1 Quantum information

From the course by Noah Linden (University of Bristol) and discussion with Thomas Hebdige and David Jennings (Imperial College London). For a comprehensive introduction see for example Nielsen and Chuang (2002) or Wilde (2013).

Quantum mechanics is essentially just linear algebra in a Hilbert space, with a few additional properties. The following definitions are exactly what you would find in a linear algebra course, apart from the notation.

1.1 Dirac notation

Dirac notation is a convenient way of denoting vectors such that it is easy to visually identify inner and outer products, and thus quickly recognise scalars, vectors and matrices:

- $|v\rangle$ denotes a column vector
- $\langle u|v\rangle$ denotes an inner product (resulting in a scalar)
- $|u\rangle\langle v|$ denotes an outer product (resulting in a matrix)

Additionally, $\overline{\alpha}$ denotes the complex conjugate of a scalar α, and $U^\dagger$ denotes the adjoint (conjugate transpose) of an operator U.

1.2 Hilbert space

A *Hilbert space* is a vector space with an inner product $\langle\cdot|\cdot\rangle$ satisfying the following:

- $\langle u|(\alpha|v\rangle + \beta|w\rangle) = \alpha\langle u|v\rangle + \beta\langle u|w\rangle$
- $\langle u|v\rangle = \overline{\langle v|u\rangle}$
- $\langle v|v\rangle \geq 0$ with equality iff $|v\rangle$ is the zero vector.

1.3 Orthonormal bases

An *orthonormal basis* of a Hilbert space $\mathcal{H}$ is a set of vectors $\{v_1, \ldots, v_n\}$ in $\mathcal{H}$ such that:

- $\text{span}(\{v_1, \ldots, v_n\}) = \mathcal{H}$
- $\langle v_i|v_j\rangle = \delta_{ij}$

Restricting to the space $\mathbb{C}^2$, which is all that is needed to understand the quantum Bernoulli factory, we have the *computational basis* $\{|0\rangle, |1\rangle\}$. This is the canonical basis and is henceforth used wherever not specified otherwise. Since it is an orthonormal basis, every vector $|v\rangle$ in $\mathbb{C}^2$ has a unique representation

$$|v\rangle = \alpha|0\rangle + \beta|1\rangle \equiv (\alpha, \beta)^T$$

for some $\alpha, \beta \in \mathbb{C}$. For reasons which will probably not become apparent in this treatment, we will restrict to *normalised* vectors, requiring also $|\alpha|^2 + |\beta|^2 = 1$. We will also consider two vectors equivalent if they differ only by an overall phase, i.e. $|u\rangle \equiv |v\rangle$ if $|u\rangle = e^{i\theta}|v\rangle$ for some θ. This is because it is impossible to distinguish between two such vectors with any measurement.

To ensure coherency with the properties of the inner product, we have that

$$\langle v| = \overline{\alpha}\langle 0| + \overline{\beta}\langle 1|.$$

The inner product of $|u\rangle = u_0|0\rangle + u_1|1\rangle$ with $|v\rangle = v_0|0\rangle + v_1|1\rangle$ is therefore computed as

$$\begin{aligned}\langle u|v\rangle &= (\overline{u_0}\langle 0| + \overline{u_1}\langle 1|)(v_0|0\rangle + v_1|1\rangle) \\ &= \overline{u_0}v_0\langle 0|0\rangle + \overline{u_0}v_1\langle 0|1\rangle + \overline{u_1}v_0\langle 1|0\rangle + \overline{u_1}v_1\langle 1|1\rangle \\ &= \overline{u_0}v_0 + \overline{u_1}v_1.\end{aligned}$$

One alternative choice of orthonormal basis which is worth mentioning is given by $\{|+\rangle, |-\rangle\}$, consisting of the states

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

1.4 Linear operators

A linear operator is an operator with the property

$$A(\alpha|u\rangle + \beta|v\rangle) = \alpha A|u\rangle + \beta A|v\rangle.$$

It is therefore fully defined according to its action on an orthonormal basis. For instance, the quantum NOT operator (denoted X) is defined by

