Chapter 1

Introduction and Overview

1.1 Perspectives

- One thing that we've always wanted to do was to obtain a *complete control single quantum systems*. Particle accelerators and superconductivity have gotten us close to doing so, but even then those systems are often very hard to control.
- Over decades, we've gotten better at doing this: we've been able to trap atoms using lasers, and now are able to actually talk about the quantum behavior of certain objects.
- At the same time, computer science was also an emerging field, with the help of Turing.
- Failure of Moore's law in recent years: we can no longer get smaller! One way out is to explore the world of quantum computation.

1.2 Quantum Bits

- A bit is the fundamental concept that we'll talk about, specifically in the quantum world they are called qubits.
- Qubits are classified by their state $|0\rangle$ and $|1\rangle$, and they can also exist in a linear combination of states:

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

  α and β are generally complex numbers, and the probability of measuring $|0\rangle$ is $|\alpha|^2$, and similarly for $|1\rangle$.
- By the law of total probability, we have that $|\alpha|^2 + |\beta|^2 = 1$.
- It's important to remember that a qubit can exist in a continuum of states between $|0\rangle$ and $|1\rangle$. A common state is the $|+\rangle$ state:

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

- A useful interpretation of $|\psi\rangle$ is the following simplification:

$$\begin{aligned}|\psi\rangle &= e^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\right)\\ &= \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\end{aligned}$$

The e^{iy} in front can be ignored, since some initial phase doesn't really matter. This is known as the **Bloch Interpretation** of a quantum state. Here, states appear on a *Bloch Sphere*, and it diagramatically shows a quantum state. That said, there is no interpretation like a bloch sphere for multiple qubits.

- The amount of information represented by one qubit is actually the same as that of a classical bit, due to the fundamental postulates of quantum mechanics.

1.2.1 Multiple Qubits

- Suppose we have two qubits. Because they're quantum, then they have basis states: $|00\rangle, |01\rangle |10\rangle, |11\rangle$. Then, we can model its quantum state as:

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

  Note that the state collapses with probability $|\alpha_x|^2$, and the state after measurement is $|x\rangle$.

- If we just measure a subset of the qubits (say, bit 0), then we're left with the post-measurement state:

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

  Note the renormalization factor of $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$ in the denominator, which ensures that normalization is still satisfied.

- An important state we'll constantly come back to is the *Bell State* or *EPR Pair*:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{1.1}$$

  This state is special because measuring the first qubit also gives you information about the state of the second qubit automatically, without measurement.

- In general, an n bit system is modeled by a state with 2^n amplitudes, meaning that $n = 500$ already gives us a value larger than the number of atoms in the universe.

1.3 Quantum Computation

1.3.1 Single Qubit States

- Recall the classical implementation of the NOT gate, which basically inverts a circuit from $0 \to 1$ or $1 \to 0$. There is also a quantum analogue, if we're given a state $\alpha|0\rangle + \beta|1\rangle$ then the corresponding state that the NOT operation should return is $\alpha|1\rangle + \beta|0\rangle$. (In other words, we flip the probability of the inputs.)

- One way to represent the NOT gate is to use a matrix (Note: this is only possible because quantum gates are linear): $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

  Why are quantum gates linear? How is it possible that the gate does not collapse the quantum state, and even if it doesn't how do we show linearity?

  It's linear in the bits because we can apply the gate individually onto each bit.

- The only constraint we have on a gate U is that it must be unitary: that is, $U^\dagger U = I$

- Some important quantum gates to know about:

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

this leaves $|0\rangle$ unchanged, but flips the sign of $|1\rangle$ to $-|1\rangle$. The other is the Hadamard gate:

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

It turns both states "halfway" between one another:

$$\alpha |0\rangle \to \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$\beta |1\rangle \to \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Pictorally, this is equivalent to rotating about the $\hat{y}$ axis by 90°, and then rotating about the $\hat{x}$ axis by 180°.

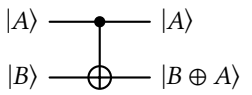
- Any arbitrary gate can be decomposed into a product:

$$e^{i\alpha} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}$$

- This means that we have an infinite number of single qubit gates! However, we don't actually need an infinite number of gates – for special values of α, β, γ, there is a way to build very good approximations for any kind of gate we come across.

1.3.2 Multiple Qubit Gates

- The simplest quantum gate is the controlled-NOT, also called a CNOT gate, which takes a control bit and a target bit, and does (or doesn't) do things based on the value of the control bit.



