CSCE 440/640 Quantum Algorithms

Homework 3

Texas A&M U, Spring 2019 — *Feb. 18, 2019*

Lecturer: Fang Song — *Due: March 6, 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. (Linear algebra modulo 2) The integers modulo 2 constitute a field F_2: a set of numbers (namely 0 and 1) for which all the standard operations of plus, minus, times, and division-by-nonzero work as expected. The set of all n-dimensional vectors in this case is denoted F_2^n. (Other examples of fields include the real numbers, the complex numbers, the rational numbers, and the integers modulo p whenever p is prime. Also, you are most likely used to the cases R^n and C^n, when the scalars are reals and complexes, respectively.)
   (a) (5 points) Show that it is possible that $u \cdot u = 0$ for some $u \neq 0$, where $u \cdot v := \sum_{i=1}^{n} u_i v_i \pmod 2$ is the "dot product" in F_2^n. Is this possible in R^n with the usual inner product?
   (b) (5 points) Recall that a set of vectors $u_1, \ldots, u_k$ is said to be linearly independent if the only linear combination $c_1 u_1 + \ldots + c_k u_k$ that equals 0 is the trivial one with $c_1 = c_2 = \ldots = c_k = 0$. The *span* (set of all linear combinations) of k linearly independent vectors is called a k-dimensional subspace. Show that in F_2^n , every k-dimensional subspace contains exactly 2^k vectors.
   (c) (5 points) Consider a system of equations $Ax = 0$ (where $A \in F_2^{m \times n}$ is a matrix and x is a vector of n unknowns). Show that the set of solutions x to $Ax = 0$ forms a subspace of dimension equal to $n - r$, where r is the maximum size of a linearly independent set of rows of A.
   (d) (5 points) For a more general system $Ax = b$ for some fixed $b \in F_2^n$, prove that either there is no solution, or else there are $2n - r$ solutions. Again r is the maximum size of a linearly independent set of rows of A.

2. (Deferred measurement) We will show that if one has a quantum circuit with partial measurement gates in the middle, one can replace it with an equivalent quantum

in which all the measurement gates are at the end without incurring much loss in efficiency.

Consider an n-qubit quantum circuit, and assuming the first intermediate measurement gate is applied to the 1st qubit at time step t. Let $|\psi_i\rangle$ denote the quantum state just prior to time t. Recall when the measurement is applied, two things happen: First, one classical bit of information b appears on the measurement gate's readout. Second, the state collapses according to the usual rules.

(a) (5 points) Now we start to make a new circuit. We introduce a new $(n+1)$st qubit, initialized in $|0\rangle$. Second, we replace the measurement gate on qubit #1 at time t with a CNOT gate whose control qubit is #1 and whose target qubit is #$(n+1)$. Finally, we immediately apply a measurement gate to the $(n+1)$st qubit, and treat its readout as "b". Assume we then henceforth ignore the (n + 1)st qubit. Show that this gives an exact simulation of the original circuit's operation.

Note that since Operations on disjoint sets of qubits commute (Cf. HW2 Problem 4a), we can imagine that instead of measuring it immediately (just after time t), we instead delay its measurement to the very end of the computation. In this way, we've effectively deferred the first intermediate measurement of the quantum circuit to the end. By repeating this for all intermediate measurement gates, we can always move all measurement gates to the end (at the cost of adding one extra qubit and CNOT each time).

(b) (Bonus 5 pts) A curious reader may ask, what if I needed the measurement outcome "b" to decide the next operation (e.g., apply X on 5th qubit if $b = 1$ and H on 7th qubit if $b = 0$) in the original circuit? Now that the measurement gets delayed, how can I proceed? Help the reader resolve this, and estimate the cost.

3. (Semi-classical quantum Fourier transform) If we will measure right after the QFT, then we can construct a simpler circuit with 1-qubit gates only.

(a) (5 points) For $k > 0$, let

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

be a two-qubit controlled phase gate. Show that it is symmetric, i.e., it gives the same operation if you reverse the control and target qubits.

(b) (10 points) Recall the QFT circuit (Fig. 1), where R_k is as above. Because of part a), we get an equivalent circuit below by flipping the control and target qubits of each phase gate (Fig. 2).

