Quantum Information & Computation

Adam Kelly

January 26, 2021

This set of notes is a work-in-progress account of the course 'Quantum Information & Computation', originally lectured by Prof Richard Jozsa in Lent 2020 at Cambridge. These notes are not a direct transcription of the lectures, but they do roughly follow what was lectured (in content and in structure).

These notes are likely to be more succinct than other lecture notes of mine, and I have left out various aspects of what was taught. If you spot any errors in this set of notes, I can be contacted at ak2316@cam.ac.uk.

1 Principles of Quantum Mechanics

1.1 Dirac Notation

Let V be a finite dimensional complex vector space with a (hermitian) inner product. In Dirac notation, we write vectors as $|v\rangle$ called *ket vectors*.

We will often work with two dimensional space V_2 with a chosen orthonormal basis $\{|0\rangle, |1\rangle\}$, labelled by bit values.

By convention, kets are always written as column vectors in components. For example,

$$|v\rangle = a\,|0\rangle + b\,|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \qquad a, b \in \mathbb{C}.$$

The *conjugate transpose* of $|v\rangle$ is a *bra vector*, written in mirror image notation,

$$\langle v| = |v\rangle^\dagger = a^*\,\langle 0| + b^*\,\langle 1| = \begin{pmatrix} a^* & b^* \end{pmatrix},$$

and bras are always written as row vectors in components.

More formally, bra vectors $\langle v|$ is an element of the duel vector space V^* of V under the canonical isomorphism $V \cong V^*$, given by the inner product. That is, $\langle v|$ is a linear map $|w\rangle \mapsto$ the inner product of $|v\rangle$ with $|w\rangle$. Note that this inner product is linear in $|w\rangle$ and antilinear in $|v\rangle$ (linear in $\langle v|$).

If $|w\rangle = c\,|0\rangle + d\,|1\rangle$, then the inner product of $|v\rangle$ with $|w\rangle$ is written by juxtaposing the bra and ket,

$$\langle v|w\rangle = |v\rangle^\dagger\,|w\rangle = \begin{pmatrix} a^* & b^* \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = a^*c + b^*d.$$

For example, the orthonormality of basis vectors can be written as $\langle i|j\rangle = \delta_{ij}$.

1.2 Tensor Products of Vectors

For some vector space V of dimension m on a basis $|e_1\rangle, \ldots, |e_m\rangle$, and another vector space V of dimension n on a basis $|f_1\rangle, \ldots, |f_n\rangle$, the *tensor product space* $V \otimes W$ has dimension mn with orthonormal basis $\{|e_i\rangle \otimes |f_j\rangle\}$, $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$, where $\otimes$ is bilinear. Then a general ket vector in $V \otimes W$ is

$$|v\rangle = \sum c_{ij} |e_i\rangle \otimes |f_j\rangle .$$

There is a natural *bilinear* map $f : V \times W \to V \otimes W$. If $|\alpha\rangle = \sum a_i |e_i\rangle$ and $|\beta\rangle = \sum b_j |f_j\rangle$, then

$$\begin{aligned}(|\alpha\rangle, |\beta\rangle) \mapsto f \mapsto |a\rangle \otimes |b\rangle \\ &= \left(\sum a_i |e_i\rangle\right) \otimes \left(\sum b_j |f_j\rangle\right) \\ &= \sum_{ij} a_i b_j |e_i\rangle \otimes |f_j\rangle .\end{aligned}$$

Note that $\otimes$ is not commutative. For example, if $V = W$ then $|\alpha\rangle \, otimes \, |\beta\rangle \neq |\beta\rangle \otimes |\alpha\rangle$ in general. We will often omit the symbol $\otimes$ and will write $|\alpha\rangle \otimes |\beta\rangle$ as $|\alpha\rangle \, |\beta\rangle$.

The mapping f is *not surjective*. With this in mind, we introduce the notions of *product* and *entangled* vectors.

Definition 1.1 (Product and Entangled)**.** Any $|\xi\rangle \in V \otimes W$ of the form $|\xi\rangle = |\alpha\rangle \otimes |\beta\rangle$ is called a *product vector*. Any $|\xi\rangle$ that is *not* a product vector is called *entangled*.

We will mostly be concerned with tensor products of the 2 dimensional V_2 with itself (possible many times over). For the k-fold tensor power, we write $\bigotimes^k V_2 = V_2 \otimes \cdots \otimes V_2$. This has dimension 2^k and orthonormal basis

$$|i_1\rangle \otimes \cdots \otimes |i_k\rangle , \qquad i_1, \ldots, i_k \in \{0, 1\}.$$

These basis vectors are labelled by 2^k k-bitstrings. We will often write $|i_1\rangle \otimes \cdots |i_k\rangle$ as $|i_1\rangle \cdots |i_k\rangle$ or $|i_1 \ldots i_k\rangle$.

