VIEWPOINT

A Quantum Conversation

Neil Gershenfeld

[ring, ring]

Alice: Hello. . .Quantum Computer Associates.

Bob: Quantum Computer? Quantum computer is more like it! That stuff will never work (other than as a make-work program for underemployed physicists). I wasn't calling for a quantum computer, just a faster one to help me find matches in a gene database.

Alice: But that means that you do want a quantum computer, because the unitary evolution of qubits under operators in $SU(N)$ is the only remaining scalable resource for computation in our universe.

Bob: Hey, I'm just a biologist! I don't know what cubes or suns you're talking about, but I do think that all this bit stuff is overrated. After all, biological systems use analog values so that instead of being limited to just 0s and 1s, they can take advantage of continuous degrees of freedom to let a signal be somewhere in between, say 1/3 or 3/4.

Alice: Ah, but biology does use the equivalent of bits when it needs to reliably correct errors, as in the four bases in the genome that let it produce the brain of a biologist. You are right, though, that part of the power of a quantum computer lies in its ability to continuously represent an arbitrary mixture of states.

Bob: Big deal—biological systems, such as DNA sequences, can easily generate lots of answers in parallel and then check to see which one is best (*1*).

Alice: The problem with that is the scaling to problems that are nontrivially large. If the number of molecules you need is exponential in the size of a problem (as it is for searching for the bits of an entry in an unordered list, like your database), then you're going to need an awfully big test tube to get anywhere. After all, 10^{23} molecules used this way can solve an exponential problem for just 23 variables.

Bob: So what's so different about quantum bits?

Alice: Qubits, as they're called, hold exponentially more information than classical bits. Instead of producing one DNA sequence for each possible answer, a single quantum register can contain all possible answers simultaneously. This is because the register can be in more than one state at the same time. Not between states, like classical analog variables; it can be in a superposition of multiple states (Fig. 1). The amount of each state represented gives the probability that a measurement of the value of the qubits will result in that state. N classical bits can be described in, well, N bits. But those bits can take on 2^N different values. Therefore, the state of a quantum register containing N qubits must be specified by giving 2^N complex numbers for all of the relative probabilities and phases of each of those states. This corresponds to a point in what is called Hilbert space (Fig. 1C). Actually, only $2^N - 1$ numbers are needed because we do know that the probabilities must sum to 1, so qubits live on the surface of an exponentially large sphere in Hilbert space, called the Bloch sphere.

Bob: Oh. That is big. But something's bothering me. I know that in DNA, adenine always bonds with thymine, and cytosine pairs with guanine. If I see one, I can always expect to find the other. Likewise, if I have two qubits in a superposition of 00 and 11, don't I know the value of the second qubit if I measure the first one? According to your rules, I can't tell whether the first one will be a 0 or a 1 when I measure it, but as soon as I do then I know the value of the second one, since they must be the same in this case. But unlike bonding, wouldn't that work no matter how far apart the qubits are? Isn't this action at a distance?

Alice: Einstein wasn't too happy about that, either. What you described is called entanglement, which is why he didn't like quantum mechanics. Although it doesn't let you send signals faster than light, it does mean that quantum bits that interact retain a spooky kind of connection that causes changes to one to appear to influence the other. This does make it possible to send quantum information over long distances through entanglement (*2*), and entanglement can be used to effectively interconnect parts of a quantum computer without physically wiring them together (*3*).

Bob: I still don't get it—I thought that a quantum system changes as soon as you look at it. How can you manipulate entanglement without destroying it?

Alice: You have to use the word "look" more carefully. Quantum computers are programmed by applying operators that correspond to rotations in Hilbert space, which preserve the amount of information in the state. These are called unitary operators, which for N qubits are elements of the group of operators $SU(N)$. Your sense of "look" refers to nonunitary operators that can add or remove information, which are used for correcting errors and some kinds of readout.

Bob: Where do these unitary operators come from? When I operate my car, I can use a map to drive it anywhere. How do you know where you're driving a quantum computer?

Alice: It's much the same, really. For example, when you parallel park, you're using a set of available operations (move-forward-and-turn, move-backwards-and-turn) to synthesize an operator unavailable on the car (move sideways). And that's just what quantum computers do. Experimental implementations have natural unitary operators, like the radio frequency pulses that rotate nuclear spins. If two operators a and b (Fig. 2A) don't commute, in other words if you get a different result if you apply them in different orders, then it's possible to generate a new operator from that difference. This is something that a fly walking on a sphere understands—where it ends up depends on the order of the directions in which it chooses to walk. In fact, most pairs of Hilbert space operators can be combined in sequences to reach any state from any other (Fig. 2A) (*4*, *5*).

