

The Entropy Power of a Sum is Fractionally Superadditive

Mokshay Madiman
Department of Statistics
Yale University
New Haven CT 06511, USA.
Email: mokshay.madiman@yale.edu

Farhad Ghassemi
Sauder School of Business
University of British Columbia
Vancouver BC, Canada V6T 1Z2.
Email: farhad@ece.ubc.ca

Abstract—It is shown that the entropy power of a sum of independent random vectors, seen as a set function, is fractionally superadditive. This resolves a conjecture of the first author and A. R. Barron, and implies in particular all previously known entropy power inequalities for independent random variables. It is also shown that, for general dimension, the entropy power of a sum of independent random vectors is not supermodular.

I. INTRODUCTION

For a \mathbb{R}^d -valued random vector X with density f with respect to the Lebesgue measure on \mathbb{R}^d , the differential entropy is

$$h(X) = - \int f(x) \log f(x) dx.$$

The entropy power of X is $\mathcal{N}(X) = e^{2h(X)/d}$. By a limiting argument, one may check that when X is supported on a strictly lower-dimensional set than \mathbb{R}^d (and hence does not have a density with respect to the d -dimensional Lebesgue measure), $h(X) = -\infty$. Throughout this note, we limit ourselves to random vectors X with $h(X) < +\infty$; in this case, $\mathcal{N}(X) \in \mathbb{R}_+ := [0, \infty)$ is a non-negative real number.

It is sometimes enough to consider a smaller collection of probability measures on \mathbb{R}^d . Consider any random vector X such that the variance of each of the d components is finite; clearly X has a well-defined, finite covariance matrix \mathbf{K}_X . For a given covariance matrix, it is well known that the maximum entropy distribution is the normal with that covariance matrix. Thus

$$h(X) \leq h(N(0, \mathbf{K}_X)) = \frac{1}{2} \log[(2\pi e)^d \det(\mathbf{K}_X)] < +\infty.$$

Thus looking at the class of component-wise finite variance random vectors is sufficient to ensure that $\mathcal{N}(X) \in \mathbb{R}_+$.

There are two main motivations for considering entropy power inequalities: the first comes from the fact that it is related to probabilistic isoperimetric phenomena including the entropic central limit theorem (see, e.g., Barron [1]), and the second comes from the fact that it can be extremely useful in the study of rate and capacity regions in multi-user information theory (see, e.g., Shannon [2], Bergmans [3], Ozarow [4], Costa [5] and Oohama [6]).

Let X_1, X_2, \dots, X_n be independent random vectors. We write $[n]$ for the index set $\{1, 2, \dots, n\}$. Define the subset

sums

$$Y_s = \sum_{i \in s} X_i.$$

One is interested in the entropy powers $\mathcal{N}(Y_s)$ of the subset sums. Specifically, we are interested in the following subset of \mathbb{R}^{2^n} :

$$\begin{aligned} \Gamma(n) = \{ & [\mathcal{N}(Y_s)]_{s \subset [n]} : X_1, X_2, \dots, X_n \\ & \text{are independent } \mathbb{R}^d\text{-valued random vectors} \} \\ = \{ & [\nu(s)]_{s \subset [n]} : X_1, X_2, \dots, X_n \\ & \text{are independent } \mathbb{R}^d\text{-valued random vectors} \}, \end{aligned} \quad (1)$$

where the set function $\nu : 2^{[n]} \rightarrow \mathbb{R}_+$ is defined for any given collection of independent \mathbb{R}^d -valued random vectors by

$$\nu(s) = \mathcal{N}\left(\sum_{i \in s} X_i\right). \quad (2)$$

We call the region $\Gamma(n)$ the d -dimensional *Stam region* in honor of Stam's pioneering role [7] in the study of entropy power and its applications.

Any inequality that relates entropy powers of different subset sums (usually called an “entropy power inequality” or EPI) gives a bound on the Stam region. Conversely, knowing the Stam region means knowing exactly all EPI's that hold and all that do not.

The objective of this note is to give inner and outer bounds on the Stam region. In particular, we show that for general dimension d , the entropy power is fractionally superadditive but not supermodular.

