Introduction to Quantum Information Science
Homework 11

Due Thursday, December 5th at 11:59 PM

Note: You should explain your reasoning, i.e. show your work, for all problems. You do not need to show us every step of each calculation, but every answer should include an explanation *written with words* of what you did.

1. Optimize Grover [6 Points] Suppose Grover's algorithm is used to search a list of size N containing a single marked item. Recall that, after t queries, the probability of having found the marked item is approximately $\sin^2\left(2t/\sqrt{N}\right)$. After approximately how many queries should you halt the algorithm if your goal is to maximize the success probability per unit of time invested? Give a formula in terms of N that works asymptotically for sufficiently large N, and explain how you derived it. Feel free to use any numerical software of your choice for approximating constants in your formula, but you must still explain your formula analytically (your final solution cannot be based only on generalizing a pattern from a few values of t).

2. The diffusion operator Recall the $N \times N$ Grover diffusion matrix D, whose diagonal entries are all $\frac{2}{N} - 1$ and whose off-diagonal entries are all $\frac{2}{N}$.

a) [2 Points] Prove that D is indeed a unitary matrix.

b) [3 Points] Prove that, up to scalar multiplication, D is actually the *only* real orthogonal matrix whose diagonal entries are all the same and whose off-diagonal entries are all the same, other than the identity matrix. This provides a big hint about how one might have discovered D if one didn't already know Grover's algorithm.

c) [3 Points] Recall $D = H^{\otimes n} A H^{\otimes n}$, where A is the diagonal matrix $\text{diag}\,(1, -1, -1, \ldots, -1)$. Show an actual circuit made of Toffoli gates, Hadamard gates, X gates, and Phase gates for applying A. Your circuit should have $O(n) = O(\log N)$ gates and is allowed to use ancilla qubits initialized to any state you like provided that you return them to that state afterwards.

3. Grover's Algorithm with Multiple Marked Items:

a) [4 Points] Given a list of size N, which is promised to contain K marked items, suppose we want to find any one of the marked items. In class, we saw when we apply Grover's algorithm unmodified to the N-element list, we have a constant probability of observing a marked item if we halt the algorithm and measure after only $O(\sqrt{N/K})$ queries.

Suppose that we cannot / don't want to apply Grover's algorithm to the entire N-element list, and instead apply Grover's algorithm to lists of size N/K. Show how we can still accomplish our original goal of finding any one of K marked items in a list of size N using $O(\sqrt{N/K})$ queries. Explain why this algorithm succeeds with constant probability (an informal, but still complete, explanation is okay).

Be precise when describing your algorithm.

b) [4 Points] Assume Grover's algorithm is optimal for the single marked item case, as proved in class. Prove that it's optimal for the multiple marked item case as well. In other words, let N and K be given. Show that any quantum algorithm that finds a marked item with constant probability, given an N-element unordered list that contains K marked items, ***must*** use $\Omega(\sqrt{N/K})$ queries to the list.
Hint: given a hypothetical quantum algorithm that was faster, can you derive a contradiction in the single-marked-item case?

c) [3 Points] Now suppose you want to find not just any one of the K marked items, but you want to find all of them. Show that Grover's algorithm can be used to do that as well with constant success probability using $O(\sqrt{NK}\log(N))$ queries.

4. [Extra Credit] The Graph Connectivity Problem In the Graph Connectivity problem, we're given an n-vertex undirected graph G in adjacency matrix format. In other words, we have an oracle that given any basis state of the form $|i,j,a\rangle$, where $i,j \in \{1,...,n\}$ and $a \in \{0,1\}$, maps the basis state to $|i,j,\text{NOT}(a)\rangle$ if G contains an edge between vertices i and j or to $|i,j,a\rangle$ otherwise. The problem is to decide whether G is connected — in other words, whether every vertex is reachable from every other.

a) [Extra Credit, 3 Points] Prove that any possible classical algorithm for this problem – even a randomized algorithm that succeeds with high probability – must make $\Omega(n^2)$ queries to the adjacency matrix. (An informal proof is okay here — we won't grade as strictly as in HW9.)
Hint: Find an example of a family of graphs such that, given a graph G from that family, a brute-force search among $\Omega(n^2)$ potential edges is the only way to decide whether G is connected.

b) [Extra Credit, 4 Points] Give a quantum algorithm that solves this problem with high probability and that makes only $O(n^{3/2}\log(n))$ queries. Prove it.
Hint: You're welcome to use Grover's algorithm as an ingredient in your algorithm, as well as your favorite classical graph search algorithms like BFS/DFS/Dijkstra! Just make sure that the error probability stays bounded.

c) [Extra Credit, 5 Points] Show that any quantum algorithm for Graph Connectivity must make $\Omega(n)$ queries.

Hint: Combine your answer from part a with the BBBV Theorem, which shows that Grover's algorithm is optimal, in the sense that $\Omega(\sqrt{M})$ quantum queries are needed to compute the OR of M independent bits.

5. The 4-Qubit Code

a) [3 Points] Show that the 4-qubit code

$$|0\rangle \rightarrow \frac{(|00\rangle + |11\rangle)^{\otimes 2}}{2},$$

$$|1\rangle \rightarrow \frac{(|00\rangle - |11\rangle)^{\otimes 2}}{2}$$

can *detect* either a bit flip or a phase flip on any of the 4 qubits.

b) [2 Points] Show that the 4-qubit code from part (a) cannot *correct* a bit flip.

c) [2 Points] Show that the 4-qubit code from part (a) cannot correct a phase flip error.

6. Error detecting code In class, we saw the simplest classical error-correcting code, which encodes one bit into three bits via $\bar{0} = 000$ and $\bar{1} = 111$, and which corrects any single bit-flip error. We then saw the quantum generalization of that code, the Shor 9-bit code, which encodes 1 qubit into 9 qubits via:

$$|\bar{0}\rangle = \frac{(|000\rangle + |111\rangle)^{\otimes 3}}{2\sqrt{2}}; \qquad |\bar{1}\rangle = \frac{(|000\rangle - |111\rangle)^{\otimes 3}}{2\sqrt{2}}$$

and which corrects any single bit-flip or phase-flip error — and therefore, by linearity, any single-qubit error at all.

a) [3 Points] Prove that any classical encoding of a single bit, which corrects an arbitrary single bit-flip error, requires at least 3 bits for the codewords, i.e. there is no such code using 2 bits.

b) [2 Points] A weaker notion than an error-correcting code is an error-*detecting* code — one that detects whether an error has occurred, though doesn't necessarily help correct the error. Give a classical error-detecting code which encodes 1 bit into 2 bits and which detects a single bit-flip error.

c) [2 Points] Now give a quantum error-detecting code which encodes 1 qubit into 2 qubits and which detects a single phase-flip error.

d) [3 Points] Give a quantum error-detecting code which encodes 1 qubit into 4 qubits and which detects a single bit-flip error or a single phase-flip error (the code is allowed to fail if both errors occur simultaneously).
Hint: Adapt the Shor code.

e) [2 Points] Consider the quantum code $|\bar{0}\rangle = |00\rangle$ and $|\bar{1}\rangle = |11\rangle$. Give an example of a qubit encoded using this code and a single-qubit error on the encoded qubit such that this code fails to even *detect* the error.