# Making Weirdness Work: Quantum Information and Computation

John Preskill
Division of Physics, Mathematics and Astronomy
California Institute of Technology
Pasadena, CA 91125
626-395-6691
preskill@theory.caltech.edu

*Abstract— Information* is something that can be encoded in the state of a physical system, and a *computation* is a task that can be performed with a physically realizable device. Therefore, since the physical world is fundamentally quantum mechanical, the foundations of information theory and computer science should be sought in quantum physics. In fact, quantum information has weird properties that contrast sharply with the familiar properties of classical information. A quantum computer -- a new type of machine that exploits the quantum properties of information -- could perform certain types of calculations far more efficiently than any foreseeable classical computer. To build a functional quantum computer will be an enormous technical challenge. New methods for quantum error correction are being developed that can help to prevent a quantum computer from crashing.

TABLE OF CONTENTS



## 1. THE FUTURE OF INFORMATION TECHNOLOGY

You are probably aware that this is 1998. We are approaching the dawn of a new millennium. And as we look back at the 20th century, one of the most notable achievements of our civilization has been the development of our information technology. I think that my laptop computer is a pretty hot machine. But surely by, say, the end of the 21st century, the information technology that impresses us so much today will have been far surpassed by new technology that we cannot even imagine today. Even so, I intend to speculate here about the future of information technology.

This sort of projection of the future of technology is a task fraught with danger. Here is one cautionary tale. We recently celebrated the 50th anniversary of the ENIAC, which many people regard as the first electronic digital computer. It is interesting to see what people were saying back in the 40's about the future of electronic computing. Here is a quote from *Popular Mechanics* that appeared in 1949: "Where a calculator on the ENIAC is equipped with 18,000 vacuum tubes and weighs 30 tons, computers in the future may have only 1,000 vacuum tubes and perhaps only weigh one and a half tons." In fact, the computing power of the ENIAC is roughly equivalent to what is in a digital watch, and we have had digital watches since the 70's. So the visionary who said this evidently was not thinking big enough, or small enough.

No one can accurately predict the future of technology; that's a given. And aside from that, I am particularly ill equipped for this task. I am a theoretical physicist, not an engineer, and I am not particularly knowledgable about how computers work. But a physicist knows without hesitating that the crowning intellectual achievement of the 20th century has been the discovery of the quantum theory, and it is natural to wonder how the development of quantum theory in the 20th century will impact the technology of the 21st century.

A physicist knows that, whatever information might be, it is something that can be encoded and stored in the state of some physical system, like the pages of a book, or the sectors of a hard disk. But we also know that all physical systems are fundamentally quantum mechanical systems. So information is something that can be encoded in a quantum state. The question addressed here is: Can the computers of the future better exploit the quantum properties of information, to perform tasks that are beyond what can conceivably be achieved with conventional silicon-based information technology?

## 2. CLASSICAL AND QUANTUM BITS

To get stated, we'll need to recall some basic facts about information. All (classical) information can be reduced to elementary units, what we call bits. Each bit is a yes or a no, which we may represent it as the number 0 or the number 1. Anyone who has played the game 20 questions knows that much information can be conveyed by yes/no answers. A highly skilled player, by asking 20 questions, could in

principle distinguish about 1,000,000 different objects. And if we are willing to allow more questions, in principle any number of objects could be distinguished. So we say that any amount of information can be encoded in the yes/no answers.

I like to visualize a bit as an object, let's say a ball, that can be either one of two colors, let's say either red or green. Bits are valuable, and we can store a ball for safekeeping by sealing it up inside a box. Then if we open the box later on, the color of the ball that pops out is the same as the color that we put in; we can recover our bit and read it.

But in quantum theory, the elementary unit of information is something rather different from the classical bit --- I'll call it a quantum bit, or a "qubit" for short. We may think of a quantum bit as a box with a ball stored inside, but in this case, we can open the box through either one of two doors, door 1 or door 2. To an experimental physicist, the two doors correspond to two different ways to measure the quantum state of an atom, or of a particle of light, but let's not worry about that, we'll just think of it as a box with two doors.

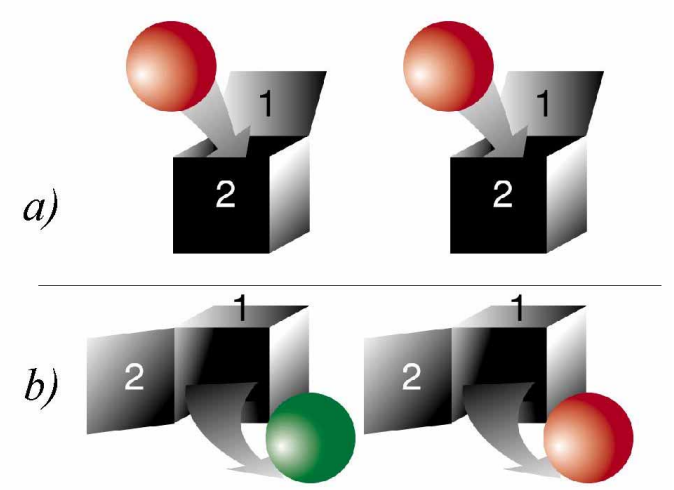


**Figure 1** If you put a ball in a quantum box (*a*), and then open the wrong door of the box (*b),* the color of the ball that comes out is *random*.

