Tsallis entropy and quantum uncertainty in information measurement

Mhlambululi Mafu[1], **Francesco Petruccione** [1,2]

[1] Centre for Quantum Technology, School of Chemistry and Physics, University of KwaZulu-Natal, P/Bag X54001 Durban 4000, South Africa

[2] National Institute for Theoretical Physics (NITheP), KwaZulu-Natal, South Africa

E-mail: mafum@ukzn.ac.za, petruccione@ukzn.ac.za

Abstract. The Tsallis entropy defines an important generalization of the usual concept of entropy which depends on parameter α. Our goal is to establish a connection between the quantum uncertainty principle and the Tsallis entropy for single discrete observables. In particular, we show that there exist a generalized uncertainty bound reached in order to appropriately express the quantum uncertainty principle in terms of the Tsallis entropy. This kind of connection forms an initial important step towards finding an important application of this α-entropy in the area of quantum communication for which they have not been extensively investigated.

1. Introduction

Depending on the application, a number of entropic forms [1] and uncertainty relations [2, 3, 4] have been derived. Amongst entropies, the most important and greatly studied entropy that has even found major applications is the Shannon entropy [5]. Many generalizations or versions of the Shannon entropy have already been found and one of the generalizations is the Tsallis entropy [6]. The Tsallis entropy was introduced by Havrda and Charvát in 1967 [7] and later studied by Darcózy in 1970 [8], it was in 1988 when Tsallis [6] exploited its features and placed a physical meaning on this entropy. Therefore, this entropy is now known as the Tsallis entropy. Similar to the Shannon entropy, the Tsallis entropy has also found many interdisciplinary applications [9]. In particular, it has been established that the Tsallis and Shannon entropies can be connected by means of some transformation [9]. Therefore, this connection between these two entropies shows a possibility of interchangeability between these two entropies, however only up to some bound.

On the other hand, the first uncertainty relation to be derived was by Hirschman [10]. This uncertainty relation was a position-momentum relation which is based on the Shannon entropy. However, the Heisenberg uncertainty principle [11] forms one of the most developed results of quantum theory. In particular, Robertson showed that a product of two standard deviations of two discrete observables A and B measured in the quantum state $|\psi\rangle$ is bounded from below [12]. This can be expressed as $\triangle A \cdot \triangle B \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle|$. This result was improved by Deutsch in 1983 [13]. The improvement on Deutsch's work was conjectured by Kraus [14] and later proved by Maassen and Uffink [15]. However, it has also been observed that this Robertson's bound does not express all the features expected from an uncertainty relation if the observables A and B are finite [16].

Recently, the entropic uncertainty relations have found several applications especially in quantum information [17, 18]. We highlight that such applications in quantum information are based on properties of the Shannon entropy. However, the Tsallis entropy has not been utilized in such applications. A major difference exists between the Shannon and the Tsallis entropy, i.e., the Shannon entropy is additive for independent probability distributions while the Tsallis entropy is non-additive [19]. Therefore, this difference proves to be a challenge in trying to immediately connect the Tsallis entropy to these applications in quantum information. Despite this major difference in the non-additivity property for independent probability distributions of the Tsallis entropy, it is the object of this paper to explicitly show a bound based on Tsallis entropy and subsequently a possible extension of the application for Tsallis entropies to physical processes in quantum information specifically on quantum key distribution. Therefore, we establish a connection between the quantum uncertainty principle and the Tsallis entropy for single discrete observables. We also show an immediate application of the Tsallis entropy on how they can be useful in quantifying information in quantum key distribution.

2. Tsallis entropy

For a probability distribution, p_i, on a finite set, the Tsallis entropy, $S_\alpha(p_i)$ for order α is defined as [6]

