KEYWORDS:
QUANTUM MECHANICS, COMMUNICATION TECHNOLOGIES, COMPUTING
DOI:
https://doi.org/10.5771/2747-5174-2021-1-44

Beyond the Binary: Building a Quantum Future

AUTHOR: Shohini Ghose

Shohini Ghose is a Professor of Physics and Computer Science and holds the NSERC Chair for Women in Science and Engineering at Wilfrid Laurier University. Her research focuses on quantum information and computation, and equity, diversity and inclusion in science.

ABSTRACT:
Quantum mechanics has not only revolutionized our understanding of the fundamental laws of the universe, but has also transformed modern computing and communications technologies, leading to our current information age. The inherently nondeterministic nature of the theory is now leading to radical and powerful new frameworks for information processing and data transmission. This new quantum revolution raises social, political and ethical questions, but also provides an opportunity to develop quantum-inspired frameworks to examine and build the quantum information era.

In the age of cute cat videos, the quantum cat stands out. Quantum mechanics has come to be associated with a rather bizarre image of a zombie cat caught in limbo between life and death. The famous 'dead-and-alive' cat was proposed by the physicist Erwin Schrodinger in a 1936 paper as an attempt to demonstrate the counter-intuitive predictions of quantum theory (Schrödinger, 1935). Schrodinger wrote about a trapped cat in a closed box being exposed to prussic acid, a poison gas that is released if a radioactive substance inside the box decays. Quantum theory describes the radioactive atoms in the box as being in an uncertain superposition of decaying and not decaying, which in turn results in the cat's gruesome dead/alive state. This seemingly extreme example is perhaps more understandable when placed in its historical context. Just a few years later, the same poison gas, under the name of Zyklon B, was deployed in far more horrifying ways in the Nazi gas chambers. Schrodinger's cat is a reminder that quantum mechanics was born in a time of war, violence, and uncertainty. Like all scientific and technological revolutions, the quantum revolution is influenced by and in turn influences our history, our politics and our society. A truly revolutionary approach to developing our quantum future must consider and address these influences.

A BINARY QUANTUM HISTORY

The global impact of quantum physics since the time of Schrodinger is undeniable. Understanding the microscopic world of atoms and nuclei unleashed the greatest destructive weapon in human history. The atom bomb laid the foundations for a binary political world divided between opposing ideologies, deadlocked in a conflict of mutually assured destruction. A parallel technological binary arose – together with the destructive power of the quantum came the spectacular benefits of electronics and laser technologies, and lifesaving medical equipment. Social binaries completed the trifecta of quantum influences: quantum-based fiber-optics, wifi and mobile computing connected humanity on a global scale while at the same time providing tools for individuals to be more isolated than ever. Never has this been more apparent than during the COVID-19 pandemic.

A century of quantum science and technology did not develop in a vacuum. As quantum science impacted the world, so too did the world impact quantum science. Big industry increasingly controlled the development and access to computing and communications technology. Governments and politics influenced what areas were funded for research and development. Socioeconomics and identity politics determined who developed the science – physics has long been a discipline that lacks diversity (Porter & Ivie, 2019). The field has been shaped by a multitude of socially constructed binaries: man/woman, rich/poor, war/peace, academia/industry, good/bad.

Ironically, the theory of quantum mechanics itself has always defied a binary approach and interpretation ever since its inception. In 1905, Einstein, building on Max Planck's work (Planck, 1900), proposed an elegant theory of light (Einstein, 1905) described as particles called 'photons,' but it conflicted with Maxwell's beautiful wave equations for light (Maxwell, 1865). De Broglie subsequently proposed a wave description of electrons and atoms and other matter (de Broglie, 1925), but that too clearly contradicted their obvious particle nature. His theory was later verified experimentally (Davisson & Germer, 1928). The particle versus wave binary description of light and matter in the universe had to be discarded, and the dichotomy had to be bridged. Schrodinger found a mathematical answer – a quantum wave equation to describe particles (Schrödinger, 1926). Wave or particle became wave and particle. Furthermore, Born proposed a radical probabilistic interpretation of Schrodinger's equation – it describes not what is, but what might be (Born, 1926).

Heisenberg's uncertainty principle cemented the idea of moving away from certainty and determinism towards a more fluid, less precise, probabilistic description of nature (Heisenberg, 1927). His was a very precise description of imprecision. At the level of individual quantum particles like electrons or photons, precisely knowing every property of the particle at a given time is impossible. A car's GPS, for example, can tell the position, speed, and direction of the car all at once, with enough precision to get you to your destination. However, a quantum GPS cannot simultaneously and accurately show all of an electron's properties, not because of a flaw in the design, but because the laws of quantum physics prohibit it. While the mathematical foundations of quantum theory are well established, this probabilistic interpretation has led to divided opinions and opposing ideas about the nature of reality, most famously exemplified in the great

debates between Bohr and Einstein (Bohr, 1949). The debate continues today despite the proven success of the theory in building our technological society – yet another unexpected binary of application versus interpretation and understanding versus confusion.

