Entropy in Quantum Information Theory

Charles Yang
(Dated: August 4, 2017)

While entropy is a concept that originated in the field of Thermodynamics, it is often applied in Information Theory. In classical information, information is described by Shannon Entropy and in quantum information as von Neumann entropy. While both describe similar concepts in each field, von Neumann Entropy is becoming a greater subject of interest due to the quickly advancing development of quantum computers.

I. QUANTUM INFORMATION

As classical information is stored on a classical bit—1 and 0—quantum information is stored on a quantum bit, or qubit—$|1\rangle$ (up) and $|0\rangle$ (down). However, due to the effects of *quantum superposition*, a qubit can be in both the "up" and "down" states at once, or a linear combination of the two:

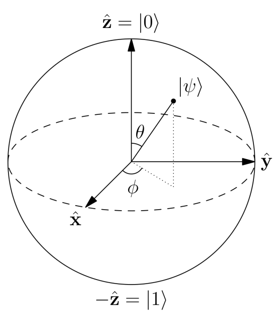
$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

where $|\psi\rangle$ is a normalized vector, so

$$\|\alpha\|^2 + \|\beta\|^2 = 1$$

$\|\alpha\|^2$ and $\|\beta\|^2$ represent the probabilities of the qubit collapsing into the $|1\rangle$ and $|0\rangle$ states respectively.

A useful way of imagining a single qubit is the Bloch Sphere:



[1]

This interpretation results in another equation

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

to represent a qubit as a point on the Bloch Sphere[2, 3]. Operations on these qubits, such as the Not Gate, are simply transformations, i.e. rotation, of $|\psi\rangle$ on the Bloch Sphere.

A system of multiple qubits can be denoted in a manner similar to the first expression, as a linear combination of the base states of the system. A two qubit system would then look like

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

with $|\psi\rangle$ again being normalized. As the only useful information in these vectors are the complex coefficients of the base states, a qubit can be rewritten as

$$(\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11})$$

This can be further generalized to n qubits as

$$|\psi\rangle = \sum_{i\in\{0,1\}^n} \alpha_i |i\rangle$$

or

$$(\alpha_{i_1}, \alpha_{i_2} \dots \alpha_{i_n})$$

Similar to how a operations on a single qubit are transformations on the state of the qubit, operations on multiple qubits are also transformations. These operations are matrix transformations on the qubit's

II. ENTROPY IN CLASSICAL INFORMATION

In Classical Information Theory, the main concept of entropy is Shannon Entropy. Given a set $\mathcal{X} = \{x_1, x_2, x_3 \dots x_n\}$, the entropy H of a variable X in terms of $\mathcal{X}$ is given by

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log_2 p(x)$$

where $p(x)$ denotes the probability of x being randomly chosen from the set $\mathcal{X}$[2, 4, 5]. Shannon Entropy in gives the average number of bits required to store X. It also describes the maximum reliable compression ratio[4]. Rewriting the above equation in terms of expected value (weighted average of all outcomes) helps to extend Shannon Entropy to joint (such as x and y together) and conditional (a y following an x).The resulting equations are

$$H(X) = -E\log_2 p(x)$$
$$H(X,Y) = -E\log_2 p(x,y)$$
$$H(Y|X) = -E\log_2 p(y|x)$$

where E represents "the expected value of," (X,Y) that X and Y occur together, and $(Y|X)$ that Y follows X[5].

III. ENTROPY IN QUANTUM INFORMATION

In Quantum Information Theory, Shannon Entropy is generalized to von Neumann Entropy. The entropy of the quantum state, or density matrix, ρ is given in a similar form

$$H(\rho) = -\mathrm{tr}(\rho \log_2 \rho)$$

where tr() signifies the sum of the main diagonal of the density matrix[2]. The density matrix arises from the wavefunction of the qubit; more specifically it is the wavefunction's outer product. For instance, take a single qubit, given by

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

the density matrix, ρ, will then be given by

$$\begin{aligned} \rho &= |\psi\rangle \langle\psi| \\ &= \begin{bmatrix} \alpha^* \\ \beta^* \end{bmatrix} \begin{bmatrix} \alpha & \beta \end{bmatrix} \\ &= \begin{bmatrix} \alpha\alpha^* & \alpha^*\beta \\ \alpha\beta^* & \beta\beta^* \end{bmatrix} \end{aligned}$$

similar results occur with vectors with more dimensions. This example is a so called "pure" state, analogous to a single letter in $\mathcal{X}$, and has entropy of 0. The overall mixed density matrix is given as a weighted average of these pure states, which is given by

$$\rho = \sum_j p_j |\psi_j\rangle \langle\psi_j|$$

Substituting ρ into the original equation for von Neumann Entropy, we can rewrite it as

$$H(\rho) = -\sum_j p_j \log_2 p_j$$

which shares many parallels with the statement of Shannon Entropy[3]. As implied by the visual similarity, von Neumann Entropy can be applied to quantum information in a similar manner to how Shannon Entropy is applied to classical information, but due to the more general nature of von Neumann Entropy, it is used in a larger variety of relations.

A. Applications of von Neumann Entropy

von Neumann Entropy builds the basis for many topics in Quantum Information Theory:

- Compression: Shumacher proved a similar relation to Shannon's Noiseless Coding Theorem, namely that $S(\rho)$ signifies the largest compression ratio without loss of data[4].

- Entanglement: von Neumann Entropy is used to measure how entangled two systems are, with $E(|\Psi_{AB}\rangle) \equiv S(\rho)$ [4, 6]. Furthermore, when generalized to n-qudits (base-n), it can be used to prove that the maximum entropy of a entangled state is $|Max\rangle = \mathfrak{F}_s \left|\vec{0}\right\rangle$ where$\mathfrak{F}_s$ represents a "string Fourier transformation"[7].

- Noisy Channels: Information sent over a noisy channel can be decoded if it is decoupled from the channel's environment[4].

[1] W. Commons, "File:bloch sphere.svg — wikimedia commons, the free media repository," (2016), [Online; accessed 1-August-2017].

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[3] J. A. Jones and D. Jaksch, *Quantum Information, Computation and Communication* (Cambridge University Press, 2012).

[4] J. Preskill, "Caltech physics 219/computer science 219, lecture notes: Quantum computing," [Online, accessed 1-August-2017].

[5] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (John Wiley & Sons, 2006).

[6] G. Jaeger, *Quantum Information* (Springer, 2007).

[7] A. Jaffe, Z. Liu, and A. Wozniakowski, "Holographic software for quantum networks," Manuscript.