C3.10 Additive and Combinatorial NT
Lecture 9: Sumset estimates and Ruzsa's covering lemma

Joni Teräväinen

Mathematical Institute

Sumsets

If G is an abelian group and $A, B \subset G$ are any finite sets, define

$$A + B := \{a + b : \ a \in A, b \in B\}.$$

Similarly define $A + B + C := (A + B) + C$ and $kA = A + \cdots + A$ (k times). Also define

$$A - B := \{a - b : \ a \in A, b \in B\}$$

Question

If $A, B \subset \mathbb{Z}$ and $|A| = m$, $|B| = n$, how large or small can $A + B$ be?

Sumsets

Question

If $A, B \subset \mathbb{Z}$ and $|A| = m$, $|B| = n$, how large or small can $A + B$ be?

Answer. We can have $|A + B| = |A||B| = mn$; take $A = \{10^k : 1 \leq k \leq m\}$, $B = \{10^k : m + 1 \leq k \leq m + n\}$.

We can have $|A + B| = |A| + |B| - 1 = m + n - 1$; take $A = [1, m] \cap \mathbb{Z}$, $B = [1, n] \cap \mathbb{Z}$.

We always have $|A + B| \geq m + n - 1$: If $A = \{a_i\}$, $B = \{b_i\}$, then

$$a_1 + b_1 < a_2 + b_1 < \cdots < a_m + b_1 < a_m + b_2 < \cdots < a_m + b_n.$$

Sets of small doubling

If $|A+A| \leq K|A|$, we say A has *doubling constant* K.

From the previous slide, if $P \subset \mathbb{Z}$ is an arithmetic progression, then $|P+P| = 2|P| - 1$.

More generally, let P be a *generalized arithmetic progression*

$$P = \{a_0 + a_1 n_1 + a_2 n_2 + \cdots + a_k n_k : \ 0 \leq n_i < N_i\}.$$

We say A has *dimension* k. The size of P is $\leq N_1 \cdots N_k$.

Note that
$P + P \subset \{a_0 + a_1 n_1 + a_2 n_2 + \cdots + a_k n_k : \ 0 \leq n_i < 2N_i\}$, so
$|P+P| \leq 2^d |P|$.

More generally, if $A \subset P$ and $|A| \geq \delta N_1 \cdots N_k$, then
$|A+A| \leq |P+P| \leq 2^d |P| \leq 2^d \delta^{-1} |A|$.

Question

What can be said about arbitrary sets with doubling constant K?

Freiman's theorem

Question

What can be said about arbitrary sets with doubling constant K?

Theorem (Freiman)

Let $A \subset \mathbb{Z}$ satisfy $|A+A| \leq K|A|$. Then there exists a generalized arithmetic progression P of dimension $\ll_K 1$ and of size $|P| \ll_K |A|$ such that $A \subset P$.

Call a set *additive* if it is a subset of an abelian group. Freiman's theorem can be generalized to additive sets, with generalized progressions replaced with cosets progressions. In this course, we will limit ourselves to the integer case.

Ruzsa's triangle inequality

Lemma (Ruzsa's triangle inequality)

Let U, V, W be additive sets. Then

$$|V - W||U| \leq |V - U||U - W|.$$

Question

Why is this a triangle inequality?

Answer. Denoting $d(U, V) := \log(|U - V|/(|U|^{1/2}|V|^{1/2}))$, it says $d(U, W) \leq d(U, V) + d(V, W)$.

Ruzsa's triangle inequality

Lemma (Ruzsa's triangle inequality)

Let U, V, W be additive sets. Then

$$|V - W||U| \leq |V - U||U - W|.$$

Proof: It suffices to define an injection $\phi : (V - W) \times U \to (V - U) \times (U - W)$. For any $d \in V - W$, select $v_d \in V, w_d \in W$ such that $d = v_d - w_d$. Then define

$$\phi(d, u) := (v_d - u, u - w_d)$$

for each $d \in V - W$ and $u \in U$.

Now let $(x, y) \in \mathrm{im}(\phi) \subset (V - U) \times (U - W)$. If $\phi(d, u) = (x, y)$ then $x + y = (v_d - u) + (u - w_d) = v_d - w_d = d$, so the value of d is determined. Hence also v_d and w_d are determined from (x, y). And we also determine u as $u = -x + v_d$. □

Ruzsa's covering lemma

Lemma (Ruzsa's covering lemma)

Let A, B be additive sets. Suppose that $|A+B| \leq K|A|$. Then there exists a set X with $|X| \leq K$ such that

$$B \subset A - A + X.$$

Proof: Let $X \subset B$ be the largest subset of B for which the sets $\{A + x : x \in X\}$ are disjoint. The union of the sets $A + x$ sets contains exactly $|A||X|$ elements, and $A + x \subset A + B$. Therefore $|X| \leq K$. By maximality of X, for every $b \in B$ there is $x \in X$ such that $A + b \cap A + x \neq \emptyset$. This means that, $b \in A - A + x$. Hence, $B \subset (A - A) + X$. □