Additive Combinatorics Lecture 7

Leo Goldmakher
Scribe: Gal Gross

Feb. 28th, 2014

Last lecture we discussed the relation between the ratios $|A+A|\,/\,|A|$ and $|A-A|\,/\,|A|$, which are both sometimes called the "doubling constant" of A. We arrived at the following result:

Theorem 1 (Plünnecke-Ruzsa)**.** Let $A \subseteq G$ with $|A+A| \leq K\,|A|$. Then for all nonnegative integers m, n we have

$$|mA - nA| \leq K^{m+n}\,|A|$$

where $mA = \underbrace{A + A + \cdots + A}_{m \text{ times}}$.

This is proved in the Lecture 6, except for a key lemma which we prove now. (In fact, this is precisely the proof we came up with collaboratively last lecture, just tidied up a bit.)

Lemma (Petridis)**.** Suppose $A \subseteq G$ is a set such that $|A+A| \leq K\,|A|$. Choose $\emptyset \neq X \subseteq A$ such that the ratio $|A+X|\,/\,|X|$ is minimized, and denote this ratio by K_0. Then for all $B \subseteq G$ we have

$$|A+B+X| \leq K_0\,|B+X|\,.$$

Before proving this, we quickly work out the trivial upper bound (to see what we're trying to beat). Fix an enumeration $B = \{b_1, b_2, \ldots, b_\ell\}$. Then

$$B + X = \bigcup_i \Big(\{b_i\} + X\Big),$$

whence

$$|A+B+X| \leq \sum_i \Big|A + \{b_i\} + X\Big| = \sum_i \Big|A+X\Big| = \sum_i K_0|X| = K_0|B|\,|X|.$$

This is much weaker than what we're trying to prove (and is too weak to work in the proof of Plünnecke-Ruzsa). Note that in the above estimates, only one involves an inequality! This tells us what the problem is: the sets $A + \{b_i\} + X$ potentially have a lot of overlap we're ignoring.

In the proof below, we'll get around this in two steps. First, we construct sets X_i which approximate $\{b_i\} + X$, but which are disjoint. Next, when considering the set $A+B+X$, we try to remove any new overlap in the sets $A + X_i$.

Proof. Fix an enumeration $B = \{b_1, b_2, \ldots, b_\ell\}$. Define the following sets recursively

$$\begin{aligned}
X_1 &= \{b_1\} + X,\\
X_2 &= (\{b_2\} + X) \setminus X_1\\
&\vdots\\
X_j &= (\{b_j\} + X) \setminus \bigsqcup_{i=1}^{j-1} X_i.
\end{aligned}$$

(Here $\sqcup$ denotes the disjoint union.) These sets clearly form a partition of $B+X$, i.e.

$$B + X = \bigsqcup_{i=1}^{\ell} X_i.$$

This implies

$$A + B + X = \bigcup_{i=1}^{\ell} (A + X_i),$$

but the sets $A + X_i$ have too much overlap for the above to be useful. However, we can do better:

$$A + B + X = \bigcup_{i=1}^{\ell} \Big((A + X_i) \setminus (A + Y_i) \Big), \tag{1}$$

where $Y_i = (\{b_i\} + X) \setminus X_i$. To see this, we start by observing the following.

Exercise 1. If $y \in Y_i$ for some $i \geq 2$, then $y \in X_j$ for some $j < i$.

Exercise 2. Prove that

$$A + B + X \subseteq \bigcup_{i=1}^{\ell} \Big((A + X_i) \setminus (A + Y_i) \Big),$$

[Hint: Given $s \in A + B + X$, consider the least m such that $s \in A + X_m$.]

Since $X_i \cap Y_i = \emptyset$, it is unlikely that $A + Y_i$ is entirely contained in $A + X_i$. This makes it difficult to appreciate how much of the overlap we're removing in (1). However, observe that

$$A + B + X \subseteq \bigcup_{i=1}^{\ell} \Big((A + X_i) \setminus (A + Y_i) \Big) \subseteq \bigcup_{i=1}^{\ell} \Big((A + \{b_i\} + X) \setminus (A + Y_i) \Big),$$

and now we have $A + Y_i \subseteq A + \{b_i\} + X$. This tells us that

$$\begin{aligned} |A + B + X| &\leq \sum_i \Big(|A + \{b_i\} + X| - |A + Y_i| \Big) \\ &= \sum_i \Big(|A + X| - |A + Y_i - \{b_i\}| \Big) \end{aligned}$$

