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}.

Solution. 1. By direct calculation,

$$\begin{aligned}(X \otimes Z)(Z \otimes X) &= (XZ \otimes ZX) \\ &= (-ZX \otimes -XZ) \\ &= (ZX \otimes XZ) \\ &= (Z \otimes X)(X \otimes Z)\end{aligned}$$

2. First notice that the above implies $-i\theta_1(Z \otimes X)t$ and $-i\theta_2(X \otimes Z)t$ commute, thus

$$\begin{aligned}exp(-i\hat{H}t) &= exp\left(-i\theta_1(Z \otimes X)t - i\theta_2(X \otimes Z)t\right) \\ &= exp\left(-i\theta_1(Z \otimes X)t\right) exp\left(-i\theta_2(X \otimes Z)t\right)\end{aligned}$$

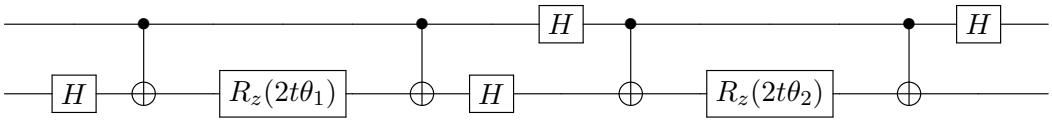
And diagonalizing each operand of the exponentials,

$$\begin{aligned}-i\theta_1(Z \otimes X)t &= -i\theta_1(I \otimes H)(Z \otimes Z)(I \otimes H)t \\ &= -i\theta_1(I \otimes H)CNOT(I \otimes Z)CNOT(I \otimes H)t \\ -i\theta_2(X \otimes Z)t &= -i\theta_2(H \otimes I)(Z \otimes Z)(H \otimes I)t \\ &= -i\theta_2(H \otimes I)CNOT(I \otimes Z)CNOT(H \otimes I)t\end{aligned}$$

So that taking exponentials yields

$$\begin{aligned}exp(-i\theta_1(Z \otimes X)t) &= (I \otimes H)CNOT(I \otimes e^{-i\theta_1 Zt})CNOT(I \otimes H) \\ &= (I \otimes H)CNOT(I \otimes R_z(2t\theta_1)CNOT(I \otimes H) \\ exp(-i\theta_2(X \otimes Z)t) &= (H \otimes I)CNOT(I \otimes e^{-i\theta_2 Zt})CNOT(H \otimes I) \\ &= (H \otimes I)CNOT(I \otimes R_z(2t\theta_2)CNOT(H \otimes I)\end{aligned}$$

Putting them in sequence and expressing as a circuit, we have



3. All but $R_z(\cdot)$ are in our gate set so that by subadditivity of errors, the error of the whole circuit is bounded above by $E(R_z(2t\theta_1), V_1) + E(R_z(2t\theta_2), V_2)$ for any approximations V_1, V_2. It follows that bounding both $E(R_z(2t\theta_1)$ and $V_1), E(R_z(2t\theta_2), V_2)$ by $\frac{10^{-17}}{2}$ gives our desired error on the entire circuit.

$$\log_2^c(\frac{2}{10^{-17}}) \approx (57.5)^{1.5} = 435.7$$

so that counting the depth of the rest with two of the above, we have expected depth of approximately

$$\lceil 7 + 2(435.7) \rceil = 879$$

4. We can do this by just observing the eigenspaces of $Z \otimes X$ and $X \otimes Z$ independently and carefully choosing vectors that are in intersections of eigenspaces.

$$E_+(Z \otimes X) = span(|0\rangle \otimes |+\rangle, |1\rangle \otimes |-\rangle)$$
$$E_-(Z \otimes X) = span(|0\rangle \otimes |-\rangle, |1\rangle \otimes |+\rangle)$$
$$E_+(X \otimes Z) = span(|+\rangle \otimes |0\rangle, |-\rangle \otimes |1\rangle)$$
$$E_-(X \otimes Z) = span(|+\rangle \otimes |1\rangle, |-\rangle \otimes |0\rangle)$$

