41076: Methods in Quantum Computing

'Introduction to Quantum Mechanics' Module

Dr. Mária Kieferová based on the materials from Dr. Min-Hsiu Hsieh
Centre for Quantum Software & Information, Faculty of Engineering and Information Technology, University of Technology Sydney

Abstract

Contents to be covered in this lecture are

1. Linear algebra
2. Quantum states
3. Quantum operations
4. No-cloning theorem
5. Measurement

In this lecture, we will examine the concepts of quantum states, operations and measurement from a more mathematical standpoint. This will give us the framework for discussing quantum protocols in subsequent lectures. The following text assumes existing familiarity with quantum states, operations and measurements on the level of UTS 41170 Introduction to Quantum Computing. If you need a refresher of these concepts before we delve into the maths, The Qiskit Textbook provides an easy to understand, high-level overview.

The language of quantum mechanics is linear algebra often written using the Dirac (bra-ket) notation. We will first establish the formalism of linear algebra in Dirac notation and review linear algebra concepts that often come up in quantum computing and quantum information.

1 Linear Algebra in Dirac notation

A d-dimensional Hilbert space $\mathcal{H}$ is a vector space equipped with an inner product. Let $\{\boldsymbol{e}_i\}_{i=0}^{d-1}$ be the computational basis, where $\boldsymbol{e_i}$ is a column vector of zeros except a '1' at the $(i+1)$-th entry. Any vector $\boldsymbol{v} \in \mathcal{H}$ can be decomposed into basis vectors $\boldsymbol{e_i}$ as

$$\boldsymbol{v} = \sum_{i=0}^{d-1} v_i \boldsymbol{e}_i, \tag{1}$$

for some complex number $v_i \in \mathbb{C}$. The inner product (or dot product) '$\cdot$' of two vectors $\boldsymbol{u}$ and $\boldsymbol{v}$ in the same basis in $\mathcal{H}$ is defined as

$$\boldsymbol{u} \cdot \boldsymbol{v} = \boldsymbol{u}^\dagger \boldsymbol{v} = \sum_{i=0}^{d-1} u_i^* v_i, \tag{2}$$

where † denotes transpose and conjugate.

An alternative way of expressing linear algebra is through bra-ket (Dirac) notation. Throughout this subject, we will denote $|i\rangle \equiv \boldsymbol{e}_i$ and write $\boldsymbol{v}$ as $|v\rangle$:

$$|v\rangle = \sum_{i=0}^{d-1} v_i |i\rangle. \tag{3}$$

This is sometimes known as amplitude encoding of a vector $v = \sum_i v_i e_i$. The inner product of $|u\rangle$ and $|v\rangle$ in $\mathcal{H}$ becomes

$$\langle u|v\rangle = \sum_{i,j} u_i^* v_j \langle i|j\rangle = \sum_i u_i^* v_i \tag{4}$$

where $\langle u| \equiv |u\rangle^\dagger$ is now a row vector and $\langle i|j\rangle = \delta_{i,j}$.

The choice of the basis state $\{|i\rangle\}$ is arbitrary as long as all states $|i\rangle$ are mutually orthogonal and normalized (of course, one could define a non-orthonormal basis but why would you?). However, choosing a convenient basis (typically either the computational basis or an eigenbasis of some operator) makes any work easier.

For a Hilbert space $\mathcal{H}$, we denote $\mathcal{L}(\mathcal{H})$ the collection of linear operators $L : \mathcal{H} \to \mathcal{H}$. We denote the identity operator $I = \sum_{i=0}^{d-1} |i\rangle\langle i|$. Given an linear operator L, there is an equivalent matrix representation $[L_{i,k}]$ in the basis spanned by $\{|i\rangle\langle k|\}$:

$$L = \sum_{i,k=0}^{d-1} L_{i,k} |i\rangle\langle k|, \tag{5}$$

where $L_{i,k} = \langle i|L|k\rangle$.

An linear operator $H \in \mathcal{L}(\mathcal{H})$ is called *Hermitian* if and only if $H^\dagger = H$. For a Hermitian matrix H, the *spectral theorem* states that there exists an orthonormal basis $\{|\nu_i\rangle\}$ and real numbers $\{\lambda_i\} \in \mathbb{R}$ so that

$$H = \sum_i \lambda_i |\nu_i\rangle\langle \nu_i|. \tag{6}$$

Equivalently, $\{\lambda_i\}$ and $\{|\nu_i\rangle\}$ are known as eigenvalues and eigenvectors of H, respectively.

