CS 190/264: Quantum Computation *Instructor: Sandy Irani*

Homework 7

Due: November 28, 2018, 2PM

Note: Undergraduates should do problems 1-4, and graduate students should do problems 2-5.

1. The function $f : \{0,1\}^n \to \{0,1\}$ is defined as $f(x) = 0$ for every $x \neq a$, and $f(a) = 1$, for some n-bit string a. Express the state of the system after five steps of Grover search using the oracle O_f.

2. Define $|\Psi\rangle = H^{\otimes n}|0\cdots 0\rangle$. Show that the operations $2|\Psi\rangle\langle\Psi| - I$ applied to a general state $\sum_x \alpha_x |x\rangle$ produces
$$\sum_x \left[-\alpha_x + 2\langle\alpha\rangle\right]|x\rangle,$$
where $\langle\alpha\rangle = \sum_x \alpha_x/2^n$ For this reason the operation $2|\Psi\rangle\langle\Psi| - I$ is sometimes called *inversion about the mean*.

3. Give a circuit which will compute $(2|0\cdots 0\rangle\langle 0\cdots 0| - I)$ on n-qubits. You can use auxiliary qubits if you need to but these should be initialized to $|0\rangle$ and reset back to $|0\rangle$ at the output of the circuit.

4. Describe what happens in Grover's algorithm if the function U_f is used where f is the all 0's function. That is, $f(x) = 0$ for every n-bit string x.

5. Suppose that a boolean function $f : \{0,1\}^n \to \{0,1\}$ has M solutions. That is, the number of x such that $f(x) = 1$ is M. Prove that any quantum circuit which has the usual black-box access to f requires $\Omega(\sqrt{N/M})$ queries to f in the worst case to find an a such that $f(a) = 1$ with at least constant probability.