ETH zürich

ETH Library

Sumset differential entropy bounds

Conference Paper

Author(s):
Kontoyiannis, Ioannis

Publication date:
2012

Permanent link:
https://doi.org/10.3929/ethz-a-007071347

Rights / license:
In Copyright - Non-Commercial Use Permitted

This page was generated automatically upon download from the ETH Zurich Research Collection.
For more information, please consult the Terms of use.

Sumset Differential Entropy Bounds

Ioannis Kontoyiannis
Department of Informatics
Athens University of Economics & Business
Patission 76, Athens 10434, Greece
Email: yiannis@aueb.gr
Web: http://pages.cs.aueb.gr/ yiannisk/

***Abstract*—Terence Tao recently developed a series of new inequalities for the (discrete) Shannon entropy, which parallel sumset and inverse sumset bounds in additive combinatorics. We examine some of their natural analogs for differential entropy. Since the main ingredient in Tao's proofs (the submodularity of the entropy function) fails in the continuous case, interesting new phenomena arise. We review some known results and present a series of new differential entropy inequalities. These results are based, in part, on joint work with Mokshay Madiman.**

I. Additive Combinatorics and Entropy

The field of *additive combinatorics* [see, e.g., [7] for an introduction] is the theory of additive structures in sets equipped with a group structure. The prototypical example is the study of arithmetic progressions in sets of integers, as opposed to the multiplicative structure that underlies prime factorization and much of classical combinatorics and number theory. There have been several major developments and a lot of high-profile mathematical activity in additive combinatorics in recent years, with perhaps the most famous example being the celebrated Green-Tao theorem on the existence of arbitrarily long arithmetic progressions within the primes.

An important collection of tools in the study of additive combinatorics is a variety of *sumset inequalities*. Here, the *sumset* $A+B$ of two discrete sets A and B is defined as, $A+B=\{a+b : a\in A, b\in B\}$, and a *sumset inequality* is an inequality connecting the cardinality $|A+B|$ of $A+B$ with the cardinalities of A and B. Therefore, roughly and somewhat incorrectly speaking, it might be said that additive combinatorics gives bounds on the sizes of discrete additive sets.

In this setting, we recall the natural connection between entropy and set cardinality established by the AEP: The entropy $H(X)$ can be thought of as the logarithm of the *effective cardinality* of the alphabet of a discrete random variable X. This suggests a correspondence between bounds for the cardinalities of sumsets like, e.g., $|A+B|$, and corresponding bounds for the entropy of sums of discrete random variables, e.g., $H(X+Y)$. This connection appears to have first been identified by Imre Ruzsa, and in the last few years it has also been explored in different directions by, among others, Tao and Vu [6], Lapidoth and Pete [1], Ruzsa [4], Madiman, Marcus and Tetali [3], Madiman and Kontoyiannis [2], and Tao [5].

II. Sumset bounds and differential entropy

This analogy can be carried further: The continuous AEP states that the differential entropy $h(X)$ of a continuous random vector X can be thought of as the logarithm of the (Euclidean or Lebesgue) "volume of the effective support" of X. It is then natural to consider whether the recent discrete sumset entropy bounds can be extended to the continuous case.

Taking as our starting point the results in Tao's recent work [5], we provide natural differential entropy analogs for the following inequalities:

- Rusza triangle inequality
- Sum-difference inequality
- Plünnecke-Rusza inequality
- Iterated sum bound
- Balog-Szemerédi-Gowers lemma
- Rusza's covering lemma
- Green-Rusza-Freiman inverse-sumset theorem

The difficulty as well as the excitement of this work stem from the fact that, in the continuous case, the natural generalizations of the proofs of the discrete versions of many of these results fail at a deep level. One reason is that the main ingredient in earlier proofs is the submodularity of the discrete entropy functional, which does not hold for differential entropy. And, further, it is the overall structure of the proofs that does not carry on to the continuous case: Not the method, but the actual intermediate steps fail to hold for differential entropy. Therefore, it is necessary to employ different tools and fundamentally new proof strategies.

References

[1] A. Lapidoth and G. Pete. On the entropy of the sum and of the difference of two independent random variables. *Proc. IEEEI 2008, Eilat, Israel*, 2008.
[2] M. Madiman and I. Kontoyiannis. The entropies of the sum and the difference of two iid random variables are not too different. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1369 –1372, june 2010.
[3] M. Madiman, A. Marcus, and P. Tetali. Entropy and set cardinality inequalities for partition-determined functions, with applications to sumsets. *Random Structures & Algorithms*, to appear, 2012.
[4] I.Z. Rusza. Sumsets and entropy. *Random Structures & Algorithms*, 34(1):1–10, 2009.
[5] T. Tao. Sumset and inverse sumset theory for Shannon entropy. *Combinatorics, Probability and Computing*, 19:603–639, 2010.
[6] T. Tao and V. Vu. Entropy methods. Available online at: http://www.math.ucla.edu/~tao/.
[7] T. Tao and V. Vu. *Additive combinatorics*. Cambridge studies in advanced mathematics. Cambridge University Press, 2006.