Suppose that we put a red or a green ball into the box, through either door 1 or door 2, close the door, and then open the same door again. The color of the ball that comes out is the same as the color that we put in, just as for a classical bit. But suppose that we put the ball into door number 1, and then we open door number 2. Then the color of the ball that comes out doesn't have anything to do with what we put in, the color is completely random --- 50% of the time it will be red and 50% of the time it will be green. If we open the wrong door, we can't read the information that was put into the box.

## 3. Hidden Information

We have now seen one way in which quantum information, information encoded in qubits, is different than classical information, information encoded in bits. You can't read quantum information unless you open the right door. But there is a more interesting difference between classical and quantum information, and to appreciate it, we'll need to suppose that we have two boxes. The boxes can be far apart. One of them is at Caltech in Pasadena, and the other is in the custody of a friend of mine who lives in the Andromeda galaxy. These boxes have some peculiar properties. First of all, if I open my box here in Pasadena, either through door 1 or door 2, the color of the ball that comes out is completely random. And the same is true for my friend in Andromeda. So when either one of us opens his box, through either door, we don't get any information; we don't find out anything about what is inside. But that's funny . . . we have two boxes so we should have been able to store two bits of information. How is that information encoded? Where is it hiding?

The answer is that the information is contained in correlations between what happens when I open a box in Pasadena and what happens when my friend opens a box in Andromeda. If I open my box through door number 1, I might find a red ball or I might find a green ball. But if I find a green ball, then if my friend also opens door number 1 or his box, he finds a green ball, too. And if I find a red ball, he always finds a red ball. Same thing if I open door number 2 and he opens door number 2 --- we are guaranteed to find balls of the same color. What he finds is *perfectly correlated* with what I find if we open the same door.

There are several different ways in which what happens when we open a box in Pasadena can be correlated with what happens when we open a box in Andromeda, and we have chosen one of those ways --- that's information. But in this case, there is no way to get access to any of the information, no way to read it, just by making observations in Pasadena or Andromeda. Instead, the information is spread out in a very nonlocal way, shared equally in a sense, between the box in Pasadena and the box in Andromeda. This property of quantum information, that it can be encoded nonlocally, is what we call *quantum entanglement*. It is the crucial way in which quantum information is different than classical information [1], and it is what underlies much of what I want to discuss here.

But not everyone is so impressed by these correlations. Correlations are not really so exotic; we encounter them all the time in everyday life. For example, I have a friend who, on any given day, decides at random to wear either red socks or green socks. (You may think my friend is rather eccentric, but among physicists he is considered quite normal.) Anyway, I can trust my friend to always wear two socks of the same color; he is very fastidious about that. So his socks are perfectly correlated. That means that, as soon

as I see one of his feet, and notice that he is wearing a red sock on that foot, I know for sure before I even look that there is a red sock on the other foot. And if I see a green sock on one foot, I know for sure that there is a green sock on the other foot, even without looking. So correlations are not at all unusual. On the one hand my friend always wears two socks of the same color, and on the other hand when we open our two quantum boxes, each through the same door, we always find two balls of the same color. Is there really any fundamental difference between these two things? Aren't the boxes just like the soxes?

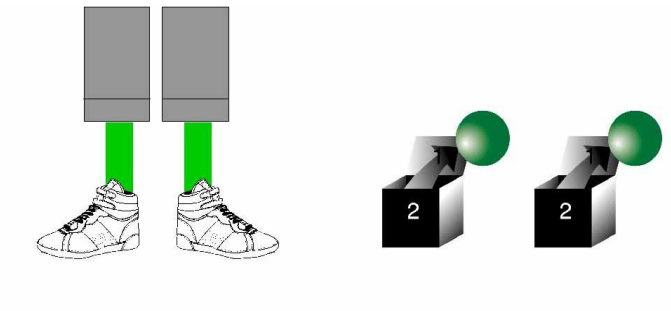


**Figure 2** Classical and quantum correlations.

## 4. Three Quantum Boxes

In fact, I want to argue that there is a profound difference between the boxes and the soxes. To explain why, it will be helpful to consider an even more peculiar friend of mine, one with three feet. This fellow also decides at random every day how to wear his socks, but he always wears an even number of red socks (either 0 or 2) and an odd number of green sock (1 or 3). I know him well, and I trust my friend; he never wears one red sock and never wears three red socks. That means that once I have seen two of his feet, I know with certainty, before I even look, what color sock is on the third foot. If I see a red sock and a green sock, the third sock must be red. If I see two green socks or two red socks, the third sock must be green.

Now I want to consider an analogous situation with quantum boxes instead of socks[2]. We have three boxes. And suppose that we decide to open door number 2 of one of the boxes, and door number 1 of the other two boxes. Every time we try this, we find that the number of red balls is even (0 or 2); we never find one red ball or three red balls. I have tried this a million times, so I am sure that it's true. Trust me.