Observe that

$$|v_1\rangle = \frac{|0\rangle \otimes |+\rangle + |1\rangle \otimes |-\rangle}{\sqrt{2}} = \frac{|00\rangle + |01\rangle + |10\rangle - |11\rangle}{2} = \frac{|+\rangle \otimes |0\rangle + |-\rangle \otimes |1\rangle}{\sqrt{2}}$$
$$|v_2\rangle = \frac{|0\rangle \otimes |+\rangle - |1\rangle \otimes |-\rangle}{\sqrt{2}} = \frac{|00\rangle + |01\rangle - |10\rangle + |11\rangle}{2} = \frac{|-\rangle \otimes |0\rangle + |+\rangle \otimes |1\rangle}{\sqrt{2}}$$
$$|v_3\rangle = \frac{|0\rangle \otimes |-\rangle + |1\rangle \otimes |+\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle + |11\rangle}{2} = \frac{|+\rangle \otimes |0\rangle - |-\rangle \otimes |1\rangle}{\sqrt{2}}$$
$$|v_4\rangle = \frac{|0\rangle \otimes |-\rangle - |1\rangle \otimes |+\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle - |10\rangle - |11\rangle}{2} = \frac{|-\rangle \otimes |0\rangle - |+\rangle \otimes |1\rangle}{\sqrt{2}}$$

where the vectors chosen are $+/-$ eigenvectors for $Z \otimes X$ and $X \otimes Z$ in the follow ways.

$$|v_1\rangle \in E_+(Z \otimes X) \cap E_+(X \otimes Z)$$
$$|v_2\rangle \in E_+(Z \otimes X) \cap E_-(X \otimes Z)$$
$$|v_3\rangle \in E_-(Z \otimes X) \cap E_+(X \otimes Z)$$
$$|v_4\rangle \in E_-(Z \otimes X) \cap E_-(X \otimes Z)$$

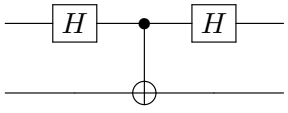
5. By the spectral theorem, if U is the unitary composed of columns $|\psi_i\rangle$ where $A|\psi_i\rangle = \lambda_i|\psi_i\rangle$, then

$$A = U \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} U^\dagger$$

Hence a unitary U diagonalizing $Z \otimes X$ and $X \otimes Z$ as $Z \otimes I$ and $I \otimes Z$, respectively, can be formed by taking the vectors in the previous question as the columns of U

$$U = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$$

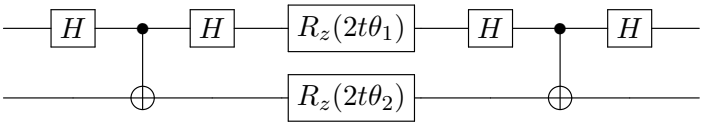
A circuit for U (up to an irrelevant phase in the last eigenvector) can be obtained by noting that $CNOT$ copies Z gates on the target, and copies X gates on the control, so in particular U can be written as



6. We can compute the two sequential exponentials of our circuit from before

$$exp(-i\theta_1(Z \otimes X)t) = U(I \otimes R_z(2t\theta_1))U^\dagger$$
$$exp(-i\theta_2(X \otimes Z)t) = U(R_z(2t\theta_1) \otimes I)U^\dagger$$

So we have the circuit



Since the $R_z(\cdot)$ are now parallel, their depths only count once collectively to the overall depth of the circuit, so that our expected depth is approximately

$$\lceil 6 + (435.7) \rceil = 442$$

□

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?

Solution. You can approach this problem either by giving a search function that has only one solution (M'), or a search function with two solutions (M, M'). Either is acceptable.

