bulge and the LMC is not easy. In particular, the contribution to the observed lensing frequency from stars in our own galactic disc and in the LMC must be established more reliably. The luminous stars in the LMC and the bulge have large radii and thus cannot strictly be treated as point sources, and the distribution of stellar radii in the lensed population is also required. As the statistics improve and the detailed nature of the experiments (MACHO, EROS, OGLE, DUO, and others) become better understood, microlensing in the galaxy should provide unique constraints on the composition of dark matter in the galaxy halos and the structure of our galaxy, and detailed follow-up observations of individual events may reveal more extra-solar planets.

An enhanced version of this Perspective, with live links, can be seen in *Science* Online on the Web at http://www.sciencemag.org/

References

1. P. Schneider, J. Ehlers, E. E. Falco, in *Gravitational Lenses* (Springer-Verlag, New York, 1992), p. 11.
2. C. Alcock *et al.* (The MACHO Collaboration), *Nature* **365**, 621 (1993).
3. ———, *Astrophys. J.* **471**, 774 (1996).
4. D. J. Lennon *et al.*, *ibid.*, p. L23.
5. M. Albrow *et al.*, in *Astrophysical Returns of Microlensing Surveys*, R. Ferlet and J.-P. Maillard, Eds. (Editions Frontieres, Gif sur Yvette, France, in press).
6. A. Gould and A. Loeb, *Astrophys. J.* **396**, 104 (1992).

QUANTUM COMPUTING

Searching a Quantum Phone Book

Gilles Brassard

What could be easier than finding someone's phone number in your city's directory, provided you know her name? It would be another matter altogether if you wanted to find the name of a stranger whose phone number you did know. If the directory is available electronically as a simple unstructured file, a computer would have to search through, on average, half of the data to locate the desired entry. It is easily proven that there can be, in general, no shortcuts. No shortcuts, that is, if we stick to computers that obey the rules of classical Newtonian physics. At a conference held in Philadelphia in May 1996, Grover presented his remarkable discovery that a quantum computer could do much better: With the use of inherently quantum-mechanical effects, it could find the desired entry in about square root as much time as its classical counterpart (*1*).

This advantage would not be dramatic for locating information in the phone directory of even a large city; however, the situation changes if we are interested in virtual databases that are so large that they would not fit in the memory of all the world's computers put together. Such databases cannot be built explicitly, of course, but they can be specified by a rule that allows the construction of any required record efficiently on demand. Consider a cryptographic example. One of the most widely used systems to protect the confidentiality of information is the Data Encryption Standard (DES). Encipherment and decipherment are controlled by a 56-bit key, which the legitimate participants must share in secret ahead of time. If an eavesdropper has intercepted matching pairs of clear and enciphered text—a classic scenario in secret intelligence—her goal is to find the key that maps one into the other.

Grover's quantum searching algorithm can in principle be used to break classical cryptographic systems such as the widely used Data Encryption Standard. Assume an eavesdropper has intercepted a matching pair of clear text and enciphered text (attackatdawn, ojbevijewbvv).

Key (name)	Ciphertext (phone number)
0000000000	sdfngdfjolgj
0000000001	ksngdjslkjdf
⋮	⋮
3726495783	kdhhhkhfushh
3726495784	**ojbevijewbvv**
3726495785	ljkdfmhsodfh
⋮	⋮
9999999998	goihgmoijopw
9999999999	hsidjgehjcuw

This problem defines a very large virtual phone book that maps each possible key to the result of enciphering "attackatdawn" with that key. Searching for the "name" corresponding to "phone number" ojbevijewbvv yields the desired secret key, 3726495784, that unlocks the remaining text.

This problem can be described by a virtual "phone directory" in which each possible key is a "name" and the enciphered text with that key is the corresponding "phone number" (see figure). Given the intercepted enciphered text, our name-finding problem corresponds to searching for the required secret key to decode the rest of the enciphered text. An exhaustive search would need to try an average of $2^{55} \approx 3.6 \times 10^{16}$ keys before hitting the right one. This would take more than 1 year even if one billion keys are tried every second. By comparison, Grover's algorithm would solve the problem after quantum-DES enciphering the known clear text a mere 185 million times.