This is interesting, because suppose that I want to know what will happen when I open the third box, either through door 1 or door 2. I can find out ahead of time, before I open that box, by opening the first two boxes. Let's say I am interested in knowing what will happen when I open door number 1 on the third box. I can open door number 1 of the first box and door 2 of the second box, and suppose that I find one green ball and one red ball. Then I know for sure that I will find a red ball when I open door 1 of the third box. Or if I would like to know what will happen when I open door number 2 on the third box, I first open door number 1 on the first two boxes. If I find two green balls, I am sure to find a green ball when I open door number 2 of the third box.

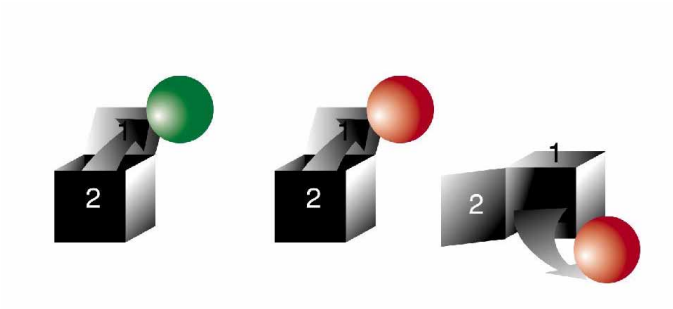


**Figure 3** A quantum correlation among three boxes.

It could be that these boxes are very far apart. Maybe one is in New York, one in Chicago, and one in Pasadena. Well, it seems obvious that opening boxes in New York and Chicago cannot have any influence on what happens when we open a box in Pasadena. So a reasonable person would say that the boxes are like socks. When I look at two of my friend's feet, and see a red sock and a green sock, I don't think that I made his third sock turn red by looking at the first two socks. I just think that I found out enough about what socks he is wearing today to know that the third sock is red. He had a red sock on that foot all along, but I didn't know it until I looked at the first two feet. So naturally, we assume that it is the same for the quantum boxes. Opening the first two boxes did not change anything inside the third box; it just gave us enough information to figure out what was in the third box all along.

All right, now let's try something new. What will happen if we open door number 2 on all three boxes? We haven't tried this before, so we don't really know. But let's try to use some theory. Let's see if we can make a prediction about what will happen before we open the boxes. That will make the experiment more fun.

How are we going to make a prediction? I'll reason this way: Another thing we haven't tried is opening door number 1 on all three boxes, so I don't know what would happen if we did that. But let's make an assumption. Let's suppose that if we open door number 1 on all three boxes, we'll find three red balls. It's just a hypothesis, but let's assume this. If that's the case, I can tell you for sure what will happen if we open door number 2 of any of the boxes. You remember, we know for sure that if we open door number 2 on one box, and door number 1 on the other two, we always find an even number of red balls. There is no doubt about that; we have checked it a million times. So, if we make our

assumption about what happens when we open door 1 on all the boxes, what can we say about what happens when we open door 2 on, say, the first box? Well, since we find two red balls when we open door 1 of the second and third boxes, we know for sure that we'll have to find a green ball when we open door 2 of the first box. Similarly, we have to find a green ball if we open door number 2 of the second box, because we find two red balls when we open door 1 on the first and third boxes. By the same argument, we have to find a green ball when we open door 2 of the third box. So from what we already know about the boxes, we can deduce that if we would find three red balls when we open door 1 of all three boxes, we must find three green balls when we open door 2 of all three boxes.

Okay. The only thing is that we don't really know what will happen when we open door number 1 of all three boxes; we just assumed we would find three red balls, and maybe that's not true. But we can make a list of all of the things that we could conceivably find were we to open door 1 on all three boxes. There are altogether eight possibilities, and here (in the first column) is the list:

| Open Door 1 | Open Door 2 |
|---|---|
| Red Red Red | Grn Grn Grn |
| Red Red Grn | Red Red Grn |
| Red Grn Red | Red Grn Red |
| Grn Red Red | Grn Red Red |
| Red Grn Grn | Grn Red Red |
| Grn Red Grn | Red Grn Red |
| Grn Grn Red | Red Red Grn |
| Grn Grn Grn | Grn Grn Grn |

Now, for each of these eight possibilities, we can use the same reasoning that I just described to infer what will happen if we open door number 2 on all the boxes, obtaining the list in the second column. And we find something interesting. For each of the eight possibilities for what could happen when we open door number 1 on all the boxes, we conclude that when we open door number 2 on all of them the number of red balls must be even --- it can be 0 or 2, but it is never 1 or 3. So, it turns out that we really can make a prediction.

Let's review what we've done. We have three boxes. And we know for sure that if we open door number 2 on one box and open door 1 on the other two, we always find an even number of red balls. No doubt about it; we've checked it a million times. Now we have been able to use simple logic to infer what must happen if we open door number 2 on all three boxes. We concluded that we must find an even number of red balls. Does our theory work?

In practice, an experiment with three quantum boxes is hard to do, but quantum mechanics makes a firm prediction about what we would find, a prediction for which ample experimental confirmation has been found in other related contexts. The result is rather shocking. Every time we open door 2 of all the boxes, we find an *odd* number of red balls, just the opposite of what we have just inferred!