$$S_\alpha(p_i) = -\sum_{i=1}^{n} p_i^\alpha \ln_\alpha p_i, \tag{1}$$

where $0 < \alpha < \infty$. The Tsallis entropy can also be expressed as $S_\alpha(p_i) = \frac{1}{1-\alpha}\left(\sum_i p_i^\alpha - 1\right)$. The α algorithm in Eq (1) is defined as $\ln_\alpha(x) = x^{1-\alpha} - 1/(1-\alpha)$ for any nonnegative real numbers α and x. At $\alpha = 1$, $S_\alpha(p_i)$ does not exist, therefore we use the L'Hopitals rule to show that the Tsallis entropy approaches the Shannon entropy as $\alpha \mapsto 1$, because the α logarithm uniformly converges to a natural logarithm as $\alpha \mapsto 1$ i.e., $\lim_{\alpha\mapsto 1} S_\alpha(p_i) = -\sum_i p_i \ln p_i$ which is the Shannon entropy [5]. In particular, there is also a close relationship between the Rényi entropy and the Tsallis entropy written as

$$H_\alpha(p_i) = \frac{1}{1-\alpha}\ln(1 + (1-\alpha)S_\alpha(p_i)). \tag{2}$$

where $H_\alpha(p_i)$ is the Rényi entropy. Among the property of these entropies, a major difference exists, the Shannon and Rényi entropies are derived to be additive whilst the Tsallis entropy is derived to be pseudo-additive for $\alpha \neq 1$ and is expressed as

$$S_\alpha(p_i, p_j) = S_\alpha(p_i) + S_\alpha(p_j) + (1-\alpha)S_\alpha(p_i)S_\alpha(p_j), \tag{3}$$

where p_i and p_j are distributions for independent random variables A and B respectively.

In order to arrive at our goal, we start by summarizing the result of Ref [13]. Of importance, Deutsch established that the generalized Heisenberg inequality does not properly express the quantum uncertainty principle except in the canonically conjugate observables. In general, he found that in order to properly quantify the quantum uncertainty principle, there exists an irreducible lower bound in the result of uncertainty of a measurement. This can be written quantitatively as

$$\mathcal{U}(\hat{A}, \hat{B}; \psi) \geq \mathcal{B}(\hat{A}, \hat{B}), \tag{4}$$

where $\mathcal{U}$ is the uncertainty in the measurement of $\hat{A}$ and $\hat{B}$ which are simultaneously prepared or measured observables, $|\psi\rangle$ is the outcome state and $\mathcal{B}$ is the irreducible lower bound as according to Ref [13]. The function $\mathcal{U}(\hat{A}, \hat{B})$ depends only on the state $|\psi\rangle$ and the sets $\{|a\rangle\}$ and $\{|b\rangle\}$ while $\mathcal{B}(\hat{A}, \hat{B})$ depends on the set $\{\langle a|b\rangle\}$ of the inner product of two eigenstates of A and B respectively.

Based on Ref [13], the most natural measure of uncertainty is the result of a measurement or preparation of a single discrete observable which can be expressed in the entropic form as

$$S_{\hat{A}}(|\psi\rangle) = -\sum_{a} |\langle a|\psi\rangle|^2 \ln |\langle a|\psi\rangle|^2. \tag{5}$$

We can recognize that the right hand side of Equation (5) is expressed in terms of the Shannon's entropy where, $p_i = |\langle a_i|\psi\rangle|^2$ and $p_j = |\langle b_j|\psi\rangle|^2$ are projectors of $|\psi\rangle$ on $\hat{A}$ and $\hat{B}$ respectively. It has been shown in Ref [14] that

$$\mathcal{U}(\hat{A}, \hat{B}; \psi) \geq 2 \ln \frac{1}{1+c}, \tag{6}$$

where $c = \max_{ij} |\langle a_i|b_j\rangle|$. As stated previously that this bound was later improved by Maassen and Uffink [15] for which they obtained

$$\mathcal{U}(\hat{A}, \hat{B}; \psi) \geq 2 \ln \frac{1}{c}, \tag{7}$$

by considering measurements from two mutually unbiased bases, therefore our aim to investigate whether the non-extensivity property of the Tsallis entropy will ever make a difference on the requirements of $\mathcal{B}$ instead of using the Shannon entropy. However, surprisingly, we reach a bound which can be expressed in a similar manner as in Ref [13].