Note that on all wires, the qubits' lifetimes end by being control bits. Show that we will obtain equivalent results if we measure each qubit after its Hadamard

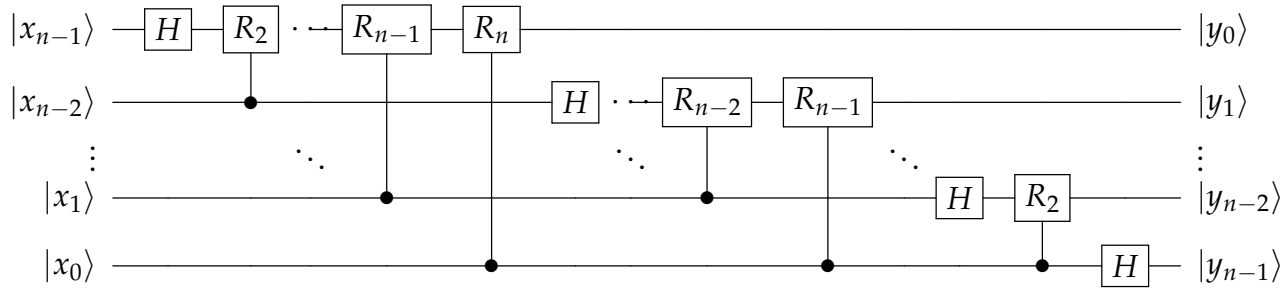

Figure 1: QFT circuit in $\mathbb{Z}_{2^n}$.

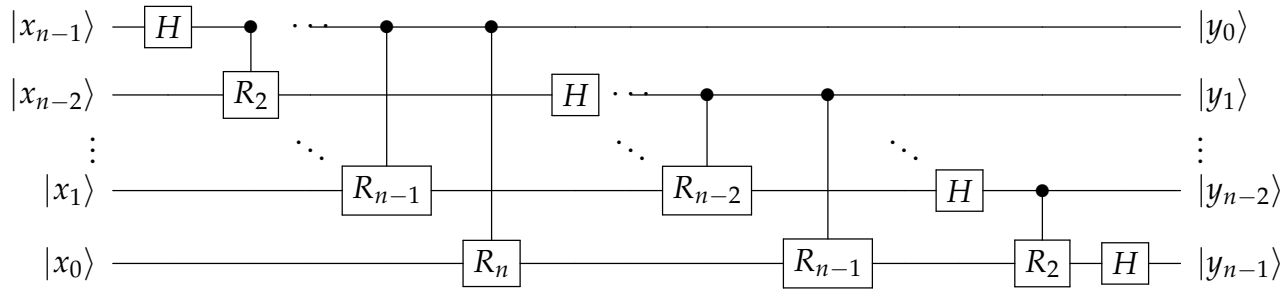

Figure 2: QFT circuit in $\mathbb{Z}_{2^n}$.

gate, then use the outcome to *classically* control whether or not to apply the phase gate, as in Fig. 3.

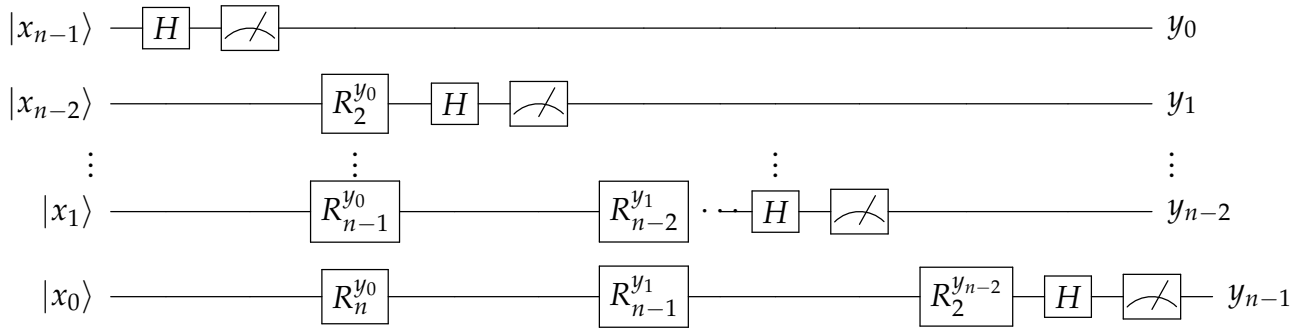

Figure 3: QFT circuit in $\mathbb{Z}_{2^n}$.

4. (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 $|\psi_x\rangle$ 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.

5. (Experimentally realizing Shor's algorithm)

(a) (5 points) Read the paper Pretending to factor large numbers on a quantum computer by Smolin, Smith, and Vargo. Summarize their main critique of prior experiments.

(b) (5 points) **[G]** Read the paper Realization of a scalable Shor algorithm by Monz et al. Do you feel it adequately addresses the criticisms in the Smolin–Smith–Vargo paper? Why or why not?