Entropy Bounds for Sums, Products, and for the Entropic Additive Energy

Rupert Li
Stanford University
rupertli@stanford.edu

Lampros Gavalakis Ioannis Kontoyiannis
University of Cambridge
{lg560, ik355}@cam.ac.uk

***Abstract*—Over the past 15 years, many entropy inequalities have been established via ideas and tools from additive combinatorics. In this work we obtain new bounds for the differential entropy of sums, products, and sum-product combinations of random variables. Partly motivated by recent work by Goh on the discrete entropic version of the notion of "additive energy", we introduce the additive energy of pairs of continuous random variables and prove various versions of the statement that "the additive energy is large if and only if the entropy of the sum is small", along with a version of the Balog–Szemerédi–Gowers theorem for differential entropy. Then, motivated in part by recent work by Máthé and O'Regan, we establish new differential entropy inequalities for products and sum-product combinations of random variables. In particular, we prove a new, general, ring Plünnecke–Ruzsa entropy inequality. In the case of discrete entropy, we provide a characterization of discrete random variables with "large doubling", analogous to Tao's Freiman-type inverse sumset theory for small doubling. Finally, we consider the natural entropic analog of the Erdős–Szemerédi sum-product phenomenon for integer-valued random variables. We show that, if it does hold, then the range of parameters for which it does would necessarily be significantly more restricted than its anticipated combinatorial counterpart.**

I. Introduction

Additive combinatorics [27] is an area of mathematics that studies additive structures abelian groups like the integers $(\mathbb{Z}, +)$. The Plünnecke–Ruzsa *sumset theory* is an important sub-field that studies *sumset inequalities*. The *sumset* of two subsets A, B of an additive group G, i.e., an abelian group $(G, +)$, is $A + B = \{a + b : a \in A, b \in B\}$. Sumset inequalities include the trivial bound $|A + B| \geq \max\{|A|, |B|\}$, as well as many more subtle results. For example, if we define the *difference set* $A - B = \{a - b : a \in A, b \in B\}$, then the *Ruzsa triangle inequality* [21] says that

$$|A - C| \leq \frac{|A - B|\,|B - C|}{|B|}, \tag{1}$$

and the *sum-difference inequality* [23] states that

$$|A + B| \leq \frac{|A - B|^3}{|A|\,|B|}. \tag{2}$$

Let X be a discrete random variable with entropy $H(X)$. The Asymptotic Equipartition Property suggests that we can think of $e^{H(X)}$ as the cardinality of the "essential support" of X, and consequently we can interpret $H(X)$ as a probabilistic analog of the log-cardinality of a discrete set A. Thus motivated, Ruzsa [24] and Tao [26] began a systematic exploration of this entropy/cardinality correspondence, showing that, taking any sumset bound and replacing discrete sets with independent discrete random variables, and log-cardinalities by entropies, typically leads to a legitimate entropy inequality. For example, for independent random variables X, Y, Z, the trivial cardinality bound above corresponds to the elementary entropy inequality $H(X + Y) \geq \max\{H(X), H(Y)\}$, the entropic version [26] of the Ruzsa triangle inequality in (1) is

$$H(X - Z) + H(Y) \leq H(X - Y) + H(Y - Z),$$

and the sum-difference inequality in (2) becomes

$$H(X + Y) + H(X) + H(Y) \leq 3H(X - Y).$$

Such entropy inequalities have been broadly generalized [4], [5], [9], [14], [17], [18] and have found numerous applications in information-theoretic problems [10], [13], [15], [25], [28]. Conversely, entropic sumset bounds have also found important applications to questions in combinatorics; see, e.g., [7], [8]

Given the wealth and utility of such discrete entropy inequalities, their extension to the case of the differential entropy has naturally been considered. An essential element in the proofs of the discrete entropic versions of most sumset inequalities is the *functional submodularity* property of discrete entropy [12], [26]. It is easy to see that functional submodularity typically fails for differential entropy [12]. Nevertheless, as was shown in [12] and [17], essentially all of the earlier discrete entropic results obtained by Ruzsa [24], Tao [26], and others, have near-identical continuous analogs.

