Introduction to Quantum Computing

Lectures by Leon Riesebos

Steven Oud
soud@pm.me

February 13, 2019

Contents

1 Fundementals: A One-Qubit World

1.1 What Is Quantum Computing?

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

1.2 What Is Quantum Computing Not?

"*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

1.3 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 $|+\rangle$.

1.4 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.

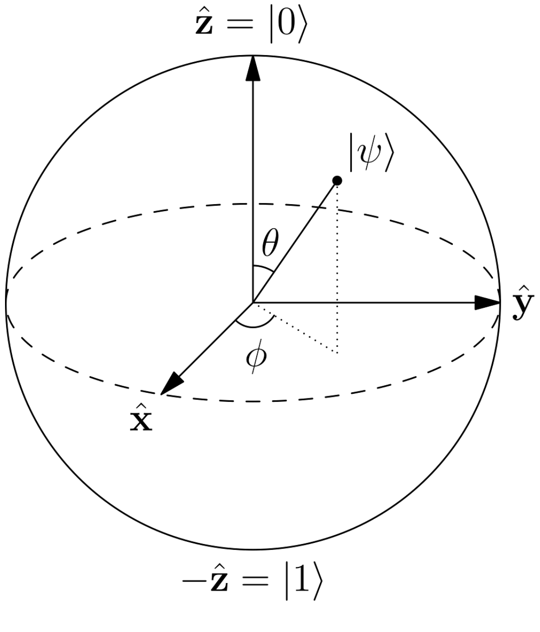


Figure 1: Bloch sphere representation of a qubit.

1.5 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 1.7. These gates only have one limitation: they have to be *unitary*, that is $U^\dagger U = I$, where $U^\dagger$ is the 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.

1.5.1 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 $X = X^\dagger$.

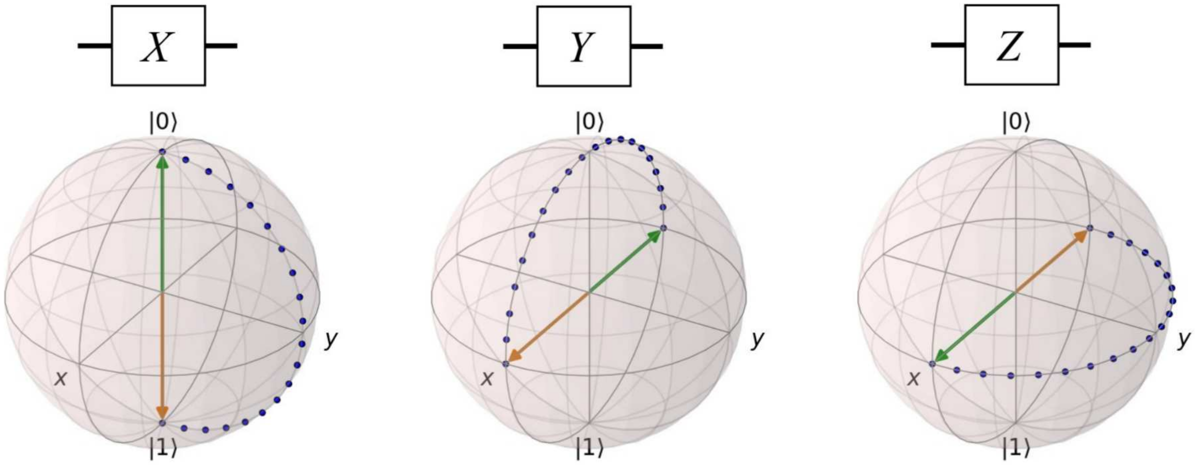
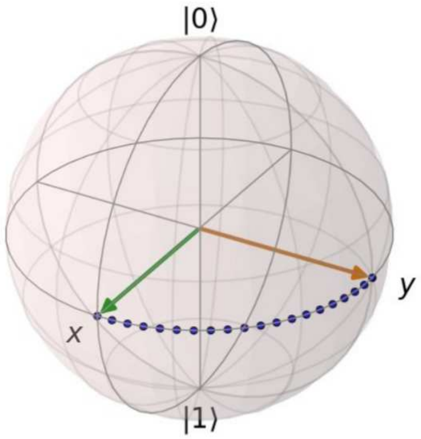


Figure 2: Pauli gates X, Y and Z visualized on the Bloch sphere.

