

# The Best Computer in All Possible Worlds

by Tim Folger

---

**D**avid Deutsch prefers not to travel. He would rather remain in his study, working. And after listening to the 42-year-old Oxford physicist for a moment, you understand his predilection. How horizons-expanding could any trip be to a man who believes that untold numbers of universes coexist with our own, and that many of them contain a David Deutsch, also happily ensconced in his study?

Deutsch's lack of intimate contact with the world at large does not preclude his ability to change it profoundly. Ten years ago he conceived of a new type of machine--a quantum computer--which at the time seemed unlikely ever to be built. Now a handful of physicists are actually trying to construct the computer Deutsch envisioned, one whose fundamental components are single atoms or even individual particles of light. If someone succeeds--and it must be said that the technological obstacles are formidable--the very existence of such a device, Deutsch believes, will validate his rather unusual view of reality, or as he might say, realities.

A quantum computer would not be merely another step down the well-trodden and seemingly endless road toward ever smaller and more powerful computers. It would in some sense be the ultimate computer, less a machine than a force of nature. Paradoxically, it would take what had appeared to be an unavoidable limitation on computer power imposed by the laws of physics and turn that limitation into a new way of processing information, one that would dwarf the capacities of any existing computer.

A remarkable device, to be sure--but one whose actuality leaves Deutsch unmoved. "I really would be hardly interested in this at all if it weren't for the implications for physics," he says. "I'm a theoretical physicist. I want to understand physics fundamentally. It's not particularly my brief to make better computers."

Nevertheless, Deutsch's work directly addresses a central problem in computer technology: namely, that components cannot continue to shrink indefinitely. At some point we will be able to squeeze no more circuits onto a chip, and thus wrest no more speed, no more power out of our powerful, speedy machines. "At the current rate, we're going to hit the atomic scale in 20 years' time," says MIT physicist Seth Lloyd. When that happens, the rules of classical physics that govern the way computers operate will begin to break down and the laws of quantum mechanics will take over.

In quantum mechanics, protons, electrons, and other particles are like slippery politicians--you can't precisely pin down their positions. In fact, the counterintuitive laws of quantum mechanics actually require a particle to be in more than one place at a time, as long as no one is watching. Only when someone tries to observe the particle will it behave reasonably and settle down.

Most physicists have viewed the strange quantum domain as a barrier, perhaps an insurmountable one, to

further increases in computer power. The unpredictable nature of quantum mechanics, they thought, would make precise computations impossible for atom-size computer circuits.

Deutsch doesn't see it that way. He believes--and a growing number of physicists are beginning to think he may be right--that quantum mechanics, far from being a limitation to computation, may be a boon. In a tour de force paper published ten years ago, Deutsch explained how it may be possible to build a computer that, by taking advantage of a particle's ability to be in many places at once, could routinely handle problems that now require so many computational steps that they are impossible to solve.

To understand Deutsch's faith, you have to start with the classic demonstration of quantum mechanical weirdness: the two-slit experiment. Cut two slits in a screen, and shine a light through them onto a piece of film. The light will produce a characteristic pattern of alternating light and dark lines. This pattern is easy to explain if you assume, as physicists did until this century, that light is a wave: the light and dark areas result from the constructive and destructive interference of waves of light traveling through the slits.

But physicists now know that light is made of particles called photons. So what happens when you send individual photons, one at a time, toward a two-slit screen? Naively one might expect the photons to produce two clusters of dots on the film, one cluster behind each slit. But instead of clusters, a wavelike interference pattern shows up. There are two ways to explain this odd result. One is strange, the other beyond the pale. Deutsch, perversely, favors the latter.

Most physicists would say that each individual photon behaves like a combination of minute waves. Somehow this "wavelike particle" spreads out so that it passes through both slits simultaneously to produce the observed interference pattern. In any case, the photon appears to follow two different paths at the same time. With more slits, the photon would simultaneously traverse even more paths. In general, a photon, according to quantum mechanics, follows every possible optical path between two points.

Deutsch's view of what's happening is, it's fair to say, different. Very different. To him, the photon does not go through both slits at the same time. Obviously, he says, the particle must pass through one slit or the other. But don't start applauding him yet for common sense. Unless, that is, you feel more comfortable with the notion of parallel universes than you do with a particle's being in two places at once in this universe.