For independent continuous random variables X, Y, Z, we have the elementary bound $h(X + Y) \geq \max\{h(X), h(Y)\}$, the Ruzsa triangle inequality [12] becomes

$$h(X - Z) + h(Y) \leq h(X - Y) + h(Y - Z),$$

and continuous sum-difference inequality [12] is simply

$$h(X + Y) + h(X) + h(Y) \leq 3h(X + Y).$$

In this paper, we continue the exploration of continuous versions of discrete entropy sumset bounds, largely motivated by recent results obtained by Goh [5] and by Máthé and O'Regan [19]. In the process, we also examine some questions regarding the entropy of sums and products of discrete random variables. **All results are given here without their proofs; these can be found in the full version of this work at [16].**

II. Preliminaries and prior work

Let $(G,+)$ be an arbitrary additive group, The *Ruzsa distance* $d(A,B)$ between two finite subsets A and B of G is

$$d(A,B) = \log \frac{|A-B|}{\sqrt{|A|\,|B|}}, \tag{3}$$

where 'log' denotes the natural logarithm. Note that the Ruzsa distance is not a metric, as $d(A,A) \neq 0$ in general. In this notation, the Ruzsa triangle inequality in (1) becomes

$$d(A,C) \leq d(A,B) + d(B,C), \tag{4}$$

and the sum-difference inequality in (2) is

$$d(A,-B) \leq 3d(A,B). \tag{5}$$

In the case $A = B$, the following tighter bounds are available, sometimes referred to as the *doubling-difference* inequality

$$\frac{1}{2}d(A,A) \leq d(A,-A) \leq 2d(A,A). \tag{6}$$

The *doubling constant* of a finite set $A \subset G$ is the ratio:

$$s(A) = \frac{|A+A|}{|A|}. \tag{7}$$

More generally, for the k-fold addition of a set A to itself, we write $kA = \{a_1 + a_2 + \cdots + a_k : a_1, a_2, \ldots, a_k \in A\}$, for any $k \geq 0$. The Plünnecke–Ruzsa inequality [20], [22] is a fundamental result in additive combinatorics, which states the following. For any subsets A, B of G, if $|A+B| \leq K\,|A|$ for some $K > 0$, then for all integers $m, n \geq 0$ we have:

$$|nB - mB| \leq K^{n+m}\,|A|\,. \tag{8}$$

The *additive energy* of two subsets A, B of G is

$$E(A,B) = |\{(a_1,a_2,b_1,b_2) \in A \times A \times B \times B : a_1 + b_1 = a_2 + b_2)\}|. \tag{9}$$

The natural interpretation of $E(A,B)$ is as a measure of the degree of additive structure present in $A+B$.

An elementary but important inequality for $E(A,B)$ is:

$$E(A,B) \geq \frac{|A|^2\,|B|^2}{|A+B|}. \tag{10}$$

One application of this inequality is in showing that a small sumset $A+B$ implies large additive energy $E(A,B)$: Since $|A+B| \geq \max\{|A|\,,|B|\}$, we always have $|A+B| \geq |A|^{1/2}\,|B|^{1/2}$. We can thus consider $|A+B|$ to be "small" if $|A+B| \leq C\,|A|^{1/2}\,|B|^{1/2}$ for some constant $C > 1$. Then (10) leads to the implication:

$$|A+B| \leq C\,|A|^{1/2}\,|B|^{1/2} \;\Rightarrow\; E(A,B) \geq \frac{1}{C}\,|A|^{3/2}\,|B|^{3/2}\,. \tag{11}$$

Let X, Y be two discrete random variables with values in an additive group G. In analogy with (3), the entropic Ruzsa distance $d(X,Y)$ between X and Y is defined as

$$d(X,Y) = H(X'-Y') - \frac{1}{2}H(X) - \frac{1}{2}H(Y),$$

where $X' \sim X$ and $Y' \sim Y$ are independent. In this notation, the entropic version of the Ruzsa triangle inequality (4) states that, for any three discrete random variables X, Y, Z,

