

CSCI3350 Introduction to Quantum Computing (2026 Spring)

Recitation

Xiao Liang

<https://xiao-liang.github.io/>

Department of Computer Science and Engineering

The Chinese University of Hong Kong

1. (0 points) Is it always true that

$$(A + B) \otimes C = A \otimes C + B \otimes C$$

for matrices of compatible sizes? Prove your claim.

Solution: Yes.

The tensor product is bilinear. If

$$A = (a_{ij}), \quad B = (b_{ij}),$$

then by definition

$$A \otimes C = (a_{ij}C)_{ij}, \quad B \otimes C = (b_{ij}C)_{ij}.$$

Hence

$$(A + B) \otimes C = ((a_{ij} + b_{ij})C)_{ij} = (a_{ij}C)_{ij} + (b_{ij}C)_{ij} = A \otimes C + B \otimes C.$$

So the identity is always true whenever the matrix sizes are compatible.

2. (0 points) Let

$$V = (I \otimes H) CZ,$$

where CZ is the controlled-Z gate. Prove that V cannot be written in the form $U_1 \otimes U_2$ for any single-qubit unitaries U_1, U_2 .

Solution: Assume, for contradiction, that

$$V = U_1 \otimes U_2$$

for some single-qubit unitaries U_1, U_2 .

Then V must map every product state to another product state, since

$$(U_1 \otimes U_2)(|\alpha\rangle \otimes |\beta\rangle) = (U_1 |\alpha\rangle) \otimes (U_2 |\beta\rangle).$$

Now consider the product state $|+\rangle \otimes |+\rangle$. We compute:

$$\text{CZ}|++\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle).$$

Applying $I \otimes H$,

$$V|++\rangle = (I \otimes H)\text{CZ}|++\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle.$$

But $|\Phi^+\rangle$ is entangled, so it is not a product state.

Thus V maps a product state to an entangled state, which is impossible for an operator of the form $U_1 \otimes U_2$. This is a contradiction.

Therefore V cannot be written as $U_1 \otimes U_2$.

3. Let $x = (x_0, \dots, x_{N-1}) \in \{0, 1\}^N$, where $N = 2^n$, and let O_x be the standard oracle

$$O_x : |j, b\rangle \mapsto |j, b \oplus x_j\rangle.$$

- (a) (0 points) Let y be the string obtained from x by flipping only its last bit x_{N-1} . Using at most one query to O_x , design a circuit that implements one query to O_y .
- (b) (0 points) Let z be the string obtained from x by forcing its last bit to be 1, i.e.,

$$z_{N-1} = 1, \quad z_j = x_j \text{ for } j \neq N-1.$$

Using at most one query to O_x , design a circuit that implements one query to O_z .

Solution:

(a) First, we show how to implement a quantum circuit T defined below:

$$T : |j, b\rangle \mapsto |j, b \oplus \delta_{j,1^n}\rangle,$$

where $\delta_{j,1^n} = 1$ iff $j = 1^n$.

This is implemented by an n -controlled X gate with all n index qubits as controls and the answer qubit as target. Equivalently, if only 1- and 2-qubit gates are allowed, compute the AND of the n index bits into ancillas, apply a CNOT from the final ancilla to the answer qubit, and then uncompute the ancillas. This flips the answer qubit exactly when $j = 1^n$, and all ancillas return to $|0\rangle$.

Next, we show how to implement O_y using at most one query to O_x , as well as the circuit T from the above:

Since y differs from x only at the last position,

$$y_j = x_j \oplus \delta_{j,1^n}.$$

So the oracle O_y can be implemented as

$$O_y = T O_x,$$

where T is the circuit from part (a). Indeed,

$$|j, b\rangle \xrightarrow{O_x} |j, b \oplus x_j\rangle \xrightarrow{T} |j, b \oplus x_j \oplus \delta_{j,1^n}\rangle = |j, b \oplus y_j\rangle.$$

Thus one query to O_x , followed by the circuit T , implements O_y .

(b) Observe that:

$$z = \begin{cases} x, & \text{if } x_{N-1} = 1, \\ y, & \text{if } x_{N-1} = 0. \end{cases}$$

Hence, if we split into the two cases for the fixed string x , then:

- if $x_{N-1} = 1$, use O_x itself;
- if $x_{N-1} = 0$, use the construction from part (a).

In either case, this uses at most one query to O_x .

Remark. If one insists on a single uniform circuit independent of the unknown value of x_{N-1} , then such a one-query construction does not exist in general.

4. Recall the four Bell states

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

- (a) (0 points) Prove that these four states form an orthonormal basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$.
 (b) (0 points) Give a two-qubit circuit that maps

$$|\Phi^+\rangle \mapsto |00\rangle, \quad |\Phi^-\rangle \mapsto |10\rangle, \quad |\Psi^+\rangle \mapsto |01\rangle, \quad |\Psi^-\rangle \mapsto |11\rangle.$$

Briefly justify your answer.

