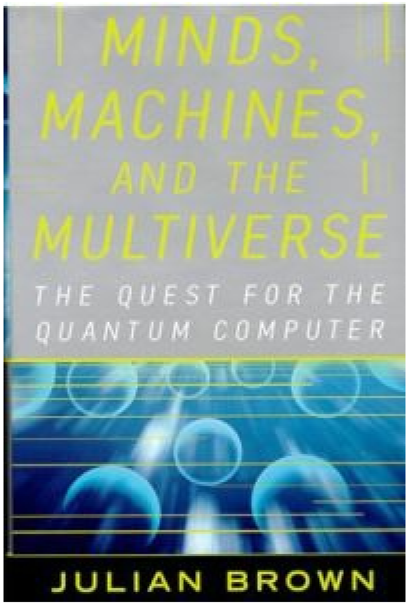

Book Minds, Machines, and the Multiverse

The Quest for the Quantum Computer

Julian Brown
Simon & Schuster, 2000

Recommendation

If you're the type of reader who loves to devour an entire book on a rainy day, you'd better wait for a Noah-size deluge before tackling Minds, Machines, and the Multiverse. Wet or dry, you will marvel at author Julian Brown's encyclopedic knowledge. He uses charts, graphs and the occasional equation to try to make the inscrutable plain. However, unless reversibility, the Fredkin Gate and the von Neumann machine mean something to you, the essence of Brown's narrative may elude you, beyond rough translation. He explains the possibility that the notion of alternative universes can be used to create a quantum computer that would be far more powerful than any computer heretofore. Brown persistently reveals possibilities that seem like dreams. *BooksInShort.com* recommends his book to those who strive for news heights of techie theory or who think of physics as a hobby. Though fascinating, it may leave mere mortals feeling uncertain and somewhat overwhelmed.

Take-Aways

- Quantum-based physics promises unimaginably powerful information processing.
- Quantum computing offers a complete scientific and social revolution, representing a bigger technological leap than the one from the abacus to the supercomputer.
- While quantum computing appears unimaginably powerful, it is not flexible.
- Quantum power rests on a "sci-fi" idea: existence of parallel universes.
- Quantum effects are only clear on the micro scale, but all objects are made of atomic particles and are equally committed to life in a quantum universe.
- Quantum computing is promising for data privacy and information security because it can factor unimaginably huge numbers at unprecedented speeds.
- If multiple universes are a reality, quantum computing can use each universe to calculate a possible outcome simultaneously.
- Quantum computing will facilitate nanotechnology.
- Quantum computing can circumvent the rapidly approaching limits of physical science.

Summary

Computing Your Way to a Brave New World

Compare an abacus to the most powerful mainframe computer in the world. Both are information-processing devices with computational capabilities, but the similarity pretty much ends there. Take that same mainframe computer, and compare it to a computer that operates based on the principles of quantum mechanics. Now understand this: the superiority of the quantum computer as compared to the mainframe is greater than the superiority of the mainframe to the abacus. The advances promised by the advent of the quantum computer are awesome, and you cannot afford to ignore what it might be able to do.

Quantum Basics

Quantum mechanics is the body of scientific knowledge based on the fact that light can be understood equally as a wave or a particle. You can either observe a photon’s state (where it is) or its direction (where it is going), but not both without affecting the outcome of the experiment. In scientific terms, this is essentially saying that the same photon is in two different states at the same time - one a wave, and one a particle. Thus the physical property of indeterminacy exists. But this principle seems impossible unless the same particle exists simultaneously in multiple universes, and indeed many sober physicists subscribe to this explanation for physical reality.

> “Today most scientists accept that Einstein was wrong and that God (metaphorically or otherwise) does indeed play dice with the universe. The outcome of every quantum event we perceive is determined by the roll of the quantum dice.”

The idea that a computer could be designed that could take advantage of this condition - and therefore could calculate simultaneously in multiple universes - sounds like something out of a hackneyed sci-fi plot. However, as with many other sci-fi inventions that eventually came to fruition (geo-stationery communications satellites, laser and particle beams, space travel), it now appears likely that quantum computing is going to leap out of the lab and into our lives. When it does so, it will have the power to change everything.

