Sam Ocko October 15, 2010

Problem Set # 5 Solutions

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

   (a) We are dealing with boolean functions that take n bits as input and output n bits. Each boolean function function has 2^n possible inputs, and it's output for each of these is described by n bits. Therefore, since it takes $n2^n$ bits to describe an arbitrary boolean function, meaning that there are 2^{n2^n} different boolean functions which take in n bits and output n bits.

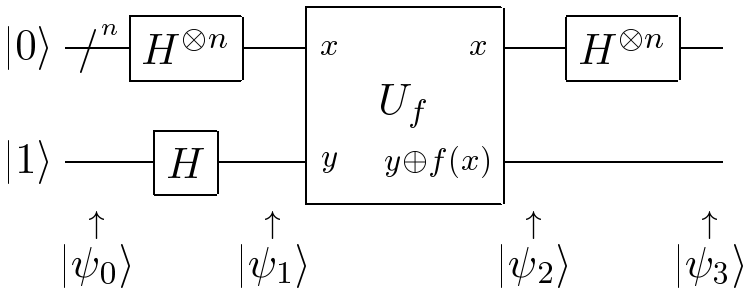
   (b) Any circuit of n NAND gates can take at most $2n$ bits, and can be described(redundantly) by a sequence of n steps each involving a single NAND gate. At each step, there are $\binom{N}{2}$ possible ways to have a NAND gate(You choose each of the two inputs). Since there are n such steps, there are at most $\binom{n}{2}^n$ possible circuits. $\binom{n}{2}^n < \left(n^2\right)^n = n^{2n}$, and thus a classical circuit composed of n NAND gates can implement at most $O(n^{2n})$ boolean functions.

   (c) An arbitrary $N \cdot N$ matrix has N^2 complex degrees of freedom. For a matrix to be unitary there are $\binom{N}{2} + N$ complex constraints(Each pair of columns is orthogonal + Normalization of each column). Therefore, an arbitrary unitary matrix has $O(N^2)$ degrees of freedom. For a system of n qubits, $N = 2^n$, and therefore an arbitrary unitary transform has $O(N^2) = O((2^n)^2) = O(2^{2n})$ degrees of freedom.

   (d) We use a similar reasoning that we did in part b. Any quantum circuit of n CNOT, Hadamard, and T gates can affect at most $2n$ qubits and may be described(redundantly) by a sequence of n steps, each involving a single CNOT, Hadamard, or T gate. At each step, there are $\binom{n}{2} + 2 \cdot n$ possible gates to apply, and thus there are at most $O((n^2)^n) = O(n^{2n})$ possible unitary transforms.

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:



$$|\psi_0\rangle = |0\rangle_1 \otimes |0\rangle_2$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle_1 \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)_2 \right)$$

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2^n}} \sum_x \left(|x\rangle_1 \otimes \frac{1}{\sqrt{2}} (|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)_2 \right) \\ &= \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle_1 \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)_2 \right) \end{aligned}$$

$$|\psi_3\rangle = \frac{1}{2^n} \left(\sum_y |y\rangle_1 \sum_x (-1)^{f(x)+x\cdot y} \right) \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)_2 \right)$$

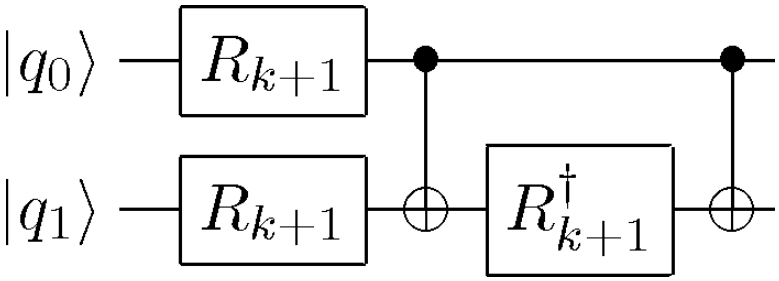
   (b) When f(x) is constant, then $\sum_x (-1)^{f(x)} = \pm 2^n$, $|\psi_3\rangle = \pm |0\rangle_1 \otimes \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)_2 \right)$ and thus we will measure all the bits in register 1 to be 0. When f(x) is balanced, then $\sum_x (-1)^{f(x)} = 0$, $\langle 0|_1 |\psi_3\rangle = 0$, and thus we will never measure all the bits in register 1 to be 0.

