I. Chuang
Vazirani Class #1
August 27, 1997

I. Quantum Physics & Church–Turing

1 Introduction: Computation & Physics

Fundamentally, any computer is a physical machine, and any computation we perform is just a physics experiment. Certainly, it is one which has been well pre-packaged for our use, but the essence is that computation is a physical process. Quantum physics is a particular process which provides unique properties that have previously been unutilized for the purpose of computation. Historically, the essence of this potential was first realized by Feynman, who noted that quantum systems appear to be exponentially hard to simulate with classical computers. He speculated that therefore, perhaps quantum computers could be exponentially more powerful than their classical counterparts.

This realization was particularly important in placing the power of quantum computation in context with computational complexity theory as a key issue. The modern Church-Turing thesis states that

> *Any "reasonable" model of computation can be efficiently simulated by a probabilistic Turing machine.*

Quantum physics is one of the most precise theories of Nature known to mankind. Its predictions have been tested to nearly 14 orders of magnitude, and confirmed. A model of computation that employs quantum physics is thus probably quite reasonable. However, as Feynman pointed out, it appears that the evolution of quantum systems cannot be efficiently simulated – with a classical Turing machine. Not even with a probabilistic one, since computational trajectories in a probabilistic Turing machine cannot interfere with each other (as is possible in a quantum computer). Quantum computers thus provide the first credible challenge to the modern Church-Turing thesis. Either the thesis is wrong, and computational theory must fundamentally change, or quantum computers are unreasonable, and our understanding of Nature is incomplete.

This motivation, along with powerful potential practical applications (such as polynomial time factoring) propels the theoretical and experimental study of quantum computation. We begin this study by laying the formal mathematical and conceptual foundations for quantum computation. The two central ideas we will cover are *state vectors* and *measurement*. Analogously to their classical counterparts, these describe the instantaneous state of the system, and describe how information is extracted from the system. The distinct features provided by quantum physics – interference, superposition, and entanglement will be briefly described.

2 Interference: Two-Slit Experiment

Consider the physical apparatus shown in Fig. 1. Electrons emitted from the gun at the left pass through a wall with two slits, and fall on a wall, where their number is counted as a function of position x by a movable detector. When slit 2 is covered, the probability distribution for the electron position is given by $P_1(x)$, which is maximum at exactly where a ballistic trajectory would place most electrons, as expected. When the other slit is closed the distribution is $P_2(x)$, which is similar. Now, for normal particles, when both slits are open, one would expect to obtain the distribution $P_{12}(x) = P_1(x) + P_2(x)$, the sum of the single slit distributions. However, that is not the case: these electrons produce an *interference* pattern, which oscillates between zero and the expected sum distribution. This behavior is analogous to what one would expect for waves, rather than particles, and is an important property of quantum systems.

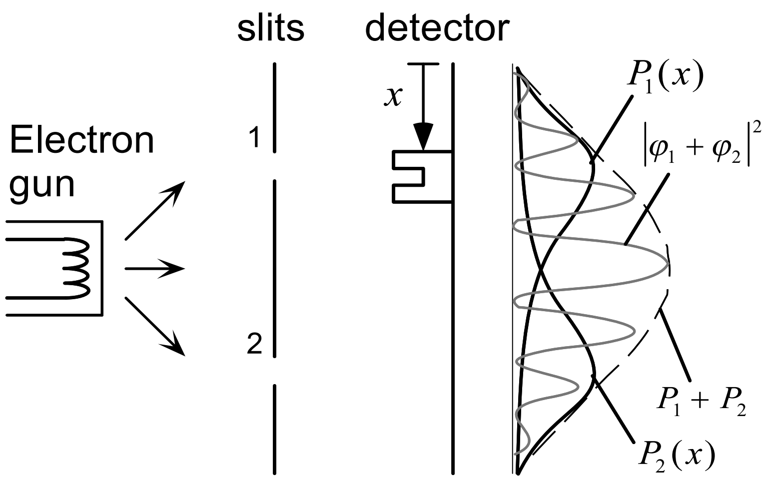

Figure 1: Two-slit experiment.

What gives is a proper description of the state of this system? The experiment shows us that probabilities are insufficient – probabilities are positive numbers and cannot cancel each other out when they add. If we had *negative* probabilities that would work. It turns out in quantum mechanics what we have are *probability amplitudes* ϕ_i, which are complex numbers whose norms give probabilities $P_i = |\phi_i|^2$. For the two-slit experiment, the output distribution is $P_{12}(x) = |\phi_1(x) + \phi_2(x)|^2 = P_1(x) + P_2(x) + 2\Re e\,(\phi_1^*(x)\phi_2(x))$. The oscillations come from the third, interference term.