Exercise 1. *Verify that Pauli X is a Hermitian operator and compute its eigenvalues and eigenvectors.*

A Hermitian operator $P \in \mathcal{L}(\mathcal{H})$ is *positive*, denoted as $P \geq 0$, if and only if $\langle v|P|v\rangle \geq 0$ for all $|v\rangle \in \mathcal{H}$. We denote $\mathcal{L}(\mathcal{H})_+ = \{P \geq 0 : P \in \mathcal{L}(\mathcal{H})\}$ the set of positive semi-definite operators on $\mathcal{H}$.

1.1 Tensor product of Hilbert spaces

Given two vectors $|u\rangle \in \mathcal{H}_A$ and $|v\rangle \in \mathcal{H}_B$, the tensor product '$\otimes$' of them is

$$|u\rangle \otimes |v\rangle = \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} u_i v_j |i\rangle \otimes |j\rangle, \tag{7}$$

a vector of $d_A d_B$-dimension. If $\{|i\rangle_A\}$ and $\{|j\rangle_B\}$ are orthonormal bases in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, then $\{|i\rangle_A \otimes |j\rangle_B\}$, $i \in \{0, \cdots, d_A - 1\}$ and $j \in \{0, \cdots, d_B - 1\}$, forms an orthonormal basis in $\mathcal{H}_A \otimes \mathcal{H}_B$. In vector notation this gives:

$$\vec{v} = \begin{pmatrix} v_0 \\ v_1 \end{pmatrix}, \quad \vec{u} = \begin{pmatrix} u_0 \\ u_1 \end{pmatrix}, \tag{8}$$

$$\vec{v} \otimes \vec{u} = \begin{pmatrix} v_0 \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \\ v_1 \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} v_0 u_0 \\ v_0 u_1 \\ v_1 u_0 \\ v_1 u_1 \end{pmatrix} \tag{9}$$

The inner product on the space $\mathcal{H}_A \otimes \mathcal{H}_B$ is defined by

$$(\langle v_1|_A \otimes \langle u_1|_B)(|v_2\rangle_A \otimes |u_2\rangle_B) = \langle v_1|v_2\rangle\langle u_1|u_2\rangle. \tag{10}$$

The resulting matrix can be also written as

$$L \otimes M = \begin{pmatrix} L_{1,1}M & \vdots & L_{1,d_A} \\ \vdots & \ddots & \vdots \\ L_{d_A,1}M & \vdots & L_{d_A,d_A} \end{pmatrix} \tag{11}$$

This definition extends to tensor product of linear operators in $\mathcal{L}(\mathcal{H})$:

$$\begin{aligned} L \otimes M &= \left(\sum_{i,j=0}^{d_A-1} L_{i,j}|i\rangle\langle j|\right) \otimes \left(\sum_{k,\ell=0}^{d_B-1} M_{k,\ell}|k\rangle\langle \ell|,\right) \\ &= \sum_{i,j=0}^{d_A-1} \sum_{k,\ell=0}^{d_B-1} L_{i,j}M_{k,\ell}|i\rangle\langle j| \otimes |k\rangle\langle \ell|. \end{aligned} \tag{12}$$

Useful properties of tensor product are summarised as follows.

1. $(A_1 \otimes \cdots \otimes A_k)(B_1 \otimes \cdots \otimes B_k) = (A_1B_1 \otimes \cdots \otimes A_kB_k)$
2. $(A_1 \otimes \cdots \otimes A_k)^{-1} = A_1^{-1} \otimes \cdots \otimes A_k^{-1}$
3. $(A_1 \otimes \cdots \otimes A_k)^\dagger = A_1^\dagger \otimes \cdots \otimes A_k^\dagger$
4. If $\lambda_1, \cdots, \lambda_k$ are eigenvalues of $A_1, \cdots, A_k$ with eigenvectors $|u_1\rangle, \cdots, |u_k\rangle$, respectively, then $\prod_{i=1}^k \lambda_i$ is an eigenvector of $A_1 \otimes \cdots \otimes A_k$ with respect to the eigenvector $|u_1\rangle \otimes \cdots \otimes |u_k\rangle$.

