PH441

Quantum computation and Quantum cryptography

Lecture 02

We have already learnt that,

A qubit – a quantum bit – is the fundamental unit of quantum information.

This week we are going to learn about it in more details. But before going over to Qubits, let us have a look at classical bits!

classical bits

A classical bit, cbits has two states 0 and 1.

Let us denote them by the symbols

$$|0\rangle \,, \quad |1\rangle$$

To do nontrivial computation one requires more than one cbit. It is convenient to represent the four states of two cbits as four orthogonal vectors in four dimensions, formed by the tensor products of two such pairs:

$$|0\rangle \otimes |0\rangle \,, \quad |0\rangle \otimes |1\rangle \,, \quad |1\rangle \otimes |0\rangle \,, \quad |1\rangle \otimes |1\rangle$$

or $\quad |0\rangle|0\rangle \,, \quad |0\rangle|1\rangle \,, \quad |1\rangle|0\rangle \,, \quad |1\rangle|1\rangle$

or more readably

$$|00\rangle \,, \quad |01\rangle \,, \quad |10\rangle \,, \quad |11\rangle$$

or most compactly of all, using the decimal representation of the 2-bit number represented by the pair of Cbits,

$$|0\rangle_2 \, , \quad |1\rangle_2 \quad |2\rangle_2 \, , \quad |3\rangle_2$$

The subscript 2 is needed. Because in going from binary to decimal, we lose the information of how many Cbits the vector describes, making it necessary to indicate in some other way whether $|3\rangle$ means $|11\rangle = |3\rangle_2$ or $|011\rangle = |3\rangle_3$ or $|0011\rangle = |3\rangle_4$ etc.

Clearly, one represents the states of n Cbits as the 2^n orthonormal vectors in 2^n dimensions

$$|x\rangle_n \, , \quad 0 \leq x < 2^n$$

given by the n-fold tensor products of n mutual orthogonal pairs of orthogonal 2 vectors

For example,

$$|19\rangle_6 = |010011\rangle = |0\rangle|1\rangle|0\rangle|0\rangle|1\rangle|1\rangle$$
$$= |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle$$

The power of tensor product is evident if we represent each cbit as column vectors as follows:

$$|0\rangle \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The corresponding column vectors for Tensor products are:

$$\begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} \longleftrightarrow \begin{pmatrix} y_0 z_0 \\ y_0 z_1 \\ y_1 z_0 \\ y_1 z_1 \end{pmatrix}$$

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} \longleftrightarrow \begin{pmatrix} x_0 y_0 z_0 \\ x_0 y_0 z_1 \\ x_0 y_1 z_0 \\ x_0 y_1 z_1 \\ x_1 y_0 z_0 \\ x_1 y_0 z_1 \\ x_1 y_1 z_0 \\ x_1 y_1 z_1 \end{pmatrix}$$

etc.

Thus, for example, the 8-dimensional column vector representing $|5\rangle_3$ is given by

$$|5\rangle_3 = |101\rangle = |1\rangle|0\rangle|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$= \begin{array}{c c} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} & \begin{matrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{matrix} \end{array}$$

which has a 0 in every entry except for a 1 in the entry labelled by the integer 5 that the three cbits represent.

This general rule for the column vector representing $|x\rangle_n$, 1 in position x and 0 everywhere else is the obvious generalization to n cbits of the form for a 1-cbit column vector.

Quantum bits

The general state of a single Qubit (Qbit) is a superposition of two classical-basis states

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where the amplitudes α and β are complex numbers constrained only by the normalization condition

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

The general state of n Qubits has the form

$$|\psi\rangle = \sum_{0 \le x < 2^n} \alpha_x |x\rangle_n \rightarrow (1)^*$$

with complex amplitudes constrained only by the normalization condition

$$\sum_{0 \le x < 2^n} |\alpha_x|^2 = 1 \rightarrow (2)$$

Let us now look at the most profound differences between Cbits and Qbits!

---

* Example 2 Qbit system

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

The most general possible state of two cbits has the form

$$|\psi\rangle = |x_1\rangle\,|x_0\rangle$$

This can be described as a state in which cbit # 1 has the state $|x_1\rangle$ and cbit # 0, the state $|x_0\rangle$: each individual cbit has a state of its own.

On the other hand, the most general state of two Qbits has the form

$$|\psi\rangle = \alpha_0\,|0\rangle_2 + \alpha_1\,|1\rangle_2 + \alpha_2\,|2\rangle_2 + \alpha_3\,|3\rangle_2$$

$$\cancel{= \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle}$$

$$\cancel{\equiv \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle}$$

$$= \alpha_3\,|1\rangle|1\rangle + \alpha_2\,|1\rangle|0\rangle + \alpha_1\,|0\rangle|1\rangle + \alpha_0\,|0\rangle|0\rangle \rightarrow (a)$$

If each Qbit had a state of its own, this 2-Qbit state would be the Tensor product of two 1 Qbit states. The 2-Qbit state would thus have the general form

$$|\psi\rangle\,|\phi\rangle = (\alpha\,|1\rangle + \beta\,|0\rangle)(\gamma\,|1\rangle + \delta\,|0\rangle)$$

$$= \alpha\gamma\,|1\rangle|1\rangle + \alpha\delta\,|1\rangle|0\rangle + \beta\gamma\,|0\rangle|1\rangle + \beta\delta\,|0\rangle|0\rangle$$

$\rightarrow (b)$

But the state $|\psi\rangle$ in (a) cannot have this form unless $\alpha_3\,\alpha_0 = \alpha_2\,\alpha_1$!

So, in a general multi-qubit state each individual

Qbit has no state of its own. This is the first major way in which Qbits differ from Cbits.

States of n Qbits in which no subset of fewer than n have states of their own are ~~catted~~ called entangled.

Generic n-Qubits are entangled. The amplitudes in the expansion (1) have to satisfy special constraints for the state to be a tensor product of states associated with fewer than n Qbits.