CS-151 Quantum Computer Science: Problem Set 4

Professor: Saeed Mehraban
TA: Dale Jacobs

Spring, 2024

Guidelines: ***The deadline to return this problem set is 11.59pm on Friday, February 23th***. *Remember that you can collaborate with each other in the preliminary stages of your progress, but each of you must write their solutions independently. Submission of the problem set should be via Gradescope only. Best wishes!*

Problem 1 (15 points). *In lecture, we defined the Clifford gates as the set of operators generated by* $\{ H, X, Y, Z, CNOT \}$.

a) *Recall the phase gate is the matrix* $S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$. *Show that* X, Y, Z *can be expressed in terms of* S *and* H *(by multiplying these matrices together).*

b) *Let* $\mathbb{P}_n$ *be the set of* n*-fold tensor products of the Pauli matrices, up to a global phase* $1, -1, i, -i$. *For instance,* $-iX \otimes Y \in \mathbb{P}_2$. *For any unitary* U, *to show that it belongs to the* ***Clifford group*** *of quantum gates it suffices to show that* $UPU^\dagger \in \mathbb{P}_n$ *where* $P \in \mathbb{P}_n$ *is a tensor product of only* I, X *and* Z. *Verify that* H, S, *and* $CNOT$ *are Clifford gates. (Hint: It is enough to verify this condition only for* ZI, IZ, XI, IX. *If you use this hint, please justify it.)*

c) *Recall that* $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$. *Show that* T *is not a Clifford gate. i.e.,* $TXT^\dagger \notin \mathbb{P}_1$. *Use this result to conclude that the Clifford gates generated by* $\{ H, S, CNOT \}$ *are not universal for quantum computation.*

Problem 2. *Let* $|\psi\rangle = |0\rangle |\phi_0\rangle + |1\rangle |\phi_1\rangle$ *be a quantum state. We will show that the probability of measuring* 0 *on the first register is* $\langle \phi_0 | \phi_0 \rangle$ *and the probability of measuring* 1 *on the first register is* $\langle \phi_1 | \phi_1 \rangle$.

a) *Let* $|\psi\rangle = \frac{2}{\sqrt{5}} |0\rangle |+\rangle + \frac{1}{\sqrt{5}} |1\rangle |-\rangle$. *Use the Born rule to find the probability of measuring* 0 *on the first register, and* 1 *on the first register.*

b) *Now prove the general case: that is, let* $|\psi\rangle = |0\rangle |\phi_0\rangle + |1\rangle |\phi_1\rangle$ *be an* $(n+1)$*-qubit quantum state. Show that the probability of measuring* 0 *on the first register is* $\langle \phi_0 | \phi_0 \rangle$ *and the probability of measuring* 1 *on the first register is* $\langle \phi_1 | \phi_1 \rangle$.

Problem 3 (20 points). *The SWAP test is a quantum procedure that allows us to distinguish whether two quantum states are close or far. The procedure is based on the swap operator, which takes two arbitrary quantum states,*

$$SWAP : |\psi\rangle |\phi\rangle \mapsto |\phi\rangle |\psi\rangle$$

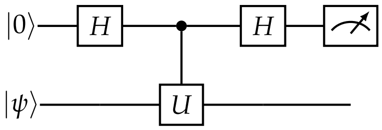
a) *Prove that* $SWAP$ *is a unitary operation.*

b) *Given two states* $|\psi\rangle$ *and* $|\phi\rangle$, *the Swap test is the following procedure: We prepare an ancilla* $|0\rangle$ *and apply a Hadamard gate to it. Controlled on this bit, we applied* $SWAP$ *to the registers* $|\psi\rangle |\phi\rangle$. *The result is the state,*

$$\frac{1}{\sqrt{2}} \left(|0\rangle |\psi\rangle |\phi\rangle + |1\rangle |\phi\rangle |\psi\rangle \right)$$

We then apply a Hadamard gate to the first register and measure in the computational basis. What is the probability obtaining 0*? How can we use this procedure to decide whether two quantum states are 'close' or 'far' from being the same?*

Problem 4. *Recall from lecture that we can obtain the real component of* $\langle\psi| U |\psi\rangle$ *using the following circuit:*



a) *Give a circuit which can be used to estimate the* ***imaginary*** *part of* $\langle\psi| U |\psi\rangle$*, and explain how to use the circuit to do so. (hint: some of the following gates may be useful)*

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Problem 5. *For this question, let*

$$|\Phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$$

be an entangled bell pair shared between two parties Alice (A) and Bob (B).

a) *Show that* $|\Phi_+\rangle$ *is not separable. That is, it cannot be written as a tensor product of single-qubit quantum states.*

b) *Let* $|\theta_\pm\rangle = \cos(\theta)|0\rangle \pm \sin(\theta)|1\rangle$ *and let* $|\phi_\pm\rangle = \cos(\phi)|0\rangle \pm \sin(\phi)|1\rangle$*. Suppose Alice and Bob share a bell pair* $|\Phi_+\rangle_{AB}$*, and Alice measures her half in the* θ *basis and Bob measures his half in the* ϕ *basis. Show that the probability that they obtain the same values (++ or – in their respective basis) is* $\cos^2(\theta - \phi)$*.*

Problem 6 (No signaling). *In this problem, we study several features of entangled states. Let*

$$|\Psi_-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

be an entangled state shared between two parties Alice (A) and Bob (B).

a) *Suppose Bob measures his half. What is the probability that he obtains* 0*?* ***[5 points]***

b) *Prove that for any* 2×2 *unitary matrix* U *the following holds up to a global phase,* ***[10 points]***

$$(U_A \otimes I_B)|\Psi_-\rangle_{AB} = (I_A \otimes U_B^{-1})|\Psi_-\rangle_{AB}$$

(Hint: For 2×2 *matrices,* $U = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix}$ *has an inverse,* $U^{-1} = \frac{1}{Det(U)} \begin{pmatrix} U_{11} & -U_{01} \\ -U_{10} & U_{00} \end{pmatrix}$*. When* U *is unitary,* $Det(U)$ *is just a global phase, so we can ignore it.)*

This means that when Alice applies a unitary gate on her half, she can assume she has not applied it, and Bob has applied U^{-1}*. Next, we show even if entangled states allow such counterintuitive correlations, Alice still cannot use them to send instant signals to Bob.*

c) *Let* $|\Psi_U\rangle_{AB} = (U_A \otimes I_B)|\Psi_-\rangle_{AB}$*. Suppose Bob measures the B half of* $|\Psi_U\rangle_{AB}$*. What is the probability that he obtains the outcome* 0*?*

d) *Briefly explain why this result means Alice cannot send instant signals to Bob.*

Problem 7 (Extra credit). *Prove that any quantum algorithm that runs in polynomial time and succeeds in giving the correct answer with a probability more than* $2/3$ *can be transformed into a polynomial-time quantum algorithm with a probability of success more than* $1 - 1/2^{n^c}$ *where* c *is an arbitrary constant.*