1.2 Trace and Partial Trace

The trace $\mathrm{Tr} : \mathcal{L}(\mathcal{H}) \to \mathbb{C}$ is a linear map defined by

$$\mathrm{Tr}\,|j\rangle\langle k| = \langle k|j\rangle = \delta_{k,j}. \tag{13}$$

Extended by linearity, the trace of a linear operator L is then

$$\begin{aligned}
\operatorname{Tr} L &= \operatorname{Tr}\left(\sum_{i,k=0}^{d-1} L_{i,k}|i\rangle\langle k|\right) \\
&= \sum_{i,k=0}^{d-1} L_{i,k} \operatorname{Tr}|i\rangle\langle k| && (14) \\
&= \sum_{i,k=0}^{d-1} \langle i|L|k\rangle \delta_{i,k} && (15) \\
&= \sum_{i=0}^{d-1} \langle i|L|i\rangle. && (16)
\end{aligned}$$

Exercise 2 (Cyclic property)**.** *Show that* $\operatorname{Tr} LM = \operatorname{Tr} ML$*.*

Exercise 3. *Show that* $\operatorname{Tr} A$ *is independent of the basis of* A*.*

Note that $\operatorname{Tr} L^\dagger M$ defines an inner product on the space of $\mathcal{L}(\mathcal{H})$, and is known as the Hilbert-Schmidt inner product.

A partial trace is a generalization of a trace. While a trace maps an operator to a scalar, partial trace maps an operator to a lower-dimensional operator. Formally, partial trace $\operatorname{Tr}_A : \mathcal{L}(\mathcal{H}_{AB}) \to \mathcal{L}(\mathcal{H}_B)$ is defined by

$$\operatorname{Tr}_A(|i\rangle\langle j|_A \otimes |k\rangle\langle \ell|_B) = \langle j|i\rangle |k\rangle\langle \ell|_B = \delta_{i,j}|k\rangle\langle \ell|_B. \tag{17}$$

For a composite system on the space $\mathcal{H}_A \otimes \mathcal{H}_B$, Tr_A gives trace only over the subsystem on $\mathcal{H}_A$. We often say that we "trace-over A.

2 Quantum States

We are already familiar with qubits defined as

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{18}$$

where $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. Instead of using the vector form in Eq. (18), we will adopt the notation convention, the Dirac notation introduced in Section 1. Specifically, we will use the ket notation $|\cdot\rangle$ to denote a column vector of length one, e.g.,

$$|\psi\rangle := \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{19}$$

and use the bra notation $\langle\cdot|$ to denote the hermitian conjugate of $|\cdot\rangle$:

$$\langle\psi| := \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}. \tag{20}$$

We will also denote the computational basis of a d dimensional Hilbert space as $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$, where $|i\rangle$ is a column vector of zeros except a '1' in the $(i+1)$-th entry. The qubit $|b\rangle$ in Eq. (18) can be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{21}$$

The quantum state $|b\rangle$ is viewed as in a *superposition* of states $|0\rangle$ and $|1\rangle$, a phenomenon unique in quantum mechanics. Generally, a quantum state in a d-dimensional Hilbert space can be expressed

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle, \tag{22}$$

where the *amplitude* α_i satisfies $\sum_i |\alpha_i|^2 = 1$.

Given two quantum states $|\psi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$, the joint quantum state is $|\varphi\rangle_{AB} \equiv |\psi\rangle_A \otimes |\phi\rangle_B \in \mathcal{H} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$, where $\otimes$ is the *tensor product* . Tensor product can also extend a joint quantum system to include n subsystems. If one of the subsystems, say $\mathcal{H}_A$, is lost from $|\varphi\rangle_{AB}$, the residue quantum state returns to

$$|\phi\rangle\langle\phi|_B = \mathrm{Tr}_A\, |\varphi\rangle\langle\varphi|. \tag{23}$$

What is interesting in quantum mechanics is that there exist pure quantum states in $\mathcal{H}$ that cannot be decomposed into tensor product of two pure states in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. A most notable example is the Bell state

$$|\Phi_+\rangle_{AB} := \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B). \tag{24}$$

Such a state is called an *entangled* state, a quantum state that contains *entanglement*.

States that we described above are known as pure states. A quantum state can also be randomly prepared: with probability p_i, the state $|\psi_i\rangle$ is prepared. For example, we can have an apparatus that at 95% of times prepares the "correct" state $|11\rangle$, in 2% of cases an error occurs and we prepare $|10\rangle$, with 2% chance we prepare $|01\rangle$ and 1% a major error leads to preparation of $|00\rangle$. The resulting state can be described as a probability distribution over the basis. Note that this is strictly different from a superposition over the states. Formally, an outcome of a probabilistic state preparation is an *ensemble* $\mathcal{E} : \{p_i, |\psi_i\rangle\}$ can be denoted by a density operator

$$\sigma := \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{25}$$

where $|\psi_i\rangle$ are individual states that could be prepared and p_i are the corresponding probabilities. We refer to objects σ as density matrices. A density matrix is the most general description of quantum states. It generalizes the concept of a pure state, if ρ is pure, it can be written as a projector on the corresponding pure state $|\psi\rangle$

$$\sigma_\psi = |\psi\rangle\langle\psi|. \tag{26}$$

Exercise 4. *There are three necessary and sufficient criteria that a matrix corresponds to a valid description to a quantum state. Show that* (25) *satisfies all three of them*

1. *ρ is Hermitian* [1]

[1] A hermitian matrix A satisfies $A^\dagger = A$.

