. **ORIGINAL RESEARCH ARTICLE**

OBVIOUS DISPARITIES ON OPTIMAL GUESSWORK WIRETAPPER MOMENTS UNDER MISMATCH RELATED TO NON-SHANNON CYPHER SYSTEM

Abstract

The invention of several significant non-Shannon entropy inequalities, the optimal Gaussing theorems, the relationship between the discrete memoryless source pair and the probability mass function, and these topics are all covered in the current communication. It may directly or indirectly prove to be significant for the literature of information theory.

Key words: Optimal guessing function, Shannon Entropy, Predictability, Source pair, Random variable, Inequality

1 INTRODUCTION:

Think about the challenge of predicting the value that a discrete random variable, X, assumed in one trial of a random experiment by asking questions of the pattern **"Did X take on its i^{th} possible value?"** until the response is "yes" In the context of sequential decoding [1] and source-channel coding [2, 3, 7], as well as in security applications [4, 5, 6, 7], the guessing problem has been studied. In the final subsection, we give a summary of earlier work. In 2023, Verma [13, 14, 15, 16] presented the properties of his own generated entropy. Although we do not go into greater detail here, it is also possible to define guessing in the presence of distortion or source uncertainty [2, 7, 8].

This issue can occur, for example, when a cryptanalyst must test each potential secret key one at a time after cryptanalyzing the possibilities. Let G represent the total number of guesses made when using the guessing method that minimizes $E(G)$, which is obviously to guess the potential values of X in decreasing order of likelihood. We can assume that these are the first, second, third, etc., conceivable values of X without losing the crucial generality, in which case the probability distribution for X, say $P = p_1, p_2, \ldots$ satisfies $p_1 \geq p_2 \geq \cdots$ and we will refer to such a P as a monotone distribution. With this approach, $E(G) = \sum ip_i$, where the summation is on i from 1 to infinity in this sum and all subsequent sums.

1.1 Definitions and Notation

In this part, we present a few definitions. A method of producing successive questions of the aforementioned kind until a YES response is given is a guessing approach for identifying X. A function $G: X \to \{1, 2, \dots\}$where $G(k)$ equals the time index of the query can be used to express any such method informally. Is $X = k$?.

Keep in mind that legitimate guessing methods' related functions G cannot be completely random. Since only one element can be probed at once, it is obvious that G must be invertible on its range of $\{1, 2, \dots\}$. Additionally, since we presume that the responses to the questions " Is X equal to k?" are noiseless, it is sufficient to take into account guessing tactics that ask the aforementioned query precisely once for each value of $k \geq 1$. Formally, this is equivalent to the mapping G being one-to-one and onto. Any function that meets these two requirements is referred to as a guessing function. A legitimate guessing strategy [11, 12] is defined by every guessing function and vice versa.

The guesser is interested in reducing the number of questions needed to identify X, assuming that she is aware of the probability distribution P (otherwise, see [8]). There are various approaches to formalize this objective, such as minimizing a positive moment $E(G^{\rho})$ (most commonly, $\rho = 1$ is of relevance), where

$$E(G^{\rho}) = \sum_{x \in X} P(x) G(x)^{\rho} = \sum_{k \geq 1} k^{\rho} \, P\left(G^{-1}(k)\right).$$

The Renyi entropy of order α of X is a generalization of the Shannon entropy [10] defined by

$$H_{\alpha}(X) = \frac{\log\left(\sum_{X \in y} P(X)^{\alpha}\right)}{1-\alpha} \qquad \forall\, \alpha \in [0, 1) \cup (1, \infty)$$

and obeys $\lim_{\alpha \to 1} H_{\alpha}(X) = H(X)$ as well as being strictly decreasing in α unless the $Y \in y$ is uniform on its support. Sometimes, related random variable $Y \in y$ with some joint distribution $P(X, Y)$ is available to the guesser, who then proceeds to guess the possible value of X as above. In this case,

$$E[G(X|Y)] = \sum_{Y \in y} P(Y) E[G(X|Y = y)].$$

With X taking values in a finite set J of size M and Y taking values in a countable set K, let (X, Y) be a pair of random variables. If $G: J \to (1, 2, \dots, M)$ is one-to-one, we can refer to a function $G(X)$ of the random variable X as a guessing function for X. If, for any fixed number $Y = y$, a function $G(X|Y)$ is a guessing function for X, then we refer to that function as a guessing function for X given Y. When the value of Y is known, $G(X|Y)$ will be interpreted as the number of guesses necessary to determine X. The moments of $G(X)$ and $G(X|Y)$ are inequalities according to the following.