$$d(X,Z) \leq d(X,Y) + d(Y,Z), \tag{12}$$

the entropic version of the sum-difference inequality (5) is

$$d(X,-Y) \leq 3d(X,Y), \tag{13}$$

and the entropic doubling-difference inequality in (6) is

$$\frac{1}{2}d(X,X) \leq d(X,-X) \leq 2d(X,X). \tag{14}$$

An entropic analog of the Plünnecke–Ruzsa inequality (8) proved by Tao [26] says that, if $X_1, \ldots, X_n$, $X'_1, \ldots, X'_m$ are independent copies of a discrete random variable X taking values in an additive group, and $H(X_1 + X'_1) \leq H(X_1) + \log K$ for some $K \geq 1$, then,

$$H(X_1 + \cdots + X_n - X'_1 - \cdots - X'_m) \leq H(X) + O(n+m)\log K.$$

Goh [5] recently introduced a version of the additive energy for discrete random variables. In analogy with the combinatorial version of additive energy (9), the *entropic additive energy* of two jointly distributed discrete random variables X and Y taking values in the same additive group is

$$A(X,Y) = H(X_1, Y_1, X_2, Y_2, X+Y),$$

where (X_1, Y_1) and (X_2, Y_2) are conditionally independent versions of (X,Y) given $X+Y$. We will also find it convenient to use the following equivalent expression for $A(X,Y)$:

$$A(X,Y) = 2H(X,Y) - H(X+Y).$$

This expression clearly leads to the same interpretation as for the combinatorial additive energy: Small entropy of the sum $X+Y$ implies large additive energy $A(X,Y)$. This interpretation is further reinforced by the entropic analog of the implication (11): If X, Y are independent, then

$$H(X+Y) \leq \frac{1}{2}H(X) + \frac{1}{2}H(Y) + \log C$$
$$\Leftrightarrow \quad A(X,Y) \geq \frac{3}{2}H(X) + \frac{3}{2}H(Y) - \log C.$$

Moreover, for arbitrary pairs of discrete random variables (X,Y), the reverse implication remains valid: If the additive energy $A(X,Y)$ is large, then $H(X+Y)$ is small.

As shown in [12], all of the entropy bounds of the previous section extend to continuous random variables. Let $h(X)$ be the *differential entropy* of a continuous random vector $X = (X_1, \ldots, X_d)$. The Ruzsa distance between two continuous random variables X, Y is

$$d(X,Y) = h(X'-Y') - \frac{1}{2}h(X) - \frac{1}{2}h(Y), \tag{15}$$

where X' and Y' are independent copies of X and Y, respectively. Then, for arbitrary continuous random variables X, Y, Z, the Ruzsa triangle inequality (12), the sum-difference inequality (13), and the doubling-difference inequality (14)

remain valid exactly as before. Another useful bound in the same spirit is the *submodularity for sums* inequality, which says that, if X, Y, Z are independent random vectors, then

$$h(X+Y+Z)+h(Y) \leq h(X+Y)+h(Y+Z). \quad (16)$$

The proof of the sum-difference inequality for differential entropy in [12] used a construction similar to Tao's proof of the discrete version [26]. In [16] we note that the submodularity-for-sums inequality can be used to provide a very short proof that works in both the discrete and continuous case.

In [12], the following version of the Plünnecke–Ruzsa inequality for differential entropy is established: Suppose $X, Y_1, Y_2, \ldots, Y_n$ are independent continuous random variables. If there are constants $K_1, K_2, \ldots, K_n \geq 1$ satisfying $h(X+Y_i) \leq h(X) + \log K_i$ for each i, then

$$h(X+Y_1+Y_2+\cdots+Y_n) \leq h(X) + \log(K_1 K_2 \cdots K_n).$$

III. Additive energy and the entropy of sums

We define the *differential entropic additive energy* of two jointly distributed continuous random variables X and Y as

$$a(X,Y) = h(X_1, X_2, X+Y),$$

where (X_1, Y_1) and (X_2, Y_2) are conditionally independent versions of (X, Y), given $X+Y$. We also have have the following alternative representation, as in the discrete case.

Lemma 1. $a(X,Y) = 2h(X,Y) - h(X+Y)$.

The proofs of all the results in this section are based on the following entropic analog of (10).

Lemma 2. *For any pair of continuous random variables X, Y,*

$$h(X+Y) + a(X,Y) = 2h(X,Y) \leq 2h(X) + 2h(Y),$$

where the slackness in the inequality is exactly $2I(X;Y) \geq 0$.

