Introduction

THE FEATURES OF THE QUANTUM WORLD

In order to learn quantum computing, it is first necessary to become familiar with some basic facts about the quantum world. In this introduction, some unique features of quantum mechanics are introduced, as well as the way they influence the tale we are about to tell.[2]

From Real Numbers to Complex Numbers

Quantum mechanics is different from most other branches of science in that it uses complex numbers in a fundamental way. Complex numbers were originally created as a mathematical curiosity: $i = \sqrt{-1}$ was the asserted "imaginary" solution to the polynomial equation $x^2 = -1$. As time went on, an entire mathematical edifice was constructed with these "imaginary" numbers. Complex numbers have kept lonely mathematicians busy for centuries, while physicists successfully ignored these abstract creations. However, things changed with the systematic study of wave mechanics. After the introduction of Fourier analysis, researchers learned that a compact way to represent a wave was by using functions of complex numbers. As it turns out, this was an important step on the road to using complex numbers in quantum theory. Early quantum mechanics was largely based on wave mechanics.

At first glance, we do not seem to experience complex numbers in the "real world." The length of a rod is a real number, not a complex number. The temperature outside today is 73°, not $(32 - 14i)°$. The amount of time a chemical process takes is 32.543 seconds, not $-14.65i$ seconds. One might wonder what possible role complex numbers can have in any discussion of the physical world. It will soon become apparent that they play an important, indeed an essential, role in quantum mechanics. We shall explore complex numbers in Chapters 1 and 2 of the text.

[2] This Introduction is not the proper place for technical details. Some of the concepts are covered in the text and some of them can be found only in quantum mechanics textbooks. See the end of Chapter 4 for some recommendations of easy, yet detailed, introductions to quantum physics.

From Single States to Superpositions of States

In order to survive in this world, human beings, as infants, must learn that every object exists in a unique place and in a well-defined state, even when we are not looking at it. Although this is true for large objects, quantum mechanics tells us that it is false for objects that are very small. A microscopic object can "hazily" be in more than one place at one time. Rather than an object's being in one position or another, we say that it is in a "superposition," i.e., in some sense, it is simultaneously in more than one location at the same time. Not only is spatial position subject to such "haziness" but so are other familiar physical properties, like energy, momentum, and certain properties that are unique to the quantum world, such as "spin."

We do not actually see superposition of states. Every time we look, or more properly, "measure," a superposition of states, it "collapses" to a single well-defined state. Nevertheless, before we measure it, it is in many states at the same time.

One is justified in greeting these claims with skepticism. After all, how can one believe something different from what every infant knows? However, we will describe certain experiments that show that this is exactly what happens.

From Locality to Nonlocality

Central to modern science is the notion that objects are directly affected only by nearby objects or forces. In order to determine why a phenomenon occurs at a certain place, one must examine all the phenomena and forces near[3] that place. This is called "locality," i.e., the laws of physics work in a local way. One of the most remarkable aspects of quantum mechanics is that its laws predict certain effects that work in a nonlocal manner. Two particles can be connected or "entangled" in such a way that an action performed on one of them can have an immediate effect on the other particle light-years away. This "spooky action at a distance," to use Einstein's colorful expression, was one of the most shocking discoveries of quantum mechanics.

From Deterministic Laws to Probabilistic Laws

To which specific state will a superposition of states collapse when it is measured? Whereas in other branches of physics the laws are deterministic,[4] i.e., there is a unique outcome to every experiment, the laws of quantum mechanics state that we can only know the probability of the outcome. This, again, might seem dubious. It was doubted by the leading researchers of the time. Einstein himself was skeptical and coined the colorful expression "God does not play dice with the Universe" to express this. However, because of repeated experimental confirmations, the probabilistic nature of quantum mechanics is no longer in question.

[3] By "near" we mean anything close enough to affect the object. In physics jargon, anything in the past light cone of the object.
[4] Statistical mechanics being one major exception.

From Certainty to Uncertainty

The laws of quantum mechanics also inform us that there are inherent limitations to the amount of knowledge that one can ascertain about a physical system. The primary example of such a limitation is the famous "Heisenberg's uncertainty principle."

There are other important features of the quantum world that we shall not explore here. These different features were all motivating forces behind the advent of quantum computing. Rather than an historical review of how these features affected quantum computing, let us look at several areas in computer science and see how the aforementioned features affected each of those areas.[5]

THE IMPLICATIONS OF THE QUANTUM WORLD ON COMPUTER SCIENCE

Architecture

The concept of superposition will be used to generalize the notion of bit to its quantum analog, the qubit. Whereas a bit can be in either one of two states, superposition will allow a qubit to be both states simultaneously. Putting many qubits together gives us quantum registers. It is this superposition that is the basis for quantum computing's real power. Rather than being in one state at a time, a quantum computer can be in many states simultaneously.