An important part of specifying a quantum state thus involves giving probability amplitudes – and the phenomena associated with this are important in the study of quantum mechanics. Here, however, our goal is different – we are interested in how information can be represented by a quantum state. To do this in the simplest terms, we turn next to a very simple physical system.

3 Quantum Bits

A quantum bit ("qubit") is a two state quantum system, such as the electron in the two lowest energy levels of a Hydrogen atom (Fig. 2). The electron has probability amplitudes α and β of being either in the ground ($n = 0$) or excited ($n = 1$) states, respectively (similar to how the particle in the two-slit experiment has a certain probability amplitude $\phi(x)$ of being at position x). One could say that the electron has not made up its mind where it shall be, and so partially exists in both energy states.

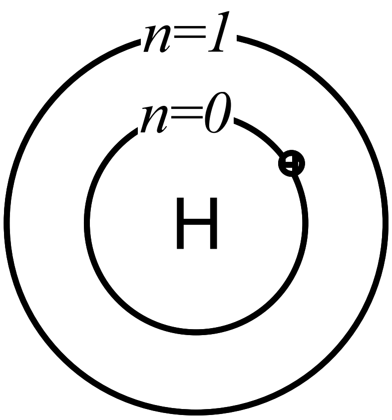

Figure 2: Qubit represented by the electron in a Hydrogen atom.

Now, the electron definitely exists, so the total probability must be one, meaning that $|\alpha|^2 + |\beta|^2 = 1$. We can thus represent the quantum state of a qubit a unit vector $(\alpha\ \beta)^T$. But a more convenient notation, which we shall adopt from physicists[1], is to denote the qubit state as $|\psi\rangle$ (a $|\cdot\rangle$ is called a "ket" – later we will use $\langle\cdot|$, which is a "bra," and write expressions such as $\langle\psi|\phi\rangle$ which are brackets). which is, for our Hydrogen atom, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

A qubit can be visualized geometrically as living on a unit three-dimensional sphere, as shown in Fig. 3. Because of the normalization constraint, we can equivalently express a qubit state as $|\psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$, where θ and ϕ are the spherical coordinates of a point on the sphere.

The paradox of a qubit is that it seems to contain an infinite amount of information, since its state is represented by two *continuous* degrees of freedom (e.g., in principle, one could store an entire Shakespeare text in the infinite decimal points of θ). However, this physically

[1]This is called Dirac notation after the famous physicist Paul Dirac, who invented it.

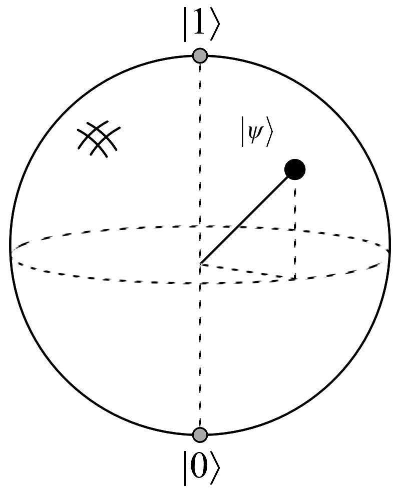

Figure 3: Qubit sphere.

unreasonable conclusion turns out to not to be the case, because of an additional and extremely important property of quantum systems.

When a qubit is measured, only one of two results are obtained: either zero or one. Here is how it works: a measurement of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ will give 0 with probability $|\alpha|^2$, leaving the state $|\psi'\rangle = |0\rangle$, or 1 with probability $|\beta|^2$, leaving the state $|\psi'\rangle = |1\rangle$. Note how the post-measurement state of the system is a new state, which is consistent with the measurement result.

Thus, from a single measurement, one obtains only one bit of information about α and β – and the paradox is resolved. Only if infinitely many identically prepared qubits were measured would one be able to completely obtain α and β. So in a sense, a qubit contains a great deal of "hidden information" – as long as it is not measured. This is an important part of what we shall exploit in quantum computation, as we see next by considering the properties of multiple qubits.

