Quantum Computation & Cryptography Workshop

The basics

States

A general qubit:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

Where a and b are the *amplitudes* for the states $|0\rangle$ and $|1\rangle$ we have:

$$\langle\psi\,|\,\psi\rangle = \|\psi\|^2 = |a|^2 + |b|^2 = 1$$

The qubit is in a *superposition* of the states $|0\rangle$ and $|1\rangle$. These states form a *basis* for the space of single qubits. The basis is *orthonormal* so:

$$\langle 0\,|\,0\rangle = \langle 1\,|\,1\rangle = 1$$

$$\langle 1\,|\,0\rangle = \langle 0\,|\,1\rangle = 0$$

We can also have another basis, given by the states:

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

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

Can also be represented as a vector, i.e.:

$$|\psi\rangle \leftrightarrow \begin{pmatrix} a \\ b \end{pmatrix}$$

And it's *adjoint* is:

$$\langle\psi| \leftrightarrow \begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix}$$

Where $\bar{a}$ and $\bar{b}$ are the *complex conjugates* of a and b. Adjoint $\leftrightarrow$ transpose + complex conjugate.
Then $\langle\psi\,|\,\psi\rangle$ which is the *inner product*, can be viewed as multiplying a column vector with a line vector:

$$\begin{pmatrix} \bar{a} & \bar{b} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2 + |b|^2 = 1$$

2-qubit states look like this:

$$|\chi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$$

If we have two qubits:

$$|\psi_1\rangle = a_1\,|0\rangle + b_1\,|1\rangle \quad |\psi_2\rangle = a_2\,|0\rangle + b_2\,|1\rangle$$

If we put them together, we have a 2-qubit state. This state is described by:

$$|\psi_1\rangle \otimes |\psi_2\rangle = (a_1\,|0\rangle + b_1\,|1\rangle) \otimes (a_2\,|0\rangle + b_2\,|1\rangle) == a_1a_2\,|00\rangle + a_1b_2\,|01\rangle + b_1a_2\,|10\rangle + b_1b_2\,|11\rangle$$

In general, an N-qubit state is a *superposition* of 2^N basis states.
It is true for any 2 states $|\psi_1\rangle$ and $|\psi_2\rangle$ that:

$$\langle\psi_1\,|\,\psi_2\rangle = \overline{\langle\psi_2\,|\,\psi_1\rangle}$$

So:

$$\langle\psi_1\,|\,\psi_2\rangle\,\langle\psi_2\,|\,\psi_1\rangle = |\,\langle\psi_2\,|\,\psi_1\rangle\,|^2 = |\,\langle\psi_1\,|\,\psi_2\rangle\,|^2$$

Unitary operators

Unitary means $UU^\dagger = U^\dagger U = I$. Where $U^\dagger$, the adjoint of U, can be thought of as the *transpose conjugate* of U. Just like $\langle\psi|$ is the adjoint of $|\psi\rangle$. The main unitaries we encounter are:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

and

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$X\,|0\rangle = |1\rangle \quad X\,|1\rangle = |0\rangle \quad X\,|+\rangle = |+\rangle \quad X\,|-\rangle = -\,|-\rangle$$

$$Z\,|0\rangle = |0\rangle \quad Z\,|1\rangle = -\,|1\rangle \quad Z\,|+\rangle = |-\rangle \quad Z\,|-\rangle = |+\rangle$$

$$H\,|0\rangle = |+\rangle \quad H\,|1\rangle = |-\rangle \quad H\,|+\rangle = |0\rangle \quad H\,|-\rangle = |1\rangle$$

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

All of these operators are their own inverses. I.e.

$$XX = YY = ZZ = HH = I$$

$$CNOT\;CNOT = I$$

Remember that unitaries act *linearly* on states. I.e., if we have:

$$|\psi\rangle = a_1 |\psi_1\rangle + a_2 |\psi_2\rangle + ... + a_N |\psi_N\rangle$$

And we act on this state with a unitary U, then we have:

$$U |\psi\rangle = U(a_1 |\psi_1\rangle + a_2 |\psi_2\rangle + ... + a_N |\psi_N\rangle)$$

By linearity, we have:

$$U |\psi\rangle = a_1 U |\psi_1\rangle + a_2 U |\psi_2\rangle + ... + a_N U |\psi_N\rangle$$

Since, in general, we express a state in a particular basis we only need to know the action of the unitary on the basis states. From there, using linearity we can compute the action of the unitary on any general state. What is the adjoint of $U |\psi\rangle$? It's none other than $\langle\psi| U^\dagger$:

$$\langle\psi| U^\dagger = \overline{a_1} \langle\psi_1| U^\dagger + \overline{a_N} \langle\psi_N| U^\dagger + ... + \overline{a_N} \langle\psi_N| U^\dagger$$

Measurement

Measurement just means projecting in a basis. The vector to which we project is chosen *randomly*. The probability of a state collapsing to a certain basis state is given by *the mod squared value of its amplitude* (Born's law). I.e., if we have:

$$|\psi\rangle = a |0\rangle + b |1\rangle = \frac{a+b}{\sqrt{2}} |+\rangle + \frac{a-b}{\sqrt{2}} |-\rangle$$

If we measure it in the $(|0\rangle, |1\rangle)$ basis, there is a $|a|^2$ probability of getting $|0\rangle$ and a $|b|^2$ probability of getting a $|1\rangle$. Respectively, if we measure in the $(|+\rangle, |-\rangle)$ basis, there is a $|a+b|^2/2$ probability of getting $|+\rangle$ and a $|a-b|^2/2$ probability of getting $|-\rangle$.