2. OUR CLAIMS

Claim 2.1 For any **OGF** (optimal guessing function) $G_P\left(\frac{X}{Y}\right)$ and $\tau \geq 0$. Show that the inequality $\frac{1}{2}(\tau+1)\ln\left[G\left(\frac{x}{y}\right)G_P\left(\frac{X}{Y}\right)^{\tau}\right]^2 \leq 2(\tau+1)\ln\sum_{y\in Y}P(y) + 2\ln\sum_{x\in X}P\left(\frac{x}{y}\right) + 2K$, where, K is defined by $\tau\ln\sum_{a\in X}P(a/y)$.

Proof: Since the inequality for **OGF** $G_P\left(\frac{X}{Y}\right)$, we have

$$G_P\left(\frac{X}{Y}\right) \leq \sum_{a\in X}\left[\frac{P(a/y)}{P(x/y)}\right]^{\frac{1}{\tau+1}}$$

For the completion of the proof, since

$$\ln E\left[G_P\left(\frac{X}{Y}\right)^{\tau}\right] \leq \ln\left[\sum_{y\in Y}P(y)\sum_{x\in X}P\left(\frac{x}{y}\right)G_P\left(\frac{X}{Y}\right)^{\tau}\right]$$

$$i.e. \qquad \ln E^2\left[G_P\left(\frac{X}{Y}\right)^{\tau}\right] \leq \ln\left[\sum_{y\in Y}P(y)^2\sum_{x\in X}P\left(\frac{x}{y}\right)^2 G_P\left(\frac{X}{Y}\right)^{2\tau}\right]$$

Now, from above discussed equations, we achieve the following result

$$\ln E^2\left[G_P\left(\frac{X}{Y}\right)^{\tau}\right] \leq \ln\sum_{y\in Y}P(y)^2 + \ln\sum_{x\in X}P\left(\frac{x}{y}\right)^2 + \ln\sum_{a\in X}\left[\frac{P(a/y)}{P(x/y)}\right]^{\frac{2\tau}{\tau+1}}$$

$$\leq \ln\sum_{y\in Y}P(y)^2 + \ln\sum_{x\in X}P\left(\frac{x}{y}\right)^{\frac{2}{\tau+1}} + \ln\sum_{a\in X}P(a/y)^{\frac{2\tau}{\tau+1}}$$

$$\leq 2\ln\sum_{y\in Y}P(y) + \frac{2}{\tau+1}\ln\sum_{x\in X}P\left(\frac{x}{y}\right) + \frac{2\tau}{\tau+1}\ln\sum_{a\in X}P(a/y)$$

$$\frac{1}{2}(\tau+1)\ln\left[G\left(\frac{x}{y}\right)G_P\left(\frac{X}{Y}\right)^{\tau}\right]^2 \leq 2(\tau+1)\ln\sum_{y\in Y}P(y) + 2\ln\sum_{x\in X}P\left(\frac{x}{y}\right) + 2\tau\ln\sum_{a\in X}P(a/y)$$

$$i.e.\ \frac{1}{2}(\tau+1)\ln\left[G\left(\frac{x}{y}\right)G_P\left(\frac{X}{Y}\right)^{\tau}\right]^2 \leq 2(\tau+1)\ln\sum_{y\in Y}P(y) + 2\ln\sum_{x\in X}P\left(\frac{x}{y}\right) + 2K$$

Hence, the inequality.

