Jerome Kyrias Carman
Physics 4D Term Paper
12/5/06

Superposition and Quantum Computing

“...linear superposition...lies at the heart of quantum parallelism, the possibility of performing a large number of operations in parallel.”[1]

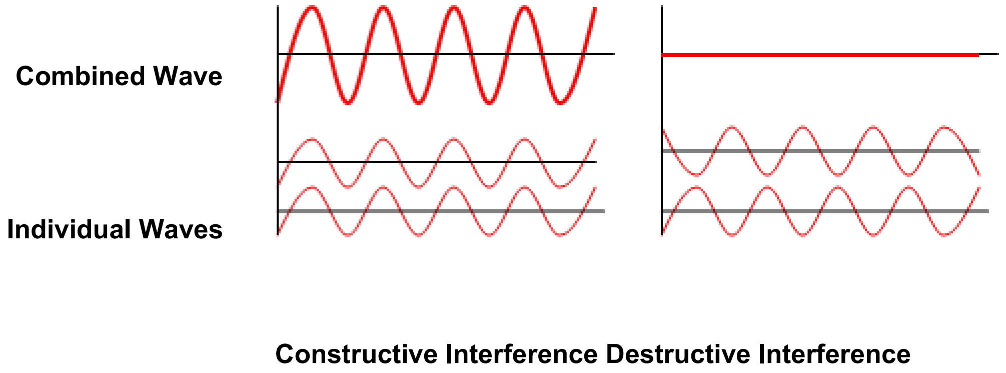
Classical computers (those you use to check your email everyday) are limited in their computational power by two key unavoidable properties of our intuitive physical world; size and time. Processor size is a well known limitation to the production of classical computers for two reasons; the maximum velocity of electromagnetic waves, and the ability to dissipate thermal heat. These are both significant barriers in the all-too-familiar Silicon Valley race towards the latest and greatest computer processor. While the efficiency with which heat is dissipated can conceivably be improved, the speed of electromagnetic waves is currently considered a universal, unavoidable constant. Hence the time limitation to processor speed. Current computer processor designs unavoidably occupy a specific amount of space through which information is carried via electromagnetic waves. This fact inherently confines the classical computer to the linear motion of time (i.e. the definition of velocity is meters **per second**). Julian Brown states in her book Minds, Machines, and the Multiverse[2], “Classical-state space is spatially unbound but is limited by the fact that time flows in only one direction...” Quantum computers, on the other hand, do not operate in the classical space defined by Isaac Newton some centuries ago. In effect, quantum computers can cheat time.

The study of quantum computation involves many fascinating topics. They range from the construction of quantum logic gates (the quantum computer equivalent to transistors) which involve the quickly growing field of nanotechnology, to theoretical mathematics (including the study of mathematical algorithms whose solutions are classically impossible), to the design of a quantum computational programming language, as well as other areas that overlap multiple scientific fields. The focus of this paper is on the phenomenon of quantum mechanics called superposition which forms the foundation for many of the intriguing aspects of quantum computers.

A Brief History of Interference

"The quantum computer...doesn't just manipulate information, it allows different universes to cooperate." [3]

What makes quantum computers so attractive is that they take advantage of a property of physics called superposition. The idea of superposition (as it relates to quantum mechanics) was realized before quantum mechanics from the study of wave interference. Wave interference is defined as the superposition of two or more waves which results in a new wave pattern. For instance, the amplitude of a resulting wave pattern at some point is equal to the sum of the amplitudes of the individual waves at that same point. Essentially the new wave is a superposition of (or a combination of) all the individual waves that created it. Intuitively this makes sense since objects can often be broken down into a sum of smaller objects.



Constructive Interference Destructive Interference

Fig. 1: Example of constructive and destructive interference in waves. The individual waves can be thought of as separate possible states which, when combined, result in a superposition state.

During the early 1800's a physicist named Thomas Young discovered the wave properties of light with his famous double-slit experiment (from which the idea of wave interference came). About a hundred years later experiments such as the photoelectric effect had demonstrated the seemingly opposite particle nature of light (photons). Yet there were some contradictions. Thomas Young's experiment was repeated, yet with a single photon rather than a beam of light. Surprisingly, even with a single photon an interference pattern was observed suggesting that the photon was able to interfere with itself! This experiment was repeated with other particles such as electrons and protons and again an interference pattern was observed. This particle/wave behavior was eventually described with Schrodinger's Wave Equation which essentially describes all matter as a wave which "collapses" into a particle when observed (more on this later).

One of the more striking results from the proposed wave nature of matter is that matter can, in a sense, exist in more than one place at the same time. In the case of Young's experiment with a single photon, the explanation is that a single photon goes through both slits and then it interferes with itself, as two waves do by superposition.[4] In Schrodinger's mathematics, the resulting wave, or state, of the photon (the observed interference pattern) is a superposition (sum) of the individual probabilities (or likelihood) of the photon traveling through one or the other slit.