Example 1.2. The vector $|v\rangle = |00\rangle + |11\rangle$ in $V_2 \otimes V_2$ is *entangled*. To see this, suppose we could write $|v\rangle$ as a product:

$$\begin{aligned}|v\rangle &= (a |0\rangle + b |1\rangle) \otimes (c |0\rangle + d |1\rangle) \\ &= ac |00\rangle + ad |01\rangle + bc |10\rangle + bd |11\rangle .\end{aligned}$$

Comparing with the coefficients of $|v\rangle$, we get $ad = 1$, $ad = 0$, $bc = 0$ and $ad = 1$. But then $abcd = (ac)(bd) = 1$ and $abcd = (ad)(bc) = 0$, which is a contradiction. Thus $|v\rangle$ must be entangled.

We can show that

$$|v\rangle = a_{00} |00\rangle + a_{01} |01\rangle + a_{10} |10\rangle + a_{11} |11\rangle$$

is entangled if and only if $\det(a_{ij}) \neq 0$. For general dimensions,

$$\sum_{i=1,j=1}^{m,n} A_{ij} |i\rangle |j\rangle$$

is a product vector if and only if the matrix $[A_{ij}]$ has rank 1.

The inner product on $V \otimes W$ is induced the inner products on V and W, 'applied slotwise'. For product states $|\alpha_1\rangle |\beta_2\rangle$ and $|\alpha_2\rangle |\beta_2\rangle$, the inner product is

$$(\langle b_1| \langle \alpha_1|)(|\alpha_2\rangle |\beta_2\rangle) = \langle \alpha_1|\alpha_2\rangle \langle \beta_1|\beta_2\rangle ,$$

and we extend by linearity to all $|\xi\rangle \in V \otimes W$.

Remark (Notation)**.** For the bra vector of $|\alpha\rangle |\beta\rangle$, we often reverse the order and write is as $\langle\beta| \langle\alpha|$. It is always important to keep track of component slots. We sometimes include explicit labels (for example, $|\alpha\rangle_A |\beta\rangle_B$ has bra vector ${}_A\langle\alpha|_B |\beta\rangle = {}_B|\beta\rangle {}_A|\alpha\rangle$).

1.3 Quantum Principles

We will now state some axioms that describe quantum mechanics.

Axiom (QM1 – Physical States)**.** The state of any (isolated) physical system S are represented by unit vectors in a complex vector space V with a given inner product.

The simplest nontrivial case is $V = V_2$, the two dimensional complex vector space. We choose a pair of orthonormal vectors $|0\rangle$ and $|1\rangle$. Then a general state is

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle , \qquad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1.$$

We say $|\psi\rangle$ is a *superposition* of $|0\rangle$ and $|1\rangle$ with *amplitudes* α and β respectively.

Definition 1.3 (Qubit)**.** A *qubit* is any quantum system with a two dimensional state space and a chosen orthonormal basis labelled $|0\rangle$, $|1\rangle$ called the *computational* basis, *standard* basis or Z-basis.

Definition 1.4 (Conjugate Basis for a Qubit)**.** Given an orthonormal pair $|0\rangle$ and $|1\rangle$, we get the orthonormal pair

$$|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) , |-\rangle \qquad = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) .$$

We call this the *conjugate* basis or X-basis.

Axiom (QM2 – Composite Systems)**.** If system S_1 has state space V_1 and system S_2 has state space V_2 then the joint system S_1S_2, obtained by taking S_1 and S_2 together, has state space $V_1 \otimes V_2$.

Comparing this axiom with the classical analog, the corresponding statement has a Cartesian product rather than a tensor product. So giving a state for a classical S_1S_2 is just giving a state for S_1 and giving a state for S_2. Thus the dimension of the system grows linearly with the number of systems, whereas in the quantum sense (with this axiom), the composite system grows *exponentially* with the number of systems.

Example 1.5 (n-qubit system)**.** An n-qubit system has as state space $V_2^{\otimes n}$, with dimension 2^n. It has the computational basis $|i_1 \dots i_n\rangle$, labelled by all 2^n n-bit string.

An n qubit state $|\psi\rangle$ is a *product state* if is the tensor product of n single qubit states $|\psi\rangle = |v_1\rangle |v_2\rangle \cdots |v_n\rangle$, otherwise it is *entangled*.

Before we state the next axiom, we need to introduce how to work with linear maps in Dirac notation.

Consider linear maps on V_2 (higher-dimensions are similar) with $|v\rangle = a|0\rangle + b|1\rangle$ and $|w\rangle = c|0\rangle + d|1\rangle$. Then the 'ket-bra' product is

$$M = |v\rangle\langle w| = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} c^* & d^* \end{pmatrix} = \begin{pmatrix} ac^* & ad^* \\ bc^* & bd^* \end{pmatrix},$$

which is a linear map on V_2. For any $|x\rangle = (x_0, x_1)^T$, we have

$$M|x\rangle = (|v\rangle\langle w|)|x\rangle = |v\rangle \langle w|x\rangle .$$

These are all rank 1 mappings, and thus is not the most general linear map.

