Dartmouth Undergraduate Journal of Science

Volume 20
Number 1 *Assembly*

Article 9

2017

# Feeding the World with Die Rolls: Potential Applications of Quantum Computing

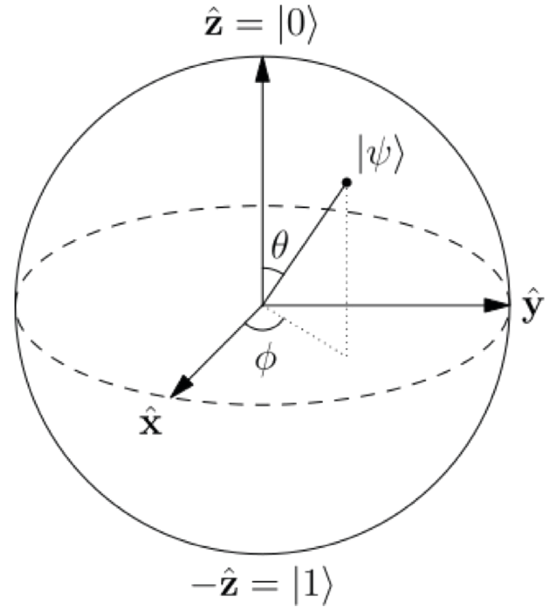


**Figure 1:** A representation of a qubit, the fundamental building block of quantum computing. **Source:** Wikimedia Commons. Included by Kevin Kang, Editor-In-Chief

# Feeding the World with Die Rolls: Potential Applications of Quantum Computing

BY SEBASTION JEON

For most people, the abstract concept of probability reminds them of boring theories covered in a typical math class. For others, who are mystified by the seemingly supernatural work of chance and fortune, it may evoke the thrill of gambling at a casino, or drawing a winning lottery ticket. Recently, researches in a variety of scientific fields have made substantial progress towards applying this theory of probability in ways that hope to aid the less fortunate. An emerging field of computing based on quantum theory, or the physics describing the uncertainty of particles, is developing an entirely new and revolutionary machine called the quantum computer. If implemented successfully, a quantum computer would not only make online transactions significantly more efficient, but also provide tangible benefits to society, especially the underprivileged. For instance, with this technology, it is possible to synthesize fertilizer more quickly and cheaply through detailed computer simulations. Although this may seem unimpressive, this application has potential to make meaningful progress toward resolving world hunger. While much of the technology necessary to construct a quantum computer is not currently available, quantum computing holds much potential for application in a plethora of modern problems.

As the name suggests, quantum computing is made possible due to principles based in quantum mechanics. Quantum computers rely on two fundamental ideas of quantum theory, the first being wave-particle duality. Wave-particle duality states that all matter demonstrates either wave-like or particle-like behavior, but not both (1). For example, according to classical physics, a particle has a fixed position in any given moment in time. Quantum theory, however, argues that the precise position of a particle cannot be determined due to its wave-like properties. Instead, only the probability that the particle is in a certain position can be determined, and the resulting particle is best described as a superposition of classical states (2). Using this property, it is possible to store information with quantum particles. Unlike the classical bit, which can hold a value of either 0 or 1, the qubit makes a probabilistic decision to be 0 or 1 (3). The advantage that this probabilistic qubit provides over the classical bit stems from its ability to hold two classical bits of information, which ultimately leads to an exponentially more space efficient computer. To put this into perspective, data that traditionally required a million units of storage would only require around twenty qubits. By compressing information with qubits, it is possible to improve virtually all electronic processes in people's daily lives to this extent.

"Data that traditionally required a million units of storage would only require around twenty qubits. By compressing information with qubits, it is possible to improve virtually all electronic processes in people's daily lives to this extent."

Quantum computers can also perform exponentially faster than classical computers due to the property of entanglement, which is another theory in quantum mechanics. Entanglement, a property that relates to 'spooky' interactions between unconnected particles, states that by changing certain properties of a quantum particle, one can instantly alter the property of another, regardless of the physical distance between the particles (4). The correlation between these two particles, which are said to be entangled, is useful because measuring information about one particle immediately yields information about the other. This allows quantum computers to manipulate multiple qubits at a time, since with a few simple operations, all of the numbers that describe the qubits can be easily affected (3). It is only due to this property of entanglement that complex superposition states can be reduced to simpler ones and ultimately produce astronomically fast computations.

