Additive Combinatorics Lecture 3

Leo Goldmakher

Scribe: Gal Gross

Jan. 24th, 2014

Today we are going to complete the proof of Solymosi's theorem. While the theorem is valid over $\mathbb{C}$, we shall only prove it over $\mathbb{R}_{>0}$. For ease of reference:

Theorem (Solymosi, 2009)**.** For all $A, B \subseteq \mathbb{R}_{>0}$,

$$|A \cdot B| \cdot |A + B| \cdot |B + B| \gg \frac{|A|^2 |B|^2}{\log(|A| |B|)}.$$

Last time we defined the notation $r_{A \oplus B}(x)$ and noted the first key insight in the proof:

$$\sum_{x \in A \cdot B} r_{A \cdot B}(x)^2 = \sum_{m \in B \div A} r_{B \div A}(m)^2. \tag{1}$$

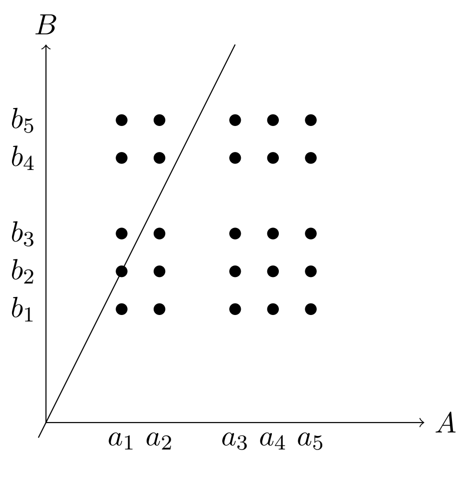
We then established the following lower bound using Cauchy-Schwarz:

$$\sum_{x \in A \cdot B} r_{A \cdot B}(x)^2 \geq \frac{|A|^2 |B|^2}{|A \cdot B|}. \tag{2}$$

It therefore suffices to prove that

$$\sum_{m \in B \div A} r_{B \div A}(m)^2 \ll |A + A| \cdot |B + B| \cdot \log(|A|). \tag{3}$$

The significance of the identity (1) is that it admits a geometric interpretation: $r_{B \div A}(m)$ enumerates the number of $(A \times B)$-lattice points on the line $\mathscr{L}_m$ through the origin with slope m. In the example below A, B are sets of positive real numbers having 5 elements each. The lattice $A \times B$ is illustrated as well as the line $\mathscr{L}_2$ going through the point (a_1, b_2). Since $\mathscr{L}_2$ only contains a single lattice point, we see that $r_{B \div A}(2) = 1$.



Proof of Solymosi's Theorem Continued. Recall that we wish to prove the upper bound (3). For aesthetic reasons, set

$$r(m) := r_{B \div A}(m)$$

for the remainder of the proof.

One difficulty in analyzing the sum (3) is that $r(m)$ varies drastically from one line to the next. To remedy this, we employ a simple but effective trick: divide and conquer. We partition the sum into pieces in such a way that within each piece, $r(m)$ doesn't vary too much:

$$\sum_{m \in B \div A} r(m)^2 = \sum_j \sum_{\substack{m \in B \div A \\ 2^{j-1} < r(m) \leq 2^j}} r(m)^2 \tag{4}$$

Suppose the inner sum on the RHS of (4) is maximized at $j = J$.

Exercise 1. Carefully prove that

$$\sum_{m \in B \div A} r(m)^2 \ll \log(|A|) \sum_{\substack{m \in B \div A \\ 2^{J-1} < r(m) \leq 2^J}} r(m)^2 \tag{5}$$

Let $\mathcal{M} := \{m \in B \div A \ : \ 2^{J-1} < r(m) \leq 2^J\}$. To conclude the proof of Solymosi's theorem, it suffices to show that

$$\sum_{m \in \mathcal{M}} r(m)^2 \ll |A + A| \cdot |B + B|.$$

Observe that for any $m, m' \in \mathcal{M}$ we have $r(m) \leq 2r(m')$; by symmetry of m and m', we deduce that $r(m) \asymp r(m')$. Now, $\mathcal{M}$ is a finite set of positive numbers; enumerate its elements

$$\mathcal{M} = \{m_1, m_2, \ldots, m_n\},$$

where $m_i < m_{i+1}$ for all i. We have

$$\sum_{i \leq n} r(m)^2 \ll \sum_{i \leq n} r(m_i) \cdot r(m_{i+1}). \tag{6}$$

Recall that $r(m)$ has a geometric interpretation: it is the number of lattice points on the line $\mathscr{L}_m$. Abusing notation, we take $\mathscr{L}_m$ to be the set of lattice points lying on the line, i.e.

$$\mathscr{L}_m := \{(x, y) \in A \times B \ : \ y = mx\}.$$

Solymosi's second key insight concerns the geometry of the sumset $\mathscr{L}_{m_i} + \mathscr{L}_{m_{i+1}}$.