An extremely large number--perhaps an infinite number--of these parallel worlds exist, says Deutsch. They reveal their existence whenever a particle has the opportunity to follow more than one path--which, of course, is essentially always the case. When a photon, for example, goes through one of the two slits, something exceedingly strange happens. In our universe, Deutsch says, the photon goes through one slit. But in some other universe, it goes through the other. These alternate realities thereafter continue to exist, with identical pasts but different futures. ("There is another universe that is as real as ours," Deutsch said during an interview, "in which I fail to get through to you today, and we'll only be talking tomorrow.") The interference pattern we see in the two-slit experiment, says Deutsch, arises because the two universes interact.

Such interference between worlds, he points out, is detectable only under very carefully controlled conditions. The interference is a rare example of two universes that have briefly diverged--in this case when the photons went through different slits--and then merged into one reality, leaving only the interference pattern as evidence of their once independent status. Normally, outside the bounds of an

experiment specifically designed to create interference, particles that split off into separate realities will go off and collide with various other particles, and these with still others, in an unending, diverging cascade. The chance that any two of these many different worlds, each marching to the beat of its own capricious quantum drummer, will subsequently evolve along identical paths is vanishingly small. So while many David Deusch occupy these assorted worlds, they will never meet. Only the evanescent warp and woof of quantum mechanical interactions stitch these universes together.

This outré version of physics is known as the “many worlds” interpretation of quantum mechanics. It was originally proposed by the late Hugh Everett--a highly regarded though maverick physicist unaffiliated with any institution--and has never had a wide following. Physicists look for elegance and simplicity in their theories; conjuring up neighboring universes to explain the behavior of photons barely seems rational, let alone elegant. What appeal does it hold for Deutsch? And what does it have to do with computers?

Deutsch prefers the many-worlds view because he finds other interpretations of quantum mechanical phenomena vague and unsatisfying. The conventional explanation, he says, holds that the act of observation somehow forces a quantum mechanical system into a particular state; before the observation, one simply cannot say that the photon is in one place or another. Aside from being vague, says Deutsch, this view implies that observers in some way alter what they perceive, which raises all sorts of impossibly knotty questions about consciousness and physics. For all its seeming outlandishness, he says, the many-worlds theory is not that strange when you consider the alternative. As for computers, he says, “If you work on the quantum theory of computation at all seriously, it’s almost impossible not to adopt the many-universes interpretation.”

Computation, he notes, is not an abstract process. Ultimately it must have some physical basis. Whether it’s atoms or photons--or electric currents in a conventional computer--something must be manipulated in some way to carry out a calculation. To make his point, Deutsch cites the work of Peter Shor, a mathematician at AT&T Bell Laboratories in New Jersey.

Last year Shor proved that a full-blown quantum computer, if one is ever built, could factor any number, no matter how long, in seconds. To say that is a task beyond the reach of today’s computers is a tremendous understatement. It is a task utterly impossible, even for the fastest supercomputer in the world--the Fujitsu Numerical Wind Tunnel, which can carry out 170 billion operations per second. Last year a network of 1,600 computers around the world managed to factor a 129-digit number in eight months. A 250-digit number would have taken centuries. Factoring such numbers is no mere academic exercise. The keys needed to decipher secret corporate and government codes rely on the premise that factoring extremely large numbers is, for now, impossible.

Even the Fujitsu can manipulate at most a few thousand numbers at any one time. Deutsch says that a quantum computer could increase that capacity almost beyond measure. The trick would be to manipulate the quantum mechanical properties of photons, atoms, or other particles. This, says Deutsch matter-of-factly, would allow the computer to carry out calculations simultaneously in many parallel universes. He estimates that a quantum computer, using just 1,000 atoms or photons in place of conventional computer circuits, would have access to more universes than there are atoms in our universe.

Shor, in constructing his proof of a quantum computer’s potential, in effect wrote a program for a computer that doesn’t exist. It factors large numbers by working on all the possible answers to a problem

simultaneously. Correct answers--that is, factors of the number in question--appear in the form of a unique interference pattern at the end of the computer's calculations, which the computer could read like some otherworldly supermarket bar code. Shor's program cleverly causes all numbers that aren't factors to cancel out in the interference pattern, like waves whose crests and troughs annihilate each other.