To quantify "large" additive energy here, note that

$$a(X,Y) \leq 2h(X,Y) - h(X|Y) = h(X,Y) + h(Y),$$

so, by symmetry,

$$a(X,Y) \leq h(X) + h(Y) + \min\{h(X), h(Y)\}. \quad (17)$$

Therefore, we can consider $a(X,Y)$ to be large if

$$a(X,Y) \geq \frac{3}{2}h(X) + \frac{3}{2}h(Y) - \log C.$$

Similarly, since

$$h(X+Y) \geq \frac{1}{2}h(X|Y) + \frac{1}{2}h(Y|X),$$

we can consider $h(X+Y)$ to be small if

$$h(X+Y) \leq \frac{1}{2}h(X|Y) + \frac{1}{2}h(Y|X) + \log C.$$

The following result shows that large $a(X,Y)$ implies small $h(X+Y)$. It is a strengthening of the corresponding discrete entropy result in [5, Proposition 3].

Corollary 3. *We have*

$$a(X,Y) \geq \frac{3}{2}h(X) + \frac{3}{2}h(Y) - \log C$$

if and only if

$$h(X) \leq h(Y) + 2\log C - 2I(X+Y;Y) + 2I(X;Y).$$

The reason why large additive energy $a(X,Y)$ implies $h(X)$ and $h(Y)$ are close is, in part, because our definition of what it means for $a(X,Y)$ to be large is symmetric in X and Y. In the asymmetric case where $h(X) < h(Y)$, say, then in view of (17) we can instead consider $a(X,Y)$ to be large if $a(X,Y) \geq 2h(X) + h(Y) - \log C$. Similarly, since $h(X+Y) \geq h(Y|X)$, we can consider $h(X+Y)$ to be small if $h(X+Y) \leq h(Y|X) + \log C$. The following result states that, if $a(X,Y)$ is large in this sense, then $h(X+Y)$ is appropriately small. This strengthens and generalizes [5, Proposition 8] to the continuous case.

Corollary 4. *We have $a(X,Y) \geq 2h(X) + h(Y) - \log C$, if and only if*

$$h(X+Y) \leq h(Y) + \log C - 2I(X;Y) \leq h(Y|X) + \log C.$$

The following result states that, if $h(X+Y)$ is large, then $a(X,Y)$ is small. Corollary 5 generalized and strengthens [5, Proposition 10].

Corollary 5. *We have $h(X+Y) \geq h(X) + h(Y) + \log C$, if and only if,*

$$a(X,Y) \leq h(X) + h(Y) + \log C - 2I(X;Y).$$

IV. The BSG theorem for differential entropy

Here we establish an entropic version of an important result in additive combinatorics, known as the Balog–Szemerédi–Gowers (BSG) theorem [1], [6]. The BSG theorem states that if $E(A,B)$ is large, then A and B must contain high-density subsets A' and B' such that $|A'+B'|$ is small. It can be viewed as a partial converse to the observation (11) that a small sumset $|A+B|$ implies a large additive energy $E(A,B)$.

An entropic BSG theorem was established by Tao in [26, Theorem 3.1], and its differential entropy analog was proved in [12, Theorem 3.14]. More recently, Gowers, Green, Manners, and Tao [8, Lemma A.2] proved a similar discrete result with better constants. However, the most faithful entropy analog of the BSG theorem is due to Goh [5], which is also the only one stated in terms of entropic additive energy.

Since the natural probabilistic analog of restricting to a subset is conditioning, all entropic BSG theorems establish the existence of particular conditionings that lead to appropriate bounds. Next, we state the differential entropy analog of Goh's BSG theorem [5, Theorem 6].

