CS 528: Quantum Computation
Problem Set 4

MW: 2:00 - 3:15 pm

Out: 04/8/2019 Due: 04/17/2019

Instructions:
I leave plenty of space on each page for your computation. If you need more sheet, please attach your work right behind the corresponding problem. Please directly hit the point when solving a problem. Cumbersome description might receive fewer credits, even it is correct. If your answer is incorrect but you your logic is on the right track, then partial credits will be given. Please staple your solution and use the space wisely.

First Names:

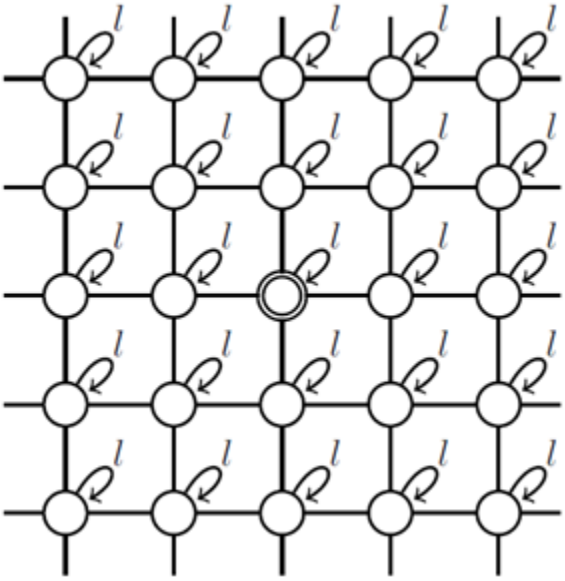
Group ID:

Score: **/190**

Problem 1 Lackadaisical Walk on 2D: 30 pts

We learned about the quantum walk with the coin operator as the regular Hadarmard operator and we know that the spreading speed (wrt to amplitudes), QW has the advantage. However, it remains an open question for QW on 2D and 1D. One of the approach for boosting 2D is by using the Lackdaisical walk "[1]". Please describe the coin operator and simulate the first step of the walk (please keep the variable l) where

Unitary Operator : $U = S(I \otimes C)$
Coin Operator $C = 2|s_c\rangle\langle s_c| - I$,
Initial Coin State: $|s_c\rangle = \frac{1}{\sqrt{4+l}}(|\uparrow\rangle + |\downarrow\rangle + |\rightarrow\rangle + |\leftarrow\rangle + |\circlearrowleft\rangle)$
Initial System State: $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{v=1}^{N} |v\rangle \otimes |s_c\rangle$
And it can be visualized (adding self loop) as the following:



[1] https://arxiv.org/abs/1706.06939

Problem 2 Ex. 8.1.2 in text : 10 pts

Let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ be the uniform superposition. Show that the operator $HU_{0\perp}H$ can be written as $(2\langle\psi|\psi\rangle - I)$

Problem 3 Analysis Technique Proof: 20 pts

(1) Show that $|1 - e^{i\theta}| = 2|\sin(\frac{\theta}{2})|$

(2) Show that $e^{iAx} = cos(x)I + isin(x)A$ where $A^2 = I$ and x is some real number.

Problem 4 Ex. 8.1.3 in text : 10 pts

Prove that any n-qubit state $|\phi\rangle$ that is orthogonal to $H|000\cdots0\rangle$ has the sum of its amplitudes equal to 0.

Problem 5 Ex. 8.2.1 in text: 10 pts

Suppose there are t soluitons to $f(x) = 1$ with $0 < t < N$ with t known. Show how to use amplitude amplication to find a solution with probability at least 2/3 using $O(\sqrt{N/t})$ application of U_f.

Problem 6 Simon's Algorithm: 40 pts

Run Simon's algorithm on the following input x (with $N = 8$):
$x_{000} = x_{101} = 000 \qquad x_{001} = x_{100} = 001$
$x_{010} = x_{111} = 010 \qquad x_{011} = x_{110} = 011$
We notice $x_i = x_{i \oplus 101}$ for all $i \in \{0,1\}^3$, so $s = 101$.
(a) Give the starting state of Simon's algorithm.

(b) Give the state after the first Hadamard transforms on the first 3 qubits.

(c) Give the state after applying the oracle.

(d) Give the state after measuring the second register (the measurement gave $|011\rangle$).

(e) Use $H^{\otimes n}|i\rangle = \frac{1}{\sqrt{2}} \sum_{j \in \{0,1\}^n} (-1)^{i \cdot j} |j\rangle$, give the state after the final Hadamard.

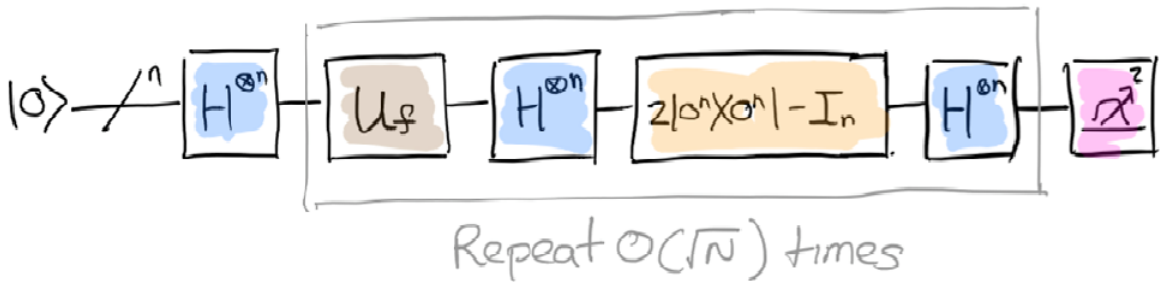
(f) We perform measurement of the first 3 qubits of the final state give the information about s?

(g) If s was 111, then after two runs we obtain $j = 011$ and $j = 101$. With 2 runs, we can determine s. Why?

(h) Is it possible to determine our $s = 101$ in two runs? Why/why not?

Problem 7 Grover's Algorithm: 10 + 5 + 5 + 5 + 5 pts

When we visualize Grover's algorith in circuit model, we can see it as



(a) We know Grover operator is a two-operation operator that $G = (2|\psi\rangle\langle\psi| - I)(I - 2|G\rangle\langle G|$ where $|\psi\rangle = H^{\otimes n}|0^{\otimes n}\rangle$ and $|G\rangle$ is the solution state. Please explain how to implement those two operations in a quantum circuit model.

(b) 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.

(c) Given sample space Ω where $|\Omega| = 2^8$ and let $S = \{x | f(x) = 1 \wedge x \in \Omega\}$. Let say $|S| = 2$ 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 **3rd digit** after the decimal point).

(d) Compute the eigenvalues and eigenvectors of Grover operator in $\{|G\rangle, |B\rangle\}$ basis.

(e) Let say your answer in (c) 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 8 Shor's Algorithm: 5 + 15 + 10 + 10 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?)