Introduction to Quantum Computing

Lectures by Leon Riesebos

Steven Oud
soud@pm.me

February 24, 2019

Contents

1 Fundementals: A One-Qubit World

Quantum computers are machines that rely on characteristically quantum phenomena, such as quantum interference and quantum entanglement, in order to perform computation.

— *Artur Ekert*

It is tempting to say that a quantum computer is one whose operation is governed by the laws of quantum mechanics. But since the laws of quantum mechanics govern the behavior of all physical phenomena, this temptation must be resisted. Your laptop operates under the laws of quantum mechanics, but it is not a quantum computer.

— *N. David Mermin*

1.1 The Qubit

A qubit - like a classical bit - has a *state*. In classical bits, this is 0 or 1. Two possible states for a qubit are $|0\rangle$ and $|1\rangle$ (called *Dirac notation*), which correspond to the states 0 and 1 for a classical bit. The difference between bits and qubits is that a qubit can be in other states than $|0\rangle$ or $|1\rangle$, often called *superpositions*. The state of a qubit can be denoted as following:

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

where α and β are complex numbers. The special states $|0\rangle$ and $|1\rangle$ are known as *computational basis states*. We cannot examine a qubit to determine its quantum state. Quantum mechanics tells us we can only acquire much more restricted information about the quantum state. When we measure a qubit we get either 0, with probability $|\alpha|^2$, or 1, with probability $|\beta|^2$. The sum of all probabilities is always equal to 1:

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

For example, a qubit in the state

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

gives 0 fifty percent of the time ($|1/\sqrt{2}|^2$), and 1 fifty percent of the time. This state is often denoted by $|+\rangle$.

1.2 Bloch Sphere

The Bloch sphere is a geometrical representation of a qubit's state. It's a spherical coordinate system in which a quantum state can be described as following:

$$|\psi\rangle = e^{i\delta}\left(cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle\right)$$

where δ, θ and ϕ are real numbers. We can ignore the factor $e^{i\delta}$ out the front, because it has no observable effect, allowing us to write

$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle$$

The numbers θ and ϕ define a point on the three-dimensional sphere (Figure 1). The Bloch sphere visualization can be very useful for describing single qubit operations. It is however limited in that there is no simple generalization of the Bloch sphere known for multiple qubits.

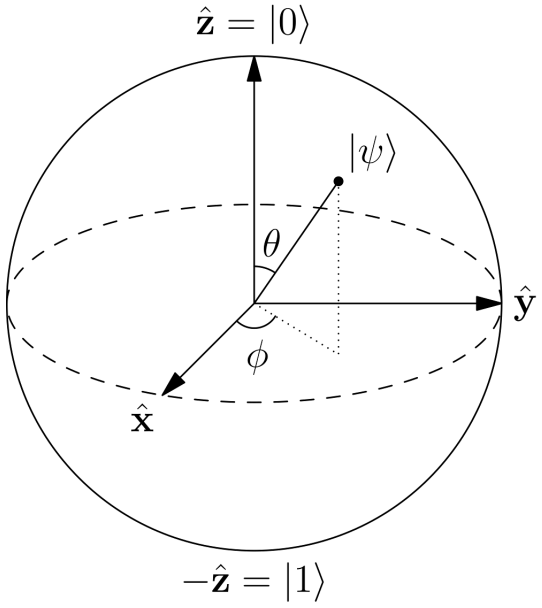


Figure 1: Bloch sphere representation of a qubit.

1.3 Single-Qubit Quantum Operations

Single-qubit quantum gates can be seen as rotations on the Bloch sphere. Quantum gates can be represented by matrices, which we will look at in Section 1.5. These gates only have one limitation: they have to be *unitary*, that is $U^\dagger U = I$, where $U^\dagger$ is the Hermitian adjoint of U. Therefore, any $2^n \times 2^n$ unitary matrix is a valid gate which acts on n qubits. Below are some notable single-qubit gates described and visualized.