First, let us describe progress on a conjecture of Madiman and Barron relating to an outer bound for the Stam region. Specifically, the following conjecture, which was stated implicitly by Madiman and Barron [8] and explicitly in [9], is proved here.

Theorem 1. [FRACTIONAL SUPERADDITIVITY OF ENTROPY POWER] *Let X_1, \dots, X_n be independent \mathbb{R}^d -valued random vectors with densities and finite covariance matrices. Then the set function $\nu : 2^{[n]} \rightarrow [0, \infty)$ defined by (2) is fractionally superadditive, i.e., for any fractional partition β using a*

collection \mathcal{C} of subsets of $[n]$,

$$\mathcal{N}(X_1 + \dots + X_n) \geq \sum_{s \in \mathcal{C}} \beta_s \mathcal{N}\left(\sum_{j \in s} X_j\right).$$

The first author also asked in [9] whether in fact the entropy power is supermodular (which is known to be a stronger property than fractional superadditivity). Our second result is to show that the answer to this question is no.

Theorem 2. *Let X_1, \dots, X_n be independent \mathbb{R}^d -valued random vectors with densities and finite covariance matrices. The set function $\nu : 2^{[n]} \rightarrow [0, \infty)$ defined by (2) is not supermodular for general d , i.e., it is not true that*

$$\nu(s \cup t) + \nu(s \cap t) \geq \nu(s) + \nu(t)$$

for all sets $s, t \subset [n]$.

In other words, to use the language of cooperative game theory (see, e.g., [9]), the Stam region is a subset of the region representing all balanced transferable-utility cooperative games, and a superset of the region representing all convex transferable-utility cooperative games.

This note is organized as follows. In Section II, we prove Theorem 1 and hence an outer bound to the Stam region. Section III proves Theorem 2 and hence an inner bound. Section IV contains some discussion.

II. COMBINATORIAL ENTROPY POWER INEQUALITIES

The classical entropy power inequality (EPI) of Shannon [2] and Stam [7] states

$$\mathcal{N}(X_1 + \dots + X_n) \geq \sum_{j=1}^n \mathcal{N}(X_j). \quad (3)$$

Recently, Artstein, Ball, Barthe and Naor [10] proved a new EPI

$$\mathcal{N}(X_1 + \dots + X_n) \geq \frac{1}{n-1} \sum_{i=1}^n \mathcal{N}\left(\sum_{j \neq i} X_j\right), \quad (4)$$

where each term involves the entropy of the sum of $n-1$ of the variables excluding the i -th. Madiman and Barron [11] and Tulino and Verdú [12] independently gave simplified proofs of this inequality. Note that the original development of (4) was motivated by the study of monotonicity properties in central limit theorems—Artstein et al. [10] resolved the long-standing monotonicity conjecture for i.i.d. summands. In [8], Madiman and Barron showed the following generalized EPI for an arbitrary collection \mathcal{C} of (possibly repeated) subsets of the index set, namely $[n] = \{1, \dots, n\}$. If r is the maximum number of subsets in \mathcal{C} in which any one index i can appear, for $i = 1, \dots, n$, then

$$\mathcal{N}(X_1 + \dots + X_n) \geq \frac{1}{r} \sum_{s \in \mathcal{C}} \mathcal{N}\left(\sum_{j \in s} X_j\right). \quad (5)$$

For example, if \mathcal{C} consists of subsets s whose elements are m consecutive indices in $[n]$, then $r = m$. On the other hand,

if $\mathcal{C} = \mathcal{C}_m$, namely the collection of all subsets of indices of size m , then $r = \binom{n-1}{m-1}$. Thus (5) extends (4) and (3).

In this paper, we prove Theorem 1, which subsumes and extends the inequalities discussed above. Recall that given \mathcal{C} , a function $\beta : \mathcal{C} \rightarrow \mathbb{R}^+$ is a *fractional partition*, if for each $i \in [n]$, we have $\sum_{s \in \mathcal{C}: i \in s} \beta_s = 1$. If there exists a fractional partition β for \mathcal{C} that is $\{0, 1\}$ -valued, then β is the indicator function for a partition of the set $[n]$ using a subset of \mathcal{C} ; hence the terminology.

The proof of Theorem 1 follows from the following proposition, combined with inequality (5).

