Introduction to Quantum Computation, UPB
Summer 2021, Assignment 8

Due: Friday, July 9, at start of tutorial

1 Exercises

1. Let $U \in \mathcal{L}(\mathbb{C}^d)$ be a unitary operator with eigenvalues $e^{2\pi i\theta_k}$ for $\theta_k \in [0,1)$. Assume for simplicity that all θ_k can be expressed perfectly using n bits.

   (a) Let $|\psi_k\rangle$ be an eigenvector of U with eigenvalue $e^{2\pi i\theta_k}$. In class, we saw that the phase estimation algorithm maps $|0^n\rangle|\psi_k\rangle \mapsto |2^n\theta_k\rangle|\psi_k\rangle$. In other words, we extract the *phase* of the eigenvalue. What happens when the input state $|\psi_k\rangle$ *is not* an eigenvector of U? In other words, suppose we instead input state $|0^n\rangle|\phi\rangle$ to the phase estimation algorithm. What state does the algorithm produce? What happens when we measure the first register of the output in the standard basis?

   (b) Suppose for all $k \in \{1,\ldots,d\}$, $\theta_k \in \{0, 1/2\}$, i.e. U has eigenvalues in $\{1,-1\}$. Given any state $|\phi\rangle$ as for part (a), give a quantum circuit for randomly projecting $|\phi\rangle$ onto either the $+1$ or -1 eigenspace of U, with the help of a classical register which indicates which of the two spaces we've projected onto. What is the expression determining the probability of projecting down to each of the two eigenspaces (this should depend on $|\phi\rangle$)?

   (c) Consider the special case of part (b) in which U is a 2×2 unitary matrix, and is Hermitian. Suppose we wish to measure state $|\phi\rangle$ via observable U, i.e. to obtain outcome 1 or -1 (the eigenvalues of U), and then project $|\phi\rangle$ onto the corresponding eigenspace. Give a simple circuit which accomplishes this.

2. Just as we defined norms of vectors, one can define norms on matrices. For $A \in \mathcal{L}(\mathbb{C}^d)$, define the *induced Euclidean norm* (a.k.a. operator or spectral norm)

$$\| A \| := \max_{v\in\mathbb{C}^d \text{ s.t. } \| v \|_2 = 1} \| Av \|_2 ,$$

   where recall $\| v \|_2 = \sqrt{\langle v, v\rangle}$ denotes the Euclidean norm of v. In other words, the spectral norm tells the maximum amount by which A can "stretch" a vector v. Based on this, we can define distance measure $d(A,B) = \| A - B \|$.

   (a) Let us first understand why the spectral norm is useful in quantum information. Given two unitaries $U, U' \in \mathcal{L}(\mathbb{C}^d)$ such that $\| U - U' \| \leq \epsilon$ for some small $\epsilon \approx 0$, and an arbitrary state $|\psi\rangle \in \mathbb{C}^d$, why is it intuitively difficult to distinguish via any measurement the output of $U|\psi\rangle$ versus $U'|\psi\rangle$?

   (b) Let us now apply the intuition behind (a) to simplify the circuit for the quantum Fourier transform. Consider phase gate

$$V = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}.$$

   Compute $d(I, V)$, for I the 2×2 identity matrix.

(c) Consider a circuit consisting of L unitary operations $U_i \in \mathcal{L}(\mathbb{C}^d)$,

$$U = U_L U_{L-1} \cdots U_1.$$

Suppose we omit an arbitrary operation U_i, i.e. set $U' = U_L \cdots U_{i+1} U_{i-1} \cdots U_1$. Show that $\| U - U' \| = \| I - U_i \|$. (Hint: Convince yourself first that the spectral norm is unitarily invariant, i.e. $\| A \| = \| UAV \|$ for any unitaries U and V.)

(d) More generally, it can be shown that if we drop a set of unitaries $S = \{U_i\}$ from U, then

$$\| U - U' \| \leq \sum_{U_i \in S} \| I - U_i \| .$$

The proof proceeds by induction on $|S|$, and the proof idea essentially is the same as for a simpler problem, which you will instead solve in this question. For any unitary matrices U, V, U', V', show that

$$\| UV - U'V' \| \leq \| U - U' \| + \| V - V' \| .$$

Intuitively, this says that if we replace "ideal" unitaries U and V with "approximate" ones U' and V', respectively, the effect of replacing UV with $U'V'$ can be bounded via the spectral norm.

(Hint: Add and subtract a carefully chosen term to $UV - U'V'$, and then apply the triangle inequality and submultiplicativity properties for the spectral norm, which say that $\| A + B \| \leq \| A \| + \| B \|$ and $\| AB \| \leq \| A \| \| B \|$, respectively.)

(e) Observe now that the quantum Fourier Transform QFT_N for $N = 2^n$ from class requires $O(n^2)$ gates. Given the exercises above, design a quantum circuit U' using just $O(n \log n)$ gates, such that $\| U - U' \| \leq 1/n$. (Hints: (1) Recall from class that for large s, the entry $e^{2\pi i/2^s} \approx 1$ in the phase gates R_s. Reflecting on this should give you an overall battle plan for how to approach this question. (2) To formalize things, start by proving that $\left| e^{2\pi i/2^s} - 1 \right| \leq 2\pi/2^s$. The Wikipedia page for trigonometric identities, as well as Taylor series truncations, will be your friends here. The answer to this hint should tell you how roughly many phase gates you need on each wire to ensure the overall error spectral norm stays below $1/n$.)

3. (a) Prove that FACTOR $\in$ NP $\cap$ co-NP. In your containment proof for co-NP, you will need to argue that the number of factors is at most polylogarithmic in the input N to FACTOR.

(b) Recall from Fact 16 of Lecture 10 that for any prime $p \in \mathbb{Z}^+$, there is a generator $g \in Z_p$, such that any $e \in Z_p$ can be written $g^k \equiv e \mod p$ for some $k \in \{1, \ldots, p-1\}$. Using Fermat's Little Theorem, prove that picking non-zero e uniformly at random from Z_p is equivalent to picking $k \in \{1, \ldots, p-1\}$ uniformly at random. In your answer, *do not* assume *a priori* that $k \in \{1, \ldots, p-1\}$ as stated in Fact 16; rather, start by assuming there is some k for each e, and use FLT to prove that indeed WLOG $k \in \{1, \ldots, p-1\}$.