   (c) **Lemma:** $\sum_x (-1)^{y \cdot x} = 2^n \delta_{xy}$
   Therefore,

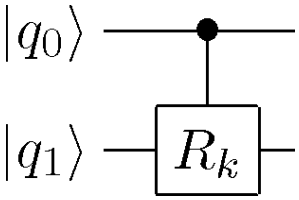
$$|\psi_3\rangle = \frac{1}{2^n}\left(\sum_y |y\rangle_1 \sum_x (-1)^{x\cdot j + x\cdot y}\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_2\right)$$
$$= \frac{1}{2^n}\left(\sum_y |y\rangle_1 \, 2^n \delta_{j,y}\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_2\right)$$
$$= |j\rangle_1 \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_2\right)$$

And thus we will always measure the first register to be j.

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



This circuit is equivalent to



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?

   To add a number by a quantum fourier transform we first apply a quantum fourier transform, then apply an appropriate set of phase shifts, then reverse the transform.

$$|x\rangle \underbrace{\rightarrow}_{QFT} \frac{1}{\sqrt{2^n}} \sum_k e^{\frac{2\pi i k x}{2^n}} |k\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_k e^{\frac{2\pi i k (x+y)}{2^n}} \underbrace{\rightarrow}_{QFT^{-1}} \rightarrow |x + y \bmod 2^n\rangle$$

To apply this phase shift we must be able to apply: $|k\rangle \rightarrow e^{\frac{2\pi i y k}{2^n}} |k\rangle$ Since both k and y are

written in binary, we write them in terms of their bits:

$$k = \sum_{j=0}^{n} k_j 2^j$$
$$y = \sum_{j=0}^{n} y_j 2^j$$

Therefore:

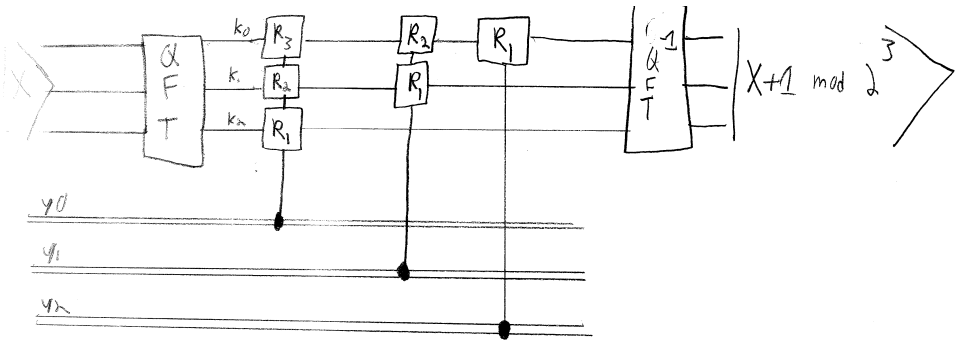
$$k * y = \sum_{j=0}^{n} \sum_{j'=0}^{n} 2^{j+j'} k_j y_{j'}$$

And written in terms of the qubits of $|k\rangle$, we want to apply the unitary

$$\bigotimes_j |k_j\rangle \rightarrow \bigotimes_j \left(\prod_{j'} e^{\frac{2\pi i y_{j'} k_j}{2^{n-j'-j}}} |k_j\rangle \right)$$

Therefore, we may decompose this unitary in terms of phase shifts of the qubits $|k\rangle$ controlled by the bits in y, where for each qubit k_j, bit $y_{j'}$, we apply a $R_{n-j-j'}$ gate on qubit k_j controlled by bit y'_j. We notice that $R_k = I$ for all $k \leq 0$, and thus we don't need to apply gates for pairs where $j + j' \geq n$.

For example, the 3-qubit circuit is:



Where

$$R_j = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^j}} \end{pmatrix}$$

When y is a power of two, we only have to apply a few gates. The larger power of two y is, the fewer gates we have to apply. For example, when $y = 2^{n-1}$, we only need to apply one gate between the Quantum Fourier transforms.

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.

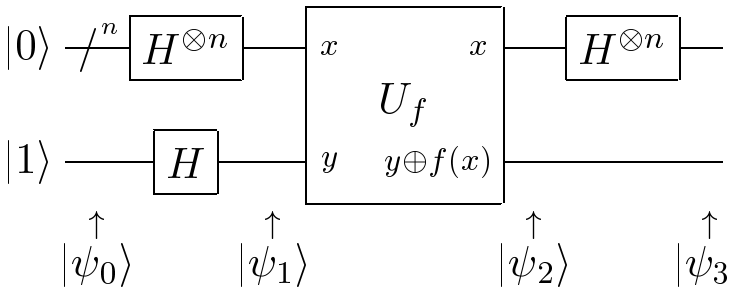
   (b) Show that a (classical) circuit composed of n NAND gates can implement at most $O(n^{2n})$ distinct boolean functions.

   (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/`