# An Introduction to Quantum Computing

Ricco Venterea[1, a)] and Urbas Ekka[2, b)]

[1)]*Department of Astronomy, Cornell University, Ithaca, New York 14850, USA*

[2)]*Department of Mathematics, University of Minnesota, Twin Cities, Minnesota 55141, USA*

[a)]*Corresponding author: rcv38@cornell.edu*

[b)]*ekka0002@umn.edu*

**Abstract.** We present an overview of quantum computing, including relevant physics, processes, and applications. This includes describing the basic framework of the quantum bit, which serves as the foundation for the rest of this paper. We found rapid developments in quantum computing, which will have important consequences for future applications in scientific fields.

## INTRODUCTION

"[I] believe it's true that with a suitable class of quantum machines you could imitate any quantum system, including the physical world" [1]. With these words Richard Feynman ushered in a revolution. He shook off the shackles of classical computing and reached for the possibilities of quantum computing.

Quantum computing seeks to expand the typical computational power of classical computing. Classical computing is fundamentally based on 0s and 1s. Unlike quantum computing, these values are independent of any measurement. But due to this rigidity, classical computing has its limitations, especially in the realm of computational speed. Certain classical problems can be solved faster with quantum computers, although those problems rely on a small number of qubits to have any practical impact. To achieve such results, quantum computers implement quantum algorithms. As an example of this speedup, researchers demonstrated the power of quantum supremacy with a processor that took 200 seconds to make measurements of a quantum circuit, a process that would otherwise have taken a classical supercomputer 10,000 years [2].

There are numerous applications for quantum computing, as quantum algorithms abound in mathematical and physical applications. One example is factoring numbers. Classically, factoring numbers is computationally expensive. Shor's quantum algorithm does this at a much higher speed. Another example is cryptography, or more specifically, quantum key distribution (QKD). Even though public key cryptography incorporates some of the strongest encryptions out there, it still can provide only up to 30 years of security [3]. This level of security is fine for most industries, but for some more sensitive industries such as healthcare or defense, something like QKD that promises a longer life-time is optimal. Another example is the use of Grover's algorithm, a quantum search algorithm used to speed up an exhaustive subroutine (generally part of NP-complete problems).

## QUANTUM BITS

Quantum computing is probabilistic, which makes it vastly different from classical computing. Qubits now take on the role of classical bits. Indeed, it is these qubits that allow quantum computations to be performed. The state (or "status") of a qubit is composed of superpositions of pure states. These pure states form a basis for the system, so any new state of the system can be written in terms of a linear combination of the pure states. A measurement can be thought of as any experiment determining the state of electrons, photons, nuclei, or phonons [4-6]. When the measurement is made, the qubit takes on a value of 0 or 1 (the familiar classical bit), with a probability given by the initial state of the system [7]. Mathematically, prior to the measurement, there is some probability $d_0^2$ of measuring 0 and probability $d_1^2$ of measuring 1 such that [4]

$$d_0^2 + d_1^2 = 1 \tag{1}$$

It should be noted that $d_0$ and $d_1$ are the weights from the linear combination of the pure states of the system. The system can thus be written as

$$d_0|0\rangle + d_1|1\rangle \tag{2}$$

where

$$|0\rangle = \begin{pmatrix}1 & 0\end{pmatrix} \qquad |1\rangle = \begin{pmatrix}0 & 1\end{pmatrix}$$

which resides in $C^2$. When dealing with multiple qubits, the complex vector space grows exponentially according to $2^n$, where n $\in$ N [8].

## QUANTUM GATES

Quantum gates are operations on qubits. A measurement of the state of the qubit always gives $|0\rangle$ or $|1\rangle$. So while the system starts with a probability distribution, it collapses to one of these two values after a measurement. Quantum gates for one qubit are represented as 2 x 2 matrices. We present an example of the quantum $X$ gate, which is similar to the NOT gate in classical computing.

$$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}|0\rangle = |1\rangle \qquad \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}|1\rangle = |0\rangle$$

When dealing with more than one qubit, the transformation matrix changes size, which is now $2^n$ x $2^n$, where $n$ is a positive integer. We provide a matrix representation of the CNOT gate, which is used in quantum entanglement [8].

$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}|00\rangle = |00\rangle \quad \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}|01\rangle = |01\rangle \quad \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}|10\rangle = |11\rangle \quad \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}|11\rangle = |10\rangle$$

## QUANTUM ENTANGLEMENT

Quantum entanglement is when the value of a qubit can be determined by measuring the state of a different qubit [8]. From a physical perspective, quantum entanglement can be described as when the state of a particle $P_1$ depends on the state of another particle $P_2$ and vice versa. Measuring the energy of $P_1$ might give the value $E_a$, which would mean the energy of $P_2$ is definitely $E_b$, or if the particle $P_1$ has an energy of $E_c$, $P_2$ has an energy of $E_d$ [9]. Thus, when the value of one qubit is known, the value of the other is also known [8]. This is incredibly useful in quantum computing, as entanglement drastically improves the processing speed.

