CS 593/MA 595 - Introduction to Quantum Computing

Quantum Computation and Quantum Information by *Isaac Chuang, Michael Nielsen*
Student: **Ralph Razzouk**

Homework 4

Only problems 1 and 7 will be graded for correctness. The other problems will be graded for completeness (that is, you have to make an "honest attempt" to solve them).

Problem 1
For this problem, you will need to use the definition of $BQP(\mathcal{G}, \delta)$ I gave in the lecture notes for lecture 4.2. Other definitions are equivalent to mine, but the problems I have written here are closely tied to my specific definition.

(a) In the lecture notes for lecture 4.2, I define $BQ(\mathcal{G}, \delta)$ to be like BQP, except we don't require there be any algorithm at all (much less a polynomial time one) to identify the quantum circuit C_x. Show that $BQ(\mathcal{G}, 0) = ALL$ if $\mathcal{G}$ is universal. Deduce that $BQ(\mathcal{G}, \delta) = ALL$ for any $0 < \delta < 1$ if $\mathcal{G}$ is universal. [Hint: your answer shouldn't need to be longer than one paragraph.]

(b) Show that if $\mathcal{G}$ is universal and $1/2 \leq \delta \leq 1$, then $BQP(\mathcal{G}, \delta) = ALL$. [Hint: your answer should only need to be two or three sentences.]

(c) Suppose, as I suggest but didn't say precisely in the notes, that we modify the definition of $BQP(\mathcal{G}, \delta)$ to the following:

$L \in BQP(\mathcal{G}, \delta)$ if there exists a classical (deterministic) polynomial-time algorithm which, for each integer $n \geq 1$, outputs a description of a quantum circuit C_n over $\mathcal{G}$ such that, for all bit strings $x \in \{0,1\}^n$, measuring the first qubit $C_n |x0 \cdots 0\rangle$ in the computational basis satisfies

$$\textit{prob}\left(\text{Output}(C_n) = L(x) \mid |x0 \cdots 0\rangle\right) \geq 1 - \delta.$$

Show that these two definitions give equal complexity classes. [Hint: as suggested in class, the distinction is simply about whether or not we "hard-code" the value of x into the circuit. Your answer shouldn't need to be more than a few sentences and a couple pictures.]

(d) (**Extra credit**) Suppose we let $\delta = 1/2$ and modify the definition of $BQP(\mathcal{G}, \delta)$ so that the greater-than-or-equal to sign "$\geq$" is now a strict inequality "$>$". Is this a "reasonable" complexity class? Do there exist uncomputable problems in it?

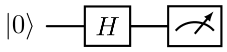
Proof. (a) Considering $\text{BQ}(\mathcal{G}, \delta)$ is equivalent to $\text{BQP}(\mathcal{G}, \delta)$, except that we remove the condition for our quantum circuit C_x over $\mathcal{G}$ to be prepared algorithmically. Now consider $\text{BQ}(\mathcal{G}, 0)$, then

$$\mathbb{P}(\text{OUTPUT}(C_x) = L(x)) \geq 1 = 1.$$

Thus, $\text{BQ}(\mathcal{G}, 0) = \text{ALL}$. Of course, here we are assuming that $\mathcal{G}$ is universal to be able to output a description of C_x.

Since, by definition, $\text{BQ}(\mathcal{G}, 0) \subseteq \text{BQ}(\mathcal{G}, \delta)$, then $\text{BQ}(\mathcal{G}, \delta) = \text{ALL}$.