Deutsch claims that if a quantum computer that can run Shor's program is ever built, it will be difficult for other physicists to deny the many-worlds model of quantum mechanics, fantastic as it seems. For example, he asks, what would happen inside a quantum computer that used Shor's program to factor a number that is, say, 250 digits long? To solve such a problem, he answers, the computer would have to perform roughly 10500 computations. "There is no way that we know to get the answer in fewer than that number of steps," he says. "If you were to write down on a piece of paper what the computer is doing, you'd have to write down about 10500 different lines of reasoning. That's an irreducible number. The outcome depends logically on all those components. Now, there are only 1080 atoms in the universe." So, if a quantum computer can solve a problem in which the number of calculations greatly exceeds the number of atoms in the universe, how did the computer do the calculation?

"It's pretty clear that it wasn't by jiggling about the atoms and energy and stuff that we see around us," says Deutsch. "Then where was it performed?"

Deutsch emphasizes again that computation is a physical process. Just as someone using an abacus must push beads around to get an answer, a computer must manipulate real particles--atoms or photons or what have you. And if a computer must manipulate more atoms than exist in one universe to complete a calculation, it must be drawing on the resources of many particles in a vast web of linked universes.

Can anyone seriously hope to build this universe-spanning machine? Deutsch is convinced the deed can be done, though a full-scale quantum computer is probably decades away, at best. "Technological progress in this area has absolutely amazed me in the last couple of years," he says. "When people asked me this question three or four years ago, I used to say this is a matter of centuries. Now I'm much more optimistic."

Deutsch's improved outlook is chiefly the result of recent developments in two laboratories. Researchers in each of the labs have built the first rudimentary components of a working quantum computer. Even though these devices are likely to be to a quantum computer what the vacuum tube is to the Numerical Wind Tunnel, they may prove the concept feasible.

The approaches of the two groups differ--one works primarily with photons, the other with atoms--but their goal is the same. Both are trying to translate the quantum mechanical properties of atomic-scale particles into the idiot-savant binary language of computing. The difficulty lies in precisely controlling their individual particles.

The experimental setup in Jeff Kimble's lab at Caltech, while impressive enough, certainly doesn't suggest the beginnings of a transuniversal computer. The device rests on a tabletop and is housed in a small vacuum chamber about the size and shape of a five-foot-long salami. Inside the chamber are two small mirrors, mounted in a metal cylinder the size of a roll of Life Savers. The mirrors are just 50 microns (.002 inch) apart. One of the mirrors is partially transparent, so that a **laser** beam can shine photons through it and into the space between the two mirrors. When the experiment is running, a beam of cesium atoms passes between the two mirrors, parallel to their surfaces and at right angles to the photons coming through the partially transparent mirror.

In conventional computers, the presence or absence of electric charge on a circuit element like a transistor stands for a zero or a one in binary code. At its simplest level, a computer works by storing or changing these binary numbers as it carries out its calculations. Kimble is trying to do something analogous with photons. He works with polarized photons-- photons that vibrate in specific, measurable directions as they travel. Photons vibrating in one direction--say, up and down--could stand for a zero; photons vibrating from side to side could stand for a one.

Ultimately, Kimble wants to send polarized photons between the two mirrors. These vibrating photons would in turn cause the cesium atoms to vibrate. The vibrating cesium atoms would create an electromagnetic field that would change the polarization of the photons--from up and down, say, to side to side. The changed photons would bounce off the fully reflective mirror, then exit through the partially transparent one, and a detector would register the new polarization. Such simple changes in polarization could be the basis for a quantum computer's calculations, changing a zero to a one to represent a single step in addition, for example.

Except for advanced supercomputers, today's computers can manipulate just one string of zeros and ones at a time. But a quantum computer using just 1,000 photons could simultaneously manipulate 21,000 strings of zeros and ones (a number that, again, exceeds the number of atoms in the universe). This is because a photon can, in the Twilight Zone of quantum mechanics, simultaneously be in two polarized states. Deutsch would say that the photon has one polarization in one universe and another in some parallel universe. Since each of the 1,000 photons can be both a zero and a one at the same time, there are 21,000 possible combinations of those photons. (There are 22 possible combinations of two numbers that are simultaneously zero and one--00, 01, 11, and 10; there are 23 possible combinations of three such numbers; and so on.) A quantum computer could work with all these states--or universes--simultaneously.