1.3.1 Pauli Gates

The most simple quantum gates are the *Pauli* gates I, X, Y and Z. I is the identity gate, which does nothing. The other gates rotate π radians (180 degrees) around the X, Y or Z-axis. These gates are self-inverse, meaning $U^2 = I$.

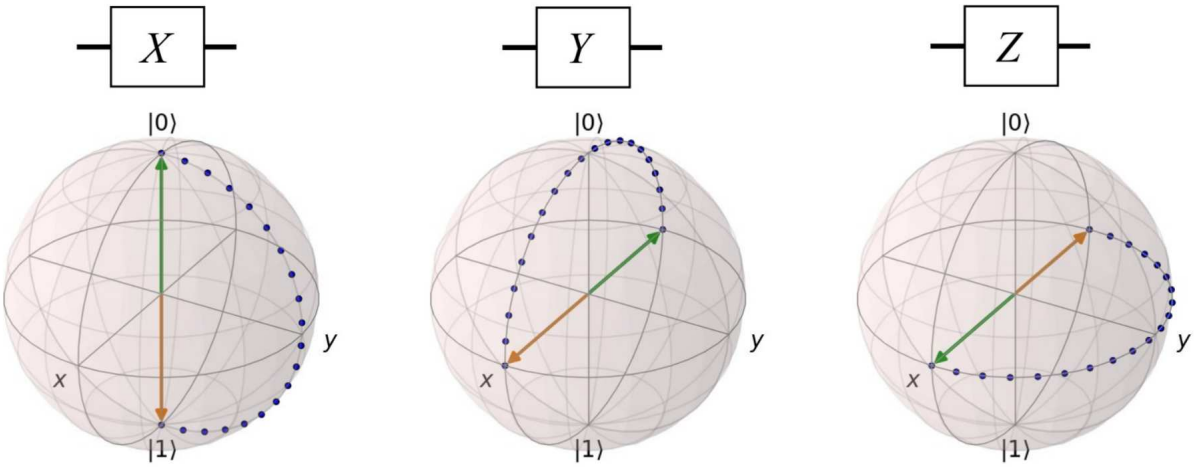
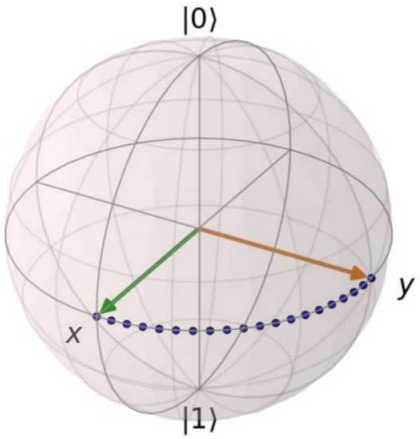


Figure 2: Pauli gates X, Y and Z visualized on the Bloch sphere.

1.3.2 S Gate

The S gate, also known as the phase (P) gate, does a Z rotation of $\pi/2$ radians (90 degrees). It's essentially half a Pauli Z gate. The S gate belongs to the Clifford gates.



1.3.3 Hadamard Gate

The Hadamard (H) gate maps the qubit-basis states $|0\rangle$ and $|1\rangle$ to superposition states with equal weight. It is the combination of two rotations, π radians about the Z-axis followed by $\pi/2$ radians about the Y-axis.

This gate is sometimes described as a "square root of NOT" gate, because it turns $|0\rangle$ into $(|0\rangle + |1\rangle)/\sqrt{2}$ (also written as $|+\rangle$), halfway between $|0\rangle$ and $|1\rangle$. The Hadamard gate also belongs to the Clifford gates.

