Part I

Introduction

1 Concepts in Quantum Shannon Theory

In these first few chapters, our aim is to establish a firm grounding so that we can address some fundamental questions regarding information transmission over quantum channels. This area of study has become known as "quantum Shannon theory" in the broader quantum information community, in order to distinguish this topic from other areas of study in quantum information science. In this text, we will use the terms "quantum Shannon theory" and "quantum information theory" somewhat interchangeably. We will begin by briefly overviewing several fundamental aspects of the quantum theory. Our study of the quantum theory, in this chapter and future ones, will be at an abstract level, without giving preference to any particular physical system such as a spin-1/2 particle or a photon. This approach will be more beneficial for the purposes of our study, but, here and there, we will make some reference to actual physical systems to ground us in reality.

You may be wondering, what is *quantum Shannon theory* and why do we name this area of study as such? In short, quantum Shannon theory is the study of the ultimate capability of noisy physical systems, governed by the laws of quantum mechanics, to preserve information and correlations. Quantum information theorists have chosen the name *quantum Shannon theory* to honor Claude Shannon, who single-handedly founded the field of classical information theory, with a groundbreaking 1948 paper (Shannon, 1948). In particular, the name refers to the asymptotic theory of quantum information, which is the main topic of study in this book. Information theorists since Shannon have dubbed him the "Einstein of the information age."[1] The name *quantum Shannon theory* is fit to capture this area of study because we use quantum versions of Shannon's ideas to prove some of the main theorems in quantum Shannon theory.

We prefer the title "quantum Shannon theory" over such titles as "quantum information science" or just "quantum information." These other titles are too broad, encompassing subjects as diverse as quantum computation, quantum algorithms, quantum complexity theory, quantum communication complexity, entanglement theory, quantum key distribution, quantum error correction, and even the experimental implementation of quantum protocols. Quantum Shannon

[1] It is worthwhile to look up "Claude Shannon—Father of the Information Age" on YouTube and watch several renowned information theorists speak with awe about "the founding father" of information theory.

theory does overlap with some of the aforementioned subjects, such as quantum computation, entanglement theory, quantum key distribution, and quantum error correction, but the name "quantum Shannon theory" should evoke a certain paradigm for quantum communication with which the reader will become intimately familiar after some exposure to the topics in this book. For example, it is necessary for us to discuss *quantum gates* (a topic in quantum computing) because quantum Shannon-theoretic protocols exploit them to achieve certain information-processing tasks. Also, in Chapter 22, we are interested in the ultimate limitation on the ability of a noisy quantum communication channel to transmit private information (information that is secret from any third party besides the intended receiver). This topic connects quantum Shannon theory with quantum key distribution because the private information capacity of a noisy quantum channel is strongly related to the task of using the quantum channel to distribute a secret key. As a final connection, perhaps the most important theorem of quantum Shannon theory is the *quantum capacity theorem*. This theorem determines the ultimate rate at which a sender can reliably transmit quantum information over a quantum channel to a receiver. The result provided by the quantum capacity theorem is closely related to the theory of quantum error correction, but the mathematical techniques used in quantum Shannon theory and in quantum error correction are so different that these subjects merit different courses of study.

Quantum Shannon theory intersects two of the great sciences of the twentieth century: the quantum theory and information theory. It was really only a matter of time before physicists, mathematicians, computer scientists, and engineers began to consider the convergence of the two subjects because the quantum theory was essentially established by 1926 and information theory by 1948. This convergence has sparked what we may call the "quantum information revolution" or what some refer to as the "second quantum revolution" (Dowling & Milburn, 2003) (with the first one being the discovery of the quantum theory).

The fundamental components of the quantum theory are a set of postulates that govern phenomena on the scale of atoms. Uncertainty is at the heart of the quantum theory—"quantum uncertainty" or "Heisenberg uncertainty" is not due to our lack or loss of information or due to imprecise measurement capability, but rather, it is a fundamental uncertainty inherent in nature itself. The discovery of the quantum theory came about as a total shock to the physics community, shaking the foundations of scientific knowledge. Perhaps it is for this reason that every introductory quantum mechanics course delves into its history in detail and celebrates the founding fathers of the quantum theory. In this book, we do not discuss the history of the quantum theory in much detail and instead refer to several great introductory books for these details (Bohm, 1989; Sakurai, 1994; Griffiths, 1995; Feynman, 1998). Physicists such as Planck, Einstein, Bohr, de Broglie, Born, Heisenberg, Schrödinger, Pauli, Dirac, and von Neumann contributed to the foundations of the quantum theory in the 1920s and

1930s. We introduce the quantum theory by *briefly* commenting on its history and major underlying concepts.

