CS 410/510 Introduction to Quantum Computing

Homework 2

Portland State U, Spring 2017 — *April 18, 2017, Update: April 30*

Student: your name — *Due: May 02, 2017*

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) "proof 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.

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. (Norms) For a vector $v = (v_0, \ldots, v_{N-1}) \in \mathbb{C}^N$, let $\|v\| := \sqrt{\sum_{i=0}^{N-1} |v_i|^2}$, which is the usual Euclidean length of v. For any $N \times N$ matrix $M \in \mathbb{C}^{n \times n}$, define its *spectral norm* $\|M\|$ as $\|M\| = \max_{|\psi\rangle} \|M|\psi\rangle\|$, where the maximum is taken over quantum states (i.e., vectors $|\psi\rangle$ such that $\||\psi\rangle\| = 1$). Define the distance between two $N \times N$ unitary matrices U_1 and U_2 as $\|U_1 - U_2\|$.
   (a) (5 points) Show that $\|A - B\| \leq \|A - C\| + \|C - B\|$, for any three $N \times N$ matrices A, B, and C. (Thus, this distance measure satisfies the *triangle inequality*.)
   (b) (5 points) Show that for any A and identity matrix I, $\|A \otimes I\| = \|A\|$.
   (c) (5 points) Show that, for any two $N \times N$ unitary matrices U_1 and U_2, and any matrix A, $\|U_1 A U_2\| = \|A\|$.

   Note: more generally we can define p-norms for $v \in \mathbb{C}^N$ as $\|v\|_p := (\sum_i |v_i|^p)^{1/p}$ for $1 \leq p < \infty$ and $\|v\|_\infty := \max_i\{|v_i|\}$. The Euclidean distance is then the special case $\|\cdot\|_2$. These vector norms give rise to *induced norms* on matrices $M \in \mathbb{C}^{N \times N}$ by $\|M\|_p := \sup\{\|Mv\|_p : v \in \mathbb{C}^N, \|v\|_p = 1\}$. Therefore the spectral norm is the induced Euclidean ($p = 2$) norm.

2. (Quantum Fourier Transform)
   (a) (12 points) Let F_N denote the N-dimensional Fourier transform

$$F_N := \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \cdots & \omega_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)^2} \end{pmatrix}, \text{ where } \omega_N := e^{2\pi i/N} (i = \sqrt{-1})$$

(an $N \times N$ matrix, with entry $\frac{1}{\sqrt{N}} e^{(2\pi i/N)jk}$ position j, k for $j, k \in \{0, 1, \ldots, N-1\}$.

i) Show that all rows in F_N are vectors of length 1, and any two rows are orthogonal.

ii) What is F_N^2? (Hint: The matrix has a very simple form.)

iii) What is the minimum j such that $F_N^j = I$ is the identity?

(b) (5 points) In class, we computed the QFT modulo $N = 2^n$ by a quantum circuit of size $O(n^2)$. Recall that it uses gates of the form

$$R_k = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^k} \end{pmatrix}$$

for $k \in \{2, \ldots, n\}$. Show that $\|R_k - I\| \leq 2\pi/2^k$, where I is the 4×4 identity matrix. (Thus, R_k gets very close to I when k increases.)

(c) (8 points) Here we compute an *approximation* of this QFT within ε by a quantum circuit of size $O(n \log(n/\varepsilon)$. The idea to start with the $O(n^2)$ circuit and then remove some of its R_k gates (it is equivalent to changing the R_k gate to identity gate). Removing an R_k gate makes the circuit smaller but also changes the unitary transformation, but if k is large then from above we can deduce that removing a R_k gate changes the unitary transformation by only a small amount. Show how to use this approach to obtain a quantum circuit of size $O(n \log(n/\varepsilon)$ that computes a unitary transformation $\tilde{F}_N$ such that $\|\tilde{F}_N - F_N\| \leq \varepsilon$. (Hint: Try removing all R_k gates where $k \geq t$, for some carefully chosen threshold t. The properties of our distance measure from the previous question should be useful for your analysis here.) For your reference the quantum circuit for QFT is given below.