Theorem 6 (Entropic BSG theorem)**.** *Suppose the continuous random variables X and Y satisfy, for some constant C,*

$$a(X,Y) \geq \frac{3}{2}h(X) + \frac{3}{2}h(Y) - \log C.$$

Then, taking (X_1, Y_1) and (X_2, Y_2) to be conditionally independent versions of (X, Y) given $X + Y$, we have

$$h(X_1|X+Y) \geq h(X) - 2\log C,$$
$$h(Y_2|X+Y) \geq h(Y) - 2\log C,$$

and, moreover, X_1 and Y_2 are conditionally independent given $X + Y$, and satisfy

$$h(X_1 + Y_2|X+Y) \leq \frac{1}{2}h(X) + \frac{1}{2}h(Y) + \log C.$$

V. Stability of large discrete entropic doubling

For a discrete random variable X taking values in an additive group G, we define the *doubling constant* $s(X)$ in analogy with the combinatorial doubling constant $s(A)$ in (7),

$$s(X) = H(X + X') - H(X),$$

where X, X' are i.i.d. Clearly, $s(X) \geq 0$, and Tao [26] showed that $s(X)$ is small if and only if X is approximately uniformly distributed on a generalized arithmetic progression. Here, we examine the behaviour of the doubling constant $s(X)$ at its other extreme. We note that $s(X)$ is always bounded above by $H(X)$, and we show that $s(X)$ is close to $H(X)$ if and only if X is approximately supported on a *Sidon set*. Recall that A is a *Sidon set* if, whenever $a + b = c + d$ for $a, b, c, d \in A$, we necessarily have $\{a, b\} = \{c, d\}$.

Goh [5] observed that, if X is supported on a Sidon set then $s(X) \geq H(X) - \log 2$. Our first result identifies a tighter upper bound to $s(X)$ and shows that it is achieved if and only if X is supported on a Sidon set.

Lemma 7. *If X is discrete random variable with probability mass function P on A, then*

$$s(X) \leq H(X) - (\log 2)\left(1 - \sum_{a\in A} P(a)^2\right), \qquad (18)$$

with equality if and only if X is supported on a Sidon set.

We now prove a stability result, showing that if $s(X)$ is close to its upper bound in (18), then X is close to being supported on a Sidon set.

Proposition 8. *Let X be a discrete random variable with probability mass function P on A. If*

$$s(X) \geq H(X) - (\log 2)\left(1 - \sum_{a\in A} P(a)^2\right) - C, \qquad (19)$$

for some $C \geq 0$, then there exists a Sidon set $B \subset A$ s.t.

$$\mathbb{P}(X \in B) \geq 1 - \frac{C}{p_*(\log 2)}, \qquad (20)$$

where $p_* = \min\{P(a) : a \in A\} > 0$.

In [16] we present examples demonstrating that the assumption that X takes on only finitely many values – equivalently, that p_* is strictly positive – cannot be removed. In fact, the dependence of the bound (20) on p_* cannot be avoided. Proposition 8 and these examples raise the following question.

Open problem. It would be interesting to determine whether there exists a function $f(C, D) \geq 0$ for $C, D \geq 0$, with $f(C, D) \to 0$ as $C \to 0$ for any fixed $D \geq 0$, such that the following holds: If X is a discrete random variable with values in A and with $H(X) \leq D$ and satisfying condition (19) of Proposition 8 with constant C, then there exists a Sidon set $B \subset A$ such that $\mathbb{P}(X \in B) \geq 1 - f(C, D)$.

Finally, we return to the obvious upper bound $s(X) \leq H(X)$. Lemma 7 shows that this is achieved if and only if X is deterministic. Our last result in this section is a stability statement, showing that if $s(X)$ is close to $H(X)$, then X is close to being deterministic.

Proposition 9. *Let X be a discrete random variable with probability mass function P on A. If $s(X) \geq H(X) - \varepsilon$ for some constant $\varepsilon > 0$, then*

$$p^* := \max_{a\in A} P(a) \geq 1 - \frac{\varepsilon}{\log 2}.$$

VI. Differential entropy bounds for products

Let X be an arbitrary continuous random variable. Since $\mathbb{P}(X = 0) = 0$, we can think of X as taking values in the set $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ equipped with the multiplication operation. Recall that $(\mathbb{R}^\times, \cdot)$ is an abelian group with Haar measure ρ given by its density $\frac{d\rho}{d\lambda}(x) = \frac{1}{|x|}$, $x \in \mathbb{R}^\times$, with respect to Lebesgue measure λ. If X has law μ with density $f = d\mu/d\lambda$ with respect to Lebesgue measure, then it also has density

$$g(x) = \frac{d\mu}{d\rho}(x) = |x|f(x), \quad x \in \mathbb{R}^\times,$$

with respect to Haar measure.

