Introduction to Quantum Computing

Lectures by Leon Riesebos

Steven Oud

soud@pm.me

March 6, 2019

Chapter 1

Fundamentals: 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 quantum bit (*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 $|1\rangle$ (denoted in *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 $|+\rangle$.
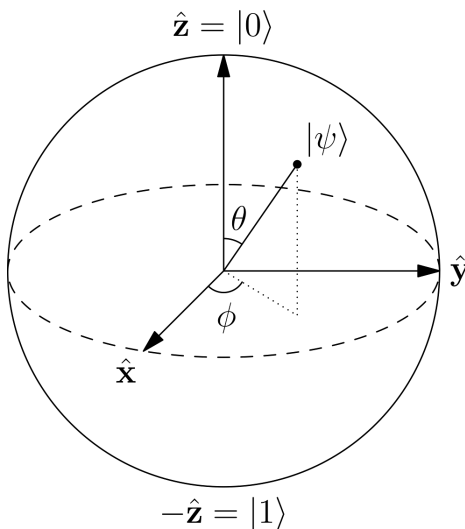
1.2 The Bloch Sphere

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. Factor $e^{i\delta}$ is the global phase of the state. This factor does not influence measurement probabilities, since $\left|e^{i\delta}\right| = 1$. Therefore we can often omit it, 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 1.1). 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 1.1: 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 $U^\dagger U = UU^\dagger = I$, where $U^\dagger$ is the conjugate transpose of U and I the identity operation. 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 $U^2 = I$.
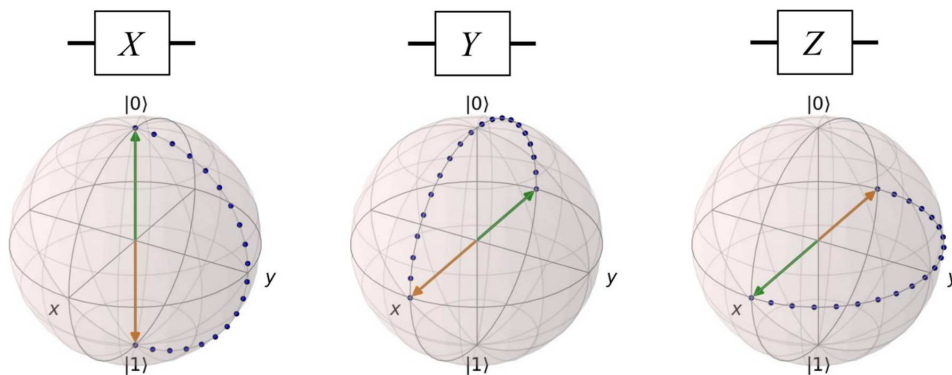

Figure 1.2: Pauli gates X, Y and Z visualized on the Bloch sphere.

1.3.2   Phase Gates

An important class of single-qubit gate are the *phase gates* R_θ, which rotate the phase of the $|1\rangle$ state by an angle θ and leaves the $|0\rangle$ state unchanged:

$$R_\theta |0\rangle = |0\rangle$$
$$R_\theta |1\rangle = e^{i\theta} |1\rangle$$

A common phase gate is the *S gate*, where $\theta = \dfrac{\pi}{2}$ (visualized in Figure 1.3). The Pauli Z gate can also be considered a phase gate where $\theta = \pi$, because

$e^{i\pi} = -1$. Thus you could also think of the S gate as half a Pauli Z gate. Another common phase gate is the *T gate*, where $\theta = \dfrac{\pi}{4}$. The probability of measuring a $|0\rangle$ or $|1\rangle$ is unchanged after these gates, however it modifies the phase of the quantum state.
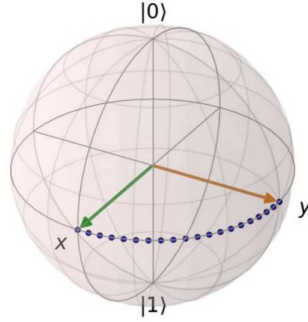
Figure 1.3: S gate rotation visualized on the Bloch sphere.

1.3.3 Hadamard Gate

The Hadamard (H) gate maps the 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.
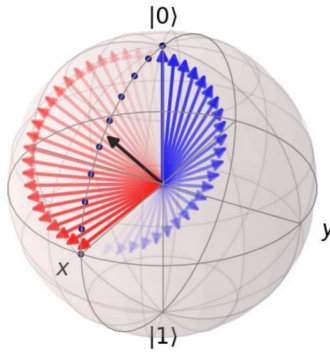
Figure 1.4: Hadamard gate visualized on the Bloch sphere.

