Opening a Quantum Door on Computing

In the quantum world, a particle — undisturbed by any attempt to observe it — can be in myriad places at the same time. Thus, a single photon traveling through a crystal simultaneously follows all possible optical paths through the material. In a sense, the photon behaves like an array of waves, and how it emerges from the crystal depends on the manner in which the waves along these different paths reinforce and cancel one another.

Computer scientists have speculated that computers operating according to the rules of quantum mechanics can potentially take advantage of a similar multiplicity of paths to solve certain types of mathematical problems much more quickly than conventional computers can.

Now, mathematician Peter W. Shor of AT&T Bell Laboratories in Murray Hill, N.J., has grounded that speculation in solid theory. He has proved that, in principle, quantum computation can provide the shortcut needed to convert the factoring of large numbers from a time-consuming chore into an amazingly quick operation (SN: 5/7/94, p.292).

"This is the first real indication that quantum computers would be useful if one could build them," Shor says.

"It's a spectacular result," comments computer scientist Umesh Vazirani of the University of California, Berkeley. "This is immensely exciting."

Shor's theoretical work not only provides a strong incentive for exploring the feasibility of building quantum computers but also brings quantum physics more directly than ever into computer science.

"What quantum computers can do is strange and different enough that it has taken computer scientists a while to think of ways of using them," says Charles H. Bennett of the IBM Thomas J. Watson Research Center in Yorktown Heights, N.Y. "We are now beginning to understand where quantum computation fits in the whole spectrum of computation, and it really has a distinctive place."

The notion of quantum computation goes back to 1982, when the late Richard P. Feynman noted that physicists always seem to run into computational difficulties whenever they try to simulate a quantum mechanical system. The necessary calculations invariably require huge amounts of time on conventional computers. He suggested that using a computer based on quantum mechanics might circumvent the problem.

In 1985, David Deutsch of the University of Oxford in England provided the first theoretical description of how a quantum computer would work. However, although such a machine was potentially more powerful than a conventional computer, Deutsch and others could come up with only highly contrived examples in which that superiority was evident.

Last year, Vazirani and Ethan Bernstein of Berkeley and later Daniel Simon of the University of Montreal established that a significant speedup was possible in certain cases. Inspired by this work, Shor found a way of applying their findings to factoring.

Suppose one wants to find the factors of a particular 100-digit number. With an ordinary computer, one could proceed by dividing the given number by all prime numbers with 50 or fewer digits and looking for any instance in which the remainder is zero. Such a procedure — and alternative, speedier methods of factoring — typically requires an extremely large number of computational steps. It's like looking for a needle in a haystack by checking the straws one by one.

A quantum computer, however, offers the possibility of handling a huge number of computational paths, or states, at the same time. The trick is to express the mathematical problem in a way that will take advantage of this intrinsic multiplicity. Shor devised such a mathematical formulation for factoring on a quantum computer.

With a quantum computer, once a calculation is set up, computation proceeds simultaneously along many paths according to the specified rules — as long as the computer is left alone to do its work. No one can look inside to check a calculation's progress. Some computational paths reinforce one another, while others cancel each other out, and the computer generates the answer in short order.

"If you do the right things, it happens sort of magically," Shor says.

Such a procedure runs counter to current thinking in computer science about computing as a step-by-step process. "It changes the set of things that you can do on a computer," says Avrim Blum of Carnegie Mellon University in Pittsburgh.

Shor has also shown that quantum computation speeds up the calculation of what are known as discrete logarithms. "I suspect there are a lot more problems where quantum computers could be useful," Shor says.

Quantum computers don't exist yet, and building them involves surmounting significant technological barriers. Nonetheless, some researchers are starting to produce designs — perhaps involving electronic states in a polymer — that may lead eventually to working models.

"People are just going to have to build these things," Blum says. "If quantum computers really work and you can factor big numbers, it'll be incredible. If they don't work because we don't understand quantum mechanics correctly, that would also be an amazing thing." *— I. Peterson*

Nicotine — chewing on it

During the past few months, events have focused a spotlight on the nicotine in cigarettes (see p. 314). But this potentially addictive drug naturally laces smokeless tobaccos, too. Moreover, unlike cigarettes, snuff and chewing tobacco labels do not disclose the amount of nicotine these products contain.

Arguing that consumers have a right to such information, three researchers with the University of Alabama at Birmingham have just analyzed and published for the first time the nicotine content — by brand — of 11 of these smokeless products.

They include the most popular moist snuffs as well as loose-leaf chewing and "plug" tobaccos.

From a health perspective, nicotine intake is important because "it drives tobacco usage patterns," says oral pathologist Brad Rodu, who headed the study. And research has linked smokeless tobacco not only to leukoplakia — oral callouses — but also to the development of oral cancers.

Five of the six analyzed snuffs led the list — carrying between 2.1 and 3.35 percent nicotine by weight. Manufacturers tend to sweeten chewing tobaccos with sugar, which can dilute their nicotine content, notes Rodu. Indeed, the two plug tobaccos weighed in with a little more than 1.6 percent nicotine each; the three loose-leaf products had 0.77 to 1.1 percent.

Ironically, the product with the least amount of nicotine was a moist snuff: Conwood Co.'s Hawken brand possessed just 0.59 percent of the drug by weight, the Birmingham team reports in the May JOURNAL OF THE AMERICAN DENTAL ASSOCIATION.

Studies show that smokeless-tobacco users subconsciously modulate how they use these products — such as by holding one wad in the cheek for 4 hours instead of replacing it every 30 minutes — to achieve a relatively constant concentration of nicotine in the blood. In fact, Rodu notes, these tobacco users often obtain as much nicotine from their "habit" as do cigarette smokers.

— J. Raloff