CSE 291 / Math 277A - Quantum Complexity Theory (Fall 2025)
Homework 3
Due Monday, November 3, 11:59pm

Instructions: Note: It is highly recommended (though not required) that you type your answers. It is your responsibility to make any handwriting clear and legible for grading. You may work with 1-2 other collaborators, but you must write the solutions separately and clearly mark the names of all people you worked with on each problem.

Problems:

1. **Two-level gates are exactly universal**

   One of the more remarkable aspects of quantum computation is that a few types of elementary operations suffice for universality. In the last homework, we explored universality in a computational sense—we can simulate any BQP computation using gates with only real amplitudes. In this problem, we will prove a more straightforward type of universality—any complex unitary can be decomposed as a product of gates from a simple gate set.

   Let's call a unitary *two-level* if it only acts nontrivially on two or fewer vector elements. So, for example, the following are examples of two-level unitaries:

$$\begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}$$

   where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is a 2×2 complex unitary matrix. Show that an arbitrary $d \times d$ unitary matrix can be decomposed as a product of two-level unitaries. Note that for the most part in this class we've focused on n-qubit unitaries, which act only the Hilbert space $(\mathbb{C}^2)^{\otimes n}$. For this problem (and often other applications), it helps to forget about that structure and just think about $d \times d$ matrices U such that $UU^\dagger = I$.

   Hint: Starting with an arbitrary unitary matrix, can you apply a two-level unitary and simplify some small part of it?

   The decomposition of U into two-level unitaries is one way to show that U can be decomposed into 1- and 2-qubit gates. That is, we now only need to show how to decompose an arbitrary two-level unitary. The questions below break down this decomposition into two steps. This is just to satisfy curiosity. These questions will not be graded!

   (a) [Optional,not graded] Show that every n-qubit two-level unitary U can be written as the product $PC^{n-1}(V)P^\dagger$, where P is a permutation and $C^{n-1}(V)$ is the single-qubit unitary gate V on qubit n controlled on the first $n-1$ qubits. That is, for all $x \in \{0,1\}$ and $y \in \{0,1\}^{n-1}$

$$C^{n-1}(V)(|y\rangle \otimes |x\rangle) = \begin{cases} |y\rangle \otimes |x\rangle & \text{if } y \neq 1^{n-1} \\ |y\rangle \otimes (V|x\rangle) & \text{if } y = 1^{n-1} \end{cases}$$

(b) [Optional, not graded] Show that every $C^{n-1}(V)$ gate can be decomposed into a product of Toffoli gates and $C^1(V)$ gates. Conclude that Toffoli plus all one- and two-qubit gates can generate any unitary. While it is not strictly required, it is easier to show this decomposition when ancilla qubits are allowed.

2. **What if we just add more quantum to our quantum complexity class?**

Recall that in the formal definition of BQP, the quantum circuit descriptions are generated by a poly-time classical Turing machine. Consider a variant BQQP (Bounded Error Quantum Quantum Polynomial Time) where the quantum circuit descriptions are themselves generated by a quantum circuit. That is, if we measure all qubits in the output of a quantum circuit, we get a (probability distribution over) encodings of another quantum circuit. You may assume the encodings are of some reasonable form (e.g., a list of gates and the qubits they act on).

In summary, a language is in BQQP if there exists a poly-time uniform family of quantum circuits whose output is an encoding of another quantum circuit that decides the language (i.e., for an input in the language, the probability the encoded circuit accepts the input is at least 2/3; and for inputs outside the language, the probability the encoded circuit accepts the input is at most 1/3.)

Prove that BQQP = BQP.

3. **Simulating BQP with counting machines**

Let $C(x, r)$ be any circuit taking an input $x \in \{0,1\}^n$ and auxillary string $r \in \{0,1\}^m$. Define

$$\Delta_C(x) = |\{r : C(x,r) = 1\}| - |\{r : C(x,r) = 0\}|$$

to be the number of strings r causing C to accept minus the number of strings r causing C to reject. Using this notation, we could define the complexity class PP in the following way:

Probabilistic Polynomial Time (PP)
$L \in$ PP if there exists a poly-time uniform family of poly-size classical circuits $\{C_n\}_{n=0}^{\infty}$ such that on input $x \in \{0,1\}^n$

- If $x \in L$, then $\Delta_C(x) > 0$
- If $x \notin L$, then $\Delta_C(x) \leq 0$

Let's define a new class of problems for which the threshold is no longer set directly at 0, but rather, there is some exponential threshold that you are close to (in the "yes" case) or far from (in the "no" case).