4 Multiple Qubits

Suppose we have two qubits. If these were represented by two Hydrogen atoms, then classically, there would be four possible states, 00, 01, 10, and 11, for the two electrons. The quantum state associates a probability amplitude with each of these, such that the state vector describing the two atoms would be

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \,, \tag{1}$$

where $\sum_{x=\{0,1\}^2} \alpha_x |x\rangle = 1$. Similar to the case for a single qubit, the measurement result x occurs with probability $|\alpha_x|^2$, leaving the state $|x\rangle$. Here, we could measure just a subset of the bits; the result is similar: measuring the first bit would give 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$, leaving the post-measurement state

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} . \tag{2}$$

Note how $|\psi'\rangle$ is re-normalized to have unit length.

For example, an important state we shall return to later is the Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle . \tag{3}$$

This state has the property that upon measuring the first qubit, one obtains two possible results:

$$Pr[0] = \frac{1}{2} \qquad |\phi'\rangle = |00\rangle \tag{4}$$

$$Pr[1] = \frac{1}{2} \qquad |\phi'\rangle = |11\rangle \tag{5}$$

Subsequent measurement of the second qubit always gives the same result as the first measurement, indicating a correlation between the two qubits. What is surprising is that this correlation is stronger than can be realized with any classical state. This result follows from Bell's theorem, and the instance we presented here is part of the Einstein-Podolsky-Rosen (EPR) paradox. We have not fully explained it here – only merely hinted at it. We shall return to this subject later.

Consider now the general case, with N qubits. Now the quantum state is specified by 2^N complex numbers. For $N = 200$ this number is larger than the estimated number of atoms in the universe! Computation with this much data is nearly inconceivable to us, but in principle, Nature can do it with only two hundred atoms. It is as if Nature is keeping 2^{200} hidden pieces of scratch paper on the side, on which she performs her calculations as the system evolves. This enormous potential computational power is what we wish to take advantage of. But how can we think of quantum physics as computation?

5 Summary

We have studied the quantum description of states, and presented rules for performing measurements and obtaining output from a state. This completes the formal description of the "static" elements of quantum computation. In the next chapter we will turn to the "dynamic" picture, and study how quantum states evolve, and thus compute.

6 Problems

1. **Dirac Notation**: $|01\rangle$ is often alternatively written as $|0,1\rangle$, $|0\rangle|1\rangle$ or $|0\rangle \otimes |1\rangle$. The tensor product operator $\otimes$ is associative and distributive. Let $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. What is $|\psi\rangle^{\otimes 4} \equiv |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$? How is it related to

$$|\phi\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \, ? \tag{6}$$

2. **The Shor State**: Many quantum algorithms produce states of the form $\sum_a |a\rangle|f(a)\rangle$. An important step in Peter Shor's quantum factoring algorithm creates the state

$$|S(N,x)\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|x^a \bmod N\rangle \, . \tag{7}$$

   Let $x = 6$, $N = 91$, and $q = 512$. What state $|S'\rangle$ is obtained after measuring the first label (the one in the left ket) if a measurement result of $a = 34$ is obtained? *Extra Credit:* how does this result give the prime factors of N?

3. **Mixed States**: You are given a black box $\mathcal{B}_1$ which accepts as input a single arbitrary qubit $\alpha|0\rangle + \beta|1\rangle$ and produces as its output $[\phi_1\rangle = \left[\alpha|0\rangle + \beta\sqrt{1-\gamma}\,|1\rangle\right] \oplus \left[\beta\sqrt{\gamma}\,|1\rangle\right]$. Here, the tensor sum operation $\oplus$ (which has lower precedence than $\otimes$) indicates different possible results, so that the output is *either* $(\alpha|0\rangle + \beta\sqrt{1-\gamma}\,|1\rangle)/\sqrt{p_1}$ with probability $p_1 = |\alpha|^2 + (1-\gamma)|\beta|^2$, or $|1\rangle$, with probability $1 - p_1$. The notation $[\cdot\rangle$ is used for such "mixed states."

   You are also given another one-qubit input black box $\mathcal{B}_2$ which produces as its output $[\phi_2\rangle = \sqrt{\eta}\left[\alpha|0\rangle + \beta|1\rangle\right] \oplus \sqrt{1-\eta}\left[\alpha|0\rangle - \beta|1\rangle\right]$, where $\eta = (1+\sqrt{1-\gamma})/2$. Can you devise a measurement which distinguishes the outputs of $\mathcal{B}_1$ and $\mathcal{B}_2$, if they are given identical inputs? If not, why?

   Mixed states and processes such as $\mathcal{B}_{1,2}$ will be important in studying decoherence and quantum error correction.