For a general linear map say

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix},$$

we note that for basis states,

$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad |1\rangle\langle 0| = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

and we can see that these are a basis for $2x2$ matrices, and we can express

$$A = a_{00}|0\rangle\langle 0| + a_{01}|0\rangle\langle 1| + a_{10}|1\rangle\langle 0| + a_{11}|1\rangle\langle 1| = \sum a_{ij}|i\rangle\langle j| .$$

Another useful property comes from the cycic property of the trace:

$$\langle v|w\rangle = \mathrm{tr}(|v\rangle\langle w|).$$

An important operation comes from the above when $|v\rangle = |w\rangle$ (in any dimension), and where $|v\rangle$ is normalized so $\langle v|v\rangle = 1$. Then $\Pi_v = |v\rangle\langle u|$ is the operation of projection onto the 1-dimensional subspace spanned by $|v\rangle$. For example, we have

$$\Pi_v \Pi_v = |v\rangle \langle v|v\rangle = |v\rangle\langle v| = \Pi_v.$$

More generally if E is any d-dimensional linear subspace of n-dimensional space V and $\{|e_1\rangle, \dots, |e_d\rangle\}$ is any orthonormal basis of E, then $\Pi_E = |e_1\rangle\langle e_1| + \cdots + |e_d\rangle\langle e_d|$ is the operation of projection on to E. Π_E is independent of the orthonormal basis chosen.

We also want to have tensor products of maps. If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{and} \quad B = \begin{pmatrix} p & q \\ v & s \end{pmatrix}$$

are linear maps on V_2 then $A \otimes B : V_2 \otimes V_2 \to V_2 \otimes V_2$ defined by the basis action

$$|i\rangle |j\rangle \longmapsto (A|i\rangle)(B|j\rangle),$$

with linear extension.

For example, for any product sate $|v\rangle |w\rangle$, we have $(A \otimes B)|v\rangle |w\rangle = (A|v\rangle)(B|w\rangle)$.

In components for the 2×2 case we have

$$A \otimes B = \begin{pmatrix} aB & bB \\ cB & dB \end{pmatrix} = \left(\begin{array}{cc|c} ap & aq & bB \\ av & as & \\ \hline & cB & dB \end{array}\right),$$

with other cases done similarily.

Some important special cases are $I \otimes A$ and $A \otimes I$, the action of A on the second (or first) component space of $V_2 \otimes V_2$. We often refer to these as *local operations* on subsystems of composite systems.

Axiom (QM3 – Physical Evolution of Quantum Systems)**.** Any physical (finite time) evolution of a quantum system is represented by a *unitary* linear operation on the vector space of states.

The analog to this from the Quantum Mechanics course would be Schrödinger's equation and specifically is the finite dimensional version of Schrödinger's equation, where instead of a hamiltonian we have a hermitian operation on the state space, where evolution is

$$\frac{\mathrm{d}|\psi\rangle}{\mathrm{d}t} = H|\psi\rangle$$

If H is time independent, then $|\psi\rangle = e^{-\frac{i}{\hbar}Ht}|\psi_0\rangle$, which is the matrix exponential. This also implies that A hermitian gives e^{iA} unitary.

Recall that a matrix U is unitary if $U^{-1} = U^\dagger$, that is, if and only if U maps any orthonormal basis to an orthonormal set of vectors, which occurs if and only if the columns or rows of the matrix of U form an orthonormal set of vectors.

The last piece of notation we will introduce is the partial inner products. For vectors in $V \otimes W$, then any ket $|v\rangle \in V$ defines a linear map $V \otimes W \to W$ called the 'partial inner product with $|v\rangle$', defined on basis vectors $|e_i\rangle |f_j\rangle \in V \otimes W$ where $|e_i\rangle |f_j\rangle \mapsto \langle v|e_i\rangle |f_j\rangle$, and similarity for $|w\rangle \in W$ giving a map $V \otimes W \to V$). If $V = W$ (as often occurs), it is important to specify which space of $V \otimes V$ is being used.

Example 1.6. For $V = V_2$, and $|\xi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \in V \otimes V$, we can form the partial inner product with $|0\rangle$ on *either* space. So first label the spaces as $V_A \otimes V_B$ where $V_A = V_B = V$. Then the orthonormality relations $\langle i|j\rangle = \delta_{ij}$ gives

$$\begin{aligned} {}_A\langle 0|\xi\rangle_{AB} &= a_A \langle 0|0\rangle_A |0\rangle_B + b_A \langle 0|0\rangle_A |1\rangle_B + c_A \langle 0|1\rangle_A |0\rangle_B + d_A \langle 0|1\rangle_A |1\rangle_B \\ &= a|0\rangle_B + b|1\rangle_B . \end{aligned}$$

That is, we pick out the terms of $|\xi\rangle_{AB}$ with a zero in the A slot.

Axiom (QM4 – Quantum Measurements & Born Rule)**.** We will come back to this.