Now on the one hand, $Y_i - \{b_i\} \subseteq X$, so by definition of K_0 we have

$$|A + (Y_i - \{b_i\})| \geq K_0 |Y_i - \{b_i\}|.$$

On the other hand, $|A + X| = K_0 |X|$. We deduce that

$$\begin{aligned} |A + B + X| &\leq K_0 \sum_i \Big(|X| - |Y_i - \{b_i\}| \Big) \\ &= K_0 \sum_i \Big(|X + \{b_i\}| - |Y_i| \Big) \\ &= K_0 \sum_i |X_i| \\ &= K_0 \, |B + X|. \end{aligned}$$

□

Exercise 3. Modify the above proof to prove the following generalization: Suppose that A and A' are finite subsets of an abelian group $(G, +)$, with $|A| = |A'|$. If $|A + A'| \leq K \, |A|$, then $|mA - nA| \leq K^{m+n} \, |A|$.

(Note: in practice, A' is usually taken to be A or $-A$.)

* * *
* *

As mentioned, Plünnecke-Ruzsa will play a key role in the proof of the Frieman-Ruzsa Theorem. As a warm-up to Freiman-Ruzsa, we first prove a beautiful result due to Ruzsa: we show that in any abelian group of bounded torsion, the only sets of small doubling are essentially subgroups. More precisely:

Theorem 2 (Ruzsa)**.** Suppose $(G,+)$ is an abelian group with exponent* r, and $A \subseteq G$ has small doubling, say, $|A+A| \leq K\,|A|$. Then there exists a subgroup $H \leq G$ such that

$$H \supseteq A \qquad \text{and} \qquad |H| \ll_{r,K} |A|\,.$$

Remark. Recall that the subscripts on the $\ll$ indicate that the implicit constant is allowed to depend on r and K, but on *nothing else*. In particular, the constant does not depend on $|A|$ at all. Thus, the result asserts that if A has small doubling, then it's possible to tack a few elements onto A to make it into a subgroup. (Note that one can make *any* set into a subgroup by adding elements to it; the point of this theorem is that one doesn't have to add many element to do so, so long as the set has small doubling.)

Before proceeding to the formal proof, let me sketch the strategy. Recall that $\langle A\rangle$ denotes the subgroup of G generated by A (i.e. the smallest subgroup of G containing A). Given A, how does one actually generate $\langle A\rangle$? By adding and subtracting elements of A from each other until you stop getting new elements. In other words,

$$\langle A\rangle = \bigcup_{m,n\geq 0} (mA - nA).$$

In particular, $A - A \subseteq \langle A\rangle$, but as you can see from above, $|A-A|$ is typically *much* smaller than $\langle A\rangle$. It is therefore somewhat surprising that we can approximate a reverse inclusion: we will construct a small set X such that $\langle A\rangle \subseteq (A-A) + \langle X\rangle$. Because X is small and G has bounded torsion, $|\langle X\rangle|$ must itself be fairly small, whence $|\langle A\rangle| \approx |A-A|$. But if A has small doubling, then $|A-A| \approx |A|$, so we deduce that $|\langle A\rangle| \approx |A|$ as claimed. It is worth pointing out that all of this strongly uses the hypotheses of the theorem; for example, the fact that we can construct a small X depends on the assumption that A has small doubling.

Proof. We shall prove the theorem for the special case where A is symmetric (i.e. $A = -A$); the proof of the general case is left as an exercise (see below).

Choose $X \subseteq 3A$ to be maximal such that the sets $A + \{x\}$ are pairwise disjoint over all $x \in X$.

Exercise 4. Prove that $3A \subseteq 2A + X$. [*Hint: Pick an arbitrary $t \in 3A$. Then $A+\{t\}$ must intersect one of the sets $A+\{x\}$ (why?). Conclude.*]

Adding A to both sides and simplifying, we find

$$4A \subseteq 3A + X \subseteq 2A + 2X.$$

Adding A to both sides of this inclusion and simplifying yields

$$5A \subseteq 3A + 2X \subseteq 2A + 3X.$$

Continuing this process, we obtain

$$nA \subseteq 2A + (n-2)X \tag{2}$$

for any $n \geq 3$.

