# 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, School of Chemistry and Physics, University of KwaZulu-Natal, P/Bag X54001 Durban 4000, South Africa

E-mail: 209526077@stu.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 $\alpha$. 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 $\alpha$-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]. The first uncertainty relation was derived by Hirschman [6]. It was a position-momentum relation which is based on the Shannon entropy. Since then, many generalizations or versions of the Shannon entropy have already been found. One of the generalizations of the Shannon entropy is the Tsallis entropy [7]. The Tsallis entropy has again found many interdisciplinary applications [8]. Furthermore, it was found that the Tsallis and the Shannon entropy can be connected by means of some transformation [8]. Therefore, to some extent this connection shows a possibility of interchangeability between these two entropies, only up to some bound. Recently, the entropic uncertainty relations have found applications in quantum cryptography [9, 10]. 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 [11]. Therefore, this difference proves to be a challenge in trying to immediately connect the Tsallis entropy to these applications.

After being introduced by Havrda and Charvát in 1967 [12] and later studied by Darcózy in 1970 [13], it was in 1988 when Tsallis [7] exploited its features and placed a physical meaning on this entropy. Therefore, this entropy is now known as the Tsallis entropy. On the other hand, the Heisenberg uncertainty principle [14] forms one of the most developed results of quantum theory. In particular, Robertson showed that a product of the two standard deviations of

two discrete observables $A$ and $B$ measured in the quantum state $|\psi\rangle$ is bounded from below [15]. 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 [16]. However, this improved result by Deutsch was conjectured by Kraus [17] and later proved by Maassen and Uffink [18]. Recently, 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 [19]. Despite of 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 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 entropies on how they can be useful in quantifying information especially in quantum key distribution.

## 2. Tsallis entropy

For a probability distribution, $p_i$ on a finite set, the Tsallis entropy, $S_\alpha(p_i)$ of order $\alpha$ is defined as [7]

$$S_\alpha(p_i) = \frac{1}{1-\alpha}\sum_i p_i^\alpha - 1, \tag{1}$$

where $0 < \alpha < \infty$. 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 $\alpha \mapsto 1$, 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. However a major difference exists, the Shannon and Rényi entropies are additive whilst the Tsallis entropy is pseudo-additive. This pseudo-additivity property in general is defined 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 [16]. 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 [16]. 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 eigenstates of $A$ and $B$ respectively.

Based on Ref [16], 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 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. However it has been shown in Ref [17] that

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

where $c = \max_{ij} |\langle a_i|b_j\rangle|$. However, as stated previously that this bound was later improved by Maassen and Uffink [18] 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 [16].

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 additivity of Tsallis entropy instead of using additivity of Shannon entropy and without loss of generality we write

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

Now we calculate the bound $\mathcal{B}$ by using the Tsallis entropy as an information measure. We proceed as follows

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

In order to maximize Equation (9), we perform the following operations:

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

Our task now is to calculate the maximum eigenvalue of the expression in Equation (10). We apply the substitution

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

in Equation (10) and arrive at an expression of the from

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

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 the eigenvalues of $(M) = a \pm \sqrt{b^2 + c^2 + d^2}$.

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 $|\psi\rangle = (1 + \cos\theta)/2$ occurs midway between $|a\rangle$ and $|b\rangle$. Therefore, we can express this as a function

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

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

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

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

$$\begin{aligned} \mathcal{B}(\hat{A}, \hat{B}) &= S_\alpha(\hat{A};\psi) + S_\alpha(\hat{B};\psi) + (1-\alpha)S_\alpha(\hat{A};\psi)S_\alpha(\hat{B};\psi) \\ &\geq \frac{1}{1-\alpha}\left[1 - \left(\frac{2}{1 + \max|\langle a|b\rangle|}\right)^{2(\alpha-1)}\right]. \end{aligned} \tag{16}$$

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

$$\mathcal{B}(\hat{A}, \hat{B}) \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{2}{1+c}\right)^{2(\alpha-1)}\right]. \tag{17}$$

However, by appealing to the Riesz's theorem [18, 20] in the region of $1/2 \leq \alpha \leq 1$, a better hence tighter bound is obtained which can be expressed as

