Preparing for a Quantum Leap in Computing

February 28 2006

Daniel Lidar

Imagine a place where anything possible always happens, like a TV screen that displays all the channels at once. If that seems beyond imagination, you are not alone. The world of quantum physics is so weird that even the scientists who study it say it challenges everyday concepts of common sense.

The field has grown from a realization that at the smallest scale — the realm where atoms and molecules roam — the classical equations that Isaac Newton used to describe the physical world no longer apply. In this realm, matter behaves differently, and many realities can co-exist. Particles like electrons, for instance, occupy several locations at the same time, behaving more like fuzzy waves than solid pebbles.

Fortunately, such weirdness mostly confines itself to the inner life of atoms. But a new quantum world is coming, where scientists hope to preserve the quirky diversity of the subatomic realm. This would allow them to devise superfast computers, design new drugs and guarantee security for sending secret messages.

Harnessing the power of the quantum realm requires coordinated planning from experts in fields ranging from physics and chemistry to electrical engineering. And that puts USC College's Daniel Lidar in a perfect position to help prepare for the quantum future. A physicist with joint appointments in the departments of chemistry and electrical engineering, Lidar is a leader in current efforts to transform quantum physics from theoretical curiosity to cutting-edge information technology.

As the son of two scientists (a biochemist and pharmacologist), Lidar was constantly exposed to scientific thinking while growing up in Israel and Holland. He earned his Ph.D. in physics from Hebrew University in Jerusalem in 1997, and soon thereafter began exploring the emerging field of quantum information theory.

After a postdoctoral position at Berkeley and several years on the faculty at the University of Toronto, he migrated to USC last fall. He was drawn by Southern California's growing status as the world's leading region for the new quantum research enterprise.

"This is a real hub," he said, noting that USC, Caltech and UC Santa Barbara all boast strong programs. "Southern California is probably the world capital of activity in my field."

In the mid-1990s, Bell Labs mathematician Peter Shor initiated the quantum information revolution by proving that a computer using quantum programming could crack the toughest of today's secret codes, used for governmental, military and financial communication. About the same time, other research showed that only another quantum system could provide absolute protection against any illicit eavesdropping.

Work by Lidar and his collaborators has focused on how to protect the delicate process of quantum computing from attack — by nature itself or malicious hackers.

So far, quantum computations have been performed only in rudimentary laboratory experiments. If feasible on a larger scale, quantum computers could solve some difficult problems at a fraction of the speed of today's fastest supercomputers. The trick relies on those multiple quantum realities. Like the TV screen showing every channel at once, a quantum computer could process all the numbers in its memory simultaneously, rather than one computation at a time. It's a bit like finding which of a thousand keys opens a lock; instead of trying one at a time, you could just spin one key in the lock until it opened. Certain problems that would tax a supercomputer for a trillion years could yield to a quantum computer in minutes.

But such speed is available only as long as the multiple quantum calculations can be protected from outside interference. And the same process nature uses to make rocks and people solid, instead of fuzzy like electrons, conspires to keep that time very, very short. That process, known as quantum decoherence, is usually an immediate and inevitable result of interaction with the environment — collisions with atoms or mere particles of light can cause a frail ensemble of multiple quantum realities to crash.

Lidar and colleagues have shown, though, that some quantum computing set-ups are at least partially immune to the ravages of decoherence. By designing an apparatus with "decoherence free subspaces," quantum information can be preserved in the face of environmental insults. The solution is to make sure that external effects exert a symmetric effect on the quantum storage sites. (If one bit of information is altered, so is its partner, so the two together retain a record of the stored information.)

A more difficult challenge may arise on a future “quantum internet” where quantum computers share data. Nobody had considered the potential for quantum viruses afflicting such a network until last year, when Lidar and post-doc Lian-Ao Wu proposed a scheme for fighting such “quantum malware” in a paper to be published in the journal Quantum Information Processing.

“Essentially the proposal is to do the analog of backup,” said Lidar, an associate professor hired as part of the College’s Senior Faculty Initiative. Only legitimate users of a system would be told when “real” data is being transmitted. During the remaining down time, the quantum data could be stored on a secure device, off the network, while bogus transmissions serve as a decoy for intruders. A hacker would never know when the system was vulnerable, and constant intrusion attempts would be easy to detect.

“It’s the first look at this problem,” Lidar said, and much further work will be needed to devise foolproof protection and a quantum virus cleanser if infection is successful.

For now, of course, quantum viruses are of no serious concern, as there is no quantum network to attack. But Lidar foresees a growing likelihood that quantum technology will soon play a significant role in sending secure messages and eventually in computing.

“It’s a field that is likely to have a widespread impact in the context of secure information transmission,” he said. “It is the most secure method of information transmission that we know of.”

As for quantum computing, its advantages are limited to certain types of problems; quantum computers are likely never to be good for word processing. But they could prove valuable in economically important realms such as designing drugs from scratch, by computing the quantum rules governing how biological molecules interact. Any such uses depend, of course, on effective hardware for building quantum computing devices, which might require advances in nanotechnology approaches for fabricating the necessary materials.

Thus while Lidar focuses on theory, he emphasizes the need to develop the experimental side of the field as well.

“My dream for USC would be to develop not only as a leading theoretical place, which I believe it is . . . but also to strongly develop the experimental capabilities here,” he said. “That would really put us on the map.”

Source: University of Southern California, By Tom Siegfried

Citation: Preparing for a Quantum Leap in Computing (2006, February 28) retrieved 23 April 2024 from https://phys.org/news/2006-02-quantum.html