1 Quantum information

From the course by Noah Linden (Bristol) and discussion with Thomas Hebdige and David Jennings (Imperial). 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.

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:

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

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 $|\alpha|^2 + |\beta|^2 = 1$. 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

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

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.

References

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

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