Proposition 1. [A SUFFICIENT CONDITION FOR FRACTIONAL SUPERADDITIVITY] *Consider a set function $v : 2^{[n]} \rightarrow \mathbb{R}_+$. Let \mathcal{C} be a r -regular multihypergraph on $[n]$, i.e., let \mathcal{C} be a collection of subsets of $[n]$ (possibly repeated), such that every index i lies in exactly r of the elements of \mathcal{C} . Suppose v satisfies, for any $r \in \mathbb{N}$,*

$$v([n]) \geq \frac{1}{r} \sum_{s \in \mathcal{C}} v(s)$$

where \mathcal{C} is any r -regular multihypergraph on $[n]$. Then,

$$v([n]) \geq \sum_{s \in \mathcal{C}} \beta_s v(s) \quad (6)$$

holds for every fractional partition β using any multihypergraph \mathcal{C} on $[n]$.

Proof: Consider the space of all fractional partitions on $[n]$, i.e.,

$$\mathcal{B} = \left\{ \beta : 2^{[n]} \setminus \phi \rightarrow \mathbb{R}_+ \mid \sum_{s \subset [n] \setminus \phi} \beta_s \mathbf{1}_s = \mathbf{1}_{[n]} \right\}.$$

Clearly, \mathcal{B} can be viewed as a subset of the Euclidean space of dimension $2^n - 1$ (since each point of it is defined by $2^n - 1$ real numbers). Furthermore, $\mathcal{B} = \mathcal{B}' \cap \mathcal{O}_+$, where

$$\mathcal{B}' = \left\{ \beta : 2^{[n]} \setminus \phi \rightarrow \mathbb{R} \mid \sum_{s \subset [n] \setminus \phi} \beta_s \mathbf{1}_s = \mathbf{1}_{[n]} \right\}$$

is an affine subspace of dimension $2^n - 1 - n$ and $\mathcal{O}_+ = \{\beta \mid \beta_s \geq 0 \forall s \in 2^{[n]} \setminus \phi\}$ is the closed positive orthant. In particular, \mathcal{B} is a non-empty, compact, convex set (in fact, a closed polytope), so that by the Krein-Milman theorem, \mathcal{B} is the convex hull of its extreme points. Thus to prove (6) for every $\beta \in \mathcal{B}$, it is sufficient to prove (6) for every $\beta \in \text{Ex}(\mathcal{B})$, where $\text{Ex}(\mathcal{B})$ denotes the set of extreme points of \mathcal{B} .

Now we follow an argument sketched by Gill and Grünwald [13] to characterize the set $\text{Ex}(\mathcal{B})$; a similar observation seems to be implicit in Friedgut and Kahn [14], and has perhaps been made even before, although we were unable to find early references. Every face of the polytope \mathcal{B} corresponds to one of the inequality constraints being tight (i.e., $\beta_s = 0$ for some set s). Now each extreme point or vertex β of the polytope \mathcal{B} is the *unique meeting point of several faces*. Let these faces correspond to setting $\beta_s = 0$ for s lying in the collection of sets \mathcal{C}' . The complement \mathcal{C} of \mathcal{C}' is called the support of the

fractional partition β . The set of fractional partitions supported by \mathcal{C} has non-zero coefficients $\beta_{\mathcal{C}} = \{\beta_s : s \in \mathcal{C}\}$ given by the solutions to the linear equation

$$M\beta_{\mathcal{C}} = \mathbf{1}, \quad (7)$$

where M is the $n \times |\mathcal{C}|$ 0-1 matrix defined by $M_{i,s} = \mathbf{1}_{i \in s}$ for $i \in [n]$, $s \in \mathcal{C}$, and $\mathbf{1}$ is the column vector in \mathbb{R}^n consisting of all ones. Since β is the unique such fractional partition, it corresponds to (7) having a unique, strictly positive solution. Consequently one must have $\beta_{\mathcal{C}} = M^+ \mathbf{1}$, where M^+ is the Moore-Penrose pseudoinverse of M . Recall that since M has rational entries, so does M^+ , and hence β is rational-valued.