Born at the dawn of the 20th century, quantum mechanics has evolved into one of the most successful scientific theories of all time. Nevertheless, information processing is firmly rooted in classical physics. This has prevented us from tapping the full potential of physical reality for computing purposes. About 12 years ago, Deutsch from Oxford University, following the lead of Benioff at Argonne National Laboratory and Feynman at the California Institute of Technology, thought of harnessing some of the strange properties of quantum mechanics to obtain unprecedented parallelism in computation (*2*).

To get a glimpse of Deutsch's insight, consider an atom that has a lone electron on its outermost orbit. By shining light on the atom, it is possible to force this electron to jump to a higher orbit: the atom becomes excited. What happens if you shine the light on an atom in the ground state, but for only half the time needed to excite it? Where will the electron end up, knowing that quantum mechanics forbids it from lying anywhere between the two orbits? The counterintuitive answer is that the electron will find itself simultaneously on both orbits. If we associate the binary value 0 to an atom in its ground state and 1 to an excited atom, we have produced a qubit—the unit of quantum information—that is in a superposition of classical states 0 and 1.

Similarly, two qubits can be in a superposition of the four classical values 00, 01, 10, and 11. More generally, a quantum register composed of n qubits can be in an arbitrary superposition of all 2^n different classical states.

The author is at the Université de Montréal, Département d'informatique et de rechérche opérationnelle, Montréal, Québec, Canada H3C 3J7. E-mail: brassard@iro.umontreal.ca

A quantum computer can process each of these classical values in quantum parallelism, so that exponentially many computations are performed at once. In principle, this phenomenon allows more work to be done in a short quantum computation involving a few thousand qubits than would be possible for a classical computer the size of the universe.

To solve the database search problem, Grover starts by setting a quantum register to a superposition of all possible names in the phone directory. A single access to the database (which may involve a computation if it is virtual) creates a superposition of all possible pairs of matching names and phone numbers. The resulting quantum state contains the desired pair, but with vanishingly small amplitude—the measure of how much it contributes to the global state—compared to the multitude of unwanted pairs. If the register were observed at that point, the odds of obtaining the relevant answer would be as small as if an arbitrary name had been tried at random by a classical computer.

Grover's discovery is a clever sequence of simple operations on the register's state. This process can be thought of as a sort of "quantum shake," which, contrary to a classical shake, brings order rather than disorder. Just as crests reinforce each other when ripples meet in water, Grover's shake uses quantum interference effects to increase the amplitude of the pair that contains the target phone number at the expense of all other pairs. This increase is so subtle that the probability of obtaining the desired result by observing the quantum register after a single shake is almost as small as before. However, the shake can be repeated over and over again, gradually boosting the amplitude of the correct answer to a detectable level. Provided the solution is unique, it is found with near certainty if the quantum register is observed after $(\frac{\pi}{4})N^{1/2}$ shakes, where N is the size of the database.

To use an analogy from Kristen Fuchs (3), Grover's quantum searching technique is like cooking a soufflé. You put the state obtained by quantum parallelism in a "quantum oven" and let the desired answer rise slowly. Success is almost guaranteed if you open the oven at just the right time. But the soufflé is very likely to fall—the amplitude of the correct answer drops to zero—if you open the oven too early. Furthermore, the soufflé could burn if you overcook it: strangely, the amplitude of the desired state starts shrinking after reaching its maximum (4). After twice the optimal number of shakes, you are no more likely to succeed than before the first shake.

