QUANTUM INFORMATION & COMPUTATION

Nilanjana Datta, DAMTP Cambridge

1 Postulates of Quantum Mechanics:

Our description of quantum mechanics below may at first sight look a little different from standard textbook presentations but in fact it's equivalent. Here we focus on quantum mechanics of physical systems with *finite* dimensional state spaces (multi-qubit systems, cf below) and unitary matrices representing finite time evolutions, whereas quantum physics textbooks traditionally begin with the infinite dimensional case viz. wavefunctions, and Schrödinger's wave equation giving infinitesimal time evolution via a Hamiltonian. We will also emphasize the quantum measurement formalism, which will be of crucial significance for us.

(QM1) Postulate 1: Quantum states *To any isolated physical (quantum-mechanical) system S there is associated a* Hilbert space*, i.e. a* complex, inner product space $\mathcal{V}$*, called the* state space *of the system. The physical state of the system S is completely described by its* state vector*, which is a* unit *vector*[1] *in the system's state space.*$\square$

Remark 1: Global and Relative Phase of state vectors

Consider two states $|\Psi\rangle$ and $|\Phi\rangle$, where $|\Psi\rangle$ is given by (1) and $|\Phi\rangle = e^{i\theta}|\Psi\rangle$, θ being a real constant. These two states differ by the factor $e^{i\theta}$, of unit modulus, which is referred to as a *global phase factor*. These states describe the same physical state of a system. This is because there are no measurements which can be used to distinguish between such states. Consequently, the state of a physical system is given by a *ray* in a Hilbert space, the latter being an equivalence class of unit vectors that differ by a global phase factor. If $|\phi\rangle \in \mathcal{V}$, then the ray is $\{e^{i\theta}|\phi\rangle : \theta \in \mathbb{R}\}$. Note, however, that the relative phase factor between two states is of physical significance, i.e., the states $a|\Psi\rangle + b|\Phi\rangle$ and $a|\Psi\rangle + be^{i\theta}|\Phi\rangle$ do *not* represent the same physical state of the system.

By slight abuse of terminology we will often say that "a system has state space $\mathcal{V}$ (of some dimension d)" when its states are the unit vectors in the vector space $\mathcal{V}$.

Superposition Principle
If $|\psi\rangle, |\phi\rangle \in \mathcal{V}$, then any state which is a superposition of these states, i.e., any state of the form

$$|\Psi\rangle = a|\psi\rangle + b|\phi\rangle, \tag{1}$$

(where the *amplitudes* $a, b \in \mathbb{C}$), also belongs to $\mathcal{V}$. This is referred to as the *Superposition Principle.*

[1] More precisely, a *ray*; see **Remark 1**.

The simplest non-trivial quantum system has a 2-dimensional vector space, $\mathcal{V} = \mathbb{C}^2$. Choosing a pair of orthonormal vectors and labelling them $|0\rangle$ and $|1\rangle$, the general state can be written $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. We say that $|\psi\rangle$ is a *superposition* of states $|0\rangle$ and $|1\rangle$ with *amplitudes* a and b.

Qubits: any quantum system, with a 2-dimensional state space $\mathbb{C}^2$ and a chosen orthonormal basis (which we write, for example, as $\{|0\rangle, |1\rangle\}$) is called a *qubit*. The basis states $|0\rangle, |1\rangle$ are called *computational basis states or standard basis states*. They will be used to represent the two corresponding classical bit values as qubit states, and then general qubit states can be thought of as superpositions of the classical bit values There are many real physical systems that can embody the structure of a qubit, for example the spin of an electron, the polarisation of a photon, superpositions of two selected energy levels in an atom etc.

Example. For a single qubit, the orthonormal states $|0\rangle$ and $|1\rangle$ give a quantum representation of the classical bit values 0 and 1. Another pair of orthonormal states that we will frequently encounter in applications is the following pair, labelled by plus and minus signs:

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

They are "equally weighted superpositions" in the sense that the squared amplitudes of 0 and 1 are equal in each state. The basis $\{|+\rangle, |-\rangle\}$ is called the *conjugate basis* (and the states themselves are called the *conjugate basis states*).

