Quantum computers

Pedram Khalili Amiri

redefining logic

Faster, smaller, less expensive—that's what we want our computers to be. No matter how good a computer chip is…it's never good enough.

We all know, at least to some extent, how today's computer works. The digital logic behind it is actually very simple and fairly intuitive: an array of 0s and 1s represents a number. One that is easy to store, manipulate and to handle with our present level of technology.

Today, this digital logic is implemented using transistors: devices that are widely believed to have been the greatest invention of the 20th century. Much time and money is being invested in developing new, smaller ones. (Just visit intel.com's news section.)

However, what is being done is merely a change of technology or a change of techniques: adjustments in the manufacturing or design procedure of semiconductors that may result in better transistors, hence, better chips. (The other way is to develop better techniques for using these transistors, to lay them out in such a way that better circuits are built.)

An alternative to this approach to advancing technology would be to think about the basic philosophy behind our computers: the digital logic they are founded on.

A simple run through suggests an interesting solution: as we want our computers to get smaller, we eventually would want the smallest unit of these computers, the *bit*, to be the smallest possible unit of matter: the *atom*.

However, using atoms as digital bits will start a completely new era in computer design. Atoms cannot be simply manipulated and used like the bits built with transistors. The behavior of matter on the atomic scale follows the rules of modern physics. This behavior cannot be understood in terms of our classical description of the world (i. e. Newtonian Mechanics or Maxwell's Equations in Electromagnetics).

The physical theory dealing with such behavior is called *quantum mechanics*. Its use in the computer industry will most probably cause a revolution in the way we use and understand computers. We are going to describe how such a *quantum computer*—a computer based on the rules of quantum mechanics—may work, and how it is going to give us incredible speed and problem-solving power that we only imagine now from watching *Star Trek*.

What is quantum mechanics?

The purpose of physics, or more generally the purpose of science, is to generate a model of the real world around us. Physical theories are, therefore, models with which we try to understand or explain why and how various phenomena around us happen. A good theory is also capable of making correct predictions, i. e. describing never-done experiments and telling you how their results will turn out. We then can perform tests in the laboratory to see whether or not these predictions hold.

Quantum mechanics is just one of these physical theories. It was developed to explain some of the experiments' results in the first half of the 20th century. We don't need to concern ourselves about the complete theory; we can just touch on the main points in order to develop our discussion about quantum computers.

One good way to quickly grasp the basics of quantum mechanics is to consider the well-known problem of light's duality. Light was initially believed to be a build up of particles. Newton, for example, was one of the most important scientists who tried to explain light's behavior this way.

Then, a Scottish physicist, James C. Maxwell, showed theoretically that light is a combination of alternating electrical and magnetic fields, hence a wave. Experiments were done and the theory proved to be valid. The famous experiment done by Heinrich Hertz, was just one of the many successful experiments. It gave evidence for the propagation of electromagnetic waves using a simple transmitter-detector system. (Hertz actually didn't use lightwaves, but his experiment gave a strong proof of the validity of Maxwell's theory in general.)

Later on, new experiments were done which again forced scientists to believe in the particle nature of light. Einstein, for example, explained the photoelectric effect in terms of the particle nature of light, and obtained a noble prize for it. So is light made up of particles or is it a wave?

The answer is very beautifully contained in the words of Richard Feynman—one of the greatest physicists of the 20th century— "it is like neither."

Light doesn't behave exactly like a wave; it also doesn't behave exactly like a particle—at least, not always. So it must be something else, something in between, or some kind of combination of the two…that's what we may think. But let's look at the answer.

The more complete description of light—and of any other "thing" in this world, including matter—states: It is made up of particles, but these particles are distributed wave-like, hence we see both effects. To be a little more technical, the probability of finding these particles in a certain point (of space and time) has a wave-like distribution.

But that rough description is obviously not enough. We need a quantitative way, an equation, to solve for the probability of finding a particle in a special point (of space and time). This is implemented by the Schrödinger Equation, named after Erwin Schrödinger, who first formulated it. This differential equation is basically the principle of conservation of energy, translated to the new probability-wave formalism of quantum mechanics. Using this equation, we can find the probability function for any particle in any given set of environmental and initial conditions.

We don't need to deal with the whole mathematics of the problem, as it is not essential to our brief discussion of quantum computing. We will only use some of its results.