David Wineland and Chris Monroe at the National Institute of Standards and Technology in Boulder, Colorado, have the same goal as Kimble but are using different means to achieve it. They hold a row of mercury ions in an electromagnetic field and use lasers to make the ions jump between two quantum energy states. The excited state represents a one in binary code; the ground, or lower, energy level is a zero. Here too--until someone makes a measurement--the ions can simultaneously be in both the ground and excited states.

Both these approaches are a long way from a working quantum computer. No one has yet figured out how to get atoms or photons to interfere in such a way that the resulting interference pattern would correspond to the answer to some calculation. Kimble and Wineland express two slightly different takes on the long-term prospects of their work.

"It's such an important problem," says Kimble, "that it deserves a long-term investment of effort and thought. We shouldn't simply flame on a lot of interest for five years and then let it die."

Wineland speaks guardedly. "I think we're in a happy state of ignorance," he says. "There doesn't seem to be any fundamental reason that this scheme wouldn't work."

Rolf Landauer, a physicist and professional gadfly at IBM's Thomas Watson Research Center, north of New York City, can list lots of reasons. "I cannot prove that it's impossible," he says. "It's going to be difficult. I would not want to invest my money in the company that proposes to do that."

Most of Landauer's criticisms boil down to one point: a quantum computer would be an extremely delicate machine. The quantum systems doing the calculations--the banks of atoms or photons--would be easily jostled by stray particles and radiation from the outside world. A single cosmic ray could savage the quantum computations.

Even if someone devises a way to shield the device from such rude and random intrusions, Landauer says, the designers of a quantum computer will have to do what no engineer has ever done: build a near-perfect machine. But inevitably, he believes, something will go wrong and throw the system out of whack, even if there is no interference from the outside. The **laser** pulses that might control the photons in some future quantum computer, for example, will at some point be a little too strong or a bit too weak. Furthermore, as the number of atoms or photons used in the computer increases, the likelihood of mistakes will necessarily grow.

"An ordinary transistor circuit is like a door," Landauer says. "You slam it open, you slam it shut. You don't have to have a delicate regard for the amount of force you use when you push it one way or the other. These quantum systems are not like that. Quantum computers don't use just an open door or a shut door. Both the open door and the shut door are present simultaneously. The problems all relate to the fact that the process is not perfect. It doesn't do exactly what you want it to do."

Landauer thinks it may be possible to build a primitive quantum computer, one that perhaps uses the mechanisms developed by Wineland, Monroe, and Kimble. But at best the machine will be an interesting toy, not a useful computer. In a few years, he says, someone like Wineland or Kimble might build a quantum computer that can factor a small number like 15. But he doesn't think anyone will progress much further than that.

Deutsch believes that Landauer raises serious and legitimate questions. But he also thinks that engineers will somehow find a way around these problems. "Landauer was probably the first physicist to understand that computation is a physical process and can't be understood without applying physics to the computational process," says Deutsch. "But he thinks that physics will impede quantum computation. He's going to be proved wrong there."

Most physicists, though, even those who think it may be possible to build a quantum computer to Deutsch's specifications, don't buy his version of physics. Some reject the many-worlds interpretation out of hand, dismissing it as a philosophical formulation with little relevance for real-world physics. Roger Penrose, an eminent mathematician and a colleague of Deutsch's at Oxford, offers a more considered rebuttal to Deutsch's ideas. Although he doesn't believe in the many-worlds view, he says that Deutsch, unlike most physicists, has taken a close look at the foundations of modern physics. If the theory of quantum mechanics can logically lead to something as outlandish as the many-worlds interpretation, says Penrose, then quantum mechanics must be a flawed theory.

"I personally think that's a good indication that there is something wrong with the theory," says Penrose. "I think you'll find that most people don't think it through that far. But Deutsch is thinking it through. He's saying if we accept the rules of quantum mechanics as they are, we are forced into this kind of picture. I'm saying that tells us we shouldn't accept the rules as they are. So we're agreeing on the logical implications but disagreeing on what that's really telling us about the world."