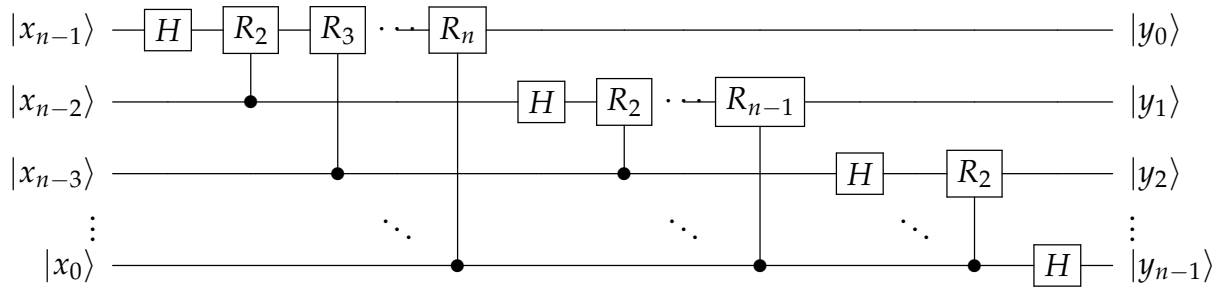

Figure 1: QFT circuit in $\mathbb{Z}_{2^n}$.

3. (Square root of a quantum operation) Let U be a unitary quantum circuit on n qubits. In this problem, we want to construct another circuit that computes a square root of U (i.e., a unitary V such that $V^2 = U$).

(a) (5 points) Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ be the matrix for a 1-qubit NOT gate. Find a 2×2 matrix V (i.e., 1-qubit gate) such that $V^2 = X$.

(b) (5 points) Suppose we construct V by simply taking the square root of each gate U_i in circuit U, does this work, i.e. is $V^2 = U$? Justify your answer.

(c) (20 points) We explore a strategy of implementing V using the *phase estimation* algorithm. Suppose U is constituted by s two-qubit gates. We study a simple case here. Let $\{|\psi_x\rangle : x \in \{0, \ldots, 2^n - 1\}\}$ be a set of orthonormal eigenvectors of U with eigenvalues in $\{\pm 1, \pm i\}$. Namely $U|\psi_x\rangle = i^{\phi_x}|\psi_x\rangle$ with $\phi_x \in \{0, 1, 2, 3\}$. We outline a construction of V as follows such that $V|\psi_x\rangle = \omega^{\phi_x}|\psi_x\rangle$ where $\omega = e^{2\pi i/8}$:

- Construct a generalized-control-U, with two control-qubits, i.e., $|ab\rangle \otimes |c\rangle \mapsto |ab\rangle \otimes U^{ab}|c\rangle$. (A word on notation: ab is the two-bit string, e.g., 01, and it is identified with an integer in $\{0, 1, 2, 3\}$.)
- Then apply the phase-estimation algorithm to this controlled-U gate, which results in a circuit that computes $ab = \phi_x$, in two ancillary qubits for any input $|\psi_x\rangle$.
- Apply gates to those two ancilliary qubits to induce the mapping $|ab\rangle \mapsto \omega^{ab}|ab\rangle$.
- Then apply the inverse of the phase-estimation circuit.

Answer the following questions:

i) Explain how to construct a circuit computing the two-qubit controlled-U operation using $3s$ 3-qubit gates. (You may assume that you can implement the single-qubit controlled version of each two-qubit gate in U by a 3-qubit gate.)

ii) Explain how to construct a circuit computing $ab = \phi_x$ on input ~~$|\phi_x\rangle$~~ $|\psi_x\rangle$ using $3s$ 3-qubit gates, one 2-qubit gate, and four 1-qubit gates.

iii) Give a quantum circuit consisting of two 1-qubit gates that maps each basis state $|ab\rangle$ to $\omega^{ab}|ab\rangle$.

iv) Verify that the construction V is correct, i.e., $V|\psi_x\rangle = \omega^{\phi_x}|\psi_x\rangle$. Explain why this implies $V^2 = U$, namely V computes the squre root of U on any input state $|\psi\rangle$.

Note: the total gate cost is $6s$ 3-qubit gates plus two 2-qubit gates plus eight 1-qubit gates. This can be converted into a circuit consisting of $O(s)$ 2-qubit gates, not much more than the original circuit.