(b) For any decision $L(x)$, let the algorithmically produced quantum circuit be the simple Hadamard gate,



Then, we have

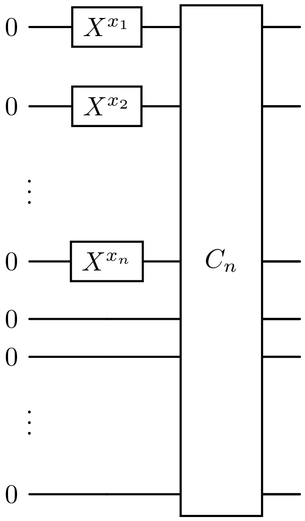
$$\mathbb{P}(\text{OUTPUT}(C_x) = L(x)) = \frac{1}{2} \geq 1 - \delta.$$

If $\frac{1}{2} \leq \delta \leq 1$, then $L \in \mathrm{BQP}(\mathcal{G}, \delta)$. Since this works of all L, then $\mathrm{BQP}(\mathcal{G}, \delta) = \mathrm{ALL}$.

(c) Call the definition from the lecture notes as Def_1 and the definition in the problem as Def_2.

$\boxed{\mathrm{Def}_2 \implies \mathrm{Def}_1}$

Suppose we have a circuit C_n for all bit-strings x of length n with input $|x0\cdots 0\rangle$. Our goal is to find C_x. Let $x = x_1 x_2 \cdots x_n$, then C_x is given by



■

Problem 2

Let $x \in \{0,1\}^n$ be a bit string of length n. Show that

$$H^{\otimes n} |x\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle .$$

Proof. We know that

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad \text{and} \qquad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

We have

$$\begin{aligned}
H^{\otimes n} |x\rangle &= H^{\otimes n} |x_0 x_1 \cdots x_n\rangle \\
&= H|x_0\rangle \otimes H|x_1\rangle \otimes \cdots \otimes H|x_{n-1}\rangle \\
&= \bigotimes_{i=0}^{2^n-1} H|x_i\rangle \\
&= \bigotimes_{i=0}^{2^n-1} \frac{|0\rangle + (-1)^{x_i}|1\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{i=0}^{2^n-1} |0\rangle + (-1)^{x_i}|1\rangle \\
&= \frac{1}{\sqrt{2^n}} \left[(-1)^{x_0}|00\cdots 0\rangle + (-1)^{x_{n-1}}|00\cdots 1\rangle + \cdots + (-1)^{x_0 \cdot x_1 \cdots x_{n-1}}|11\cdots 1\rangle\right] \\
&= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle ,
\end{aligned}$$

where $x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-1} y_{n-1}$. ■

Problem 1.1
(Probabilistic classical algorithm) Suppose that the problem is not to distinguish between the constant and balanced functions with certainty, but rather, with some probability of error $< 1/2$. What is the performance of the best classical algorithm for this problem?

Proof. A Boolean function $f : \{0,1\}^n \to \{0,1\}$ is said to be balanced if $f(x) = 1$ for exactly half of all possible 2^n values of x.
Evaluating only once does not give us any information about whether or not f is constant or balanced, so our success rate after a single evaluation is $\epsilon = \frac{1}{2}$, since it is a random guess.
Consider now the case where we do two evaluations:

- If we obtain two different results, then we immediately conclude that f is balanced.
- If we obtain two results that are the same, then if f is balanced, the probability that the first evaluation returned the given result is $\frac{1}{2}$, and the probability that the second evaluation returned the same result as the first is $\frac{2^{n-1}-1}{2^n-1}$ (as there are 2^{n-1} of each result of 0 and 1, 2^n total results, $2^{n-1}-1$ of the given result left after the first evaluation, and $2^n - 1$ total uninvestigated cases after the first evaluation).

Therefore, if f is balanced, this occurs with probability $\frac{1}{2}\frac{2^{n-1}-1}{2^n-1}$, which we can see is

$$2^{n-1} < 2^n \implies \frac{2^{n-1}-1}{2^n-1} < 1 \implies \frac{1}{2}\left(\frac{2^{n-1}-1}{2^n-1}\right) < \frac{1}{2}.$$

Thus, if we get the same result in two evaluations, we can conclude that f is constant with error $\epsilon < \frac{1}{2}$.
Therefore, only 2 evaluations are required for this algorithm. ■

Problem 4
Suppose Alice has a state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$. Show that if she and Bob share n Bell pairs $|\beta_{00}\rangle$, then to teleport her state $|\psi\rangle$ to Bob, it suffices to simply teleport each qubit in her state to Bob one at a time using the single qubit teleportation protocol. [Hint: induction. $n = 2$ is the most interesting case.]