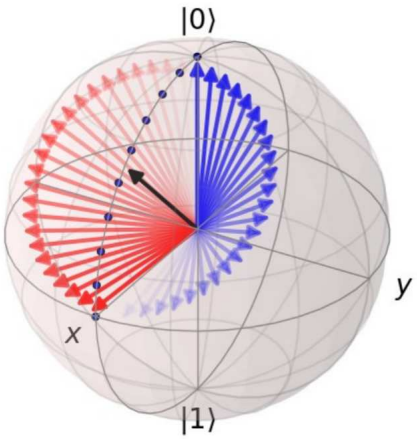


Figure 3: Hadamard gate visualized on the Bloch sphere.

1.4 Measurement

Measuring a qubit collapses its state. The probabilistic result of a qubit measurement can be calculated based on the probability amplitudes:

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

$$P(|0\rangle) = |\alpha|^2$$

$$P(|1\rangle) = |\beta|^2$$

Consider the following simple single-qubit circuit:

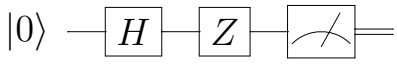


Figure 4: A simple quantum circuit. The output of measuring a qubit is a classical bit, which is distinguished from a qubit by drawing a double-line wire. A visualization of this circuit on the Bloch sphere can be seen in Figure 5.

We start with computing $H\,|0\rangle = |+\rangle$, followed by $Z\,|+\rangle = |-\rangle$. Finally we measure. We can calculate the probabilities:

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

$$P(|0\rangle) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

$$P(|1\rangle) = \left|\frac{-1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Giving us equal probabilities of our state being measured as $|0\rangle$ or $|1\rangle$.

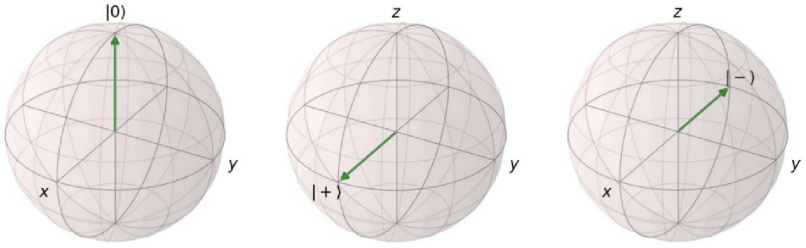


Figure 5: States of our qubit throughout the circuit from left to right: $|0\rangle \rightarrow H\,|0\rangle \rightarrow ZH\,|0\rangle$.

1.5 Vector Notation

Earlier we showed that we can represent a quantum state using the following formula:

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

The quantum states $|\psi\rangle$, $|0\rangle$ and $|1\rangle$ in the formula above are vectors. We define $|0\rangle$ and $|1\rangle$ as following:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

A quantum state has to be a normalized vector since we are talking probabilities, where $|\alpha|^2 + |\beta|^2 = 1$. In general, a qubit's state is a unit vector in a two-dimensional complex vector space. A state can be written out as a linear combination:

$$|\psi\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

The single-qubit gates can then be represented by 2×2 unitary matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Then a computation like $X\,|0\rangle$ can be calculated by matrix vector multiplication:

$$X\,|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

And we find that $X\,|0\rangle = |1\rangle$. Or, more general:

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

You can combine quantum gates by multiplying their matrices. For example, let's verify that H is self-inverse by applying it to itself:

$$H^2 = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = I$$

The result is the identity gate, showing that the inverse of H is indeed itself. It is also a *Hermitian matrix*, because it is equal to its own Hermitian adjoint: $H = H^\dagger$.

2 Fundementals: A Multi-Qubit World

2.1 The Step to Multi-Qubit

We can represent multiple qubits using the *Kronecker product*:

$$|ab\rangle = |a\rangle \otimes |b\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

To represent $|00\rangle$ for example:

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\begin{bmatrix}1\\0\end{bmatrix}\\0\begin{bmatrix}1\\0\end{bmatrix}\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

Note that the size of the vector of two qubits is twice as big as the vector for one qubit. This is where some of the power of quantum computers comes from. With n qubits you can represent 2^n states at the same time - an exponential growth from classical bits.

