# Quantum Information

University of Toronto
PHY293

Noel Jakubik

22 December 2020

# Introduction

Quantum information is governed by the laws of quantum mechanics that deals with physics at the subatomic scale. Information in a quantum state is stored in a *qubit*, as opposed to a classical bit, that exists in both binary states at any given time; a certain probability of existing in each state. This is the principle of superposition and it allows for phenomena like quantum entanglement along with applications such as quantum cryptography. This report will discuss the properties of quantum states and how this information is governed by quantum mechanics.

# Discussion

The Schrodinger Equation is a linear partial differential equation. With regards to the superposition principle, this means that a linear combination of the fundamental linearly independent solutions is also a solution. This corresponds directly to quantum information where the state of a quantum particle is some combination of the basis states[1]. The base states in quantum information are denoted as $|0\rangle$ and $|1\rangle$, known as Dirac notation[2]. As such, the superposition of these states to form a *qubit* can be written as

$$|\psi\rangle = c_1|0\rangle + c_2|1\rangle$$

where $c_1, c_2$ are complex probability amplitudes where the sum of their absolute values squared is one[3]. According to two postulates of quantum mechanics, the qubit states are governed by the time dependent Schrodinger Equation, shown below, and immediately collapse into a basis state once observed[4].

$$i\hbar\frac{\partial\Psi}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2\Psi}{\partial x^2} + V\Psi$$

The Bloch Sphere (shown in Figure 1) is a representation of a qubit; demonstrating its vector property and how it can exist as some combination of the $|0\rangle$ and $|1\rangle$ states as some point on the surface[5].

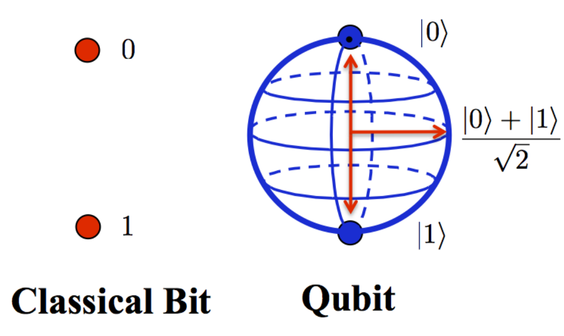


Figure 1: Difference between a classical bit and qubit (Bloch Sphere)[6]

The state of a quantum system can be described using a density matrix $\rho$ that is defined as

$$\rho \equiv \sum p_i|\psi\rangle\langle\psi|$$

where $\psi$ is the pure state and $p$ is the probability[7]. This lends itself to the new definition of entropy used in quantum mechanics, the *von Neumann entropy*, defined as[8]

$$S = -tr(\rho \ln \rho)$$

This newly defined entropy is an extension of the classical *Shannon entropy* definition such that it pertains to quantum systems. This is where the main difference between classical information and quantum information lies. Quantum systems have properties such as entanglement and superposition that have no classical counterpart. This allows for a fundamentally different type of computation and information relationship to exist. The dependency of particles on others in entanglement allows for use in cryptography, teleportation, and potentially computation[9].

The main applications of quantum information lie in computation and encryption. Quantum computing is widely regarded as the next stage in computation, although, this is only partially true. Quantum computers only prevail over classical computers in very difficult computations, such as prime number factorization. Shor's algorithm to find prime factors is suited for a quantum computer because it is capable of simultaneous computations[10]. For commercial use, a quantum computer will not work any better or any more efficiently than a classical computer; quantum computers are meant to solve a different type of problem, optimization, than classical computers.

With regards to cryptography, *quantum key distribution* is the predominant solution to classical security issues. The superposition of bits is what makes quantum encryption so powerful[11]. The principle that a bit exists as some combination of two states until it is observed ensures the security of some communicated message. Any interception of the message will be known because the qubits will collapse into a basis state as soon as they are observed by an outside party[12]. Quantum information has the potential of changing the way computations are executed and data is encrypted. The principles that quantum mechanics lends allows for a new way to use and apply information.

# Conclusion

The rise in recent understanding of quantum mechanics has allowed for the development of a new field known as quantum information. Quantum information behaves differently than classical information and this difference in properties can be used in various applications such as encryption and computing. The principle of superposition in bits allows for various phenomena that can be effectively exploited to improve efficiency in a variety of currently difficult computations.

# References


[1] P. E. Black, D. R. Kuhn, and C. J. Williams, "Quantum Computing and Communication," ScienceDirect, 2002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0065245802800079. [Accessed: 22-Dec-2020].

[2] "Fundamentals of quantum information," Physics World, 03-May-2019. [Online]. Available: https://physicsworld.com/a/fundamentals-of-quantum-information/. [Accessed: 22-Dec-2020].

[3] P. G. Kwiat and D. F. V. James, "Entanglement and Quantum Information," Encyclopedia of Modern Optics II, Volume 1 , 2018. [Online]. Available: https://www.sciencedirect.com/sdfe/pdf/download/eid/3-s2.0-B9780128092835009642/first-page-pdf. [Accessed: 22-Dec-2020].

[4] A. Rae, "Quantum Information," in Quantum Mechanics: Sixth Edition, J. Napolitano, Ed. Boca Raton, FL: CRC Press, 2016, pp. 345–354.

[5] D. Marinescu and G. Marinescu, "Bloch Sphere," Classical and Quantum Information Theory, 2012. [Online]. Available: https://www.sciencedirect.com/topics/mathematics/bloch-sphere. [Accessed: 22-Dec-2020].

[6] rotowhirlrotowhirl 3355 bronze badges, DaftWullieDaftWullie 34.6k11 gold badge1919 silver badges7171 bronze badges, and Zixuan LiuZixuan Liu 4144 bronze badges, "Polarization and qubit information," Quantum Computing Stack Exchange, 01-Dec-1967. [Online]. Available: https://quantumcomputing.stackexchange.com/questions/4693/polarization-and-qubit-information. [Accessed: 23-Dec-2020].

[7] A. Tokmakoff, "5.1: Introduction to the Density Matrix," Introduction to the Density Matrix, 12-Dec-2020. [Online]. Available: https://chem.libretexts.org/Bookshelves/Physical and Theoretical Chemistry Textbook Maps/Book: Time Dependent Quantum Mechanics and Spectroscopy (Tokmakoff)/05: The Density Matrix/5.01: Introduction to the Density Matrix. [Accessed: 22-Dec-2020].

[8] C. Timpson, "Quantum Information Theory and The Foundations of Quantum Mechanics," thesis, The Queen's College, Oxford, 2004.

[9] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eible, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," Institut fur Experimentalphysik, Universitat Innsbruck, Technikerstr, pp. 575–576, 1997.

[10] "Docs and Resources," IBM Quantum Experience. [Online]. Available: https://quantum-computing.ibm.com/docs/iqx/guide/shors-algorithm. [Accessed: 22-Dec-2020].

[11] "Quantum Cryptography, Explained," Quantum Xchange. [Online]. Available:

https://quantumxc.com/quantum-cryptography-explained/. [Accessed: 22-Dec-2020].

[12] A. Sadovsky and J. Ortiz, "Quantum Cryptography," Modern Cryptography: Theory and Applications. [Online]. Available: https://cs.stanford.edu/people/eroberts/courses/soco/projects/2004-05/cryptography/quantum.html. [Accessed: 22-Dec-2020].