If we review our reasoning to try to figure out where we went wrong, there seems to be only one place where we could have tripped up. We made the eminently reasonable assumption that the act of opening a box in New York and opening a box in Chicago could have no influence on the contents of a box in Pasadena. That's certainly how it works for socks. But our "experiment'' has shown that it doesn't work that way for boxes. The boxes are not like the soxes. The experimental evidence has left us with no choice but to conclude that opening two of the boxes doesn't just tell us what was in the third box all along; opening those boxes actually shapes what we will find when we open the third box. Hence there is a strange kind of nonlocality built into the foundations of quantum physics.[1]

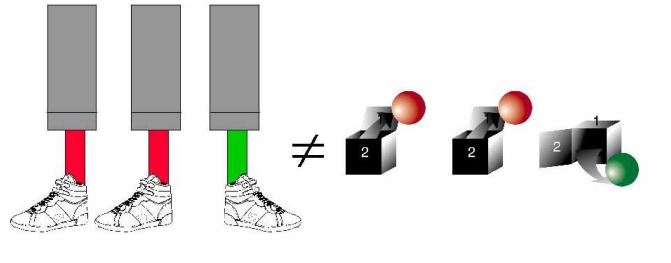


**Figure 4** Boxes are not like soxes.

Not everyone is happy about this. One who was unhappy was Albert Einstein. He derided these nonlocal correlations between boxes as "spooky action at a distance" (except he said it in German). Einstein argued from this syllogism: A. I am Albert Einstein. B. I do not understand quantum mechanics. Therefore, C. Quantum mechanics is wrong. Actually, it is a strong argument. But we have been living with quantum mechanics for over seventy years now, and we still can't find anything wrong with it. So it seems that it doesn't really matter whether Einstein liked it or not, we have to accept that this weird nonlocality is an essential part of the description of Nature.

The human mind does not seem to be well equipped to grasp this aspect of Nature, and so we speak of the weirdness of quantum theory. Some people think that weirdness is ugly, but I don't really think so. If Nature is weird, so be it, and let's try to get used to it. But we can also go a step further, and see if we can put the weirdness to work. Does quantum weirdness enable us to perform tasks that would be impossible in a less weird world?

## 5. Quantum Copying

As we search for ways to exploit the weird properties of

[1] But it is important to understand that this "nonlocality'' does not enable us to send any message to a remote location faster than a light signal could travel there.

quantum information, a good place to start is to think about copying information. How would a quantum copy machine operate? Suppose we have a quantum box, and I happen to have put a ball inside through door 2. The copier looks at the box and builds a second box. Now if we open both boxes, the original and the copy, through door number 2, we will find balls of the same color. And if I have put a ball in the original box through door number 1, then when I open both the original and the copy through door number 1, I will find balls of the same color.

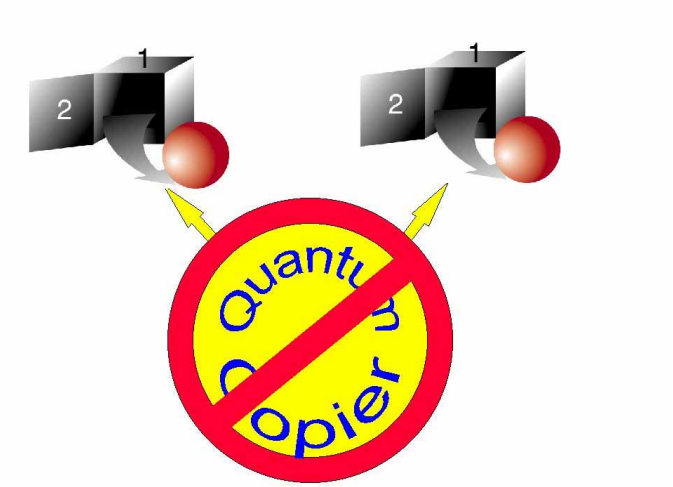


**Figure 5** Quantum information cannot be copied perfectly.

But there is no such machine. The trouble is that to copy what is inside, the copier needs to open the box. But it has no way of knowing whether I put my ball in door 1 or door 2. It might guess right, and open the correct door, and then it can make a good copy. But if it guesses wrong and opens the wrong door, it will damage the information that I stored in the box, and it won't be able to copy it faithfully. Quantum information cannot be copied[3].

This is disconcerting. Sometimes it is very useful to be able to copy information. On the other hand, sometimes it might be a good feature if information cannot be copied. For example, were we to carry quantum dollar bills, we would not have to worry about counterfeiters. Well, I don't know what kind of money people will be carrying around in their pockets one hundred years from now; I don't even know if they'll have pockets. But one thing I am sure about. Even at the end of the 21st century, humans are going to want to keep secrets. That we can't copy quantum information might be a good thing, if it enables us to build a quantum telephone that cannot be tapped[4].

You see, I have a friend named Alice, and Alice is very anxious to place a very private phone call to a man named Bob. But Alice has a very nosy friend named Eve, and Eve is habitually listening in on the extension. Alice needs to find a way of calling Bob where she can be sure that Eve is not eavesdropping. Obviously, Alice and Bob should use some sort of code. But it happens that Eve, in addition to being very nosy, is also extremely smart. And she likes nothing better than breaking codes --- she absolutely revels in code-breaking. Alice is not at all confident that she is smart enough to think up a code that Eve cannot break.