1.5.2 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.



1.5.3 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.

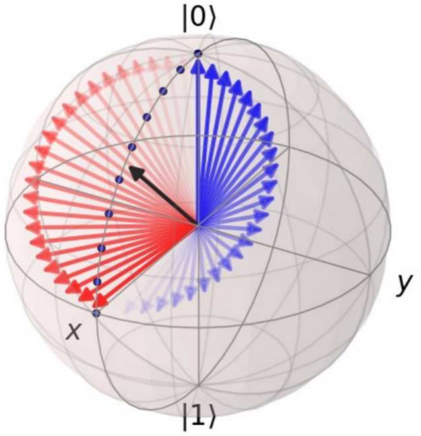


Figure 3: Hadamard gate visualized on the Bloch sphere.

1.6 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:

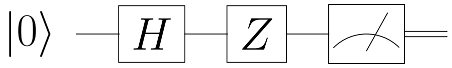


Figure 4: A simple quantum circuit. The output of measuring a qubit is a classical bit, which is distinguished from a qubit by drawing a double-line wire. A visualization of this circuit on the Bloch sphere can be seen in Figure 5.

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 $|1\rangle$.

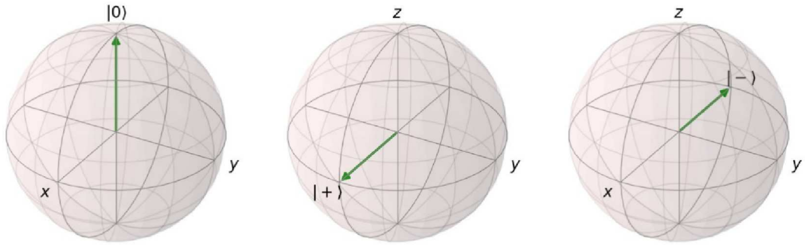


Figure 5: States of our qubit throughout the circuit from left to right: $|0\rangle \rightarrow H\,|0\rangle \rightarrow ZH\,|0\rangle$.

1.7 Matrix Notation

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

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

For computational purposes we can use vectors to represent a quantum state. We define $|0\rangle$ and $|1\rangle$ as following:

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

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

Then by filling in the formula we can represent our quantum state with a vector. This 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.

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

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 itself, or $H = H^\dagger$, making it a *Hermitian matrix*.

2 Fundementals: A Multi-Qubit World

2.1 The Step To Multi-Qubit

We can represent multiple qubits using the *Kronocker 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.

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 $H_0|0_1 0_0\rangle$. That is, put the first 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 size. We can achieve this by taking the Kronocker product of the identity matrix and our single-qubit matrix (in this case H):

$$H_0|0_1 0_0\rangle = (I_1 \otimes H_0)|0_1 0_0\rangle$$

Writing it out:

$$I_1 \otimes H_0 = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \otimes \begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\right)$$

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

[1] Note that when I say "first" 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.

Then we can put our state $|00\rangle$ 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 $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$.

2.2 Common Two-Qubit Gates

2.2.1 CNOT Gate

The quantum gate controlled-NOT (C_{NOT}) 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 C_{NOT} can be seen in Figure 6. Qubit A represents the control and B represents the target qubit.

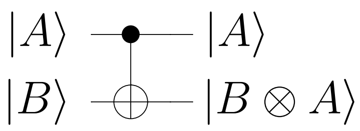


Figure 6: Circuit representation of C_{NOT}, where $\otimes$ is addition modulo two.

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

Figure 7: Matrix representation of C_{NOT}.

2.2.2 CZ Gate

2.3 Toffoli Gate

2.4 Entanglement

Two qubits are entangled iff they have nonzero concurrence.