DoubleThink

How much information is really there in a quantum state?

fq(x) News

by KATE BECKER

Conference Idea: How much information is in a quantum state? February 29, 2008

So you'd like to be in two places at once.

Picking up the kids at school while, say, getting a pedicure at the spa. Burning the midnight oil at the office while simultaneously snug in bed, resting up for the morning.

It's not impossible, but you might have to lower your expectations a little. And by *little*, think *microscopic*: Small enough to slip through the cracks of classical physics and land squarely in the subatomic domain of quantum mechanics.

CASLAV BRUKNER
University of Vienna

In quantum mechanics, there is nothing odd at all about an electron or a photon being in two places at once. It's called *superposition* and, in fact, it's mandatory. While quantum superposition might not help you make dinner while you're doing the laundry—at least, not any time soon—it could make ultrapowerful, screamingly fast computers.

Traditional computers "think" in binary code. Every "bit," or grain of memory, in your desktop is occupied by a one or a zero stored physically as voltage within a transistor. A quantum computer would tear out those transistors and replace them with electrons, photons, or atoms that are governed by quantum rules. For a quantum computer, zeros and ones aren't either/or: because of superposition, a quantum bit, or "qubit" can hold both one and zero at the same time.

What's the advantage? In a traditional computer, three bits can represent any number between zero and seven. But in a quantum computer, three qubits can represent all of the numbers from zero through seven *simultaneously*. Because quantum computers are intrinsically parallel, they can achieve exponentially greater processing power than traditional models with the same number of qubits. (You could achieve the same power classically, but you would have to enlist eight computers.)

> Not in my lifetime – and I don't intend to die tomorrow.
>
> - *Paul Benioff*, on when we should expect real quantum computers

So what's the downside? According to Paul Benioff, a theorist from the Argonne National Laboratory, you won't be making quantum computations any time soon. "Not in my lifetime," he quips," and I don't intend to die tomorrow."

The Measure of a Qubit

So, how much information is in a qubit? It seems like a simple enough question. But, as Caslav Brukner, a physicist at the University of Vienna, says, "The answer depends on what you want to do with a qubit."

If you just want to measure the value of a single qubit, the information in that qubit can be almost infinite, explains Benioff. Say the qubit is in a superposition of the "1" and "0" states. The probability of finding it in either state is written as a numerical coefficient. If the qubit has a 50-50 chance of landing in either state, that coefficient is one divided by the square root of two. Try writing that number in binary and you'll find you need a whole army of bits to get the same information stored in a single qubit. (See the Sidebar.)

But that isn't the kind of quantum computer most physicists are dreaming of. "The more useful information is strings of qubits representing other states," says Benioff, and that means using one of the strangest properties of quantum mechanics: entanglement.

MAX TEGMARK
MIT

Entangled particles are like movie twins separated at birth—even apart, they share an eerie connection. Depending on how the particles are prepared, they may have the same or opposite values of some essential property, like angular momentum ("spin," in physics-speak).

In movies with good and evil twins, the "anticorrelation" scenario is familiar. Thanks to superposition, each particle is actually in a combination of states until outside intervention forces a choice. So each "twin" is both good and evil, simultaneously, until compelled to take a stand; as soon as one "twin" picks a side, the other instantaneously settles on the opposite. (In the movies, this is the point of dramatic moral dilemma; in quantum physics, this is when the particle is measured.)

"What is important is that information in entangled systems reside more in the correlations (or anticorrelations, as in the case of the good and the evil twin) between quantum systems, i.e. in their relative properties, than in the properties of individual systems themselves," explains Brukner.

By storing information not in individual qubits but in the relation between the qubits, entanglement can speed up processing exponentially. "Entanglement is very definitely your friend," says Max Tegmark, a physicist at MIT. But there's a hitch, explains Benioff: To calculate the result of an operation on a single value, you have to repeat your calculation over and over again--which might just make you wish you'd stuck with classical computers running in parallel.

