

Homework 8

Due: December 5, 2018, 2PM

Note: Undergraduates should do problems 1-5, and graduate students should do problems 3-6.

- Suppose you are given black box access to a function $f : \{0, 1\}^{12} \rightarrow \{0, 1\}$ via the usual unitary U_f . The number of distinct 12-bit strings x such that $f(x) = 1$ is 57. Suppose you use Grover's Algorithm to find a specific 12-bit string x such that $f(x) = 1$.
 - What is the optimal number of iterations of Grover's Algorithm in this case?
 - If you iterate Grover's Algorithm for the optimal number of iterations, then what is the probability that the string you measure causes f to evaluate to 1?
- Suppose that you use the approximate counting algorithm presented in class to estimate $|\{x \mid f(x) = 1\}|$ for some function $f : \{0, 1\}^{20} \rightarrow \{0, 1\}$. The number of auxiliary bits $m = 12$. At the end of the algorithm you measure the string 000001111101. What is your best guess for $|\{x \mid f(x) = 1\}|$?
- Suppose that you use the approximate counting algorithm presented in class to estimate $M = |\{x \mid f(x) = 1\}|$ for some function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. The number of auxiliary bits is m . Consider the idealized case in which $\sin(\pi\phi) = \sqrt{M/2^n}$ and $\phi = j/2^m$ for some integer j . When the m bits are measured at the end of the quantum circuit, what are the possible outcomes and the probabilities of each outcome?

You may need the fact that the eigenvectors of the matrix

$$\begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}.$$

are

$$|v_1\rangle = \begin{pmatrix} i \\ 1 \end{pmatrix} \quad |v_2\rangle = \begin{pmatrix} -i \\ 1 \end{pmatrix}.$$

- Give a quantum circuit that on input $|000\rangle$ outputs $\frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)$. You should only require the typical gates used in class: H , X , Z , CNOT, Fredken (controlled swap).
- Give a quantum circuit that computes $I_{(1,2,3)} - 2(|10\rangle\langle 10| \otimes I_{(3)})$. $I_{(1,2,3)}$ is the identity operator on qubits 1, 2, and 3. $I_{(3)}$ is the identity operator on qubit 3. You should only require the typical gates used in class: H , X , Z , CNOT, Fredken (controlled swap). 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.
- Prove that at the end of the phase estimation algorithm, with at least constant probability, the measured outcome is an integer j such that $|j/2^m - \phi| \leq 2^{-(m+1)}$.