What it does is read off the control qubit, and if it's 0, then the target is unchanged. Otherwise, we flip the target:

$$|00\rangle \to |00\rangle$$
$$|01\rangle \to |01\rangle$$
$$|10\rangle \to |11\rangle$$
$$|11\rangle \to |10\rangle$$

Given this representation, we can also write it as an operation of $|A, B\rangle \to |A, B \oplus A\rangle$, where the $\oplus$ signifies addition mod 2. It's also possible to write CNOT in matrix form, which is:

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

it's also possible to verify that $U_{CN}^\dagger U_{CN} = I$.

- Other classical gates like the NAND and XOR gates cannot be implemented this way, because there is a fundamental loss of information when information is passed through them – for instance, given $A \oplus B$ from an XOR gate, it's impossible to tell (with certainty) what A and B were.

  One requirement of our quantum gates is that they must be unitary and hence reversible, so these other gates cannot be implemented quantumly.

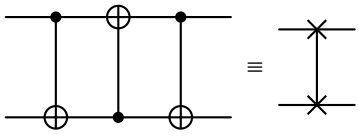
- It also turns out that any multiple qubit logic gate can be implemented by using only CNOT and single qubit gates: this is the quantum analogue to the NAND universality found in classical computation.

1.3.3 Measurements in Bases other than the computational basis

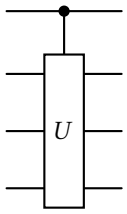
- There are many basis states one could pick for a qubit. In general, given any two $|a\rangle$ and $|b\rangle$ (provided they are not the same) for a qubit it is possible to use these as a basis for any arbitrary state.
- If they are orthonormal, they have the added benefit that performing a measurement will give state $|a\rangle$ and $|b\rangle$ with a known probability.

1.3.4 Quantum Circuits

- Circuits are read left to right, and each line represents a wire in a quantum circuit. One of the most common is the swap circuit, which swaps the states of two qubits. This is implemented using three CNOT gates:



- Loops, joining, and separation of wires are **not** allowed in quantum circuits.
- Any unitary matrix U that acts on n qubits can be represented as some arbitrary gate, and we can also add control to it:



  Here, the U gate would be controlled by whatever the state of the first bit is.
- Measurement is also important, which changes a quantum wire into a classical one, through a meter symbol:

  The classical wire is represented as a double wire.

1.3.5 No Cloning

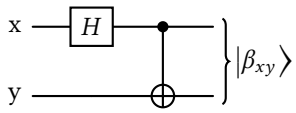
- Classically, it's easy to copy a qubit by using a CNOT gate, but this is not always possible for quantum circuits.
- In the case where $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$, then a CNOT gate is able to copy the state $|\psi\rangle$ onto a second qubit. However, for a general state $|\psi\rangle$, the equation for the output state (after copying) is:

$$|\psi\rangle\,|\psi\rangle = a^2\,|00\rangle + ab\,|01\rangle + ab\,|10\rangle + b^2\,|11\rangle$$

  If we want to copy the bit, then we'd want only the $|00\rangle$ or $|11\rangle$ states. This means that $ab = 0$, which only occurs when a or b are zero, so this copying process is impossible for general states.
- More succinctly, a quantum cloning device can only clone orthogonal states, and a general cloning device is not possible. There is a detailed proof of this later on in the textbook that we'll get to.

1.3.6 Bell States

Consider a slightly more complicated circuit:



Recall what the Hadamard gate does: it takes a state $|00\rangle$ and transforms it into $(|0\rangle+|1\rangle)|0\rangle/\sqrt{2}$, then the CNOT then gives the output state $(|00\rangle + |11\rangle)/\sqrt{2}$. Note the reason that this happens is because the CNOT gate is conditioned on the first bit, hence it flips the product state $|10\rangle$ into $|11\rangle$. Therefore, the output states are:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$
$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

What is the purpose of such a circuit? Doesn't the Hadamard gate on its own do this already?

The Hadamard gate does something similar but not identical: it takes a single bit state and superimposes it, but here we're placing *two* states in superposition with each other.

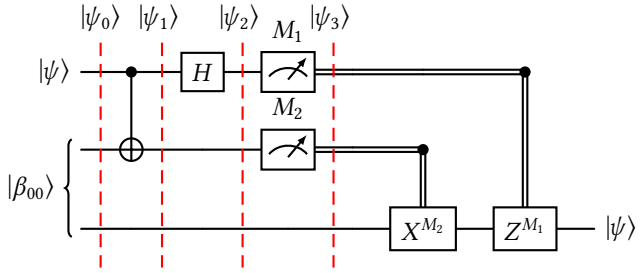
These states are called the *Bell states* (or also the *EPR States*), which exhibit some strange properties.

