QIC 710 Problem Set 3 (due Thursday, 10/14/10)

1. Prove that we can assume without loss of generality that all amplitudes in a quantum computation are real numbers, by showing that any quantum circuit with two-qubit gates can be simulated with an equivalent quantum circuit with three-qubit gates (and the same number of gates), such that all amplitudes in the simulating circuit are real.

2. Using $U_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$ and phase kickback, we have seen how to implement the unitary $U'_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$. Now assume that you are given U'_f, and show how to implement U_f.

3. Simon's problem generalized: Let $y_1, \ldots, y_k \in \{0,1\}^n$ be distinct, nonzero strings. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a 2^k-to-1 function satisfying $f(x) = f(x \oplus y_j)$ for $j = 1, \ldots, k$. Give a quantum query algorithm, using U_f, that outputs a basis for the space spanned by the $\{y_j\}$, making as few calls to U_f as you can. Justify intuitively (no proof is required) what is the classical query complexity of this problem?

4. Consider the quantum circuit for computing the Fourier transform mod 2^n presented in class; it uses $\Theta(n^2)$ basic gates. Now assume that you only want to compute the Fourier transform approximately to within ϵ (in operator norm). How much more efficient can you make the circuit?

5. Let $a|N$ and $b|N$. What is the Fourier transform mod N of the uniform superposition on all $0 \leq x < N$ such that $a|x$ or $b|x$? (Notation: $x|y$, read "x divides y," means that y is an integer multiple of x.)