But Alice knows that if she only had a string of random numbers, and she could send those random numbers to Bob, then Alice could use the random number as a key to code her message, and Bob could use the key for decoding. Then if Eve were to intercept the message, it would be completely random junk, and there would be no way for Eve to decode it. That is, there would be no way for Eve to decode the message unless she had the key. So the problem that Alice and Bob need to solve is: How can Alice send the random key to Bob, and be assured that there is not way for Eve to have intercepted the key?

Let's see how quantum information can be used to solve this problem. Alice first assembles some random bits --- balls that are either red or green. Then she gets some boxes, and decides at random to put each ball into either door 1 or door 2 of the corresponding box. She seals the boxes shut, and then sends them to Bob. Bob does not know which door Alice used on each of the boxes. But he decides at random to open each box through door 1 or door 2. Now it will happen by chance that about half the time, Bob will open the same door that Alice used, and in those cases the ball that Bob finds will be of the same color as the ball that Alice put in the box. But about half the time, Bob will open the wrong door, and then he won't find out anything about what Alice put in the box.

But now that Bob has safely recovered and opened the boxes, so it is too late for Eve to do anything about it, Alice can make a public announcement telling which door she used on each of the boxes; it doesn't matter if Eve finds out at this point. With this information, Bob now knows for which boxes he opened the right door, and he can share that information publicly with Alice. (That is, it becomes public knowledge that Bob opened the right door, but he doesn't tell anyone what he found in the box.) Now Bob and Alice share a set of random bits; Alice has successfully sent the key to Bob.

What about Eve? She will surely try to intercept some of the boxes while they are being shipped from Alice to Bob. But to find out what is inside, she will need to open the boxes. If she happens to open the right door (the door that Alice used), then she can copy the information, and Bob will never be the wiser. But sometimes she will open the wrong door, and so might change the color of the ball. Now Bob and Alice can conduct a test to see what Eve has been up to. They can publicly compare a small portion of their key, to make sure that Bob really received what Alice sent. If they agree, then they can be highly confident that Eve didn't open any boxes (or at least that she opened very few boxes). But if they disagree, then they know that Eve has been up to no good.

We can't stop Eve from trying to eavesdrop; that's what Eves do. But because quantum information cannot be copied without disturbing the information, we can detect Eve's activity. If the test is unsuccessful, then Alice won't use that key to encode a message. But if the test is successful, Alice can converse with Bob secure in the knowledge that Eve cannot listen in.

## 6. Quantum Computing

We have discussed one feature of quantum information (it cannot be copied) that can be put to use: it can be used for private communication. But there are deeper properties of quantum information that I think have far greater technological potential. To understand why, let's return to the differences between classical bits and quantum bits.

Let's suppose that we have 10 boxes containing classical bits. There are a lot of possible arrangements of those classical bits --- lots of ways to put red and green balls in the boxes. But any one arrangement is very simple to describe; I just have to tell you whether each ball is green or red. With quantum bits things are different. Suppose we have 10 quantum boxes. Now it is quite complicated to describe even one typical arrangement of the 10 boxes. In this case, it is not correct to say that each ball is either red or green. Typically, each ball has the potential to be red and the potential to be green, depending on which door we open. Furthermore, the boxes are correlated. Opening any one of the 10 boxes has an "influence" on what happens when we open the other nine, so our description must include a characterization of those influences. It turns out that to give a complete mathematical description of a typical configuration of 10 quantum boxes, I would have to write down about 1,000 numbers.

And the complexity of the description rapidly escalates as I add more boxes. With 20 quantum boxes, we need about 1,000,000 numbers to give a complete descriptions of all the influences of each box on the others. With 30 boxes, we need 1,000,000,000 numbers. It turns out that for a relatively modest number of boxes (about 300), to write down a complete description of a typical configuration would require more numbers than the number of atoms in the visible universe. It is clear that no such description could ever be written down, even in principle.

So there is no hope of even describing the typical state of a few hundred qubits, no way to write down the description using ordinary classical bits. This feature of quantum information seemed very intriguing to Richard Feynman. Feynman was led to ask a very interesting question[5]; he wondered, might it be possible that a computer that operates on qubits (rather than classical bits) would be capable of performing tasks that would be inconceivable using conventional silicon-based digital technology? Feynman's idea was that there may be problems that are very hard to solve using ordinary computers that would become easy to solve if we used a quantum computer instead.

To get a better feel for what this idea means, let's consider an example of a problem that is hard for ordinary computers to solve. You probably know what a prime number is --- we say that a whole number is prime if it cannot be divided evenly by any whole number aside from itself and 1. Now, with prime numbers, we can play an interesting game, called Find the Factors. I give you a number that can be expressed as a product of two prime numbers, and you have to tell me what those prime factors are. (It's like *Jeopardy*: I give you the answer, the product of the two numbers, and you have to tell me the question: What two numbers did I multiply together to get the product?