REFRAMING COMPUTING

The ubiquitous nature of binary thought and behaviour is perhaps unsurprising when viewed from the context of information theory. In mathematics and computing, the most fundamental unit of information is a binary digit, or 'bit' that can have one of two values: '0' or '1'. This deceptively simple encoding of information is spectacularly powerful. All information is encodable in bits and combinations of bits using Boolean logic allows universal computing (Boole, 1847) (Bird, 2007). In other words, given enough resources, every possible algorithm and information processing task can be implemented with binary logic. The age of information grew out of this stunning insight. The impacts of binary computing are evident and embedded everywhere in science, society and culture. And yet, quantum mechanics, which drove this binary-based computing and technological revolution, is far from a simple binary theory. A deeper understanding of the nonbinary power of the theory is now beginning to drive a second quantum revolution.

In the language of computing, quantum theory predicts that a quantum bit (qubit) may not be precisely '0' or '1', but may be more fluid in its value – it has some probability of being measured as a '0' and some probability of being '1' (Nielsen & Chuang, 2010). Furthermore, this type of everchanging information cannot be precisely copied – a result enshrined in the quantum no-cloning theorem (Nielsen & Chuang, 2010). Such imprecision does not seem to bode well for precision calculations and measurements, until one breaks out of the constraints of deterministic binary thinking and embraces quantum uncertainty as an additional, powerful resource. This reframing led to the development of the first quantum encryption protocol – a way to hide information from prying eyes using the laws of quantum physics (Bennett & Brassard, 1984). Thanks to no-cloning, hackers cannot precisely or secretly copy private information encoded in qubits. Whereas current encryption standards rely on complex mathematical algorithms (Rivest et al., 1978), quantum security is based on the fundamental laws of nature. Additional computing power would thus not help the eavesdroppers as they would still be bound by the same laws of physics. Since the first quantum encryption proposals in the 1980's, quantum cryptography has been steadily growing into a global industry potentially worth billions, that could transform information and communication security.

While no-cloning led to a radical rethinking of data encoding and transmission, the qubit also enabled a radical expansion of computing beyond deterministic combinations of zeroes and ones to probabilistic logical operations and measurements. This was not just another step in the development of ever-faster algorithms for our current binary logic based computers, but a fundamentally different approach to computing itself. A useful historical analogy would be to consider the difference between a horse and cart and a steam-powered locomotive engine. While both technologies focused on transportation, they relied on entirely different scientific processes and differed in capacity and efficiency. Compared to current binary-based classical computing, quantum computing is in some respects like the locomotive compared to the cart, and perhaps even more different. Furthermore, just like the steam engine led to the Industrial Revolution beyond just the field of transportation, quantum information processing offers the promise of a new quantum revolution that could impact a broad spectrum of science and society.

Although the power of quantum computing is not infinite, certain types of problems and calculations seem to be particularly conducive to a probabilistic quantum approach. The most famous example is Shor's quantum factoring algorithm that finds the prime factors of an integer number N – a task that is thought to be computationally intractable to solve in polynomial time using current computers when the integer N is larger than a few hundred digits in size (Shor, 1994). Shor's algorithm can perform the task almost exponentially faster than the best known classical algorithm. The algorithm thus poses a threat to worldwide encryption protocols whose security relies on the computational complexity of factoring large integers (Rivest et al., 1978). Shor's insight kickstarted the effort to develop additional quantum-based approaches to solve computationally challenging problems. A plethora of possible applications have started to emerge.

The simulation and analysis of molecular properties and quantum chemistry for pharmaceutical applicationsand materials design may be a particularly important application of future quantum computers (Nielsen & Chuang, 2010). Since it operates according to the same quantum mechanical rules as the molecules it is simulating, a quantum computer would be uniquely suitable for such tasks and could potentially outperform the fastest supercomputers today. Quantum computers are also well-suited to solving complex optimization problems (Finilla et al., 1994) and searching through large amounts of unsorted data (Grover, 1996). The importance of search and optimization in our current age of information is obvious; quantum information processing could impact big data in multiple sectors including healthcare, environment, finance, transportation, manufacturing and much more.