Information theory is the second great foundational science for quantum Shannon theory. In some sense, it is merely an application of probability theory. Its aim is to quantify the ultimate compressibility of information and the ultimate ability for a sender to transmit information reliably to a receiver. It relies upon probability theory because a "classical" uncertainty, arising from our lack of total information about any given scenario, is ubiquitous throughout all information-processing tasks. The uncertainty in classical information theory is the kind that is present in the flipping of a coin or the shuffle of a deck of cards, the uncertainty due to imprecise knowledge. "Quantum" uncertainty is inherent in nature itself and is perhaps not as intuitive as the uncertainty that classical information theory measures. We later expand further on these differing kinds of uncertainty, and Chapter 4 shows how a theory of quantum information captures both kinds of uncertainty within one formalism.[2]

The history of classical information theory began with Claude Shannon. Shannon's contribution is heralded as one of the single greatest contributions to modern science because he established the field in his seminal 1948 paper (Shannon, 1948). In this paper, he coined the essential terminology, and he stated and justified the main mathematical definitions and the two fundamental theorems of information theory. Many successors have contributed to information theory, but most, if not all, of the follow-up contributions employ Shannon's line of thinking in some form. In quantum Shannon theory, we will notice that many of Shannon's original ideas are present, though they take a particular "quantum" form.

One of the major assumptions in both classical information theory and quantum Shannon theory is that local computation is free but communication is expensive. In particular, for the classical case, we assume that each party has unbounded computation available. For the quantum case, we assume that each party has a fault-tolerant quantum computer available at his or her local station and the power of each quantum computer is unbounded. We also assume that both communication and a shared resource are expensive, and for this reason, we keep track of these resources in a *resource count*. Though sometimes, we might say that classical communication is free in order to simplify a scenario. A simplification like this one can lead to greater insights that might not be possible without making such an assumption.

We should first study and understand the postulates of the quantum theory in order to study quantum Shannon theory properly. Your heart may sink when you learn that the Nobel Prize-winning physicist Richard Feynman is famously quoted as saying, "I think I can safely say that nobody understands quantum mechanics." We should clarify Feynman's statement. Of course, Feynman does

[2] Von Neumann established the density matrix formalism in his 1932 book on the quantum theory. This mathematical framework captures both kinds of uncertainty (von Neumann, 1996).

not intend to suggest that no one knows how to work with the quantum theory. Many well-abled physicists are employed to spend their days exploiting the laws of the quantum theory to do fantastic things, such as the trapping of ions in a vacuum or applying the quantum tunneling effect in a transistor to process a single electron. I am hoping that you will give me the license to interpret Feynman's statement. I think he means that it is very difficult for us to understand the quantum theory intuitively because we do not experience the phenomena that it predicts. If we were the size of atoms and we experienced the laws of quantum theory on a daily basis, then perhaps the quantum theory would be as intuitive to us as Newton's law of universal gravitation.[3] Thus, in this sense, I would agree with Feynman—nobody can really understand the quantum theory because it is not part of our everyday experiences. Nevertheless, our aim in this book is to work with the laws of quantum theory so that we may begin to gather insights about what the theory predicts. Only by exposure to and practice with its postulates can we really gain an intuition for its predictions. It is best to imagine that the world in our everyday life does incorporate the postulates of quantum mechanics, because, indeed, as many, many experiments have confirmed, it does!

We delve into the history of the convergence of the quantum theory and information theory in some detail in this introductory chapter because this convergence does have an interesting history and is relevant to the topic of this book. The purpose of this historical review is not only to become familiar with the field itself but also to glimpse into the minds of the founders of the field so that we may see the types of questions that are important to think about when tackling new, unsolved problems.[4] Many of the most important results come about from asking simple, yet profound, questions and exploring the possibilities.

We first briefly review the history and the fundamental concepts of the quantum theory before delving into the convergence of the quantum theory and information theory. We build on these discussions by introducing some of the initial fundamental contributions to quantum Shannon theory. The final part of this chapter ends by posing some of the questions to which quantum Shannon theory provides answers.

[3] Of course, Newton's law of universal gravitation was a revolutionary breakthrough because the phenomenon of gravity is not entirely intuitive when a student first learns it. But, we do experience the gravitational law in our daily lives and I would argue that this phenomenon is much more intuitive than, say, the phenomenon of quantum entanglement.

[4] Another way to discover good questions is to attend parties that well-established professors hold. The story goes that Oxford physicist David Deutsch attended a 1981 party at the Austin, Texas house of renowned physicist John Archibald Wheeler, in which many attendees discussed the foundations of computing (Mullins, 2001). Deutsch claims that he could immediately see that the quantum theory would give an improvement for computation. A bit later, he published an algorithm in 1985 that was the first instance of a quantum speed-up over the fastest classical algorithm (Deutsch, 1985).