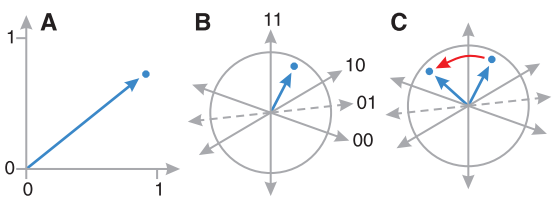

Fig. 1. (**A**) Two-dimensional state vector for two classical degrees of freedom. (**B**) Four-dimensional state vector for two quantum degrees of freedom. (**C**) A unitary operator rotating a state vector in Hilbert space.

Physics and Media Group Massachusetts Institute of Technology Media Laboratory, Cambridge, MA 02139, USA.

Bob: Even if it's possible to go anywhere, you just convinced me how big Hilbert space is. How do you figure out how to string together operators to get somewhere useful?

Alice: That's the art of quantum computer programming. String is the right term: the challenge in compilation for a quantum computer is to represent a desired algorithm as a string of available operators. There's no general theory for how to do this, but it is understood in important cases, including efficiently finding the prime factors that are the foundation of current cryptosystems (*6*), using a quantum computer to model another quantum system that's too big to study on a classical computer (*7*, *8*), and your task of finding an entry in an unordered list (*9*, *10*).

Bob: I don't need a quantum computer to search a list.

Alice: Yes, but if there are N entries, it will take you on the order of $N/2$ queries to find a particular entry if they're arranged randomly. Grover's algorithm does that in $\sqrt{N}$ steps, which is an enormous savings for a large search problem (Fig. 2B). Instead of searching through a million sequences in your database, you need only check the equivalent of a thousand (assuming, of course, that you can find a quantum computer large enough to hold the database).

Bob: That doesn't sound possible—how can it work?

Alice: Grover's algorithm starts by putting the system in a superposition of all possible answers, so that it has a small component in the direction of the correct answer. The answer is there, but it's like a needle in a haystack. The algorithm then repetitively applies a sequence of operators that rotate the state toward the correct answer, amplifying that component relative to the others. After roughly $\sqrt{N}$ steps, all of the probability moves from the haystack to the needle so that its value can be determined by a simple measurement. You can think of this process as using the size of Hilbert space to take a shortcut that reaches the answer without having to pass through all of the classical steps that would lie between a starting guess and the right answer.

Bob: What keeps these rotations aimed in the right direction? Isn't it possible to make mistakes?

Alice: Boy, is it! Quantum information is unusually fragile, because most any interaction with an external environment entangles a qubit with so many other degrees of freedom that its value effectively gets lost. This is called decoherence, but just as computer memories (and DNA polymerase) use additional information to recognize and fix mistakes, it's possible to introduce extra qubits to detect and correct errors in a qubit without measuring (and hence disturbing) its value (*11*, *12*).

Bob: What's so bad about making measurements?

Alice: The problem is that they force the system to choose one of the available states with a likelihood given by its relative magnitude. Here, let me show you. If you pick up your QCA FiberFone, I'll put a single photon (*13*, *14*) into my end of the optical fiber. Its state can be in one of two transverse oscillation (polarization) directions (Fig. 2C). If you measure the polarization with an apparatus aligned in the same direction as the one that I used to prepare the photon, you'll find the same direction that I chose. But if your apparatus is aligned differently, then the photon will be randomly forced into one of your directions with a probability given by the overlap with my axes. Now, before I send my photon, you should pick a direction for your polarizer—but don't tell me what that is. Ready? Here comes my photon. . .

Bob: . . .got it. I chose 0° and 90° for my polarizer axes. . .

Alice: . . .so did I. . .

Bob: . . .and the photon came out in the 90° direction.

Alice: Hey! That's not what I sent!

Bob: Huh? I thought you said. . .

Alice: That means that something must have interacted with the photon along the way (*15*). Or someone. . .

Eve: I didn't do it.

Alice, *Bob*: Who are you?!

Eve: Oops. I, um, work for the government.

Alice, *Bob*: The government?

Eve: Yes, an agency of the government. With a Three Letter Acronym.

Alice: Not again! Ever since we added "Quantum" to our name, these spooks keep popping up. But it's easy to spook them.

Eve: Who, me? I'm just, um, looking for a faster computer. I have a large bag of money here. . .but I can't tell you what's in it.