If this theoretical quantum computer could be constructed, the technology could be applied to decode much of today's encryption systems and radically change the field of cryptography and cybersecurity as a whole. In 1994, computer scientist Peter Shor discovered a quantum algorithm that efficiently factors large numbers. In his paper, Shor provides efficient algorithms that can be used with a quantum computer (5). This result not only possesses great theoretical significance, as it shows that quantum computers can tackle problems that classical computers cannot, but also challenges many modern encryption schemes, such as the Rivest-Shamir-Adleman (RSA) algorithm. As the RSA algorithm's security relies upon the difficulty in factoring very large numbers, if one can quickly factor these large numbers, the encryption scheme is weakened, thereby making it possible to undo the security measures and access the data (6). In fact, some computer scientists argue that Shor's results on factorizations render all commercial encryption schemes insecure (7). Quantum computing's ability to decrypt the RSA and similar algorithms has many ramifications with varying degrees of value to society. In one perspective, this technology is evidently beneficial to intelligence agencies, since it would allow them to decode opposing security measures and breach their data storages. This also implies, however, that other sources of information can be just as easily breached by people with malicious intentions. Because the construction of a practical quantum computer threatens the security of digital commerce and communication (7), it is necessary to resolve these issues before attempting to commercialize quantum computers.

Another somewhat surprising application of quantum computers in biochemistry is resolving the problem of nitrogen fixation, or the synthesis of a chemical compound known as ammonia. Due to ammonia's importance as part of some of the most ubiquitous fertilizers in the modern world, efficient large-scale production of ammonia has historically been in great demand. Before attempting to discuss how quantum computing can help solve the problem of nitrogen fixation, it is necessary to understand the deficiencies in classical processes used to generate ammonia. Since its development in the early 20th century, ammonia has been produced in substantial quantities through the Haber-Bosch process, which utilizes a synthesis reaction with hydrogen and nitrogen gas. Although the reactants can easily be obtained, the Haber process requires extremely high pressure and temperature conditions, as well as an expensive metal catalyst (8). These conditions are necessary in order to force the chemical bonds in the reactants to break and reform into products. The dissociation of the triple bond in the nitrogen molecule (9), which is one of the strongest chemical bonds in nature, is a demanding source of energy in the process. Large-scale production of ammonia through the Haber-Bosch process requires such an energy intensive method of maintaining a regulated environment for the catalyst that it burdens the global economy and energy reserves, consuming up to 2% of the world's annual energy production (10). Applications of quantum computing capabilities attempts to completely circumvent these problems surrounding the creation of a specialized environment by simulating a different, more natural method of ammonia synthesis.

