COS 598A
March 1, 2002
Due: March 15, 2002

Homework Set 2

Problem 1 This problem is about reversible classical circuits.
(a) Prove that the 3-bit Toffoli gate cannot be implemented using only 1-bit and 2-bit reversible gates (even allowing extra scratch pad bits).
(b) Design a clean reversible classical circuit for computing $(\neg(x_1 \wedge x_2)) \wedge (((\neg x_1) \wedge x_3) \wedge x_4)$, using 1-bit negation gates, 2-bit control-NOT gates, and 3-bit Toffoli gates.

Problem 2 In class, an implementation of the 3-bit quantum Toffoli gate was given, with the use of only 1-bit and 2-bit quantum gates. Prove that the construction computes the correct function.

Problem 3 This problem shows the universality of 1-bit quantum gates and 2-bit quantum CNOT gates as a complete set of primitives for quantum computation.
(a) Prove that any 2-bit quantum gate can be implemented using only 1-bit quantum gates and 2-bit quantum CNOT gates, without introducing extra scatch pad bits.
(b) Prove that any n-bit unitary transformation can be implemented as a quantum circuit using only 1-bit and 2-bit quantum gates, without introducing extra scratch pad bits.

Problem 4 Give a (non-quantum) polynomial time algorithm for factoring an input integer N where N is a power of some unknown prime.

Problem 5 In class an element $a \in Z_N^*$ is called *good*, if its period s is even and $a^{s/2} mod N \neq -1$. Let c_N be the probability that a random element a uniformly chosen from Z_N^* is good. Calculate c_N for $N = 35$.

Problem 6 Consider Shor's quantum factoring applied to input integer N, using quantum Fourier transform QF_M.
(a) Determine the probability of success in one run of the algorithm, for $N = 15$ and $M = 4096$.
(b) Repeat (a) for $N = 35$ and $M = 4096$.