CS 593/MA 592 - Intro to Quantum Computation
Homework 4

Due Monday, February 19 at 8pm (upload to Brightspace)

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).

1. For this problem, you will need to use the definition of $BQP(\mathcal{G}, \delta)$ I give 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 $0 \leq \delta \leq 1$ 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 of $C_n|x0\ldots0\rangle$ in the computational basis satisfies
      $$prob(\text{Output}(C_n) = L(x) \mid |x0\ldots0\rangle) \geq 1 - \delta.$$

   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?

2. Let $x \in \{0,1\}^n$ be a bit string of length n. Show that
$$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y}|y\rangle.$$

3. Do Exercise 1.1 in Nielsen and Chuang.

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.]

5. Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, and define two unitaries

$$\begin{aligned} U_f : (\mathbb{C}^2)^{\otimes n+1} &\to (\mathbb{C}^2)^{\otimes n+1} \\ |x, a\rangle &\mapsto |x, a \oplus f(x)\rangle \end{aligned}$$

$$\begin{aligned} R_f : (\mathbb{C}^2)^{\otimes n} &\to (\mathbb{C}^2)^{\otimes n} \\ |x\rangle &\mapsto (-1)^{f(x)}|x\rangle \end{aligned}$$

where $x \in \{0,1\}^n$ and $a \in \{0,1\}$.

Using only "standard" gates (like Hadamards or CNOTs), show how to implement U_f with a circuit involving R_f, a few additional gates and maybe a few additional ancillas. Do the converse too.

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 $C|0\cdots 0\rangle$ 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 $1/2^n$ for the argument that $BQP \subseteq PSPACE$ to work.[1]

   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).

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).

   (b) Now, instead, suppose you had the following power: given a description of a quantum circuit C with the promise that either $|\langle 0|C|0\rangle|^2 \geq 2/3$ or $|\langle 0|C|0\rangle|^2 \leq 1/3$, decide which of the two is the case.

   Show that you could use this power (together with classical polynomial time effort) to solve every problem in BQP. To do so, you should use *uncomputation* to convert every quantum circuit C that solves an instance of a problem in BQP to another quantum circuit C' satisfying the above promise. See the figure below.

[1] 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.

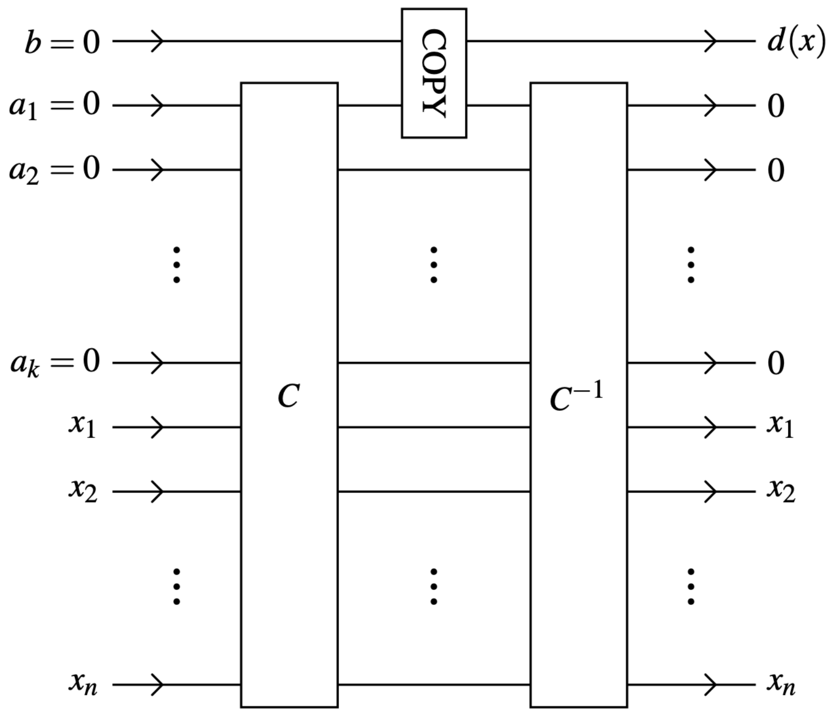

Figure 5. Using uncomputation to reset ancilla values.