1. The search function is just $f : \{0,1\}^{32} \to \{0,1\}$ defined by

$$f(M') = \begin{cases} 1 & \text{if } h(M') = H \\ 0 & \text{otherwise} \end{cases}$$

Given a classical implementation of h, f can be implemented by translating the implementation of h into a reversible circuit, then performing a bitwise comparison by XORing with the string $11\cdots1 \oplus H$ and taking the product of all the bits. In particular, the string $11\cdots1 \oplus H \oplus h(M')$ will be the all 1 string if and only if $h(M') = H$.

A single-solution function is given by

$$f'(M') = \begin{cases} 1 & \text{if } h(M') = H \wedge M' \neq M \\ 0 & \text{otherwise} \end{cases}$$

which can again be implemented

2. We saw in class that for a small number of solutions M, the optimal number of iterations of

$$\frac{\pi}{4} \cdot \frac{\sqrt{2^n}}{\sqrt{M}}$$

For f we have $M = 2$ and $n = 32$, giving $\frac{\pi}{4} \cdot \frac{\sqrt{2^n}}{\sqrt{M}} \approx 36396$, while for f' we get $\frac{\pi}{4} \cdot \frac{\sqrt{2^n}}{\sqrt{M}} \approx 51471$.

3. Recall that the initial state of Grover's algorithm is

$$|\psi\rangle = \sin(\theta)|\psi_{good}\rangle + \cos(\theta)|\psi_{bad}\rangle$$

where $\sin^2(\theta) = \frac{M}{2^n}$ and each iteration rotates this state by an angle of 2θ. After k iterations we have the state

$$\sin((2k+1)\theta)|\psi_{good}\rangle + \cos((2k+1)\theta)|\psi_{bad}\rangle$$

For f we have $\theta \approx \sqrt{\frac{2}{2^{32}}}$ which gives us $\sin^2((2 \times 36396 + 1)\sqrt{\frac{2}{2^{32}}}) \approx 0.9999999997$ to find **either** M **or** M', or probability $\frac{1}{2} \cdot 0.9999999997$ of getting exactly M'. For f' we have probability $\sin^2((2 \times 51471 + 1)\sqrt{\frac{1}{2^{32}}}) \approx 0.9999999999$ of finding the unique string M'.

□

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?

Solution. Let

$$|0\rangle_L = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|1\rangle_L = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

It can be checked that they are orthonormal. And indeed for $|\psi\rangle = \alpha|0\rangle_L + \beta|1\rangle_L$,

$$\begin{aligned}(X \otimes X)|\psi\rangle &= \alpha(X \otimes X)|0\rangle_L + \beta(X \otimes X)|1\rangle_L \\ &= \alpha|0\rangle_L + \beta|1\rangle_L \\ &= |\psi\rangle\end{aligned}$$

It fails for independent bit flips since each such bit flip is a linear map from the even parity subspace to the odd parity subspace and vice versa. □

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. $\rho^\dagger = \rho$.

Solution. Recall that $\{I, X, Y, Z\}$ is a basis for $M_2(\mathbb{C})$, thus every density matrix can be expressed as a linear sum $\rho = aI + bX + cY + dZ$ where $a, b, c, d \in \mathbb{C}$. Computing the action of the completely depolarizing channel,

$$\begin{aligned}\rho \mapsto &\frac{1}{4}I\rho I + \frac{1}{4}X\rho X + \frac{1}{4}Y\rho Y + \frac{1}{4}Z\rho Z \\ =&\frac{1}{4}(aI + bX + cY + dZ) \\ &+ \frac{1}{4}(aI + bX - cY - dZ) \\ &+ \frac{1}{4}(aI - bX + cY - dZ) \\ &+ \frac{1}{4}(aI - bX - cY + dZ) \\ &= aI\end{aligned}$$

Since a density matrix has trace 1, it follows that $tr(aI) = 2a = 1$, and $a = \frac{1}{2}$. □

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,

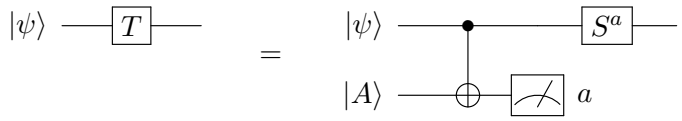
$$X_L = X \otimes X \otimes X \otimes X \otimes X \otimes X \otimes X$$
$$Z_L = Z \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z$$
$$S_L^\dagger = S \otimes S \otimes S \otimes S \otimes S \otimes S \otimes S$$

   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*).