After generalizing the notion of bit, the notion of a gate that manipulates bits will be extended to the quantum setting. We shall have quantum gates that manipulate qubits. Quantum gates will have to follow the dynamics of quantum operations. In particular, certain quantum operations are reversible, and hence certain quantum gates will have to be reversible.[6]

Algorithms

The field of quantum algorithms uses superposition in a fundamental way. Rather than having a computer in one state at a time, one employs that aspect of the quantum world to place a quantum computer in many states simultaneously. One might think of this as massive parallelism. This needs special care: we cannot measure the computer while it is in this superposition because measuring it would collapse it to a single position. Our algorithms will start with the quantum computer in a single position. We shall then delicately place it in a superposition of many states. From there, we manipulate the qubits in a specified way. Finally, (some of) the qubits are measured. The measurement will collapse the qubits to the desired bits, which will be our output.

[5] For an historical view of quantum computing as seen through the major papers that launched the subject, see Appendix A.

[6] It so happens that reversible computation has a long history predating quantum computing. This history will be reviewed in due course.

Entanglement will also play a role in quantum computing, as the qubits can be entangled. By measuring some of them, others automatically reach the desired position.

Consider searching for a particular object in an unordered array. A classical algorithm examines the first entry in the array, then the second entry, and so on. The algorithm stops when either the object is found or the end of the array is reached. So for an array with n elements, in the worst-case scenario, an algorithm would have to look at n entries of the array.

Now imagine a computer that uses superposition. Rather than having the machine look at this entry or that entry, let it look at *all* entries simultaneously. This will result in a fantastic speedup. It turns out that such a quantum computer will be able to find the object in $\sqrt{n}$ queries to the array. This is one of the first quantum algorithms and is called "Grover's algorithm."

Another algorithm that demonstrates the power and usefulness of quantum computing is Shor's algorithm for factoring numbers. The usual algorithm to factor a number involves looking at many possible factors of the number until a true factor is found. Shor's algorithm uses superposition (and a touch of number theory) to look at many possible factors simultaneously.

Shor's algorithm is partially based on earlier quantum algorithms that were created to solve slightly contrived problems. Although these earlier algorithms (Deutch, Deutch-Joza, and Simon's periodicity algorithm) solve artificial problems, we shall study them so that we can learn different techniques of quantum software design.

Programming Languages

Algorithms must eventually develop into concrete software if they are to be useful in real-life applications. The bridge that makes this step possible is programming. Quantum computing is no exception: researchers in the field have started designing quantum programming languages that will enable future generations of programmers to take control of quantum hardware and implement new quantum algorithms. We shall introduce a brief survey of programming languages (for the first time, to our knowledge, in a quantum computing textbook), starting with quantum assembler and progressing to high-level quantum programming, in particular quantum functional programming.

Theoretical Computer Science

The goal of theoretical computer science is to formalize what engineers have done, and more important, to formalize what the engineers *cannot* do. Such an analysis is carried out by describing and classifying theoretical models of computation. The superposition of quantum mechanics has a vague feel of nondeterminism that theoretical computer scientists have used (of course, nondeterminism is a purely fictional concept and superposition is an established fact of the physical world). The indeterminacy of which state the superposition will collapse to is related to a probabilistic computation. We will be led to generalize the definition of a Turing machine to that

of a quantum Turing machine. With a clear definition in place, we will be able to classify and relate all these different ideas.

We shall not only be interested in what a quantum Turing machine can do. We are also interested in the question of efficiency. This brings us to quantum complexity theory. Definitions of quantum complexity classes will be given and will be related to other well-known complexity classes.

Cryptography

Indeterminacy and superposition will be used in quantum versions of public key distribution protocols. The fact that a measurement disturbs a quantum state shall be used to detect the presence of an eavesdropper listening in on (measuring) a communication channel. Such detection is not easily achievable in classical cryptography. Whereas classical public key distribution protocols rely on the fact that certain inverse functions are computationally hard to calculate, quantum key distribution protocols are based on the fact that certain laws of quantum physics are true. It is this strength that makes quantum cryptography so interesting and powerful.

There is also a public key protocol that uses entanglement in a fundamental way. Related to cryptography is teleportation. In teleportation, a state of a system is transported as opposed to a message. The teleportation protocol uses entangled particles that can be separated across the universe.

The most amazing part of quantum cryptography is that it is not only a theoretical curiosity. There are, in fact, actual commercially available quantum cryptography devices currently in use.

