CS 410/510 Introduction to Quantum Computing

Homework 3

Portland State U, Spring 2018 — *May 2, 2018, Update: May 16*
Lecturer: Fang Song — *Due: May 18, 2018*

Instructions. Your solutions will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) summary that describes the main idea. For this problem set, a random subset of problems will be graded. Problems marked with "**[G]**" are required for graduate students. Undergraduate students will get bonus points for solving them. Download the TeX file if you want to typeset your solutions using LaTeX.

You may collaborate with others on this problem set. However, you must ***write up your own solutions*** and ***list your collaborators*** for each problem.

1. (QFT and periodic states) Let m be some integer and $M = 2^m$. Denote $\omega_M = e^{2\pi i/M}$ and $[M] = \{0, 1, \ldots, M-1\}$. Recall the Quantum Fourier Transform F_M:

$$\forall x \in [M], \quad |x\rangle \overset{F_M}{\mapsto} \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \omega_M^{xy} |y\rangle \,.$$

   (a) (3 points) Let $|\alpha\rangle := \sum_{x=0}^{M-1} \alpha_x |x\rangle$ be an arbitrary m-qubit state (note: $\sum_{x=0}^{M-1} |\alpha_x|^2 = 1$). Show that

$$F_M|\alpha\rangle = |\hat{\alpha}\rangle := \sum_{y=0}^{M-1} \hat{\alpha}_y |y\rangle \,,$$

   where $\hat{\alpha}_y = \frac{1}{\sqrt{M}} \sum_x \omega_M^{xy} \alpha_x$, for all $y \in [M]$.

   (b) (5 points) (Index shift) Let $j \in [M]$, and define $|\alpha_{+j}\rangle := \sum_x \alpha_x |x + j \bmod M\rangle$. Compute $|\hat{\alpha}_{+j}\rangle := F_M|\alpha_{+j}\rangle =$?. According to your result, explain that measuring $|\hat{\alpha}\rangle$ and $|\hat{\alpha}_{+j}\rangle$ produce the same probability distribution.

   (c) (7 points) (Periodic state) Consider an integer r such that $M = \ell \cdot r$ for some $\ell \in \mathbb{Z}$. Let $b \in \{0, 1, \ldots, r-1\}$. Define

$$|P_{r,b}\rangle := \frac{1}{\sqrt{\ell}} \sum_{k=0}^{\ell-1} |kr + b\rangle = \frac{1}{\sqrt{\ell}} (|0 + b\rangle + |r + b\rangle + \ldots + |(\ell-1)r + b\rangle) \,.$$

   Show that

$$F_M|P_{r,b}\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \omega_r^{bk} |k\ell\rangle = \frac{1}{\sqrt{r}} (|0\rangle + \omega_r{}^b |\ell\rangle + \ldots + \omega_r^{b(r-1)} |(r-1)\ell\rangle) \,.$$

(d) (5 points) Given multiple copies of $|P_{r,b}\rangle$, how to find r?

2. (Shor's algorithm) In this problem, we analyze Shor's algorithm for order finding that we've seen briefly in class. Our goal is to find the order of a mod a positive integer N, i.e., the smallest r such that $a^r = 1 \bmod N$. $E_a : |x\rangle|y\rangle \mapsto |x\rangle|y + a^x \bmod N\rangle$ is the unitary circuit implementing the modular exponentiation function $x \in \mathbb{Z}_{2^m} \mapsto a^x \bmod N$.

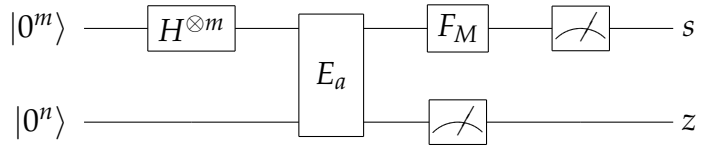

Figure 1: Shor's algorithm

(a) (4 points) Consider the point right after applying E_a. Since the bottom register will no longer be used, we may assume that it gets measured immediately. Suppose that the outcome is $z = a^b \bmod N$ for some $b \in [r]$, what is the state on the top register then?

(b) (4 points) Assuming it happens that $r|M = 2^m$. How to find r?

(c) (4 points) In general, we may not be able to pick an m such that $r|M$ (since we do not know r). In this case ($r \nmid M$), what is the state after applying F_M?

(d) (Bonus 6 points) Continuing part (c), how to find r in the general case?

3. (Grover's algorithm) Consider as usual a function $f : \{0,1\}^n \to \{0,1\}$. Define $A = f^{-1}(1) := \{x \in \{0,1\}^n : f(x) = 1\}$ and $B = f^{-1}(0) := \{x \in \{0,1\}^n : f(x) = 0\}$. Let $a = |A|$ be the number of "marked" items and $b = N - a$ where $N = 2^n$. We further define $|A\rangle := \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle$ and $|B\rangle := \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$.