TOWARDS A QUANTUM FUTURE

The quantum gold rush has begun. Across the globe, governments and private investors are pouring billions of dollars into quantum research and development. The use of satellites to distribute quantum keys for encryption has recently been demonstrated, laying the groundwork for a future global quantum communication network (Yin et al., 2020). Full-stack quantum computing hardware and software is being developed by IBM, Google, Microsoft, Amazon, and other companies. There is no clear winner in the current race as yet. Although small-scale quantum computers are currently operational, coping with errors is a major roadblock to scaling up the technology.

The quantum computational power of qubits is inextricably linked to their fluid identities as superpositions of '0's and '1', and these superpositions are delicate and easily destroyed by even the tiniest noise and disturbances. In the quantum world, unwanted interactions of the qubits with their environment (noise) can 'collapse' the qubit superpositions into a definite value of 0 or 1 and in doing so, can destroy the quantum computation. Classical certainty in this context is thus to be avoided. Preserving and protecting quantum information from errors can require enormous effort. Current quantum computers must be operated in enclosed environments with temperatures well below those of outer space (Moss, 2021). Even this level of protection often fails, causing errors in the outputs of the computers. Error correction techniques have been developed that can diagnose and correct the errors without destroying the fragile quantum superpositions of qubits (Shor, 1995), but efficiently implementing such quantum error correction remains a major engineering roadblock.

Given the many engineering challenges, the future of quantum technology is (appropriately) uncertain. But quantum science is teaching us to embrace uncertainty. What began as a revolutionary idea about the power of nonbinary, probabilistic quantum computing could potentially grow into a technological and social revolution. The field is in its infancy, which provides a unique opportunity to explore, assess and shape its future impact on science and society.

Arguably the most immediate impact of quantum computing will be on data security since current classical encryption protocols are increasingly vulnerable to more powerful classical computers as well as future quantum computers. Furthermore, quantum encryption protocols that can protect against attacks by quantum computers can already be implemented using currently available laser, wifi and fiberoptics technologies (Chen, 2021). Small scale quantum encrypted networks and proof-of-principle demonstrations of quantum encryption have already been implemented. A larger scale shift to quantum-secure architectures and supporting infrastructure will require long-term planning, resources and global co-operation. Although international scientific collaborations are common, at the level of national governments and in industry, competition and secrecy rather than co-operation is the driving force. Moving beyond the binary would require building an ecosystem of co-operation balanced with competition.

While quantum based data security appears to be inevitable, the remaining landscape of quantum computing apps is not so clear as yet, although some broad areas of application have been identified as described above. It's worth noting that the uncountable applications of classical computers in every part of society was equally unclear just fifty years ago. Looking back on those fifty years provides useful insights into the positive and negative impacts of the classical information age. With a fifty-year advance warning, the quantum information age could be more deliberately and responsibly shaped by building on the positives while anticipating and addressing the negatives.

The potential of quantum technology to transform security, health, finance and energy

raises a multitude of questions. Who will develop and control the technology? Who will have access and for what purpose? How can the technology be developed in a sustainable and inclusive manner? How will social, political and financial structures evolve and adapt to a quantum world? In recent times, the development of AI and Blockchain has highlighted the importance of considering emerging technologies' social, legal, and environmental implications (Mantelero, 2018) (Goodkind et al., 2020). History offers additional lessons: despite its obvious benefits to society, the Industrial Revolution also unleashed environmental repercussions that are being felt acutely today. Despite all of this, no clear plan or global conversation about the broader societal, environmental and ethical implications of quantum science and technology exists as yet.

In building a roadmap for a just, equitable and sustainable quantum future, lessons can be learned from quantum theory itself. The main insight is that deterministic classical physics and the binary model of the classical bit are limited in their scope. Quantum theory tells us the universe is far more fluid and that nonbinary models of information processing can be powerful. Another important insight is that precision is fundamentally limited and hence information cannot be precisely cloned. A third major insight is about quantum interactions. The power of quantum algorithms such as Shor's factoring or quantum search comes from harnessing a special type of quantum correlation called entanglement (Einstein et al.,1935). Two entangled qubits can be connected in a balancing act of certainty and uncertainty – individually they remain unpredictable, but jointly they are perfectly in sync – for example, either they are both '0' or they are both '1', although individually they are a mix of both values. An early example of entanglement was Schrodinger's fabled cat: the radioactive atom is in a fluid superposition of decayed (corresponding to the value '0') or not decayed (corresponding to the value '1'), but if it is decayed (0), then the cat is certainly dead (corresponding to value '0') and if it has not decayed then the cat is certainly alive ('1'). Thus, cat and atom are perfectly synced but still in superposition. Entanglement is strange and powerful, but also fragile and difficult to create and preserve, particularly for macroscopic objects such as cats. Schrodinger considered it to be a preposterous and clearly impossible scenario, and yet entanglement fuels powerful quantum computing protocols today.