Information Theory

It is impossible to discuss topics such as compression, transmission, and storage, without mentioning information. Information theory, now an established field, was introduced by Claude Shannon in the forties, and has developed a vast array of techniques and ideas that find their use in computer science and engineering. As this book deals with quantum computation, it is imperative that we ask: is there a satisfactory notion of quantum information? What is the information content encoded by a stream of qubits? It turns out that such notions exist. Just as classical information is related to measures of order (the so-called entropy of a source of signals), quantum information is paired with the notion of quantum entropy. We shall explore, chiefly through examples, how order and information in the quantum realm differ from familiar notions, and how these differences can be exploited to achieve new results in data storage, transmission, and compression.

Hardware

There is no future for quantum computing without quantum computers. We are going to spell out the challenges behind the implementation of quantum machines, especially one that is embedded in the very nature of the quantum world: decoherence.

We shall also describe the desirable features that a prospective quantum machine must exhibit in order to be useful.

A few proposals for quantum hardware will be showcased. The emphasis here is not on technical details (this is a book for computer scientists, not a quantum engineering handbook!). Instead, our goal is to convey the gist of these proposals and their chances of success as they are currently assessed.

1

Complex Numbers

You, have you really understood all that stuff?
What?
The story of imaginary numbers?

Robert Musil, *The Confusions of Young Törless* (1907)[1]

Complex numbers lie at the very core of quantum mechanics and are therefore absolutely essential to a basic understanding of quantum computation. In this chapter we present this important system of numbers from both the algebraic and the geometric standpoints. Section 1.1 presents some motivation and the basic definitions. The algebraic structure and operations on complex numbers are given in Section 1.2. The chapter concludes with Section 1.3, where complex numbers are presented from a geometric point of view and advanced topics are discussed. Our hope is that this chapter will help you get a little closer to what Sir Roger Penrose has very aptly called the "magic of complex numbers" (Penrose, 2005).

Reader Tip. Many readers will find that they are already familiar with some of the material presented in this chapter. The reader who feels confident in her comprehension of the fundamental knowledge of complex numbers, the basic operations, and their properties can safely move on to later chapters. We suggest, though, that you at least skim through the following pages to see what topics are covered. Return to Chapter 1 as a reference when needed (using the index to find specific topics). ♡

[1] For the German-speaking reader, here is the original text (the translation at the beginning is ours):

Du, hast du das vorhin ganz verstanden?
Was?
Die Geschichte mit den imaginären Zahlen?

Musil's *Törless* is a remarkable book. A substantial part is dedicated to the struggle of young Törless to come to grips with mathematics, as well as with his own life. Definitely recommended!

1.1 BASIC DEFINITIONS

The original motivation for the introduction of complex numbers was the theory of algebraic equations, the part of algebra that seeks solutions of polynomial equations. It became readily apparent that there are plenty of cases in which no solution among familiar numbers can be found. Here is the simplest example:

$$x^2 + 1 = 0. \tag{1.1}$$

Indeed, any possible x^2 would be positive or zero. Adding 1 ends up with some quantity to the left that is strictly positive; hence, no solution exists.

Exercise 1.1.1 Verify that the equation $x^4 + 2x^2 + 1 = 0$ has no solution among the real numbers. (Hint: Factor the polynomial.) ■

The aforementioned argument seems to dash any hope of solving Equation (1.1). But does it?

Before building any new number system, it pays to remind ourselves of other sets of numbers that we usually work with

- positive numbers, $\mathbb{P} = \{1, 2, 3, \ldots\}$;
- natural numbers, $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$;
- integers (or whole numbers), $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$;
- rational numbers, $\mathbb{Q} = \left\{\frac{m}{n} | m \in \mathbb{Z}, n \in \mathbb{P}\right\}$;
- real numbers, $\mathbb{R} = \mathbb{Q} \bigcup \{\ldots, \sqrt{2}, \ldots, e, \ldots, \pi, \ldots, \frac{e}{\pi} \ldots\}$;

In none of these familiar number systems can a valid solution to Equation (1.1) be found. Mathematics often works around difficulties by simply *postulating* that such a solution, albeit unknown, is available somewhere. Let us thus boldly assume that this enigmatic solution does indeed exist and determine what it looks like: Equation (1.1) is equivalent to

$$x^2 = -1. \tag{1.2}$$

What does this state? That the solution of Equation (1.1) is a number such that its square is -1, i.e., a number i such that

$$i^2 = -1 \quad \text{or} \quad i = \sqrt{-1}. \tag{1.3}$$

Of course we know that no such number exists among known (i.e., real) numbers, but we have already stated that this is not going to deter us. We will simply allow this new creature into the realm of well-established numbers and use it as it pleases us. Because it is *imaginary*, it is denoted i. We will impose on ourselves an important restriction: aside from its weird behavior when squared, i will behave just like an ordinary number.

