CSCE 440/640 Quantum Algorithms

Homework 4

Texas A&M U, Spring 2019 — *March 29, 2019*

Lecturer: Fang Song — *Due: April 10, 2019, before class*

Instructions. Only PDF format is accepted (type it or scan clearly). 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. 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.

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 $x \in \mathbb{Z}_{2^m} \mapsto a^x \bmod N$.

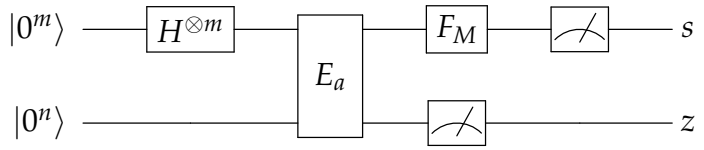

Figure 1: Shor's algorithm

(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?

(e) (Bonus 6 points) In class, we showed that factorization reduces to order finding. Show the converse reduction, i.e., if one can solve factorization efficiently, one can also solve order finding efficiently.

3. (Mixed states and density matrix)

(a) (5 points) A density matrix ρ corresponds to a pure state if and only if $\rho = |\psi\rangle\langle\psi|$ for some $|\psi\rangle$. 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 Alice's 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 Bob's perspective (who does not know the coin value)? Write down the matrix.

(d) (10 points) Let $\{p_i, |\psi_i\rangle\}_{i=0}^1$ and $\{q_j, |\phi_j\rangle\}_{j=0}^1$ be two ensembles of pure states. Define $|\tilde{\psi}_i\rangle = \sqrt{p_i}|\psi_i\rangle$ and $|\tilde{\phi}_j\rangle = \sqrt{q_j}|\phi_j\rangle$ for all i, j. Show that the two ensembles produce the same density matrix **if and only if** there is a unitary $U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$ such that

$$|\tilde{\psi}_0\rangle = u_{00}|\tilde{\phi}_0\rangle + u_{01}|\tilde{\phi}_1\rangle, \text{ and } |\tilde{\psi}_1\rangle = u_{10}|\tilde{\phi}_0\rangle + u_{11}|\tilde{\phi}_1\rangle\,.$$

4. (OR gate as a quantum operation) Recall the binary OR operation, denoted as $\vee$, defined as $a \vee b = 0$ if $a = b = 0$ and $a \vee b = 1$ otherwise. Here we consider operations that map the two-qubit state $|a, b\rangle$ to the one-qubit state $|a \vee b\rangle$, for all $a, b \in \{0, 1\}$. Of course, no unitary operation can perform this mapping, since the input and output dimension do not match; however, general quantum operations can compute this mapping.

   (a) (6 points) Give a sequence of 2×4 matrices $A_1, \ldots, A_k$ with $\sum_{j=1}^k A_j^\dagger A_j = I$ that compute the OR operation in the sense that, for all $a, b \in \{0, 1\}$, when $\rho = |a, b\rangle\langle a, b|$, $\sum_{j=1}^k A_j \rho A_j \dagger = |a \vee b\rangle\langle a \vee b|$.

   (b) (4 points) The operation from part (a) maps all basis states to pure states. Does it map all pure input states to pure output states? Either prove it, or provide a counterexample.

5. (8 points) (Partial trace) Let $\rho_{AB} = (\rho_{ij})_{4\times 4}$, where $\rho_{ij} \in \mathbb{C}, \forall i, j \in \{0, 1, 2, 3\}$, be the density matrix of two qubits A and B. Let $Tr_A(\cdot)$ and $Tr_B(\cdot)$ be the operation that traces out subsystem A and B respectively. Show that

$$Tr_A(\rho_{AB}) = \begin{pmatrix} \rho_{00} + \rho_{22} & \rho_{01} + \rho_{23} \\ \rho_{10} + \rho_{32} & \rho_{11} + \rho_{33} \end{pmatrix} \text{ and } Tr_B(\rho_{AB}) = \begin{pmatrix} \rho_{00} + \rho_{11} & \rho_{02} + \rho_{13} \\ \rho_{20} + \rho_{31} & \rho_{22} + \rho_{33} \end{pmatrix}.$$

6. (Entropy) Let $H(\cdot)$ denote the Shannon entropy and $S(\cdot)$ be the von Neumann entropy. $S(A : B)$ denotes quantum mutual information.

   (a) (5 points) Let X be a random variable taking values in $\{0, \ldots, 2^{m^2}\}$ with probability distribution $p_x = \begin{cases} 1 - 1/m & \text{if } x = 0 \\ \frac{1}{m2^{m^2}} & \text{otherwise} \end{cases}$. Calculate $H(X)$? Conclude that $H(X) \to \infty$ as $m \to \infty$, but one sample of X is almost certainly 0.

   (b) (5 points) Let $\rho = p|0\rangle\langle 0| + (1 - p)|+\rangle\langle +|$. Compute $S(\rho)$. How does it compare to the entropy of a biased coin X where HEADS appears with probability p?