1.4 Measurement

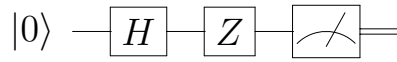Measuring a qubit collapses its state. The probabilistic result of a qubit measurement can be calculated based on the probability amplitudes:

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

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

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

Consider the following simple single-qubit circuit:

Figure 1.5: 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 1.6.

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 $|1\rangle$.
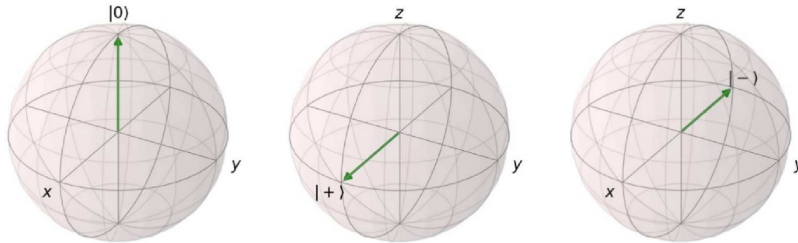
Figure 1.6: States of our qubit throughout the circuit from left to right: $|0\rangle \rightarrow H |0\rangle \rightarrow ZH |0\rangle$.

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:

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

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

A quantum state has to be a normalized vector. 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:

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

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

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

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

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

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

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

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

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

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 conjugate transpose: $H = H^\dagger$.

Chapter 2

Fundamentals: A Multi-Qubit World

We can represent multiple qubits using the *Kronecker product* to combine single qubit states:

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

More generally, we say that any linear combination $\sum_i \alpha_i |\psi_i\rangle$ is a quantum state with states $|\psi_i\rangle$ and amplitude α_i for state $|\psi_i\rangle$. To represent $|00\rangle$ for example:

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

Note that the state vector of two qubits is twice as big as the state vector for one qubit. This is where some of the potential power of quantum computers comes from. With n qubits you can represent 2^n states - the state space grows exponentially with the number of qubits, unlike 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:

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

2.1   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:

$$
\begin{aligned}
I_0 \otimes H_1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\
&= \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right] \\
&= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}
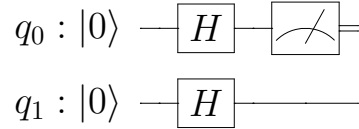\end{aligned}
$$

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

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

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

2.2   Partial Measurement

Say we measure the qubit $|q_0\rangle$ 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 $|q_0\rangle$ we have a 50/50 probability of getting a 0 or 1. Measuring $|q_0\rangle$ collapses the state to one of the following states:

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

This is called measurement projection. We have two possible states for q_0 after measurement: 0 or 1. Qubit $|q_1\rangle$ will stay in superposition because we haven't measured it. Notice how the first qubits (underlined) in both states are the same. This makes sense, we've measured that one so we're certain of its state.

2.3 Common Two-Qubit Gates

2.3.1 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 2.1. 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.
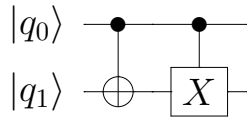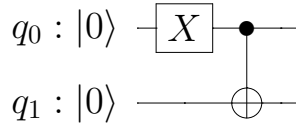

Figure 2.1: Circuit representations of CNOT. We will use the left representation.

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

Figure 2.2: Matrix representation of CNOT.

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


First we put $|q_0\rangle$ (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:

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

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

2.3.2 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.
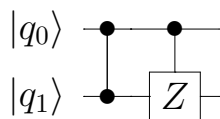
Figure 2.3: Circuit representations of CZ.

2.3.3 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:

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

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:

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

2.4 Toffoli Gate

We can simulate any 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 2.4), 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 $|111\rangle$.

$$a \; \bullet \; a$$
$$b \; \bullet \; b$$
$$c \; \oplus \; c \otimes ab$$
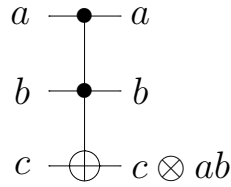
Figure 2.4: Circuit representation of the Toffoli gate, where $\otimes$ is addition modulo two.

