1 Introduction

In the last decades of the twentieth century, scientists sought to combine two of the century's most influential and revolutionary theories: information theory and quantum mechanics. Their success gave rise to a new view of computation and information. This new view, quantum information theory, changed forever how computation, information, and their connections with physics are thought about, and it inspired novel applications, including some wildly different algorithms and protocols. This view and the applications it spawned are the subject of this book.

Information theory, which includes the foundations of both computer science and communications, abstracted away the physical world so effectively that it became possible to talk about the major issues within computer science and communications, such as the efficiency of an algorithm or the robustness of a communication protocol, without understanding details of the physical devices used for the computation or the communication. This ability to ignore the underlying physics proved extremely powerful, and its success can be seen in the ubiquity of the computing and communications devices around us. The abstraction away from the physical had become such a part of the intellectual landscape that the assumptions behind it were almost forgotten. At its heart, until recently, information sciences have been firmly rooted in classical mechanics. For example, the Turing machine is a classical mechanical model that behaves according to purely classical mechanical principles.

Quantum mechanics has played an ever-increasing role in the development of new and more efficient computing devices. Quantum mechanics underlies the working of traditional, classical computers and communication devices, from the transistor through the laser to the latest hardware advances that increase the speed and power and decrease the size of computer and communications components. Until recently, the influence of quantum mechanics remained confined to the low-level implementation realm; it had no effect on how computation or communication was thought of or studied.

In the early 1980s, a few researchers realized that quantum mechanics had unanticipated implications for information processing. Charles Bennett and Gilles Brassard, building on ideas of Stephen Wiesner, showed how nonclassical properties of quantum measurement provided a provably secure mechanism for establishing a cryptographic key. Richard Feynman, Yuri Manin, and others recognized that certain quantum phenomena—phenomena associated with so-called

entangled particles—could not be simulated efficiently by a Turing machine. This observation led to speculation that perhaps these quantum phenomena could be used to speed up computation in general. Such a program required rethinking the information theoretic model underlying computation, taking it out of the purely classical realm.

Quantum information processing, a field that includes quantum computing, quantum cryptography, quantum communications, and quantum games, explores the implications of using quantum mechanics instead of classical mechanics to model information and its processing. Quantum computing is not about changing the physical substrate on which computation is done from classical to quantum, but rather changing the notion of computation itself. The change starts at the most basic level: the fundamental unit of computation is no longer the bit, but rather the quantum bit or qubit. Placing computation on a quantum mechanical foundation led to the discovery of faster algorithms, novel cryptographic mechanisms, and improved communication protocols.

The phrase *quantum computing* does not parallel the phrases *DNA computing* or *optical computing*: these describe the substrate on which computation is done without changing the notion of computation. *Classical computers*, the ones we all have on our desks, make use of quantum mechanics, but they compute using bits, not qubits. For this reason, they are not considered quantum computers. A quantum or classical computer may or may not be an optical computer, depending on whether optical devices are used to carry out the computation. Whether the computer is quantum or classical depends on whether the information is represented and manipulated in a quantum or classical way. The phrase *quantum computing* is closer in character to *analog computing* because the computational model for analog computing differs from that of standard computing: a continuum of values, rather than only a discrete set, is allowed. While the phrases are parallel, the two models differ greatly in that analog computation does not support entanglement, a key resource for quantum computation, and measurements of a quantum computer's registers can yield only a small, discrete set of values. Furthermore, while a qubit can take on a continuum of values, in many ways a qubit resembles a bit, with its two discrete values, more than it does analog computation. For example, as we will see in section 4.3.1, only one bit's worth of information can be extracted from a qubit by measurement.

The field of quantum information processing developed slowly in the 1980s and early 1990s as a small group of researchers worked out a theory of quantum information and quantum information processing. David Deutsch developed a notion of a quantum mechanical Turing machine. Daniel Bernstein, Vijay Vazirani, and Andrew Yao improved upon his model and showed that a quantum Turing machine could simulate a classical Turing machine, and hence any classical computation, with at most a polynomial time slowdown. The standard quantum circuit model was then defined, which led to an understanding of quantum complexity in terms of a set of basic quantum transformations called quantum gates. These gates are theoretical constructs that may or may not have direct analogs in the physical components of an actual quantum computer.

In the early 1990s, researchers developed the first truly quantum algorithms. In spite of the probabilistic nature of quantum mechanics, the first quantum algorithms, for which superiority

over classical algorithms could be proved, give the correct answer with certainty. They improve upon classical algorithms by solving in polynomial time with certainty a problem that can be solved in polynomial time only with high probability using classical techniques. Such a result is of no direct practical interest, since the impossibility of building a perfect machine reduces any practical machine running any algorithm to solving a problem only with high probability. But such results were of high theoretical interest, since they showed for the first time that quantum computation is theoretically more powerful than classical computation for certain computational problems.