Okay, let's start with this one:

$$91 = ? \times ?$$

91 can be written as a product of two prime numbers. What are they? Right, it's $91=7\times13$. But as the numbers get bigger, the game gets a lot harder. Can you do this one?

$$2537 = ? \times ?$$

With a piece of paper and a pencil and a few minutes, you can probably figure out that $2537=43\times59$. As you can see, as the size of the number that we are trying to factor increases, the difficulty of the game escalates very rapidly. Until we get to this one:

$$\begin{array}{l}180708208868740480595165616440590556627810251676940134917012702145005666254024404838734112759081230337178188796656318201321488055 7\end{array} = ? \times ?$$

This 130-digit number can be expressed as a product of two 65-digit prime factors. Finding the factors is hard, but it is not quite impossible --- this may be the hardest factoring problem that has ever been solved by a computer. It was done last year, and it is interesting how it was done --- the computation involved a network of hundreds of powerful workstations collaborating and communicating over the internet, and it took several months[6]. But as we add further digits to the number to be factored, the time required to do the computation grows so explosively that, say, factoring a 200-digit number is still far beyond what existing computers can accomplish. So perhaps this is a good context to consider Feynman's challenge. Classical computers will never be able to factor very large numbers. Could a quantum computer do better?

Why is factoring so hard? Searching for the prime factors of

our number is like trying to unlock a padlock; if we can find the right key (the right prime factors) the key will open the lock. But there are many, many keys to try, many possible prime numbers that might divide our number. We can solve the problem by trying one key after another, until we finally find the key that opens the lock, but because there are so many keys, this takes a very long time. With a quantum computer we can do much better --- we can try many, many keys in many, many locks all at the same time. As we have seen, a collection of a modest number of qubits (just a few hundred) can in a sense encode an enormous amount of information. By performing our computation only once, but on qubits rather than ordinary bits, we can achieve the same effect as if we had performed the computation with ordinary bits over and over and over again.

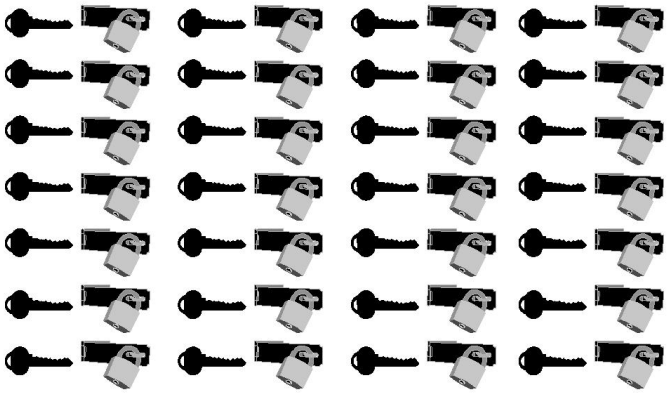

**Figure 6** With a quantum computer, we can make many attempts to solve a hard problem all at once.

The secret of the quantum computer is that we can invoke a kind of massive parallelism, we can do a very large number of computations all at the same time. Designers of conventional computers often speak of parallelism, of computers with many processors working together on a problem. But a quantum computer can achieve a level of parallelism that we could never dream of with a conventional machine --- with only hundreds of qubits, we can perform simultaneously a number of computations that exceeds the number of atoms in the visible universe. We'll never build a conventional computer with that many processors.

What might this mean in practice? With conventional computers, we can now factor a 130-digit number in a few months, let's say one month. But if we take into account how the difficulty of the computation grows as we add digits, we can estimate that that same network of computers would be able to factor a 400-digit number in about 10 billion years, about the age of the universe. So factoring a 400-digit number really is Mission: Impossible. Even with vast advances in computing power, we won't be factoring 400-digit numbers anytime soon. But suppose we had a quantum computer that could also factor a 130-digit number in one month. (That's a very big assumption, but let's make it anyway.) Because of the massive parallelism that a quantum computer can employ, the time it takes to do the computation grows at a much more modest rate. We can estimate that it would take a few years to factor the 400-digit number, which would be feasible. Because of this much more favorable scaling of the computation time with the size of the problem, quantum computers will always have a huge advantage over classical computers for sufficiently complex problems. (That a quantum computer could be an efficient factoring engine was pointed out by an exceptionally clever computer scientist named Peter Shor[7].)

## 7. Quantum Hardware

Perhaps you are persuaded that a quantum computer would be a wonderful thing to have if we could only build one. But how will we build one? What sort of hardware will a quantum computer have? If we want to be able to manipulate quantum bits, one way to do that (perhaps not the only way, but one way) would be to encode and process the information at the level of single atoms. The technology now exists to suspend an array of individual atoms in a vacuum using electromagnetic fields, and to store the trapped atoms for a long time. Each atom can be in either one of two possible quantum states, so we can still represent them as red or green balls. Since they are individual atoms, such tiny little fellows, you might think it would be hard to see whether each atom is red or green. But in fact that is not very hard. We can shine a laser on each of the atoms, and if the color of the laser light is chosen just right, then all of the red atoms will scatter the light so they will glow visibly; the green atoms won't interact with the light at all, so they will remain dark. We easily see, then, which of the atoms are red and which are green.

Of course, we want to do a lot more than just look to see if the atoms are red or green; we want to process the information in the atoms and build up a complex and interesting quantum computation. And in particular, if the quantum computer is to realize its potential to perform tasks beyond what classical computers can do, it must prepare and manipulate configurations of the atoms in which they have complicated nonlocal correlations. I will briefly sketch how this might be done[8]. First we shine a laser on one of the atoms. If we choose the color of the laser light just right, then the light will not interact with the atom at all if the atom is red. But if the atom is green and we leave the laser on for just the right amount of time, then the atom will change from green to red, and at the same time the laser will stimulate that atom, and all the atoms in the trap, to begin vibrating back and forth. If we now direct a laser at another of the atoms, and we choose the proper color for the laser light, then this laser will not interact with the atom if it is not vibrating, but if it is vibrating, and we leave the laser on just long enough, that atom will change color, and the vibration of all the atoms will cease.