1.3.7 Quantum Teleportation

Suppose we have two people, Alice and Bob, who create an EPR and they each take one qubit and move very far from each other. Now, suppose Alice wanted to deliver a qubit $|\psi\rangle$ to Bob. Is this possible? The answer to that is suprisingly, yes!

On the surface it looks impossible, since firstly, we don't know what the state $|\psi\rangle$ is, and even if we did, because the values α, β that are used to encode $|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$ are *complex valued*, this requires an infinite number of information to encode! However, here we utilize **quantum teleportation** in order to solve the problem.

Basically, the idea is that Alice first interacts $|\psi\rangle$ with her half of the EPR pair, and then measures the two qubits. Based on the results (either 00, 01, 10, 11), she sends this information to Bob, and Bob can recover the $|\psi\rangle$ this way. The circuit is as follows:



To read this circuit, the first two lines correspond to Alice's state, and the third line corresponds to Bob's state, where he's recovered $|\psi\rangle$. Specifically, alice has $|\psi\rangle$ and the *first* of the EPR state $|\beta_{00}\rangle$. The basic idea is this: we send in the state $|\psi\rangle|\beta_{00}\rangle$ as indicated on the left. Remember that $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, so the product state is expressed as:

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right]$$

Then, as the state goes through the CNOT gate, we get:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\right]$$

The CNOT gate flips the *first* qubit when the state $|\psi\rangle = |1\rangle$, which is why the second term has the first bits inverted compared to $|\psi_0\rangle$. We then send the first qubit through a Hadamard gate, which rotates the first qubit:

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left[\alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}}(|00\rangle + |11\rangle) + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}}(|10\rangle + |01\rangle\right] = \frac{1}{2}l\left[\alpha(|0\rangle + |1\rangle(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right]$$

We can regroup terms and that gives us the following:

$$|\psi_2\rangle = \frac{1}{2}\left[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right]$$

Now, we look at these four terms. The first term is Alice's qubits in the state $|00\rangle$, and Bob's in the state $\alpha|0\rangle + \beta|1\rangle$, which is $|\psi\rangle$. Therefore, if Alice measures her qubits and finds them in the state $|00\rangle$, then we know that Bob's system is in the state $|\psi\rangle$. On the other hand, if she measures 01, then we know that Bob's state is $\alpha|1\rangle + \beta|0\rangle$. Effectively, if Alice could communicate her measurement result to Bob, then Bob would know his state. Once she does communicate, then in order to recover $|\psi\rangle$, Bob could use the Z and X gates in order to recover $|\psi\rangle$. Specifically, he needs to apply $Z^{M_1}X^{M_2}$ to his state, notice the matrix product goes from right to left, but the circuit is written from left to right.

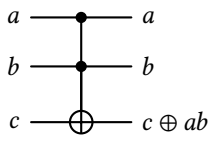
How is it that the first two qubits now belong to Alice? Initially she had $|\psi\rangle$, and one half of $|\beta_{00}\rangle$, not the whole thing, so how did she suddenly become in possession of the entire $|00\rangle$? Alternatively, she coudln't possibly have measured the entire state $|00\rangle$, since she only has possession of one of these qubits?

Another thing to note is that Alice needs to communicate her result (classically) to Bob in order for him to recover the result. Because this cannot be done faster than light, this is what prevents information from being transported faster than light.

1.4 Quantum Algorithms

1.4.1 Classical computations on a quantum computer

Not surprisingly, any classical logic circuit can be implemented using a quantum circuit. However, they cannot be used to *directly* simulate a classical circuit, because classical circuits can contain reversible elements whereas quantum circuits cannot. However, we can build *equivalent* circuits, using the Toffoli gate:



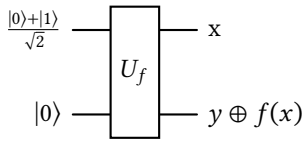
This gate flips the state of c if both a and b are set to 1, otherwise c is left alone. Because the inverse of the Toffoli gate is itself (applying the gate twice on a state c returns it back to its original state), this gate is reversible. We can then use this to simulate gates such as NAND and FANOUT.

One can write down the 8×8 matrix U that represents the quantum Toffoli gate and check that it is indeed unitary, but that's too much work. However, the principle that it can be done ensures that we can simulate all classical logic on a quantum circuit if we'd like. Randomness is also easy to simulate on a quantum computer – for instance, if we wanted to generate a fair coin toss, we'd just generate the state $(|0\rangle + |1\rangle)/\sqrt{2}$ and measure it, which would give us either state with equal probability.