Grover's algorithm is still theoretical, as is the earlier quantum algorithm discovered in 1994 by Shor to factor large numbers, which would bring most of contemporary cryptography to its knees (5), because there are no quantum computers in operation today, and there is no conclusive evidence that there ever will be. This theoretical dream may turn into a technological nightmare (6). Nevertheless, several teams have started experimenting with basic quantum computation. In particular, the Institute for Quantum Information and Computing, led by Kimble at the California Institute of Technology, has received a $5 million grant from the Defense Advanced Research Project Agency to investigate the feasibility of quantum computing (7). Similarly, the Los Alamos Quantum Computation Project, led by Hughes, has received a significant grant from the National Security Agency. Other major efforts are led by Monroe and Wineland at the National Institute of Standards and Technology in Boulder, Colorado, and by Blatt and Zeilinger in Innsbruck, Austria. Related experiments are led by Haroche, Raimond and Brune at the École Normale Supérieure in Paris.

Showing too much unbridled optimism would be highly premature, but even the staunchest critics agree that exciting fundamental physics is likely to come out of these experiments. Most physicists expect that currently planned experiments, involving a few quantum bits and gates, will allow the production and study of counterintuitive quantum states that have been theoretically predicted but never observed. Moreover, these experiments may provide valuable technical expertise regarding the feasibility of larger scale quantum computation. Although it may turn out that a practical implementation of such brilliant ideas as Grover's quantum search algorithm will never be realized, intriguing new ideas have already emerged from the study of quantum information theory, such as quantum cryptography (8), quantum teleportation (9), and quantum error correction (10). Whatever the future has in store for quantum computation, fundamental physics will benefit from it.

References and Notes

1. L. K. Grover, in *Proceedings of 28th Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 1996), pp. 212–219.
2. D. P. DiVincenzo, *Science* **270**, 255 (1995); D. Deutsch, *Proc. R. Soc. London Ser. A* **400**, 97 (1985).
3. K. Fuchs, private communication.
4. M. Boyer, G. Brassard, P. Høyer, A. Tapp, in *Proceedings of 4th Workshop on Physics and Computation* (New England Complex Systems Institute, Cambridge, MA, 1996), pp. 36–43. This paper is available from the Los Alamos e-Print archive: http://xxx.lanl.gov/abs/quant-ph/9605034
5. I. L. Chuang, R. Laflamme, P. W. Shor, W. H. Zurek, *Science* **270**, 1633 (1995); P. W. Shor, in *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994), pp. 124–134.
6. S. Haroche and J.-M. Raimond, *Phys. Today* **49**, 51 (August 1996).
7. G. Taubes, *Science* **273**, 1164 (1996).
8. J. Glanz, *ibid.* **269**, 29 (1995).
9. G. Taubes, *ibid.* **274**, 504 (1996).
10. B. Cipra, *ibid.* **272**, 199 (1996).

SIGNAL TRANSDUCTION

Akt Signaling: Linking Membrane Events to Life and Death Decisions

Brian A. Hemmings

Modules made of protein kinases control cellular processes. This discovery—perhaps the most important in signal transduction research during the past 5 years—is typified by growth factor stimulation of the Ras-Raf–MAP kinase module (1). One of the many initial events that occur after growth factors bind to their cognate growth factor receptor tyrosine kinases (RTKs) is the recruitment and activation of the phosphoinositide 3-kinases (PI 3-kinases). Inositol lipids phosphorylated at the D3 position by PI 3-kinases act as second messengers somewhat analogous to cyclic adenosine 3′,5′-monophosphate (cAMP) and calcium. The serine/threonine protein kinase Akt (also called protein kinase B or PKB), identified first as an oncogene, is one of the major targets of PI 3-kinase–generated signals (2–5). Results on pages 661 and 665 of this issue of *Science* and elsewhere (6–10) now provide new information on the mechanism of signal propagation from RTKs to Akt and reveal that Akt may participate in growth factor maintenance of cell survival.

Crucial to the discovery of Akt (11–13) and its function was the recognition that Akt is a proto-oncogene (12) and the characterization of its pleckstrin homology (PH) domain (14). The recognition that PH domains can bind lipids suggested a mechanism linking the activation of PI 3-kinase and Akt activity (6, 9, 10, 15). PI 3-kinase activity is potently inhibited by wortmannin

The author is at the Friedrich Miescher Institute, Post Office Box 2543, CH-4002 Basel, Switzerland. E-mail: hemmings@fmi.ch