Homework 9

Introduction to Quantum Information Science
Due Monday, April 17th at 11:59 PM

1. In the continued fraction step of Shor's algorithm, recall that we needed the following key fact: if a given real number, say x, is sufficiently close to a rational number a/b with a "conspicuously large denominator," then that rational number is unique. Prove that, indeed, there can be at most one rational a/b, with a and b positive integers, that's at most ϵ away from x and that satisfies $b < 1/\sqrt{2\epsilon}$. Explain how this relates to the choice, in Shor's algorithm, to choose Q to be quadratically larger than the integer N that we're trying to factor. *Hint: Recall that the achievable precision, ϵ, goes inversely with the dimension Q of the Fourier transform.*

2. 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 $\sin^2(2T/\sqrt{N})$. After approximately how many queries should you halt the algorithm, if your goal is to maximize the success probability per unit of time invested? (Feel free to give a numerical answer, and to use any software of your choice.)

3. Grover's Algorithm with Multiple Marked Items:

a) 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 a classical reduction implying that Grover's algorithm can be used to solve this problem with only $\mathcal{O}(\sqrt{N/K})$ queries. But suppose, instead, that we just apply Grover's algorithm – the same algorithm from the single marked item case – directly to the N-element list, without first picking a random subset of size N/K. Show that, in this case as well, we have a constant probability of observing a marked item if we halt the algorithm and measure after only $\mathcal{O}(\sqrt{N/K})$ queries.

b) 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) Now suppose you want to find, not just one of the marked items, but all K of them. Show that Grover's algorithm can be used to do that as well, with constant success probability, using $\mathcal{O}(\sqrt{NK}\log(N))$ queries to the list. Or for extra credit, eliminate the $\log(N)$ factor and show that $\mathcal{O}(\sqrt{NK})$ queries suffice.

4. 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) 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.

b) Give a quantum algorithm that solves this problem with high probability, and that makes only $\mathcal{O}(n^{3/2} \log(n))$ queries. *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) Show that any quantum algorithm for Graph Connectivity must make $\Omega(n)$ queries. (For this, you can assume the optimality of Grover's algorithm.)