We consider two observables $\hat{A}$ and $\hat{B}$ which are simultaneously measured or prepared and a state $|\psi\rangle$ which represents the outcome of a measurement or preparation. Therefore, for our scenario in order to find the bound on $\mathcal{B}(\hat{A}, \hat{B})$ we relate this function to the pseudo-additivity property of Tsallis entropy instead of using additivity of Shannon entropy and without loss of generality we write Equation (3) as

$$\mathcal{U}(\hat{A}, \hat{B}; \psi) = S_\alpha(\hat{A}; \psi) + S_\alpha(\hat{B}; \psi) + (1-\alpha) S_\alpha(\hat{A}; \psi) S_\alpha(\hat{B}; \psi). \tag{8}$$

Now we calculate the bound $\mathcal{U}$ by using the Tsallis entropy as an information measure by proceeding as follows

$$\begin{aligned}
\mathcal{U}(\hat{A}, \hat{B}; \psi) &= -\sum_{a} |\langle\psi|a\rangle|^{2\alpha} \ln_\alpha |\langle\psi|a\rangle|^2 - \sum_{b} |\langle\psi|b\rangle|^{2\alpha} \ln_\alpha |\langle\psi|b\rangle|^2 \\
&+ (1-\alpha) \sum_{a} |\langle\psi|a\rangle|^{2\alpha} \ln_\alpha |\langle\psi|a\rangle|^2 \sum_{b} |\langle\psi|b\rangle|^{2\alpha} \ln_\alpha |\langle\psi|b\rangle|^2 \\
&= -\sum_{ab} |\langle\psi|a\rangle|^{2\alpha} |\langle\psi|b\rangle|^{2\alpha} [(\ln_\alpha |\langle\psi|a\rangle|^2 + \ln |\langle\psi|b\rangle|^2) \\
&- (1-\alpha) \ln_\alpha |\langle\psi|a\rangle|^2 \ln_\alpha |\langle\psi|b\rangle|^2].
\end{aligned} \tag{9}$$

We can maximize the parenthesized quantity in Equation (9), by performing the following operations:

$$\begin{aligned}
\mathcal{U}(\hat{A}, \hat{B}; \psi) &= \max_{|\psi\rangle} |\langle\psi|a\rangle\langle b|\psi\rangle| \\
&\leq \max_{|\psi\rangle} | \left(\frac{|a\rangle\langle a| + |b\rangle\langle b|}{2} \right) |.
\end{aligned} \tag{10}$$

In the following analysis, we are going to restrict our attention to two vectors at a time. In order to calculate the maximum eigenvalue of the expression in Equation (10), we apply the following substitution

$$|a\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \;\; |b\rangle = \begin{pmatrix}\cos\theta e^{-i\alpha}\\ \sin\theta\end{pmatrix}$$

and arrive at an expression of the form

$$\begin{aligned}\left(\frac{|a\rangle\langle a| + |b\rangle\langle b|}{2}\right) &= \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}\cos^2\theta & \cos\theta\sin\theta e^{-\alpha}\\ \sin\theta\cos\theta e^{-i\alpha} & \cos^2\theta\end{pmatrix}\\ &= \frac{\mathbb{1}}{2} + \frac{\sin\theta\cos\alpha}{2}X - \frac{\sin\theta\cos\theta\sin\alpha}{2}Y + \frac{\cos^2\theta}{2}Z, \end{aligned} \tag{11}$$

where X, Y and Z are the Pauli matrices.

Theorem: If we consider $M = a\mathbb{1} + bX + cY + dZ$ where $a, b, c, d \in \mathbb{R}^+$ where $m = a \pm \sqrt{b^2 + c^2 + d^2}$ are the eigenvalues of M.

Based on Equation (9) find that $a = \frac{1}{2}$, $b^2 = \frac{\sin^2\theta\cos^2\theta\cos^2\alpha}{4}$, $c^2 = \frac{\sin^2\theta\cos^2\theta\sin^2\alpha}{4}$ and $d^2 = \frac{\cos^4\theta}{4}$. By substitution and some few algebraic steps we arrive at the value of

$$m = \frac{1}{2} \pm \frac{\cos\theta}{2}. \tag{12}$$

The maximum eigenvalue of M i.e., $m_{\max} = (1 + \cos\theta)/2$ corresponds to $|\psi\rangle$ and occurs midway between $|a\rangle$ and $|b\rangle$. Therefore, we can express this as a function

$$\begin{aligned} f(a,b) = \mathcal{U}(\hat{A}, \hat{B}; \psi) &= -2\ln\left[\frac{1 + \langle a|b\rangle}{2}\right]\\ &= 2\ln\frac{2}{1 + \langle a|b\rangle}. \end{aligned} \tag{13}$$