Claim 2.2 For any **OGF** (optimal guessing function) $G_P\left(\frac{X}{Y}\right)$ and $\tau \geq 0$. Show that the inequality $\ln E\left[G_P\left(\frac{X}{Y}\right)^{-\epsilon}\right] \leq \ln\sum_{y\in Y}P(y) + \frac{1}{-\epsilon+1}\ln\sum_{x\in X}P\left(\frac{x}{y}\right) - R_\epsilon(P)$, where $\beta = \frac{1}{2^{1-\alpha}-1}$.

Proof: Since for any **OGF** $G_P\left(\frac{X}{Y}\right)$, we have

$$G_P\left(\frac{X}{Y}\right) \leq \sum_{a\in X}\left[\frac{P(a/y)}{P(x/y)}\right]^{\frac{1}{\tau+1}}$$

We achieve the result as follows

$$\ln E\left[G_P\left(\frac{X}{Y}\right)^{\tau}\right] = \ln\left[\sum_{y\in Y} P(y)\sum_{x\in X} P\left(\frac{x}{y}\right) G_P\left(\frac{X}{Y}\right)^{\tau}\right]$$

Now, from the above discussed equations, we achieve the following result

$$\ln E\left[G_P\left(\frac{X}{Y}\right)^{\tau}\right] \leq \ln\left[\sum_{y\in Y} P(y)\sum_{x\in X} P\left(\frac{x}{y}\right)\left[\sum_{a\in X}\left[\frac{P(a/y)}{P(x/y)}\right]^{\frac{1}{\tau+1}}\right]^{\tau}\right]$$

$$\leq \ln\sum_{y\in Y} P(y) + \ln\sum_{x\in X} P\left(\frac{x}{y}\right)^{\frac{1}{\tau+1}} + \ln\left[\sum_{a\in X}\left[\frac{P(a/y)}{P(x/y)}\right]^{\frac{1}{\tau+1}}\right]^{\tau}$$

$$\leq \ln\sum_{y\in Y} P(y) + \frac{1}{\tau+1}\ln\sum_{x\in X} P\left(\frac{x}{y}\right) + \frac{1}{\tau+1}\ln\sum_{x\in X} P\left(\frac{a}{y}\right)^{\tau}$$

$$\leq \ln\sum_{y\in Y} P(y) + \frac{1}{\tau+1}\ln\sum_{x\in X} P\left(\frac{x}{y}\right) + \frac{1}{\tau+1}\ln\sum_{x\in X} P\left(\frac{a}{y}\right)^{\tau}$$

On replacing τ by $-\epsilon$, we have

$$\leq \ln\sum_{y\in Y} P(y) + \frac{1}{-\epsilon+1}\ln\sum_{x\in X} P\left(\frac{x}{y}\right) + \frac{1}{-\epsilon+1}\ln\sum_{x\in X} P\left(\frac{a}{y}\right)^{-\epsilon}$$

$i.e.$ $$\ln E\left[G_P\left(\frac{X}{Y}\right)^{-\epsilon}\right] \leq \ln\sum_{y\in Y} P(y) + \frac{1}{-\epsilon+1}\ln\sum_{x\in X} P\left(\frac{x}{y}\right) - R_{\epsilon}(P)$$

Hence, the inequality.

Claim 2.3 Let $\tau > 0$. Consider a source pair (X, Y) with PMF P. If $\nu = \frac{1}{1+\tau}$. then $\frac{H^{\alpha}(P)}{(1+\ln X)^{\tau}}$ is less than or equal to

$$\frac{1}{2^{1-\nu}-1}\sum_{x\in X}\sum_{y\in Y}\left[P(x,y)\left(\sum_{a\in X} P(a,y)^{\frac{1}{1+\tau}}\right)^{\tau} - \sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}\right]\left[\sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}\right]^{-1}$$

and in particular, $\nu = \frac{1}{2}$ then, $\frac{H^{\alpha}(P)}{(1+\ln X)^{\tau}}$ is less than or equal to

$$\frac{1}{\sqrt{2}-1}\cdot\sum_{x\in X}\sum_{y\in Y}\left[P(x,y)\left(\sum_{a\in X} P(a,y)^{\frac{1}{1+\tau}}\right)^{\tau} - \sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}\right]\left[\sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}\right]^{-1}.$$

