CS 410/510 Introduction to Quantum Computing

Homework 5

Portland State U, Spring 2020 *05/10/2020*
Lecturer: Fang Song *Due: 11:59pm PDT,* ***05/17/2020***

Instructions. This problem set contains 12 pages (including this cover page) and 3 questions. Problems marked with "[**G**]" are required for 510 students. Students enrolled in 410 will get bonus points for solving them. A random subset of problems will be graded.

Your solutions will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct, and 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.

You need to submit a PDF file via Gradescope before the deadline. Either a clear scan of you handwriting or a typeset document is accepted. You will get 5 bonus points for typing in LaTeX (Download and use the accompany TeX file).

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. (Norm) For a vector $v = (v_0, \ldots, v_{k-1}) \in \mathbb{C}^k$, 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 $E(M_1, M_2) := \|M_1 - M_2\|$. Show that

   (a) (5 points) Show that for any $k \times k$ matrices A, B and C,

   $$E(A, B) \leq E(A, C) + E(C, B) .$$

   (Thus, this distance measure satisfies the *triangle inequality*.)

(b) (5 points) Show that, for any two $k \times k$ unitary matrices U_1 and U_2, and any matrix A, $\|U_1 A U_2\| = \|A\|$.

(c) (5 points (bonus)) Show that

$$E(U_2U_1, V_2V_1) \leq E(U_2, V_2) + E(U_1, V_1)\,.$$

2. (Approximate QFT)

   (a) (5 points) We showed in class a circuit implementing the n-qubit QFT using Hadamard and controlled-R_k gates, where $R_k|x\rangle = e^{2\pi i x/2^k}|x\rangle$ for $x \in \{0,1\}$. How many gates in total does that circuit use? Express your answer both exactly and using Θ notation. (Recall that we say $f(n) = \Theta(g(n))$ if $f(n) = O(g(n))$ and $g(n) = O(f(n))$.)

(b) (5 points) Let cR_k denote the controlled-R_k gate, with $\mathrm{c}R_k|x\rangle|y\rangle = e^{2\pi i x y}|x\rangle|y\rangle$ for $x, y \in \{0, 1\}$. Its matrix form reads

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

Show that $E(\mathrm{c}R_k, I) \leq 2\pi/2^k$, where I denotes the 4×4 identity matrix, and where $E(U, V) = \|U - V\|$ as defined in Problem 1. (Hint: you may use the fact that $\sin x \leq x$ for any $x \geq 0$.)

(c) (8 points) Let F denote the exact QFT on n qubits. Suppose that for some constant c, we delete all the controlled-R_k gates with $k > \log_2(n) + c$ from the QFT circuit, giving a circuit for another unitary operation F'. Show that $E(F, F') \leq \varepsilon$ for some ε that is independent of n, where ε can be made arbitrarily small by choosing c arbitrarily large. (Hint: you may use Problem 1 part c without proving it.)

(d) (7 points (bonus)) For a fixed c, how many gates are used by the circuit implementing F'? It is sufficient to give your answer using Θ notation. Let $n = 8$ and $c = 1$, implement the F' in QISKIT. Include your circuit diagram or openQASM code.

3. (Factoring 21)

   (a) (4 points) Suppose that, when running quantum factoring algorithm to factor the number 21, you choose the value $a = 2$. What is the order r of a mod 21?

(b) (5 points) Compute $gcd(21, a^{r/2} - 1)$ and $gcd(21, a^{r/2} + 1)$. How do they relate to the prime factors of 21?

(c) (6 points) Give an expression for the probabilities of the possible measurement outcomes when performing phase estimation with m bits of precision. For $m = 7$, plot the probabilities. You are encouraged to use software to produce your plot.

(d) (5 points (bonus)) How would your above answers change if instead of taking $a = 2$, you had taken $a = 5$?