0278-6648/02/$17.00 © 2002 IEEE

Uncertainty and quantum states

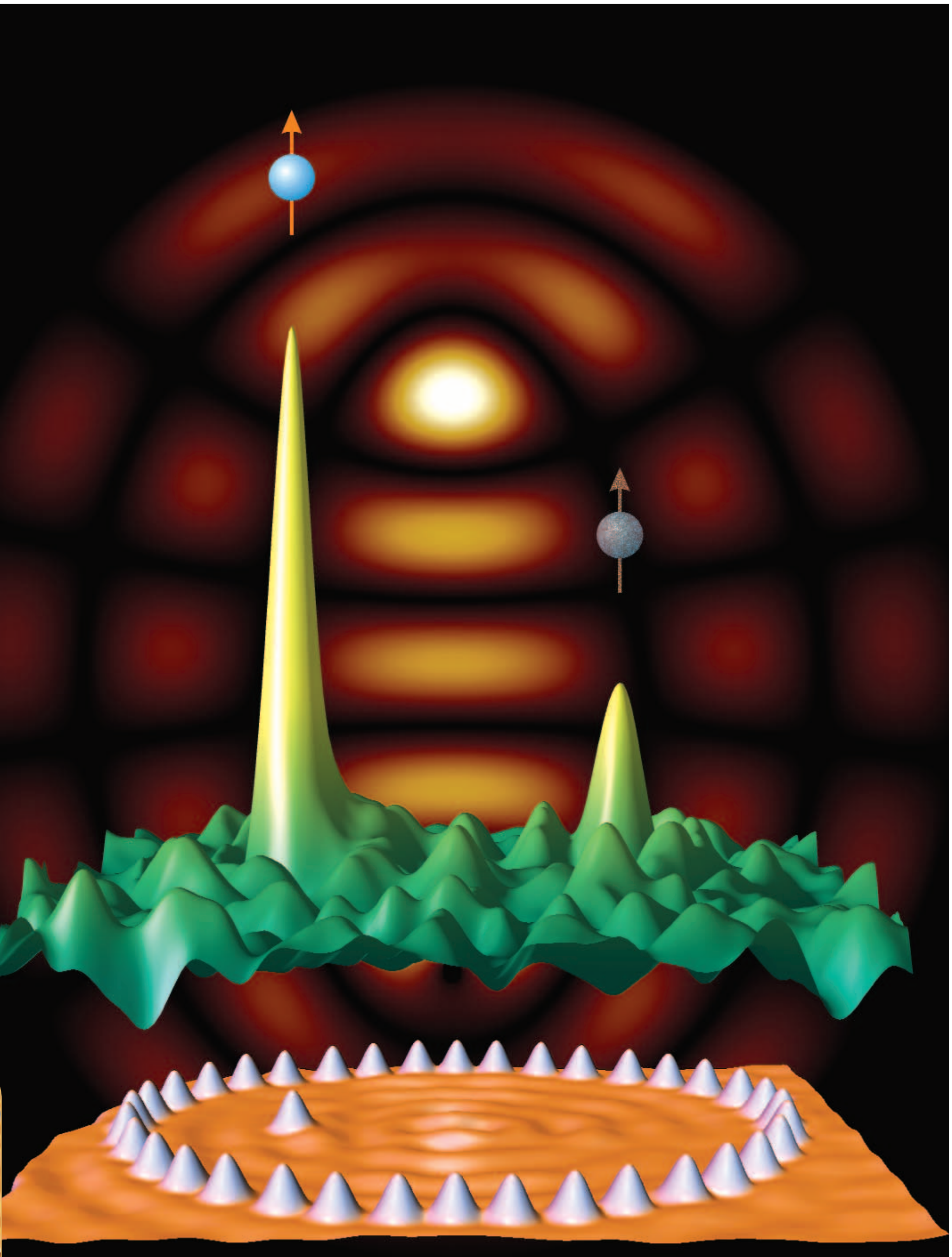
The first thing we think of when confronted with probabilities is *uncertainty*. In fact, probabilities always tell us something, but never everything about a phenomenon. When we say that the probability of seeing ‘1’ in rolling a die is 1/6, we mean that on average, we will see a "1" in every six throws. It doesn’t tell us what we will see in one throw, nor does it guarantee that we will see, for example, one hundred 1s in 600 tosses.

