CMPT 476/776: Introduction to Quantum Algorithms
Assignment 5

Due **April 9th, 2026 at 11:59pm on crowdmark**
Complete individually and submit in PDF format.

Question 1 [10 points]: Hamiltonian simulation

In this question we will devise a circuit to simulate the Hamiltonian

$$\hat{H} = \theta_1(Z \otimes X) + \theta_2(X \otimes Z)$$

1. Show that $Z \otimes X$ and $X \otimes Z$ commute. (**Hint:** recall from a previous assignment that every pair of distinct, non-identity Pauli matrices anti-commute, in the sense that $AB = -BA$).

2. Recalling that $e^{A+B} = e^A e^B$ when A and B commute, give a two-qubit circuit over the gate set $\{CNOT, X, Z, H, R_Z(\theta) \mid \theta \in \mathbb{R}\}$ simulating $U(t) = e^{-i\hat{H}t}$.

3. In practice, to implement $U(t)$ we would need to implement it over a physically implementable gate set. Recalling that the Solovay-Kitaev theorem states any single-qubit rotation can be approximated to accuracy ϵ in **depth** (i.e. number of time steps, or operations performed in sequence) $\approx \log_2^c(1/\epsilon)$ where $c \approx 1.5$ over the *Clifford+T* gate set $\{CNOT, X, Z, H, T, T^\dagger\}$, calculate the expected depth of your circuit after approximating over the Clifford+T gate set to error 10^{-17}.

4. Two matrices A, B are *simultaneously diagonalizable* if there exists some unitary U such that $A = U\Lambda_A U^\dagger$, $B = U\Lambda_B U^\dagger$. It can be shown that two Hermitian operators A, B are simultaneously diagonalizable if and only if they commute.

   Find an orthonormal basis for the 4-dimensional *joint eigenspace* of $Z \otimes X$ and $X \otimes Z$. That is, find some set $\{|v_i\rangle\}$ of 4 unit vectors such that

$$\begin{aligned} (Z \otimes X)|v_i\rangle &= \lambda_{a,i}|v_i\rangle \\ (X \otimes Z)|v_i\rangle &= \lambda_{b,i}|v_i\rangle \\ \forall i \neq j, \qquad \langle v_i|v_j\rangle &= 0 \end{aligned}$$

5. Use these eigenvectors to design a unitary U simultaneously diagonalizing $Z \otimes X$ and $X \otimes Z$ as $Z \otimes I$ and $I \otimes Z$, respectively. Give a circuit over $\{CNOT, X, Z, H\}$ implementing U.

6. Now using the circuit from the previous question (or just U if you could not complete it), give an **efficient** circuit over $CNOT$, X, Z, H, and **parallel** $R_Z(\theta)$ gates simulating $U(t) = e^{-i\hat{H}t}$. Calculate the estimated depth of this circuit after approximation to error 10^{-17}.

Question 2 [4 points]: Collision finding with Grover's algorithm

Suppose you're given a 32-bit hash H of a message M with a two-to-one cryptographic hash function — that is $H = h(M)$ where $h : \{0,1\}^{32} \to \{0,1\}^{32}$ and h has the property that for every $H = h(M)$ there exists **exactly one collision** $M' \neq M$ such that $h(M') = H$.

Explain how you would apply Grover's algorithm to find the unique collision $M' \neq M \in \{0,1\}^{32}$ such that $h(M') = H$. Specifically,

1. What would the search function f be? How would you implement this as a quantum circuit? **You do not need to give an explicit circuit.**
2. How many iterations would you need to maximize the probability of success?
3. What is the resulting approximate probability of success?

Question 3 [2 points]: Decoherence-free subspaces

In class we saw that we can protect against errors via active error correction. If we have very specific types of noise, such as bit flips that only occur in pairs, e.g.

$$\mathcal{E}_{X\otimes X}(\rho) = (1-p)\rho + p(X\otimes X)\rho(X\otimes X),$$

we can sometimes use passive encoding with a *decoherence-free subspace* — that is, a subspace of the Hilbert space which is invariant to the type of noise in the system.

Give a 2-qubit decoherence free subspace for the double bit flip channel $\mathcal{E}_{X\otimes X}$. That is, find orthogonal two-qubit states $|0\rangle_L, |1\rangle_L \in \mathbb{C}^4$ such that $(X\otimes X)|\psi\rangle = |\psi\rangle$ for any $|\psi\rangle = \alpha|0\rangle_L + \beta|1\rangle_L$. Why doesn't this work if bit flips are independent, i.e. can apply to only one qubit of a pair?

Question 4 [3 points]: The completely depolarizing channel

A *quantum channel* is like a unitary transformation, but for density matrices. That is, a quantum channel is a linear transformation that maps density matrices to density matrices. One way to represent a channel is by its **Kraus operators** — a set $\{K_i\}$ of operators on a hilbert space $\mathcal{H}$ such that $\sum_i K_i^\dagger K_i = I$. The channel then maps $\rho \to \sum_i K_i \rho K_i^\dagger$.

The **completely depolarizing channel** has Kraus operators $\{\frac{1}{2}I, \frac{1}{2}X, \frac{1}{2}Y, \frac{1}{2}Z\}$ where I, X, Y, Z are the Pauli matrices. Show that the completely depolarizing channel sends every 2×2 density matrix to the matrix $\frac{1}{2}I$, also known as a *maximally mixed state*.

Hint: remember that a density matrix ρ is Hermitian, i.e. $\rho^\dagger = \rho$.

Question 5 [4 points]: Logical gates

In *fault tolerant quantum computing*, we encode the state of a logical qubit in many physical qubits through the use of an *error correcting code*. One such code is the *Steane code*, which encodes one logical qubit using 7 physical qubits. The encoding is as follows:

$$|0\rangle_L = \frac{1}{\sqrt{8}}\left(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\right)$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}\left(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\right)$$

Since we need *continuous* error correction to protect the state from coherence, we can't decode the state to apply physical gates. Instead, we apply *encoded gates* U — circuits which **act like** U **on** $|0\rangle_L$ **and** $|1\rangle_L$. The best-case scenario is for an encoded U gate — denoted U_L — to be equal to the $U \otimes U \otimes \cdots \otimes U$ on the physical qubits. This is called a *transversal gate*.

1. Verify that X, Z, and $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ are all transversal in the Steane code — that is,

$$X_L = X \otimes X \otimes X \otimes X \otimes X \otimes X \otimes X$$
$$Z_L = Z \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z$$
$$S_L^\dagger = S \otimes S \otimes S \otimes S \otimes S \otimes S \otimes S$$

   You do **not** need to show the entire calculation, just explain why. As a hint, think about the number of 1's in each $|\cdot\rangle$ above.

2. Is the $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ gate transversal in the Steane code? Explain why or why not.

3. Another method used to implement encoded gates uses a technique called *gate teleportation*, where a special state $|A\rangle$ called a *magic state* is prepared "offline" and then consumed in such a way as to produce the effect of a particular gate. You saw a similar effect in a previous assignment, as well as the midterm.

   Verify the circuit equality below, which shows that the state $|A\rangle = TH|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$ can be used to teleport a T gate into a circuit, given the ability to prepare $|A\rangle$ states (this is usually achieved by using something called *magic state distillation*).