C3.10 Additive and Combinatorial NT
Lecture 11: Freiman homomorphisms and Ruzsa's model lemma

Joni Teräväinen

Mathematical Institute

Our eventual goal is to prove

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 $A \subset P$.

In this lecture, we will prove Ruzsa's model lemma, which is an ingredient for this.

Freiman isomorphisms

Definition (Freiman homomorphisms)

Let A, B be additive sets, and let $s \geq 2$. We say that $\phi : A \to B$ is a *Freiman s-homomorphism* if

$$a_1 + \cdots + a_s = a_1' + \cdots + a_s', \quad a_i, a_i' \in A$$
$$\Longrightarrow \phi(a_1) + \cdots + \phi(a_s) = \phi(a_1') + \cdots + \phi(a_s').$$

Definition (Freiman isomorphisms)

We say that $\phi : A \to B$ is a *Freiman s-isomorphism* if ϕ is a Freiman s-homomorphism, and ϕ^{-1} exists and is also a Freiman s-homomorphism.

Examples

Examples of Freiman s-homomorphisms:

- Any group homomorphism $\phi : G_1 \to G_2$, G_i abelian.
- Any map $\phi : A \to B$, where A contains no nontrivial additive relations.
- The canonical map $\pi_m : [1, m] \cap \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ ($x \mapsto x \pmod{m}$) is a Freiman s-homomorphism, and is also a Freiman isomorphism if m is a prime large enough in terms of s.
- The canonical map $\phi : \{0, 1\}^n \to (\mathbb{Z}/2\mathbb{Z})^n$ ($(x_i) \mapsto (x_i \pmod{2})$) is a Freiman s-homomorphism and a bijection, but is not a Freiman 2-isomorphism.

Lemma (Basic properties of Freiman isomorphisms)

1. If $\phi : A \to B$, $\psi : B \to C$ are Freiman s-homomorphisms, so is $\psi \circ \phi : A \to C$.
2. If ϕ is a Freiman s-homomorphism, it is also a Freiman s'-homomorphism, $s' < s$.
3. If $\phi : A \to B$ is a Freiman s-homomorphism, for any $k, \ell \geq 0$ it induces a Freiman $\lfloor s/(k+\ell) \rfloor$-homomorphism $kA - \ell A \to kB - \ell B$.
4. All of the above holds for isomorphisms as well.
5. If P is a GAP and $\phi : P \to B$ is a Freiman 2-isomorphism, then $\phi(B)$ is a GAP of the same dimension.
6. $\pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is a Freiman s-isomorphism when restricted to $[t, t + m/s)$.

Proof: (1) Trivial.
(2) Trivial, since we can consider relations
$a_1 + \cdots + a_{s'} + 0 + \cdots + 0 = a'_1 + \cdots + a'_{s'} + 0 + \cdots + 0.$
(3) Define a map $\tilde{\phi} : kA - \ell A \to kB - \ell B$ by

$$\tilde{\phi}(a_1 + \cdots + a_k - a'_1 - \cdots a'_\ell) = \phi(a_1) + \cdots + \phi(a_k) - \phi(a'_1) - \cdots - \phi(a'_\ell).$$

One easily checks that $\tilde{\phi}$ is well-defined and a Freiman homomorphism of order $\lfloor s/(k+\ell) \rfloor$.
(4) Similar to the above.
(5) Let $P = \{x_0 + \ell_1 x_1 + \cdots + \ell_k x_k : 0 \le \ell_i < L_i\}$. Define y_i by $y_0 = \phi(x_0)$, $y_0 + y_i = \phi(x_0 + x_i)$. We claim that $\phi(x_0 + ... + \ell_k x_k) = y_0 + ... + \ell_k y_k$. For this use induction on $\ell_1 + \cdots + \ell_k$.
(6) π_m is clearly a Freiman homomorphism of any order. By translation, we may assume that $t = 0$. Now, note that since $a_i \in [0, m/s)$, we have $a_1 + \cdots + a_s \pmod{m} = a_1 + \cdots + a_s$. □

Ruzsa's model lemma

Proposition (Ruzsa)

Let $A \subset \mathbb{Z}$ be a finite set and $s \geq 2$ is an integer. Let $m \geq |sA - sA|$. Then there $A' \subset A$ with $|A'| \geq |A|/s$ which is Freiman s-isomorphic to a subset of $\mathbb{Z}/m\mathbb{Z}$.

