CS 410/510 Introduction to Quantum Computing
Homework 2

Portland State U, Spring 2018 — *Update: April 25, 2018*
Lecturer: Fang Song — *Due: May 02, 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. (Linear algebra)

   (a) (6 points) A linear operator on a vector space V (think of $\mathbb{C}^k$) is a linear transformation $T : V \to V$ of the vector space to itself. A vector $|\psi\rangle$ is called an eigenvector of an operator T if $T|\psi\rangle = \lambda|\psi\rangle$ for some constant $\lambda \in \mathbb{C}$. λ is called the eigenvalue corresponding to the eigenvector $|\psi\rangle$. Find the eigenvalues and eigenvectors of Pauli operator X. Show that the eigenvectors form an orthonormal basis of $\mathbb{C}^2$. Do the same for $X \otimes X$.

   (b) (6 points) An operator T is called *Hermitian*, if $T^\dagger = T$. Prove that the eigenvalues of a Hermitian operator are all real numbers. Show that the eigenvalues of unitary operators are of the form $e^{i\theta}$ for some $\theta \in [0, 2\pi)$.

   (c) (4 points) Show that for any $x \in \{0,1\}^n$, $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle$. $x \cdot y := \sum_{i=1}^n x_i y_i$ is the dot product over $\mathbb{Z}_2^n$.

   (d) (4 points) Let $x, y \in \{0,1\}^n$ and let $s = x \oplus y$. Show that

   $$H^{\otimes n}\frac{1}{\sqrt{2}}(|x\rangle + |y\rangle) = \frac{1}{\sqrt{2^{n-1}}} \sum_{z:z\cdot s=0} (-1)^{x\cdot z}|z\rangle\,.$$

   (e) (5 points) Suppose that $|v_1\rangle, |v_2\rangle, \ldots |v_k\rangle \in \mathbb{C}^k$ form an orthonormal basis. Show that $\sum_{i=1}^k |v_i\rangle\langle v_i|$ is the identity matrix.

   (f) (5 points) [**G**] Show that every unitary one-qubit gate with real entries can be written as a rotation matrix, possibly preceded and followed by Z-gates. In other words, show that for every 2×2 real unitary U, there exist signs $s_1, s_2, s_3 \in \{1, -1\}$ and angle $\theta \in [0, 2\pi)$ such that

$$U = s_1 \begin{pmatrix} 1 & 0 \\ 0 & s_2 \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & s_3 \end{pmatrix}.$$

(g) (8 points) For a vector $v = (v_0, \dots, v_{k-1}) \in \mathbb{C}^k$, let $\|v\| := \sqrt{\sum_{i=0}^{k-1} |v_i|^2}$, which is the usual Euclidean length of v. For any $k \times k$ matrix $M \in \mathbb{C}^{k\times k}$, 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 $k \times k$ unitary matrices M_1 and M_2 as $\|M_1 - M_2\|$. Show that

i) $\|A - B\| \le \|A - C\| + \|C - B\|$, for any three $k \times k$ matrices A, B, and C. (Thus, this distance measure satisfies the *triangle inequality*.

ii) Show that, for any two $k \times k$ unitary matrices U_1 and U_2, and any matrix A, $\|U_1 A U_2\| = \|A\|$.

2. (Simple search algorithms) In the context of this question, we are interested in exact solutions (with failure probability zero).

(a) (6 points) (1-out-of-4 search) Consider a black-box function $f : \{0,1\}^2 \to \{0,1\}$ with the property that there is a unique $x \in \{0,1\}^2$ such that $f(x) = 1$ and the goal is to determine x. How many classical queries are necessary to solve this problem? Design a quantum algorithm that finds x using 1 quantum query.

(b) (6 points) (2-out-of-4 search) Given a black-box for a function $f : \{0,1\}^2 \to \{0,1\}$ with exactly two $x \in \{0,1\}^2$ such that $f(x) = 1$ and the goal is to determine both x's. Prove that 3 classical queries are necessary to solve this problem and that 2 quantum queries are sufficient to solve this problem.

3. (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 $j, k \in \{0, 1, \dots, N-1\}$.

i) Let $N = 3$. Calculate $F_3(0,1,0)^T$ and $F_3(1,\omega,\omega^2)^T$. $(\cdot)^T$ denotes the transpose.

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

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

iv) 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). If k is large then 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.

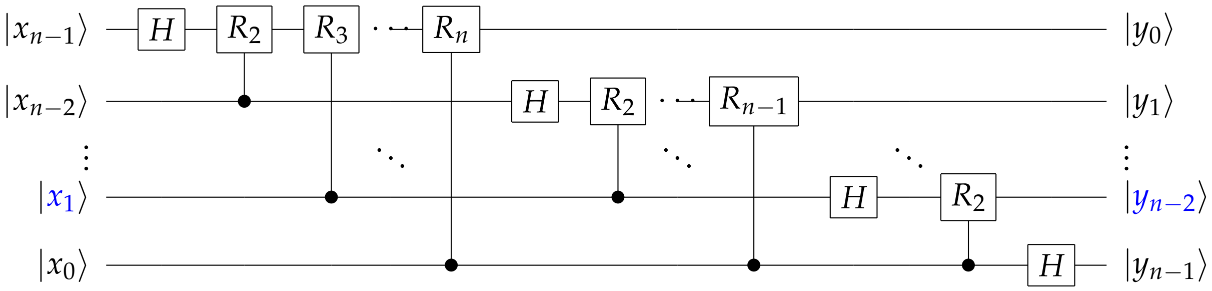

Figure 1: QFT circuit in $\mathbb{Z}_{2^n}$.