MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MIT 2.111/8.411/6.898/18.435
Quantum Information Science I

September 30, 2010

Problem Set #5
(due in class, 14-Oct-10)

1. **Most unitary transforms are hard to approximate**.

   (a) Show that there exist $O(2^{n2^n})$ distinct boolean functions of n bits.

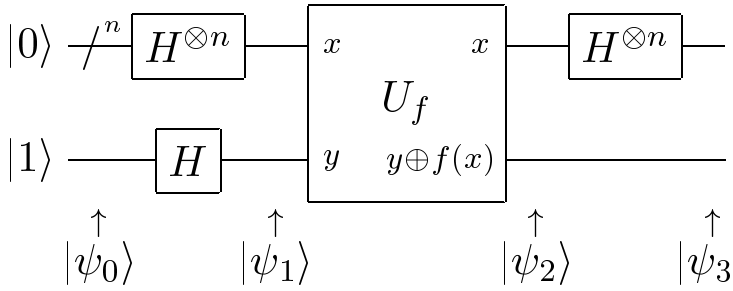
   (b) Show that a (classical) circuit composed of n NAND gates can implement at most $O(n^{2n})$ distinct boolean functions.

   (c) Show that an arbitrary unitary transform applied to n qubits is described by $O(2^{2n})$ real degrees of freedom.

   (d) How many distinct unitary transforms can be produced by a quantum circuit composed of n controlled-NOT, Hadamard, and T gates?

2. **Deutsch-Jozsa algorithm and its generalizations**. Let $f(x)$ be a function which maps n bits to one bit, which is implemented by a unitary transform U_f, satisfying $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, where the first register contains n qubits, and the second, one qubit.

   (a) Give the quantum states $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$, arising in this quantum circuit:



   (b) Suppose that we are promised $f(x)$ is either constant for all possible values of x, or balancecd, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half. What results are obtained for these two cases (constant and balanced), when the n qubits of the top register are measured?

   (c) Suppose that the function is $f_j(x) = x \cdot j$, where j is an n-bit integer, and $x \cdot j = \sum_k x_k j_k$ is the binary dot product of the binary representations of the two numbers. What result is obtained when the n qubits of the top register are measured?

3. **Gates needed in the quantum Fourier transform**. Give a decomposition of the controlled-R_k gate into single qubit and CNOT gates.

4. **Addition by Fourier transforms**. Consider the task of constructing a quantum circuit to compute $|x\rangle \rightarrow |x + y \mod 2^n\rangle$, where y is a fixed constant, and $0 \leq x < 2^n$. Show that one efficient way to do this, for values of y such as 1, is to first perform a quantum Fourier transform, then to apply single qubit phase shifts, then an inverse Fourier transform. What values of y can be added easily this way, and how many operations are required?

5. **Recent quantum algorithms**. Find a recent paper in the literature about quantum algorithms (theory – not implementation), and write a short ($<$ 500 word) summary of it, on the QIS wiki. See instructions, and suggestions for sources in the literature, on the course homepage, `http://web.mit.edu/2.111/`