In [17] it was observed that a number of entropy inequalities for sums also hold for random variables taking values in arbitrary locally compact, Polish, abelian groups $(G, *)$, with addition replaced by the group operation $*$, and with differential entropy replaced by its obvious analog,

$$\widetilde{h}(X) = -\int g \log g \, d\rho,$$

where ρ denotes the Haar measure on G. In the case of $(\mathbb{R}^\times, \cdot)$, we call $\widetilde{h}(X)$ the *multiplicative entropy* of a continuous random variable X, and observe that, if X has density f with respect to Lebesgue measure, then $\widetilde{h}(X)$ and the usual differential entropy $h(X)$ are related via $\widetilde{h}(X) = h(X) - \mathbb{E}[\log |X|]$. The joint multiplicative entropy of a finite collection of continuous random variables is defined in the obvious way, and we similarly define the conditional multiplicative entropy, the multiplicative mutual information, and so on.

Here we note a number of "multiplicative" entropy inequalities that we will find useful in Section VII. All these results follow from the correspondence noted in [17].

The following is the multiplicative version of Ruzsa's triangle inequality.

Proposition 10 (Multiplicative Ruzsa triangle inequality)**.** *Let X, Y, and Z be independent continuous random variables such that $\log|X|$, $\log|Y|$, and $\log|Z|$ are integrable. Then*

$$h(X/Z) \le h(X/Y) + h(Y/Z) - h(Y) + \mathbb{E}[\log|Y|].$$

Similarly, the multiplicative analog of the submodularity-for-sums bound in (16) is:

Proposition 11. *Let X, Y, and Z be independent, continuous random variables, such that $\log|X|$, $\log|Y|$ and $\log|Z|$ are integrable. Then*

$$h(XYZ) + h(Y) \le h(XY) + h(YZ).$$

Next, we define the *multiplicative Ruzsa distance* between two continuous random variables X and Y, where $\log|X|$ and $\log|Y|$ are integrable, as with the additive version in (15),

$$\widetilde{d}(X,Y) = \widetilde{h}(X'/Y') - \frac{1}{2}\widetilde{h}(X) - \frac{1}{2}\widetilde{h}(Y),$$

where $X' \sim X$ and $Y' \sim Y$ are independent.

The *doubling constant* $\sigma(X)$ and the *difference constant* $\delta(X)$ of a continuous random variable X are defined analogously to the discrete case as,

$$\sigma(X) = h(X+X') - h(X), \quad \delta(X) = h(X-X') - h(X),$$

where X, X' are i.i.d. In this notation, the doubling-difference inequality for differential entropy states that

$$\frac{1}{2} \le \frac{\sigma(X)}{\delta(X)} \le 2.$$

The natural multiplicative analogs of $\sigma(X)$ and $\delta(X)$ are,

$$\widetilde{\sigma}(X) := h(XX') - h(X) - \mathbb{E}[\log|X|] = \widetilde{d}(X, 1/X),$$
$$\widetilde{\delta}(X) := h(X/X') - h(X) + \mathbb{E}[\log|X|] = \widetilde{d}(X, X),$$

where X, X' are i.i.d. The following is the multiplicative version of the doubling-difference inequality.

Theorem 12 (Square-quotient inequality)**.** *Let X be a continuous random variable such that $\log|X|$ is integrable. Then*

$$\frac{1}{2} \le \frac{\widetilde{\sigma}(X)}{\widetilde{\delta}(X)} \le 2.$$

Finally, we observe that the same inductive application of Proposition 11 as was done for the additive case in [17], immediately gives the following multiplicative version of the Plünnecke–Ruzsa inequality (PRI).

Theorem 13 (Multiplicative PRI)**.** *Let X and $Y_1, Y_2, \dots, Y_n$ be independent, continuous random variables, such that $\log|X|$ and all $\log|Y_i|$, $1 \le i \le n$, are integrable. Suppose there are finite constants $K_1, K_2, \dots, K_n$ satisfying $h(XY_i) \le h(X) + \log K_i$ for each i. Then:*

$$h(XY_1Y_2\cdots Y_n) \le h(X) + \log(K_1K_2\cdots K_n).$$

VII. Bounds for sum-product combinations

The following inequality is the continuous version of an inequality proved for discrete entropy by Máthé and O'Regan in [19, Proposition 4.1].