Using the fact that $\sum_a |\langle\psi|a\rangle|^2 = 1$ and $\sum_b |\langle\psi|b\rangle|^2 = 1$, we can express

$$\begin{aligned} \sum_{a,b} |\langle\psi|a\rangle|^2 \cdot |\langle\psi|b\rangle|^2 \cdot f(a,b) &\geq \min_{a,b} f(a,b)\\ &\geq 2\ln\frac{2}{1 + \langle a|b\rangle}. \end{aligned} \tag{14}$$

3. Results

Considering that

$$\min\left[\frac{\ln 2}{1 + \langle a|b\rangle}\right] = \frac{\ln 2}{1 + \max|\langle a|b\rangle|}, \tag{15}$$

we can put everything together as

$$\mathcal{U}(\hat{A}, \hat{B}; \psi) = S_\alpha(\hat{A}; \psi) + S_\alpha(\hat{B}; \psi) + (1 - \alpha)S_\alpha(\hat{A}; \psi)S_\alpha(\hat{B}; \psi). \tag{16}$$

It is immediately seen that $\mathcal{U}(\hat{A}, \hat{B}; \psi) \geq 0$, with $\mathcal{U}(\hat{A}, \hat{B}; \psi) = 0$ if and only if $|\psi\rangle$ is a common eigenstate of $\hat{A}$ and $\hat{B}$. Besides this, $\mathcal{U}(\hat{A}, \hat{B}; \psi)$ is never greater than $(1 - N^{2(\alpha-1)})/1 - \alpha$, where N is the parenthesized quantity inside the square brackets in the equation below.

$$\mathcal{U}(\hat{A}, \hat{B}; \psi) \geq \frac{1}{1 - \alpha}\left[1 - \left(\frac{2}{1 + \max|\langle a|b\rangle|}\right)^{2(\alpha-1)}\right]. \tag{17}$$

If we take $c = \max_{ij}|\langle a_i|b_j\rangle|$, where $|a_i\rangle$ and $|b_j\rangle$ are the eigenvectors of $\hat{A}$ and $\hat{B}$ respectively, we obtain the bound

$$\mathcal{U}(\hat{A}, \hat{B}; \psi) \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{2}{1+c}\right)^{2(\alpha-1)}\right]. \tag{18}$$

However, by appealing to the Riesz's theorem [15, 20] in the region of $1/2 \leq \alpha \leq 1$, a better hence tighter bound is obtained which can be expressed as

$$\mathcal{U}(\hat{A}, \hat{B}; \psi) \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{1}{c}\right)^{2(\alpha-1)}\right]. \tag{19}$$

This result has the same form as shown in Ref [13]. This gives an irreducible lower bound (generalized uncertainty measure) of the uncertainty on the simultaneous measurement of observables when we use the Tsallis entropy to express the quantum uncertainty relation. Based on this connection, we can directly use this result as an information measure in quantum key distribution protocols where the two legitimate parties, Alice and Bob generate a secret key based on the measurements of the states which they receive. However, this communication takes place in the presence of an eavesdropper, Eve who tries to learn the information being communicated. The eavesdropper can perform any kind of attack on the communication channel but however is only limited by the laws of physics [21]. Provided the correlations are stronger between the measurements of the two legitimate parties, they can still generate a secret key. We therefore appeal to the result by Devetak and Winter [22]. This result quantifies the amount of extractable key, and is expressed as

$$K \geq H(X|E) - H(X|B), \tag{20}$$

where K is the final shared secret key, $H(X|E)$ is the amount of key that Alice can extract from a string X when given the uncertainty of the adversary about X, and $H(X|B)$ is the amount of information that Bob needs to correct his errors, using optimal error correction, given by his uncertainty about the shared string X. Therefore, without loss of generality we can simply re-write this lower bound in terms of Tsallis entropy as

$$K \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{1}{c}\right)^{2(\alpha-1)}\right] - S_\alpha(X|B) - S_\alpha(Y|B). \tag{21}$$