Proof: The inequality for **OGF** is

$$\frac{H^{\nu}(P)}{\lambda} + 1 \geq E(G_P(X,Y)^{\tau})$$

and

$$H^{\nu}(P) \geq \frac{H^{\nu}(P)}{(1+\ln X)^{\tau}}$$

So, $\frac{H^{\nu}(P)}{(1+\ln X)^{\rho}} = \lambda[E(G_P(X,Y)^{\tau}) - 1]$

$= \lambda\left[\sum_{y\in Y}\sum_{x\in X} p(x,y)G_P(x,y)^{\tau} - 1\right]$

For $\tau > 0$ and each $y \in Y$

$$\sum_{a\in X}\left(\frac{P(a,y)}{P(x,y)}\right)^{\frac{1}{1+\tau}} \geq G_P(x,y)$$

Now, $\lambda\left[\sum_{y\in Y}\sum_{x\in X} P(x,y)G_P(x,y)^{\tau} - 1\right]$

$$\leq \lambda\left[\sum_{y\in Y}\sum_{x\in X} P(x,y)\left(\sum_{a\in X}\left(\frac{P(a,y)}{P(x,y)}\right)^{\frac{1}{1+\tau}}\right)^{\tau} - 1\right]$$

$$\leq \lambda\left[\sum_{y\in Y}\sum_{x\in X} \frac{P(x,y)\left(\sum_{a\in X} P(a,y)^{\frac{1}{1+\tau}}\right)^{\tau} - \sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}}{\sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}}\right]$$

$$\leq \lambda\sum_{x\in X}\sum_{y\in Y}\left[P(x,y)\left(\sum_{a\in X} P(a,y)^{\frac{1}{1+\tau}}\right)^{\tau} - \sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}\right]\left[\sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}\right]^{-1}$$

Setting, $\lambda = \frac{1}{2^{1-\nu}-1}$. Hence, $\frac{H^{\nu}(P)}{(1+\ln X)^{\tau}}$ is less than or equal to

$$\frac{1}{2^{1-\nu}-1}\sum_{x\in X}\sum_{y\in Y}\left[P(x,y)\left(\sum_{a\in X} P(a,y)^{\frac{1}{1+\tau}}\right)^{\tau} - \sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}\right]\left[\sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}\right]^{-1}$$

and in particular, $\nu = \frac{1}{2}$ then, $\frac{H^{\frac{1}{2}}(P)}{(1+\ln X)^{\tau}} \leq$

$$\frac{1}{\sqrt{2}-1}.\sum_{x\in X}\sum_{y\in Y}\left[P(x,y)\left(\sum_{a\in X} P(a,y)^{\frac{1}{1+\tau}}\right)^{\tau} - \sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}\right]\left[\sum_{x\in X}\left(P(x,y)^{\frac{1}{1+\tau}}\right)^{\tau}\right]^{-1}.$$

Hence, the required inequality.

CONCLUSION

We developed an entirely novel and explicit accurate characterisation of the expected number of guesses for a single attacker in the unrestricted attacker case in terms of Renyi entropy. Another new result obtained in the paper is Claim 2.3, an interesting derivation of the union bound which is widely used in information theory, in terms of the expected number of guesses in a conditional guessing scheme which takes the output of a communication channel as its input.

REFERENCES

1. Arikan, E. (1996): An Inequality on Guessing and Its Application to Sequential Decoding, IEEE Transactions on Information Theory, 42(1) 99-105.

2. Arikan, E. and Merhav, N. (1998): Guessing subject to distortion, IEEE Transactions on Information Theory, 44(3):1041-1056.

3. Arikan, E. and Merhav, N. (1998): Joint Source-channel Coding and Guessing with Application to Sequential Decoding, IEEE Transactions on Information Theory, 44(5):1756-1769.