Exercise 2. Show that:

(a) Any point in $\mathscr{L}_{m_i} + \mathscr{L}_{m_{i+1}}$ lies in between the lines $\mathscr{L}_{m_i}$ and $\mathscr{L}_{m_{i+1}}$. Conclude that if $i \neq j$ then $(\mathscr{L}_{m_i} + \mathscr{L}_{m_{i+1}}) \cap (\mathscr{L}_{m_j} + \mathscr{L}_{m_{j+1}}) = \emptyset$.

(b) For all $p \in \mathscr{L}_m + \mathscr{L}_{m'}$, we have $r_{\mathscr{L}_m + \mathscr{L}_{m'}}(p) = 1$.

(c) Conclude that $|\mathscr{L}_m + \mathscr{L}_{m'}| = |\mathscr{L}_m| \cdot |\mathscr{L}_{m'}|$.

Applying the above exercise to (6), we have ("$\sqcup$" denotes disjoint union)

$$\begin{aligned}\sum_{i \leq n} |\mathscr{L}_{m_i}|^2 \ll \sum_{i \leq n} |\mathscr{L}_{m_i}| \, |\mathscr{L}_{m_{i+1}}| &= \sum_{i \leq n} |\mathscr{L}_{m_i} + \mathscr{L}_{m_{i+1}}| \\ &= \left| \bigsqcup_{i \leq n} (\mathscr{L}_{m_i} + \mathscr{L}_{m_{i+1}}) \right| \leq |A \times B + A \times B| = |A + A| \cdot |B + B|.\end{aligned}$$

$\square$

Exercise 3. Justify the inequality step ("$\leq$") in the calculation above. Can you come up with an example of A and B where it's a tight bound? What about where it's a poor bound?

Exercise 4. Above, we were a bit sloppy with the 'extra' term $\mathscr{L}_{m_{n+1}}$. Fix the proof to account for this. [*One way to do this is to define* $\mathscr{L}_{m_{n+1}}$ *to be* $\{0\} \times B$. *But there are other ways as well.*]

* * *
* *

If you reflect back to our first lecture you'd realize that we were focusing on sets of integers; consider Erdős-Szemerédi Conjecture for example. It turns out, however, that a more natural setting for the type of questions we've been asking are arbitrary fields and abelian groups.

For instance, let $(G, +)$ be an abelian group. Let $A \subseteq G$ be finite. How big is $|A+A|$? We have the trivial bounds $|A| \leq |A+A| \leq \frac{1}{2}|A|(|A|+1)$. When is the lower bound tight? In class we interactively came up with the following:

Proposition. Given an abelian group $(G, +)$ and a finite subset $A \subseteq G$, we have $|A+A| = |A|$ iff A is a coset of a subgroup of G.

Exercise 5. Prove the above proposition.

Exercise 6. Let $(G, +)$ be an abelian group, and let $A \subseteq G$ be finite. Prove that $|A-A| = |A|$ iff A is a coset of a subgroup of G.

Note that cosets of subgroups of $\mathbb{Z}$ are precisely arithmetic progressions. Thus the proposition above gives some intuition for the Freiman-Rusza theorem. More generally, suppose that $|A+A| \leq K|A|$ for some constant K (called the "doubling constant" of A). What can we say about A now? If K isn't too big, then A should hopefully "look like" a coset.

Until very recently, no one new how to think cohesively about additive combinatorics. Ben Green (one of the pioneers in the field) commented on this in a 2009 paper. However, a current viewpoint on the field is the following: *Additive Combinatorics is the study of approximate algebraic structures.* For example, one can characterize cosets of subgroups by the condition that they satisfy $|A+A| = |A|$. What happens when one weakens this to $|A+A| \leq K|A|$? Then A becomes a coset of an approximate subgroup.

* * *
* *

In the final part of the lecture, we considered a lovely result due to Izabella Łaba (who, like Solymosi, is a professor at UBC).

Theorem (Łaba, 2001)**.** Let G be an abelian group. If $A \subseteq G$ is a finite subset such that $|A-A| < \frac{3}{2}|A|$, then $A-A$ is a subgroup of G.

Exercise 7. Show (by example) that the doubling constant $\frac{3}{2}$ in Łaba's Theorem is tight.

Next, we outlined a proof of this result.

Exercise 8. Show that:

1. $\forall x \in A-A\,,\ |A \cap (A+x)| > \frac{1}{2}|A|$. Conclude that $(A+x) \cap (A+y) \neq \emptyset$ for any $x, y \in A-A$.
2. Show that $A-A$ is closed under differences. Conclude that it is a subgroup of G.