Exercise 5. Prove that $\langle A\rangle = \bigcup_{n\geq 3} nA$.

Taking the union of the inclusions (2) over all $n \geq 3$, we deduce that

$$\langle A\rangle \subseteq 2A + \langle X\rangle.$$

Exercise 6. Prove that $|\langle X\rangle| \leq r^{|X|}$. Deduce that

$$|\langle A\rangle| \leq K r^{|X|}\,|A|.$$

To conclude the proof, it suffices to show that $|X| \ll_{K,r} 1$, i.e. that the size of X does not depend on the size of A. (Note that this is a pretty fantastic claim, since X is defined in terms of A!) Since $X \subseteq 3A$, it is tempting to applying Plünnecke-Ruzsa directly, but this only gives the bound $|X| \leq K^3|A|$, which is much too weak for our purposes. The following exercise shows that we can do much better.

*Recall that the *exponent* of a group is the smallest positive integer e such that $\underbrace{g+g+\cdots+g}_{e} = 0$ for any $g \in G$.

Exercise 7. Prove that $|X| \leq K^4$. [*Hint: Apply Plünnecke-Ruzsa to the set* $A + X$.]

Putting all the above together, we conclude that

$$|\langle A\rangle| \leq K\, r^{K^4}\, |A|.$$

This concludes the proof of Ruzsa's theorem for symmetric A. For the general case, see the exercise below. □

Exercise 8. Prove the general case of the theorem (where A is not symmetric). [*Hint: Let* $X \subseteq 2A - A$ *be maximal such that* $A + \{x\}$ *are all disjoint.*]

Note that we did better than simply prove $|H| \ll_{r,K} |A|$; we've shown that $|H| \leq K r^{K^4} |A|$. Is this bound optimal?

Conjecture 1 (Ruzsa)**.** Ruzsa's Theorem holds with $|H| \leq r^{CK} |A|$, for some constant C.

This conjecture is best-possible, as can be seen by the following simple example. Let p be some prime number and consider $G = (\mathbb{F}_p^n, +)$. This is an abelian group with exponent r. Let U, V be two subgroups such that $U \cap V = \{0\}$. Let $V' = \{v_1, \ldots, v_\ell\}$ be a set of linearly independent vectors from V. Take $A := U \times V'$, so that $|A| = \ell\, |U|$. Since $A + A = U \times \{v_i + v_j : 1 \leq i \leq j \leq \ell\}$, we have $|A + A| = |U| \cdot \frac{1}{2}\ell(\ell + 1)$. Thus,

$$\frac{|A + A|}{|A|} = \frac{1}{2}(\ell + 1).$$

However, it is easy to see that

$$\langle A\rangle = U \times \operatorname{span} V' = U \times (\mathbb{F}_p v_1 + \mathbb{F}_p v_2 + \cdots + \mathbb{F}_p v_\ell)$$

so that

$$|\langle A\rangle| = |U| \cdot p^\ell = \frac{p^\ell}{\ell}\, |A|\,.$$

Now, simply choose $\ell = 2K - 1$. Since $\langle A\rangle$ is the smallest subgroup containing A, we must have

$$H \geq \frac{p^{2K-1}}{2K - 1}\, |A|\,.$$

This shows that the bound in Ruzsa's conjecture is in optimal form. In 2012, Lovett and Zohar showed that the conjecture holds for any prime exponent.

We conclude by discussing an open question which has recently generated considerable interest.

Conjecture 2 (Polynomial Freiman-Ruzsa)**.** Let $(G, +)$ be an abelian group with exponent r. Let $A \subseteq G$. If $|A + A| \leq K\, |A|$, then there exists a constant $C_r > 0$ and a subset $A' \subseteq A$ such that

- $|A'| \geq \frac{1}{K^C}\, |A|$, and
- $|\langle A'\rangle| \leq K^C\, |A'|\,.$

The way to think about this theorem is that A' is simply A minus a small number of "throw-away" elements. As we've seen with our example above, if we restrict ourselves to A, the bound must be at least exponential in K. Polynomial Freiman-Ruzsa conjectures that if we allow ourselves to throw away some small number of elements from A, we can improve the bound to being polynomial in K. This conjecture, if true, would have significant consequences (both within additive combinatorics and in applications to computer science).