1.1 Overview of the Quantum Theory

1.1.1 Brief History of the Quantum Theory

A physicist living around 1890 would have been well pleased with the progress of physics, but perhaps frustrated at the seeming lack of open research problems. It seemed as though the Newtonian laws of mechanics, Maxwell's theory of electromagnetism, and Boltzmann's theory of statistical mechanics explained most natural phenomena. In fact, Max Planck, one of the founding fathers of the quantum theory, was searching for an area of study in 1874 and his advisor gave him the following guidance:

"In this field [of physics], almost everything is already discovered, and all that remains is to fill a few holes."

Two Clouds

Fortunately, Planck did not heed this advice and instead began his physics studies. Not everyone agreed with Planck's former advisor. Lord Kelvin stated in his famous April 1900 lecture that "two clouds" surrounded the "beauty and clearness of theory" (1st Baron Kelvin, 1901). The first cloud was the failure of Michelson and Morley to detect a change in the speed of light as predicted by an "ether theory," and the second cloud was the ultraviolet catastrophe, the prediction of classical theory that a blackbody emits radiation with an infinite intensity at high ultraviolet frequencies. In that same year of 1900, Planck started the quantum revolution that began to clear the second cloud. He assumed that light comes in discrete bundles of energy and used this idea to produce a formula that correctly predicts the spectrum of blackbody radiation (Planck, 1901). A great cartoon lampoon of the ultraviolet catastrophe shows Planck calmly sitting fireside with a classical physicist whose face is burning to bits because of the intense ultraviolet radiation that his classical theory predicts the fire is emitting (McEvoy & Zarate, 2004). A few years later, in 1905, Einstein contributed a paper that helped to further clear the second cloud (Einstein, 1905) (he also cleared the first cloud with his other 1905 paper on special relativity). He assumed that Planck was right and showed that the postulate that light arrives in "quanta" (now known as the photon theory) provides a simple explanation for the photoelectric effect, the phenomenon in which electromagnetic radiation beyond a certain threshold frequency impinging on a metallic surface induces a current in that metal.

These two explanations of Planck and Einstein fueled a theoretical revolution in physics that some now call the first quantum revolution (Dowling & Milburn, 2003). Some years later, in 1924, Louis de Broglie postulated that every individual element of matter, whether an atom, electron, or photon, has both particle-like behavior and wave-like behavior (de Broglie, 1924). Just two years later, Erwin Schrödinger used the de Broglie idea to formulate a wave equation, now known as Schrödinger's equation, that governs the evolution of a closed

quantum-mechanical system (Schrödinger, 1926). His formalism later became known as wave mechanics and was popular among physicists because it appealed to notions with which they were already familiar. Meanwhile, in 1925, Werner Heisenberg formulated an "alternate" quantum theory called matrix mechanics (Heisenberg, 1925). His theory used matrices and theorems from linear algebra, mathematics with which many physicists at the time were not readily familiar. For this reason, Schrödinger's wave mechanics was more popular than Heisenberg's matrix mechanics. In 1930, Paul Dirac published a textbook (now in its fourth edition and reprinted 16 times) that unified the formalisms of Schrödinger and Heisenberg, showing that they were actually equivalent (Dirac, 1982). In a later edition, he introduced the now ubiquitous "Dirac notation" for quantum theory that we will employ in this book.

After the publication of Dirac's textbook, the quantum theory then stood on firm mathematical grounding and the basic theory had been established. We thus end our historical overview at this point and move on to the fundamental concepts of the quantum theory.

1.1.2 Fundamental Concepts of the Quantum Theory

Quantum theory, as applied in quantum information theory, really has only a few important concepts. We review each of these aspects of quantum theory briefly in this section. Some of these phenomena are uniquely "quantum" but others do occur in the classical theory. In short, these concepts are as follows:[5]

1. indeterminism,
2. interference,
3. uncertainty,
4. superposition,
5. entanglement.

The quantum theory is *indeterministic* because the theory makes predictions about probabilities of events only. This aspect of quantum theory is in contrast with a deterministic classical theory such as that predicted by the Newtonian laws. In the Newtonian system, it is possible to predict, with certainty, the trajectories of all objects involved in an interaction if one knows only the initial positions and velocities of all the objects. This deterministic view of reality even led some to believe in determinism from a philosophical point of view. For instance, the mathematician Pierre-Simon Laplace once stated that a supreme intellect, colloquially known as Laplace's demon, could predict all future events from present and past events:

> "We may regard the present state of the universe as the effect of its past and the cause of its future. An intellect which at a certain moment would know all forces that set nature in motion, and all positions of all items of which nature is composed, if this

[5] I have used Todd A. Brun's list from his lecture notes (Brun, n.d.).

intellect were also vast enough to submit these data to analysis, it would embrace in a single formula the movements of the greatest bodies of the universe and those of the tiniest atom; for such an intellect nothing would be uncertain and the future just like the past would be present before its eyes."