(QM2) Postulate 2: Composite systems *The state space of a composite physical system is the tensor product of the state spaces of its component systems. Hence, if system S_1 had state space $\mathcal{V}$ and system S_2 has state space $\mathcal{W}$ then the joint (or composite)system obtained by taking S_1 and S_2 together, has states given by arbitrary unit vectors in the* tensor product *space $\mathcal{V} \otimes \mathcal{W}$. In other words, the state space of the composite system S_1S_2 is $\mathcal{V} \otimes \mathcal{W}$.* □

Product states and entangled states of n qubits: A system comprising n qubits thus has state space $(\mathbb{C}^2)^{\otimes n}$ of dimension 2^n. An n-qubit state $|\psi\rangle$ is a called a *product state* if it is the product of n single-qubit states $|\psi\rangle = |v_1\rangle\,|v_2\rangle \ldots |v_n\rangle$ and $|\psi\rangle$ is called *entangled* if it is not a product state.

As mentioned previously, the *computational basis* or *standard basis* for n qubits is given by the tensor products of $|0\rangle$'s and $|1\rangle$'s in each slot, giving the 2^n orthonormal vectors $|i_1\rangle\,|i_2\rangle \ldots |i_n\rangle$ where each $i_1, \ldots i_n$ is 0 or 1. Thus the basis vectors are labelled by n-bit strings and we often write $|i_1\rangle\,|i_2\rangle \ldots |i_n\rangle$ simply as $|i_1 i_2 \ldots i_n\rangle$.

We note the significant fact that as the number of qubits grows *linearly*, the full state description (given as the full list of amplitudes) grows *exponentially* in its complexity. However the description of any product state grows only linearly with n (each successive $|v_i\rangle$ is described by two further amplitudes) so this exponential complexity of state description is intimately related to the phenomenon of entanglement that arises for tensor products of spaces. With this in mind, it is especially interesting to contrast (QM2) with its classical counterpart – for *classical* physics, the state space of a composite system is

the *Cartesian* product of the state spaces of its constituent parts. Thus if a classical system S requires K parameters for its state description then a composite of n such systems will require only nK parameters i.e. a linear growth of description, in contrast to the exponential growth for quantum systems.

1.1 Linear operators/maps: Dirac notation

Observables

Another key concept of Quantum Mechanics is that of observables. An observable is a property of the physical system which can be measured (at least in principle). Mathematically an observable is a linear, self-adjoint (or Hermitian) operator. A linear operator A acting on a Hilbert space $\mathcal{V}$ is a map:

$$A : |\psi\rangle \to A|\psi\rangle \ ; \ \ A(a|\psi\rangle + b|\phi\rangle) = aA|\psi\rangle + bA|\phi\rangle, \quad \text{for} \quad |\psi\rangle, |\phi\rangle \in \mathcal{V},\, a, b \in \mathbb{C}.$$

For an operator A acting on a Hilbert space $\mathcal{V}$ there exists a unique linear operator $A^\dagger$ acting on $\mathcal{V}$ such that

$$\langle v|Aw\rangle = \langle A^\dagger v|w\rangle.$$

The operator $A^\dagger$ is the adjoint of A. A linear operator A is represented by a matrix. Its adjoint $A^\dagger$ is represented by the transpose of the complex conjugate of this matrix. An operator A is a self-adjoint (or Hermitian) operator if $A = A^\dagger$. From the definition of the adjoint it is easy to see that $(AB)^\dagger = B^\dagger A^\dagger$. By convention, if $|\psi\rangle$ is a vector in the Hilbert space on which the operator $\mathbf{A}$ acts, then we define

$$|\psi\rangle^\dagger = \langle\psi|.$$

Hence,

$$(A|\psi\rangle)^\dagger = \langle\psi|A^\dagger.$$

There are four observables acting in the single qubit space, which are of particular significance in Quantum Information Theory. These are represented by the following 2×2 matrices:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Here σ_0 is the 2×2 identity matrix and σ_x, σ_y and σ_z are the Pauli matrices. The action of these operators on the basis vectors $|0\rangle$ and $|1\rangle$ of the single qubit space are:

$$\begin{aligned} \sigma_0|0\rangle &= |0\rangle \quad ; \quad \sigma_0|1\rangle = |1\rangle \\ \sigma_x|0\rangle &= |1\rangle \quad ; \quad \sigma_x|1\rangle = |0\rangle \\ \sigma_y|0\rangle &= i|1\rangle \quad ; \quad \sigma_y|1\rangle = -i|0\rangle \\ \sigma_z|0\rangle &= |0\rangle \quad ; \quad \sigma_z|1\rangle = -|1\rangle \end{aligned} \tag{2}$$

