Homework #1
Due by 8:00 am, 10/8/2025

1. (a) [5 pt] Let $\vec{a}$ and $\vec{b}$ be two real three-dimensional vectors. Prove that

$$(\vec{a}\cdot\vec{\sigma})(\vec{b}\cdot\vec{\sigma}) = (\vec{a}\cdot\vec{b})I + i(\vec{a}\times\vec{b})\cdot\vec{\sigma}$$

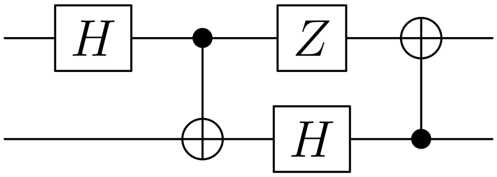
where $\vec{\sigma}$ represents the three Pauli operators σ_x, σ_y and σ_z.

(b) [5 pt] Let $\vec{v}$ be a real three-dimensional unit vector and θ be a real number. Prove that

$$\exp(i\theta\vec{v}\cdot\vec{\sigma}) = I\cos\theta + i\vec{v}\cdot\vec{\sigma}\sin\theta$$

where $\vec{v}\cdot\vec{\sigma} \equiv \sum_{i=1}^{3} v_i\sigma_i$.

2. Consider the following quantum circuit C

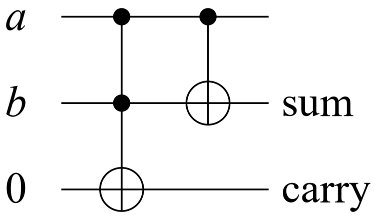


(a) [5 pt] Write down the unitary matrix U corresponding to C, with respect to the computational basis.

(b) [5 pt] Write down a quantum circuit for the unitary U^{-1}.

(c) [5 pt] If C is applied to the initial state $|0\rangle|0\rangle$ and is followed by a measurement in the computational basis, what is the distribution of the measurement outcome?

3. [10 pt] The following circuit realizes a quantum half adder



Write down the output for all the possible input states $|a\rangle|b\rangle$ in the computational basis and verify that it satisfies the truth table for a half adder. Explain why it is not necessary to preserve the second input $|b\rangle$ for the function to be reversible.

4. [10 pt] Suppose we have a quantum circuit on n qubits which consists of poly(n) gates picked from a universal set of $\{H, S, T, \text{CNOT}\}$, followed by a final measurement of all the qubits in the computational basis. Further assume that at each step of the computation (after each gate) the quantum state is unentangled, meaning that it can always be expressed as the tensor product of the single-qubit states of the n qubits. Prove that this quantum circuit can be simulated efficiently by a classical computer. That is, it takes poly(n) time for a classical computer to exactly sample the probability distribution of the measurement outcome. Therefore, we say that quantum entanglement is necessary for quantum speedup.

5. A simple case of Grover's algorithm. Consider an unstructed search problem in the 4-element set $\{0,1\}^{\otimes 2}$ with the unique solution $\omega = 01$.

(a) [5 pt] Write down the matrix for the oracle U_ω, with respect to the computational basis.

(b) [5 pt] Write down the matrix for the operator U_S, and further compute the matrix for a Grover iteration, both with respect to the computational basis.

(c) [10 pt] How many Grover iterations should be used to find the solution? Verify that for this $N = 4$ case, the computed number of Grover iterations can give the solution ω with 100% probability. Further, what is the probability to find the solution if one more Grover iteration is applied?

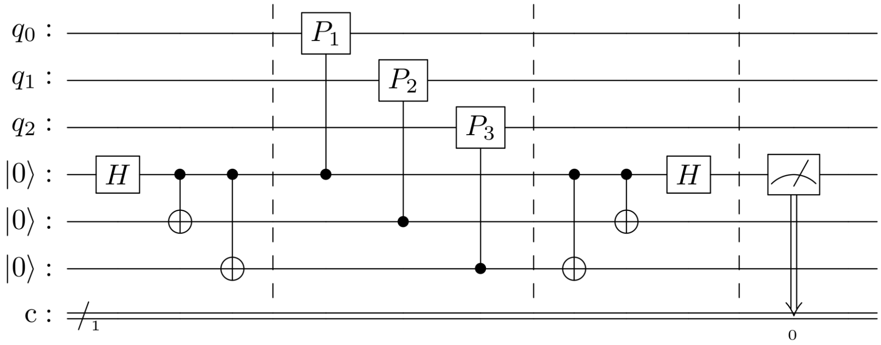
6. [10 pt] Classical algorithm for factoring. Suppose we want to factor $L = 85$ and we choose $a = 3$ which is coprime to L. Follow the steps in the lecture note to find the order of a modulo L, and use it to factor L. [You can write a computer program to find the order.]

7. Consider 7 physical qubits encoding the Steane code with stabilizers $X_4X_5X_6X_7$, $X_2X_3X_6X_7$, $X_1X_3X_5X_7$, $Z_4Z_5Z_6Z_7$, $Z_2Z_3Z_6Z_7$ and $Z_1Z_3Z_5Z_7$. Suppose all the encoding, stabilizer measurement and error correction operations are perfect, but after encoding, each qubit is subjected to an independent depolarization error with small probability $p \ll 1$. That is, with independent probability distribution $\{1-p, p/3, p/3, p/3\}$, each physical qubit undergoes a gate $\{I, X, Y, Z\}$.

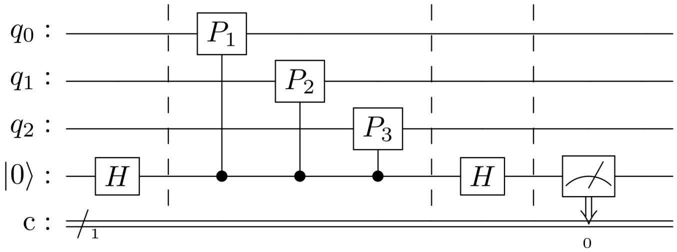
(a) [10 pt] For all the possible single-qubit Pauli X and Pauli Z errors, determine the error syndrome when measuring the stabilizers of the Steane code.

(b) [5 pt] What is the error syndrome for a two-qubit error X_1X_5 on the first and the fifth qubits? Under the assumption of small and independent errors, what is the most likely cause for this error syndrome? If we design the quantum error correction step to correct this most likely cause, can we correct this two-qubit error?

8. [10 pt] In the fault-tolerant measurement of a multi-qubit Pauli observable, we use multiple ancilla qubits in a GHZ state rather than a single ancilla to prevent the propagation of errors. Prove that the following two circuits are equivalent in the ideal case, where P_1, P_2 and P_3 are arbitrary Pauli gates.



q_0 :
q_1 :
q_2 :
$|0\rangle$:
$|0\rangle$:
$|0\rangle$:
c :
1
H
P_1
P_2
P_3
H
0



q_0 :
q_1 :
q_2 :
$|0\rangle$:
c :
1
H
P_1
P_2
P_3
H
0