CSE 291 / Math 277A - Quantum Complexity Theory (Fall 2025)
Homework 4
Due Friday, November 14, 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. **A decision version of Simon's problem**

Let's start by recalling the "search variant" of Simon's problem introduced in class:

Simon's problem

Function:	$f\colon \{0,1\}^n \to \{0,1\}^n$
Promise:	Outputs of f are paired by secret $s \in \{0,1\}^n$. That is, $f(x) = f(y)$ iff $x \oplus y = s$.
Question:	Determine the secret string s.

This is a *search problem* because the goal is to output the entire secret bitstring s. The goal for this problem is to understand a decision-variant of Simon's problem, where the goal will be to simply answer some yes/no question about the secret bitstring s.

To start, we need a slight generalization of the analysis for Simon's algorithm that we performed in class. Recall that for that analysis, we implicitly assumed that $s \neq 0^n$.

(a) Show that there this is a polynomial-time quantum query algorithm that always outputs the secret bitstring (with high probability), including the case where s is the all-zeros string.

Notice that whether or not $s = 0^n$ induces a dichotomy in the functions f satisfying the Simon's promise: if $s \neq 0^n$, then f is 2-to-1; if $s = 0^n$, then f is 1-to-1. A *k-to-1 function* f is such that every element in the image of f has exactly k inputs that map to it.

Let's now define a decision variant of Simon's problem based on this fact: given oracle access to a function f satisfying the Simon's promise, output "YES" if the function is 2-to-1 and output "NO" if the function is 1-to-1.

Our goal for the next couple of problems will be to see how this language fits into the complexity class NP, so let's start by giving a definition of NP in this oracle setting: a promise language $L = (\Pi_{\text{yes}}, \Pi_{\text{no}})$ is in NP if there exists a poly-time uniform family of poly-size classical circuits $\{C_n\}_{n=0}^{\infty}$ such that for all $f\colon \{0,1\}^n \to \{0,1\}^n$

- If $f \in \Pi_{\text{yes}}$, then $C_n(y) = 1$ for some $y \in \{0,1\}^{\mathsf{poly}(n)}$
- If $f \in \Pi_{\text{no}}$, then $C_n(y) = 0$ for all $y \in \{0,1\}^{\mathsf{poly}(n)}$

It's worth emphasizing that the circuits in this description have oracle access to f (i.e., can apply f as a gate). For the decision Simon's problem, Π_{yes} is the set of of all functions that satisfy Simon's promise with some secret string $s \neq 0$, and Π_{no} is the set of functions satisfying Simon's promise with $s = 0^n$.

(b) Show that the decision Simon's problem is in NP.
Hint: what is an efficiently verifiable certificate showing that f is 2-to-1?

Let's look at what happens if we were to flip the YES and NO instances of Simon's problem. That is, in the flipped Simon's problem, output "YES" if f is 1-to-1 and "NO" if f is 2-to-1. Using part (a), this version of the problem is no different than the previous one for a quantum computer—just find s and decide accordingly. However, for a NP machine, this change makes a big difference.

(c) Show that the flipped Simon's problem is not in NP.
Hint: Is there a certificate for f being 1-to-1? Concretely, if C_n can output 1 for some $f \in \Pi_{yes}$, can you trick C_n into outputting 1 for some function $g \in \Pi_{no}$?

While you're not being asked to show this, the flipped Simon's problem implies there is an oracle $\mathcal{O}$ relative to which $\mathsf{BQP}^{\mathcal{O}} \not\subseteq \mathsf{NP}^{\mathcal{O}}$. This gives evidence that $\mathsf{BQP} \neq \mathsf{NP}$.

2. **Parallel Grover search**

Grover's algorithm shows that the unstructed search problem can be solved using $O(\sqrt{2^n})$ quantum queries. In this question we ask if this algorithm can be parallelized. Specifically, let's consider a new generic outline for an arbitrary query algorithm that applies k oracles in parallel:

$$U_T O_f^{\otimes k} U_{T-1} \cdots U_1 O_f^{\otimes k} U_0 \left|0^{nk}\right\rangle$$

That is, the algorithm alternates between applying unitary gates $U_i \in \mathbb{C}^{2^{nk} \times 2^{nk}}$ and k oracle gates in parallel (i.e., $O_f^{\otimes k}$).

(a) Show that there is quantum algorithm of the above form that solves the unstructured search problem in depth $T = O(\sqrt{2^n/k})$.
Hint: Use Grover's algorithm.

Suppose that we wanted to devise an algorithm where the quantum queries were "maximally parallel", that is, $T = 1$ and all oracles are applied in a single layer. The above algorithm suggests that we need to set $k = 2^n$. In other words, we've completely lost the Grover speedup! We'd like to get a parallelization scaling that goes as $1/k$, but instead we have an algorithm that scales as $1/\sqrt{k}$.

(b) Modify the BBBV lower bound to show that such scaling is unavoidable. That is, show that every quantum algorithm making k queries in parallel requires oracle depth $T = \Omega(\sqrt{2^n/k})$.
Hint: How do you define a new "query magnitude" so that it properly captures all the basis states that are queried during a parallel layer of oracle gates?

3. **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.