Applications of the sum-product theorem in finite fields

Avi Wigderson
Institute for Advanced Study, Princeton
avi@ias.edu

Abstract

About two years ago Bourgain, Katz and Tao [1] proved the following theorem, essentially stating that in every finite field, a set which does not grow much when we add *all pairs of elements, and when we* multiply *all pairs of elements, must be very close to a subfield.*

Theorem 1 *[1] For every $\epsilon > 0$ there exists a $\delta > 0$ such that the following holds. Let F be any field with no subfield of size $\geq |F|^{\epsilon}$. For every set $A \subseteq F$, with $|F|^{\epsilon} < |A| < |F|^{1-\epsilon}$, either the sumset $|A + A| > |A|^{1+\delta}$ or the product set $|A \times A| > |A|^{1+\delta}$.*

This theorem revealed its fundamental nature quickly. Shortly afterwards it has found many diverse applications, including in Number Theory, Group Theory, Combinatorial Geometry, and the explicit construction of Extractors and Ramsey graphs, mostly described in the references below.

In my talk I plan to explain some of the applications, as well as to sketch the main ideas of the proof of the sum-product theorem.

References

[1] J. Bourgain, N. Katz, and T. Tao, "A Sum-Product Estimate in Finite Fields and Application", *GAFA*, 14 (1) (2004), pp. 27-57.

[2] J. Bourgain, A. A. Glibichuk and S. Konyagin, "Estimates for the Number of Sum Products and for Exponential Sums in Fields of Prime Order", *J. London Math. Soc.*, 73 (2) (2006), pp. 1-19.

[3] J. Bourgain, A. Gamburd, "New Results on Expanders", to appear in *Comptes Rendus Mathematique*.

[4] J. Bourgain, "On the Construction of Affine Extractors", to appear in *GAFA*.

[5] B. Barak, R. Impagliazzo and A. Wigderson, "Extracting Randomness Using Few Independent Sources", *Proc of the 45th FOCS*, 2004, pp. 384-393.

[6] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov and A. Wigderson, "Simulating Independence: New Constructions of Condensers, Ramsey Graphs, Dispersers, and Extractors", *Proc. of the 46th STOC*, 2005, pp. 1-10.

[7] B. Barak, A. Rao, R. Shaltiel and A. Wigderson, "2-Source Dispersers for Sub-Polynomial Entropy and Ramsey Graphs Beating the Frankl-Wilson Construction", to appear in the *Proc. of 47th STOC*.

Proceedings of the 21st Annual IEEE Conference on Computational Complexity (CCC'06)
0-7695-2596-2/06 $20.00 © 2006 IEEE