18.435/2.111 Homework # 5

Due Thursday, October 19

1: Suppose you have a function f such that there is a unique $y \neq 0$ with

$$\begin{aligned} f(y) &= 1 \\ f(x) &= 0 \qquad\qquad \text{if } x \neq y \end{aligned}$$

If you define g so

$$\begin{aligned} g(0) &= 1 \\ g(x) &= f(x) \qquad\qquad \text{if } x \neq 0 \end{aligned}$$

then g has a unique c such that $g(x+c) = g(x)$. Finding this c would be equivalent to solving an NP-complete problem. Because g is not two-to-one, Simon's algorithm does not necessarily work on it. But exactly how does Simon's algorithm stop working if you try to apply it to g? Would it work for some functions h where $h(x+c) = h(x)$, but h is not strictly two-to-one?

2: Explain how you would adapt Simon's algorithm to find c if you had a three-to-one function over a ternary alphabet (0,1,2 mod 3) such that

$$f(x) = f(x+c)$$

for some non-zero c.

3: Exercise 5.6 in Nielsen and Chuang.
The quantum circuit construction of the quantum Fourier transform apparently requires gates of exponential precision in the number of qubits used. However, such precision is never required in any quantum circuit of polynomial size. For example, let U be the ideal quantum Fourier transform on N qubits, and V be the transform which results if the controlled-R_k gates are performed to a precision $\Delta = 1/p(n)$ for some polynomial $p(n)$. Show that the error $E(U,V) \equiv \max_{|\psi\rangle} ||(U-V)\,|\psi\rangle\,||$ scales as $n^2/p(n)$, and thus polynomial precision in each gate is sufficient to guarantee polynomial accuracy in the output state.