1.4.2 Quantum Parallelism

In essence, this is the idea that quantum computers have the ability to evaluate a function $f(x)$ on many different inputs of x simultaneously. For simplicity, we'll let $f(x) : \{0,1\} \to \{0,1\}$ for now. To compute this function, we can start with a 2-qubit state $|x, y\rangle$, and we can transform this into the state $|x, y \oplus f(x)\rangle$ (here, the $\oplus$ refers to addition modulo 2). We'll call the transformation U_f, which maps $|x, y\rangle \to |x, y \oplus f(x)\rangle$. We won't concern ourselves with the exact implementation of U_f for now, but we know that it can be done, because it is reversible (check this).

Now, we want to compute U_f on the states $x = (|0\rangle + |1\rangle)/\sqrt{2}$ and $y = |0\rangle$:



Applying U_f on this states gives the result:

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

As I understand it, U_f outputs the following on the inputs:

$$|\psi\rangle = \left| \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |0\rangle \oplus f\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \right\rangle$$

How is f evaluated here? How does it equal the resulting state?

Firstly, since $y = |0\rangle$, then the resulting second value in the state is just $f(x)$. Then, because x is a superposition of the states $|0\rangle$ and $|1\rangle$, then we get the states $|0, f(0)\rangle$ and $|1, f(1)\rangle$ with equal probability, which is why we can express $|\psi\rangle$ as the state written in the book.

This state is remarkable, since it implies that we've computed $f(0)$ and $f(1)$ simultaneously, without the need to build multiple circuits. This procedure is generalized in what's known as the **Hadamard Transform**, which is basically the product state of n Hadamard gates acted on the state $|0\rangle$. On n qubits, the resulting state is:

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

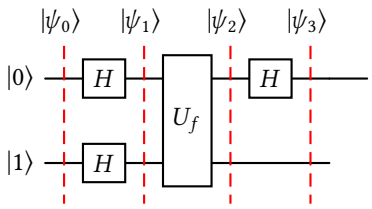
Then, in order to evaluate a function $f(x)$, we can prepare a state $|0\rangle^{\otimes n} |0\rangle$, where the first n qubits are sent through n Hadamard gates, and when this state is passed through U_f, we get:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

This is not immediately useful however: upon measurement, we still only get one value of $f(x)$ as an output. The real power of quantum parallelism is the ability to extract information about more than one value of $f(x)$ with superposition.

1.4.3 Deutsch's Algorithm

Deutsch's algorithm combines quantum parallelism (what we just saw) with interference. First, we'll set up two bits in the states $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$, by acting the Hadamard gate on the states $|0\rangle$ and $|1\rangle$ respectively. Then, we'll apply U_f, then apply one final Hadamard gate to the result of x:



Again, these states are sent through the Hadamard gate, so we have

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

If we apply U_F to this state, this gives us the state $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$. Therefore, if we were to apply U_F to $|\psi_1\rangle$, we get:

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & f(0) = f(1) \\ \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & f(0) \neq f(1) \end{cases}$$

Then, passing the first bit through the Hadamard gate again reverses the rotation, so we get:

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & f(0) = f(1) \\ \\ \pm|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & f(0) \neq f(1) \end{cases}$$

Then, since $f(0) \oplus f(1)$ is 0 if $f(0) = f(1)$ and 1 otherwise (because if $f(0) \neq f(1)$ then one of $f(0)$ or $f(1)$ must be 1), then we can rewrite this as:

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

The power of this resulting state is that by measuring the first qubit alone, we can determine $f(0) \oplus f(1)$, meaning that we can determine both $f(0)$ and $f(1)$ with a *single* evaluation! The reason this works is becuase here, we've created a state where the result of $f(0)$ affects $f(1)$, so we are able to determine the identities of $f(0)$ and $f(1)$ with a single evaluation.

1.4.4 The Deutsch-Jozsa Algorithm

This is the algorithm that solves Deutsch's problem, which is phrased as follows: Given $f(x)$, it is one of two kinds: either $f(x)$ is constant for all x, or $f(x) = 1$ for half the inputs and $f(x) = 0$ for the other half.

In the classical case, we'd require at least $2^{n-1} + 1$ values in order to determine the identity of f. However, if we were to do this with a quantum computer, we can accomplish this much faster, using only $O(n)$ time.

To solve this, we'll use Deutsch's algorithm, except this time on n bits. We start with the state

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$$

Then, when we perform a Hadmard transform on these first n qubits, we get:

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Then, using U_f we get:

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$