Entanglement is therefore best suited to a specific range of tasks that depends on "determining some property in general of all the outputs," Benioff explains. "For these problems the quantum computer is scalable whereas the classical parallel computations are not." One well-known example is Shor's algorithm, a factoring procedure that could encrypt—and decrypt—information in a flash.

A pair of entangled qubits can also be used to recreate the state of a third qubit in a new location—a neat trick called quantum teleportation. This could turn out to be the ideal way to transfer data inside a quantum computer without any moving parts, or to send information between two computers thousands of miles apart.

All Tangled Up

Yet entanglement is also the Achilles' heel of today's nascent quantum computers. "The main problem is that classical computers are robust," says Benioff. By "robust," Benioff doesn't mean that you can drop your laptop on the sidewalk and expect it to start up like nothing ever happened. But it does mean that your computer can tolerate temperatures above minus 273° C—the near-absolute zero chill in which quantum computers operate—and that it can withstand exposure to light and the occasional electromagnetic field.

The qubits inside a quantum computer, on the other hand, must be perfectly isolated from their environment to prevent a phenomenon called decoherence from upsetting the delicate entanglements inside. "Decoherence is enemy number one" for a quantum computer, says Tegmark. A single "snooping photon" could wipe a quantum computer's memory clean.

"We have the technology to isolate a few qubits for a little while," says Benioff, but the trick is isolate many qubits for a time that is much longer than their computational "step-time": that is, the time it takes a quantum computer to finish a thought. Do that, says Benioff, and "we'd have [quantum computers] right away."

But Brukner isn't optimistic about finding quantum desktops for sale at your local Staples any time soon: "All current realizations of quantum computation involve only a few qubits." Comparing the capacities of these prototypes even to ENIAC, the famous 30-ton progenitor of modern computers, is "a bold extrapolation."

Beyond Quantum Computers

So, ideally anyway, quantum computers could crunch numbers exponentially faster than classical computers. But Benioff and Brukner are hoping for even more: They believe quantum computers may provide deeper insight into the nature of physical reality.

Benioff is developing a quantum theory of numbers that may help explain why mathematics is such an effective tool for describing physics. "If you look at notions of mathematical existence, most people accept the Platonic view—that is, that mathematical objects have an ideal existence independent of space time, and that they have an essential connection to physics," explains Benioff. "There's something wrong with that."

Instead, Benioff takes numbers themselves to be fundamental. "All physical representations of numbers as strings of digits are strings of qubits," says Benioff. "We already do that with quantum computers."

At the same time, says Brukner, "We are still missing a simple, intuitively clear and generally accepted principle(s) which can serve as the foundation of quantum theory." Brukner continues: "It is my belief that once we have these principle(s), the concept of information will play a fundamental role in them and in a reconstruction of the mathematical structure of quantum mechanics."

"Even if we do not see a functional quantum computer in foreseeable future, we have learned a lot tackling this problem," says Brukner, ”and judging from the history of physics, it will probably be so, that one day this knowledge will be used in domains of physical science that have a priori nothing in common with quantum computation."

Here's hoping Brukner will start with a inventing a good twin to pick up the kids while we rest at the spa.

Counting in Binary

Let's take a moment to revisit a skill you probably learned in nursery school: counting. In the traditional base ten system, you count by cycling through ten symbols—0, 1, 2, 3, 4, 5, 6, 7, 8, 9. When you get to the top of the order, you add an extra digit and repeat the process.

The binary, or base two, system works in exactly the same way—just without the numbers three through nine. So let's count: 0, 1, 10, 11, 100, 101, 110, 111.

That works for whole numbers. But what about something like the square root of two? In decimal representation, the first six digits of this never-ending number are:

1.41421

The binary representation starts off:

1.01101

Just as digits to the right of the decimal point in base ten represent successively smaller powers of ten, in base two, they indicate negative powers of two: instead of the tenths, hundredths, and thousandths place, binary has the 2^{-1}, 2^{-2}, and 2^{-3} place.