QUANTUM COMPUTATION - FALL 2006 - EXERCISE 3

Due: Wednesday 21/12/05. Submition in triplets, to the TIRGUL.

1. Teleportation

1.1. Consider a qubit which is entangled to another qubit and their joint state is $|\alpha\rangle$. If we teleport the first qubit to another location, what is the final state of the whole system?

1.2. Suppose Alice and Bob share two pairs of EPR states, and they wish to apply Teleportation of a state of two qubits instead of one. The two qubits may be in an arbitrary quantum state. Write a quantum circuit that does the trick, and prove that it works for any initial state of two qubits.

2. Measuring In A Non Standard Basis

Let $|\alpha\rangle$ be an arbitrary state in a Hilbert space of dimension n, and let $V = \{|v_1\rangle, \ldots, |v_n\rangle\}$ be an orthonormal basis to that space. Show that there exist a unitary matrix U, such that measuring $|\alpha\rangle$ in the basis V is equivalent to measuring $|U\alpha\rangle$ in the *standard* basis.

3. Locality

Consider a bipartite quantum state $|\psi\rangle_{A,B}$. Show that if Alice performs an arbitrary unitary operation on her part of the system, and then Bob measures his qubits in the standard basis, then the measurement outcome is independent of Alice's actions.

Conclude that there is no measurement that Bob can perform to tell which unitary operation Alice performed on her qubits.

4. Principle Of Delayed Measurement

4.1. Show that measuring a qubit in the standard basis commutes with the operations NOT and Toffoli, and also with any operation of the type Control-U, for any unitary U (when the measurement is of the control qubit).

4.2. Suppose we have a quantum algorithm (circuit) which is allowed to perform intermediate measurements (in the standard basis) and proceed according to the results of all the previous measurements (namely, the gates which we apply might depend on the results of the measurements). Prove that there is a quantum algorithm (circuit) 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.

5. Quantum Vs. Classical Number Of Queries

5.1. Suppose you are given a function on n bit strings, $f_a(x) = a \cdot x \mod 2$ (the function depends on the n bit string a). You have access to the function via a black box. Your goal is to find the string a. How many queries would you need classically? Give an algorithm and prove why you would need that many queries.

5.2. Apply the same ideas from the Deutch Josza and the Simon algorithm to derive a quantum algorithm that will discover a in as few queries as possible. How many queries would you need? Prove that your algorithm is correct.

6. Fourier Transform

6.1. Describe the matrix that applies the Fourier transform over the group $\mathbb{Z}_4^n$. Design an efficient quantum circuit to apply this transformation. Analyze its complexity.

6.2. Consider two functions, f and h, from the Abelian group modulo N to the complex numbers. Define a third function g, called the *convolution* of f and h, and denoted $g = f * h$, by

$$g(x) = f * h(x) = \sum_{y=0}^{N-1} f(y)h(x-y).$$

Denote by $\hat{f}$ the Fourier transform of f, i.e. $\hat{f} = FT_N \cdot f$. Prove that for every x it holds that

$$(f \hat{*} h)(x) = \hat{f}(x) \cdot \hat{h}(x).$$