18.435/2.111 Homework # 4

Due Thursday, October 9.

1: This problem is in Nielsen and Chuang, but I left my copy at home. Suppose you want to do a quantum Fourier transform, and immediately measure the results, but your system only can perform one-qubit gates. Show how you can obtain the results of a quantum Fourier transform using just measurements and one-qubit gates (which may be conditioned on the results of classical outcomes of the measurements).

2: Suppose you have a quantum phase oracle that takes

$$|\, x\rangle \rightarrow (-1)^{f(x)} \,|\, x\rangle$$

where f is a function from strings of n bits to $\{0, 1\}$ such that there is a c such that $f(x) = f(x + c)$.

2a: Modify Simon's algorithm to show how you can find a vector t such that $t \cdot c$ is even without using any extra work qubits.

2b: Suppose that $f(x) = 0$ except for two values, d and $d + c$, which have $f(x) = 1$. Approximately how many times do you need to run the algorithm in part (a) before you find a non-zero t? How many function evaluations will it take you to find c? How does this compare to the time it would take on a classical computer?

2c: Suppose that f is random except for the condtion that $f(x) = f(x + c)$. Show that Simon's algorithm is efficient in this case.