QUANTUM COMPUTATION - EXERCISE 4

Due: December 30 (submission in pairs).

1. Breaking The RSA Cryptosystem

1.1. Describe the RSA public-key cryptosystem.

1.2. Suppose you are given a black box that runs Shor's algorithm and finds the order of an element in a group. Show how an eavesdropper can use the black box to read a message that was encrypted with the RSA public-key *directly* (i.e without factoring N).

2. l_2 Norm

In the lower bound we saw in class for a quantum search in the black box model, we used the following fact: We have two vectors (on $n \geq 1$ qubits). Suppose $\Pr(0)$ when measuring the first qubit in the vector $|v_1\rangle$ is larger than $2/3$. Suppose $\Pr(0)$ when measuring the first qubit in the vector $|v_2\rangle$ is smaller than $1/3$. Then $\| \, |v_1\rangle - |v_2\rangle \, \|_2$ is at least $1/10$. Prove this fact.

3. Quantum Algorithms With Intermediate Measurements

Suppose we have a quantum algorithm which is allowed to perform intermediate measurements (in the standard basis) and proceed according to the results of all the previous measurements. Prove that there is a quantum algorithm that uses only unitary operations, and measures only at the end, which performs the same task, and simulates the first algorithm in polynomial time and space.

Remark 1. *Observe that in the lower bound for database search we allowed only unitary transformations. The theorem you just proved shows that the lower bound applies also for algorithms which are allowed to perform intermediate measurements.*

4. Grover's Algorithm

We use $\tilde{O}(N)$to denote a function that is $O(N)$ up to polylogarithmic factors in N.

4.1. Suppose the number of marked items in the database is exactly 1. How many Grover iterations should we apply in order to maximize our probability of success? What is the best approximation you can give to that optimal success probability?

4.2. Suppose the number of marked items in the database is exactly M, where $1 < M \ll N$. How many Grover iterations should we apply in order to maximize our probability of success? What is the best approximation you can give to that optimal success probability?

4.3. Design an algorithm that would work in time $\tilde{O}(\sqrt{N/M})$ even if you don't know M, but you know that M is in the range 2^i to 2^{i+1}.

4.4. Suppose now that $0 \leq M \ll N$, and suppose that we don't know M *a priori*. Show how Grover's algorithm can be used to find a marked item in time $\tilde{O}(\sqrt{N/M})$, or output an appropriate message in the case there is no marked item in the database. (**Hint:** use question 4.3, and do binary search. Explain how you check that an item is indeed a *good* item, and in what circumstances you output the *no solution* message.)

4.5. Explain how to adopt your answer to question 4.4, to solve any NP decision problem, with quadratic speedup over a classical exhaustive search.