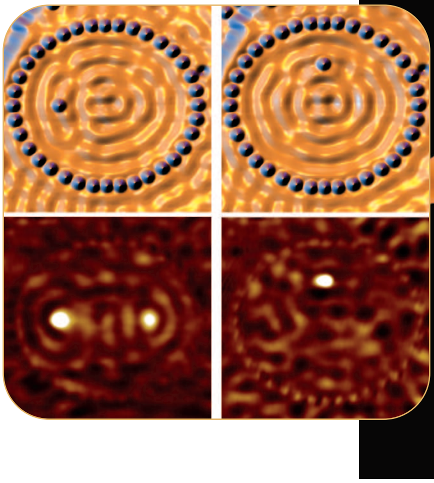
You may have heard about Heisenberg’s Uncertainty principle. This principle is a little more complicated, and different, from the dice example. But that example can help us understand why we can’t determine the position of a particle exactly (i.e. without error).

Heisenberg’s Uncertainty principle essentially says that *position* doesn’t really have a meaning for something like an electron (provided that we know at least "something" about its velocity, or momentum), as the error in measuring its position is too great. For ordinary objects, like a chair or a stone, this minimum error is too small to be accounted for; but in analyzing the behavior of an electron, it plays a crucial role.

So, how can we describe the circumstances an electron is in if we don't use concepts like position, speed and such? The solution is provided by Schrödinger's equation itself.

The new term we use to describe the behavior of electrons, or any other thing that is small enough to show quantum effects, is called a *quantum state*. In fact, each quantum state is associated with a probability distribution for the position of the particle, not with the position itself. It is also associated with some restrictions on some of the particle’s properties, such as energy or spin. This simply means that to analyze the behavior of a particle such as an electron, photon, etcetera, we will have to use the Schrödinger equation. This will lead us to a series of so called quantum states. In each of those quantum states,





Inset: When a magnetic cobalt atom is placed at a focus point of an elliptical corral (upper left), some of its properties also appear at the other focus (lower left), where no atoms exist. When the cobalt atom is not placed at a focus point (upper right), the mirage disappears (lower right). In the big picture, a change in the surface electrons due to the cobalt’s magnetism—the Kondo resonance—appears as a bright spot at each focus. This phenomenon, called the “quantum mirage” effect, uses the wave nature of electrons rather than a wire. (PHOTO CREDITS: IBM) the electron has a well-defined probability distribution, and energy level, or/and spin state and so on.

These general concepts of quantum mechanics provide the foundation to discuss Quantum Information Theory, a possible way to build computers in the future.

Quantum bits

Let's consider a quantum system (a particle in specifically defined environmental conditions) with which we can associate two quantum states. This can be a particle having the spin states "up" or "down," for example. We will denote the first one of these two states with |0>, and the other one with |1>, similar to the 0 and 1 states of the classical theory of computation.

But there are two differences when compared with the classical theory:

1) The |0> and |1> states are quantum states. Thus, they do not denote for example the voltage of a pin on some chip, but the state associated with one of the quantized properties of some quantum system. This property can be the spin, or energy level, or angular momentum, etc. of an electron in some potential field.

2) Most importantly, these quantum states *do not* have the intuitive properties of their classical counterparts. A great difference when compared with classical bits—in fact, this difference has in it the heart of quantum computation—is that a quantum system does not necessarily have to be in one of the two states |0> and |1>. It can simply be in any superposition of the two states. Thus, we can write:

$$\text{state} = a\,|0> + b\,|1> .$$

This is a very straightforward result deduced from the Schrödinger equation. But we don't care about the mathematics here. The interpretation of a superposed state would involve the uncertainty principle: we cannot say definitely which state the system is in. The point is that we can only measure one of the two states |0> and |1> when carrying out a measurement operation on the system.

This means that, for a system which is in a state of the form just described, a measurement will only yield |0> or |1>, not the actual state before the measurement.

Further, according to a form of the uncertainty principle, the actual state of the system after the measurement will be the measured state: |0> or |1>. This means that carrying out the measurement will destroy the actual state of the system. It will collapse to one of the two states depending on the coefficients, a and b. In fact, the probability of finding |0> or |1> is:

$$P(\,|0>\,) = a^2 \quad \text{and} \quad P(\,|1>\,) = b^2$$

Since the result has to be one of those two states, we have:

$$a^2 + b^2 = 1$$

Actually, the mathematics to really show that all these results are true would be rather complicated, so we won't give them here.