Proof. By translation, we may assume that A consists of positive integers. Let q be a large enough prime number. Then $\pi_q : A \to \pi_q(A) \subset \mathbb{Z}/q\mathbb{Z}$ is a Freiman s-isomorphism.
We will choose $\phi = \phi_\lambda$ for some $\lambda \in (\mathbb{Z}/q\mathbb{Z})^*$, where $\phi_\lambda := \pi_m \circ \pi_q^{-1} \circ D_\lambda \circ \pi_q$ is given by

$$\mathbb{Z} \xrightarrow{\pi_q} \mathbb{Z}/q\mathbb{Z} \xrightarrow{D_\lambda} \mathbb{Z}/q\mathbb{Z} \xrightarrow{\pi_q^{-1}} \{1, \ldots, q\} \xrightarrow{\pi_m} \mathbb{Z}/m\mathbb{Z},$$

where $D_\lambda(x) = \lambda x$.

Here π_q, D_λ and π_m are Freiman homomorphisms of any order. By part (6) of the Lemma, π_q^{-1} is a Freiman homomorphism on any $\pi_q(I_j)$, $j = 0, 1, \ldots, s-1$, where $I_j := \{n \in \mathbb{Z} : \frac{jq}{s} < n \leq \frac{(j+1)q}{s}\}$. Since the $\pi_q(I_j)$ partition $\mathbb{Z}/q\mathbb{Z}$, it follows from the pigeonhole principle that for each λ there is some j such that

$$A'_\lambda := \{a \in A : D_\lambda(\pi_q(a)) \in \pi_q(I_j)\},$$

satisfies $|A'_\lambda| \geq |A|/s$. Thus, ϕ_λ is a Freiman s-homomorphism on A'_λ.

Proof of Ruzsa's model lemma

We need to show that there is a choice of λ for which ϕ_λ is invertible when restricted to A'_λ, and for which its inverse is also a Freiman s-homomorphism.

If this is not true, then for every λ there exists $d = d_\lambda \neq 0$ such that for some $a_i, a'_i \in A_\lambda$ we have $d = a_1 + ... + a_s - a'_1 - ... - a'_s$ and $\pi_m(\pi_q^{-1}(\lambda d)) = 0$.

Fix d and say that λ is *bad for d* if this happens.

Note that $\pi_q^{-1} \circ \pi_q(\lambda d)$ takes every value in $\{1, ..., q-1\}$ exactly once as λ varies. The number of $x \in \{1, .., q-1\}$ such that $\pi_m(x) = 0$ is $\leq (q-1)/m$. Since d takes values in $sA - sA \setminus \{0\}$, we have

$$|\bigcup_d \{\lambda \in (\mathbb{Z}/q\mathbb{Z})^* : \lambda \text{ bad for } d\}| \leq \frac{q-1}{m} \cdot (|sA - sA| - 1) < q - 1,$$

so a suitable λ exists. $\square$

A corollary

The following corollary will be used in the proof of Freiman's theorem.

Corollary

Let $A \subset \mathbb{Z}$ be a finite set with doubling constant K. Then there is a prime $q \leq 2K^{16}|A|$ and a subset $A' \subset A$ with $|A'| \geq |A|/8$ such that A' is Freiman 8-isomorphic to a subset of $\mathbb{Z}/q\mathbb{Z}$.

Proof. The Plünnecke–Ruzsa inequality gives $|8A - 8A| \leq K^{16}|A|$. Now Bertrand's postulate gives that there is a prime p satisfying $|8A - 8A| \leq q \leq 2|8A - 8A| \leq 2K^{16}|A|$. By Ruzsa's model lemma there is a subset $A' \subset A$ with $|A'| \geq |A|/8$ which is Freiman 8-isomorphic to a subset of $\mathbb{Z}/q\mathbb{Z}$.