Additive Combinatorics Lecture 8

Leo Goldmakher

Scribe: Gal Gross

March 7th, 2014

In this lecture we will finally begin the proof of the Freiman-Ruzsa Theorem, bringing together many of the techniques we've learned in past lectures. Before we begin, recall that for a finite $A \subseteq \mathbb{Z}$ we have $|A+A| \geq 2|A|-1$, with equality iff A is an arithmetic progression. If $A+A$ is slightly larger – say, $|A+A| \leq 4|A|$ – it's tempting to guess that A still looks roughly like an AP. To state this precisely, we need the notion of a generalized arithmetic progression.

Definition. A set $P \subseteq \mathbb{Z}$ is called a GENERALIZED ARITHMETIC PROGRESSION (or **gAP**) if it is of the form

$$P = \{x_0 + j_1x_1 + j_2x_2 + \cdots + j_dx_d : 0 \leq j_k < m_k \quad \forall k\},$$

where $x_0 \in \mathbb{Z}$ and $x_i \in \mathbb{Z} \setminus \{0\}$ for all $1 \leq i \leq d$. The minimal number d for which P can be written as above is called the DIMENSION of P, denoted $\dim P$. The case $\dim P = 1$ corresponds to P being an arithmetic progression.

Note that $|P| \leq m_1m_2 \ldots m_d$. If equality holds, then P is called a PROPER gAP.

Exercise 1. Let P be some gAP.

(a) Prove that $\dim(P+P) \leq \dim P$.

(b) Give an example where equality fails to hold.

(c) Prove that $|P+P| \leq 2^d |P|$.

Exercise 2. Let $A \subseteq \mathbb{Z}$ be finite. How can you embed A in a gAP P (that is, $A \subseteq P$), such that $|P|$ is comparable to $|A|$? Calculate a few representative examples, trying to keep the dimension of P small.

Theorem (Freiman-Ruzsa)**.** Let $A \subseteq \mathbb{Z}$ be a finite set with $|A+A| \leq K|A|$. Then there exists a gAP $P \subseteq \mathbb{Z}$ such that

- $P \supseteq A$;
- $|P| \ll_K |A|$;
- $\dim P \ll_K 1$.

Thus, any set of small doubling "looks like" an arithmetic progression (recall that the smaller the dimension, the more the gAP looks like a *bona fide* AP). Before we move on to the proof of this theorem, let us mention some recent developments. The theorem was originally proved by Freiman in 1962, but it wasn't until Ruzsa significantly simplified the proof in 1994 that it began attracting widespread attention. In 2007, Green and Ruzsa generalized the theorem to arbitrary abelian groups. Even though a gAP is a perfectly well-defined object in an arbitrary abelian group, it is not quite the right notion to use when generalizing Freiman-Ruzsa; instead, one embeds sets of small doubling into a *coset progression*, i.e. a set of the form $H+P$ where H is a subgroup and P is a gAP. In 2012, Breuillard, Green, and Tao generalized the theorem further, to arbitrary (non-abelian) groups. The correct generalization of gAP in that setting is quite complicated.

The starting point in Ruzsa's proof of Freiman-Ruzsa is to translate the original problem to an easier one. By adding and subtracting more and more copies of A, one obtains a much 'smoother' set with more and more additive structure. Ruzsa observed that it suffices to find a large gAP in $mA - nA$.

Claim 1. Suppose we find fixed non-negative integers m and n such that $mA - nA$ contains a proper gAP P satisfying $|P| \gg_K |A|$ and $\dim P \ll_K 1$. Then there exists a gAP Q such that $A \subseteq Q$, $|Q| \ll_{m,n,K} |A|$, and $\dim Q \ll_{m,n,K} 1$.

Proof. We may assume that $|P| \asymp |A|$, for otherwise replace P by another gAP, P', with this property; where P' is obtained from P by simply "trimming" P appropriately. Similarly to Ruzsa's theorem (Lecture 7), pick the maximal $X \subseteq A$ with the property that the sets $P + \{x\}$ are pairwise disjoint as x runs over all $x \in X$. By Plünnecke-Ruzsa we have

$$|X| = \frac{|P + X|}{|P|} \ll_{m,n,K} \frac{|A|}{|A|} = 1.$$

Observe that $A \subseteq X + P - P$. By Exercise 1 above we have

$$|P - P| \leq 2^{\dim(P-P)} |P| \leq 2^{\dim P} |P| \ll |P| \ll |A| .$$

Let Q be the smallest gAP containing $X + P - P$. Note that $P - P$ is already a gAP, and even if we treat each element of X as a new generator, we obtain a gAP Q as in the claim. □

Exercise 3. Carefully make precise the last sentence.