By writing all the coefficients of β with a common denominator, one sees that (6) may be written as

$$v_n([n]) \geq \frac{1}{R} \sum_{s \in \mathcal{C}} c_s v_n(s),$$

where c_s is a positive integer. One may write this as

$$v_n([n]) \geq \frac{1}{R} \sum_{s \in \mathcal{C}''} v_n(s),$$

where \mathcal{C}'' is the multihypergraph with c_s copies of the set s . Note that \mathcal{C}'' is clearly R -regular. ■

Remark 1. Theorem 1 is a considerably more informative statement than its predecessors such as (5), as pointed out in [9]. Recall that entropy power inequalities have been key to the determination of some capacity and rate regions, and that rate regions for several multi-user problems (such as the m -user Slepian-Wolf problem) involve subset sum constraints. Vaguely motivated by this, one may consider the “rate” region of all $(R_1, \dots, R_n) \in \mathbb{R}_+^n$ satisfying $\sum_{j \in s} R_j \geq \mathcal{N}(T^s)$ for each $s \subset [n]$. Then Theorem 1 is equivalent to the existence of a point in this region such that the total sum $\sum_{j \in [n]} R_j = \mathcal{N}(T^{[n]})$. Although we are not yet aware of a specific multiuser capacity problem with precisely this rate region, this fact appears intriguing.

III. ENTROPY POWER IS NOT SUPERMODULAR

Observe that if the function ν defined in (2) were supermodular, then specializing to multivariate Gaussians would imply a similar supermodularity for the d -th root of the determinant of sums of positive definite matrices. To be precise, consider the set function

$$\nu_G(s) = \det\left(\sum_{k \in s} \mathbf{S}_k\right)^{\frac{1}{d}}, \quad s \subset [n],$$

where $\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_n$ are $d \times d$ positive definite matrices. (Here we use ν_G to indicate that this is the function ν specialized to Gaussians.)

One may simply prove that ν_G is not supermodular by constructing numerical counterexamples. However we attempt to give some additional insight into why supermodularity fails by the following reasoning. To prove that ν_G is not supermodular, we first show that its continuous analogue is

not supermodular (in the continuous sense). In other words, let $v : \mathbb{R}_+^n \rightarrow \mathbb{R}_+$ be defined by

$$v(\mathbf{x}) = \det\left(\sum_{k \in [n]} x_k \mathbf{S}_k\right)^{\frac{1}{d}},$$

where $\mathbf{S}_1, \mathbf{S}_2, \dots, \mathbf{S}_n$ are $d \times d$ positive definite matrices. We will show that the function v is not supermodular, i.e., there are $\mathbf{x}, \mathbf{x}' \in \mathbb{R}_+^n$ such that the following inequality is violated

$$v(\mathbf{x}) + v(\mathbf{x}') \leq v(\mathbf{x} \vee \mathbf{x}') + v(\mathbf{x} \wedge \mathbf{x}') \quad (8)$$

where $\mathbf{x} \vee \mathbf{x}'$ denotes the componentwise maximum and $\mathbf{x} \wedge \mathbf{x}'$ denotes the componentwise minimum of \mathbf{x} and \mathbf{x}' .

To show that (8) is violated, it suffices to show that

$$\frac{\partial^2 v(\mathbf{x})}{\partial x_j \partial x_i} < 0 \quad (9)$$

for some $\mathbf{x} \in \mathbb{R}_+^n$ (see, e.g., Topkis [15], Page 42). We note that

$$\begin{aligned} \frac{\partial^2 v(\mathbf{x})}{\partial x_j \partial x_i} &= \frac{1}{d} \det\left(\sum_{k \in [n]} x_k \mathbf{S}_k\right)^{\frac{1}{d}} \times \\ &\left[\frac{1}{d} \text{tr} \left\{ \left(\sum_{k \in [n]} x_k \mathbf{S}_k \right)^{-1} \mathbf{S}_i \right\} \text{tr} \left\{ \left(\sum_{k \in [n]} x_k \mathbf{S}_k \right)^{-1} \mathbf{S}_j \right\} \right. \\ &\quad \left. - \text{tr} \left\{ \left(\sum_{k \in [n]} x_k \mathbf{S}_k \right)^{-2} \mathbf{S}_i \mathbf{S}_j \right\} \right]. \end{aligned} \quad (10)$$

However, it is easy to show (see, e.g., Zhang [16], page 166) that there are $d \times d$ positive definite matrices \mathbf{A} and \mathbf{B} for which

$$\frac{1}{d} \text{tr}(\mathbf{A}) \text{tr}(\mathbf{B}) < \text{tr}(\mathbf{AB}).$$

Hence, the last term in (10) can be negative. As a numerical example, consider $d = 2$ and

$$\mathbf{A} = \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 2 & 3 \\ 3 & 7 \end{bmatrix}.$$

It then holds that $\frac{1}{d} \text{tr}(\mathbf{A}) \text{tr}(\mathbf{B}) = 18$ whereas $\text{tr}(\mathbf{AB}) = 19$.