For multi-qubit states the rule remains that the state vector has to be normalized. For two qubits for example: $\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle = 1$. Or, more general, for a n qubit state:

$$\sum_{i}^{2^n} |\alpha_i|^2 = 1$$

2.2 Quantum State Evolution

Doing single-qubit operations on a multi-qubit state is possible by combining the identity and our single-qubit gate. Say we want to compute $H_1\,|0_0 0_1\rangle$. That is, put the second qubit through a Hadamard gate.[1] To do so, the gate matrix's column width has to be equal to the quantum state vector's dimension. We can achieve this by taking the Kronecker product of the identity matrix and our single-qubit matrix (in this case H):

$$H_1\,|0_0 0_1\rangle = (I_0 \otimes H_1)\,|0_0 0_1\rangle$$

[1] Note that when I say "second" qubit, I'm talking about the most right, or least significant qubit. I will number them for this example but assume it from here on out.

Writing it out:

$$I_0 \otimes H_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1}$$

$$= \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) \tag{2}$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \tag{3}$$

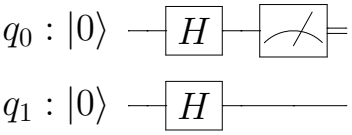
Then we can put our $|00\rangle$ state through it:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

Which can also be written in Dirac notation as $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$.

2.3 Partial Measurement

Say we want to measure the first qubit, q_0, in the following circuit:



First, we put both qubits in our state $|00\rangle$ through a Hadamard gate. This puts it in the following state:

$$(H \otimes H)\,|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

When we measure q_0 we have a 50/50 probability of getting a 0 or 1. We get either of the following states based on $M(q_0)$:

$$|\psi\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|\underline{0}0\rangle + |\underline{0}1\rangle) \text{ if } M(q_0) = 0 \\ \frac{1}{\sqrt{2}}(|\underline{1}0\rangle + |\underline{1}1\rangle) \text{ if } M(q_0) = 1 \end{cases}$$

We have two possible states after measurement, a state where q_0 is 0 or a state where q_0 is 1. Qubit q_1 will stay in superposition because we haven't measured that one. Notice how the first qubits (underlined) in both states are the same. This makes sense, we've measured that one so we're sure of its state.

2.4 Common Two-Qubit Gates

2.4.1 CNOT Gate

The quantum gate controlled-NOT ($CNOT$, sometimes called $controlled-X$) is comparable to a classical computer's XOR, but it's reversible. This gate has two input qubits, the *control* qubit and *target* qubit. If the control qubit is set to 0, then the target qubit is left alone. If the control qubit is set to 1, then the target qubit is flipped. The circuit representation for $CNOT$ can be seen in Figure 6. Qubit q_0 represents the control qubit and q_1 represents the target qubit. It's essentially a Pauli X gate with a control qubit. $CNOT$ is Hermitian and belongs to the Clifford gates.

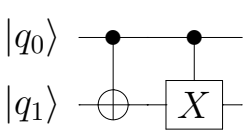
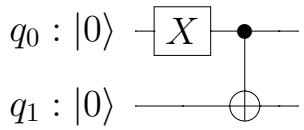


Figure 6: Circuit representations of $CNOT$. We will use the left representation.

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Figure 7: Matrix representation of $CNOT$.

Let's look at an example of a $CNOT$ gate. Consider the following circuit:



First we put q_0 (the control qubit) in the $|1\rangle$ state by applying an X gate, giving us the state $|10\rangle$. Then we apply the $CNOT$ gate:

$$CNOT\,|10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle$$

The target qubit was flipped because the control qubit was set to 1, giving us $|11\rangle$.

2.4.2 CZ Gate

CZ, or the controlled-Z gate, acts in a similar way to other controlled gates. That is, do the operation on the target qubit if the control qubit is set to 1, otherwise do nothing. In CZ the operation is the Pauli Z gate. CZ is also Hermitian and belongs to the Clifford gates.