While Penrose doesn't put much stock in Deutsch's metaphysics, he doesn't discount the idea of a quantum computer. "I see no fundamental reason that it can't be built," he says, "although the technology

is quite a long way from being able to do that at the moment.”

Seth Lloyd of MIT agrees with that assessment. “It’s just hard to string a lot of atoms together. I mean, these things are wicked small,” he says, lapsing into technical jargon. “They’re sensitive little buggers too. But people are getting to the point where they can control these things. It’s a big technological crapshoot. In the not-too-distant future people might be able to do full-blown quantum computation.”

Lloyd, like Deutsch, is a theorist. But unlike Deutsch, he is deeply interested in the practical problems associated with building a quantum computer. Some of Lloyd’s ideas have inspired experimentalists like Kimble, Wineland, and Monroe. Although he doesn’t subscribe to the many- worlds idea, Lloyd does share Deutsch’s taste for the wilder side of physics. “I got into this for what you might almost call a cosmic reason,” says Lloyd. In short, he doesn’t think you have to wait until some sharp coterie of physicists manages to assemble a quantum computer. He believes that a massive quantum computer is already up and running: the universe itself. Its ongoing calculations are the world outside your window.

“I wanted to get a handle on why the universe is so complex,” he says. “Or at any rate why there seems to be so much information processing going on. You can look at life and almost all the things--well, all the things--that we see going on around us in terms of information processing. You could say that life is an example of information being processed in the service of getting a free lunch out of your environment. A typical event in evolution, for example, is some organism suddenly, by a mutation, being able to produce an enzyme that allows it to digest something it couldn’t get at before. The free lunch is there, but in order to get it, you’ve got to be able to process information.”

Lloyd thinks that the nascent theories about quantum computation might one day provide a useful framework for understanding how complicated systems like stars, planets, and people arise in such a seemingly chaotic cosmos. Nature, as far as we know, is best described by quantum mechanics. Perhaps when we fully understand all the implications of that theory--which has been around now for only 70 years or so--intelligence, life, and structure in the universe will no longer look accidental or random, but natural and inevitable.

“Quantum mechanics is inherently probabilistic,” he says. “God does play dice. But playing dice supplies you with, if you like, the program. These little rolls of the quantum dice supply this random program for the universe. But what starts off as a random program gets transformed by the natural information-processing capacity of the universe into this very complicated, intricate, information-laden world we see around us.”

Aside from these more imaginative speculations, Lloyd has come up with several schemes for designing a quantum computer. One of his ideas is similar to Wineland and Monroe’s--it actually preceded their work--but instead of trapping atoms in an electromagnetic field, Lloyd would use atoms that are already naturally entrapped in a crystal lattice. Like Monroe and Wineland, he would change the states of these atoms by bombarding them with **laser** light.

“I call this the Santa Fe computer,” he says, taking an affectionate gibe at a city as famed for flakiness as New York is for abrasiveness. “It’s a crystal in which you excite intelligent vibrations by shining colored lights on it.”

Recently a roll of the quantum dice found Lloyd in Santa Fe, relaxing in a bar where he got into a conversation with a patron on the stool next to him.

“What do you do?” Lloyd asked.

“I heal crystals,” the patron said.

“What do you mean?”

“You know, crystals have vibrations and they carry energy. And when somebody with negative energy comes around, the crystals can absorb it. So I perform rituals to get rid of the negative energy in the crystals.”

Lloyd nodded. “Well, how much energy do you think is in these crystals?”

“Huge amounts, vast quantities of energy.”

“Hey, I’m a physicist,” said Lloyd, “and I happen to know that the actual amount of available energy in one of these crystals is a darned sight smaller than the energy in an equivalent-size piece of cheese.”

With that the conversation ended. Too bad. The peeved New Ager missed out on a chance to hear about life, quantum computers, and the universe. And if David Deutsch had been there, the conversation might really have taken off. Perhaps in some other universe, it did.