Finally, note that the violation of supermodularity in the discrete domain follows from this result of violation of supermodularity in continuous domain. Indeed, we have shown that there is $\mathbf{x} \in \mathbb{R}_+^n$ such that (9) is true. It then follows that there are $\Delta_i, \Delta_j > 0$ such that

$$\begin{aligned} &v([x_1, \cdot, x_i + \Delta_i, \cdot, x_j, \cdot, x_N]) + v([x_1, \cdot, x_i, \cdot, x_j + \Delta_j, \cdot, x_N]) \\ &> v([x_1, \cdot, x_i + \Delta_i, \cdot, x_j + \Delta_j, \cdot, x_N]) + v(\mathbf{x}). \end{aligned}$$

Consider $\mathbf{A} = \Delta_i \mathbf{S}_i$, $\mathbf{B} = \Delta_j \mathbf{S}_j$, $\mathbf{C} = \sum_{k \in [n]} x_k \mathbf{S}_k$. Evidently, $\mathbf{A}, \mathbf{B}, \mathbf{C}$ are positive definite. However, according to the above inequality and the definition of the function v , we have shown that

$$\begin{aligned} &\det(\mathbf{A} + \mathbf{C})^{\frac{1}{d}} + \det(\mathbf{B} + \mathbf{C})^{\frac{1}{d}} \\ &> \det(\mathbf{A} + \mathbf{B} + \mathbf{C})^{\frac{1}{d}} + \det(\mathbf{C})^{\frac{1}{d}}, \end{aligned}$$

so that neither ν_G nor ν is supermodular.

IV. DISCUSSION

The study of the Stam region is analogous in some sense to the study of the entropic region defined using the joint entropy of subsets of random variables, on which there has been much progress in recent decades. Let us briefly reveal the analogy. Let X_s denote $(X_i : i \in s)$ and H denote the discrete entropy, where $(X_i : i \in [n])$ is a collection of *dependent* random variables taking values in some discrete space.

- Major contributions were made by Han and Fujishige in the 1970's. In particular, the fact that $g(s) = H(X_s)$ is a submodular set function goes back at least to Fujishige [17].
- Madiman and Tetali [18] clarified the relationship between submodularity and fractional subadditivity inequalities. In particular, they obtained (as a special case of their main result) the following lower and upper bounds for joint entropy of a collection of random variables: for any fractional partition β using any collection of sets \mathcal{C} ,

$$\sum_{s \in \mathcal{C}} \beta_s H(X_s | X_{s^c}) \leq g([n]) \leq \sum_{s \in \mathcal{C}} \beta_s g(s). \quad (11)$$

Inequality (11) generalized earlier inequalities of Han [19], Fujishige [17] and Shearer [20].

- Motivated by the problem of characterizing the class of all entropy inequalities for the joint distributions of a collection of dependent random variables, Yeung and collaborators [21] observed in the 1990's that there exist so-called non-Shannon inequalities that do not follow from submodularity of entropy.

As noted in [22], it does not seem to be easy to derive entropy lower bounds for sums and inequalities for joint distributions using a common framework; even the recent innovative treatment of entropy power inequalities by Rioul [23], which partially addresses this issue, requires some delicate analysis in the end to justify the vanishing of higher-order terms in a Taylor expansion. However, upper bounds for entropy of sums tend to be provable by elementary means; see [22] for a study of the continuous case, and [24] for a study of the discrete case.

To conclude, let us observe that the Stam region is in a sense simpler than the entropic region studied by Yeung et al. While Theorem 1 is analogous in some sense to the upper bound in (11), Theorem 2 shows that the analogue of Fujishige's submodularity is not true.

