Technology

Surfing the Wavefunction

James Hugo Mackay, *United States*

James Hugo Mackay is driven by a curiosity for the fundamental interactions of nature and love bagpiping, classical music, and pugs!

Advancements in computation as we know it have always been driven by breakthroughs in semiconductor manufacturing. The Silicon Age saw the world transform into a digital society, with global citizens enjoying the convenience of mobile devices, remote communication, and the World Wide Web. Moore's law — a statement of the biennial doubling of computational capacity — consistently promised exponential gains. However, an inevitable barrier lurked ahead: as ever-miniaturising transistors dangerously approach atomic scales, quantum mechanics, which is the physics of the subatomic universe, is beginning to interfere with hardware. In a turn of the tables, this seeming barrier to computational progress now points in the direction of the next technological gold mine: quantum computing. By exploiting the laws of quantum mechanics for computation, this revolutionary technology offers paradigm-shifting methods to solve problems previously thought impossible.

The groundwork for this field was laid in the early 1980s by the three theoretical physicists Paul Benioff, Richard Feynman, and David Deutsch. Through the turn of the decade, Feynman, who had pioneered the field of quantum electrodynamics in the '60s, in collaboration with Benioff, first conceived the 'quantum computer'. Building on the early foundational work of these two, Deutsch, canonically referred to as The Father of Quantum Computing, formalised this notion in his 1985 paper entitled Quantum theory, the Church-Turing principle and the universal quantum computer. These founding fathers, with the help of a few others, demonstrated to the scientific community the pragmatic potential of this new application of quantum physics. Inspired by the theoretical proposition of such a technology, engineers soon began development of the first proof-of-concept quantum machines. And thus, the Quantum Revolution was set in motion.

The advantages of quantum computing boil down to two quantum mechanical phenomena: superposition and entanglement. Whereas classical computers deal with bits and logic gates, quantum computers deal with qubits (quantum bits) and quantum gates. Qubits, the unit of information on a quantum computer, exist in a state of superposition and entanglement and are operated on by quantum gates. Though the mathematical rigour may be ignored, it is useful to attain a high-level understanding of this terminology. Succinctly, the state of a quantum system is detailed by its wavefunction. Until it is measured, the wavefunction exists in a superposition of multiple states. These postulates are unintuitive as they do not share a perfect classical analogue, but as a loose metaphor, a spinning coin is in a superposition of heads and tails until it falls (i.e., is measured), and its wavefunction collapses to either heads or tails. When quantum particles interact, their wavefunctions interfere and can become entangled to conserve physical quantities (e.g., energy or momentum).

By leveraging these principles, quantum computers exploit the immense data storage ability inherent to quantum systems. A simplified but effective demonstration of the advantage quantum computers have over classical ones is the task of solving a maze. The traditional computer would try each possible path until one completes the maze, whereas the quantum computer would simultaneously try each path, storing each as a possible quantum state. This is possible only for the quantum computer because the wavefunction of the entangled qubits can be made to exist in a superposition of states, where each state is a possible path, but a classical computer must store these paths separately, which is far less efficient. This is the fundamental advantage of quantum computing. The realisation of this theoretical advantage is a milestone in the quantum revolution known as 'quantum supremacy'. This was in fact achieved by Google in October 2019.

The experimental implementation of qubits can effectively take the form of any two-state quantum object, whose states would represent 1 and 0 for computation. This flexibility has allowed unique perspectives on designing quantum hardware to flourish. With regard to qubits alone, polarised photons, magnetised electrons, or trapped ions are among the many forms that have been experimented with. Furthermore, entire paradigms of universal quantum computation have emerged, namely gate model, measurement-based, and adiabatic quantum computing. These each provide unique benefits or inherent orientations toward certain classes of problems, making them fit for certain applications. This diverse family of quantum machines has a lot to offer across a spectrum of applications.

Research in the most notable STEM frontiers can be notoriously computationally demanding. With the aid of quantum computers, many scientific and societal breakthroughs would be unlocked. Teaching neural networks, a core process in machine learning, requires vast sets of training data and thus a lot of time. The integration of quantum algorithms into these methods, known as quantum-enhanced machine learning, would improve data storage and reduce computation time significantly. Financial modelling lends itself particularly well to quantum computing for structural similarities that emerge in the mathematics of both finance and quantum mechanics. Similarly, medicine development involves complex molecules, which are quantum systems themselves and thus can be efficiently simulated by such a computer. None of these computational applications were thought feasible before the quantum revolution; with the ingenious paradigm of quantum computing, the seemingly impossible problems of financial modelling, drug development, and countless others may soon be landmarks of the past.

Causing the most panice is the threat quantum algorithms pose to data encryption methods and cybersecurity. The standard Rivest-Shamir-Adleman (RSA) encryption relies on classical computers' utter inability to efficiently factor large numbers; however, a quantum computer running Shor's algorithm—a factoring algorithm invented by physicist Peter Shor—could do this with ease, threatening this widely used encryption format. Fortunately, quantum encryption algorithms have been under development to rival algorithms like Shor's. A global transition to the Quantum Age may very well be primarily motivated by a new arms race in cybersecurity, in which quantum computers are the desired weapons.

The main barrier in effectively scaling up quantum computers is a notorious issue called decoherence. Defined as the separation of an entangled quantum system into its constituents, this phenomenon makes accessing the computational power of quantum physics a delicate and precarious task. Decoherence occurs when noise from the classical world, i.e. heat, sufficiently disturbs the ultra-sensitive entangled system with excess energy, like warm air sublimating dry ice, causing it to lose its useful properties. Consequently, these quantum systems can only exist at very low temperatures. Thus, much of the recent progress in quantum computing has been either in cooling methods or in making quantum systems more resilient to environmental disturbances.

Powerful tech corporations are already funding their own quantum programs. This capitalist investment, namely from Google, IBM, Amazon, Microsoft, Intel, and D-Wave Systems, is a major factor driving the Quantum Revolution. An example of this is the aforementioned demonstration of quantum supremacy by Google in 2019. For the foreseeable future, however, quantum computers are likely to remain expensive scientific instruments, inaccessible to the public as mainstream appliances.

The natural world is described by the same mathematics that so elegantly functions as the language of quantum mechanics. This maths governs the world in uncontrollable ways which humans nevertheless strive to understand, for intellectual satisfaction and societal gain. However, classical computers are not built to efficiently emulate these types of systems. At this alone, traditional computers are philosophically distanced from the problems they are pushed to solve, not to mention the size barrier transistors are approaching. In this way, the relevance and retrospective necessity of simulating nature using quantum mechanics itself is intuitively evident. The prolific field of quantum computing is truly opening the door to a civilization of previously science-fictional capability.