Quantum resources such as entanglement and superposition emerge from fundamental quantum postulates – a set of rules that describes the properties and behaviour of quantum particles. These postulates can also provide inspiration for a quantum-based framework to create a socially responsible quantum future. Such a quantum-inspired framework could shift away from traditionally binary thinking in science, politics, ethics, and other spheres. It could allow for fluidity and inclusion rather than limited choices between polarized dichotomies. It could focus on the creation of powerful quantum-like connections that create strong synergies, while still balancing individual differences. And it could include mechanisms to identify weaknesses and 'noise', and resources for continuous improvement to address global challenges and protect against inequities, instability and conflict.

Deterministic classical physics has shaped classical thinking and social behaviour for centuries. The coming age of quantum computing and quantum communication could have a ground shifting impact on society and thought. Preparing for such a paradigm shift will require more than the development of technology and more than a standard assessment of societal impact through a traditional classical lens. It will mean expanding our classical viewpoint and adopting a broader quantum mindset. Is such a fundamental shift possible? Will it be successful? While quantum theory would indicate that the answer is 'maybe', the promise of quantum computing indicates that it's worth trying.

ACKNOWLEDGMENTS

This work is supported by the Natural Sciences and Engineering Council of Canada. Wilfrid Laurier University is located in the traditional territory of the Neutral, Anishnawbe and Haudenosaunee peoples. We thank them for allowing us to conduct research on their land.

REFERENCES:

Bennett, C., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing,, 175, 8.

Bird, J. (2007). Engineering Mathematics. Newnes.

Bohr, N. (1949). Discussions with Einstein on Epistemological Problems in Atomic Physics. In Albert Einstein: Philosopher-Scientist. Cambridge University Press.

Boole, G. (1847). The Mathematical Analysis of Logic Being an Essay Towards a Calculus of Deductive Reasoning. London: Macmillan.

Born, M. (1926). Zur Quantenmechanik der Stoßvorgänge. Zeitschrift für Physik, 37, 863.

Chen, Y. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature, 589, 214.

Davisson, C., & Germer, L. (1928). Reflection of Electrons by a Crystal of Nickel. Proceedings of the National Academy of Sciences of the United States of America, 14, 317.

de Broglie, L. (1925). Recherches sur la théorie des quanta (Researches on the quantum theory), Thesis,. Annales de Physique, 3, 22.

Einstein, A. (1905). On a Heuristic Point of View about the Creation and Conversion of Light. Annalen der Physik, 17, 132.

Einstein, A., Podolsky, B., & Rosen, N. (1935). Can Quantum-Mechanical Description of Physical Reality be Considered Complete? Physical Review, 47, 77.

Finilla, A., Gomez, M., Sebenik, C., & Doll, D. (1994). Quantum annealing: A new method for minimizing multidimensional functions. Chemical Physics Letters, 219, 343.

Goodkind, A., Jones, B., & Berrens, R. (2020). Cryptodamages: Monetary value estimates of the air pollution and human health impacts of cryptocurrency mining. Energy Research & Social Science, 59, 101289.

Grover, L. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing., 212.

Heisenberg, W. (1927). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Zeitschrift für Physik, 43, 172.

Juan, Y., Li, Y.-H., Liao, S.-K., et al. (2020). Entanglement-based secure quantum cryptography over 1120 kilometres. Nature, 582, 501.

Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Computer Law & Security Review, , 34, 754.

Maxwell, J. C. (1865). A dynamical theory of the electromagnetic field. Philosophical Transactions of the Royal Society of London, 155, 459.

Moss , S. (2021). Cooling quantum computers. Cooling Supplement. Retrieved from https://www.datacenterdynamics.com/en/analysis/cooling-quantum-computers/

Nielsen, M., & Chuang, I. (2010). Quantum Computation and Quantum Information. Cambridge: Cambridge University Press.

Planck, M. (1900). Über eine Verbesserung der Wienschen Spektralgleichung. Verhandlungen der Deutschen Physikalischen Gesellschaft, 2, 237.

Porter, A., & Ivie, R. (2019). Women in Physics and Astronomy, 2019. AIP Report.

Rivest, R., Shamir , A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 120.

Schrödinger, E. (1926). An Undulatory Theory of the Mechanics of Atoms and Molecules. Physical Review, 28, 1049.

Schrödinger, E. (1935). Naturwissenschaften, 23, 807.

Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press, 124.

Shor, P. (1995). Scheme for reducing decoherence in quantum computer memory. Physical Review A, 52, R2493.