Tfy-44.140 Quantum computing 6. Exercise Spring 2007 23.4.2007
Nakahara, Voutilainen

1. Shor's algorithm
a) Factorize $N = 35$ using the algorithm described in Sec. 8.2 of the lecture notes.If you happen to choose such m that the algorithm is completed already after the first step, choose again. There are m's whose period is less than 10 so that if your m does not give $P < 10$, try another m.

b) Let $N = 4$ and $m = 3$. Find the wave function $|\psi_3\rangle$ and Prob(y) $(y \in S_n)$.

c) Suppose we have a general two-register system, each consisting of n qubits. Let $f(x)$ be a periodic function with the period P and apply a transformation yielding the state

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x, f(x)\rangle \tag{1}$$

Show that after applying DFT on this state, the observation of the first register yields one of the values

$$0, \frac{1 \cdot 2^n}{P}, \frac{2 \cdot 2^n}{P}, \frac{3 \cdot 2^n}{P}, \ldots, \frac{(P-1) \cdot 2^n}{P}. \tag{2}$$

The cancellation observed here is extensively used in the Shor's algorithm.

2. Suppose you have two n qubit registers initialized to state where all bits are zero. The states available to you can be numbered with $x \in S_n = \{0, 1, 2, \ldots N-1\}$, where $N = 2^n$. A normalized but otherwise arbitrary state then reads $|\phi\rangle = \sum_{x=0}^{N-1} w_x |x\rangle, \quad \sum_x |w_x|^2 = 1$.

a) Define a function $f : S_n \to \{0, 1\}$ such that

$$f(x) = \begin{cases} 1 & (x = z) \\ 0 & (x \neq z) \end{cases}, \tag{3}$$

i.e., it gives one only for a single input z and zero for all the others. What do you get by operating with the transformation

$$R_f(x, y) = e^{i\pi f(x)} \delta_{xy} \tag{4}$$

on state $|\phi\rangle$?

b) Define another transformation

$$D = -I + 2|\phi_0\rangle\langle\phi_0|, \quad |\phi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \tag{5}$$

Show that

$$D|\phi\rangle = \sum_{x=0}^{N-1} (\overline{w} - (w_x - \overline{w}))|x\rangle, \quad \overline{w} = \frac{1}{N} \sum_{x=0}^{N-1} w_x. \tag{6}$$

c) Now, use $U_f = DR_f$ on $|\phi\rangle$. What is the result? Repeat the operation k times. What is the result now? Hint: Find first a recursion relation for the coefficients of the states between successive operations of U_f. Then, try to solve the final coefficients from this relation starting from the initial state $|\phi_0\rangle$.

d) Sketch the quantum circuit diagram for the algorithm described above. You are free to use oracles (blocks that instantaneously perform a single task). Can you find any uses for this?