Additive Combinatorics Lecture 6

Leo Goldmakher
Scribe: Gal Gross

Feb. 14th, 2014

Recall that $|[n]+[n]| = |[n]-[n]|$, where $[n] := \{1, 2, \dots, n\}$. Is it always the case that $A + A = A - A$? We came up with the counterexample $A = \{1, 2, 4\}$, where $|A + A| = 6$ but $|A - A| = 7$. In this case the difference set is larger than the sumset. What about in reverse? Does there exist $A \subset \mathbb{Z}$ for which $|A - A| < |A + A|$? Some playing around led to no such examples, and one might be tempted to conjecture that $|A + A| \leq |A - A|$ for all finite sets $A \subset \mathbb{Z}$. We even came up with a heuristic argument for why this might be the case: addition is commutative, while subtraction is not, so where $A + A$ automatically has many coincidences which $A - A$ does not.

Unfortunately, this argument is not rigorous. In fact, one can make an equally convincing argument in reverse: in $A - A$ there are many ways to make 0, so there are automatically many coincidences in $A - A$. This is exactly what happens for the set $A = \{0, 2, 3, 4, 7, 11, 12, 14\}$ (due to John Conway): we have $|A + A| = 26$ but $|A - A| = 25$.

Nonetheless, empirically, sets for which the sumset is larger than the difference set are rare. This led us to the following questions (some of which may be open):

1. Find the smallest set A such that $|A + A| > |A - A|$.
2. Is it true that for "most" $A \subseteq \mathbb{Z}$ we have $|A + A| \leq |A - A|$?
3. Are there infinitely many fundamentally different $A \subseteq \mathbb{Z}$ such that $|A + A| > |A - A|$?
4. Classify all $A \subseteq \mathbb{Z}$ such that $|A + A| > |A - A|$.
5. Is it true that for any $A \subseteq \mathbb{Z}$ we have $\Big||A - A| - |A + A|\Big| \ll 1$? [**Update:** The answer is NO!]

* * *
* *

We went back to discussing the general case of Abelian groups. For the remainder of the lecture we take $(G, +)$ to be an abelian group and A, B, C, X, Y, Z to be finite subsets of G.

Recall that the DOUBLING CONSTANT of A is defined to be $|A + A| / |A|$. Some people use the same name for $|A - A| / |A|$. This is unfortunate, since (as we saw above) the relationship between these two quantities is mysterious. Nonetheless, it turns out that there is a relationship between them:

Proposition 1. $\frac{|A-A|}{|A|} \leq \left(\frac{|A+A|}{|A|}\right)^2$ for all finite $A \subseteq G$.

We will deduce this from a more general relation:

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

Written in this form, the inequality looks a lot less natural than the one in the Proposition. After a bit of playing around, we realized there was a more symmetric way of writing the general inequality.

Theorem 1 (Ruzsa's triangle inequality)**.** For all finite sets $X, Y, Z \subseteq G$ we have

$$\frac{|X-Z|}{\sqrt{|X|}\sqrt{|Z|}} \leq \frac{|X-Y|}{\sqrt{|X|}\sqrt{|Y|}} \cdot \frac{|Y-Z|}{\sqrt{|Y|}\sqrt{|Z|}}.$$

Although this does look a bit reminiscent of a triangle inequality, the name of the theorem may strike you as strange. We quickly realized that taking logarithms makes this a legitimate triangle inequality. More precisely:

Definition (Ruzsa Distance)**.** For any $A, B \subseteq G$ we define

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

Exercise 1. Prove that $d(\cdot,\cdot)$ satisfies the following properties of a metric:

1. Non-negativity. $d(A,B) \geq 0$.
2. Symmetry. $d(A,B) = d(B,A)$.
3. Triangle Inequality. $d(A,B) \leq d(A,C) + d(C,B)$. [*We did this collaboratively in class. In case you missed it, here's a hint: a good way to prove $|X| \leq |Y|$ is find an injection mapping $X \hookrightarrow Y$.*]
4. Why isn't the Ruzsa distance a metric?

Just to illustrate the utility of the triangle inequality, we give a short proof of Proposition 1. We have

$$\frac{|A-A|}{|A|} = e^{d(A,A)} \leq e^{d(A,-A)+d(-A,A)} = \left(e^{d(A,-A)}\right)^2 = \left(\frac{|A+A|}{|A|}\right)^2.$$

Note that an immediate corollary of Proposition 1 is that if $|A+A| \leq K|A|$, then $|A-A| \leq K^2|A|$. It turns out that this can be generalized:

Theorem 2 (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 $kA = \underbrace{A + A + \cdots + A}_{k \text{ times}}$.

The original proof of this theorem was long and complicated, using deep results from graph theory. Several years ago, Giorgis Petridis (then a PhD student of Gowers) discovered a simple and elegant combinatorial proof which we give below.

Proof of Plünnecke-Ruzsa. Pick the nonempty set $X \subseteq A$ which minimizes the quotient $\frac{|A+X|}{|X|}$; say,

$$\frac{|A+X|}{|X|} = K_0.$$

In particular, note that $K_0 \leq K$. Petridis observed that this X enjoys the following remarkable property.

Lemma. For all $B \subseteq G$, we have $|A+B+X| \leq K_0\,|B+X|$.

We will prove this lemma next class. For the moment, we deduce Plünnecke-Ruzsa from it. We have

$$\begin{aligned} |mA| \leq |mA+X| &= |A+(m-1)A+X| \\ &\leq K_0\,|(m-1)A+X| \leq \cdots \leq K_0^{m-1}\,|A+X| \\ &\leq K_0^m\,|X|\,. \end{aligned}$$

Thus, if $n = 0$, we are done. Otherwise we use the same technique to deduce

$$|nA| \leq K_0^n |X|.$$

Now, we wish to find an upper bound on $|mA - nA|$. This suggests using the Ruzsa triangle inequality to bound $d(mA, nA) \leq d(mA, \cdot) + d(\cdot, nA)$. What can we put in place of $\cdot$? Examining our above bounds, we see that we not only bounded $|mA|$, we also bounded $|mA + X|$. In other words, we know something about the distance from mA to $-X$! Taking this hint, we consider Ruzsa's triangle inequality:

$$d(mA, nA) \leq d(mA, -X) + d(-X, nA).$$

Expanding and simplifying yields

$$|mA - nA| \leq \frac{|mA + X| \cdot |nA + X|}{|X|} \leq \frac{K_0^m |X| \cdot K_0^n |X|}{|X|} = K_0^{m+n} |X| \leq K^{m+n} |A|. \qquad \square$$

This completes the proof of the Plünnecke-Ruzsa theorem, up to Petridis' lemma. At the end of last class, we collaboratively came up with a proof of the lemma. We will write down a tidied-up version of the proof next lecture.