The Pauli matrices satisfy the following relations:

$$\sigma_x\sigma_y = i\sigma_z\,;\ \sigma_y\sigma_z = i\sigma_x\,;\ \sigma_z\sigma_x = i\sigma_y\,;$$

Heuristically, the action of the Pauli matrices on the state of a qubit can be interpreted as follows

σ_x : a bit flip ; σ_z : a phase flip ; $\sigma_y(= i\sigma_x\sigma_z)$: a combined (bit and phase) flip.

Dirac notation for linear maps/operators:

To illustrate the Dirac notation for linear maps, we will consider the case of linear maps on $\mathbb{C}^2$ and its tensor powers. With $|v\rangle = a\,|0\rangle + b\,|1\rangle$ and $|w\rangle = c\,|0\rangle + d\,|1\rangle$ in $\mathbb{C}^2$, standard matrix multiplication for the outer product gives

$$M = |v\rangle\,\langle w| = \begin{pmatrix} a \\ b \end{pmatrix} (c^*\ d^*) = \begin{pmatrix} ac^* & ad^* \\ bc^* & bd^* \end{pmatrix} \tag{3}$$

which is a linear map on $\mathcal{V} \equiv \mathbb{C}^2$ (acting by matrix multiplication on column vectors). In fact for any $|x\rangle \in \mathbb{C}^2$ we have $M\,|x\rangle = (|v\rangle\,\langle w|)\,|x\rangle = |v\rangle\,\langle w|x\rangle$, i.e. the vector $|v\rangle$ multiplied by scalar $\langle w|x\rangle$. Such outer products do not give all linear maps from $\mathbb{C}^2$ to $\mathbb{C}^2$ but only rank 1 mapping, and the kernel of the linear map M is the subspace of vectors orthogonal to $|w\rangle$).

Note that

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

so if $A : \mathbb{C}^2 \to \mathbb{C}^2$ is any linear map with matrix representation

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then we can write

$$A = a\,|0\rangle\langle 0| + b\,|0\rangle\langle 1| + c\,|1\rangle\langle 0| + d\,|1\rangle\langle 1|\,.$$

More formally, this just expresses the fact that $\{|0\rangle\langle 0|\,, |0\rangle\langle 1|\,, |1\rangle\langle 0|\,, |1\rangle\langle 1|\}$ is a basis for the vector space $\mathcal{V} \otimes \mathcal{V}^*$ of linear maps on $\mathcal{V} \equiv \mathbb{C}^2$.

Not also from eqn. (3) the calculational fact that an inner product can be expressed as a trace (of the corresponding outer product):

$$\langle w|v\rangle = \mathrm{Tr}\ |v\rangle\,\langle w|\,.$$

Projection operators

An important special case of eq. (3) is when $|v\rangle = |w\rangle$ and $|v\rangle$ is normalised (i.e. $\langle v|v\rangle = 1$). Then $\Pi_v = |v\rangle\,\langle v|$ is the operator of *projection onto* $|v\rangle$, satisfying $\Pi_v\Pi_v = \Pi_v$. The latter property can be seen very neatly in Dirac notation: $\Pi_v\Pi_v = (|v\rangle\,\langle v|)(|v\rangle\,\langle v|) =$

$|v\rangle\langle v|v\rangle\langle v| = |v\rangle\langle v| = \Pi_v$ as $\langle v|v\rangle = 1$. If $|a\rangle$ is any vector orthogonal to $|v\rangle$ then $\Pi_v|a\rangle = |v\rangle\langle v|a\rangle = 0$. It then easily follows that for any vector $|x\rangle$, $\Pi_v|x\rangle$ is the vector obtained by projection of $|x\rangle$ into the one dimensional subspace spanned by $|v\rangle$. Similarly for any vector space $\mathcal{W}$ (of any dimension), if $|w\rangle$ is any normalised vector in $\mathcal{W}$, then $\Pi_w = |w\rangle\langle w|$ is the linear operation of projection into the one-dimensional subspace spanned by $|w\rangle$.

