Binary a Bit Behind Quantum Math

by Mark K. Anderson

2:00 a.m. Jan. 16, 2001 PST

AMSTERDAM, Netherlands -- Information, as the Internet adage would dictate, may indeed want to be free. But liberty has a way of changing the liberated in unexpected ways.

This past week, Amsterdam's Center for Mathematics and Computer Science hosted the fourth annual workshop that tracks and tames information in its wild state.

The classical computer bit -- that domesticated, obedient creature that forms the basis for everything from Palms to Crays -- may have built the digital age, but it is probably too simplistic to use in computers that will solve the complex equations of the future.

See also:
Quantam Quest: An End to Errors
Quantum Physics Meets the Qubit
Read more Technology news

Yes, we can continue to force our computers into the overgrown-abacus mold. And for many applications, this simple 0-or-1 notion of the bit will probably continue to suffice. But developing future systems limited by binary states is like putting lead shoes on a roadrunner.

Scientists and mathematicians have been finding recently that the continued reliance on the bit is also based upon the erroneous assumption that the laws of physics aren't a better choice for describing the nature of information itself.

As microchips pack more and more stuff into less and less space, it's becoming increasingly clear that a fundamental day of reckoning is coming.

At the molecular level and below, computing and information take on entirely new characteristics. Bits, processors and algorithms take a turn toward the puckish -- as with everything else quantum physics touches.

Suddenly, instead of simple a computation such as 4 plus 5, computers can add every number their memory registers represent with every other number simultaneously. So instead of single answers, entire tables are generated in an instant.

Extracting those tables, of course, is a far trickier matter -- and represents the lion's share of the problem in devising effective quantum algorithms.

Still, judging from the diverse new ideas on display at Quantum Information Processing 2001, there's now a growing set of quantum computing applications that the fastest conventional computer can't touch.

The technology remains in the prototype-of-prototype phase, but that hasn't stopped the would-be programmers from dreaming. One algorithm, which could throw open the gates of computer security systems around the world, has obvious and immediate import. Another, which would perform searches at head-spinning speeds that no conventional computer could approach, probably has yet to find its killer app.

Most tantalizing, though, was the new algorithm, presented by MIT's Edward Farhi, that has shown initial promise in solving perhaps the most challenging class of problems in computer science today: the "NP-complete" problem.

"NP-complete" is a category used in computer science that represents those intractably hard problems that can only be crunched on a computer if you're dealing with particularly simple case studies or,

otherwise, if you have a few hundred years to wait around for an answer.

Examples of NP-complete problems abound, and to make the prey even more attractive, it's also been proven that solving one NP-complete problem is tantamount to solving the whole lot of them.

"You have to choose your problem very carefully," Farhi said in a recent interview. "It's not universal. It's not like a quantum computer will do anything faster. So you have to be careful. But NP-complete is the big enchilada."

Ronald de Wolf, of Amsterdam's CWI, also proposed a new application for quantum information and information processing. He discussed the use of digital "fingerprints" -- sometimes called "hashing" -- in data security and searching applications.

To illustrate how the process works, he drew an analogy to the forensic technique. A suspect is hauled into the precinct for questioning. He's fingerprinted, and his prints are checked against the FBI's master database.
"Instead of keeping dangerous criminals in the police station, they just need their fingerprints, and that suffices for checking identity with you," de Wolf said. "That's a very convenient scheme. You can replace the criminal by their fingerprints, and for the purposes of equality testing, that's good enough."

De Wolf proposed a quantum fingerprinting scheme where exponentially less quantum information represents a cornucopia of data such that only 40 quantum bits ("qubits") would be needed to fingerprint a novel of 1,000 pages.

Once constructed, a quantum fingerprint of a large data set -- say, for instance, a genetic sequence -- can then be held up to entire databases to seek out a match.

Quantum fingerprinting, however, cannot be used for storing and retrieving information. Like its forensic namesake, both quantum and classical fingerprinting were devised as a tool for comparison and not for re-creation of the original.

However, de Wolf and his collaborators also found that their quantum methods could be partially applied to compress and store certain types of data sets. It is possible, they found, to achieve similarly impressive results in the case of sparse fields where there are lots of zeroes and only a sprinkling of ones or vice versa.

IBM's Charles Bennett and David DiVincenzo, along with Giles Brassard of the University of Montreal, each presented their work on degrees of equivalence between quantum and classical information as well as the ways these kinds of bits and qubits can be communicated.

In short, not all information is created equal. Quantum data, for instance, cannot be copied -- but it can be instantaneously teleported from one place to another. The two forms of information can also co-mingle to create new kinds of communication not possible with either one alone.

Brassard spoke about what he termed "spooky communication," where, in some applications, two erstwhile correspondents can work together without ever communicating with one another.

Even in circumstances where they would otherwise need to get on the phone or exchange e-mail, quantum information allows them to collaborate in silence. All that's needed is a shared source known as quantum entanglement -- a well studied but paradoxical phenomenon where operations on one particle can affect the physical state of a neighboring particle, even if it has since been moved meters, miles or light-years away.

"Entanglement," as Bennett simply put it in a keynote address at the conference banquet, "is sexy."

On the other hand, Gerard 't Hooft inserted a cautionary note with his talk on recent attempts to reduce or eliminate the paradoxes in quantum physics -- and, perhaps with it, reduce or eliminate the power of quantum computers over their classical cousins.

'T Hooft, who won a 1999 Nobel Prize for his work on the so-called Standard Model of particle physics, asserted a hunch he's been pursuing -- along with many great minds before him, including Einstein -- that the laws of nature at the deepest levels do indeed return to the discrete and deterministic qualities embodied in the classical bit.

At such infinitesimal scales of size and time, the "classical" computer, he conjectured, would always

outperform any quantum-powered machine.

"If I could make a gigantic computer and if I could scale the performance such that the memory cells become the size of the 'Planck length,' ten to the minus 33 cm, and the clock speed would be the 'Planck time,' ten to the minus 41 seconds," 't Hooft said, "then that computer I claim would outperform any quantum computer."

'T Hooft welcomed his audience to build their own quantum computers and attempt to falsify his assertion.

Of course, neither 't Hooft's universal computing machine nor a working quantum alternative is up and running, so for the time being, the conference's many results took their shape via pen, paper and overhead projector.

Even for the qubit's greatest boosters, it seems that old-time classical info still rules the day.

Related Wired Links:

The Lightness in Being Innovative
Nov. 16, 2000

It Ain't Easy Being Light
Nov. 13, 2000

Becoming Your Own Hospital
Nov. 11, 2000

Kurzweil: Rooting for the Machine
Nov. 3, 2000