Example 1.1.1 What is the value of i^3? We shall treat i as a legitimate number, so

$$i^3 = i \times i \times i = (i^2) \times i = -1 \times i = -i. \tag{1.4}$$

□

Exercise 1.1.2 Find the value of i^{15}. (Hint: Calculate i, i^2, i^3, i^4, and i^5. Find a pattern.) ■

In opening the door to our new friend i, we are now flooded with an entire universe of new numbers: to begin with, all the multiples of i by a real number, like $2 \times i$. These fellows, being akin to i, are known as **imaginary numbers**. But there is more: add a real number and an imaginary number, for instance, $3 + 5 \times i$, and you get a number that is neither a real nor an imaginary. Such a number, being a hybrid entity, is rightfully called a **complex number**.

Definition 1.1.1 *A* complex number *is an expression*

$$c = a + b \times i = a + bi, \tag{1.5}$$

where a, b are two real numbers; a is called the real part of c, whereas b is its imaginary part. The set of all complex numbers will be denoted as $\mathbb{C}$. When the $\times$ is understood, we shall omit it.

Complex numbers can be added and multiplied, as shown next.

Example 1.1.2 Let $c_1 = 3 - i$ and $c_2 = 1 + 4i$. We want to compute $c_1 + c_2$ and $c_1 \times c_2$.

$$c_1 + c_2 = 3 - i + 1 + 4i = (3 + 1) + (-1 + 4)i = 4 + 3i. \tag{1.6}$$

Multiplying is not as easy. We must remember to multiply each term of the first complex number with each term of the second complex number. Also, remember that $i^2 = -1$.

$$\begin{aligned} c_1 \times c_2 &= (3 - i) \times (1 + 4i) = (3 \times 1) + (3 \times 4i) + (-i \times 1) + (-i \times 4i) \\ &= (3 + 4) + (-1 + 12)i = 7 + 11i. \end{aligned} \tag{1.7}$$

□

Exercise 1.1.3 Let $c_1 = -3 + i$ and $c_2 = 2 - 4i$. Calculate $c_1 + c_2$ and $c_1 \times c_2$. ■

With addition and multiplication we can get all polynomials. We set out to find a solution for Equation (1.1); it turns out that complex numbers are enough to provide solutions for *all* polynomial equations.

Proposition 1.1.1 (Fundamental Theorem of Algebra). Every polynomial equation of one variable with complex coefficients has a complex solution.

Exercise 1.1.4 Verify that the complex number $-1 + i$ is a solution for the polynomial equation $x^2 + 2x + 2 = 0$. ■

This nontrivial result shows that complex numbers are well worth our attention. In the next two sections, we explore the complex kingdom a little further.

Programming Drill 1.1.1 *Write a program that accepts two complex numbers and outputs their sum and their product.*

1.2 THE ALGEBRA OF COMPLEX NUMBERS

Admittedly, the fact that we know how to handle them does not explain away the oddity of complex numbers. What *are* they? What does it mean that i squared is equal to -1?

In the next section, we see that the geometrical viewpoint greatly aids our intuition. Meanwhile, we would like to convert complex numbers into more familiar objects by carefully looking at how they are built.

Definition 1.1.1 tells us *two* real numbers correspond to each complex number: its real and imaginary parts. A complex number is thus a two-pronged entity, carrying its two components along. How about *defining* a complex number as an ordered pair of reals?

$$c \longmapsto (a, b). \tag{1.8}$$

Ordinary real numbers can be identified with pairs $(a, 0)$

$$a \longmapsto (a, 0), \tag{1.9}$$

whereas imaginary numbers will be pairs $(0, b)$. In particular,

$$i \longmapsto (0, 1). \tag{1.10}$$

Addition is rather obvious – it adds pairs componentwise:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2). \tag{1.11}$$

Multiplication is a little trickier:

$$(a_1, b_1) \times (a_2, b_2) = (a_1, b_1)(a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1). \tag{1.12}$$

Does this work? Multiplying i by itself gives

$$i \times i = (0, 1) \times (0, 1) = (0 - 1, 0 + 0) = (-1, 0), \tag{1.13}$$

which is what we wanted.

Using addition and multiplication, we can write any complex number in the usual form:

$$c = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \times (0, 1) = a + bi. \tag{1.14}$$

We have traded one oddity for another: i was previously quite mysterious, whereas now it is just $(0, 1)$. A complex number is nothing more than an ordered pair of ordinary real numbers. Multiplication, though, is rather strange: perhaps the reader would have expected a componentwise multiplication, just like addition. We shall see later that by viewing complex numbers through yet another looking glass the strangeness linked to their multiplication rule will fade away.

Example 1.2.1 Let $c_1 = (3, -2)$ and $c_2 = (1, 2)$. Let us multiply them using the aforementioned rule:

$$\begin{aligned} c_1 \times c_2 &= (3 \times 1 - (-2) \times 2, -2 \times 1 + 2 \times 3) \\ &= (3 + 4, -2 + 6) = (7, 4) = 7 + 4i. \end{aligned} \tag{1.15}$$

□