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

Equivalently, X can be expressed as a matrix with respect to the computational basis:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

In Dirac notation, X can be written in terms of outer products of basis states:

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|$$

Then if X acts on the state $|v\rangle = \alpha|0\rangle + \beta|1\rangle$, we have

$$\begin{aligned} X|v\rangle &= (|0\rangle\langle 1| + |1\rangle\langle 0|)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha|0\rangle\langle 1|0\rangle + \alpha|1\rangle\langle 0|0\rangle + \beta|0\rangle\langle 1|1\rangle + \beta|1\rangle\langle 0|1\rangle \\ &= \alpha|1\rangle + \beta|0\rangle \end{aligned}$$

as desired.

- A linear operator U is said to be *self-adjoint* (or *hermitian*) if $U^\dagger = U$
- A linear operator U is said to be *unitary* if $UU^\dagger = U^\dagger U = I$

For example, the operator X is self-adjoint and unitary.

1.5 Rules of Quantum Mechanics

1. *States* of a quantum mechanical system correspond to normalised vectors in Hilbert space, up to an overall phase.
2. *Evolutions* of the system correspond to unitary operators.
3. *Measurements* on quantum states correspond to self-adjoint operators — see below.

1.5.1 Spectral theorem and measurement

The outcome of a measurement depends on the state of the system and the type of measurement performed. The spectral theorem states that every self-adjoint operator A can be represented by its spectral decomposition

$$A = \sum_i \lambda_i P_i \tag{1}$$

where $\{\lambda_1, \ldots, \lambda_k\}$ is the set of *distinct* eigenvalues of A, and P_i is the projection operator onto the eigenspace corresponding to eigenvalue λ_i.

When we measure a state $|x\rangle$ using operator A, the measurement outcome we observe is one of the eigenvalues of A. In particular, we observe λ_i with probability $\langle x|P_i|x\rangle$. Making a measurement causes the system to collapse into the eigenstate corresponding to the observed eigenvalue; that is, the state after measurement is proportional to $P_i|x\rangle$.

To give a concrete example, let us consider again the operator X. This operator has eigenvalues ± 1 corresponding to eigenvectors (known as *eigenstates* in quantum mechanics) $|+\rangle$ and $|-\rangle$ respectively. Therefore X admits the diagonal representation

$$X = |+\rangle\langle +| - |-\rangle\langle -|$$

which is of the form (1). Now suppose we make a measurement on the state $|v\rangle = |0\rangle$, using X. The outcome of the measurement will be an eigenvalue of X: either $+1$ or -1. We observe the outcome $+1$ with probability

$$\langle v|P_{+1}|v\rangle = \langle 0|+\rangle \langle +|0\rangle = 1/2$$

in which case the state after measurement is

$$P_{+1}|v\rangle = |+\rangle\langle +|0\rangle \propto |+\rangle.$$

Alternatively, with probability $1/2$ we observe the outcome -1 and the state after measurement is $|-\rangle$. In this example, the two outcomes are equally likely because the state is 'equidistant' from the two eigenstates of X. In general, outcomes that leave the state after measurement closer to the original state are more likely. We will see what is meant by distance between states in Section [REF].

1.6 Quantum randomness

It is worth remarking at this point on the difference between quantum and classical randomness. As statisticians we are used to dealing with randomness, but we accept that randomness is always part of a model, and is not purported to exist in nature. We artificially introduce random variables into our models to account for a lack of information, either about the state of the system or about the (presumably deterministic) processes that govern certain phenomena.

On the contrary, our uncertainty about the outcome of a measurement on a quantum system is of a different kind. This uncertainty is not a symptom of our lack of knowledge: even when we know exactly the state of the system, as in the example above [REF], we are still unable to predict with certainty the outcome of a measurement on the system. The randomness here is intrinsic; it really does exist in nature.

1.7 The Bloch sphere

References

Nielsen, M. A. and Chuang, I. (2002), *Quantum computation and quantum information*, AAPT.

Wilde, M. M. (2013), *Quantum information theory*, Cambridge University Press.