Lecture 6

Introduction to quantum information processing

As mentioned, quantum information involves complex numbers. Let's recall the main facts that we need about them. In the following, a, b, c, d, θ will denote real numbers and i the imaginary unit.

1. The imaginary unit i is defined by $i^2 = -1$.
2. $(a+ib)(c+id) = ac + iad + ibc - bd = (ac - bd) + i(ad + bc)$.
3. $|a+ib| = \sqrt{a^2+b^2}$. The length of $a+ib$ in Argand diagram: this just means treating $a+ib$ as (a,b).
4. Euler's formula: $e^{i\theta} = \exp(i\theta) = \cos(\theta) + i\sin(\theta)$. Quiz: what is $|e^{i\theta}|$.
5. Complex conjugate: $(a+ib)^* = a - ib$.

Puzzle 2. *Comment: these properties follow from the above definitions and are commonly used, if you're rusty on complex numbers, you should prove them to check your understanding.*

1. *For all $z \in \mathbb{C}$, we have $|z|^2 = zz^*$.*
2. *Let $r_1, r_2, \theta_1, \theta_2 \in \mathbb{R}$. If $z_1 \coloneqq r_1 \exp(i\theta_1)$ and $z_2 \coloneqq r_2 \exp(i\theta_2)$, then $z_1 z_2 = r_1 r_2 \exp(i(\theta_1 + \theta_2))$.*

Definition 3 (Quantum state)**.** A *quantum state* of n qubits is described by a column vector of length 2^n:

$$\vec{\alpha} \coloneqq [\alpha_{0^n}, \alpha_{0^{n-1}1}, \ldots, \alpha_{1^n}]^\top \tag{21}$$

such that

1. $\alpha_x \in \mathbb{C}$ for all $x \in \{0,1\}^n$,
2. $\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$

Vectors $\vec{\alpha}$ of the above form are also referred to as *amplitude vectors*.

Warning: it is NOT true that every randomized state is a quantum state. Quantum computation still generalizes randomized computation due to complex numbers generalizing non-negative numbers but the generalization is more sophisticated through the formalism of density matrices (we will cover later).

Example 1. *Here are some examples and non-examples*

1. *$[1,0]^\top$ and $[0,1]^\top$ are quantum states (in fact, also randomized states and deterministic states)*
2. *$[1/2,\ 1/2]^\top$ is a randomized state but NOT a quantum state.*
3. *$[1/\sqrt{2}, 1/\sqrt{2}]^\top$ is a quantum state.*
4. *$[1/2, 1/\sqrt{2}]^\top$ is NOT a quantum state.*
5. *$[1/\sqrt{2}, i/\sqrt{2}]^\top$ is a quantum state.*
6. *$[(1+i\sqrt{3})/2, 0]^\top$ is a quantum state. It can be written as $[e^{i\pi/3}, 0]^\top$.*
7. *$[(1+2i)/\sqrt{3}, -2/3]^\top$ is NOT quantum state.*
8. *Comment: ask someone to give a 4-qubit quantum state Another example $[1/2, 1/2, 1/2, 1/2]$.*
9. *If $p = [p_{00}, p_{01}, p_{10}, p_{11}]$ is a randomized state. Then $p = [\sqrt{p_{00}}, \sqrt{p_{01}}, \sqrt{p_{10}}, \sqrt{p_{11}}]$ is a quantum state. If $\theta_{00}, \theta_{01}, \theta_{10}, \theta_{11}$ are real numbers, then $p = [\sqrt{p_{00}}e^{i\theta_{00}}, \sqrt{p_{01}}e^{i\theta_{01}}, \sqrt{p_{10}}e^{i\theta_{10}}, \sqrt{p_{11}}e^{i\theta_{11}}]$ is a quantum state. In fact, any 2-qubit quantum state is of this form (why?) and the obvious generalization of this statement to n qubits also holds. Note a complex number of unit modulus is also called a "phase", so $e^{i\theta_{00}}$ is a phase.*

Puzzle 3. *It is easy to see that every deterministic state is a quantum state. Is it possible for a randomized* but non-deterministic state *to be a quantum state? Comment: do at home.*

We will soon introduce Dirac notation, for which the notion of a Kronecker or tensor product is useful to define first.

Definition 4 (Kronecker or tensor product)**.** Let $A \in \mathbb{C}^{m_1 \times m_2}$ and $B \in \mathbb{C}^{n_1 \times n_2}$. Write

$$A \coloneqq \begin{pmatrix} a_{1,1}, & \dots & a_{1,m_2} \\ a_{2,1}, & \dots & a_{2,m_2} \\ \dots & & \\ a_{m_1,1}, & \dots, & a_{m_1,m_2} \end{pmatrix}. \tag{22}$$

The matrix $A \otimes B$ is the matrix in $\mathbb{C}^{m_1 n_1 \times m_2 n_2}$ defined by

$$A \otimes B \coloneqq \begin{pmatrix} a_{1,1}B, & \dots & a_{1,m_2}B \\ a_{2,1}B, & \dots & a_{2,m_2}B \\ \dots & & \\ a_{m_1,1}B, & \dots, & a_{m_1,m_2}B \end{pmatrix}. \tag{23}$$

Comment: Do one or two examples, one involving only column vectors (column vectors are matrices with width 1). When you need to manipulate tensor products, the first thing to try is not to invoke the definition but use its properties – see later. Esoteric aside: you might be wondering why two different words are used for the same thing, the reason is that tensor product is a more abstract concept for which Kronecker product is an instantiation; there are other instantiations in other contexts but in quantum information, Kronecker product is the main instantiation.

