Chapter 1

Quantum Computing

1.1 Learning Problems

1.1.1 A Motivating Example

Suppose you're involved in a simple card game: A dealer places two cards (you can assume that the cards are either red or black, with equal probability of occurring) face down on a table. You win the game and a substantial prize if you can guess whether the two face-down cards share the same color. You're allowed to ask the dealer to reveal cards to you, but for each card revealed your potential prize gets smaller.

How many of the cards do you need to see to determine with certainty whether the cards share the same color? Maybe you don't need to know for certain. How does the probability of you being able to guess the correct answer relate to the number of cards seen?

If you have no information at all, you can't do substantially better (or worse) than a fifty-percent chance. In fact, seeing only a single card, does not give you any more knowledge of what the answer to the question is. If you wanted to know with certainty what the answer was, you would need to see both cards.

This is of course a very simple game, but it is an example of a type of problem that we refer to as *learning problems* or often *oracle problems*. These problems consist of a learner who is trying to determine the answer to some question, generally to find the output of a certain function. The learner starts out with incomplete information, but is given access to an *oracle function* she can query to gain more information. An oracle function–also sometimes called a black-box function–is one that you can evaluate the oracle at any input of your choosing, but you have no information about the function other than its responses to your inputs. The learner's goal is to determine the answer to the question in as few questions as possible.

We rephrase the scenario given above in this language. Choose 0 to represent a black card and 1 to represent a red card. Suppose the two facedown cards are labeled a and b.

Example 1.1. Given oracle access to a function $f : \{a, b\} \to \{0, 1\}$. What is the minimum number of queries required to determine $f(a) \oplus f(b)$ where $\oplus$ denotes

addition mod 2?

1.2 Quantum Computing

Now we introduce the concepts required for quantum computation. In the quantum world, the *qubit* is the fundamental unit of information. In the same way that we can express any classical algorithm as a circuit of logical operations on bits, we can express any quantum operation as a sequence of *unitary* operations on *qubits*.

1.2.1 Qubits

The following treatment of quantum computing is largely taken from [3] and [2]. The goal of this chapter is to introduce a minimal model of quantum computing that is sufficient for the tasks we will need in chapters 2 and 3. It can be hard to follow quantum computing if one is not already familiar with it as there is a lot of notation and formal definitions. Moreover, since quantum mechanics has a reputation for being unintuitive, it is often hard to feel like the intuitions one has are correct. However, I think that quantum circuits do a very good job of capturing the intuition from classical computing and so I have tried to include many simple examples of circuits. For a very detailed and gentle introduction to the subject, I strongly recommend reading [2]. For a much more expansive view of the entire subject of quantum computing and topics not covered here, I would refer to Nielsen and Chuang's text [3].

Whereas the state of a bit has *two* possible values—either 0 or 1—the state of a qubit is a unit vector in complex vector space spanned by *two* basis states. We give the following precise definition

Whereas a bit has two states—0 or 1—a qubit has *two basis states*. The following definition makes this precise

Definition 1.1. The state of a *qubit* is a unit vector in $\mathbb{C}^2$. That is, a pair of complex numbers

$$(\alpha, \beta) \in \mathbb{C}^2$$

satisfying the normalization condition

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

We refer to the space $\mathbb{C}^2$ as the *state space* of a qubit and consider it to be an inner product space equipped with the standard inner product on $\mathbb{C}^n$.[1] We choose the standard basis $\{(0,1),(1,0)\}$ to represent $\mathbb{C}$. In order to make the analogy with bits more clear, we denote

$$|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

[1] In quantum mechanics literature, state spaces of quantum systems are always referred to as *Hilbert spaces* regardless of their dimension. This can be confusing as *Hilbert spaces* in mathematics are generally associated with infinite dimensional spaces. Since all of the spaces in this thesis will be finite dimensional (and isomorphic to $\mathbb{C}^{2^n}$), it is easier to avoid the confusion and use the term state space instead.

The symbol $|\ \rangle$ is called a *ket* and is used to denote a vector representing a quantum state. It comes from the *bra-ket* notation which is widely used in the greater theory of quantum mechanics.