(a) (4 points) Run Grover's algorithm with f on input $|0^n\rangle$. Namely we apply unitary $G := -HZ_0HZ_f$ repetitively on $|\psi_0\rangle := H|0^n\rangle$ where $Z_0 : |x\rangle \mapsto -|x\rangle$ iff. $x = 0^n$ and $Z_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$. Denote $|\psi^0\rangle = H|0^n\rangle$ and $|\psi^t\rangle := G^t|\psi^0\rangle$ for $t \geq 1$. Show that every $|\psi^t\rangle$ can be written as $\sin(\theta_t)|A\rangle + \cos(\theta_t)|B\rangle$. How does θ_t change to θ_{t+1}? (Hint: geometric interpretation of Grover's algorithm)

(b) (6 points) Show that $|\langle\psi^t|A\rangle|^2 \geq 1/2$ if we pick t to be the nearest integer to $\frac{1}{2}(\frac{\pi}{2\theta_0} - 1)$. As a result, measuring $|\psi^t\rangle$ will give an x of A with probability at least $1/2$. Assuming a is known to us. How to find an element of A with high probability using $O(\sqrt{N/a})$ queries to f?

(c) (Bonus 8 points) What if a is unknown? Show how to find a marked item with probability ≥ 0.99 within $O(\sqrt{N/a})$ queries. (Hint: what if one picks $t \in \{1, \ldots, \sqrt{N} + 1\}$ at random and run Grover's algorithm, how likely will one find a marked element? Then how about picking random $t \in \{1, \ldots T\}$ with a small T in the beginning and try? If fail increment T slowly but exponentially.)

4. (Amplitude estimation) Consider a unitary U on n qubits such that

$$U|0^n\rangle = \sin(\theta)|\psi_A\rangle + \cos(\theta)|\psi_B\rangle\,,$$

with $0 < \theta < \pi/2$, where $|\psi_A\rangle = \sum_{x\in A}\alpha_x|x\rangle$ and $|\psi_B\rangle = \sum_{x\in B}\beta_x|x\rangle$ with $A, B \subseteq \{0,1\}^n$ and $A \cap B = \emptyset$. Let Z_f be an efficient operator such that

$$Z_f|\psi_A\rangle = -|\psi_A\rangle, \quad Z_f|\psi_B\rangle = |\psi_B\rangle\,.$$

The goal is to compute $\sin(\theta)$.

(a) (5 points) Let Q be the rotation of 2θ on the plane spanned by $\{|\psi_A\rangle, |\psi_B\rangle\}$. In particular

$$Q|\psi_A\rangle = \cos(2\theta)|\psi_A\rangle - \sin(2\theta)|\psi_B\rangle, \quad Q|\psi_B\rangle = \sin(2\theta)|\psi_A\rangle + \sin(2\theta)|\psi_B\rangle\,.$$

Show how to implement Q efficiently.

(b) (5 points) Let $|\psi_+\rangle := \frac{1}{\sqrt{2}}(|\psi_B\rangle - i|\psi_A\rangle)$ and $|\psi_-\rangle := \frac{1}{\sqrt{2}}(|\psi_B\rangle + i|\psi_A\rangle)$. Show that $|\psi_+\rangle$ and $|\psi_-\rangle$ are eigenvectors of Q with eigenvalues $e^{i2\theta}$ and $e^{-i2\theta}$ respectively.

(c) (5 points) Design an efficient quantum algorithm to estimate θ. (Hint: how does $H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}}\sum|x\rangle$ relate to $|\psi_+\rangle$ and $|\psi_-\rangle$?)

(d) (Bonus 5 points) Back to Grover's search problem. Can you design a quantum algorithm that (approximately) counts the number of marked elements?

5. (Mixed states and density matrix)

(a) (5 points) A density matrix ρ corresponds to a pure state if and only if $\rho = |\psi\rangle\langle\psi|$. Show that ρ corresponds to a pure state if and only if $Tr(\rho^2) = 1$.

(b) (5 points) Show that every 2×2 density matrix ρ can be expressed as an equally weighted mixture of pure states. That is $\rho = \frac{1}{2}|\psi_1\rangle\langle\psi_1| + \frac{1}{2}|\psi_2\rangle\langle\psi_2|$ (Note: the two states need not be orthogonal).

(c) (5 points) Imagine two parties Alice and Bob. Alice flips a biased coin which is HEADS with probability $\cos^2(\pi/8)$. Alice prepares $|0\rangle$ when she sees coin 0 and $|1\rangle$ otherwise. From Alices perspective (who knows the coin value), the density matrix of the state she created will be either $|0\rangle\langle 0|$ or $|1\rangle\langle 1|$. She then sends the qubit to Bob. What is the density matrix of the state from Bobs perspective (who does not know the coin value)? Write down the matrix.