The End of Moore’s Law

In 1964, the co-founder of Intel, Gordon Moore, observed that the chip density of microprocessors was doubling about every 18 months - that statement is known today as "Moore’s Law." His prediction held up well, but big limitations await it. The current pattern of exponentially increasing computer power may be reaching its practical limits. Transistors are becoming feasible below .08 microns, but the cost of further reductions is rising.

> “The idea that one can compute using no energy at all may sound too good to be true, but remarkably enough, it seems that it is possible, in theory at any rate.”

In 1997, Hewlett Packard research czar Stan Williams predicted that by 2010 economic and physical factors will start limiting our ability to sustain Moore’s Law. (Others have placed the limit closer to 2015). That’s pretty sobering, because the evolution of the microprocessor has driven technological and economic development for more than 25 years. As transistor size continues to dwindle over the next decade, chip manufacturers will enter a world of different physical properties, the world of quantum mechanics. This world may promise a way to meet their goal: more, smaller, better, faster and cheaper. It is the world of parallel universes.

Welcome to the Multiverse

Quantum mechanics is generally considered a description of how particles such as photons behave on a very small, atomic scale. The reality, however, is that quantum mechanics applies both on the atomic scale and the everyday macro scale in which we live. This should be plain, given that the larger world is but an aggregation of the particles that comprise it. We do not need to consider indeterminacy in our every waking action - "Excuse me but which universe am I in?" - because the more unusual aspects of quantum mechanics are unseen in larger systems. Unseen, but still present.

> “The fact that in everyday life we see so many things decaying appears to be the result of our universe having started off

> in an exceedingly ordered state. The reason for this special initial state remains one of the great unsolved puzzles of physics."

The idea that quantum mechanics can best be explained by a many-universes interpretation came from scientist Hugh Everett III in 1957. The modern concept holds that our universe is only part of an infinitely larger and more complex structure, called the multiverse.

Essentially, the multiverse can be viewed as a system of parallel universes. It contains endless copies of our universe, some of which are only slightly or infinitesimally different, while others are drastically different. Each time there is an event, no matter how minute - such as the radioactive decay of an atom - the assemblage of universes differentiates itself, with many universes following different paths. This ability to take any number of possible paths explains indeterminacy, which does not reflect a shortcoming in our scientific instrumentation as much as it reflects the underlying reality those instruments strive to measure. This all certainly sounds outlandish. But, it led scientist David Deutsch to advance the notion of "quantum parallelism," the idea that a computer could calculate simultaneously in parallel universes, arriving at the correct answer far more quickly than could a computer limited to calculations in only one universe.

The Limitations of Quantum Computing

Lest the rhetoric carries you away, please be advised that quantum computing has tremendous potential, but it is certainly not a panacea for all computing challenges.

> "Although quantum computing offers seemingly unlimited amounts of massive parallelism without the need for extra hardware, there is also a price to be paid: It's impossible to read all the darned answers."

The catch is that although you may be able to produce exponentially more calculation paths, the indeterminacy of quantum mechanics limits the information that can be pulled from the calculation. For example, in a classical computer, you could analyze each step in each calculation as it proceeded. We know from the nature of quantum mechanics, however, that conducting such operations in a quantum mode would inevitably alter the outcome of the calculation. This alone appears to define what the quantum computer can be used for - so don't expect the Purchasing Department to send a memo that you will be getting a shiny new Quantum Desktop anytime soon.

> "Actually, in the modern multiverse theory, it's wrong to imply that universes split at each quantum event. They merely differentiate from one another, but nevertheless, to take account of this for every activity right down to the choice of path taken by a single photon, it is necessary to contemplate a stupendous number of universes embarking on different evolutionary journeys."

The price of the almost limitless parallelism implied by quantum computing is that it would be very difficult for the envisioned quantum computer to observe a result without changing the result. In the world of quantum mechanics, that's the inevitable trade-off. The alternative is to perform a complex calculation that is designed so that all of the diverging pathways come back together at the end to provide a single answer. Like the citizen of ancient Greece who seeks enlightenment from the Oracle, you want to be very careful how you pose the question so that the answer you receive back is as lucid as possible. "Be careful what you ask for" may become the clichŽ of the "Quantum Era," which appears to lie ahead.