Solution: (a) Each Bell state has norm 1. For example,

$$\langle \Phi^+ | \Phi^+ \rangle = \frac{1}{2} (\langle 00| + \langle 11|)(|00\rangle + |11\rangle) = 1.$$

Similarly for the other three.

They are pairwise orthogonal. For instance,

$$\langle \Phi^+ | \Phi^- \rangle = \frac{1}{2} (\langle 00| + \langle 11|)(|00\rangle - |11\rangle) = 0,$$

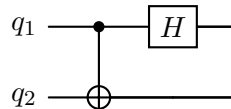
and

$$\langle \Phi^\pm | \Psi^\pm \rangle = 0$$

because $|00\rangle, |11\rangle$ are orthogonal to $|01\rangle, |10\rangle$.

So the four Bell states are orthonormal. Since $\mathbb{C}^2 \otimes \mathbb{C}^2$ has dimension 4, any orthonormal set of 4 vectors is an orthonormal basis. Therefore these four Bell states form an orthonormal basis.

(b) A suitable circuit is the inverse of the usual Bell-state preparation circuit:



that is: first apply CNOT (control on the first qubit, target on the second), then apply H to the first qubit.

Check on each Bell state:

$$|\Phi^+\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = |+\rangle \xrightarrow{H \otimes I} |00\rangle,$$

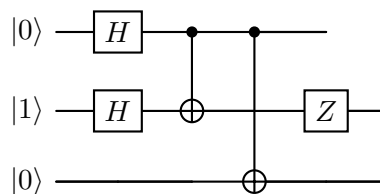
$$|\Phi^-\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) = |-\rangle \xrightarrow{H \otimes I} |10\rangle,$$

$$|\Psi^+\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = |+\rangle \xrightarrow{H \otimes I} |01\rangle,$$

$$|\Psi^-\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) = |-\rangle \xrightarrow{H \otimes I} |11\rangle.$$

So this circuit has exactly the required action.

5. Consider the following quantum circuit:



(a) (0 points) Compute the final three-qubit state in the computational basis.

(b) (0 points) If the third qubit is measured in the computational basis at the end, what are the possible outcomes and their probabilities?

Solution: (a) Start with $|010\rangle$.

After the two Hadamard gates on the first two qubits,

$$|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |1\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

so the state becomes

$$\frac{1}{2}(|000\rangle - |010\rangle + |100\rangle - |110\rangle).$$

After the first CNOT (qubit 1 controls qubit 2),

$$\frac{1}{2}(|000\rangle - |010\rangle - |100\rangle + |110\rangle).$$

After the second CNOT (qubit 1 controls qubit 3),

$$\frac{1}{2}(|000\rangle - |010\rangle - |101\rangle + |111\rangle).$$

Finally, applying Z to the second qubit changes the sign of the terms with second qubit equal to 1. Thus the final state is

$$\boxed{\frac{1}{2}(|000\rangle + |010\rangle - |101\rangle - |111\rangle)}.$$

(b) The third qubit is 0 in the first two basis states and 1 in the last two basis states. Hence:

$$\Pr(0) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}, \quad \Pr(1) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

So the possible outcomes are:

$$\boxed{0 \text{ with probability } \frac{1}{2}, \quad 1 \text{ with probability } \frac{1}{2}.}$$

If desired, the corresponding post-measurement states of the first two qubits are:

$$\text{outcome 0 : } \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle),$$

$$\text{outcome 1 : } -\frac{1}{\sqrt{2}}(|10\rangle + |11\rangle),$$

where the minus sign is a global phase and may be ignored.

6. (0 points) Let

$$|\Psi\rangle_{AB} = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle,$$

where $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. Suppose Alice applies an arbitrary single-qubit unitary V to her qubit A , while Bob does nothing to qubit B .

Prove that if Bob now measures his qubit in the computational basis, then his outcome proba-

bilities are unchanged by Alice's action. In other words, show that the probabilities of outcomes 0 and 1 remain

$$|a|^2 + |c|^2 \quad \text{and} \quad |b|^2 + |d|^2,$$

respectively.

Solution: Write

$$V = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix},$$

with V unitary.

Then

$$(V \otimes I) |\Psi\rangle_{AB} = aV|0\rangle|0\rangle + bV|0\rangle|1\rangle + cV|1\rangle|0\rangle + dV|1\rangle|1\rangle.$$

Expanding,

$$(V \otimes I) |\Psi\rangle_{AB} = |0\rangle \left((\alpha a + \beta c) |0\rangle + (\alpha b + \beta d) |1\rangle \right) + |1\rangle \left((\gamma a + \delta c) |0\rangle + (\gamma b + \delta d) |1\rangle \right).$$

Bob measures the second qubit.

