# Quantum Information and Computing

*Summer of Science '22*

Hanan Basheer

June 2022

# Contents

# Part I

# Introduction

**Quantum computation and Quantum Information** is the study of the information processing tasks that can be accomplished using a quantum mechanical system.

A series of crises had arisen in physics in the 20th Century. The problem was that the theories of physics at that time (now dubbed classical physics) were predicting absurdities such as the existence of an 'ultraviolet catastrophe' involving infinite energies, or electrons spiralling inexorably into the atomic nucleus. At first, such problems were resolved by adding ad hoc hypotheses to classical physics, but as a better understanding of atoms and radiation was gained these attempted explanations became more and more convoluted. The crisis came to a head in the early 1920s after a quarter-century of turmoil and resulted in the creation of the modern theory of *quantum mechanics*.

**Quantum mechanics** is a mathematical framework or set of rules for the construction of physical theories. The rules of quantum mechanics are simple but even experts find them counterintuitive, and the earliest antecedents of quantum computation and quantum information may be found in the long-standing desire of physicists to better understand quantum mechanics.

A related historical strand contributing to the development of quantum computation and quantum information is the interest, dating to the 1970s, in obtaining *complete control over single quantum systems*. Why this effort to attain complete control over single quantum systems? Setting aside the many technological reasons and concentrating on pure science, the principal answer is that researchers have done this on a hunch. Often the most profound insights in science come when we develop a method for probing a new regime of Nature.

Quantum computation and quantum information fit naturally into this program. They provide a useful series of challenges at varying levels of difficulty for people devising methods to better manipulate single quantum systems, stimulate the development of new experimental techniques and provide guidance as to the most interesting directions in which to take experiment. Conversely, the ability to control single quantum systems is essential if we are to harness the power of quantum mechanics for applications to quantum computation and quantum information.

One paradigm is provided by the theory of quantum computation, which is based on the idea of using quantum mechanics to perform computations, instead of classical physics. It turns out that while an ordinary computer can be used to simulate a quantum computer, it appears to be impossible to perform the simulation in an efficient fashion. Thus quantum computers offer an essential speed advantage over classical computers. This speed advantage is so significant that many researchers believe that no conceivable amount of progress in classical computation would be able to overcome the gap between the power of a classical computer and the power of a quantum computer.

The remarkable first step taken by Deutsch, in proposing an example showing quantum computers might have computational powers exceeding those of classical computer, was improved in the subsequent decade by many people, culminating in Peter Shor's 1994 demonstration that two enormously important problems – the problem of finding the prime factors of an integer, and the

so-called 'discrete logarithm' problem – could be solved efficiently on a quantum computer. This attracted widespread interest because these two problems were and still are widely believed to have no efficient solution on a classical computer. Shor's results are a powerful indication that quantum computers are more powerful than Turing machines, even probabilistic Turing machines.

At the same time computer science was exploding in the 1940s, another revolution was taking place in our understanding of communication. In 1948 Claude Shannon published a remarkable pair of papers laying the foundations for the modern theory of information and communication. This was the beginning of **Information Theory**. Perhaps the key step taken by Shannon was to mathematically define the concept of *information*. The first, Shannon's noiseless channel coding theorem, quantifies the physical resources required to store the output from an information source. Shannon's second fundamental theorem, the noisy channel coding theorem, quantifies how much information it is possible to reliably transmit through a noisy communications channel.

Quantum information theory has followed with similar developments. In 1995, Ben Schumacher provided an analogue to Shannon's noiseless coding theorem, and in the process defined the 'quantum bit' or 'qubit' as a tangible physical resource. However, no analogue to Shannon's noisy channel coding theorem is yet known for quantum information. Nevertheless, in analogy to their classical counterparts, a theory of quantum error-correction has been developed which, as already mentioned, allows quantum computers to compute effectively in the presence of noise, and also allows communication over noisy quantum channels to take place reliably. The theory of quantum error-correcting codes was developed to protect quantum states against noise.

One of the earliest discoveries in quantum computation and quantum information was that quantum mechanics can be used to do key distribution in such a way that security of the parties trying to communicate can not be compromised. This procedure is known as **Quantum Cryptography** or quantum key distribution. The basic idea is to exploit the quantum mechanical principle that observation in general disturbs the system being observed. Thus, if there is an eavesdropper listening in as two parties attempt to transmit their key, the presence of the eavesdropper will be visible as a disturbance of the communications channel which the parties are using to establish the key. These parrties can then throw out the key bits established while the eavesdropper was listening in, and start over.

Perhaps the most striking of these is the study of **Quantum Entanglement**. Entanglement is a uniquely quantum mechanical resource that plays a key role in many of the most interesting applications of quantum computation and quantum information. In recent years there has been a tremendous effort trying to better understand the properties of entanglement considered as a fundamental resource of Nature, of comparable importance to energy, information, entropy, or any other fundamental resource.

# Part II

# Quantum Bits and Computation

The *bit* is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the *quantum bit*, or *qubit* for short. In this section we introduce the properties of single and multiple qubits, comparing and contrasting their properties to those of classical bits.

Just as a classical bit has a state – either 0 or 1 – a qubit also has a state. Two possible states for a qubit are the states $|0$ and $|1$, which as you might guess correspond to the states 0 and 1 for a classical bit. Notation like '$|$' is called the *Dirac notation*. The difference between bits and qubits is that a qubit can be in a state other than $|0$ or $|1$. It is also possible to form linear combinations of states, often called *superpositions*:

$$|\psi = \alpha|0 + \beta|1 \tag{1}$$

We can examine a bit to determine whether it is in the state 0 or 1. For example, computers do this all the time when they retrieve the contents of their memory. Rather remarkably, we cannot examine a qubit to determine its quantum state, that is, the values of $\alpha$ and $\beta$. Instead, quantum mechanics tells us that we can only acquire much more restricted information about the quantum state.

The ability of a qubit to be in a superposition state runs counter to our 'common sense' understanding of the physical world around us. A classical bit is like a coin: either heads or tails up. For imperfect coins, there may be intermediate states like having it balanced on an edge, but those can be disregarded in the ideal case. By contrast, a qubit can exist in a continuum of states between $|0$ and $|1$ – until it is observed. Let us emphasize again that when a qubit is measured, it only ever gives '0' or '1' as the measurement result – probabilistically. For example, a qubit can be in the state

$$\frac{1}{\sqrt{2}}|0 + \frac{1}{\sqrt{2}}|1 \tag{2}$$

One picture useful in thinking about qubits is the following geometric representation. Because $|\alpha|^2 + |\beta|^2 = 1$, we may rewrite Equation (1) as

$$|\psi = \cos\frac{\theta}{2}|0 + e^{i\phi}\sin\frac{\theta}{2}|1 \tag{3}$$

The numbers $\theta$ and $\phi$ define a point on the unit three-dimensional sphere. This sphere is often called the *Bloch sphere*. It provides a useful means of visualizing the state of a single qubit, and often serves as an excellent testbed for ideas about quantum computation and quantum information.