How this relates to quantum computers is essentially analogous to the idea of parallel processing. A simple example of parallel processing would be a situation where someone, let's call her Alice, is given a task involving ten independent calculations. By herself this task might take a few hours. Instead she decides to delegate one calculation each to ten different people. If each person completes their calculation in twenty minutes then the entire task is done in twenty minutes rather than hours. Currently people already do this by networking multiple computers together. Superposition, however, allows a single quantum computer to accomplish this with Alice being analogous to a single qubit (one bit in a quantum computer) and each task being delegated to a different dimension. In addition, there are theoretically an infinite number of dimensions which rivals any parallel processing network that could be setup with classical computers. The theory behind this rather outlandish concept of delegating tasks to multiple dimensions involves some relatively complicated math. Yet we will delve into it briefly here with some simple examples.

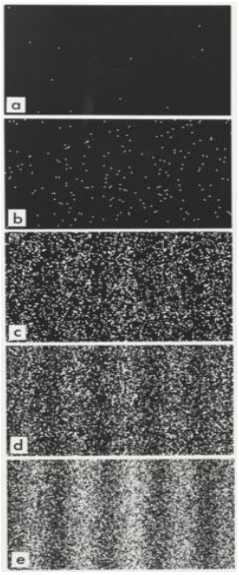


Fig. 2: Build up of electrons over time results in an interference pattern

Is It Dead Or Alive?

"Just as individual subatomic particles cannot necessarily be pinned down to one place, so individual logic states may not necessarily be tied to one value." [5]

Consider a classical computer bit which represents one digit in a binary number system (this digit, or bit, can represent either a 1 or a 0). This type of number system is used in order to translate the calculations of a classical computer processor into information. Currently a positive voltage in a transistor represents a 1 and a negative voltage represents a 0. The more commonly known byte is called a register which contains eight bits. A classical byte can represent a total of 2^8 different values, or the numbers 0 thru 255. An example of an eight bit register (a byte) which represents the value 146 is

01001001

In Dirac bra-ket notation (which is more applicable to quantum mechanics) this eight bit register would be written as

|01001001>

The computation of a byte can only be done one bit at a time. Hence it takes some amount of time to calculate the value of eight different bits. To allow a byte to run through all 256 possible values requires the total time needed to evaluate each of eight bits 256 times. Hence the classical computer has an unavoidable dependence on time since a bit can represent only a 1 **or** a 0 at any particular moment in time. Considering a one bit register (i.e. one bit), an equation[6] can be written which roughly expresses the probability that it exist as either a 1 or a 0;

$$b = a_1|0> + a_2|1>$$

where the boundary conditions on a_1 and a_2 are

- $(a_1)^2 + (a_2)^2 = 1$
- a_1 and a_2 are integers ≥ 0 (this integer restriction is arbitrary and chosen only to support this analogy)

Hence a classical bit can have exactly two forms

$$\text{if } a_1 = 1 \text{ and } a_2 = 0 \text{ then } b = 0$$

$$\text{if } a_1 = 0 \text{ and } a_2 = 1 \text{ then } b = 1$$

A qubit (quantum bit), on the other hand, differs dramatically from a classical bit. While a classical bit can exist either in the state |0> **or** |1>, a qubit in a superposition state is equal to the vector addition of both possible states |0> **and** |1>. A single qubit can be represented as

$$|\Psi> = \alpha_1|0> + \alpha_2|1>$$

where α_1 and α_2 are complex numbers who's square represent the probability of the associated state (otherwise known as a basis vector)[6] and follow the normalization condition, just as in the previous classical example,

$$|\alpha_1|^2 + |\alpha_2|^2 = 1$$

except that they do not have the integer restriction. In order to represent the state of any quantum particle, including qubits, it's wave function |Ψ> is expressed as a vector in a complex vector space whose two components are complex numbers (the reason for this originates mathematically from Schrodinger's equation).

This idea of probability is key to understanding superposition as it relates to quantum mechanics. Essentially the particular state of any quantum particle (solution to it's wave function) has no real physical interpretation except through probability. Another way of saying this is that the state (position, velocity, etc.) of an electron cannot be predicted exactly, only probabilistically. In contrast, observation of a classical bit is completely deterministic with the measured value having a probability of 1, or 100%, as we saw earlier. This means that the probability of that bit having that particular value **before** measurement is 100%, no questions asked. Qubits, on the other hand, are stochastic, meaning there is an uncertainty associated with it's state **before** measurement.[7]

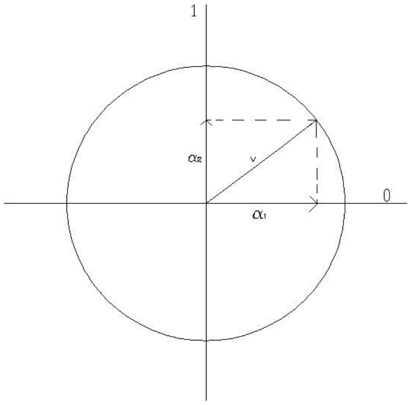
For example, using the famous Schrodinger's cat thought experiment, all the cats we have ever seen are projections of a |cat> generated by the environment into either the |dead> or the |alive> state[8]

$$|cat> = \frac{1}{\sqrt{2}}\ |alive> + \frac{1}{\sqrt{2}}\ |dead>$$

with the normalization condition

$$(\frac{1}{\sqrt{2}})^2+(\frac{1}{\sqrt{2}})^2=1$$

To further emphasize this idea since it is at the heart of quantum computing, take our single qubit |Ψ>, which is a two dimensional system, and express it as a vector $\vec{v}$ whose coordinates represent a point on a unit circle with the coordinate axis being the different possible states of the qubit.



