Entropy Power Inequality and Mrs. Gerber's Lemma for Abelian Groups of Order 2^n

Varun Jog, Venkat Anantharam
UC Berkeley

Introduction

• The Entropy Power Inequality (EPI) proposed by Shannon in 1948 [1] is an inequality in the so called "entropy power" of valued random variables. Entropy power of a random variable **X** is defined as

$$N(\mathbf{X}) = \frac{1}{2\pi e} e^{\frac{2}{n} h(\mathbf{X})}$$

The EPI states that for independent random variables **X** and **Y**,

$$N(\mathbf{X}) + N(\mathbf{Y}) \leq N(\mathbf{X} + \mathbf{Y})$$

and equality holds iff **X** and **Y** are Gaussian with proportional covariance matrices.

• The EPI has been generalized in a variety of ways. Notable generalizations include Costa's [2] concavity of entropy power and Zamir and Feder's [3] generalization to linear transformations of random variables.

• Several attempts have been made to obtain discrete versions of the EPI. Shamai and Wyner [4] used a result called Mrs. Gerber's Lemma (MGL) proved by Wyner and Ziv [5] to obtain a binary analog of EPI.

• We approach the discrete EPI problem in a different, straight-forward way and attempt to get a version of the EPI for finite abelian groups.

Our Interpretation

• Even though the EPI is thought of as an inequality in terms of "entropy power", it is essentially a sharp lower bound on *h*(**X**+**Y**) in terms of *h*(**X**) and *h*(**Y**). Thus, for any abelian group *G* with the binary operation +, we can examine the function

$$f_G(x, y) = \min_{H(X)=x, H(Y)=y} H(X+Y)$$

where X,Y are *G* valued random variables.

• For real valued random variables,

$$f_{\mathbb{R}}(x, y) = \frac{1}{2} \log \left(e^{2x} + e^{2y}\right)$$

• For $\mathbb{Z}_2$ we have

$$f_{\mathbb{Z}_2}(x, y) = H(H^{-1}(x) \star H^{-1}(y))$$

Key Observation

Wyner and Ziv's MGL can be stated in terms of

MGL: $f_{\mathbb{Z}_2}(x, y)$ *is convex in x for a fixed y, and vice versa.*

The above convexity property holds even for $f_{\mathbb{R}}$!

It is natural to make the conjecture:

Conjecture (Generalized MGL): *For a finite abelian group G, is convex in x for a fixed y, and vice versa.*

Proof Technique and Results

• We prove that $\frac{\partial f_{\mathbb{Z}_2}}{\partial x}$ decreases along lines through the origin

• Using this we prove that $f_{\mathbb{Z}_2}$ is concave along such lines, and also that the pair of partial derivatives $\left(\frac{\partial f_{\mathbb{Z}_2}}{\partial x}, \frac{\partial f_{\mathbb{Z}_2}}{\partial y}\right)$ uniquely determines a point (x, y).

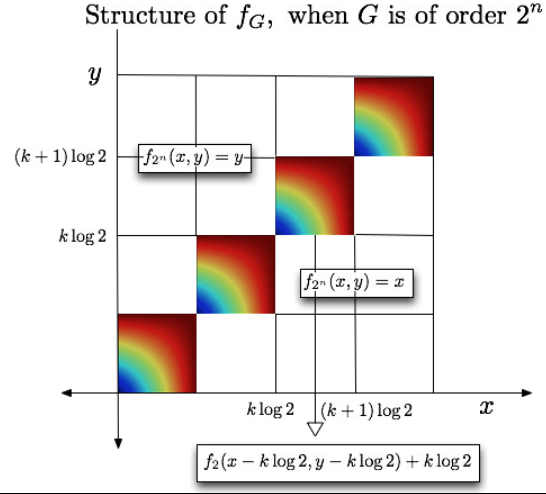
• We use the above lemmas and explicitly determine $f_{\mathbb{Z}_4}$. Using this as the base case for induction, we make a guess and prove the explicit form of $f_{\mathbb{Z}_{2^n}}$.

• It is then easily checked that the form of $f_{\mathbb{Z}_{2^n}}$ indeed does satisfy the conjecture.

• Now that we have the form of f_G for cyclic groups, we extend it to arbitrary groups of order 2^n by using the fundamental theorem of abelian groups and inducting over the number of cyclic groups being direct summed.

• We also describe those distributions where minimum entropy is attained for such groups, these can be thought of as analogs to Gaussians in the real case.

Structure of f_G, when G is of order 2^n



Acknowledgements

Research support from the ARO MURI grant W911NF-08-1-0233, "Tools for the Analysis and Design of Complex Multi-scale Network", from the NSF grant CNS-0910702, from the NSF Science & Technology Center grant CCF-0939370, "Science of Information", from Marvell Semiconductor Inc., and from the U.C. Discovery program is gratefully acknowledged.

References

1. C. Shannon, "A mathematical theory of communications, I and II," Bell Syst. Tech. J, vol. 27, pp. 379–423, 1948.
2. M. Costa, "A new entropy power inequality," Information Theory, IEEE Transactions on, vol. 31, no. 6, pp. 751–760, 1985.
3. R. Zamir and M. Feder, "A generalization of the entropy power inequality with applications," Information Theory, IEEE Transactions on, vol. 39, no. 5, pp. 1723–1728, 1993.
4. S. Shamai and A. Wyner, "A binary analog to the entropy-power inequality," Information Theory, IEEE Transactions on, vol. 36, no. 6, pp. 1428–1430, 1990.
5. A. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications– I," Information Theory, IEEE Transactions on, vol. 19, no. 6, pp. 769–772, 1973.