REFERENCES

- [1] A. Barron, "Entropy and the central limit theorem," *Ann. Probab.*, vol. 14, pp. 336–342, 1986.
- [2] C. Shannon, "A mathematical theory of communication," *Bell System Tech. J.*, vol. 27, pp. 379–423, 623–656, 1948.
- [3] P. Bergmans, "A simple converse for broadcast channels with additive white gaussian noise," *IEEE Trans. Inform. Theory*, vol. 20, no. 2, pp. 279–280, 1974.
- [4] L. Ozarow, "On a source coding problem with two channels and three receivers," *Bell System Tech. J.*, vol. 59, no. 10, pp. 1909–1921, 1980.
- [5] M. Costa, "On the Gaussian interference channel," *IEEE Trans. Inform. Theory*, vol. 31, no. 5, pp. 607–615, 1985.
- [6] Y. Oohama, "The rate-distortion function for the quadratic gaussian ceo problem," *IEEE Trans. Inform. Theory*, vol. 44, no. 3, pp. 1057–1070, 1998.
- [7] A. Stam, "Some inequalities satisfied by the quantities of information of Fisher and Shannon," *Information and Control*, vol. 2, pp. 101–112, 1959.
- [8] M. Madiman and A. Barron, "Generalized entropy power inequalities and monotonicity properties of information," *IEEE Trans. Inform. Theory*, vol. 53, no. 7, pp. 2317–2329, July 2007.
- [9] M. Madiman, "Cores of cooperative games in information theory," *EURASIP J. on Wireless Comm. and Networking*, no. 318704, 2008.
- [10] S. Artstein, K. M. Ball, F. Barthe, and A. Naor, "Solution of Shannon's problem on the monotonicity of entropy," *J. Amer. Math. Soc.*, vol. 17, no. 4, pp. 975–982 (electronic), 2004.
- [11] M. Madiman and A. Barron, "The monotonicity of information in the central limit theorem and entropy power inequalities," in *Proc. IEEE Intl. Symp. Inform. Theory*, Seattle, July 2006, pp. 1021–1025.
- [12] A. M. Tulino and S. Verdú, "Monotonic decrease of the non-gaussianity of the sum of independent random variables: A simple proof," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 4295–7, September 2006.
- [13] R. D. Gill and P. D. Grünwald, "An algorithmic and a geometric characterization of coarsening at random," *Ann. Statist.*, vol. 36, no. 5, pp. 2409–2422, 2008.
- [14] E. Friedgut and J. Kahn, "On the number of copies of one hypergraph in another," *Israel Journal of Mathematics*, vol. 105, pp. 251–256, 1998.
- [15] D. M. Topkis, *Supermodularity and complementarity*, ser. Frontiers of Economic Research. Princeton, NJ: Princeton University Press, 1998.
- [16] F. Zhang, *Matrix theory: Basic results and techniques*. New York: Springer-Verlag, 1999.
- [17] S. Fujishige, "Polymatroidal dependence structure of a set of random variables," *Information and Control*, vol. 39, pp. 55–72, 1978.
- [18] M. Madiman and P. Tetali, "Information inequalities for joint distributions, with interpretations and applications," *Submitted*, 2007.
- [19] T. S. Han, "Nonnegative entropy measures of multivariate symmetric correlations," *Information and Control*, vol. 36, no. 2, pp. 133–156, 1978.
- [20] F. Chung, R. Graham, P. Frankl, and J. Shearer, "Some intersection theorems for ordered sets and graphs," *J. Combinatorial Theory, Ser. A*, vol. 43, pp. 23–37, 1986.
- [21] J. Zhang and R. Yeung, "On characterization of entropy function via information inequalities," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1440–1452, 1998.
- [22] M. Madiman, "On the entropy of sums," in *Proc. IEEE Inform. Theory Workshop*, Porto, Portugal, 2008.
- [23] O. Rioul, "A simple proof of the entropy-power inequality via properties of mutual information," in *Proc. IEEE Int. Symp. Inform. Theory*, Nice, France, 2007, pp. 46–50.
- [24] M. Madiman, A. Marcus, and P. Tetali, "Entropy and set cardinality inequalities for partition-determined functions, with applications to sumsets," *Preprint*, 2008.