Proposition 14. *Let X, Y, Z be continuous random variables such that $\log|X|$ is integrable. Then*

$$h(X(Y+Z)) + h(X,Y,Z) \le h(X,Y+Z) + h(XY,XZ) - \mathbb{E}[\log|X|].$$

Using the additive PRI of [12] together with the multiplicative PRI of Theorem 13, gives the following general ring PRI. As before, we note that its obvious discrete analog also holds.

Theorem 15 (General ring PRI)**.** *Suppose that continuous random variables $\{X_{ij} \,;\, 1 \le i \le m, 1 \le j \le n\}$ are i.i.d. and distributed as X. Assuming $\log|X|$ is integrable, we have*

$$h\left(\sum_{i=1}^{m}\prod_{j=1}^{n} X_{i,j}\right) \le h(X_{1,1}X_{1,2}\cdots X_{1,n}) + (m-1)\big[(n+2)(n-1)\widetilde{\sigma}(X) + (n-1)\delta(X) + \sigma(X)\big].$$

VIII. On the entropic sum-product phenomenon

For $A \subset \mathbb{Z}$, let $A \cdot A = \{a_1a_2 : a_1, a_2 \in A\}$. In 1983, Erdős and Szemerédi [3] observed that $A+A$ and $A \cdot A$ cannot both be small simultaneously. Specifically, they showed that there is a positive constant ε such that, for $A \subset \mathbb{Z}$,

$$\max\{|A+A|, |A\cdot A|\} \ge |A|^{1+\varepsilon-o(1)},$$

where the $o(1) \to 0$ as $|A| \to \infty$. Although they did not provide an explicit estimate for ε, it is widely conjectured (but still unproven) that the result should hold for any $\varepsilon \le 1$. The best result to date is by Bloom [2], with $\varepsilon = \frac{1}{3} + \frac{2}{951}$.

For i.i.d. $\mathbb{Z}$-valued random variables X, X', Goh [5] conjectured that, as $H(X) \to \infty$,

$$\max\{H(X+X'), H(X\cdot X')\} \ge (1+\epsilon-o(1))H(X), \quad (21)$$

for some $\varepsilon > 0$. In this section we show that, if such a result were to hold, it would necessarily be with $\varepsilon \le 1/3$. Yet another example is given in [16].

Example 16. *For $n \ge 1$, consider the random variable X which takes value 0 with probability $\frac{1}{3}$, and with probability $\frac{2}{3}$ takes a value uniformly at random in $\{1, 2, \dots, n\}$. If X, X' are i.i.d., then it can be shown without too much effort that:*

$$\max\{H(X+X'), H(X\cdot X')\} \le \left(\frac{4}{3} + o(1)\right) H(X).$$

By taking $n \to \infty$, we can obtain arbitrarily large $H(X)$, so this example shows (21) *cannot hold in general for any $\varepsilon > \frac{1}{3}$.*

Acknowledgment

This work was supported in part by the EPSRC-funded INFORMED-AI project EP/Y028732/1. Rupert Li was partially supported by a Hertz Fellowship and a PD Soros Fellowship.

REFERENCES

[1] A. Balog and E. Szemerédi. A statistical theorem of set addition. *Combinatorica*, 14(3):263–268, September 1994.

[2] T.F. Bloom. Control and its applications in additive combinatorics. *arXiv e-prints*, 2501.09470 [math.NT], January 2025.

[3] P. Erdős and E. Szemerédi. On sums and products of integers. In P. Erdős, L. Alpár, G. Halász, and A. Sárközy, editors, *Studies in pure mathematics*, pages 213–218. Birkhäuser, Basel, 1983.

[4] L. Gavalakis, I. Kontoyiannis, and M. Madiman. The entropic doubling constant and robustness of Gaussian codebooks for additive-noise channels. *IEEE Trans. Inform. Theory*, 70(12):8467–8477, December 2024.

[5] M. Goh. On an entropic analogue of additive energy. *arXiv e-prints*, 2406.18798 [math.CO], June 2024.

[6] W.T. Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geom. Funct. Anal.*, 8(3):529–551, July 1998.