1.2.2 Measurement

Although a qubit has a quantum state in $\mathbb{C}^2$, the we cannot directly observe this quantum state. Despite having what seems like a much richer state, when we try to measure qubits using any sort of detector, they snap into the states $|0\rangle$ or $|1\rangle$. This of course defies any reasonable expectations one would have about the world, and has raised much philosophical debate about how it should be interpreted. However, regardless of what interpretation we take, it remains an experimental fact. The following postulate formalizes this concept as a process called *measurement in the computational basis* .

Postulate 1. *Given a qubit ψ, we may perform* measurement *of ψ in the* computational basis. *If ψ was in state $\alpha|0\rangle + \beta|1\rangle$ prior to the measurement, after the measurement it will be in state $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$.*

This is only a specific case of a much more general postulate of measurement in quantum mechanics. However, this conception of measurement will be sufficient enough for many of the results in quantum computing and all of the results that we will need to consider. A more in depth discussion of the postulates of quantum mechanics and how they relate to quantum computing can be found in [3].

If we naively think of the state of a qubit as being in $\mathbb{R}^2$ rather than $\mathbb{C}^2$ by just ignoring the imaginary part, we can generate some limited geometric intuition about what is going on.

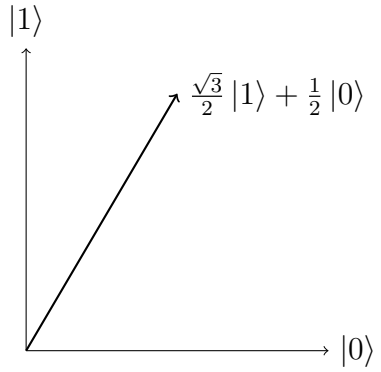


Figure 1.1: A qubit with state $\frac{\sqrt{3}}{2}|1\rangle + \frac{1}{2}|0\rangle$ pictured in the plane by ignoring the imaginary part.

A measurement on the pictured qubit will return 0 with probability 3/4 and 1 with probability 1/4. This perspective hopefully makes it clear why the state of a qubit had to be a unit vector. When written in the standard basis, the coefficients of

$|0\rangle$ and $|1\rangle$ correspond to the probability of a measurement producing that outcome. Thus requiring that this state be a unit vector is equivalent to requiring that the total probabilities sum to one.

This also motivates the other postulate of quantum mechanics that we will need to formalize this model of quantum computation.

Postulate 2. *The valid operations on quantum states are those given by* unitary transformations.

The unitary transformations on $\mathbb{C}^n$ are exactly the *isometries* of $\mathbb{C}^n$, that is, the ones that preserve the inner-product. This is, perhaps not too surprising, given that preserving the metric is necessary condition to ensure that the probabilities sum to one.

Definition 1.2. The set of unitary transformations on $\mathbb{C}^n$ can be represented as the set of $n \times n$ matrices U satisfying the identity $U^{-1} = U^\dagger$ where $U^\dagger$ denotes the conjugate-transpose of U.

A consequence of this postulate of quantum mechanics is that quantum information cannot be destroyed without a making a measurement.

1.2.3 Gates

By postulate 2, the valid operations on a qubit are the 2×2 unitary matrices.

This part of quantum computing can be confusing at first, since the notation constantly switches between kets and matrices.

Example 1.2. The quantum `NOT` gate is the single qubit gate defined by

$$|0\rangle \mapsto |1\rangle$$
$$|1\rangle \mapsto |0\rangle$$

It should be noted that it is common to refer to the quantum `NOT` gate by the letter X.

In standard vector notation this is

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

Which gives us that the quantum `NOT` gate is represented by the matrix

$$X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Example 1.3. A very important single qubit gate is the *Hadamard* gate. The Hadamard gate, denoted H, can be defined in terms of its action on the standard basis as

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

These states appear frequently and so it is common to give them their own notation. We define

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

and

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

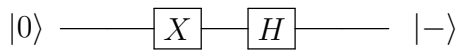
The Hadamard gate has matrix representation

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

1.2.4 Quantum Circuits

Much like in classical computation, it is convenient to represent manipulations of qubits as circuits. A *quantum circuit* is made up of qubits, wires, and gates. It is perhaps easiest to define by giving examples.