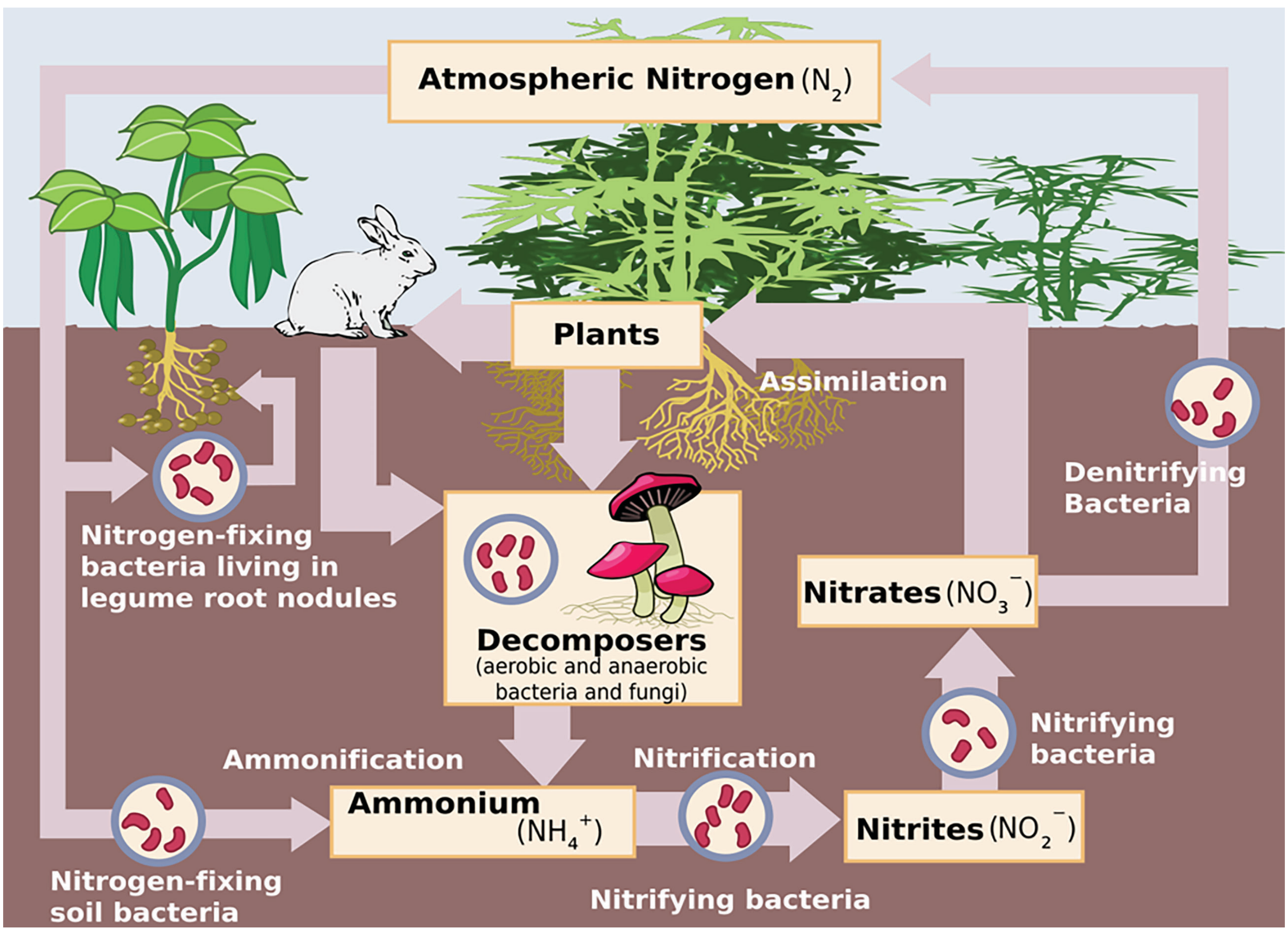


**Figure 2:** The process of nitrogen fixation. **Source:** Wikimedia Commons. Included by Kevin Kang, Editor-In-Chief

Instead of relying on the more industrial Haber-Bosch process, by simulating the reaction mechanism of the enzyme nitrogenase, a natural producer of ammonia, quantum computers have the capability to discover alternative methods of nitrogen fixation. Without relying on factory conditions, nitrogenase is able to split the nitrogen bond at standard temperature and pressure (10), allowing for far more energy-efficient nitrogen fixation. Although the classical computer is not powerful enough for the task of developing nitrogenase, the computing speed of a quantum computer enables it to understand how the steps of ammonia synthesis take place on a molecular level (11). A precise understanding of these steps will allow biochemical engineers to replace the energy-inefficient Haber-Bosch nitrogen fixing process. If quantum computing improves to the point where it can conceivably simulate nitrogen fixation, it could have profound social implications. Most notably, less energy-intensive ammonia synthesis will allow for cheaper fertilizer, thereby reducing the cost of producing food. This technology would not only lessen the global economic burden of producing fertilizer, but also provide underprivileged communities access to affordable food, marking a bold step towards resolving world hunger.