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

$$U_{CCX} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

It is a non-Clifford gate.

2.5 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. 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?

$$C\left(\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\right) = 2\left|\frac{1}{2}\left(\frac{1}{2}\right) - \frac{1}{2}\left(\frac{1}{2}\right)\right| = 0$$
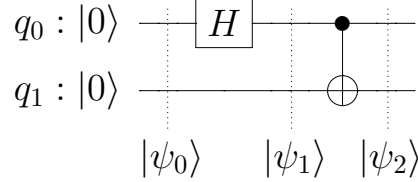
A concurrence of 0, so it is indeed not entangled.

2.6 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:

$$q_0 : |0\rangle \quad \boxed{H} \quad \bullet$$
$$q_1 : |0\rangle \quad \oplus$$
$$|\psi_0\rangle \qquad |\psi_1\rangle \quad |\psi_2\rangle$$

We start with our state $|00\rangle$ at $|\psi_0\rangle$. We put $|q_0\rangle$ 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 $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ at $|\psi_2\rangle$.

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.

$$q_0 : |0\rangle \quad \boxed{H} \quad \bullet \quad \boxed{\nearrow}$$
$$q_1 : |0\rangle \quad \oplus \quad \boxed{\nearrow}$$
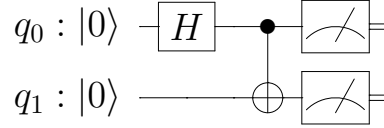
You will find that the measurement results are correlated:

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

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

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).

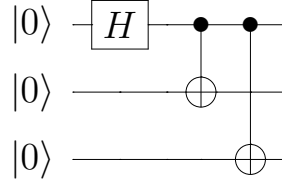## 2.7 Greenberger-Horne-Zeilinger State

A Greenberger-Horne-Zeilinger (GHZ) state is a certain type of entangled state. It is a $M > 2$ system state:

$$|\text{GHZ}\rangle = \frac{|0\rangle^{\otimes M} + |1\rangle^{\otimes M}}{\sqrt{2}}$$

Where $|i\rangle^{\otimes M}$ means the Kronecker product with itself M times. For example $M = 3$:

$$|\text{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

GHZ states are used for example in cryptography for secret sharing.

Figure 2.5: Circuit creating a three-qubit GHZ state.

2.8 Calculating Parity

Parity checking is one of the simplest forms of error detecting code. It tells us if the number of ones in a set of bits is even or odd. For example, 001 has a parity of 1 (odd) and 110 has a parity of 0 (even). We introduce a quantum algorithm for calculating the parity of an n-qubit state. For this example we'll determine the parity of a two-qubit state. Consider the circuit in Figure 2.6. We will calculate the parity of $|q_0 q_1\rangle$ with $|q_2\rangle$.
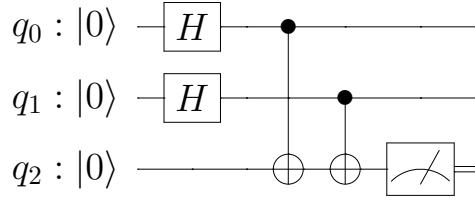
Figure 2.6: Circuit for calculating parity: $\text{CNOT}_{1,2}\text{CNOT}_{0,2}H_1 H_0 |000\rangle$.

We start with putting $|q_0\rangle$ and $|q_1\rangle$ in an arbitrary superposition. In this case we apply a Hadamard gate to both qubits, giving us the state

$$|\psi\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle)$$

Then we apply a $\text{CNOT}_{0,2}$ operation

$$|\psi\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |101\rangle + |111\rangle)$$

And a CNOT$_{1,2}$, giving us the final state

$$|\psi\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$$

If you look closely at this state, you can see that $|q_2\rangle$ corresponds to the parity of $|q_0q_1\rangle$. We have essentially calculated the parities of all possible states of $|q_0q_1\rangle$ in parallel. However, we cannot observe a quantum state to extract all the possible states' information. We are limited to measuring one outcome. When we measure $|q_2\rangle$ the state partially collapses leaving only the states with parity q_2. Let's take a look at the possible states after measuring $|q_2\rangle$:

$$|\psi\rangle = \begin{cases} \dfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes |0\rangle \text{ if } M(q_2) = 0 \\ \dfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \otimes |1\rangle \text{ if } M(q_2) = 1 \end{cases}$$

Measuring a 0 leaves us with even parity states and measuring a 1 leaves us with odd parity states. $|00\rangle$ and $|11\rangle$ have even parity ($q_2 = 0$), $|01\rangle$ and $|10\rangle$ have odd parity ($q_2 = 1$).

