IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Guessing Under Source Differential Entropies

Dr.Rajesh Kumar Saini

Seth R. N. Ruia Govt. College

Ramgarh Shekhawati (Sikar)

Abstract :-

The special case of guessing n-string put out by a discrete memoryless source (DMS) with single letter alphabet A. The parameters of this DMS are unknown to the guesser. We review know result for the problem of guessing , introduce the guessing moment for the source with using Havrda and Charvat entropy of order α and this entropy indicates the exponent of the minimum guessing moment to within $(1+\ln X)$.

Keywords :-

Guessing moment , Havrda and Charvat entropy ,discrete memoryless source (DMS) , probability mass function (PMF), expected value.

1. Introduction:-

Let X be a random variable on a finite set X with probability mass function (PMF) given by { P(x) : x ∈ X }. Suppose that we wish to guess the realization of this random variable X by asking questions of the form "Is X equal to x ?" stepping through the element of X, until the answer is "Yes"(Massey[1994],Arikan[1996]) if we know the PMF P ,the best strategy is to guess in the decreasing order of P probabilities.

When P is known, Massey [1994] Arikan [1996] sought to lower bound the minimum expected number of guesses. For a given guessing strategy G, Let G(x) denote the number of guesses required when X=x. The strategy that minimum E[G(x)], the expected number of guesses , proceeds in the decreasing order of P-probabilities. Arikan [1996] showed that the exponent of the minimum value, i.e. $\log[\min_G E[G(X)]]$, satisfies

$$H_{\frac{1}{2}}(P)-\log(1+\ln X) \leq \log[\min_G E\{G(X)\}] \leq H_{\frac{1}{2}}(P)$$

Where $H_\alpha(P)$ is the Renyi order of entropy of order $\alpha>0$. Boztas[1997] obtains a tighter upper bound.

For $\rho>0$, Arikan [1996] also considered minimization of $[E\{G(X)^\rho\}]^{1/\rho}$ over all guessing strategies G; the exponent of minimum values satisfies

$$H_\alpha(P)-\log(1 + InX) \leq \frac{1}{\rho} log\ [min_G E\{G(X)^\rho\}] \leq H_\alpha(P)$$

$$Where\ \alpha = \frac{1}{1+\rho}$$

Arikan [1996] applied these results to a discrete memoryless source on X with letter probabilities given by the PMF P, and obtained that the minimum guessing moment , $\min_G E\{G(X^n)^\rho\}$, grows exponentially with n.Xt minimum growth rate of this quantity is given by the Renyi emtropy $H_\alpha(P)$.This gave an operational significance for the Renyi entropy. In particular the minimum expected number of guesses grows exponentially with n and has a minimum growth rate of $H_{1/2}(P)$. The study of $EG(X)^\rho$ as a function that characterizes the large deviations behaviour of number of guesses. Merhav and Arikan [1999] for more details.

2. Methods of Guuessing Source of Differential Entropy

Suppose now that the guesser only knows that the source belongs to a family t of PMFs. The uncertainity set may be finite or infinite in size. The guesser's strategy should not be turned to any one particular PMF in t, but should be designed for the entire uncertainty Set. Thus for any given strategy, and for any source P∈ t ,we can define a notion of penality or rebundancy R(P,G), given by

$$R(P,G) = \frac{1}{\rho}\log[E\{G(X)^\rho\}] - \frac{1}{\rho}\log[E\{G_P(X)^\rho\}]$$

Which represents the increase in the exponent of the guessing moment normalized by ρ.

Let X and Y be finite alphabet sets. Consider a correlated pair of random variables (X, Y) with joint PMF P on X>Y . Given side information Y=y, we should like to guess the realization of X. Formally a guessing list G with side information is a function G:X × Y →{1,2,…….X} such that for each y∈Y, the function G(y):X→{1,2,3…….X} is a one-to-one function that denotes the order in which the elements of X will be guessed when the guesser observes Y=y. Naturally , knowing the PMF P, the best strategy which minimizes the expected number of guesses given Y=y , is to guess in the decreasing order of P(y)-probabilities . Let us denote such an order G ρ, due to lack of exact knowledge of P, suppose we guess in the decrease order of probabilities of another PMG Q. This situation leads to mismatch. In this section, we analyse the performance of guessing strategies under mismatch.

In some of the results we will have ρ>0 and in others ρ>-1, ρ≠0. The ρ>0 case is of primary interest in the context of guessing. The order case is also of interest in Campbell's average exponential coding length problem where similar quantities are involved.