The application of Laplace's statement to atoms is fundamentally incorrect, but we can forgive him because the quantum theory had not yet been established in his time. Many have extrapolated from Laplace's statement to argue the invalidity of human free will. We leave such debates to philosophers.[6]

In reality, we never can possess full information about the positions and velocities of every object in any given physical system. Incorporating probability theory then allows us to make predictions about the probabilities of events and, with some modifications, the classical theory becomes an indeterministic theory. Thus, indeterminism is not a unique aspect of the quantum theory but merely a feature of it. But this feature is so crucial to the quantum theory that we list it among the fundamental concepts.

Interference is another feature of the quantum theory. It is also present in any classical wave theory—constructive interference occurs when the crest of one wave meets the crest of another, producing a stronger wave, while destructive interference occurs when the crest of one wave meets the trough of another, canceling out each other. In any classical wave theory, a wave occurs as a result of many particles in a particular medium coherently displacing one another, as in an ocean surface wave or a sound pressure wave, or as a result of coherent oscillating electric and magnetic fields, as in an electromagnetic wave. The strange aspect of interference in the quantum theory is that even a single "particle" such as an electron can exhibit wave-like features, as in the famous double-slit experiment (see Greene (1999) for a history of these experiments). This quantum interference is what contributes wave–particle duality to every fundamental component of matter.

Uncertainty is at the heart of the quantum theory. Uncertainty in the quantum theory is fundamentally different from uncertainty in the classical theory (discussed in the former paragraph about an indeterministic classical theory). The archetypal example of uncertainty in the quantum theory occurs for a single particle. This particle has two complementary variables: its position and its momentum. The uncertainty principle states that it is impossible to know both its position and momentum precisely. This principle even calls into question the meaning of the word "know" in the previous sentence in the context of quantum theory. We might say that we can only know that which we measure, and thus, we can only know the position of a particle after performing a precise measurement that determines it. If we follow with a precise measurement of its momentum, we lose all information about the position of the particle after learning its momentum. In quantum information science, the BB84 protocol for

[6] John Archibald Wheeler may disagree with this approach. He once said, "Philosophy is too important to be left to the philosophers" (Misner *et al.*, 2009).

quantum key distribution exploits the uncertainty principle and statistical analysis to determine the presence of an eavesdropper on a quantum communication channel by encoding information into two complementary variables (Bennett & Brassard, 1984).

The *superposition* principle states that a quantum particle can be in a linear combination state, or *superposed state*, of any two other allowable states. This principle is a result of the linearity of quantum theory. Schrodinger's wave equation is a linear differential equation, meaning that the linear combination $\alpha\psi + \beta\phi$ is a solution of the equation if ψ and ϕ are both solutions of the equation. We say that the solution $\alpha\psi + \beta\phi$ is a coherent superposition of the two solutions. The superposition principle has dramatic consequences for the interpretation of the quantum theory—it gives rise to the notion that a particle can somehow "be in one location and another" at the same time. There are different interpretations of the meaning of the superposition principle, but we do not highlight them here. We merely choose to use the technical language that the particle is in a superposition of both locations. The loss of a superposition can occur through the interaction of a particle with its environment. Maintaining an arbitrary superposition of quantum states is one of the central goals of a quantum communication protocol.

The last, and perhaps most striking, "quantum" feature that we highlight here is *entanglement*. There is no true classical analog of entanglement. The closest analog of entanglement might be a secret key that two parties possess, but even this analogy does not come close. Entanglement refers to the strong quantum correlations that two or more quantum particles can possess. The correlations in quantum entanglement are stronger than any classical correlations in a precise, technical sense. Schrödinger first coined the term "entanglement" after observing some of its strange properties and consequences (Schrödinger, 1935). Einstein, Podolsky, and Rosen then presented an apparent paradox involving entanglement that raised concerns over the completeness of the quantum theory (Einstein *et al.*, 1935). That is, they suggested that the seemingly strange properties of entanglement called the uncertainty principle into question (and thus the completeness of the quantum theory) and furthermore suggested that there might be some "local hidden-variable" theory that could explain the results of experiments. It took about 30 years to resolve this paradox, but John Bell did so by presenting a simple inequality, now known as a Bell inequality (Bell, 1964). He showed that any two-particle classical correlations that satisfy the assumptions of the "local hidden-variable theory" of Einstein, Podolsky, and Rosen must be less than a certain amount. He then showed how the correlations of two entangled quantum particles can violate this inequality, and thus, entanglement has no explanation in terms of classical correlations but is instead a uniquely quantum phenomenon. Experimentalists later verified that two entangled quantum particles can violate Bell's inequality (Aspect *et al.*, 1981).

In quantum information science, the non-classical correlations in entanglement play a fundamental role in many protocols. For example, entanglement is the