Suppose that Alice's measurements are represented by X and X' and Bob's measurements are represented by Y and Y', therefore in order to generate a secret key the two parties need to communicate the choice of their measurements to each other. Based on the property that measurements cannot decrease entropy [23] we can write

$$K \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{1}{c}\right)^{2(\alpha-1)}\right] - S_\alpha(X|X') - S_\alpha(Y|Y'). \tag{22}$$

By assuming symmetry i.e., $S_\alpha(X|X') = S_\alpha(Y|Y')$, this gives us a simple proof against collective attacks which was shown in Ref [24] for the BB84 protocol by using the Shannon entropy. The conditional Tsallis entropy is defined in the Appendix.

4. Conclusion

We have shown that the quantum uncertainty principle can be expressed in terms of the Tsallis entropy. We remark that this result preserves a form similar to the most important result which

was obtained by Deutsch [13]. Regardless of the Tsallis entropies being non-additive, we have shown that a limit with a similar form can be reached as was shown by Deutsch's derivation which is based on the Shannon entropy. We highlight this result provides an initial step in finding more interesting applications of the Tsallis entropy in the area of quantum information for example, as a measure of information in quantum key distribution protocols for evaluating important parameters such as secret key.

Acknowledgments
We would also like to thank the reviewers for providing valuable comments on the earlier version of our manuscript can be improved. This work is based on research supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

References

[1] Scarfone A M 2013 *Entropy* **15** 624–649
[2] Hall M J 1999 *Physical Review A* **59** 2602
[3] Busch P, Heinonen T and Lahti P 2007 *Physics Reports* **452** 155–176
[4] Zozor S, Portesi M and Vignat C 2008 *Physica A: Statistical Mechanics and its Applications* **387** 4800–4808
[5] Shannon C 2001 *ACM SIGMOBILE Mobile Computing and Communications Review* **5** 3–55
[6] Tsallis C 1988 *Journal of Statistical Physics* **52** 479–487
[7] Havrda J and Charvát F 1967 *Kybernetika* **3** 0–3
[8] Daróczy Z 1970 *Information and control* **16** 36–51
[9] Fiori E R and Plastino A 2012 *arXiv preprint arXiv:1201.4507*
[10] Hirschman I 1957 *American Journal of Mathematics* **79** 152–156
[11] Heisenberg W 1927 *Zeitschrift für Physik A Hadrons and Nuclei* **43** 172–198
[12] Robertson H P 1929 *Phys. Rev.* **34**(1) 163–164 URL `http://link.aps.org/doi/10.1103/PhysRev.34.163`
[13] Deutsch D 1983 *Phys. Rev. Lett.* **50**(9) 631–633 URL `http://link.aps.org/doi/10.1103/PhysRevLett.50.631`
[14] Kraus K 1987 *Phys. Rev. D* **35**(10) 3070–3075 URL `http://link.aps.org/doi/10.1103/PhysRevD.35.3070`
[15] Maassen H and Uffink J B M 1988 *Phys. Rev. Lett.* **60**(12) 1103–1106 URL `http://link.aps.org/doi/10.1103/PhysRevLett.60.1103`
[16] Prevedel R, Hamel D R, Colbeck R, Fisher K and Resch K J 2011 *Nature Physics* **7** 757–761
[17] Damgård I B, Fehr S, Renner R, Salvail L and Schaffner C 2007 *Advances in Cryptology-CRYPTO 2007* (Springer) pp 360–378
[18] Berta M, Christandl M, Colbeck R, Renes J M and Renner R 2010 *Nature Physics*
[19] Dukkipati A, Murty M N and Bhatnagar S 2006 *Physica A: Statistical Mechanics and its Applications* **361** 124–138
[20] Hardy G, Littlewood J and Pólya G 1934 *Inequalities* (Cambridge University Press, London and New York)
[21] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301–1350
[22] Devetak I and Winter A 2005 *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science* **461** 207–235
[23] Nielsen M A and Chuang I L 2010 *Quantum Computation and Quantum Information* (Cambridge University Press)
[24] Shor P W and Preskill J 2000 *Physical Review Letters* **85** 441–444