ON THE ENTROPY OF THE SUM AND OF THE DIFFERENCE OF INDEPENDENT RANDOM VARIABLES

Amos Lapidoth

ETH, Zurich
Switzerland
lapidoth@isi.ee.ethz.ch

Gábor Pete

University of Toronto, Canada
and MSRI, Berkeley, USA
gabor@math.toronto.edu

ABSTRACT

We show that the entropy of the sum of independent random variables can greatly differ from the entropy of their difference. The gap between the two entropies can be arbitrarily large. This holds for regular entropies as well as differential entropies. Our results rely heavily on a result of Ruzsa, who studied sums and differences of finite sets.

Index Terms— Differential Entropy, Entropy, Sum, Difference.

1. INTRODUCTION AND MAIN RESULTS

If a chance variable X takes value in a countable set $\mathcal{X}$, then its entropy, which is denoted by $H(X)$, is given by

$$H(X) = \sum_{\substack{x \in \mathcal{X} \\ P_X(x) > 0}} P_X(x) \log \frac{1}{P_X(x)}, \tag{1}$$

where $P_X(x)$ denotes the probability that X takes on the value x. If the random variables X and Y take value in the integers $\mathbb{Z}$, then we can discuss their sum $X + Y$, their difference $X - Y$, and the associated entropies $H(X + Y)$ and $H(X - Y)$. Our main result is that there does not exist a universal bound on $H(X - Y) - H(X + Y)$ for independent random variables X, Y. That is, for every $M > 0$ there exist independent random variables X and Y taking value in the integers such that $H(X - Y) - H(X + Y) > M$. In fact, X and Y can be chosen independent and identically distributed (IID).

Theorem 1 *Given any $M > 0$, there exist IID random variables X and Y taking value in the integers such that*

$$H(X - Y) - H(X + Y) > M. \tag{2}$$

This theorem strengthens a result of Cohen and Zamir [1] who showed the existence of IID X and Y for which $|H(X + Y) - H(X - Y)|$ is as close to 1 bit as desired.

The result extends also to differential entropy. Recall that the differential entropy of a random variable Z of density $f_Z(\cdot)$ is dented by $h(Z)$ and is given by

$$h(Z) = -\int_{\{z \in \mathbb{R} : f_Z(z) > 0\}} f_Z(z) \log f_Z(z) \, \mathrm{d}z. \tag{3}$$

Theorem 2 *Given any $M > 0$, there exist IID random variables X_c and Y_c of finite differential entropy such that*

$$h\bigl(X_{\mathrm{c}} - Y_{\mathrm{c}}\bigr) - h\bigl(X_{\mathrm{c}} + Y_{\mathrm{c}}\bigr) > M. \tag{4}$$

Theorem 1 is based on a key result by Ruzsa [2]. Before stating this result we introduce some additional notation. If $\mathcal{A}$ is a finite set, then we denote its cardinality (the number of its elements) by $\# \mathcal{A}$. And if $\mathcal{A}$ and $\mathcal{B}$ are nonempty subsets of the integers, then we define the sets

$$\mathcal{A} + \mathcal{B} = \{a + b : a \in \mathcal{A},\ b \in \mathcal{B}\}, \tag{5}$$

$$\mathcal{A} - \mathcal{B} = \{a - b : a \in \mathcal{A},\ b \in \mathcal{B}\}. \tag{6}$$

Ruzsa used the Probabilistic Method to prove:

Theorem 3 (Ruzsa) *For every $n > n_0$ there exists a subset of the integers $\mathcal{A} \subset \mathbb{Z}$ of cardinality n such that*

$$\#\bigl(\mathcal{A} - \mathcal{A}\bigr) \geq n^2 - n^{2-c} \tag{7a}$$

and

$$\#(\mathcal{A} + \mathcal{A}) \leq n^{2-c}, \tag{7b}$$

where

$$c > 0 \tag{7c}$$

is a positive universal constant.

In Section 2 we shall see how Theorem 1 follows from Theorem 3. In Section 3 we shall see how Theorem 2 follows from Theorem 1.

1-4244-2482-5/08/$20.00 ©2008 IEEE

2. PROOF OF THEOREM 1

Let X and Y be IID and uniformly distributed over the set $\mathcal{A}$ whose existence is guaranteed in Theorem 3. Then

$$\begin{aligned} H(X+Y) &\leq \log \#(\mathcal{A}+\mathcal{A}) \\ &\leq \log n^{2-c}, \end{aligned} \tag{8}$$

where the first inequality follows because $H(Z)$ is upper bounded by log of the cardinality of its support set (with equality achieved by the uniform distribution) and where the second inequality follows by (7b).