To project a vector we have a mathematical object called *projector* which does this for us. If our basis is $(|0\rangle, |1\rangle)$ the projectors are $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$.

In general, when we have a state $|\psi\rangle$ and we perform a measurement with N possible outcomes, we have a set of projectors P_1 up to P_N. The probability of getting a particular outcome is given by:

$$p(i) = \langle\psi | P_i | \psi\rangle$$

And if we get outcome i, then the state after measurement is:

$$\frac{P_i |\psi\rangle}{\sqrt{\langle\psi | P_i | \psi\rangle}} = \frac{P_i |\psi\rangle}{\sqrt{p(i)}}$$

If you want to measure one qubit out of a multi-qubit state, then the projector for the multi-qubit state takes the projector on the qubit we measure and tensors it with identity on the other qubits. For example, if we have the state:

$$|\chi\rangle = a |00\rangle + b |01\rangle + c |10\rangle + d |11\rangle$$

And we measure the first qubit in the $(|+\rangle, |-\rangle)$ basis, we have the projectors $|+\rangle\langle+| \otimes I$ and $|-\rangle\langle-| \otimes I$. So the probability of getting the first outcome (i.e., the qubit being in $|+\rangle$ post-measurement) is:

$$p(+) = \langle\psi|\,(|+\rangle\langle+| \otimes I)\,|\psi\rangle = \langle\psi|\,(a(|+\rangle\langle+|\otimes I)\,|00\rangle + b(|+\rangle\langle+|\otimes I)\,|01\rangle + c(|+\rangle\langle+|\otimes I)\,|10\rangle + d(|+\rangle\langle+|\otimes I)\,|11\rangle)$$

And now we act with the projector on the first qubit, and leave the second qubit unchanged. Note that:

$$\langle+\,|\,0\rangle = \langle+\,|\,1\rangle = \frac{1}{\sqrt{2}}$$

So:

$$p(+) = \frac{1}{\sqrt{2}}\langle\psi|\,(a\,|+\rangle\,|0\rangle + b\,|+\rangle\,|1\rangle + c\,|+\rangle\,|0\rangle + d\,|+\rangle\,|1\rangle)$$

Expressing $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ we get:

$$\begin{aligned} p(+) &= \frac{1}{2}\langle\psi|\,(a\,|00\rangle + a\,|10\rangle + b\,|01\rangle + b\,|11\rangle + c\,|00\rangle + c\,|10\rangle + d\,|01\rangle + d\,|11\rangle) \\ &= \frac{1}{2}\langle\psi|\,((a+c)\,|00\rangle + (b+d)\,|01\rangle + (a+c)\,|10\rangle + (b+d)\,|11\rangle) \end{aligned}$$

So:

$$p(+) = \frac{1}{2}\langle\psi|\,((a+c)\,|00\rangle + (b+d)\,|01\rangle + (a+c)\,|10\rangle + (b+d)\,|11\rangle)$$

Note that:

$$\langle\psi\,|\,00\rangle = \bar{a} \quad \langle\psi\,|\,01\rangle = \bar{b} \quad \langle\psi\,|\,10\rangle = \bar{c} \quad \langle\psi\,|\,11\rangle = \bar{d}$$

So:

$$p(+) = \frac{1}{2}(\bar{a}(a+c) + \bar{b}(b+d) + \bar{c}(a+c) + \bar{d}(b+d))$$

$$p(+) = \frac{1}{2}(|a|^2 + |b|^2 + |c|^2 + |d|^2 + \bar{a}c + \bar{b}d + \bar{c}a + \bar{d}b) = \frac{1}{2}(1 + \bar{a}c + \bar{b}d + \bar{c}a + \bar{d}b)$$

The state after measurement is:

$$\frac{(|+\rangle\langle+| \otimes I)\,|\psi\rangle}{\sqrt{p(+)}} = \frac{1}{\sqrt{p(+)}}((a+c)\,|00\rangle + (b+d)\,|01\rangle + (a+c)\,|10\rangle + (b+d)\,|11\rangle)$$

By grouping terms after the second qubit, we get:

$$\frac{1}{\sqrt{p(+)}}(((a+c)\,|0\rangle + (a+c)\,|1\rangle) \otimes |0\rangle + ((b+d)\,|0\rangle + (b+d)\,|1\rangle) \otimes |1\rangle)$$

But $|0\rangle + |1\rangle = \sqrt{2}\,|+\rangle$, which makes sense since we projected the first qubit to $|+\rangle$, so we have:

$$\frac{\sqrt{2}}{\sqrt{p(+)}}((a+c)\,|+\rangle\,|0\rangle + (b+d)\,|+\rangle\,|1\rangle) = \frac{\sqrt{2}}{\sqrt{p(+)}}\,|+\rangle \otimes ((a+c)\,|0\rangle + (b+d)\,|1\rangle)$$

We can see that the first qubit is $|+\rangle$, as expected, while the second is in a superposition state.