These results caught the interest of various researchers, including Peter Shor, who in 1994 surprised the world with his polynomial-time quantum algorithm for factoring integers. This result provided a solution to a well-studied problem of practical interest. A classical polynomial-time solution had long been sought, to the point where the world felt sufficiently confident that no such solution existed that many security protocols, including the widely used RSA algorithm, base their security entirely on the computational difficulty of this problem. It is unknown whether an efficient classical solution exists, so Shor's result does not prove that quantum computers can solve a problem more efficiently than a classical computer. But even in the unlikely event that a polynomial-time classical algorithm is found for this problem, it would be an indication of the elegance and effectiveness of the quantum information theory point of view that a quantum algorithm, in spite of all the unintuitive aspects of quantum mechanics, was easier to find.

While Shor's result sparked a lot of interest in the field, doubts as to its practical significance remained. Quantum systems are notoriously fragile. Key properties, such as quantum entanglement, are easily disturbed by environmental influences that cause the quantum states to *decohere*. Properties of quantum mechanics, such as the impossibility of reliably copying an unknown quantum state, made it look unlikely that effective error-correction techniques for quantum computation could ever be found. For these reasons, it seemed unlikely that reliable quantum computers could be built.

Luckily, in spite of serious and widespread doubts as to whether quantum information processing could ever be practical, the theory itself proved so tantalizing that researchers continued to explore it. As a result, in 1996 Shor and Robert Calderbank, and independently Andrew Steane, saw a way to finesse the seemingly show-stopping problems of quantum mechanics to develop quantum error correction techniques. Today, quantum error correction is arguably the most mature area of quantum information processing.

How practical quantum computing and quantum information will turn out is still unknown. No fundamental physical principles are known that prohibit the building of large-scale and reliable quantum computers. Engineering issues, however, remain. As of this writing, laboratory experiments have demonstrated quantum computations with several quantum bits performing dozens of quantum operations. Myriad promising approaches are being explored by theorists and experimentalists around the world, but much uncertainty remains as to how, when, or even whether, a quantum computer capable of carrying out general quantum computations on hundreds of qubits will be built.

Quantum computational approaches improve upon classical methods for a number of specialized tasks. The extent of quantum computing's applicability is still being determined. It does not provide efficient solutions to all problems; neither does it provide a universal way of circumventing the slowing of Moore's law. Strong limitations on the power of quantum computation are known; for many problems, it has been proven that quantum computation provides no significant advantage over classical computation. Grover's algorithm, the other major algorithm of the mid-1990s, provides a small speedup for unstructured search algorithms. But it is also known that this small speedup is the most that quantum algorithms can attain. Grover's search algorithm applies to unstructured search. For other search problems, such as searching an ordered list, quantum computation provides no significant advantage over classical computation. Simulation of quantum systems is the other significant application of quantum computation known in the mid-1990s. Of interest in its own right, the simulation of increasingly larger quantum systems may provide a bootstrap that will ultimately lead to the building of a scalable quantum computer.

After Grover's algorithm, there was a hiatus of more than five years before a significantly new algorithm was discovered. During that time, other areas of quantum information processing, such as quantum error correction, advanced significantly. In the early 2000s, several new algorithms were discovered. Like Shor's algorithm, these algorithms solve specific problems with narrow, if important, applications. Novel approaches to constructing quantum algorithms also developed. Investigations of quantum simulation from a quantum-information-processing point of view have led to improved classical techniques for simulating quantum systems, as well as novel quantum approaches. Similarly, the quantum-information-processing point of view has led to novel insights into classical computing, including new classical algorithms. Furthermore, alternatives to the standard circuit model of quantum computation have been developed that have led to new quantum algorithms, breakthroughs in building quantum computers, new approaches to robustness, and significant insights into the key elements of quantum computation.

However long it takes to build a scalable quantum computer and whatever the breadth of applications turns out to be, quantum information processing has changed forever the way in which quantum physics is understood. The quantum information processing view of quantum mechanics has done much to clarify the character of key aspects of quantum mechanics such as quantum measurement and entanglement. This advancement in knowledge has already had applications outside of quantum information processing to the creation of highly entangled states used for microlithography at scales below the wavelength limit and for extraordinarily accurate sensors. The precise practical consequences of this increased understanding of nature are hard to predict, but the unification of the two theories that had the most profound influence on the technological advances of the twentieth century can hardly fail to have profound effects on technological and intellectual developments throughout the twenty-first.