Proof. Denote Alice's state as

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle ,$$

where α_i are complex amplitudes and $|i\rangle$ represents the computational basis states of n qubits. The single qubit teleportation protocol works as follows:

1. Alice performs a Bell measurement on the qubit she wants to teleport and her corresponding qubit from the shared Bell pair.
2. Alice sends the classical result of the measurement to Bob.
3. Depending on the measurement outcome, Bob applies a set of unitary operations (identity, X, Z, or XZ) to his remaining qubit to recover the state $|\psi\rangle$.

Now, let's proceed with the proof by induction.

- **Base case:** When $n = 1$, Alice has a single qubit state $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$. Teleporting this state using the single qubit teleportation protocol is straightforward and well-known.
- **Inductive hypothesis:** Assume that for some $k \geq 1$, teleporting an k-qubit state using k shared Bell pairs via the single qubit teleportation protocol is successful.

- **Inductive step:** Consider the case when $n = k + 1$. We want to show that if Alice and Bob share $k + 1$ Bell pairs, Alice can teleport her $(k + 1)$-qubit state to Bob using the single qubit teleportation protocol applied sequentially.
- **Proof:** Alice can isolate the first qubit of her state $|\psi\rangle$ and the first qubit from the first Bell pair, then perform a Bell measurement and send the result to Bob. Bob receives this classical information and performs the necessary unitary operations on his remaining qubits to obtain the state of Alice's first qubit. Now, Alice and Bob are left with k qubits each. By the inductive hypothesis, Alice can use the remaining k Bell pairs to teleport her remaining k-qubit state to Bob's k qubits one at a time. Thus, the claim holds for all n.

Therefore, to teleport Alice's n-qubit state $|\psi\rangle$ to Bob, it suffices to teleport each qubit in her state to Bob one at a time using the single qubit teleportation protocol. ■

Problem 6

I said something slightly misleading/incomplete in class during lecture 5.2 when I sketched the idea of the proof that BQP is in $PSPACE$. Recall that I proved a lemma: for any $\epsilon > 0$, any bit strings $x, y \in \{0, 1\}^n$ and any quantum circuit C on n qubits (over some fixed gate set $\mathcal{G}$), we may compute an approximation to the amplitude $\langle y|C|x\rangle$ in $PSPACE$ in the size of the circuit C.

After that, I very hastily explained that from here, we could, in $PSPACE$, decide whether or not the probability that the first qubit of the output of $C|0\cdots0\rangle$ returns 0 is $< 1/3$ or $\geq 2/3$, and thus, decide whether the circuit is answering YES or NO.

I had insinuated that we only needed the case $\epsilon = 1/3$ in the lemma, but this is not true strictly speaking as I explained it (but see problem 7(b) below, in which case it is!). We need to be able to compute these amplitudes to precision $\frac{1}{2^n}$ for the argument that $BQP \subseteq PSPACE$ to work. Note: The amplitudes in the computational basis of course in principal determine the *marginal* probability that the first bit returns, say, 1, but we need to know the amplitudes to exponential precision if we want to know this marginal probability to $O(1)$ precision.

With this in mind, prove the following: for any quantum circuit C on n qubits (over some fixed gate set $\mathcal{G}$) and any two bit strings $x, y \in \{0, 1\}^n$, we may compute a complex number z such that

$$|z - \langle y|C|x\rangle| < \frac{1}{2^n}$$

in $PSPACE$ (as a function of the size of C).