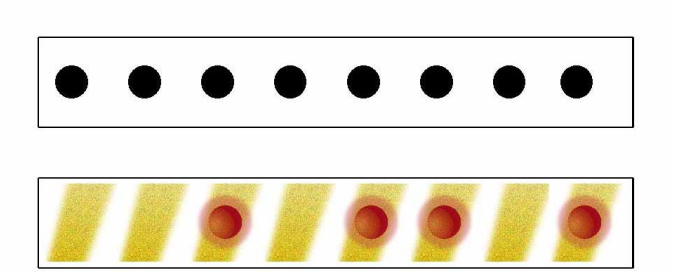

**Figure 7** Reading out quantum information in an ion trap. When the laser is turned on, the red balls glow, and the green balls remain dark.

Look at what we have achieved. If the first atom is red, no laser ever interacts with any atom and nothing ever happens. But if the first atom is green, then the two atoms change color. This operation therefore induces a correlation between the colors of two atoms in the trap. By performing many such operations in succession, we can build up a complex and interesting quantum computation.

It is currently possible to do experiments like this involving one or two qubits and one or two operations[9]. But for a quantum computer to be able to do computations that compete with the best that digital computers can achieve, we will need to scale this up enormously. We'll need machines with thousands of qubits (not necessarily atoms in a trap, but qubits of some kind) capable of performing millions or billions of operations. Clearly, the technology has a long way to go before quantum computers can fulfill their destiny to become the world's fastest machines.

## 8. Quantum Error Correction

How hard will it be to build a large-scale quantum computer that really works? As a theorist, I am interested in any obstacles that may be a matter of principle rather than just a technological barrier. A particular serious concern is that quantum computers will be far more susceptible to making errors than conventional computers. How will we prevent a quantum computer from crashing?

Errors can be a problem even with classical information. We all have bits that we cherish, because information can be very valuable to us, but everywhere there are dragons lurking who delight in tampering with our bits. With classical information there are well known ways to protect ourselves against the dragons. Say we have a ball that is supposed to be red. Then we can store three copies of the red ball. Once in a while a dragon may appear and paint one of our balls green. But there is a busy little beaver who checks the balls periodically, and whenever he sees that one of the balls is a different color than the others, he changes the color of that ball so that it matches the color of the other two. We see that redundancy (having three red balls instead of just one) can protect us from errors. If the busy beaver is quick enough, he can prevent the dragon from damaging our bits.

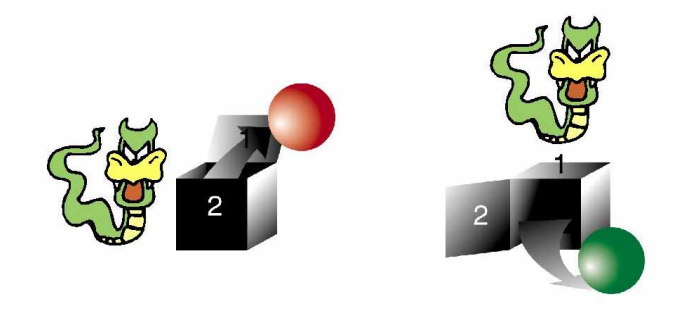


**Figure 8** Two types of errors in quantum information. The dragon can change the color of the ball through either door.

But what can we do to protect a *quantum* bit from the dragon? Here too we can try to use redundancy for protection, but we can't do it in quite the same way as with classical bits. We can't replace our box by three identical boxes, the original plus three replicas, because we have already seen that quantum information cannot be copied. Furthermore, when the dragon comes along he might open door number 1 of the box, change the color of the ball, and reclose the box, or he might open door 2, change the color, and close the box. The beaver needs to be able to fix the error without knowing whether the dragon opened door 1 or door 2.

It turns out that it really is possible to protect quantum information from errors[10]. With quantum information, though, it isn't enough to replace a box by three boxes, we actually need five boxes. And the boxes are not all identical replicas of the information that we want to safeguard. Instead, the information to be protected is encoded in correlations involving all five of the boxes, like the nonlocal correlations between Pasadena and Andromeda. That way, there isn't any information in any one of the boxes; instead it is shared among all the boxes. That means that if the dragon damages one of the boxes, the information still remains intact, because it wasn't in that box anyway. Now the beaver can come along and figure out which box the dragon has messed with, and reset that box to its original state. So it seems that redundancy can be used to protect quantum information just as it can protect classical information. However, the redundancy works in a quite different way --- information is protected by storing it in correlations involving many boxes.