Alice: Well, the challenge in building a quantum computer is to reconcile the need for complete isolation from the external environment, in order to protect the quantum coherence, while still providing external access for programming. There are a number of promising approaches to doing this, including trapping ions (*16*, *17*) and atoms (*18*), addressing nuclear spins in solids (*19*) and liquids (*20*, *21*), and using confined (*22*) and superconducting (*23*) electronic states. . .

Eve: Good. Which one should I buy?

Alice: . . .but currently each of these approaches also has significant limitations. A truly scalable computer is likely to be a hybrid that takes advantage of the benefits of each: the nonunitary operations available with optical excitations, the addressability of lithographic techniques, and the coherence protection provided by using ensembles of computers.

Eve, *Bob*: So does this mean that I get my faster computer?

Alice: Not yet—that kind of experimental synthesis is many years—and grants—away. But it's also not the most interesting question. If natural mechanisms can be used to create quantum computers, it means that nature is a kind of computer. There's nothing fundamental about the representation used in the equations of physics; partial differential equations are appropriate for one kind of information technology: a pencil and a piece of paper. A computational description of a physical system can be appropriate for questions beyond computation, such as asking an experimental system of interest to effectively execute a program that provides an answer to a physical question (*24*). Although this is still preliminary, there's an emerging sense that the language of quantum computing

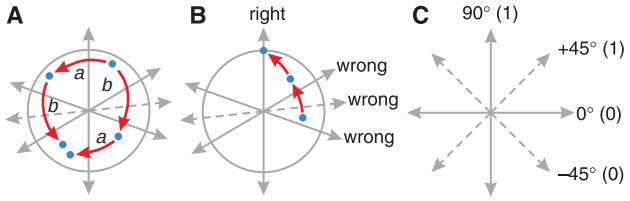

Fig. 2. (**A**) Generating a new operator from the difference between applying two noncommuting operators in reverse order. (**B**) Grover's algorithm identifying the answer to a search query. (**C**) Overlapping representations of bits in orthogonal pairs of photon polarizations.

may enhance our ability to understand as well as control quantum systems.

Bob: I thought all the fuss about quantum computing was about engineering—but that sounds like something you'd read in *Science*.

Alice: Nah, they'd never publish something like this.

References

1. L. M. Adleman, *Science* **266**, 1021 (1994).
2. C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
3. D. Gottesman, I. Chuang, *Nature* **402**, 390 (1999).
4. A. Barenco *et al.*, *Phys. Rev. A* **52**, 3457 (1995).
5. A. Y. Kitaev, *Russ. Math. Surv.* **52**, 1991 (1997).
6. P. W. Shor, *SIAM J. Comput.* **26**, 1484 (1997).
7. R. P. Feynman, *Int. J. Theoret. Phys.* **21**, 467 (1982).
8. S. Lloyd, *Science* **273**, 1073 (1996).
9. L. K. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).
10. I. L. Chuang, N. Gershenfeld, M. Kubinec, *Phys. Rev. Lett.* **80**, 3408 (1998).
11. A. R. Calderbank, P. W. Shor, *Phys. Rev. A* **54**, 1098 (1996).
12. A. M. Steane, *Phys. Rev. Lett.* **77**, 793 (1996).
13. J. Kim, O. Benson, Y. Yamamoto, *Nature* **397**, 500 (1999).
14. P. Michler *et al.*, *.Science* **290**, 2282 (2000).
15. C. H. Bennett, G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Bangalore, India, December 1984 (IEEE, New York, 1984), pp. 175–179.
16. J. I. Cirac, P. Zoller, *Phys. Rev. Lett.* **74**, 4091 (1995).
17. C. E. Wieman, D. E. Pritchard, D. J. Wineland, *Rev. Mod. Phys.* **71**, S253 (1999).
18. J. Ye, D. W. Vernooy, H. J. Kimble, *Phys. Rev. Lett.* **83**, 4987 (1999).
19. B. E. Kane, *Nature* **393**, 133 (1998).
20. N. A. Gershenfeld, I. L. Chuang, *Science* **275**, 350 (1997).
21. D. G. Cory, A. F. Fahmy, T. F. Havel, *Proc. Natl. Acad. Sci. U.S.A.* **94**, 1634 (1997).
22. D. Loss, D. P. DiVincenzo, *Phys. Rev. A* **57**, 120 (1998).
23. J. E. Mooij *et al.*, *Science* **285**, 1036 (1999).
24. N. Linden, H. Barjat, E. Kupce, R. Freeman, *Chem. Phys. Lett.* **307**, 198 (1999).