Part I of this book covers the basic building blocks of quantum information processing: quantum bits and quantum gates. Physical motivation for these building blocks is given and tied to the key quantum concepts of quantum measurement, quantum state transformations, and entanglement between quantum subsystems. Each of these concepts is explored in depth. Quantum key

distribution, quantum teleportation, and quantum dense coding are introduced along the way. The final chapter of part I shows that anything that can be done on a classical computer can be done with comparable efficiency on a quantum computer.

Part II covers quantum algorithms. It begins with a description of some of the most common elements of quantum computation. Since the advantage of quantum computation over classical computation is all about efficiency, part II carefully defines notions of complexity. Part II also discusses known bounds on the power of quantum computation. A number of simple algorithms are described. Full chapters are devoted to Shor's algorithm and Grover's algorithm.

Part III explores entanglement and robust quantum computation. A discussion of quantum subsystems leads into discussions of quantifying entanglement and of decoherence, the environmental errors affecting a quantum system because it is really a part of a larger quantum system. The elegant and important topic of quantum error correction fills a chapter, followed by a chapter on techniques to achieve fault tolerance. The book finishes with brief descriptions and pointers to references for many quantum information processing topics the book could not cover in depth. These include further quantum algorithms and protocols, adiabatic, cluster state, holonomic, and topological quantum computing, and the impact quantum information processing has had on classical computer science and physics.

2 Single-Qubit Quantum Systems

Quantum bits are the fundamental units of information in quantum information processing in much the same way that bits are the fundamental units of information for classical processing. Just as there are many ways to realize classical bits physically (two voltage levels, lights on or off in an array, positions of toggle switches), there are many ways to realize quantum bits physically. As is done in classical computer science, we will concern ourselves only rarely with how the quantum bits are realized. For the sake of concretely illustrating quantum bits and their properties, however, section 2.1 looks at the behavior of polarized photons, one of many possible realizations of quantum bits.

Section 2.2 abstracts key properties from the polarized photon example of section 2.1 to give a precise definition of a quantum bit, or qubit, and a description of the behavior of quantum bits under measurement. Dirac's bra / ket notation, the standard notation used throughout quantum information processing as well as quantum mechanics, is introduced in this section. Section 2.4 describes the first application of quantum information processing: quantum key distribution. The chapter concludes with a detailed discussion of the state space of a single-qubit system.

2.1 The Quantum Mechanics of Photon Polarization

A simple experiment illustrates some of the nonintuitive behavior of quantum systems, behavior that is exploited to good effect in quantum algorithms and protocols. This experiment can be performed by the reader using only minimal equipment: a laser pointer and three polaroids (polarization filters), readily available from any camera supply store. The formalisms of quantum mechanics that describe this simple experiment lead directly to a description of the quantum bit, the fundamental unit of quantum information on which quantum information processing is done. The experiment not only gives a concrete realization of a quantum bit, but it also illustrates key properties of quantum measurement. We encourage you to obtain the equipment and perform the experiment yourself.

photons with associated basis $\{|u\rangle, |u^{\perp}\rangle\}$, the state $|v\rangle = a|u\rangle + b|u^{\perp}\rangle$ is measured as $|u\rangle$ with probability $|a|^2$ and as $|u^{\perp}\rangle$ with probability $|b|^2$.

This behavior of measurement is an axiom of quantum mechanics. It is not derivable from other physical principles; rather, it is derived from the empirical observation of experiments with measuring devices. If quantum mechanics is correct, all devices that measure single qubits must behave in this way; all have associated bases, and the measurement outcome is always one of the two basis vectors. For this reason, whenever anyone says "measure a qubit," they must specify with respect to which basis the measurement takes place. Throughout the book, if we say "measure a qubit" without further elaboration, we mean that the measurement is with respect to the standard basis $\{|0\rangle, |1\rangle\}$.

Measurement of a quantum state changes the state. If a state $|v\rangle = a|u\rangle + b|u^{\perp}\rangle$ is measured as $|u\rangle$, then the state $|v\rangle$ changes to $|u\rangle$. A second measurement with respect to the same basis will return $|u\rangle$ with probability 1. Thus, unless the original state happens to be one of the basis states, a single measurement will change that state, making it impossible to determine the original state from any sequence of measurements.

