CS4268, AY 2025-26 Sem 2

Lecturer: Divesh Aggarwal [1] Tutorial Week 5

1 [Tensor Product Practice.]

In this problem, you may assume that $(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD)$ (provided A has the same number of columns as C has rows, and similarly for B and D). We sort of saw this in class, by observing that the two matrices $(A \otimes B) \cdot (C \otimes D)$ and $(AC) \otimes (BD)$ act in the same way on each basis vector $|i\rangle \otimes |j\rangle$, namely by mapping it to $(AC\,|i\rangle) \otimes (BD\,|j\rangle)$.

(a) In typical linear algebra notation, given an $m \times n$ matrix A, one names its entries A_{ij} for $1 \le i \le m$, $1 \le j \le n$. Show that with bra-ket notation, one can instead name them $\langle i|A|j\rangle$.

(b) Show that the definition of the Kronecker product follows from the rule about multiplication I said you could assume. Basically, explain what's going on in this equation:

$$\langle ik|A \otimes B|j\ell\rangle = \langle i|A|j\rangle\langle k|B|\ell\rangle.$$

(c) The "element-wise product" of matrices $A, B \in \mathbb{C}^{m\times n}$ is the matrix $A \circ B \in \mathbb{C}^{m\times n}$ defined by

$$\langle i|A \circ B|j\rangle = \langle i|A|j\rangle\langle i|B|j\rangle.$$

Show that $(A \otimes B) \circ (C \otimes D) = (A \circ C) \otimes (B \circ D)$.

(d) Show that if A and B are invertible matrices, then so is $A \otimes B$, and in fact

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

(e) Verify that

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger.$$

(f) [**] Suppose $|u_1\rangle, \ldots, |u_d\rangle$ is an orthonormal basis for $\mathbb{C}^d$, and $|v_1\rangle, \ldots, |v_e\rangle$ is an orthonormal basis for $\mathbb{C}^e$. Show that the collection $|u_i\rangle \otimes |v_j\rangle$ (for all $1 \le i \le d$, $1 \le j \le e$) is an orthonormal basis for $\mathbb{C}^{de}$. (Hint/request: exploit Dirac's bra-ket notation to the hilt.)

2 [1 ebit + 1 qubit $\geq$ 2 bits.]

(a) [**] Alice and Bob prepare an EPR pair (that is, two qubits in the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$). They each take one qubit home. Suddenly, Alice decides she wishes to convey one of 4 messages to Bob; in other words, she wants to convey a classical string $uv \in \{0,1\}^2$ to Bob.

[1] Problems are taken from the homework sheets of Ryan O'Donnell's course in 2018; https://www.cs.cmu.edu/~odonnell/quantum18/

Alice does the following in the privacy of her own home: First, if $u = 1$, she applies a NOT gate to her qubit (else if $u = 0$ she does nothing here). Next, if $v = 1$, she applies a "Z" gate,

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

to her qubit (else if $v = 0$, she does nothing here). Finally, she walks to Bob's house and silently hands him her qubit.

Show that by measuring in an appropriate basis, Bob can exactly determine Alice's message $uv \in \{0,1\}^2$.

(b) Work out a circuit using only CNOT gates, 1-qubit gates, and "standard" measurement gates, which actually outputs Alice's message with 100% probability.

3 [Indistinguishable States.]

(a) [**] Let $|\psi\rangle$ and $|\psi^\perp\rangle$ be orthonormal qubit states. Show

$$\tfrac{1}{\sqrt{2}}\,|\psi\rangle \otimes |\psi\rangle + \tfrac{1}{\sqrt{2}}\,|\psi^\perp\rangle \otimes |\psi^\perp\rangle$$

is precisely equal to the Bell state

$$\tfrac{1}{\sqrt{2}}\,|00\rangle + \tfrac{1}{\sqrt{2}}\,|11\rangle\,.$$

(b) [**] Let $|u\rangle \in \mathbb{C}^2$ be a qubit state and let $|v\rangle = c\,|u\rangle$, where c is a complex number of magnitude 1 (for example, $c = -1$ or $c = i$). (In this scenario, c is called a "global phase".)

Suppose someone hands you a qubit $|\psi\rangle$ and promises you that $|\psi\rangle$ is either $|u\rangle$ or $|v\rangle$. (You know, mathematically, exactly what $|u\rangle$ and $|v\rangle$ are; but you do not know whether $|\psi\rangle$ is $|u\rangle$ or $|v\rangle$.) Show, to the best of your abilities, that there is nothing you can possibly do to tell the difference. You should at least show that applying 1-qubit unitaries and 1-qubit measurements in any combination does not help. (If you want to be even more sophisticated, show that it doesn't help even if you introduce additional qubits in known states, and then apply unitaries and measurements to this larger-dimensional system.)

(c) [**] Suppose someone hands you a qubit $|\psi\rangle$ and promises you that they prepared it according to one of the following two scenarios:

Scenario 1: They flipped a fair coin, and set $|\psi\rangle = |0\rangle$ if the result was Heads and set $|\psi\rangle = |1\rangle$ if the result was Tails.

Scenario 2: They flipped a fair coin, and set $|\psi\rangle = |+\rangle$ if the result was Heads and set $|\psi\rangle = |-\rangle$ if the result was Tails.

Show, to the best of your abilities, that there is nothing you can possibly do to tell whether they employed Scenario 1 or Scenario 2. (Same comments as in (b) about what you should at least do, and what you can further strive to do.)

4 [Elementary Number Theory.]

Let $M > 1$ be an integer. Let $\mathbb{Z}_M^*$ denote the set of all integers $0 \leq A < M$ which have a reciprocal modulo M (meaning an integer R such that $A \cdot R = 1 \pmod{M}$).

(a) Show that $A \in \mathbb{Z}_M^*$ if and only if $\gcd(A, M) = 1$. (Hint: for the "if", do a careful analysis of Euclid's Algorithm from last homework to show that the GCD of two numbers is always an "integer linear combination" of the two numbers.)

(b) Let $\varphi(M)$ denote $|\mathbb{Z}_M^*|$. Show that if M is prime then $\varphi(M) = M - 1$, and that if M is the product of two distinct primes, $M = P \cdot Q$, then $\varphi(M) = (P-1)(Q-1)$.

(c) Show that $\mathbb{Z}_M^*$ is "closed under multiplication" $\pmod{M}$; i.e., if $A, B \in \mathbb{Z}_M^*$ then $A \cdot B \pmod{M}$ is also in $\mathbb{Z}_M^*$.

(d) Suppose we make the "multiplication table" for $\mathbb{Z}_M^*$; i.e., the array whose rows and columns are indexed by $\mathbb{Z}_M^*$, and whose (A, B)th entry is $A \cdot B \pmod{M}$. Show that in each row, all entries are distinct.

(e) By using the previous result, and by considering the product of all entries in row A, deduce that

$$A^{\varphi(M)} = 1 \pmod{M}.$$

(f) Conclude "Fermat's Little Theorem": if P is prime and $1 \leq A < P$, then

$$A^{P-1} = 1 \pmod{P}.$$

5 [Hadamard Transform I.]

[**] Suppose we start with n qubits in the state $|000\cdots 0\rangle$. Then, for a certain subset $S \subseteq [n]$, suppose we apply the Hadamard gate H to qubit i for each $i \in S$. Describe the resulting state in the most succinct/compelling way that you can. You might want to introduce the "indicator-string" $y \in \{0,1\}^n$ for the set S, and/or use the word "XOR", in your description.