Dirac notation. Conventional in Dirac notation to write $\vec{\alpha}$ as $|\alpha\rangle$ and the above Eq. (21) as

$$|\alpha\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle \quad \text{or} \quad |\alpha\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x_1\rangle |x_2\rangle \dots |x_n\rangle \quad \text{or} \quad |\alpha\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \tag{24}$$

The notation $|\alpha\rangle$ indicates that the object is a column vector with label α; it is pronounced "ket α". Comment: could use whatever label you want, often see $|\psi\rangle$, $|\phi\rangle$, but can also write $|\text{whatever}\rangle$ First observe that this way of writing is in one-to-one correspondence with the vector way of writing. In addition, the first expression is also compatible with the definition of Kronecker product under the following convention in Dirac notation:

$$|0\rangle \coloneqq \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle \coloneqq \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{25}$$

In $\mathbb{C}^d$ for $d > 2$, conventional in Dirac notation to write either

$$|0\rangle = [1, \dots, 0]^\top, \dots, |d-1\rangle = [0, \dots, 1]^\top, \tag{26}$$

which is compatible with the $d = 2$ case above, but also

$$|1\rangle = [1, \dots, 0]^\top, \dots, |d\rangle = [0, \dots, 1]^\top \tag{27}$$

Comment: note that the latter indexing is not the same as the $d = 2$ case. In HW1, Q3, the latter indexing is used. It should be clear from context what the convention is. In general, Kronecker products are often suppressed between kets.

For example, when $d = 3$:

$$\frac{1}{\sqrt{3}} \sum_{i=1}^{3} |i\rangle |i\rangle = \frac{1}{\sqrt{3}} \sum_{i=1}^{3} |i\rangle \otimes |i\rangle = \frac{1}{\sqrt{3}} \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right) = \frac{1}{\sqrt{3}} [1,0,0,0,1,0,0,0,1]^\top, \tag{28}$$

and for column vectors $|u_1\rangle, |u_1\rangle, |u_1\rangle$ and $|v_1\rangle, |v_2\rangle, |v_3\rangle$, the notation $\frac{1}{\sqrt{3}} \sum_{i=1}^{3} |u_i\rangle |v_i\rangle$ means

$$\frac{1}{\sqrt{3}} \sum_{i=1}^{3} |u_i\rangle \otimes |v_i\rangle . \tag{29}$$

Fact 1 (Properties of Kronecker product)**.** Let A, B, C, D be complex matrices (not necessarily square, or have the same dimensions). Let $\alpha, \beta \in \mathbb{C}$. Then

1. Bilinearity. Suppose A, B have the same dimensions. Then

$$C \otimes (\alpha A + \beta B) = \alpha(C \otimes A) + \beta(C \otimes B) \quad \text{and} \quad (\alpha A + \beta B) \otimes C = \alpha(A \otimes C) + \beta(B \otimes C). \tag{30}$$

2. Associativity. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$.

3. Mixed product property. Suppose AC and BD are well-defined. Then

$$(A \otimes B) \cdot (C \otimes D) = AC \otimes BD. \tag{31}$$

(Saying AC is well-defined is equivalent to saying the width of A is the same as the height of C, so they can be multiplied together.) Comment: In class, I wrote A, C have the same dimensions and B, D have the same dimensions; that's incorrect as AC and BD could still be ill-defined.

Quiz: Commutativity? That is, is it true that $A \otimes B = B \otimes A$ for all A, B?

Definition 5 (Complex conjugate, transpose, complex conjugate transpose, unitary)**.** Let $A \in \mathbb{C}^{L \times R}$.

1. Complex conjugate of A is denoted $A^* \in \mathbb{C}^{L \times R}$ and defined entrywise by $(A^*)_{ij} \coloneqq A^*_{ij}$
2. Transpose of A is denoted $A^\top \in \mathbb{C}^{R \times L}$ and defined entrywise by $A^\top_{i,j} = A_{j,i}$.
3. The complex conjugate transpose of A is denoted $A^\dagger$ and defined by $(A^*)^\top$. Comment: check this equals $(A^\top)^*$.

We say a complex matrix U is *unitary* if U is square and

$$U^\dagger U = I, \tag{32}$$

where I denotes the identity matrix.

Definition 6. We say (column vectors) $|u_1\rangle, \ldots, |u_d\rangle \in \mathbb{C}^d$ form an orthonormal basis if there exists a $d \times d$ unitary matrix U such that

$$|u_i\rangle = U |i\rangle \tag{33}$$

for all $i \in \{1, \ldots, d\}$.

The following observation may also be useful for HW1, Q3. Suppose $A \in \mathbb{C}^{d \times d}$, then

$$A |i\rangle = \sum_{j=1}^{d} A_{j,i} |j\rangle \tag{34}$$

for all $i \in \{1, \ldots, d\}$.