## QUANTUM CIRCUITS

Much like using classical bits for classical computations, a collection of quantum bits is used for quantum computations. This collection is called a quantum register, with all qubits set in the initial state $|0\rangle$. A quantum circuit is thus a series of quantum gates that takes qubits as input from the quantum register [8]. Schematically, quantum gates are operations on quantum bits, with quantum circuits being this collection of operations to achieve an end goal. There are various quantum gates which can be ordered in several ways within quantum circuits.

## QUANTUM ANNEALING

There are also more specialized forms of quantum computing. One such example is quantum annealing, which is especially powerful in problems with low-energy solutions, such as optimization and sampling problems. There may be many local minima, so to ensure the global minimum is reached, the energy of the system is temporarily changed through an iterative process. An example of such a process is the quantum unconstrained binary optimization algorithm [10]. There are generally two steps in finding the global minimum. If the system's energy decreases, the process is repeated. If the energy does not decrease, the process is not repeated right away but instead kept with some probability

$$P \propto \exp\{-\frac{\Delta E}{k_B T}\} \tag{3}$$

where $\Delta E \equiv E_{final} - E_{initial}$, with temperature $T$ and Boltzmann constant $k_B$. As this process seeks to find the minimal energy, this corresponds to an energy state with minimal temperature $T$. Therefore, as the process is repeated, the temperature starts from a very high value, eventually approaching zero. When the temperature is zero, the energy is equal to the internal system's energy. So at the end of this process, the global minimum energy is found with a high degree of certainty and thus solves the optimization problem [11].

## CONCLUSION

Quantum computing utilizes qubits in place of its classical bit counterpart. The qubit is composed of the superposition of the pure states, and the quantum gates apply operations to these qubits. Collecting these gates together gives us a quantum circuit whose orientation is used to define the quantum algorithm. Furthermore, quantum entanglement between qubits and quantum annealing are utilized to maximize the efficiency of the system.

With Rigetti Computing proposing methods to rapidly improve quantum models, inching closer to overtaking classical computing in the realm of satellite image classification, and IonQ further developing frameworks to better simulate molecular interactions, we come closer and closer to the quantum world Richard Feynman imagined all those years ago [12, 13].

## REFERENCES


1. R. Feynman, "Simulating Physics with Computers," Int. J. Theor. Phys. **21**, 467–488 (1982), (keynote speech).
2. F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. Buell, B. Burkett, Y. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, et al., Nature **574**, 505–510 (2019).
3. D. Stebila, M. Mosca, and N. Lütkenhaus, in *Quantum Communication and Quantum Networking*, edited by A. Sergienko, S. Pascazio, and P. Villoresi, QuantumComm (Springer, Naples, Italy, 2009), Vol. 36, pp. 283–296.
4. C. Bernhardt, *Quantum Computing for Everyone* (MIT Press, Cambridge, MA, 2019).
5. A. A. Wood, R. M. Goldblatt, R. E. Scholten, and A. M. Martin, Phys. Rev. Research **3**, 043174 (2021).
6. E. Berrios, M. Gruebele, D. Shyshlov, L. Wang, and D. Babikov, J. Phys. Chem. A **116**, 11347–11354 (2012).
7. R. Feynman, "The Concept of Probability in Quantum Mechanics," (Berkeley Symposium on Mathematical Statistics and Probability, 1951), pp. 533–541.
8. R. S. Sutor, *Dancing with Qubits: How Quantum Computing Works and How It Can Change the World* (Packt Publishing Ltd., Birmingham, UK, 2019).
9. D. J. Griffiths and D. F. Schroeter, *Introduction to Quantum Mechanics*, 3rd ed. (Cambridge University Press, 2018).
10. G. G. Guerreschi, preprint arXiv: 2101.07813 [quant-ph], 1–16 (2021).
11. B. K. Chakrabarti and A. Das, Transverse Ising model, glass and quantum annealing, in *Quantum Annealing and Related Optimization Methods* (Springer, 2005).
12. M. Henderson, J. Gallina, and M. Brett, Quantum Mach. Intell. **3** (2021), 10.1007/s42484-020-00034-6.
13. Y. Nam, J.-S. Chen, N. C. Pisenti, K. Wright, C. Delaney, D. Maslov, K. R. Brown, S. Allen, J. M. Amini, J. Apisdorf, K. M. Beck, A. Blinov, Chaplin, M. Chmielewski, C. Collins, S. Debnath, K. M. Hudek, A. M. Ducore, Keesan, S. M. Kreikemeier, et al., npj Quantum Inf. **6** (2020), 10.1038/s41534-020-0259-3.