Assignment 6
Due: 11:59pm, November 2, 2021

1. **Approximating unitary transformations [15 points; 5 each].** There are situations where it is easier to approximate a unitary transformation than to compute it exactly. For a vector $v = (v_0, \ldots, v_{m-1})$, let $\|v\| = \sqrt{\sum_{j=0}^{m-1} |v_j|^2}$, which is the usual Euclidean length of v. For any $m \times m$ matrix M, define its *(spectral) norm* $\|M\|$ as

$$\|M\| = \max_{\|v\|=1} \|Mv\|.$$

Define the *distance* between two $m \times m$ unitary matrices U_1 and U_2 as $||U_1 - U_2||$.

   (a) Show that $||A - B|| \leq ||A - C|| + ||C - B||$, for any three $m \times m$ matrices A, B, and C. (Thus, this distance measure satisfies the *triangle inequality.*)

   (b) Show that, for any any $m \times m$ matrix A and the $\ell \times \ell$ identity matrix I, $||A \otimes I|| = ||A||$.

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

2. **Approximate Fourier transform [15 points]**. In the video lectures (and lecture notes), we computed F_{2^n} by a quantum circuit of size $O(n^2)$. Here, we compute an approximation of F_{2^n} within ϵ by a quantum circuit of size $O(n \log(n/\epsilon))$.

   (a) [5 points] Recall that our quantum circuits for F_{2^n} use controlled-phase gates, of the form

$$P_k = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^k} \end{bmatrix},$$

   for values of k that range between 2 and n. Show that $||P_k - I|| \leq 2\pi/2^k$, where I is the 4×4 identity matrix. (Thus, P_k gets very close to I when k increases.)

   (b) [10 points] The idea behind the approximate circuit for F_{2^n} is to start with the $O(n^2)$ circuit and then remove some of its P_k gates. Removing a P_k gate makes the circuit smaller but also changes the unitary transformation (it is equivalent to changing the P_k gate to an I gate). From part (a) and the properties of our measure of distance between unitary transformations from the previous question, we can deduce that if k is large enough then removing a P_k gate changes the *overall* unitary transformation by only a small amount. Show how to use this approach to obtain a quantum circuit of size $O(n \log(n/\epsilon))$ that computes a unitary transformation $\tilde{F}_{2^n}$ such that

$$||\tilde{F}_{2^n} - F_{2^n}|| \leq \epsilon.$$

   (Hint: Try removing all P_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.)