The number α_1 is the vector projection of $\vec{v}$ onto the 0-axis and α_2 the vector projection of $\vec{v}$ onto the 1-axis, and the square of each represents the probability of observing the qubit in either state 0 or state 1 respectively. This is a useful example since the vector $\vec{v}$ is a superposition of the two possible states |0> and |1>.

The implications of this superposition idea become more obvious when we consider a quantum register consisting of more than one qubit. A two qubit register may exist as one of four basis states

|00> |01> |10> |11>

or a superposition of all of them in what is called mathematically a Hilbert space with 2^2 dimensions. Here is where the parallel processing idea comes in. Say the answer to some calculation was 3 (the state |11>). A classical computer would have to compute each bit seperately then add them together to get the answer. A quantum computer, however, would perform all four possible calculations (exist in all four possible states) simultaneously and, when measured, the α term associated with the |11> state would dominate probabilistically and that answer would fall out in a single calculation. Now apply this idea to an even larger register; say a 100 qubit register. This register has 2^{100} different possible solutions (approximately 1.26 x 10^{30}). A classical computer would have to compute the value of 100 bits each 2^{100} times to determine all possible solutions. For comparison, if we assume that the universe is approximately 14 billion years old, then it is approximately 4.41 x 10^{17} seconds old. If we take a modern computer which can calculate around 1.0 x 10^9 calculations per second, then this computer, if allowed to run consistently from the beginning of the universe, would have made about 4.41 x 10^{26} calculations total. Yet a 2^{100} bit register has 1.26 x 10^{30} possible solutions so there would not even be enough time since the beginning of the universe for this computer to calculate all possible solutions for this register. By contrast, a 100 qubit register can theoretically do this same calculation in one step!

The Big Picture

The superposition of a quantum state is fundamental to the field of quantum computing, but it is only the tip of the iceberg. Topics such as entanglement are closely tied with the superposition of a multiple qubit system. In fact, it is because of entanglement that the superposition state is so useful. Entanglement also yields some of the more unintuitive and amazing properties of quantum mechanics.

In addition, there are significant challenges in the ability to read and decipher the information held in a qubit register. Issues such as decoherence, where any interaction of the qubit register with the physical environment (even cosmic radiation such as neutrinos) causes the superposition state to become entangled with those particles and "collapse" into a state where the original information encoded becomes altered. Interestingly, a field called quantum cryptography has grown out of just this phenomenon since any direct observation of a quantum register results in the collapse of its superposition state.

Even the topic of what a qubit is made of, and the circuitry involved in creating and maintaining a qubit register in a superposition state is a vast and complicate topic. Yet, with all these issues scientists have successfully, as of 2005, created and executed a 7-qubit quantum processor.[9] While the future of quantum computers is still far from being a publicly viable product, the successes have shown that many of the outlandish phenomena of quantum mechanics are a reality. This realization has solidified the field of quantum computation and revealed the possibility of accomplishing calculations that are theoretically impossible for classical computers. If viable, quantum computers may one day reveal many secrets of our intricate, fascinating world and possibly implement a paradigm shift in this digital era.

References

[1] Bellac, Michael Le, A Short Introduction to Quantum Information and Quantum Computation, (Cambridge University Press, New York, 2006), p. 2

[2] Brown, Julian, Minds, Machines, and the Multiverse, (Simon and Shuster, New York, 2000), p. 27

[3] Brown, Julian, Minds, Machines, and the Multiverse, (Simon and Shuster, New York, 2000), p. 39

[4] Marinesku, Dan C., Approaching Quantum Computing, (Pearson/Prentice Hall, New Jersey, 2005), p.86

[5] Brown, Julian, Minds, Machines, and the Multiverse, (Simon and Shuster, New York, 2000), p. 33

[6] Marinesku, Dan C., Approaching Quantum Computing, (Pearson/Prentice Hall, New Jersey, 2005), p.98

[7] Marinesku, Dan C., Approaching Quantum Computing, (Pearson/Prentice Hall, New Jersey, 2005), p.6

[8] Marinesku, Dan C., Approaching Quantum Computing, (Pearson/Prentice Hall, New Jersey, 2005), p.114

[8] Marinesku, Dan C., Approaching Quantum Computing, (Pearson/Prentice Hall, New Jersey, 2005), p.9

Figures

Fig. 1: http://en.wikipedia.org/wiki/Image:Interference_of_two_waves.png, © GNU Public License

Fig. 2: http://en.wikipedia.org/wiki/Image:Double-slit_experiment_results_Tanamura_2.jpg, © GNU Public License