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

This result has the same form as shown in Ref [16]. 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, now 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. 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. However, this communication takes place in the presence of an eavesdropper, Eve. The eavesdropper can perform any kind of attack on the communication channel and is only limited by the laws of physics. 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 [21] who quantified the amount of extractable key which can be expressed as, $K \geq H(X|E) - H(X|B)$. Without loss of generality, we can simply re-write this lower bound in terms of Tsallis entropy as

$$K \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{1}{c}\right)^{2(\alpha-1)}\right] - S_\alpha(X|B) - S_\alpha(Y|B). \tag{19}$$

However, based on the property that measurements cannot decrease entropy we can write

$$K \geq \frac{1}{1-\alpha}\left[1 - \left(\frac{1}{c}\right)^{2(\alpha-1)}\right] - S_\alpha(X|X') - S_\alpha(Y|Y'). \tag{20}$$

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 [22] for the BB84 protocol by using the Shannon entropy. The conditional Tsallis entropy is defined in the Appendix.

## 3. Conclusion

Based on the above calculations, we have shown that the quantum uncertainty principle can be expressed in terms of the Tsallis entropy. We remark that this result preserves a similar form with the result which was obtained by Deutsch [16]. Therefore, we can conclude that the regardless of the Tsallis entropies being non-additive, we can reach the some limit as was shown by Deutsch's derivation which was derived based on the Shannon entropy. We highlight this result may provide 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 where we evaluate for important parameters such as secret key generation rates. The most important question is, whether the Tsallis entropies can gives us better bounds when compared to the Shannon and Rènyi entropies will remain a project for future research.


## Acknowledgments

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] Hirschman I 1957 *American Journal of Mathematics* **79** 152–156
[7] Tsallis C 1988 *Journal of Statistical Physics* **52** 479–487
[8] Fiori E R and Plastino A 2012 *arXiv preprint arXiv:1201.4507*
[9] Damgård I B, Fehr S, Renner R, Salvail L and Schaffner C 2007 *Advances in Cryptology-CRYPTO 2007* (Springer) pp 360–378
[10] Berta M, Christandl M, Colbeck R, Renes J M and Renner R 2010 *Nature Physics*
[11] Dukkipati A, Murty M N and Bhatnagar S 2006 *Physica A: Statistical Mechanics and its Applications* **361** 124–138

[12] Havrda J and Charvát F 1967 *Kybernetika* **3** 0–3
[13] Daróczy Z 1970 *Information and control* **16** 36–51
[14] Heisenberg W 1927 *Zeitschrift für Physik A Hadrons and Nuclei* **43** 172–198
[15] Robertson H P 1929 *Phys. Rev.* **34**(1) 163–164 URL `http://link.aps.org/doi/10.1103/PhysRev.34.163`
[16] Deutsch D 1983 *Phys. Rev. Lett.* **50**(9) 631–633 URL `http://link.aps.org/doi/10.1103/PhysRevLett.50.631`
[17] Kraus K 1987 *Phys. Rev. D* **35**(10) 3070–3075 URL `http://link.aps.org/doi/10.1103/PhysRevD.35.3070`
[18] 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`
[19] Prevedel R, Hamel D R, Colbeck R, Fisher K and Resch K J 2011 *Nature Physics* **7** 757–761
[20] Hardy G, Littlewood J and Pólya G 1934 *Inequalities* (Cambridge University Press, London and New York)
[21] Devetak I and Winter A 2005 *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science* **461** 207–235
[22] Shor P W and Preskill J 2000 *Physical Review Letters* **85** 441–444

## 4. Appendix

In this section we give some useful definitions of the properties of the Tsallis entropy for the evaluation of Equations (19) and (20). The conditional Tsallis entropy of the conditional probability distribution for random variables $A$ and $B$ is defined as

$$\begin{aligned} S_\alpha(A|B_j) &= \frac{1}{1-\alpha}\left[\sum_i (p_{ij}(A|B))^\alpha - 1\right] \\ &= \frac{1}{1-\alpha}\left[\frac{\sum_i (p_{ij}(A,B))^\alpha}{(p_j(B))^\alpha} - 1\right], \end{aligned} \tag{21}$$

which is a generalization of the conditional Shannon entropy and is expressed as

$$H(A|B_j) = -\sum_i p_{ij}(A|B)\ln p_{ij}(A|B), \tag{22}$$

where $p_j(B)$ and $p_{ij}(A,B)$ are the marginal and joint probabilities respectively.