Consider the following very simple circuit

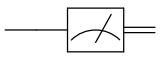


This circuit depicts a single qubit starting in state $|0\rangle$. As it travels through the wire left to right, X takes it to $|1\rangle$ and then H takes $|1\rangle$ to $|-\rangle$. This circuit represents the equation

$$|-\rangle = HX|0\rangle$$

Of course by associativity, we could have used a single gate HX.

We allow for one special gate that is not unitary to denote measurement. The measurement gate is depicted



The two parallel lines indicate that the wire is carrying classical information.

1.2.5 Multiple qubits

Up until this point we have only considered single-qubit systems. However, computation is not very interesting if we're only restricted to a single qubit.

Consider a string of two bits. This string has four possible values: 00, 01, 10, 11. Much like in the single bit case, while a string of two bits has four possible states,

a string of two qubits has four basis states. Keeping with the analogy to bits from before, we number these basis vectors in binary and call them $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ which represent $(1,0,0,0), (0,1,0,0), (0,0,1,0)$, and $(0,0,0,1)$ respectively.

Formally, the state space of two qubits is given by $\mathbb{C}^2 \otimes \mathbb{C}^2$, where $\otimes$ denotes the *tensor product* of two vector spaces. If ψ and φ are two qubits with states $|\psi\rangle$ and $|\varphi\rangle$ respectively, then we denote their combined state $|\psi\rangle |\varphi\rangle := |\psi\rangle \otimes |\varphi\rangle$. It is also common to write $|\psi\varphi\rangle$.

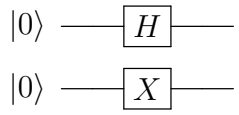
Definition 1.3. Let V and W be vector spaces with bases $\{v_1, ...v_n\}$ and $\{w_1, ...w_m\}$ respectively. Let B be the set of all formal pairs $v_i \otimes w_j$ (read v_i tensor v_j) for each $1 \leq i \leq n$ and $1 \leq j \leq m$.

The *tensor product space* $V \otimes W$ is defined to be the vector space spanned by the basis B.

The tensor product is a complicated construction and defining it in full generality here would take us beyond the scope of this thesis. Luckily, all of the spaces we are working with are finite and we have already chosen bases, so we don't need to worry about this. For the purposes of quantum computing this definition is sufficient.

In general, the combined state space of two quantum systems is given by their tensor product. The state space of an n-qubit system is $\mathbb{C}^{2\otimes n} = \mathbb{C}^2 \otimes \mathbb{C}^2 ... \otimes \mathbb{C}^2$ (n times). A useful way to think about this is that the tensor product combines the two states without adding any relationship between the 2 qubits.

This construction naturally allows us to extend our circuit diagrams to multiple qubits. Consider the following two qubit circuit

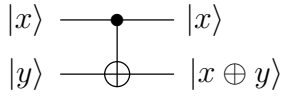


This circuit starts in state $|00\rangle$. The first qubit gets mapped by the Hadamard to $|+\rangle$ and the second qubit is mapped by the X gate to $|1\rangle$. Thus it returns $|+\rangle |1\rangle$. Algebraically, this expresses the equation

$$(H \otimes X)(|00\rangle) = |+\rangle |1\rangle$$

This example could have really just been two single qubit circuits. The two wires run entirely in parallel here. However, most quantum circuits are not like this. Most of the two qubit gates cannot be split up as a product of single qubit gates.

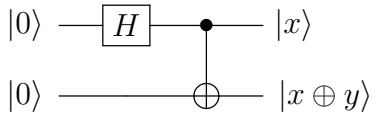
Consider the `Controlled-NOT` gate defined as



It has the following action on the standard basis: If the top register is $|0\rangle$, then the bottom register is unchanged. If the top register is a $|1\rangle$, then it acts as a not gate on the bottom register. Thus it has matrix representation

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

As an example consider the circuit



This circuit starts in state $|00\rangle$. The first timestep applies a Hadamard to the top wire and the identity to the bottom wire, thus it changes the state to $|+\rangle|0\rangle$. To compute the action of the `Controlled-NOT` notice that

$$|+\rangle|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|0\rangle\big) = \frac{1}{\sqrt{2}}\big(|00\rangle + |10\rangle\big)$$

Thus,

$$\texttt{CNOT}|+\rangle|0\rangle = \texttt{CNOT}\frac{1}{\sqrt{2}}\big(|00\rangle + |10\rangle\big) = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

Therefore this circuit sends $|0\rangle|0\rangle$ to $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$.