Despite the exponential increases in memory and speed of quantum computers that open up potentially new applications for computing, critical physical and logistical limitations currently prevent us from tackling these problems. Perhaps the most pressing challenge to quantum computing is the construction of a quantum computer in the physical world. Firstly, in order for the data stored in qubits to remain stable, all computations must be done in extremely low temperatures while also maintaining strict conditions regarding pressure and magnetic fields, all of which limits the commercial viability of quantum computers (12). The technology to simulate an environment conducive to quantum computing simply cannot conceivably exist in a household or an office, and as long as these challenges persist, it is unlikely that quantum computers will replace classical, commercially available computers. Quantum computers in laboratories are also limited by the sheer number of qubits required for practical applications. Although the most advanced quantum computers currently have around two thousand qubits, applications such as nitrogen fixation are expected to require "only" millions of qubits (11). Similarly, the quantum computers currently in development do no better than classical computers at breaking encryption schemes, as even a human with pencil and paper can factor the largest number factored by a quantum computer to date, a relatively unimpressive record set in 2014 (13). Despite recent breakthroughs in quantum computing, it is clear that more progress in resolving physical limitations of the technology is necessary before quantum computers can see practical usage.

Regardless of current physical and logistical limitations, it is clear that many people among the scientific community believe that using principles from quantum theory to construct a computer is a novel idea. Combining ideas from multiple disciplines of science, the study of quantum computing is likely to attract popularity from researchers in a variety of fields. More theory in quantum physics is necessary to prove precisely how effective these computers can be. Furthermore, engineers and even biologists must be involved in order for this technology to leave a lasting impact on humanity. Although many more breakthroughs are necessary before quantum computing becomes a viable technology, this innovation can potentially be one of the defining ideas of the current generation. The problems that advanced quantum computers would be able to solve would not only benefit industries, but also be able to provide large amounts of humanitarian support with applications such as nitrogen fixation. Due to its potential to make these meaningful, large scale impacts on society, it should be evident that further studies and research in the field of quantum computing is a worthwhile pursuit regardless of current limitations. D

CONTACT SEBASTIAN JEON AT SEBASTIANJEON0@GMAIL.COM

**References**

1. Jagielski, B. (2009) Elements of the Wave-Particle Duality of Light. Master Thesis, University of Oslo, Oslo.
2. Black, P. E., D., Kuhn, R., & Williams, C. J. (2002). *Quantum Computing and Communication* (Vol. 56, pp. 189-244, Rep.). Gaithersburg, MD: National Institute of Science and Technology. doi:https://doi.org/10.1016/S0065-2458(02)80007-9
3. Brassard, G., Chuang, I., Lloyd, S., & Monroe, C. (1998, September). *Quantum Computing* [Scholarly project]. Retrieved September 7, 2017, from http://www.pnas.org/content/95/19/11032.full.pdf
4. Cho, A. (2015). More evidence to support quantum theory's 'spooky action at a distance'. *Science.* doi:10.1126/science.aad1685
5. Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing,26*(5), 1484-1509. doi:10.1137/s0097539795293172
6. Singh, G., & Supriya, S. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications, 67*(19), 33-38. doi:10.5120/11507-7224
7. Rieffel E.G., Polak W.H.: Quantum Computing: A Gentle Introduction. MIT Press, Cambridge (2011)
8. Modak, Jayant. (2002). Haber process for ammonia synthesis. Resonance. 7. 69-77. 10.1007/BF02836187.
9. Kitano, M., Kanbara, S., Inoue, Y., Kuganathan, N., Sushko, P. V., Yokoyama, T., . . . Hosono, H. (2015). Electride support boosts nitrogen dissociation over ruthenium catalyst and shifts the bottleneck in ammonia synthesis. *Nature Communications, 6*, 6731. doi:10.1038/ncomms7731
10. Reiher, M., Wiebe, N., Svore, K. M., Wecker, D., and Troyer, M. Elucidating reaction mechanisms on quantum computers. arXiv:1605.03590 (2016).
11. Hoffman, B. M., Lukoyanov, D., Dean, D. R., & Seefeldt, L. C. (n.d.). Towards Quantum Simulations [Review of *Elucidating Reaction Mechanisms on Quantum Computers*]. 1-3.
12. Dragoman, D., & Dragoman, M. (2014, November 30). *Two- and three- qubit room-temperature graphene quantum gates* [Scholarly project]. Retrieved September 8, 2017, from https://arxiv.org/ftp/arxiv/papers/1412/1412.0235.pdf
13. Dattani, N. S. & Bryans, N. Quantum factorization of 56153 with only 4 qubits. *arXiv*:1411.6758 (2014).