To sum up, a system with the properties mentioned is called a quantum bit, or *qubit.* A qubit can be in a superposition of its two basic states, and a measurement on it will yield only one (and exactly one) of these two states. Thus, the effect of the other one (the coefficient a or b associated with it) will disappear.

Obviously, building a computer based on qubits means we have to dramatically change our approach. The computer would have to work in a completely new way. The algorithms needed to manipulate and make qubits function are called *quantum algorithms.*

Quantum algorithms

We will now briefly discuss how a qubit can be manipulated to realize the counterparts of algorithms and programs—as we know them now—on a quantum computer. You may have already guessed that what we actually said is that any state of a qubit can be represented with a vector-like form. That is, we can write:

$$\text{state} = a\,|0> + b\,|1>$$

where:

$$a^2 + b^2 = 1 .$$

Therefore, all we have to do is carry out some kind of transformation on the vector (actually on the qubit represented by the vector). The transformation should increase the possibility of the appearance of the correct answer (|0> or |1>) depending on what the calculation is and what answer is correct for that calculation. Keep in mind, that this qubit is just one in a series of qubits carrying some information, a so-called *quantum register*. A series of such transforms carried out on a qubit is then called a quantum algorithm.

You may ask, however, how these transformations can be carried out without destroying the qubit's state (since we said that measuring a qubit will destroy its content and make it collapse into one state or another). The answer is simple. These transformations do not have anything to do with measurement. Instead, they make use of the interference property of the probability waves of the qubits.

We know that waves—any type—have an interference property. This means that they can make each other disappear (interfere destructively) or emphasize each other (interfere constructively). That's just the same for probability waves. Without getting too specific, the transformations on qubits are actually actions taken to make unwanted (incorrect) answers to interfere destructively, leaving only the correct answer with a considerable probability of appearance.

Several quantum algorithms have already been designed and, even tested, on tiny quantum computers with a small set of qubits. The results have been tremendous: quantum algorithms show the potential of being much faster than their classical counterparts.

A good example is Shor's algorithm for factoring integer numbers. Actually, the ability of classical computers to factor numbers is so restricted that it is widely relied upon to develop secure codes. In contrast, quantum computers using Shor's algorithm would be fast enough to make almost any security system, based on this principle, unsafe. That is certainly one of the main reasons why military research institutions have been attracted by the field and are funding research programs to discover its potential.

Ironically, quantum computation theory itself delivers a unique, completely safe way of encoding data. Only the person who is intended to receive the message will actually receive it, other people trying to figure out the code (transformations needed to extract the message) will get only one try. This is based on the uncertainty principle and the collapsing of quantum bits upon measurement. If the first try is not a hit (and it usually isn't), they will have destroyed the message, they will not be able to try any alternatives.

Another one is the Grover's Algorithm. This is an algorithm for searching through lists, to find someone's phone-number for example. Grover's algorithm is also considerably faster than any classical one, especially at large numbers of entries in the database. In a database with N entries, a classical search algorithm would normally need N/2 tries for finding the desired item, where as Grover's algorithm needs only a number on the order of the square-root of N, which is much faster.

It would not be appropriate to develop the concept of quantum algorithms further in this introductory article, for a discussion of this subject see the book by Nielsen and Chuang and the qubit.org website (See *Read more about it*).

Entanglement and teleportation

One of the strangest predictions of the quantum theory is a phenomenon that is called *entanglement*. This phenomenon is closely related to a technique called *teleportation*. A discussion of quantum computation theory cannot be regarded as complete unless these two terms are defined and explained somewhat.

To put it simply, qubits can be linked in such a way as to share the same destiny. That seems mysterious, actually what it says is mysterious, and the phenomenon is called entanglement. If two quantum systems (i.e. qubits) are entangled, and measuring one of the two has given the result, say |0>, measuring the other one will only give |1>.

Regardless how far the two systems are from each other, this effect occurs instantaneously. That is, qubits that are entangled will feel the effect of measurements carried out on the other one without any delay, even if the distance between them is several light-years. Note: this does not mean a faster-than-light communication, but as said before, it is better interpreted as the two systems sharing the same destiny.