Solution. 1. The X gate maps each basis vector of $|0\rangle_L$ to the basis vector of $|1\rangle_L$ right below. The Z gate does nothing to $|0\rangle_L$ since each basis vector has even parity, and adds a -1 overall phase to $|1\rangle_L$ since each basis vector has odd parity. The $S^\dagger$ gate does nothing to $|0\rangle_L$ since each basis vector has $0 \mod 4$ $|1\rangle$ bits, and applies a $(-i)$ overall phase phase since each basis vector of $|1\rangle_L$ has $3 \mod 4$ $|1\rangle$ bits.

2. No, it can be seen directly that a transversal T acting on $|0\rangle_L$ will yield

$$|0\rangle_L = \frac{1}{\sqrt{8}}\big(|0000000\rangle + e^{3i\pi/4}|1010101\rangle + e^{3i\pi/4}|0110011\rangle + e^{3i\pi/4}|1100110\rangle$$
$$+ e^{3i\pi/4}|0001111\rangle + e^{3i\pi/4}|1011010\rangle + e^{3i\pi/4}|0111100\rangle + e^{3i\pi/4}|1101001\rangle\big)$$

   which is not equivalent to $|0\rangle_L$.

3. Consider arbitrary qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Clearly the LHS yields

$$T|\psi\rangle = \alpha|0\rangle + \beta\omega|1\rangle$$

Consider the state on the RHS after applying the CNOT, we have

$$\begin{aligned}|\psi'\rangle := CNOT(|\psi\rangle \otimes |A\rangle) &= CNOT(\frac{\alpha}{\sqrt{2}}|00\rangle + \frac{\beta}{\sqrt{2}}|10\rangle + \frac{\alpha\omega}{\sqrt{2}}|01\rangle + \frac{\beta\omega}{\sqrt{2}}|11\rangle) \\ &= \frac{\alpha}{\sqrt{2}}|00\rangle + \frac{\beta}{\sqrt{2}}|11\rangle + \frac{\alpha\omega}{\sqrt{2}}|01\rangle + \frac{\beta\omega}{\sqrt{2}}|10\rangle\end{aligned}$$

Then the probability of measuring $0, 1$ respectively on the second qubit are

$$\begin{aligned}p(0) &= \left\| \frac{\alpha}{\sqrt{2}}|00\rangle + \frac{\beta\omega}{\sqrt{2}}|10\rangle \right\|^2 \\ &= \frac{|\alpha|^2 + |\beta\omega|^2}{2} \\ &= \frac{|\alpha|^2 + |\beta|^2}{2} \\ &= \frac{1}{2} \\ p(1) &= 1 - p(0) = \frac{1}{2}\end{aligned}$$

The resulting states for each outcome are

$$\begin{aligned}\text{measurement outcome 0: } & \alpha|00\rangle + \beta\omega|10\rangle \\ & = (\alpha|0\rangle + \beta\omega|1\rangle) \otimes |0\rangle \\ \text{measurement outcome 1: } & (S \otimes I)(\alpha\omega|01\rangle + \beta|11\rangle) \\ & = \alpha\omega|01\rangle + \beta i|11\rangle \\ & = \omega(\alpha|0\rangle + \beta\omega|1\rangle) \otimes |1\rangle\end{aligned}$$

Both of which have the desired qubit state (up to global phase) in the first register.

□