[7] W.T. Gowers, B. Green, F. Manners, and T. Tao. Marton's conjecture in abelian groups with bounded torsion. *arXiv e-prints*, 2404.02244 [math.NT], April 2024.

[8] W.T. Gowers, B. Green, F. Manners, and T. Tao. On a conjecture of Marton. *Ann. of Math.*, 201(2):515–549, March 2025.

[9] B. Green, F. Manners, and T. Tao. Sumsets and entropy revisited. *Random Struct. Algorithms*, 66(1):e21252, 2025.

[10] R. Gül, D. Stotz, S.A. Jafar, H. Bölcskei, and S. Shamai. Canonical conditions for $K/2$ degrees of freedom. *IEEE Trans. Inform. Theory*, 68(3):1716–1730, March 2022.

[11] V.A. Kaimanovich and A.M. Vershik. Random walks on discrete groups: Boundary and entropy. *Ann. Probab.*, 11(3):457–490, August 1983.

[12] I. Kontoyiannis and M. Madiman. Sumset and inverse sumset inequalities for differential entropy and mutual information. *IEEE Trans. Inform. Theory*, 60(8):4503–4514, August 2014.

[13] A. Lapidoth and G. Pete. On the entropy of the sum and of the difference of two independent random variables. In *25th IEEE Convention of Electrical and Electronics Engineers in Israel*, pages 623–625, 2008.

[14] C.W.K. Lau and C. Nair. Information inequalities via ideas from additive combinatorics. In *2023 IEEE International Symposium on Information Theory (ISIT)*, pages 2452–2457, Taipei, Taiwan, June 2023.

[15] C.W.K. Lau, C. Nair, and D. Ng. A mutual information inequality and some applications. *IEEE Trans. Inform. Theory*, 69(10):6210–6220, October 2023.

[16] R. Li, L. Gavalakis, and Kontoyiannis. Entropic additive energy and entropy inequalities for sums and products. *arXiv e-prints*, 2506.20813 [cs.IT], June 2025.

[17] M. Madiman and I. Kontoyiannis. Entropy bounds on abelian groups and the Ruzsa divergence. *IEEE Trans. Inform. Theory*, 64(1):77–92, January 2018.

[18] A.V. Makkuva and Y. Wu. Equivalence of additive-combinatorial linear inequalities for Shannon entropy and differential entropy. *IEEE Trans. Inform. Theory*, 64(5):3579–3589, May 2018.

[19] A. Máthé and W.L. O'Regan. Discretised sum-product theorems by Shannon-type inequalities. *J. London Math. Soc.*, 112:e70389, 2025.

[20] H. Plünnecke. Eine zahlentheoretische Anwendung der Graphtheorie. *J. Reine Angew. Math*, 243:171–183, 1970.

[21] I.Z. Ruzsa. On the cardinality of $A+A$ and $A-A$. In *Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II*, volume 18 of *Colloq. Math. Soc. János Bolyai*, pages 933–938. North-Holland, Amsterdam-New York, 1978.

[22] I.Z. Ruzsa. An application of graph theory to additive number theory. *Sci. Ser. A Math. Sci. (N.S.)*, 3:97–109, 1989.

[23] I.Z. Ruzsa. Sums of finite sets. In G.V. Chudnovsky D.V. Chudnovsky and M.B. Nathanson, editors, *Number Theory: New York Seminar*. Springer-Verlag, 1996.

[24] I.Z. Ruzsa. Sumsets and entropy. *Random Struct. Algorithms*, 34(1):1–10, January 2009.

[25] D. Stotz and H. Bölcskei. Degrees of freedom in vector interference channels. *IEEE Trans. Inform. Theory*, 62(7):4172–4197, July 2016.

[26] T. Tao. Sumset and inverse sumset theory for Shannon entropy. *Comb., Probab. Comput.*, 19(4):603–639, July 2010.

[27] T. Tao and V. Vu. *Additive combinatorics*. Cambridge studies in advanced mathematics. Cambridge University Press, Cambridge, U.K., 2006.

[28] Y. Yao and S.A. Jafar. The capacity of 3 user linear computation broadcast. *IEEE Trans. Inform. Theory*, 70(6):4414–4438, June 2024.