For outcome 0, the amplitudes are

$$\alpha a + \beta c \quad \text{and} \quad \gamma a + \delta c.$$

Hence

$$\Pr(0) = |\alpha a + \beta c|^2 + |\gamma a + \delta c|^2.$$

But this is exactly

$$\left\| V \begin{bmatrix} a \\ c \end{bmatrix} \right\|^2.$$

Since V is unitary, it preserves norms, so

$$\Pr(0) = \left\| \begin{bmatrix} a \\ c \end{bmatrix} \right\|^2 = |a|^2 + |c|^2.$$

Similarly, for outcome 1,

$$\Pr(1) = |\alpha b + \beta d|^2 + |\gamma b + \delta d|^2 = \left\| V \begin{bmatrix} b \\ d \end{bmatrix} \right\|^2 = |b|^2 + |d|^2.$$

Therefore Bob's measurement probabilities are unchanged by Alice's local unitary:

$$\boxed{\Pr(0) = |a|^2 + |c|^2, \quad \Pr(1) = |b|^2 + |d|^2.}$$

7. (0 points) Let $s \in \{0, 1\}^n$ be an unknown bit string. You are given oracle access to the function

$$f_s(x) = s \cdot x \pmod{2},$$

where $s \cdot x$ denotes the bitwise inner product modulo 2. The corresponding oracle acts as

$$O_{f_s} : |x, b\rangle \mapsto |x, b \oplus f_s(x)\rangle.$$

Design a quantum algorithm that determines s using exactly one query to the oracle. Your answer should include:

- the initial state,
- the sequence of gates,
- and a proof of correctness.

Solution: This is the Bernstein–Vazirani algorithm.

Initial state. Start with

$$|0^n\rangle |1\rangle.$$

Sequence of gates.

1. Apply $H^{\otimes n}$ to the first register and H to the last qubit.
2. Query the oracle O_{f_s} once.
3. Apply $H^{\otimes n}$ again to the first register.
4. Measure the first register in the computational basis.

Computation. After the first Hadamards,

$$|0^n\rangle |1\rangle \mapsto \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

So the state is

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |-\rangle, \quad \text{where } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Now apply the oracle. Since

$$O_{f_s}(|x\rangle |-\rangle) = (-1)^{f_s(x)} |x\rangle |-\rangle,$$

we get

$$\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f_s(x)} |x\rangle |-\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{s \cdot x} |x\rangle |-\rangle.$$

Apply $H^{\otimes n}$ to the first register. Using the standard identity

$$H^{\otimes n} |s\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{s \cdot x} |x\rangle,$$

it follows that

$$H^{\otimes n} \left(\frac{1}{\sqrt{2^n}} \sum_x (-1)^{s \cdot x} |x\rangle \right) = |s\rangle.$$

Therefore the final state is

$$|s\rangle |-\rangle.$$

Proof of correctness. Measuring the first register now yields s with probability 1. Thus the algorithm determines the unknown string s using exactly one oracle query.

8. Suppose you are given an oracle O_f for a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, where

$$O_f : |x, b\rangle \mapsto |x, b \oplus f(x)\rangle.$$

Let $a \in \{0, 1\}^n$ and $c \in \{0, 1\}$ be fixed known strings. Define

$$g(x) = f(x \oplus a) \oplus c.$$

- (a) (0 points) Using at most one query to O_f , design a circuit that implements O_g .
 (b) (0 points) Briefly justify why your circuit is correct.

Solution: (a) Let X^a denote the operation that applies an X gate to input qubit i exactly when $a_i = 1$. Also, if $c = 1$, apply an X gate to the answer qubit; if $c = 0$, do nothing.

A circuit for O_g is:

$$\begin{aligned} |x, b\rangle &\xrightarrow{X^a \text{ on input, } X^c \text{ on answer}} |x \oplus a, b \oplus c\rangle \\ &\xrightarrow{O_f} |x \oplus a, b \oplus c \oplus f(x \oplus a)\rangle \xrightarrow{X^a \text{ on input}} |x, b \oplus c \oplus f(x \oplus a)\rangle. \end{aligned}$$

Since

$$g(x) = f(x \oplus a) \oplus c,$$

this final state is

$$|x, b \oplus g(x)\rangle.$$

Thus this implements O_g using exactly one query to O_f .

(b) The correctness follows directly from the computation above:

$$b \mapsto b \oplus c \mapsto b \oplus c \oplus f(x \oplus a) = b \oplus g(x).$$

Meanwhile the input register is first changed from x to $x \oplus a$ so that the oracle sees the correct argument, and then changed back to x . Therefore the overall transformation is exactly

$$|x, b\rangle \mapsto |x, b \oplus g(x)\rangle.$$