This state is an example of another important property of quantum systems that cannot be seen with only one qubit. It is what is referred to as an *entangled state* meaning that it has no representation as the product of single qubit states.

1.2.6 Quantum Oracles

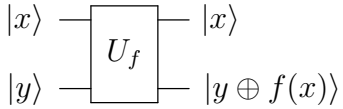
The majority of the problems in quantum computing will be phrased as oracle problems. The motivation for this is that oracle problems are easy to express and of importance classically, yet extend very naturally to analogous problems in the quantum setting.

The way that we give circuits for oracle problems is by adding an extra black-box gate to our collection. The issue here is that the black-box functions in most oracle problems are not unitary and thus not realizable on a quantum computer. The way to fix this, is to encode the oracle function f as a unitary matrix in a fashion similar to the `Controlled-NOT` gate.

Given a function $f : \{0,1\}^n \to \{0,1\}^m$, let $U_f : \mathbb{C}^{2\otimes n} \bigotimes \mathbb{C}^{2\otimes m} \to \mathbb{C}^{2\otimes n} \bigotimes \mathbb{C}^{2\otimes m}$ be the unitary map defined by

$$|x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |x \oplus y\rangle$$

In a circuit we write this as



In this context, the wires labeled $|x\rangle$ and $|y\rangle$ represent the states of potentially multiple qubits and are referred to as *registers*.

1.2.7 Quantum Algorithms

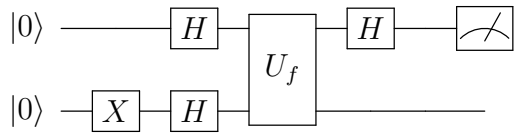
We now present examples of oracle problems that have efficient quantum algorithms.

Deutsch's Algorithm

First, let's revisit the problem given in the beginning this chapter in Example 1. Recall we had the following problem:

Problem 1. Given oracle access to a function $f : \{a, b\} \to \{0, 1\}$. What is the minimum number of queries required to determine $f(a) \oplus f(b)$ where $\oplus$ denotes addition mod 2?

The following quantum circuit is known as *Deutsch's Algorithm*.



The Bernstein-Vazirani Algorithm

Problem 2. Let $s \in \{0, 1\}^m$ be a hidden m-bit binary string and let $b \in \{0, 1\}$ be a hidden bit. Given oracle access to a function $f : \{0, 1\}^n \to \{0, 1\}$ defined by $f(\vec{x}) = \vec{x} \cdot \vec{s} + b \pmod 2$, how many queries are required to determine the values of $\vec{s}$ and b?

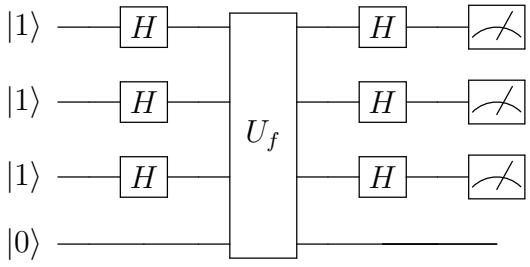
The trick to this problem is to utilize a technique sometimes referred to as *Fourier sampling*.

Note that writing $|+\rangle^{\otimes n}$ in the standard basis yields

$$|+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Where $\{0, 1\}^n$ is the set of all n length binary strings. Thus one can think of the state $|+\rangle^{\otimes n}$ as the generalization of the $|+\rangle$ state to multiple qubits. It is an evenly weighted sum of each of the qubits corresponding to length n binary strings.

Define a circuit with state space $\mathbb{C}^{\otimes 2n} \otimes \mathbb{C}^2$. We initialize the system by setting the first n qubits to $|1\rangle$ and the response qubit to $|0\rangle$.



References

[1] G. James and M. Liebeck. *Representations and Characters of Groups*. Cambridge University Press, 2001.

[2] Andy Matuschak and Michael A. Nielsen. *Quantum Computing for the Very Curious*.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.