4. Dragomir, S. S. and Boztas, S. (1997): Some Estimates of the Average Number of Guesses to Determine a Random Variable, Proc. IEEE International Symposium on Information Theory.

5. Dragomir, S. S. and Boztas, S. (1998): Estimation of Arithmetic Means and Their Applications in Guessing Theory, Mathematical and Computer Modelling, 28(10):31-43.

6. Merhav, N. and Arikan, E. (1999): The Shannon Cipher System with a Guessing Wiretapper, it IEEE Transactions on Information Theory, 45(6):1860-1866.

7. Merhav, N., Roth, R. M., Arikan, E. (1999): Hierarchical guessing with a fidelity criterion, IEEE Transactions Information Theory, 45(1):330-337.

8. Pliam, J. O. (2000): On the incomparability of Entropy and Marginal Guesswork in Brute-force Attacks, Proc. INDOCRYPT 2000, Lecture Notes in Computer Science 1977:67–79.

9. Sundaresan, R. (2007): Guessing Under Source Uncertainty, IEEE Transactions on Information Theory 53(1): 269 - 287, 2007.

10. Shannon, C.E. (1948): A mathematical theory of communication, Bell. System Tech. J., 27 (1948), 379-423, 623-659.

11. Verma, R. K. (2023): "On Some Fated Class of Inconsistency Analogous to p-Valent Subclasses" Asian Journal of Mathematical Sciences (AJMS), 2023, Volume 19, Issue 6, Page 1-7, (ISSN: 2456-477X), DOI: 10.9734/AJMS/2023/v19i6661.

12. Verma, R. K. (2023): On Optimal Channel Capacity Theorems via Verma Information Measure with Two-Sided Input in Noisy State, Asian Journal of Probability and Statistics (AJPAS), 2023, Volume 22, Issue 2, Page 1-7, DOI:10.9734/AJPAS/2023/v22i2478.

13. Verma, R. K. (2023): On Optimality of Entropy Like Functional in Terms of Distance Function, as a book Chapter-2 in Research Highlights in Mathematics and Computer Science (RHMCS), Vol. 7, pp. 10-20, DOI: 10.9734/bpi/rhmcs/v7/18679D.

14. Verma, R. K. (2023): On Optimization Policy for Verma Entropy by Dynamic Programming, Asian Journal of Probability and Statistics (AJPAS), Vol. 21 (4), pp. 14-21, DOI: 10.9734/AJPAS/2023/v21i4469.

15. Verma, R. K. (2023): Some New Series of Inequalities Premised on Verma Measures of Information, Asian Journal of Probability and Statistics (AJPAS), Vol. 22 (1), pp. 56-63, DOI: 10.9734/AJPAS/2023/v22i1477.

16. Verma, R. K. (2023): Optimal Code Word Length Via Modified Verma Information Measures for Discrete Noiseless Channel in Intuitionistic Fuzzy Environment, International Journal of Fuzzy Mathematics and Systems (IJFMS), Vol. 13(1), pp. 11-20.

Biography of author

Dr. Rohit Kumar Verma,
Associate Professor &
HOD, Department of
Mathematics,
Bharti Vishwavidyalaya, Durg, C.G., India.

He is a well known author in the field of the journal scope. He obtained his highest degree from RSU, Raipur (C.G.) and worked in engineering institution for over a decade. Currently he is working in a capacity of Associate Professor and HOD, Department of Mathematics, Bharti Vishwavidyalaya, Durg (C.G.). In addition to 35 original research publications in the best journals, he also published two research book by LAP in 2013 and 2023 in the areas of information theory and channel capacity that fascinate him. He is the Chairperson, the Board of Studies Department of Mathematics at Bharti Vishwavidyalaya in Durg, C.G., India. He has published two patents in a variety of fields of research. In addition to numerous other international journals, he reviews for the American Journal of Applied Mathematics (AJAM). In addition to the Indian Mathematical Society (IMS), he is a member of the Indian Society for Technical Education (ISTE).