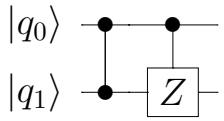


Figure 8: Circuit representations of CZ.

2.4.3 Controlled Gates

Controlled gates act on two or more qubits, where one or more qubits act as control for some operation. Generally, if U is a gate that operates on single qubits with the following matrix representation:

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

then the controlled-U gate is a gate that operates on two qubits where the first qubit serves as control. The general matrix representation of the controlled-U then looks as following:

$$C(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

2.5 Toffoli Gate

We can simulate a classical circuit using a quantum circuit. Most classical gates however are non-reversible. This is a problem for our quantum circuit, as it requires gates to be reversible. We can make use of a reversible gate

known as the *Toffoli gate* to make a quantum equivalent of any classical gate.

The Toffoli gate has three inputs and outputs (Figure 9), where two of the input qubits act as control bits. The third qubit is the target bit which is flipped if both control qubits are set to 1, otherwise it's left alone. For example, applying the Toffoli gate to the state $|110\rangle$ flips the third qubit, resulting in the state $|111\rangle$.

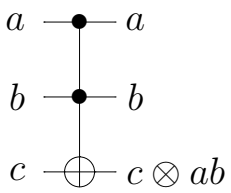


Figure 9: Circuit representation of the Toffoli gate, where $\otimes$ is addition modulo two.

The Toffoli, or controlled-controlled-X (CCX) gate can be represented by a 8×8 matrix:

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

It is a non-Clifford gate.

2.6 Entanglement

Two qubits are entangled if and only if the state of those two qubits can *not be expressed as two individual states* (non-separable). Let's first take a look at a separable, or non-entangled state:

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

This state can be separated and expressed as the following two individual states:

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

However, consider the following state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

This is an entangled state. It cannot be expressed as two individual states. How do we know if a state is entangled? We say two qubits are entangled if they have *nonzero concurrence*. The concurrence of a state can be calculated using the following formula:

$$C(|\psi\rangle) = 2|\alpha_{00}\alpha_{11} - \alpha_{01}\alpha_{10}|$$

We can check if our entangled state is indeed entangled:

$$C\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right) = 2\left|\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\right)\right| = 1$$

It has a non-zero concurrence, so we can say it's entangled. How about our non-entangled state?

$$C\left(\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\right) = 2\left|\frac{1}{2}\left(\frac{1}{2}\right) - \frac{1}{2}\left(\frac{1}{2}\right)\right| = 0$$

A concurrence of 0, so it is indeed not entangled.

2.7 The Bell States

The *Bell states* are four maximally entangled quantum states of two qubits:

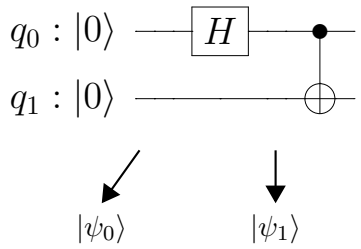
$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

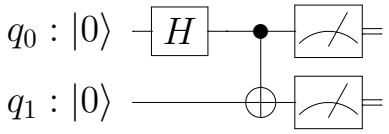
$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

We can create a Bell state with the following circuit:



We start with our state $|00\rangle$ at $|\psi_0\rangle$. We put q_0 through a Hadamard gate, giving us the state $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ at $|\psi_1\rangle$. Finally we $CNOT$ that state giving us the final Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

The significance of Bell states becomes apparent when we start measuring qubits of a Bell state. Take the circuit we used before to create the Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and measure both qubits.



You will find that the measurement results are correlated:

$$M(q_1) = 0 \text{ if } M(q_0) = 0$$

$$M(q_1) = 1 \text{ if } M(q_0) = 1$$

If you measure q_0 to be 0, q_1 will also be 0 and vice versa. Note that in our example entangled state they correlate as being equal, but for the entangled state $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ they correlate as being opposites (measuring q_0 as 0 means q_1 will be 1).