CS 518: Problem Set 4

Section: MW 12-1:30 pm

Total: 100pts Due: 12/14/2015

Problem 1 Euclidean Algorithm: 15pts

Shor's algorithm is to find the order of some function (N is the number we want to factorize, a is a number that is co-prime with N. We want to find the order r such that $a^r \equiv 1 \bmod N$). However, at the end of the day we would need to use Eclidean's algorithm on the calculated r from Shor's algorithm such that we can do factoring (i.e. $\gcd(a^{r/2}-1, N)$ and $\gcd(a^{r/2}+1, N)$). Please prove that Euclidean's algorithm does find the gcd of two given numbers.

Problem 2 Shor's Algorithm: 5 + 15 + 10 + 5 pts

In Shor's algorithm, we have two registers, let say Reg1 and Reg2, and we want to factorize the number N. Reg1 consists of l qubits and that of Reg2 is $n = \lceil \log N \rceil$.
(a) Why is n chosen to be that number?
(b) Why is it required that $N^2 < q = 2^l \leq 2N^2$?
(c) Use Shor's algorithm to find the period of the function $f(x) = 7^x \bmod 10$ by using a Fourier transform over $q = 128$ (in another word, Reg1 has 7 qubits and it is obvious $N^2 = 10^2 < q = 2^7 = 128 \leq 2N^2$). Write down all intermediate superpositions of the algorithm. You may assume youre lucky, meaning the first run of the algorithm already gives a $b = cq/r$ where c is coprime with r.
(d) When we were working on the analysis, we have two cases. One is (I) $r|q$ (this means r divides q) and $rb/q \in \mathbb{Z}$ and the other is (II) $rb/q \notin \mathbb{Z}$. We briefly mentioned that for each measured b, its correponding amplitude should be huge. Why and how is that affecting the complexity of the algorithm? (this is to say, the cost of Shor's algorithm basically comes from continued fraction algorithm ($(\log N)^3 \approx l^3$) while the cost from quantum part is constant. Why?)

Problem 3 Grover's Algorithm: 15 + 5 + 5 + 5 pts

(a) Show that in $\{|G\rangle, |B\rangle\}$ basis, we may write the Grover iteration as

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

where θ is a real number in the range 0 to $\pi/2$ (assuming for simplicity that $M \leq N/2$), chosen so that

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N}.$$

Here N is the size of state (sample) space and M is the number of solutions.
(b-1) Given sample space Ω where $|\Omega| = 2^{10}$ and let $Sx = \{x | f(x) = 1 \wedge x \in \Omega\}$. Let say $|S_x| = 4$ and you run Grover in order to find the possible solutions. What is the number of required invocations of Grover operator? (Please do not directly square root the ratio. Please compute exactly to the **2nd digit** after the decimal point).
(b-2) Please compute the eigenvalues of Grover operator in the $\{|G\rangle, |B\rangle\}$ basis.
(b-3) Let say your answer in (b-1) is T. What is the success probability you obtain a true solution when you measure after running the Grover operator $\lfloor T \rfloor$ times ?

Problem 4 Quantum Phase Estimation (QPE) : 15 + 5 pts

Given an arbitrary Grover operator in the matrix format (let say just like the previous problem).

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

(a) Let suppose we have an input $|k_1k_2k_3\rangle$ to a regular QFT_{2^3}. Please show $\mathrm{QFT}_{2^3}|k_1k_2k_3\rangle$ is equivalent to the first part of QPE (i.e. before QFT inverse) acting on $|000\rangle$ where the unitary U has the eigenvector $|\psi\rangle$ such that $U|\psi\rangle = e^{2\pi i 0.k_1k_2k_3}|\psi\rangle$. [It might be helpful if you draw the circuit because in the textbook, the order has to be reversed].
(b) Please compute the eigenvalue(s) and eigenvector(s) of G.

Problem 5 Random Walk: Bonus: 5 pts

Given a symmetric matrix G (assume all real entries), we know its eigenvalues must be real. Please show that the eigenvectors of distinct eigenvalues of G are orthogonal.