Assignment 7
Due: 11:59pm, Thursday, November 11, 2021

1. **Analysis of Grover's algorithm for some special densities of satisfying inputs [20 points; 5 each].** Let $f : \{0,1\}^n \to \{0,1\}$ (where $n \geq 2$). Recall that Grover's algorithm creates the initial state $H|00...0\rangle|-\rangle$ and then iterates the operation $-HU_0HU_f$.

   In each case below, determine the state after one single iteration of Grover's algorithm. Also, what's the probability that, if this state is measured, the outcome is a satisfying input to f?

   (a) The case where f has no satisfying inputs.

   (b) The case where f has $\frac{1}{4}2^n$ satisfying inputs.

   (c) The case where f has $\frac{1}{2}2^n$ satisfying inputs.

   (d) The case where f has 2^n satisfying inputs.

2. **Search problem when the density of inputs is $\frac{1}{2}$ [5 points].** Suppose you know that $f : \{0,1\}^n \to \{0,1\}$ has $\frac{1}{2}2^n$ satisfying inputs, but you have no idea where they are. Classically, you can find a satisfying input with high probability by making f-queries at random points; however, in order to be *guaranteed* to find a satisfying input requires many queries. Give a quantum algorithm that finds a satisfying input with one single f-query.

3. **Searching for a secret state [5 points].** Suppose that $|\psi\rangle$ is a secret n-qubit state. You have no idea what this state is, and your goal is to create it. How? What you are given is two n-qubit unitary operations as black-boxes.

   The first unitary B maps $|0^n\rangle$ to a state that has overlap $\frac{1}{2}$ with $|\psi\rangle$, in the sense that

$$\langle\psi|B|0^n\rangle = \tfrac{1}{2}. \tag{1}$$

   The second unitary U_ψ has the property that

$$U_\psi|\phi\rangle = \begin{cases} -|\phi\rangle & \text{if } \ |\phi\rangle = |\psi\rangle \\ |\phi\rangle & \text{if } \langle\phi|\psi\rangle = 0. \end{cases} \tag{2}$$

   (This is equivalent to saying that $U_\psi = I - 2|\psi\rangle\langle\psi|$.)

   Show how to construct an n-qubit quantum circuit that maps the state $|0^n\rangle$ to the state $|\psi\rangle$, where the circuit can use U_ψ, B, and B^* operations as its gates, as well as additional unitary operations that you can choose.[1]

   If you get stuck, there's a hint on the next page ... but first try this without the hint.

[1] Of course, the additional unitaries of your choosing cannot depend on what $|\psi\rangle$ is, which is unknown to you.

Hint for question 3 (first try without looking at this)

Consider the ideas behind Grover's algorithm, in the case where f has $\frac{1}{4}2^n$ satisfying inputs (as in question 1(b)).

You are already given one reflection, U_ψ.

Can you construct a useful second reflection, using B, B^*, and a unitary operation of your own choosing?