2.9   Quantum Teleportation

Quantum teleportation it a technique for moving arbitrary quantum states around. It uses an *EPR pair* (a pair of qubits that is in a Bell state) that is shared between the sender and receiver. Note that it is impossible to clone a qubit state. This is referred to as the *no-cloning theorem*. Quantum teleportation works as following: Alice and Bob generate an EPR pair and both take one qubit before they get separated. Alice wants to deliver a qubit $|\phi\rangle$, whose state is unknown, to Bob. Alice interacts the qubit $|\phi\rangle$ with her half of the EPR pair, and then measures the two qubits in her possession. At this point, Alice's qubits are in one of the four classical states 00, 01, 10 or 11. She sends this information to Bob. Bob then performs one of four operations on his half of the EPR pair, recovering Alice's quantum state $|\phi\rangle$.

The quantum circuit in Figure 2.7 teleports the unknown state $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$. We start at $|\psi_0\rangle$ with the state $|\phi\rangle|00\rangle$. Then we create an EPR pair with $|q_1q_2\rangle$, where $|q_1\rangle$ belongs to Alice and $|q_2\rangle$ to Bob. This gives us the following state at $|\psi_1\rangle$:

$$|\psi_1\rangle = |\phi\rangle \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
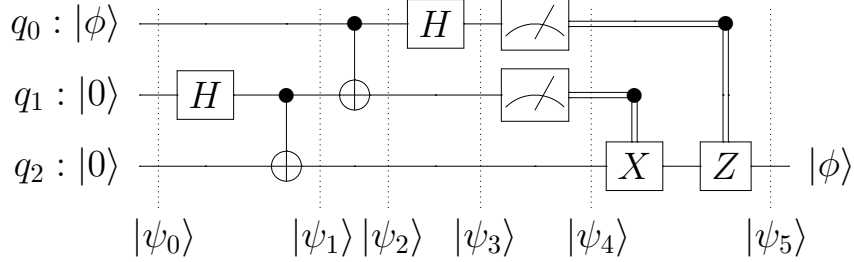
Figure 2.7: Quantum circuit teleporting a quantum state $|\phi\rangle$.

Which we can rewrite as following

$$|\psi_1\rangle = \alpha |0\rangle + \beta |1\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}}\Big(\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle)\Big)$$

Alice then sends her qubits through a $\text{CNOT}_{0,1}$ gate, obtaining

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\Big(\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|10\rangle + |01\rangle)\Big)$$

She then sends q_0 through a Hadamard gate, giving

$$|\psi_3\rangle = \frac{1}{2}\Big(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\Big)$$

This state can be rewritten in the following way:

$$|\psi_3\rangle = \frac{1}{2}\Big(|00\rangle (\alpha |0\rangle + \beta|1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle)$$

$$+ |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle)\Big)$$

This expression breaks down in four terms. The first term has Alice's qubits in state $|00\rangle$ and Bob's qubit in state $\alpha |0\rangle + \beta |1\rangle$, which is our original state $|\phi\rangle$. So in the case that Alice measures $M(q_0 q_1) = 00$ at $|\psi_4\rangle$, Bob's qubit will be in state $|\phi\rangle$. Depending on Alice's measurement at $|\psi_4\rangle$, Bob may have to "fix" his state to recover $|\phi\rangle$ by applying the appropriate gate(s). For example, if Alice measures 00, Bob doesn't have to do anything. If Alice measures 01, Bob can fix his state by applying an X gate. If Alice measures 10, Bob can fix his state by applying a Z gate. And if Alice measures 11, Bob can fix his state by first applying an X gate and then a Z gate. After fixing his state, Bob ends up with Alice's state $|\phi\rangle$ at $|\psi_5\rangle$.

Note that quantum teleportation does *not* allow for faster than light communication. This is because Bob needs to be told of the result of Alice's measurements through a classical channel in order to complete the teleportation. Also note that we did not clone the quantum state $|\phi\rangle$, we merely moved it. Teleporting a state depends on the measurement and thus collapsing of the original state $|\phi\rangle$, so it never allows for cloning.