Entanglement unties a tough quantum computing problem

September 28 2006

Error correction coding is a fundamental process that underlies all of information science, but the task of adapting classical codes to quantum computing has long bumped up against what seemed to be a fundamental limitation.

But a new approach by three theorists working at the USC Viterbi School of Engineering dramatically changes the rules of the game. Adding entangled photons as part of the message stream, they report in *Science*, opens the door to use of the entire error coding playbook.

"This method allows the use of highly efficient turbo codes, operating close to the theoretical limits of efficiency, something never before possible," says Todd Brun, an associate professor in the Viterbi School's department of electrical engineering, who is lead author on the study.

Error correction coding dates back to the classic work by Claude Shannon, founder of the field of information science, who proved messages could survive noise perfectly intact up to a certain limit -- a limit called "channel capacity" -- if they were made redundant.

The simplest error correction code is simply to repeat the same message over and over People talking frequently use informal error-correction codes, on phones, for example: "That's C as in Charlie, A as in AppleÉ"

More formally, following Shannon's insight, mathematicians over the past five decades have developed much, much more efficient methods.

These sophisticated error correction codes work by spreading one or more bits of information redundantly among a larger number of bits. If errors occur, they can be detected (and reversed) by measuring the encoded bits. These measurements--called error syndromes--are the key to the correction process.

Irving Reed, co-creator of one of the most widely used of these codes, the Reed-Solomon codes, discusses their importance to computer science and electronics in general in his 2005 memoir, *Alaska to Algorithms*.

"The human mind is capable by the use of context and language redundancy to intuitively perform error-correction. But electronic equipment is extremely fussy: it demands a perfection that isn't found in the noisy real world. Error coding permits these fastidious machines to function as part of real world systems, in real time."

Quantum computing systems, which process quantum data ("qubits") carried on single photons, are even more fastidious than electronic ones, making error codes are even more necessary.

Brun says that in quantum mechanics not all measurements can be done simultaneously. "This was most famously demonstrated by Heisenberg in his uncertainty principle," which states that it's impossible to determined simultaneously both the position and the momentum of a particle.

"When most classical error correction codes are translated into quantum codes, it is no longer possible to measure all of their syndromes; measuring some of the error syndromes disrupts the measurement of others.

The solution devised by the co-authors--Brun, assistant professor Igor Devetak, and graduate student Min-Hsiu Hsieh--is to include some entangled qubits in the mix.

Entangled qubits are a remarkable species that come in linked pairs. They are created when (for example) high-energy photons goes through certain materials, which convert them into two lower energy photons.

These twin daughters remain linked even when they are separated, so something that happens to one is echoed in the other, instantaneously, no matter how far apart they are, an effect that, even though it's predicted by quantum mathematics, remains so strange and counter-intuitive that it is sometimes called "spooky physics."

Entanglement has attracted intense interest as a way of encryption, since any attempt to intercept a message carried on entangled photons is immediately shows up on the remote daughters as a warning.

The USC method doesn't use a continuous stream of entangled photons. Rather, it mixes normal and entangled ones. One property of entanglement provides that two measurements which would be incompatible on a single qubit can sometimes be done by measuring both halves of an entangled pair Ñ and it is this property that Brun and his collaborators use.

"The protocol mixes entangled qubits into its encoding process in such a way that it becomes possible to measure incompatible error syndromes. This means that any classical code--including highly efficient Turbo codes--can be turned into a quantum code," said Brun.

The USC researchers, and particularly Hsieh, are working to calculate the optimal mix of entangled v. unentangled photons for optimal error coding performance. "But we think this is a significant result and a promising direction," concludes Brun.

Source: University of Southern California