CO481/CS467/PHYS467 Assignment 3

Due March 3, 2025, 8:30am

Instruction: Please submit your solutions to Crowdmark by the due date and time. Take special care to place the answer to each question in the right place. Questions are ordered according to the sequence of topics covered in class, and not by difficulty. Also, if you do not prove an earlier part of a question, you can still use the earlier part to answer a later part.

Question 1. Approximating the quantum Fourier transform on n qubits [14 marks]

Recall the definition of error in approximating a unitary U by V:

$$E^*(U,V) := \max_{|\psi\rangle_{RS}} \|(I \otimes U)|\psi\rangle - (I \otimes V)|\psi\rangle\|,$$

where U, V are $l \times l$ unitaries acting on an l-dimensional system S, and I acts on an arbitrary system R with finite dimension. Recall also that

$$E^*(U,V) = E(U,V) := \max_{|\mu\rangle_S} \|(U - V)|\mu\rangle_S\|.$$

You can use the fact that $E(U,V)$ is subadditive ((4.69) in NC and (4.3.3) in KLM):

$$E(U_m U_{m-1} \cdots U_1, V_m V_{m-1} \cdots V_1) \leq E(U_m, V_m) + E(U_{m-1}, V_{m-1}) + \cdots E(U_1, V_1).$$

Consider the circuit on p91 of topic07-1b.pdf (and the discussion leading to it). We use the notation C_n for the circuit implementing the quantum Fourier transform over $\mathbb{Z}_{(2^n)}$, and the notation F_n for the unitary matrix describing this quantum Fourier transform.

(a) [2 marks] For each $k \in \{2, 3, \cdots, n\}$, how many c-$R_k$ gates are there in C_n? What is the total number of gates in C_n (count each Hadamard or c-R_k gate as one gate)?

(b) [3 marks] Show that $E(\text{c-}R_k, I) \leq \frac{2\pi}{2^k}$. You may use the fact $\sin x \leq x$ for any $x \geq 0$.

The goal of this question is to find a circuit $\tilde{C}_n$ that computes a unitary $\tilde{F}_n$ that approximates F_n to error ϵ, but $\tilde{C}_n$ uses many fewer gates than C_n. Part (b) shows that for large k, c-R_k is close to the identity operation on 2 qubits. So we take the approach to omit from C_n the c-R_k gates for large k, and bound the error incurred.

Starting from C_n, consider the circuits $C_{n,n}, C_{n,n-1}, \cdots, C_{n,k}, \cdots, C_{n,r}$ where $C_{n,n}$ is obtained by omitting all the c-R_n gates from C_n, $C_{n,n-1}$ is obtained by omitting all the c-R_{n-1} gates from $C_{n,n}$, and recursively, each $C_{n,k}$ is obtained by omitting all the c-R_k gates from $C_{n,k+1}$, for $n-1 \geq k \geq r$. Let $F_{n,k}$ be the resulting unitary from the circuit $C_{n,k}$.

(c) [4 marks] Show that $E^*(F_{n,k+1}, F_{n,k}) \leq (n-k+1)\frac{2\pi}{2^k}$.

Hint: you will need to use the equality $E^*(U,V) = E(U,V)$, subadditivity, and parts (a) and (b). Please explain how these results are applicable in your answer.

(d) [2 marks] Upper bound $E^*(F_n, F_{n,r})$ by $\frac{4\pi n}{2^r}$.

You can use without proof $E^*(F_n, F_{n,r}) \leq E^*(F_n, F_{n,n}) + E^*(F_{n,n}, F_{n,n-1}) + \cdots + E^*(F_{n,r+1}, F_r)$ which is a simple extension of subadditivity.

(e) [1 mark] Determine $\tilde{r}$ so that $E^*(F_n, F_{n,\tilde{r}}) \leq \epsilon$.

(f) [2 marks] If we approximate C_n by $\tilde{C}_n = C_{n,\tilde{r}}$ for $\tilde{r}$ obtained from part (e), show that $\tilde{C}_n$ has $\approx n \log\left(\frac{n}{\epsilon}\right)$ gates for large n (after dropping some unimportant terms).

Question 2. Period finding [8 marks]

You are given a blackbox function $f : \mathbb{Z} \to \{1, \cdots, 20\}$. You are also given the partial information that f is periodic with unknown period r, but you are given the upper bound $r \leq 15$. You run the period finding algorithm (see topic07-1c.pdf and the references to the 3 textbooks there) with dimension $d = 256$. You run the quantum subroutine 4 times, getting 4 measurement outcomes $x = 64, 107, 108, 235$.

(a) [2 mark] Give 2 reasons for choosing $d = 256$.

(b) [6 marks] What is r? You will need to use continued fraction expansion (CFE), and the use of a computer *for this part* is allowed. Show all your other steps and provide full justification in each step (e.g., what condition you use to stop the CFE, or why you think a data point is spurious).

Question 3. Solving the collision problem using Grover search [4 marks]

Recall that the quantum search algorithm can find a marked item in a search space of size N using $O(\sqrt{N/M})$ queries, where M is the total number of marked items.

In the collision problem, you are given a black-box function $f\colon \{1, 2, \dots, N\} \to S$ (for some set S) with the promise that f is two-to-one. In other words, for any $x \in \{1, 2, \dots, N\}$, there is a unique $x' \in \{1, 2, \dots, N\}$ such that $x \neq x'$ and $f(x) = f(x')$. The goal of the problem is to find **any** such pair (x, x') (called a collision).

(a) [2 marks] For any $K \in \{1, 2, \dots, N\}$, consider the following quantum algorithm for the collision problem:

1. Query $f(1), f(2), \dots, f(K)$.
2. If a collision is found, output it.
3. Otherwise, using Grover's algorithm to search for a value $x \in \{K + 1, K + 2, \dots, N\}$ such that $f(x) = f(x')$ for some $x' \in \{1, 2, \dots, K\}$.

How many quantum queries does this algorithm need to make in order to find a collision? Your answer should depend on N and K, and can be expressed using big-O notation.

(b) [2 marks] Make a good choice of K and show that $O(N^{1/3})$ queries are sufficient.