More generally, if $\mathcal{E}$ is any linear subspace of a vector space $\mathcal{V}$ and $\{|e_1\rangle, \ldots, |e_d\rangle\}$ is any orthonormal basis of $\mathcal{E}$ (which thus has dimension d), then $\Pi_{\mathcal{E}} = |e_1\rangle\langle e_1| + \ldots + |e_d\rangle\langle e_d|$ is the operator of projection into $\mathcal{E}$. This property is easily checked by extending the given basis of $\mathcal{E}$ to a full orthonormal basis of the whole space $\mathcal{V}$. Then by writing any vector $|\psi\rangle$ in $\mathcal{V}$ in terms of this basis we readily see that $\Pi_{\mathcal{E}}|\psi\rangle$ is indeed its projection into $\mathcal{E}$.

Finally a point about notation: if $|x\rangle = A|v\rangle$ then the corresponding bra vector is given by $\langle x| = (A|v\rangle)^\dagger = |v\rangle^\dagger A^\dagger = \langle v|A^\dagger$. This follows from the fact that taking adjoints of matrix products reverses the product order $(MN)^\dagger = N^\dagger M^\dagger$. Thus for example in the inner product construction we can write $\langle a|M|b\rangle$ as $\langle a|x\rangle$ or as $\langle y|b\rangle$ where $|x\rangle = M|b\rangle$ but $|y\rangle = M^\dagger|a\rangle$ (so $\langle y| = \langle a|M$) i.e. the central M in $\langle a|M|b\rangle$ acts as M if viewed as acting to the right, but acts as $M^\dagger$ if viewed as acting to the left i.e. on the ket $|a\rangle$ before it is turned into a bra vector.

Tensor products of maps/operators
If

$$B = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

is a second linear map on $\mathbb{C}^2$ then the tensor product of maps $A \otimes B : \mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$ is defined by its action on the basis $|i\rangle|j\rangle \to A|i\rangle B|j\rangle$ for $i, j \in \{0, 1\}$. Extending this linearly defines $A \otimes B$ on general vectors in $\mathbb{C}^2 \otimes \mathbb{C}^2$. In particular for product vectors we get $(A \otimes B)(|v\rangle|w\rangle) = A|v\rangle \otimes B|w\rangle$.

The 4×4 matrix of components of $A \otimes B$ has a simple block form, as can be seen by writing down its action on basis states in components (giving the columns of the matrix of $A \otimes B$). We get the following pattern (similar to our previous pattern for components of tensor products of vectors):

$$A \otimes B = \begin{pmatrix} aB & bB \\ cB & dB \end{pmatrix} = \begin{pmatrix} ap & aq & bp & bq \\ ar & as & br & bs \\ cp & cq & dp & dq \\ cr & cs & dr & ds \end{pmatrix}.$$

Important special cases of tensor product maps are $A \otimes I$ and $I \otimes A$, being the action of A on the first (resp. second) component space of $\mathbb{C}^2 \otimes \mathbb{C}^2$, leaving the other space "unaffected".

Example: for $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and A as above, we have

$$\begin{aligned} (A \otimes I)|\Phi\rangle &= \tfrac{1}{\sqrt{2}}[A|0\rangle]|0\rangle + (A|1\rangle)|1\rangle = \tfrac{1}{\sqrt{2}}(a|0\rangle + c|1\rangle)|0\rangle + \tfrac{1}{\sqrt{2}}(b|0\rangle + d|1\rangle)|1\rangle \\ &= \tfrac{1}{\sqrt{2}}(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle). \end{aligned}$$

On the other hand $(I \otimes A)\,|\Phi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle\,(A\,|0\rangle) + \frac{1}{2}\,|1\rangle\,(A\,|1\rangle)$ giving $\frac{1}{\sqrt{2}}(a\,|00\rangle + c\,|01\rangle + b\,|10\rangle + d\,|11\rangle)$, which is different. $\square$

1.2 Postulate (QM3): physical evolution of quantum systems

Any physical (finite time) evolution of an closed (isolated) quantum system is represented by a unitary *operation on the corresponding vector space of states.* $\square$