This has been experimentally proven by the famous EPR experiment, and the entangled pairs are commonly called EPR pairs. The experiment is named after Einstein, Podolsky and Rosen who actually devised it as a way to show that quantum theory is not consistent with reality. It consisted of examining whether entangled pairs really feel the effect of measurements made on each other instantly or not. Einstein, Podolsky and Rosen predicted this to be impossible, and hence wanted to use it as a proof of the incompleteness of quantum theory. Contrary to their prediction, the EPR pairs behaved exactly in the way quantum theory had described.

Based on the concept of entanglement, a way of "transporting" (or to be more accurate, "reproducing at another place the state of") qubits has been found that is called teleportation. This has also been carried out experimentally on very simple systems.

Teleportation is being considered as a way of transmitting the contents of quantum registers over a distance. This is an essential issue to resolve if any practical quantum computer is to be built in the future.

Decoherence of qubits & possible practical implementations

In discussing qubits and quantum algorithms, we did not mention one very important thing: To do all that can be done with a qubit, there is a very limited timeframe to work in. That is because *superpositions* of states (states of the form: a |0> + b |1>) are generally very unstable, and will collapse into one of the pure states |0> or |1> quickly as a result of interactions with the environment.

This result is also easily derived from the solution of the Schrödinger equation, but we are not going to prove it here. The time remaining before the state of a qubit is completely destroyed is called the *decoherence time*. The whole process is known as *decoherence*.

The decoherence time is an extremely important factor when considering practical implementations of quantum computers. To build a quantum computer that works, we will have to design the system in such a way that environmental effects are minimized as much as possible so as to increase the decoherence time. A reasonable amount of calculations should be carried out on a qubit before it decoheres.

Ways of building such systems have and are still being investigated. Some of the most promising ones are systems based on Nuclear Magnetic Resonance (NMR) and the so-called Ion Traps (systems in which ions are cooled down to such a low energy that their vibrational states can be used as qubits).

In addition, error correction algorithms are being investigated for qubits to be recovered if their states were affected by, say, transmission over a distance. The function of these algorithms is essentially the same as that of the error correction algorithms of today's digital communication systems. Although, their structure is completely different from the classical ones used.

Read more about it

- M.A.Nielsen, I.A.Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
- C. Paquin, "Computing in the Quantum World," [online], Available: http://www.iro.umontreal.ca/~paquin/Qu/quantumComp.pdf
- J. Mullins, "The Topsy Turvy World of Quantum Computing," *IEEE Spectrum*, vol. 38, no. 2, pp. 42-49, February 2001.
- J. Preskill, "Quantum Computing: Pro and Con," *Proc. Roy. Soc.* Lond. A454, pp. 469-486, 1998.
- D. Deutsch, "Quantum Theory, the Church-Turing principle and the universal quantum computer," *Proc. Roy. Soc.* Lond. A400, 96, 1985.
- R. P. Feynman, R. B. Leighton, M. Sands, *The Feynman Lectures on Physics*,Volume III, Addison-Wesley, 1966.
- S. Gasiorowicz, *Quantum Physics*, Second Edition, John Wiley & Sons, 1996.
- In addition, lots of useful information on the subject can be found at the website of the Oxford University Center for Quantum Computation: <http://www.qubit.org/>

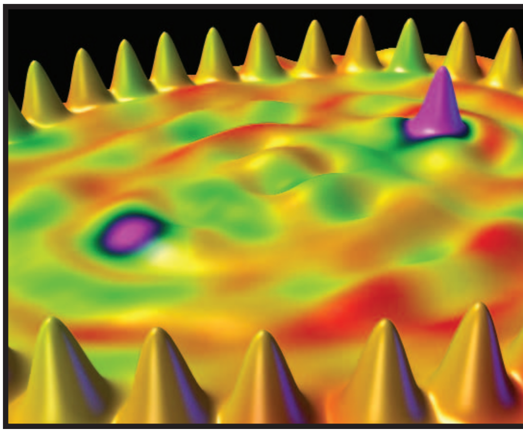


PHOTO CREDIT: IBM

About the author

Pedram Khalili Amiri was born in Tehran, Iran. Currently, he is an undergraduate student at Sharif University of Technology in Tehran, where he is studying Electrical Engineering. His interests include Quantum Computation, Semiconductor Device Physics and Fabrication, and Microelectronic Circuits. He would like to pursue an MS degree in either solid-state electronics or applied physics. He is also an experienced web-developer and has worked in the field for a company in Tehran.