2. *ρ is positive semi-definite* [2]

3. *Tr*$[\rho] = 1$.

The density matrix representation of a quantum state is considered to be the most general form in the following sense. If the ensemble only contains one entry, namely, $\sigma_{\mathcal{E}} \equiv |\psi_0\rangle\langle\psi_0|$ is of rank one, we say that the quantum state is *pure*. Otherwise, it is *mixed*.

Exercise 5. *For a density operator* $\sigma \in \mathcal{D}(\mathcal{H})$, *show that* $\operatorname{Tr}\sigma^2 \leq 1$ *with equality if and only if* σ *is pure.*

The density matrix representation also incorporates the notion of classical random bit; namely if $\sigma_{\mathcal{E}}$ is diagonal

$$\sigma_{\mathcal{E}} := \begin{pmatrix} p_0 & 0 \\ 0 & p_1 \end{pmatrix}, \tag{27}$$

then this means that the state $\sigma_{\mathcal{E}}$ is prepared in $|0\rangle$ with probability p_0 and in $|1\rangle$ with probability p_1.

Another way of thinking about mixed states is that they are a part of an entangled state. Say that Alice and Bob share an entangled pair $\frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$. We can use partial trace to compute the description of the state that each of them has.

Exercise 6. *Let* $|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$. *Compute* $\operatorname{Tr}_A(|\Phi\rangle\langle\Phi|_{AB})$ *and* $\operatorname{Tr}_B(|\Phi\rangle\langle\Phi|_{AB})$.

For an entangled state, if its partial system is lost, then it will decay into a mixed state. Consider

Let us return to the scenario of a quantum ensemble $\mathcal{E} : \{p_x, |\psi_x\rangle\}_{x\in\mathcal{X}}$. Suppose that the person, say Alice, who prepares this ensemble can keep track of 'which state' she prepared. In other words, she has the additional classical label $|x\rangle\langle x|$ attached to the state $\sigma_x \in \mathcal{D}(\mathcal{H}_B)$, where $\{|x\rangle\}$ forms an orthonormal basis of $\mathcal{H}_X$. Such a hybrid classical-quantum system can be described as

$$\sigma_{XB} = \sum_{x\in\mathcal{X}} p_x |x\rangle\langle x| \otimes |\psi_x\rangle\langle\psi_x|. \tag{28}$$

This is an example of *the Church of the Larger Hilbert Space*. Forgetting (or lost) the classical information will result in

$$\sigma_B = \operatorname{Tr}_X \sigma_{XB} = \sum_{x\in\mathcal{X}} p_x |\psi_x\rangle\langle\psi_x|,$$

given in Eq. (25).

Consider a general mixed state $\sigma_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, we say σ_{AB} is *separable* if

$$\sigma_{AB} = \sum_i p_i \sigma_A^i \otimes \sigma_B^i \tag{29}$$

where $\sum_i p_i = 1$. In other words, σ_{AB} is *separable* if it can be written as convex combination of product states.

[2] Eigenvalues of a positive semi-definitive matrix are real and larger or equal than 0.

3 Quantum Operations

The time evolution of a close quantum system is modelled by a unitary U; namely,

$$|\psi\rangle \to U|\psi\rangle. \tag{30}$$

For a general quantum state described by a density matrix (30) takes form

$$\rho \to U\rho U^\dagger = \sum_i U|\psi_i\rangle\langle\psi_i|U^\dagger. \tag{31}$$

The unitary evolution can be viewed as solving the Schrodinger equation

$$i\hbar\frac{d}{dt}|\psi\rangle = H|\psi\rangle \tag{32}$$

where $\hbar$ is the Planck constant and H is the system *Hamiltonian.* Eigenvalues of Hamiltonian define the allowed energies of a system.

Exercise 7. *Define purity of a quantum state as* $\mathrm{Tr}[\rho^2]$*. Show that unitary operations preserve purity, i.e. a pure state never gets mapped onto a mixed state and vice versa.*

Purity can be used as test of entanglement test if the larger state is pure. If the larger state is not entangled, the purity of both subsystems will be 1, otherwise the state was entangled.

References