VIEWPOINT

The World-Wide Telescope

Alexander Szalay,[1] Jim Gray[2]

All astronomy data and literature will soon be online and accessible via the Internet. The community is building the Virtual Observatory, an organization of this worldwide data into a coherent whole that can be accessed by anyone, in any form, from anywhere. The resulting system will dramatically improve our ability to do multi-spectral and temporal studies that integrate data from multiple instruments. The Virtual Observatory data also provide a wonderful base for teaching astronomy, scientific discovery, and computational science.

Many fields are now coping with a rapidly mounting problem: how to organize, use, and make sense of the enormous amounts of data generated by today's instruments and experiments. The data should be accessible to scientists and educators so that the gap between cutting-edge research and education and public knowledge is minimized and should be presented in a form that will facilitate integrative research. This problem is becoming particularly acute in many fields, notably genomics, neuroscience, and astrophysics. The availability of the Internet is allowing new ideas and concepts for data sharing and use. Here we describe a plan to develop an Internet data resource in astronomy to help address this problem in which, because of the nature of the data and analyses required of them, the data remain widely distributed rather than gathered in one or a few databases (e.g., GenBank). This approach may be applicable to many other fields. Our goal is to make the Internet act as the world's best telescope—a World-Wide Telescope.

Today, there are many impressive archives painstakingly constructed from observations associated with an instrument. The Hubble Space Telescope (HST) (*1*), the Chandra X-Ray Observatory (*2*), the Sloan Digital Sky Survey (SDSS) (*3*), the Two Micron All Sky Survey (2MASS) (*4*), and the Digitized Palomar Observatory Sky Survey (DPOSS) (*5*) are examples of this. Each of these archives is interesting in itself, but temporal and multi-spectral studies require combining data from multiple instruments. Furthermore, yearly advances in electronics bring new instruments, doubling the amount of data we collect each year (Fig. 1). For example, approximately a gigapixel is deployed on all telescopes today, and new gigapixel instruments are under construction. A night's observation requires a few hundred gigabytes of memory. The processed data for a single spectral band over the whole sky, a few terabytes. It is impossible for each astronomer to have a private copy of all the data they use. Many of these new instruments are being used for systematic surveys of our galaxy and of the distant universe. Together they will give us an unprecedented catalog to study the evolving universe, provided that the data can be systematically studied in an integrated fashion.

Online archives already contain raw and derived astronomical observations of billions of objects from both temporal and multi-spectral surveys. Together, they house an order of magnitude more data than any single instrument. In addition, all the astronomy literature is online and is cross-indexed with the observations (*6*, *7*).

Why is it necessary to study the sky in such detail? Celestial objects radiate energy over an extremely wide range of wavelengths from radio waves to infrared, optical to ultraviolet, x-rays and even gamma rays. Each of these observations carries important information about the nature of the objects. The same physical object can appear to be totally different in different wavebands (Fig. 2). A young spiral galaxy appears as many concentrated "blobs," the so-called HII regions in the ultraviolet, whereas in the optical it appears as smooth spiral arms. A galaxy cluster can only be seen as an aggregation of galaxies in the optical, whereas x-ray observations show the hot and diffuse gas between the galaxies.

The physical processes inside these objects can only be understood by combining observations at several wavelengths. Today, we already have large sky coverage in 10 spectral regions; soon we will have additional data in at least five more bands. These will reside in different archives, making their integration all the more complicated.

Raw astronomy data is complex. It can be in the form of fluxes measured in finite size pixels on the sky, spectra (flux as a function of wavelength), individual photon events, or

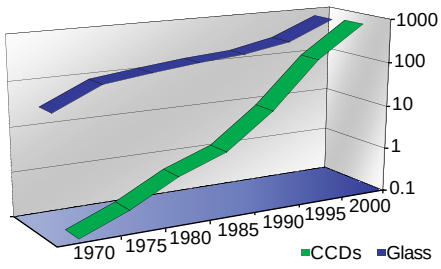

Fig. 1. Telescope area doubles every 25 years, whereas telescope CCD pixels double every 2 years. This rate seems to be accelerating. It implies a yearly data doubling. Huge advances in storage, computing, and communications technologies have enabled the Internet and will enable the Virtual Observatory.

[1]The Johns Hopkins University, Baltimore, MD 21218, USA. [2]Microsoft Bay Area Research Center, San Francisco, CA, USA.