3. Main Results :-

Let a source on X<Y (Vinocha, O. P. and R. K. Saini [2007,2010]) the Harvarda and Charvada entropy of order α,with α>0, is given by

$$H^\alpha(P) = \beta\left[\sum_{y\in Y}\left[\sum_{y\in X} p(x,y)^\alpha\right]^{\frac{1}{\alpha}} - 1\right]$$

Where $\beta=\frac{1}{(2^{1-\alpha}-1)}$.

Theorem1: Let ρ>0. Consider a source pair (X,Y) with PMF P. Let Q be another PMF with Supp(Q) = X×Y. Let G_Q be the guessing list with side information Y obtained under the assumption that the PMF is Q,with ties broken using an arbitrary but fixed rule. Then the guessing moment for source with PMF P under G_Q satisfies

$$\left[E\left(G_Q(X,Y)^\rho\right) - 1\right]$$

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

where the expectation E is with respect to P and $\beta = \frac{1}{2^{1-\alpha}-1}$.

Proof: For ρ>0, for each y∈Y, observe that

$$G_Q(x.y) \leq \sum_{a\in X} 1\{Q(a,y) \geq Q(x,y)\} \leq \sum_{a\in X} \left(\frac{Q(a,y)}{Q(x,y)} \right)^{\frac{1}{\rho}}$$

……..(2.1)

We know

$$E\left[G_Q(X,Y)^{\rho}\right] - 1 = \sum_{y\in Y} \sum_{x\in X} p(x,y) G_Q(x,y)^{\rho} - 1$$

……. (2.2)

Put the value of equation (2.1)in equation (2.2)

$$E\left[G_Q(X,Y)^{\rho}\right] - 1 \leq \sum_{y\in Y} \sum_{x\in X} p(x,y) \left[\sum_{a\in X} \left(\frac{Q(a,y)}{Q(a,y)} \right)^{\frac{1}{1+\rho}} \right]^{\rho} - 1$$

Multiply both side by β where $\beta = \frac{1}{2^{1-\alpha}-1}$

$$\beta\left[E\left[G_Q(X,Y)^{\rho}\right] - 1\right] \leq \beta \left[\sum_{y\in Y} \sum_{x\in X} p(x,y) \left[\sum_{a\in X} \left(\frac{Q(a,y)}{Q(x,y)} \right)^{\frac{1}{1+\rho}} \right]^{\rho} - 1 \right]$$

Theorem 2: Let ρ>0. Consider a source pair(X,Y) with PMF P.Let Q be another PMF with sup(Q) = X×Y. Let G_Q be the guessing list with side information Y obtained under the assumption that the PMF is Q, with ties broken using an arbitrary but fixed rule. Then the guessing moment for the source with PMF P under G_p satisfies

$$\beta[E[G_P(X,Y)^{\rho}] - 1] \leq H^{\alpha}(P)$$

Proof: We know

$$\beta[E[G_P(X,Y)^{\rho}] - 1]$$

$$\leq \beta \left[\sum_{y\in Y} \sum_{x\in X} p(x,y)\, G_p(x,y)^{\rho} - 1 \right]$$

…….(2.3)

For ρ>0,for each y∈Y,observe that

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

……..(2.4)

Put the value of equation (2.4)in equation(2.3)

$$\beta[\mathrm{E}[G_P(X,Y)^\rho] - 1] \leq \beta\left[\sum_{y\in Y}\sum_{x\in X} p(x,y)\left[\sum_{a\in X}\left(\frac{P(a,y)}{P(x,y)}\right)^{\frac{1}{1+\rho}}\right]^\rho - 1\right]$$

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

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

$$\leq \beta\left[\sum_{y\in Y}\left[\sum_{x\in X} p(x,y)^{\frac{1}{1+\rho}}\right]^{\rho+1} - 1\right]$$

Put $\alpha=\frac{1}{1+\rho}$

$$\leq \beta\left[\sum_{y\in Y}[\sum_{x\in X} p(x,y)^{\alpha}]^{\frac{1}{\alpha}} - 1\right]$$

$\beta[E[G_P(X,Y)^\rho] - 1] \leq H^\alpha(P)$

where $\beta = \frac{1}{2^{1-\alpha}-1}$

Theorm3: Let ρ>0. Consider a source pair (X,Y) with PMF P. Let G be an arbitrary guessing list with side information Y. Then there is a PMF G_Q on X>Y with Supp(Q)=X×Y , and

$$\beta\left[\sum_{y\in Y}\sum_{x\in X} P(x,y)\left(\sum_{a\in X}\left(\frac{Q_G(a,y)}{Q_G(x,y)}\right)^{\frac{1}{1+\rho}}\right)^\rho\right]$$

$$\leq \beta\mathrm{E}[G(x,y)^\rho(1+lnX)^\rho]$$

Proof: ρ>0 for each y ϵ Y , we have

$$\sum_{x\in X}\left[\frac{1}{G(x,y)}\right]^{1+\rho} = \sum_{i=1}^{X}\frac{1}{i^{1+\rho}} = c < \infty$$

Define the PMF of Q_G as

$$Q_G(x,y) = \frac{1}{Y\ \mathrm{C}\ G(X,Y)^{1+\rho}}$$

Note that Supp(Q) = X × Y . Clearly guessing in the decreasing order of Q_G probabilities leads to the guessing order G.