The evolution of an isolated (closed) quantum system is described by a unitary transformation. If a system is in a state $|\psi(t_1)\rangle$ at time t_1 and a state $|\psi(t_2)\rangle$ at a later time t_2, then

$$|\psi(t_2)\rangle = U(t_1, t_2)|\psi(t_1)\rangle,$$

where $U(t_1, t_2)$ is a unitary operator which depends only on t_1 and t_2. More precisely, the time evolution of a state vector is governed by the *Schrödinger equation*:

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle,$$

where H is a self-adjoint operator, called the *Hamiltonian*, which generates the unitary transformation ($\hbar$ is a constant called the Planck's constant). In particular, for a time-independent Hamiltonian, we have

$$U(t_1, t_2) = e^{-\frac{i}{\hbar}H(t_2 - t_1)}.$$

Note that the unitary evolution of a closed system is *deterministic*. Given an initial state $|\psi(0)\rangle$, the theory predicts the state $|\psi(t)\rangle$ at all later times t.

Unitary Operators:

Recall that a linear operator U on any vector space is unitary if its matrix has $U^{-1} = U^\dagger$ (where dagger is conjugate transpose). We have the following equivalent characterisations (useful for recognising unitary operations). U is unitary:
if and only if U maps an orthonormal basis to an orthonormal set of vectors;
if and only if the columns (or rows) of the matrix of U form an orthonormal set of vectors.

After the fourth postulate (QM4)) we will introduce a number of particular unitary operators on one and two qubits that will be frequently used.

Dirac notation: partial inner products for vectors in $\mathcal{V} \otimes \mathcal{W}$

For expressing our final quantum postulate (QM4) it will be useful to introduce a 'partial inner product' operation on tensor product spaces. Any ket $|v\rangle \in \mathcal{V}$ defines a linear map $\mathcal{V} \otimes \mathcal{W} \to \mathcal{W}$ which we call "*partial inner product* with $|v\rangle$". It is defined on the basis $\{|e_i\rangle\,|f_j\rangle\}$ of $\mathcal{V} \otimes \mathcal{W}$ by the formula $|e_i\rangle\,|f_j\rangle \to \langle v|e_i\rangle\,|f_j\rangle \in \mathcal{W}$, and on general vectors in $\mathcal{V} \otimes \mathcal{W}$ by linear extension of its basis action. Similarly for any $|w\rangle \in \mathcal{W}$ we get a partial

inner product mapping $\mathcal{V} \otimes \mathcal{W}$ to $\mathcal{V}$. If $\mathcal{V}$ and $\mathcal{W}$ are instances of the same space (e.g. we will often have them both being $\mathbb{C}^{\otimes 2}$) then it is important to specify (e.g. with a subscript label on the kets) which of the two spaces is supporting the bra-ket construction of the inner product.

Example. For $|v\rangle \in \mathcal{V}$ and $|\xi\rangle \in \mathcal{V} \otimes \mathcal{V}$ we can form the partial inner product on the first or second space. To make the position explicit we will introduce subscripts to label the slots, writing $\mathcal{V} \otimes \mathcal{V}$ as $\mathcal{V}_1 \otimes \mathcal{V}_2$, and writing ${}_1\langle v|\xi\rangle_{12} \in V_2$ for partial inner product on the first slot, and ${}_2\langle v|\xi\rangle_{12} \in \mathcal{V}_2$ for partial inner product on the second slot.
Thus for example, if $\mathcal{V} = \mathbb{C}^2$ and $|\xi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$ then the orthonormality relations $\langle i|j\rangle = \delta_{ij}$ give ${}_1\langle 0|\xi\rangle_{12} = a\,|0\rangle + b\,|1\rangle$ and ${}_2\langle 0|\xi\rangle_{12} = a\,|0\rangle + c\,|1\rangle$ i.e. we just pick out the terms of $|\xi\rangle$ that contain 0 in the first, respectively second, slot. $\square$

The partial inner product operation is in fact just the familiar operation of contraction of tensor indices (with a complex conjugation). In index notation (with components always relative to an orthonormal product basis), if $|\xi\rangle \in \mathcal{V} \otimes \mathcal{V}$ and $|v\rangle \in \mathcal{V}$, have components ξ_{ij} and v_k respectively then the partial inner products of $|v\rangle$ with $|\xi\rangle$ on the two slots are respectively $v_i^* \xi_{ij}$ and $v_j^* \xi_{ij}$ (with the summation convention applied i.e. repeated indices are summed).