Almost Wide Probabilistic Polynomial Time (AWPP)
$L \in$ AWPP if for every polynomial r, there is a polynomial p and a poly-time uniform family of poly-size classical circuits $\{C_n\}_{n=0}^{\infty}$ such that on input $x \in \{0,1\}^n$

- If $x \in L$, then $(1 - 2^{-r(n)}) \leq \Delta_C(x)/2^{p(n)} \leq 1$

- If $x \notin L$, then $0 \leq \Delta_C(x)/2^{p(n)} \leq 2^{-r(n)}$

It is known that $\mathsf{AWPP} \subseteq \mathsf{PP}$, but it is not known if $\mathsf{PP} \subseteq \mathsf{AWPP}$. In other words, if we can prove $\mathsf{BQP} \subseteq \mathsf{AWPP}$, then we have improved the result $\mathsf{BQP} \subseteq \mathsf{PP}$ shown in class. In fact, this is exactly what we will show in this problem. Moreover, AWPP is the smallest-known classical complexity class that contains BQP. To be clear, AWPP is quite a bit more contrived than PP, but it is instructive nevertheless.

Let $L \in \mathsf{BQP}$ be a language recognized by the quantum circuit family $\{Q_n\}_{n=0}^{\infty}$. Before we prove that $L \in \mathsf{AWPP}$, let's restrict the form of the circuit family. For example, we have already shown that we can assume without of generality that

- Each circuit Q_n is comprised of Hadamard and Toffoli gates.
- If $x \in L$, Q_n accepts x with high probability ($1 - 2^{-r(n)}$ for any polynomial r)
- If $x \notin L$, Q_n accepts x with low probability ($2^{-r(n)}$ for any polynomial r)

(a) Show that for every quantum circuit Q_n, there is an equivalent poly-size circuit Q'_n where the probability of accepting $x \in \{0,1\}^n$ is only based on a *single* outcome (i.e., measuring all of the output bits, rather than just the first output bit). That is,

- If $x \in L$, then $|\langle x, 0^m| Q'_n |x, 0^m\rangle|^2 \geq 2/3$
- If $x \notin L$, then $|\langle x, 0^m| Q'_n |x, 0^m\rangle|^2 \leq 1/3$

Hint: Use a trick called "uncomputing". The idea is as follows: if we start in a state $|x, 0^m\rangle$ and apply Q, we get the state $|\psi\rangle = Q|x, 0^m\rangle$. If we were to then apply $Q^\dagger$ to $|\psi\rangle$, we end back in the state $|x, 0^m\rangle$. The insight is that we can still "uncompute" (i.e., apply $Q^\dagger$) even when we start from a state that is only close to $|\psi\rangle$.

(b) Show that there is a poly-size classical circuit C_n such that

$$|\langle x, 0^m| Q_n |x, 0^m\rangle|^2 = \left(\frac{\Delta_{C_n}(x)}{\sqrt{2^{h(n)}}}\right)^2$$

where $h(n)$ is the number of Hadamard gates in Q_n.

(c) [Optional question, not graded] For each C_n, show there is a poly-size circuit D_n such that $\Delta_C(x)^2 = \Delta_D(x)$.

(d) Show that $L \in \mathsf{AWPP}$.

Note 1: You may assume there is a black-box way to amplify the acceptance probabilities in part (a) to $2^{-r(n)}$ vs $1 - 2^{-r(n)}$ for arbitrary polynomial r.

Note 2: In the above questions, I haven't asked you to reason about uniformity. Since almost all reasonable approaches will lead to uniform circuit families, you are not being asked to show this.

4. **Project precursor problems**

The purpose of this problem is to practice generating research ideas in quantum complexity theory. Concretely, your goal is to write down (at least) 2 research questions that

you don't know the answer to. You should write these questions with the intention that one of them may become the basis for your final project in this class (you will repeat this exercise on future homework).

For each question, you should pick some topic/theorem/area that we've learned about in class and propose some way to extend it. To reiterate—the purpose is to practice coming up with interesting *questions*, not necessarily answers. You also shouldn't yet worry about whether or not your question has been already answered somewhere in the quantum literature.