We have

$$\beta\left[\sum_{y\in Y}\sum_{x\in X} P(x,y)\left(\sum_{a\in X}\left(\frac{Q_G(a,y)}{Q_G(x,y)}\right)^{\frac{1}{1+\rho}}\right)^\rho\right]$$

$$=\beta\left[\sum_{y\in Y}\sum_{x\in X} P(x,y)\left(\sum_{a\in X}\left(\frac{Y\ \mathrm{C}\ G(x,y)^{1+\rho}}{Y\ \mathrm{C}\ G(a,y)^{1+\rho}}\right)^{\frac{1}{1+\rho}}\right)^\rho\right]$$

$$=\beta\left[\sum_{y\in Y}\sum_{x\in X} P(x,y)G(x,y)^\rho\left(\sum_{a\in X}\frac{1}{G(a,y)}\right)^\rho\right]$$

Where the last inequality follows in Arikan[1996]

$$\sum_{a\in X}\frac{1}{G(a,y)}=\sum_{i=1}^{X}\frac{1}{i}\leq 1+lnX$$

$$\beta\left[\sum_{y\in Y}\sum_{x\in X}P(x,y)\left(\sum_{a\in X}\left(\frac{Q_G(a,y)}{Q_G(x,y)}\right)^{\frac{1}{1+\rho}}\right)^{\rho}\right]$$

$$\leq \beta E[G(x,y)^{\rho}(1+lnX)^{\rho}]$$

Theorm4: Let ρ>0. Consider a source pait(X,Y) with PMF P.

Let α = $\frac{\alpha}{1+\rho}$ Then

$$\frac{H_{\alpha}(P)}{(1+lnX)^{\rho}} \leq H^{\alpha}(P)$$

Proof: We have

$$\frac{H_{\alpha}(P)}{(1+lnX)^{\rho}}=\frac{\beta\left[\sum_{y\in Y}[\sum_{x\in X}p(x,y)^{\alpha}]^{\frac{1}{\alpha}}-1\right]}{(1+lnX)^{\rho}}$$

$$\leq\frac{\beta\left[\sum_{y\in Y}[\sum_{x\in X}p(x,y)^{\alpha}]^{\frac{1}{\alpha}}-1\right]}{\left(\sum_{a\in X}\frac{1}{G(a,y)}\right)^{\rho}}$$

$$\leq\beta\left[\sum_{y\in Y}[\sum_{x\in X}p(x,y)^{\alpha}]^{\frac{1}{\alpha}}-1\right]max\ G(x,y)^{\rho}$$

$$\leq\beta\left[\sum_{y\in Y}[\sum_{x\in X}p(x,y)^{\alpha}]^{\frac{1}{\alpha}}-1\right]$$

$$\leq H^{\alpha}(P)$$

4.Conclusion :-

The performance of such a guessing strategy on any particular source will not be better then the optimal strategy for that source. Indeed, for any source P the exponent of $[E\{G(X)^{\rho}\}]$ is at least as large as that of the optimal strategy $[E\{G_p(X)^{\rho}\}]$ where G_p is the guessing strategy matched to P that guesses in the decreasing order of P probabilities.

5. References : -

1. **Arikan, E. [1996]:** "An inequality on guessing and its application to sequential decoding," IEEE Trans. Inf. Theory, vol. 42, no. 1, pp. 99-105,Jan.
2. **Massey**,**J.L.[1994]:** "Guessing and entropy," in Proc. IEEE Int. Symp on Theory (Trondheim, Norway, 1994), p 204
3. **MerhavN. and E. Arikan[1999]:** "The Shannon cipher system with a pessing wiretapper," IEEE Trans. Inf. Theory, vol. 45, pp. 1860-1866, Sep.
4. **Vinocha, O. P. and R. K. Saini [2007] :** "Convergence of Haarvda and Charvat entropies."published in Ganita Sandesh vol. 21, No. 2, 2007,215-222 Rajasthan Ganita Parishad, ISSN 0970 – 9169.
5. **Vinocha, O. P. and R. K. Saini [2010] : "**A Renyi`s Entropy Power Inequality."Published in Pure and Applied Mathematika Sciences. Vol. LXXI, No. 1-2, March 2010, pp 107 – 113.