--Play a word-association game with DNA. What comes to mind? Genes. Heredity. A certain West Coast trial. Computation--no, that probably won’t make your list. But it should. While David Deutsch and other physicists are trying to figure out how to build a quantum computer, Len Adleman, a mathematician at the University of Southern California, has already used DNA molecules to solve a classic math problem. Granted, the problem was rather simple, but Adleman clearly demonstrated DNA’s computational potential--and that’s a lot more than can be said for anyone working with photons.

Adleman tackled a version of the “traveling salesman” problem, in which a person is presented with a map of a certain number of cities, a number of specified roads connecting the various cities, and a starting and an ending point. The task is to find a path that passes through each city only once. With just a few cities and roads, the problem can be solved with pencil and paper. But as soon as you get up to as few as 60 cities, a conventional computer, which must process all possible routes one at a time, takes impossibly long to find the answer.

How does DNA do better? To understand, you first need to recall the basic structure of the DNA molecule, which normally consists of two strands intertwined to form the famous double helix. Projecting from each strand at regular intervals, like the rungs on a ladder, are four chemical subunits--the bases adenine, cytosine, thymine, and guanine, usually abbreviated as A, C, T, and G. An A on one strand always binds with a T on the other; C always binds with G.

As set up by Adleman, the task was to find the correct route through 7 cities connected by 14 streets. He represented each city as a single strand of DNA 20 bases long. The sequence C-C-T-A-G-T-C-A-G-A-A-C-G- T-T-C-G-A-A-A, say, might represent Chicago; C-C-C-A-T-T-A-A-A-G-A-T-T-A-C- C-C-G-T-C might be New York.

Now we get to the clever part: picture these two 20-base-long DNA “cities” laid end to end. A road connecting the two is represented by another 20-base strand of DNA that partially overlaps both cities: the first 10 bases of the road will be complementary to the 10 bases at the end of one city and to 10 at the beginning of the other. Since T always binds to A, and G to C, the sequence

T-G-C-A-A-G-C-T-T-T-G-G-G-T-A-A-T-T-T-C, for example, would link Chicago and New York.

Adleman mixed in a test tube some 100 trillion DNA molecules containing all 7 cities and 14 roads, and let them join up as they saw fit. Many of the combinations that formed from the random pasting turned out to be useless--two cities repeatedly linked by the same road, for example. But because Adleman used so many copies of each DNA city and street, at least one of the combinations that formed was bound to link the cities correctly. Using standard biomolecular techniques, Adleman was able to extract the molecule that encoded the route that passed through each city just once.

Though he took a week to solve a fairly simple problem, Adleman opened up a whole new way of thinking about what makes a computer a computer. "DNA is designed by nature to process information," points out Eric Baum, a computer scientist at the NEC Research Institute in New Jersey. Instead of using the standard computer binary code of zeros and ones, DNA uses A's, T's, C's, and G's. And rather than carrying out a few calculations simultaneously, trillions of DNA molecules can react at once.

Other researchers have expanded on Adleman's idea. Richard Lipton, a Princeton computer scientist, showed that a DNA computer could, in principle, break a coding system widely used by government agencies and private corporations. The system, known as the data encryption standard system, or Des, has 256 possible ways to encrypt a message. Each involves 16 stages of scrambling the order of parts of the message, adding parts together, and rescrambling. The sentence "He left the room" might be scrambled as follows: First it would become "He the room left." Then fragments of the sentence would be added: "He room the room left he he," and so on for 14 more rounds of contortion until the simple message is lost in a thicket of disguise. (And of course, all this camouflaging is done mathematically, after the words have been turned into numbers.) It's practically impossible for a conventional computer to break the code by testing one of the 256 keys at a time. Even a supercomputer, performing thousands of operations at once, would take decades. But just about two-tenths of an ounce of DNA in solution would probably be enough to solve the problem.

"It would take about four months to make this magic soup that would contain all the answers," says Lipton. "But once that's done you can break the system at relatively rapid rates."

DNA will probably be useful only for certain specialized computing tasks. Even though a DNA computer can perform an amazing number of calculations in an instant, extracting an answer is time-consuming. "You're not going to throw away your laptop," predicts Lipton. "Or it's not going to slosh around as you type on it. Of course, in the 1950s if you had said everyone would eventually own a computer, you would have been put in a loony bin. Maybe I'm wrong, too."

--Shanti Menon