C2: Quantum information basics

Rob Smith

Lecture 5

6 Two qubits and beyond

A system with two qubits $|a\rangle$ and $|b\rangle$ can be described by four orthonormal basis states (e.g. $|0_a0_b\rangle$, $|0_a1_b\rangle$, $|1_a0_b\rangle$ and $|1_a1_b\rangle$); we thus have a 4-dimension Hilbert space. For 3 qubits this rises to 8-dimensional and in general for n–qubits we have a 2^n dimensional Hilbert space, it is this exponential increase in the size of the Hilbert space that gives quantum computers their potential power.

6.1 Product states

A product state is any state that can be written as a direct product of (in this context) single–qubit states. Such a state is *separable.* Any states which are not separable are said to be *entangled.* The basis states mentioned above are examples of product states, e.g. $|1_a0_b\rangle = |1_a\rangle \otimes |0_b\rangle$. As you would expect these two–qubit states can be acted on by single–qubit gates, so, for example, a Hadamard gate acting on qubit $|b\rangle$ would give

$$|00\rangle = |0\rangle \otimes |0\rangle \xrightarrow{\mathrm{H}_b} |0\rangle \otimes |+\rangle = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle). \tag{32}$$

Here $\mathrm{H}_b = \mathbb{1} \otimes \mathrm{H}$ (i.e. we apply the identity to qubit $|a\rangle$ and a Hadamard to qubit $|b\rangle$) whereas $\mathrm{H}_a = \mathrm{H} \otimes \mathbb{1}$. Performing a Hadamard on both qubits, which is known as a bilateral operation, would be written as $\mathrm{H} \otimes \mathrm{H}$ or $\mathrm{H}^{\otimes 2}$; note this is equivalent to H_a followed by H_b or vice-versa.

6.1.1 Direct products

In matrix form the direct product is given by:

$$\begin{pmatrix}\alpha_a\\ \beta_a\end{pmatrix} \otimes \begin{pmatrix}\alpha_b\\ \beta_b\end{pmatrix} = \begin{pmatrix}\alpha_a\begin{pmatrix}\alpha_b\\ \beta_b\end{pmatrix}\\ \beta_a\begin{pmatrix}\alpha_b\\ \beta_b\end{pmatrix}\end{pmatrix} = \begin{pmatrix}\alpha_a\alpha_b\\ \alpha_a\beta_b\\ \beta_a\alpha_b\\ \beta_a\beta_b\end{pmatrix}. \tag{33}$$

So

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \quad |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}. \tag{34}$$

The same approach applies to operators, for example:

$$\mathrm{H}_b = \mathbb{1} \otimes \mathrm{H} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{pmatrix}. \tag{35}$$

6.2 Two–qubit gates

The gate $H^{\otimes 2}$ is an example of a two–qubit gate, but much more interesting two–qubit gates are those that can't be written as a direct product of single–qubit gates (which as we have already said are equivalent to a sequence of single–qubit gates). An important example of a two–qubit gate is the controlled–NOT (cNOT or cX) gate which either performs a NOT operation or an identity operation on one of the qubits depending on the state of the other qubit (which remains unchanged). In matrix form we have

$$\mathrm{c}_a\mathrm{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \mathrm{c}_b\mathrm{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{36}$$

where the $_{a,b}$ tell you which qubit is the control qubit. Other two–qubit gates include controlled–Z gate and the controlled–phase gate:

$$\mathrm{c}_a\mathrm{Z} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \mathrm{c}_a\Phi = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{37}$$

6.2.1 Complete gate set

The cNOT gate together with the single qubit H and T gates are universal for quantum computing – any operation can be built from a network of these gates.

6.3 Entangled states

Performing H_a and then $\mathrm{c}_a\mathrm{X}$ on the state $|00\rangle$ gives the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The state $|\psi\rangle$ is an *entangled* state; it is inseparable – it cannot be written as a direct product of two single–qubit states. We have to take the two–qubit state as a whole. Consider measuring qubit $|a\rangle$ – we have an equal chance of getting $|0\rangle$ or $|1\rangle$, but if we get $|1\rangle$ then we will *always also* get $|1\rangle$ if we subsequently measure $|b\rangle$. The fate of the two qubits are completely intertwined.

There are an infinite number of possible entangled states but four important ones are the Bell states which are maximally entangled. They are:

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle) \pm |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ \pm 1 \end{pmatrix}, \tag{38}$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle) \pm |10\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ \pm 1 \\ 0 \end{pmatrix}. \tag{39}$$

Note that these states form an alternative orthonormal basis. So, just as a superposition of product states can be entangled, a superposition of entangled states can be separable.