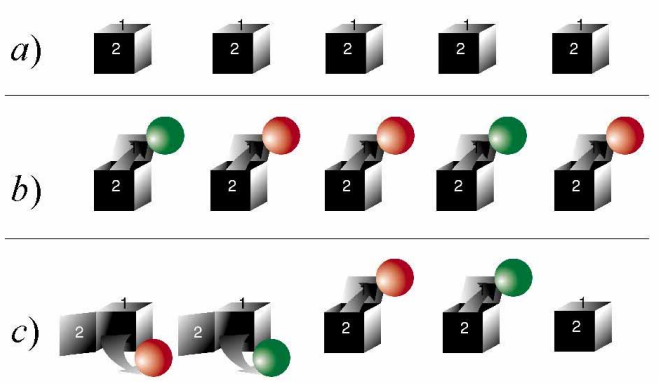


**Figure 9** A simple quantum error-correcting code. (*a*) One qubit of information is encoded in correlations among five different boxes. (*b*) We can measure the encoded qubit by opening door number 1 on all five boxes, and observing whether the number of green balls is even or odd. (*c*) Different types of errors modify the correlations among the boxes in distinguishable ways. We may diagnose the error by opening door number 1 of two boxes and door number 2 of two other boxes --- if the number of green balls is odd, then an error has been detected. Four such measurements of four boxes each suffice to identify which box is damaged and what action will repair it.

## 9. The Road Ahead

I have described a lot of properties of quantum information. We saw that the fundamental unit of quantum information is the qubit, which we may envision as a box with a ball inside that is either red or green, such that we can open the box to see what is inside through either one of two doors. The qubits can have peculiar correlations that we cannot reconcile with our usual classical notion of a correlation: the boxes are not like the soxes. Quantum information cannot be copied, and we may therefore use it for private communication. The mathematical description of even a modest number of qubits is exceedingly complex, and we may therefore use qubits to perform massively parallel computations, achieving an enormous speedup compared to the time required to do a computation on a conventional computer. We can safeguard quantum information from errors by encoding the information in correlations involving many boxes. And I have told you that the first experiments that process quantum information have been carried out in the last few years.

Clearly the technology must progress a long way before quantum computers are ready to fulfill their destiny as the world's fastest machines[11]. There is a long road ahead. When will quantum computers that solve hard problems become a reality? I really have no idea. But we have come a long way in the 50 years since the ENIAC, and it seems reasonable to me that in another 50 years quantum computers will be in widespread use. I could be completely wrong. Maybe quantum computers will never be widely used. Or perhaps I am being way too conservative, like *Popular Mechanics* in 1949.

And what of the shorter-term prospects for putting the weirdness of quantum theory to work for fun and profit? The technology for quantum communication is much more mature than that for quantum computation. Prototype key exchange devices have already been built and tested. These might conceivably see commercial use in just a few years, though at first they would be only for the most paranoid users requiring the utmost in privacy. Ideas generated by recent work on quantum computation are leading experimental physicists to develop new methods for preparing exotic quantum states, and for performing new types of measurements that we could not even conceive of a few years ago. And recent theoretical developments are deepening our understanding of quantum information and the ways it differs from classical information. Particularly significant, I think, is the finding that quantum information can be protected from errors with suitable coding methods; I expect that development to have broad ramifications throughout experimental physics.

The road to quantum computation may be a long one, and there is no telling for sure how long, but it certainly has been and will continue to be a fascinating voyage.

## References

[1] J. S. Bell, *Physics* **1**, 195, 1964.

[2] D. M. Greenberger, M. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Mechanics, and Conceptions of the Universe*, ed. M Kafatos, Dordrecht, the Netherlands; Kluwer, 1989, p. 69; N. D. Mermin, *Physics Today*, June 1990, p.9.

[3] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature* **299**, 802, 1982; D. Dieks, "Communication by electron-paramagnetic-resonance devices, *Physics Letters A* **92**, 271, 1982.

[4] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, New York; IEEE, 1984, p. 175.

[5] R. P. Feynman, "Simulating physics with computers," *International Journal of Physics* **21**, 467, 1982.

[6] A. K. Lenstra, J. Cowie, M. Elkenbracht-Huizing, W. Furmanski, P. L. Montgomery, D. Weber, and J. Zayer, "RSA factoring-by-web: the world-wide status, online document http://www.npac.syr.edu/factoring/status.html, 1996.

[7] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings of the 35th Annual*

*Symposium of Fundamentals of Computer Science*, Los Alamitos, CA; IEEE, 1994, p 124.

[8] J. I. Cirac and P. Zoller, Quantum computations with cold trapped ions," *Physical Review Letters* **74**, 4091, 1995.

[9] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, "Measurement of conditional phase shift for quantum logic," *Physical Review Letters* **75**, 4710, 1995; C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a fundamental quantum logic gate," *Physical Review Letters* **75**, 4714, 1995.

[10] P. Shor, "Scheme for reducing decoherence in computer memory," *Physical Review A* **52**, R2493, 1995; A. M. Steane, "Error correcting codes in quantum theory," *Physical Review Letters* **78**, 2252, 1996.

[11] J. Preskill, *Proceedings of Royal Society of London A* **454**, 469, 1998.

***John Preskill*** *is Professor of Theoretical Physics at Caltech, and a member of QUIC, a Caltech-based institute devoted to the study of quantum information and computation. His other research interests include the theory of elementary particles, quantum gravity, and the very early universe. He received an A.B. from Princeton in 1975 and a Ph.D. from Harvard in 1980.*