Chapter 13

Quantum Information

In Chapter 10 of these notes the multi-state model for quantum systems was presented. This model was then applied to systems intended for energy conversion in Chapter 11 and Chapter 12. Now it is applied to systems intended for information processing.

The science and technology of quantum information is very new. The concept of the quantum bit (named the qubit) was first presented, in the form needed here, in 1995. There are still many unanswered questions (for example the quantum version of the channel capacity theorem is not known). As a result, the field is in a state of flux, and there are gaps in our knowledge which may become apparent in this chapter.

13.1 Quantum Information Storage

We have used the bit as the mathematical model of the simplest classical system that can store information. Similarly, we need a quantum model, which will be called the "qubit." At its simplest, a qubit can be thought of as a small physical object with two states, which can be placed in one of those states and which can subsequently be accessed by a measurement instrument that will reveal that state. However, quantum mechanics both restricts the types of interactions that can be used to move information to or from the system, and permits additional modes of information storage that have no classical counterparts.

An example of a qubit is the magnetic dipole which was used in Chapters 9, 11, and 12 of these notes. Other examples of potential technological importance are quantum dots (three-dimensional wells for trapping electrons) and photons (particles of light with various polarizations).

Suppose our system is a single magnetic dipole. The dipole can be either "up" or "down," and these states have different energies. The fact that the system consists of only a single dipole implies that the system is fragile. To preserve the state of the system, and therefore its information, the system must remain isolated. The slightest interaction with its environment is enough to change its state.

The reason that classical bits are not as fragile is that they use more physical material. For example, a semiconductor memory may represent a bit by the presence or absence of a thousand electrons. If one is missing, the rest are still present and a measurement can still work. In other words, there is massive redundancy in the mechanism that stores the data. Redundancy is effective in correcting errors. For a similar reason, it is possible to read a classical bit without changing its state, and it is possible for one bit to control the input of two or more gates (in other words, the bit can be copied).

However, there are at least three reasons why we may want to store bits without such massive redundancy. First, it would be more efficient. More bits could be stored or processed in a structure of the same size or cost. The semiconductor industry is making rapid progress in this direction, and before 2015 it should be

Author: Paul Penfield, Jr.

This document: http://www.mtl.mit.edu/Courses/6.050/2006/notes/chapter13.pdf
Version 1.3, May 11, 2006. Copyright © 2006 Massachusetts Institute of Technology

possible to make memory cells and gates that use so few atoms that statistical fluctuations in the number of data-storing particles will be a serious problem. Second, sensitive information stored without redundancy could not be copied without altering it, so it would be possible to protect the information securely, or at least know if its security had been compromised. And third, the properties of quantum mechanics could permit modes of computing and communications that cannot be done classically.

A model for reading and writing the quantum bit is needed. Our model for writing (sometimes called "preparing" the bit) is that a "probe" with known state (either "up" or "down") is brought into contact with the single dipole of the system. The system and the probe then exchange their states. The system ends up with the probe's previous value, and the probe ends up with the system's previous value. If the previous system state was known, then the state of the probe after writing is known and the probe can be used again. If not, then the probe cannot be reused because of uncertainty about its state. Thus writing to a system that has unknown data increases the uncertainty about the environment. The general principle here is that discarding unknown data increases entropy.

The model for reading the quantum bit is not as simple. We assume that the measuring instrument interacts with the bit in some way to determine its state. This interaction forces the system into one of its stationary states, and the state of the instrument changes in a way determined by which state the system ends up in. If the system was already in one of the stationary states, then that one is the one selected. If, more generally, the system wave function is a linear combination of stationary states, then one of those states is selected, with probability given by the square of the magnitude of the expansion coefficient.

We now present three models of quantum bits, with increasingly complicated behavior.

13.2 Model 1: Tiny Classical Bits

The simplest model of a quantum bit is one which we will consider only briefly. It is not general enough to accommodate many interesting properties of quantum information.

This model is like the magnetic dipole model, where only two states (up and down) are possible. Every measurement restores the system to one of its two values, so small errors do not accumulate. Since measurements can be made without changing the system, it is possible to copy a bit. This model of the quantum bit behaves essentially like a classical bit except that the physical quantities associated with it are very small.