To lower bound $H(X-Y)$ we first note that

$$\frac{1}{n^2} \leq \Pr(X-Y=z) \leq \frac{1}{n}, \quad z \in \mathcal{A}-\mathcal{A}. \tag{9}$$

Here the lower bound on $\Pr(X-Y=z)$ follows because the fact that z is in $\mathcal{A}-\mathcal{A}$ implies that there exist $x', y' \in \mathcal{A}$ such that $x'-y'=z$ and thus

$$\begin{aligned} \Pr(X-Y=z) &\geq \Pr(X=x', Y=y') \\ &= n^{-2}. \end{aligned}$$

The upper bound on $\Pr(X-Y=z)$ follows because to each $x \in \mathcal{A}$ there corresponds at most one $y \in \mathcal{A}$ such that $x-y=z$, so the number of pairs $x, y \in \mathcal{A}$ satisfying $x-y=z$ is upper bounded by the cardinality of $\mathcal{A}$, i.e., by n.

By (9) it follows that for $n \geq 3$ and $z \in \mathcal{A}-\mathcal{A}$,

$$\frac{1}{n^2} \leq \Pr(X-Y=z) \leq 1/3, \tag{10}$$

and since $\xi \mapsto \xi \log(1/\xi)$ is monotonic in the interval $(0, 1/e)$,

$$\Pr(X-Y=z) \log \frac{1}{\Pr(X-Y=z)} \geq \frac{1}{n^2} \log n^2, \tag{11}$$

for all $n \geq 3$ and $z \in \mathcal{A}-\mathcal{A}$. Summing (11) over all $z \in \mathcal{A}-\mathcal{A}$ we obtain

$$H(X-Y) \geq \frac{\#(\mathcal{A}-\mathcal{A})}{n^2} \log n^2. \tag{12}$$

Combining (12) and (7a) we obtain

$$H(X-Y) \geq \frac{n^2-n^{2-c}}{n^2} \log n^2. \tag{13}$$

Comparing (13) and (8) we thus obtain that

$$\lim_{n\to\infty} \bigl(H(X-Y) - H(X+Y)\bigr) = \infty, \tag{14}$$

at least like $c \log n$. This concludes the proof of Theorem 1.

3. PROOF OF THEOREM 2

We next derive Theorem 2 from Theorem 1. To that end, let U and V IID, uniformly distributed over the interval $(-1/4, 1/4)$, and independent of (X, Y). Define

$$\begin{aligned} X_{\text{c}} &= X+U \\ Y_{\text{c}} &= Y+V, \end{aligned}$$

where X and Y are the random variables taking value in the integers whose existence is guaranteed by Theorem 1.

Since both U and V have a symmetric distribution, it follows that the laws of $U-V$ and $U+V$ are identical. Both take value in the interval $(-1/2, 1/2)$ according to the density

$$g(z) = \begin{cases} 2\bigl(1-2|z|\bigr) & \text{if } |z| \leq 1/2, \\ 0 & \text{otherwise.} \end{cases}$$

Since X and Y take value in the integers $\mathbb{Z}$, it follows that the density of $X_{\text{c}}+Y_{\text{c}}$ at $\xi \in \mathbb{R}$ is given by

$$\Pr(X+Y=\nu)\, g\bigl(|\xi-\nu|\bigr),$$

where ν is the integer closest to ξ. Consequently,

$$h\bigl(X_{\text{c}}+Y_{\text{c}}\bigr) = H(X+Y) + h(U+V). \tag{15}$$

Similarly, the density of $X_{\text{c}}-Y_{\text{c}}$ at ξ is given by

$$\Pr(X-Y=\nu)\, g\bigl(|\xi-\nu|\bigr),$$

where ν is the integer closest to ξ, and

$$h\bigl(X_{\text{c}}-Y_{\text{c}}\bigr) = H(X-Y) + h(U-V). \tag{16}$$

It thus follows from (15) and (16) that

$$h\bigl(X_{\text{c}}-Y_{\text{c}}\bigr) - h\bigl(X_{\text{c}}+Y_{\text{c}}\bigr) = H(X-Y) - H(X+Y), \tag{17}$$

which can be made as large as we wish by Theorem 1.

4. ADDITIONAL READING

Ruzsa's result falls in the general area of "Additive Combinatorics." For more on this area see [3].

5. ACKNOWLEDGMENT

The authors are grateful to Amir Dembo and Yuval Peres for establishing the scientific link that led to this collaboration.

6. REFERENCES

[1] A.S. Cohen and R. Zamir, “Entropy amplification property and the loss for writing on dirty paper,” *IEEE Transactions on Information Theory,* pp. 1477–1487, Vol. 54, No. 4, April 2008.

[2] I.Z. Ruzsa, “On the number of sums and differences,” *Acta Math. Hung.*, Vol. 59, No. 3–4, 1992, pp. 439–447.

[3] T. Tao and V. H. Vu, *Additive Combinatorics,* Cambridge University Press, 2006.