> "As you can see, it's hard to put some of these ideas into words without walking into an intellectual quagmire."

The notion of the limitations of quantum calculations is essential to explain why quantum computers won't be employed to do the same tasks that massively parallel computer platforms currently handle, such as large-scale weather forecasting and aerodynamic modeling. Although scientists are learning how to squeeze more information out of quantum calculations, it appears unlikely the technology will be applied to many computational tasks. Quantum computers are good at processing unimaginably huge numbers, if you don't need to vary the inputs during the computation in order to study how changing one factor will change others. So while there are some things quantum computers will be able to do that are beyond classic-design computer systems, it is quite possible that there will be other tasks quantum computers will not be able to handle at all.

Quantum Espionage

Cryptography may be one fertile area for quantum computing. With the growing need for privacy and data protection on the Internet, cryptography is certainly in the economic mainstream and no longer restricted to the cloak-and-dagger set. Quantum computers are expected to factor vast numbers at incredible speeds, and many cryptographic systems rely on the fact that it is very difficult to factor large numbers. One hot prospect for quantum applications is to create secure communications systems that would be impossible to crack without access to quantum-based computing capability.

Visions of a Quantum Future

What does the quantum future hold? One area of great promise is the field of nanotechnology. In 1996 an institution established by scientists called the Foresight Institute offered a prize of $250,000 for the first person to design and build two devices considered crucial to the future development of technology on an atomic scale: a nano-computing device and a nanoscale robotic arm. These two devices would be critical to constructing a nanoassembler - envisioned as a tiny robot that could be programmed to snap atoms together like Lego blocks, thereby building whatever machine or structure was desired.

> “As we have seen, regarding the universe from a computational standpoint may cast new light on questions about origins. But it may also tell us something about our fate too.”

Quantum computing would play a key role. Essentially, the nanoassembler would be a "universal constructor," a machine first imagined by mathematician John von Neumann. One thing a nanoassembler would build is more copies of itself. Self-replication would mean the nanoassemblers would cost almost nothing to make. The only limits to what they could build would be the supply of raw materials and the limitations of physics. Nanotechnology could be used to construct anatomically perfect silicon chips. Thus, it is quite possible that genuine artificial intelligence could be achieved, and computers would surpass accumulated human knowledge, at which point they would begin to redesign themselves. The evolution of computers would then be determined by the computers themselves, creating a feedback loop that would lead to a period of explosive and unpredictable change. Some scientists have predicted that this would lead to a "singularity of developmental discontinuity," in other words, a point in human development after which all bets are off and predicting subsequent events becomes impossible. Some who envision this singularity anticipate its occurrence around the year 2035, although others say 2020. Other scientists remain skeptical of these claims.

The DNA Computer

Quantum computing may also have a role in creating an organic or "DNA computer." Indeed, one could look at cellular activity on a molecular scale and argue that nanotechnology already exists within the processes of our own bodies. Life on Earth depends on nanomachines that coordinate the processes necessary for life and its reproduction. Scientists are increasingly interested in the computational and information processing aspects of biological systems. DNA has always been a fascinating information storage system. Genetic computers, like quantum computers, will not replace microprocessors for everyday calculations. There are some operations that they will be able to perform, however, where current technology falls short.

Toward A Quantum Consciousness

Two arguments have been made against the likelihood of developing artificial intelligence. One is that acts of human intuition are ultimately non-computable, as they contain a random element. And secondly, that the human ability to outwit computers involves a type of quantum processing that transcends the known limitations of physics. In other words, how can we get a computer to emulate consciousness, if we do not understand how it works ourselves? But if the brain operates as a type of quantum computer, and quantum computer technology becomes feasible, the implications for artificial intelligence are vast. The key to developing artificial consciousness may well lie with quantum computers. Perhaps the development of life has itself always depended on a faster, nonclassical means of computation. If that is true, then the best proof of the feasibility of quantum computing may be your own existence.

About the Author

Julian Brown specializes in physics and computing as a science journalist. *New Science Magazine* has featured his work prominently, and he has produced science specials for BBC and BBC World Service. He teamed up with Paul Davies to edit *The*

Ghost in the Atom and *Superstrings: A Theory of Everything.*