While the mathematics of measuring a qubit in the superposition state $a|0\rangle + b|1\rangle$ with respect to the standard basis is clear, measurement brings up questions as to the meaning of a superposition. To begin with, the notion of superposition is basis-dependent; all states are superpositions with respect to some bases and not with respect to others. For instance, $a|0\rangle + b|1\rangle$ is a superposition with respect to the basis $\{|0\rangle, |1\rangle\}$ but not with respect to $\{a|0\rangle + b|1\rangle, \overline{b}|0\rangle - \overline{a}|1\rangle\}$.

Also, because the result of measuring a superposition is probabilistic, some people are tempted to think of the state $|v\rangle = a|0\rangle + b|1\rangle$ as a probabilistic mixture of $|0\rangle$ and $|1\rangle$. It is not. In particular, it is not true that the state is really either $|0\rangle$ or $|1\rangle$ and that we just do not happen to know which. Rather, $|v\rangle$ is a definite state, which, when measured in certain bases, gives deterministic results, while in others it gives random results: a photon with polarization $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)$ behaves deterministically when measured with respect to the Hadamard basis $\{|\nearrow\rangle, |\nwarrow\rangle\}$, but it gives random results when measured with respect to the standard basis $\{|\uparrow\rangle, |\rightarrow\rangle\}$. It is okay to think of a superposition $|v\rangle = a|0\rangle + b|1\rangle$ as in some sense being in both state $|0\rangle$ and state $|1\rangle$ at the same time, as long as that statement is not taken too literally: states that are combinations of $|0\rangle$ and $|1\rangle$ in similar proportions but with different amplitudes, such as $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle + \mathbf{i}|1\rangle)$, represent distinct states that behave differently in many situations.

Given that qubits can take on any one of infinitely many states, one might hope that a single qubit could store lots of classical information. However, the properties of quantum measurement severely restrict the amount of information that can be extracted from a qubit. Information about a quantum bit can be obtained only by measurement, and any measurement results in one of only two states, the two basis states associated with the measuring device; thus, a single measurement yields at most a single classical bit of information. Because measurement changes the state, one cannot make two measurements on the original state of a qubit. Furthermore, section 5.1.1 shows that an unknown quantum state cannot be cloned, which means it is not possible to measure a qubit's state in two ways, even indirectly by copying the qubit's state and measuring the copy.

Thus, even though a quantum bit can be in infinitely many different superposition states, it is possible to extract only a single classical bit's worth of information from a single quantum bit.

2.4 A Quantum Key Distribution Protocol

The quantum theory introduced so far is sufficient to describe a first application of quantum information processing: a key distribution protocol that relies on quantum effects for its security and for which there is no classical analog.

Keys—binary strings or numbers chosen randomly from a sufficiently large set—provide the security for most cryptographic protocols, from encryption to authentication to secret sharing. For this reason, the establishment of keys between the parties who wish to communicate is of fundamental importance in cryptography. Two general classes of keys exist: symmetric keys and public-private key pairs. Both types are used widely, often in conjunction, in a wide variety of practical settings, from secure e-commerce transactions to private communication over public networks.

Public-private key pairs consist of a public key, knowable by all, and a corresponding private key whose secrecy must be carefully guarded by the owner. Symmetric keys consist of a single key (or a pair of keys easily computable from one another) that are known to all of the legitimate parties and no one else. In the symmetric key case, multiple parties are responsible for guarding the security of the key.

Quantum key distribution protocols establish a symmetric key between two parties, who are generally known in the cryptographic community as Alice and Bob. Quantum key distribution protocols can be used securely anywhere classical key agreement protocols such as Diffie-Hellman can be used. They perform the same task; however, the security of quantum key distribution rests on fundamental properties of quantum mechanics, whereas classical key agreement protocols rely on the computational intractability of a certain problem. For example, while Diffie-Hellman remains secure against all known classical attacks, the problem on which it is based, the discrete logarithm problem, is tractable on a quantum computer. Section 8.6.1 discusses Shor's quantum algorithm for the discrete log problem.

The earliest quantum key distribution protocol is known as BB84 after its inventors, Charles Bennett and Gilles Brassard, and the year of the invention. The aim of the BB84 protocol is to establish a secret key, a random sequence of bit values 0 and 1, known only to the two parties, Alice and Bob, who may use this key to support a cryptographic task such as exchanging secret messages or detecting tampering. The BB84 protocol enables Alice and Bob to be sure that if they detect no problems while attempting to establish a key, then with high probability it is secret. The protocol does not guarantee, however, that they will succeed in establishing a private key.

Suppose Alice and Bob are connected by two public channels: an ordinary bidirectional classical channel and a unidirectional quantum channel. The quantum channel allows Alice to send a sequence of single qubits to Bob; in our case we suppose the qubits are encoded in the polarization states of individual photons. Both channels can be observed by an eavesdropper Eve. This situation