This model has proven useful for energy conversion systems. It was used in Chapter 12 of these notes.

13.3 Model 2: Superposition of States (the Qubit)

The second model makes use of the fact that the states in quantum mechanics can be expressed in terms of wave functions which obey the Schrödinger equation. Since the Schrödinger equation is linear, any linear combination of wave functions that obey it also obeys it. Thus, if we associate the logical value 0 with the wave function ψ_0 and the logical value 1 with the wave function ψ_1 then any linear combination of the form

$$\psi = \alpha\psi_0 + \beta\psi_1 \tag{13.1}$$

where α and β are complex constants with $\mid \alpha \mid^2 + \mid \beta \mid^2 = 1$, is a valid wave function for the system. Then the probability that a measurement returns the value 0 is $\mid \alpha \mid^2$ and the probability that a measurement returns the value 1 is $\mid \beta \mid^2$. When a measurement is made, the values of α and β are changed so that one of them is 1 and the other is 0, consistent with what the measurement returns.

It might seem that a qubit defined in this way could carry a lot of information because both α and β can take on many possible values. However, the fact that a measurement will return only 0 or 1 along with the fact that these coefficients are destroyed by a measurement, means that only one bit of information can be read from a single qubit, no matter how much care was exerted in originally specifying α and β precisely.

13.4 Model 3: Multiple Qubits with Entanglement

Consider a quantum mechanical system with four states, rather than two. Let us suppose that it is possible to make two different measurements on the system, each of which returns either 0 or 1. It is natural to denote the stationary states with two subscripts, one corresponding to the first measurement and the other to the second. Thus the general wave function is of the form

$$\psi = \alpha_{00}\psi_{00} + \alpha_{01}\psi_{01} + \alpha_{10}\psi_{10} + \alpha_{11}\psi_{11} \tag{13.2}$$

where the complex coefficients obey the normalization condition

$$1 =\mid \alpha_{00} \mid^2 + \mid \alpha_{01} \mid^2 + \mid \alpha_{10} \mid^2 + \mid \alpha_{11} \mid^2 \tag{13.3}$$

You may think of this model as two qubits, one corresponding to each of the two measurements. These qubits are not independent, but rather are **entangled** in some way. Then it is natural to ask what happens if one of them is measured. A measurement of, for example, the first qubit will return 0 with probability $\mid \alpha_{00} \mid^2 + \mid \alpha_{01} \mid^2$ and if it does the wave function collapses to only those stationary states that are consistent with this measured value,

$$\psi = \frac{\alpha_{00}\psi_{00} + \alpha_{01}\psi_{01}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \tag{13.4}$$

(note that the resulting wave function was "re-normalized" by dividing by $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$).

There is no need for this system to be physically located in one place. In fact, one of the most interesting examples involves two qubits which are entangled in this way but where the first measurement is done in one location and the second in another. A simple case is one in which there are only two of the four possible stationary states initially, so $\alpha_{01} = 0$ and $\alpha_{10} = 0$. This system has the remarkable property that as a result of one measurement the wave function is collapsed to one of the two possible stationary states and the result of this collapse can be detected by the other measurement, possibly at a remote location.

It is possible to define several interesting logic gates which act on multiple qubits. These have the property that they are reversible; this is a general property of quantum-mechanical systems.

Among the interesting applications of multiple qubits are

- Computing some algorithms (including factoring integers) faster than classical computers
- Teleportation (of the information needed to reconstruct a quantum state)
- Cryptographic systems
- Backwards information transfer (not possible classically)
- Superdense coding (two classical bits in one qubit if another qubit was sent earlier)

These applications are described in several books and papers, including these three:

- T. P. Spiller, "Quantum Information Processing: Cryptography, Computation, and Teleportation," Proc. IEEE, vol. 84, no. 12, pp. 1719–1746; December, 1996. Although this article is now several years old, it is still an excellent introduction.
- Michael A. Nielsen and Isaac L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, Cambridge, UK; 2000
- Hoi-Kwong Lo, Sandu Popescu, and Tim Spiller, "Introduction to Quantum Computation and Information," World Scientific, Singapore; 1998. The book is based on a lecture series held at Hewlett-Packard Laboratories, Bristol, UK, November 1996–April, 1997