamard gates in D. All zero paths contribute 0.

3. Let N_+ be the number of paths contributing $+2^{-h/2}$ and N_- the number of paths contributing $-2^{-h/2}$. Show that the sign of a_x is the sign of $N_+ - N_-$.

4. Design a polynomial-time randomized classical algorithm whose acceptance probability is larger than $1/2$ exactly when $N_- > N_+$. Conclude that $\mathsf{BQP} \subseteq \mathsf{PP}$.