# Quantum-Quick Queries

## Using quantum computation, in theory, to speed up database searches

By IVARS PETERSON

You're looking for a particular name in a telephone directory. If the list is alphabetical and you know exactly how the name is spelled, it won't take long to locate the required item.

If the listing is completely random, however, the only way to find the name is by checking each entry, one by one. It's like drawing names out of a rather large hat.

You could get lucky and pick the desired name on the first try, or you might have to go through every name before you find the correct one. On average, you would need to check half the entries to find the one you want.

Now, a computer scientist has found an ingenious procedure—an algorithm that relies on quantum mechanical principles—that significantly speeds up the process of identifying a particular item in an unsorted list. Whereas the best possible conventional method of searching the 100,000 entries in a small city's telephone directory requires an average of 50,000 steps, the new method takes only 100 tries.

Lov K. Grover of AT&T Bell Laboratories in Murray Hill, N.J., described his novel algorithm earlier this year at a Philadelphia meeting on the theory of computing.

"It's really a new and very exciting idea," says Gilles Brassard of the University of Montreal.

The only problem is that Grover's method requires a quantum computer, in which the familiar binary logic of 0s and 1s of existing computers is replaced by elements called quantum bits (qubits) that behave according to the laws of quantum mechanics (SN: 1/14/95, p. 30). At present, the development of a quantum machine capable of performing large-scale calculations remains much more a dream than an achievable goal.

Nonetheless, Grover's work provides fresh insights into fundamental aspects of computation and possibly into quantum mechanics itself.

The theory of quantum mechanics offers a remarkably complete and accurate description of the behavior of atoms, electrons, and other microscopic entities. According to the theory, these entities can behave as both particles and waves.

Computer scientists have found ways to take advantage of the wavelike properties of these objects to perform, in principle, large numbers of calculations simultaneously to pinpoint a specific answer. They can set up calculations so that computational paths yielding undesirable results cancel each other out, in the way that wave crests and troughs nullify each other when ripples meet, while the computational paths leading to the answer reinforce each other.

In 1994, Peter W. Shor of Bell Labs provided the first example of an important calculation that could theoretically be performed much more efficiently on a quantum computer than on a conventional computer. His algorithm involved the use of quantum-mechanical operations to factor whole numbers (SN: 5/14/94, p. 308).

Grover's search algorithm represents a new, simpler way of using a quantum computer to speed up a calculation.

In this scheme, each name on a list is represented by a different quantum-mechanical state of, say, an electron or photon. By transforming these states appropriately as determined by the search target, it's possible to cancel out some and reinforce others. "After you go through a specific number of steps, only certain configurations would survive," Grover says.

In effect, repeated application of the procedure to all the states simultaneously amplifies the one state corresponding to the desired name, so that it stands out among all the possibilities. The number of steps required to do this amplification is proportional to the square root of the number of states (or names). Thus, for 100,000 names, only 100 steps are needed.

"It's a wonderful algorithm—a useful tool to have in your bag of tricks," says Umesh Vazirani of the University of California, Berkeley.

Grover believes he can make his search method even faster. "It's a matter of finding the right quantum-mechanical algorithm," he says.

Researchers are already exploring extensions of Grover's method. The same idea could apply to various computations that involve searching through many possibilities to identify the best example of a particular condition—a type of problem often encountered and studied in theoretical computer science.

For example, quantum computers could be used as a more efficient alternative to conventional computers for finding, say, the smallest value in a large array of numbers or even cracking the widely used, powerful cryptographic system known as the Data Encryption Standard.

Computer scientists may also find it possible to combine Grover's scheme with other quantum-mechanical algorithms to design superior procedures for searching databases in which items are in alphabetical order or have some other sort of structure.

Grover's technique could easily lead to more dramatic speed-ups for other problems, Shor says. "I think it has a lot of promise."

Recently, Brassard, Michel Boyer, and Alain Tapp of the University of Montreal and Peter Hoyer of Odense University in Denmark extended Grover's method to the case of finding any match in lists containing more than one item that satisfies the required condition. They also developed an efficient way of approximately counting the number of such solutions that may exist within a given database when that number is not known at the start.

The prospects for building a quantum computer, unfortunately, remain dim, mainly because of the difficulty of keeping a large number of quantum states isolated from other photons and external disturbances.

"Although the idea of quantum computing involves some fascinating new physics that goes far beyond the rather mundane problem of merely computing faster, we believe that performing large-scale computations will remain an impossible dream for the foreseeable future," physicists Serge Haroche and Jean-Michel Raimond of the École Normal Supérieure in Paris comment in the August PHYSICS TODAY.

At the same time, efforts to study such quantum systems, even in their most rudimentary forms, could very well provide deeper insights into quantum mechanics (SN: 7/2/94, p. 6; 6/24/95, p. 388), which Haroche and Raimond characterize as "the most counterintuitive theory yet discovered by physicists." □