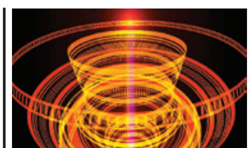
GUY HARRISON

Guy Harrison, a software professional with more than 20 years of experience, is a partner at Toba Capital and the author of *Next Generation Databases* (Apress). Contact him at guy@tobacapital.com.

What Does Quantum Supremacy Mean for Databases?



EMERGING TECHNOLOGIES

Researchers at Google recently announced they had achieved "quantum supremacy" by performing a non-trivial computation on a quantum computer that decisively outperformed a "classical" computer performing the same task. Although IBM disputed some details of the achievement, this announcement will probably stand as a milestone in the development of quantum computing technology. In minutes Google's quantum computer performed the calculation that would have taken most traditional computers thousands of years.

Quantum computing—and quantum theory itself—involves some of the most mind-boggling concepts in science and technology. For almost 100 years, scientists have understood that elementary particles such as electrons and photons exist simultaneously in multiple locations and in multiple states. Most famously, when a single photon is propelled toward a barrier with two slits, it will pass through both of those slits—so the photon is in two places at the same time.

Quantum computers use this "superimposition" behavior of elementary particles to create *qubits*. Qubits are analogous to bits in a classical computer, but while a bit can hold only 0 or 1, a qubit can hold 0 and 1 simultaneously. While an 8-bit memory register can hold any single number between 1 and 256, an eight-qubit memory register can hold and process all of those numbers simultaneously. A 256-qubit computer could process more numbers simultaneously than there have been nanoseconds since the Big Bang.

As quantum computing becomes more powerful, the implications are ever harder to ignore.

As the Danish physicist Niels Bohr once said, "Anyone who is not shocked by the quantum theory has not understood it!" The implications of quantum theory have a variety of interpretations, all of which seem within the realms of science fiction or fantasy. For most of the 20th century, the majority of physicists believed in the "Copenhagen" interpretation, in which observation caused the collapse of quantum states from probability waves to a fixed reality. In other words, physicists believed that consciousness essentially created reality.

Over the past few decades, an increasing number of physicists have come to prefer the "many worlds" interpretation. In this interpretation, every possible quantum state actually occurs, each in a different parallel universe. By this construction, there are an infinite number of universes representing every possible variation on our reality. There are parallel realities in which Hilary Clinton is president of the U.S. or in which the Allies lost World War II, and so on.

These weird implications of quantum theory could be restricted to late-night dinner party conversation or TV shows, except that quantum physics underlies almost every significant technology we use—from the GPS in your mobile phone that can help you find the nearest Starbucks to the MRI machine that could save your life.

As quantum computing becomes more powerful, these implications are ever harder to ignore. And, as quantum pioneer David Deutsch said, quantum computing is the "first technology that allows useful tasks to be performed in collaboration between parallel universes, and then sharing the results." In other words, the massive parallelism of a quantum computer results from the computations being parallelized across multiple universes!

Establishing a stable quantum computer with sufficient processing power to perform useful tasks is an incredibly difficult engineering challenge. The components of a quantum computer need to be maintained at near absolute zero, and the fundamental elements of computation are represented by individual subatomic particles. Nevertheless, it seems increasingly likely that a workable quantum computer with non-trivial processing capacity is imminent.

Such a computer could break most existing encryption routines with ease, and the cryptography community is already working hard to develop and implement quantum-proof encryption. For databases, the implications are harder to foresee. A true quantum database—one that, at its core is based on qubits and not bits—could store exponentially more information than existing databases and could query that information instantaneously.

We are a long way from such a quantum database. Nevertheless, it seems that within the next few decades, quantum computing will become a commercial reality and the impact on all aspects of computer science, including databases, will be revolutionary. ■