Proof. The quantum circuit C is related to a decision problem in BQP, then the size of C is a polynomial. Suppose $C = U_1 U_2 \cdots U_{p(n)}$, then

$$\langle y|C|x\rangle = \sum_{x_1,\ldots,x_{p(n)-1}} \left\langle y\middle|U_{p(n)}\middle|x_{p(n)-1}\right\rangle \left\langle x_{p(n)-1}\middle|U_{p(n)-2}\right\rangle \cdots \langle U_2|x_1\rangle \langle x_1|U_1|x\rangle\,.$$

We want to compute an approximation of z within an error of $\frac{1}{2^n}$. Suppose every matrix element is represented with an accuracy of $\frac{1}{2^m}$. Moreover, suppose we have an error in the multiplication of two terms (rounding error) which is $O\left(\frac{1}{2^m}\right)$. We have the multiplication of $p(n)$ terms, resulting in a total error of $\frac{p(n)}{2^m}$. Computing the sum means adding these numbers, resulting in $(2^n)^{p(n)}$ total addition operations. Suppose, again, that each addition operation results in an error $\frac{1}{2^m}$.

- If addition is perfect and multiplication is error-prone, then the total error is $\frac{p(n)}{2^m}$. Then, we need to have

$$\begin{aligned} \frac{p(n)}{2^m} &< \frac{1}{2^n} \\ 2^m &> p(n)2^n \\ m &> n + \log(p(n)) \\ \implies m &\in \Theta(n). \end{aligned}$$

- If multiplication is perfect and addition is error-prone, then the total error is $\frac{(2^n)^{p(n)}}{2^m}$. Then, we need to have

  $$\begin{aligned} \frac{(2^n)^{p(n)}}{2^m} &< \frac{1}{2^n} \\ 2^m &> (2^n)^{p(n)+1} \\ m &> n(p(n)+1) \\ \implies m &\in \Theta(q(n)), \end{aligned}$$

  where $q(n)$ is a polynomial in n.

Since m represents the number of bits needed to store z, then we need a polynomial space in n to approximate $\langle y|C|x\rangle$ to n bits.
Therefore, we may compute a complex number z such that

$$|z - \langle y|C|x\rangle| < \frac{1}{2^n}$$

in $PSPACE$. ■

Problem 7
In this problem we will explore some examples of "BQP-universal" problems.

(a) Suppose you had the power to decide the following problem: given a description of a quantum circuit C on n qubits, decide if the probability that C outputs 1 in its first qubit when input the basis state $|0\cdots 0\rangle$ is greater than or equal to 2/3.

Show that you could use your power (together with classical polynomial time effort) to solve every problem in BQP. (This should only take one short paragraph to explain. It should follow essentially from the definition of BQP).

Proof. Assume $L \in BQP(\mathcal{G}, \delta)$, then we can algorithmically generate a quantum circuit C_x such that

$$\mathbb{P}(\text{OUTPUT}(C_x) = L(x) \mid |00\cdots 0\rangle) \geq 1 - \delta,$$

where $0 < \delta < \frac{1}{2}$.
Having the freedom to choose δ, take $\delta = \frac{1}{3}$, and now we have $L(x) = 0$ or $L(x) = 1$. It must be that if

$$\mathbb{P}(\text{OUTPUT}(C_x) = 1) \geq \frac{2}{3},$$

then $L(x) = 1$. Otherwise, $L(x) = 0$.
In fact, we have

- If $\mathbb{P}(\text{OUTPUT}(C_x) = 1) \geq \frac{2}{3}$ and $L(x) = 0$, then it means that

  $$\mathbb{P}(\text{OUTPUT}(C_x) = L(x)) < \frac{1}{3},$$

  which is a bad circuit to begin with.

- If $\mathbb{P}(\text{OUTPUT}(C_x) = 1) < \frac{2}{3}$ and $L(x) = 1$, then it means that

  $$\mathbb{P}(\text{OUTPUT}(C_x) = L(x)) < \frac{2}{3},$$

  which is also a contradiction.

■