10/5 Ben Green

Freiman–Ruzsa Theorem

Let A be a finite set of integers with $\sigma(A) \leq K$.
Then there is a proper generalized arithmetic progression (GAP)

$$P = \{ x_0 + l_1 x_1 + \dots + l_d x_d : 0 \leq l_i < L_i \}$$

where dimension $d \leq K^c$ and size$(P) = L_1 \dots L_d \leq \exp(K^c)(A)$ such that $A \subseteq P$.

Remark: Apart from the issue of dependency on K, this theorem is necessary and sufficient, indeed $\sigma[P] \leq 2^d$, and so if $A \subseteq P$ is a set of size $\eta(P)$ then $\sigma(A) \leq \frac{2^d}{\eta}$.

Freiman homomorphisms and isomorphisms:

Let $s \geq 2$ be integer, and let $\varphi : A \to B$ be a map between two sets in some ambient abelian group.
Then we say that φ is a Freiman s-homomorphism if:

whenever $a_1 + \dots + a_s = a_1' + \dots + a_s'$
$\Rightarrow \varphi(a_1) + \dots + \varphi(a_s) = \varphi(a_1') + \dots + \varphi(a_s')$.

"φ preserves additive relations of length $\leq s$"!

We say φ is a Freiman s-isomorphism if φ has an inverse φ^{-1} which is also an s-hom.

NB: It is perfectly possible for φ to be a bijective Freiman homomorph. but not an isomorphism, e.g.

the obvious map $\varphi : \{0,1\}^n \longrightarrow (\mathbb{Z}/2\mathbb{Z})^n$

$$\{0,1\}^n \subset \mathbb{Z}^n$$

is a Freiman hom. of all orders, but never a Freiman isomorphism.

<u>Remark</u>: The map we used in the Behrend example

$$\varphi : \{0,\dots,L-1\}^d \longrightarrow \mathbb{Z}$$

defined by $\varphi(x_1 \dots x_d) = x_1 + (2L)x_2 + \dots + (2L)^{d-1} x_d$, is a Freiman isomorphism of order 2 onto its image.

<u>Exercise</u>: If $A \underset{2}{\cong} B$, then $(\#3\text{APs in } A) = (\#3\text{APs in } B)$.

Freiman isomorphic order 2

<u>Lemma</u>: (Basic properties of Freiman homs).

(i) If $2 \leq s' \leq s$ and $\varphi : A \to B$ is a Freiman s-hom, then it is also an s'-hom.

(ii) Suppose $\varphi : A \to B$ is a Freiman s-hom, then φ induces a Freiman s'-hom

$$\tilde{\varphi} : kA - lA \longrightarrow kB - lB \quad \text{in a natural way}$$

provided $s' \leq \dfrac{s}{|k|+|l|}$.

$$[\tilde{\varphi}(a_1 + \dots + a_k - a_1' - \dots - a_l') := \varphi(a_1) + \dots + \varphi(a_k) - \varphi(a_1') - \dots - \varphi(a_l').$$

(iii) The "unwrapping map" $\varphi : \mathbb{Z}/m\mathbb{Z} \hookrightarrow \{0,1,\dots,m-1\}$

is a Freiman s-homo. when restricted to any interval length $\leq \frac{m}{s}$.

(iv) If $P \subseteq \mathbb{Z}$ is a ~~proper~~ GAP and if $\varphi : P \to Q$ is a Freiman 2-hom.
Then Q is also a GAP of same dimension and size.

If P is proper and if φ is an isomorphism, then Q is proper and $|P| = |Q|$.

[<u>Hint</u>: If $P = \{x_0 + l_1 x_1 + \dots + l_d x_d\}$ then
$Q = \{y_0 + l_1 y_1 + \dots + l_d y_d\}$

where ~~$\varphi(x_0 + \dots + x_i)$~~ $\varphi(x_0 + x_i) = y_0 + y_i$
$\varphi(x_0) := y_0$
these define $y_0 \dots y_d$

Proof by induction on $|l_1| + \dots + |l_d|$.]

<u>Proposition</u> (Ruzsa's model lemma)

Let $A \subseteq \mathbb{Z}$ and suppose $\sigma[A] \leq K$.
Let $s \geq 2$ be an integer, and $p \geq K^c$ be a prime.
Then there is a subset $A' \subseteq A$, $|A'| \geq \frac{|A|}{s}$ which is Freiman isomorphic to a subset of $\mathbb{Z}/p\mathbb{Z}$.

<u>Proof</u>: Assume w.l.o.g that all elements of A are >0.

Let q be a large prime, $q \gg 2s \max A$.

Consider the composition

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\pi_q"] & \mathbb{Z}/q\mathbb{Z} \arrow[r, "D_\lambda", "\text{dilation by } \lambda \in (\mathbb{Z}/q\mathbb{Z})^*"'] & \mathbb{Z}/q\mathbb{Z} \arrow[r, "\psi", "\text{unwrap} \to \{0,\dots,q-1\}"'] & \mathbb{Z} \arrow[d, "\pi_p"] \\ & & & \mathbb{Z}/p\mathbb{Z} \end{tikzcd}$$

Let $\varphi := \pi_p \circ \psi \circ D_\lambda \circ \pi_q$

Note that π_q, D_λ are group homs,

and ψ is a Freiman s-hom. when restricted to any subinterval of $\mathbb{Z}/q\mathbb{Z}$ of length q/s.

Noting that the composition of Freiman s-homs is an s-hom, it follows by the Pigeonhole Principle that there is, for each λ, a set $A' \subseteq A$, $|A'| \geq \frac{|A|}{s}$ such that $\varphi|_{A'}$ is a Freiman s-hom.

What about the inverse of φ?

If φ fails to be a Freiman s-iso, then there are $a_1 \dots a_s\, a_1' \dots a_s'$

with $a_1 + \dots + a_s \neq a_1' + \dots + a_s'$, yet $\varphi(a_1) + \dots + \varphi(a_s) = \varphi(a_1') + \dots + \varphi(a_s')$. $(*)$

Fix $d = a_1 + \dots + a_s - a_1' - \dots - a_s'$, $d \neq 0$.

For how many λ does $(*)$ happen?

As λ ranges over $(\mathbb{Z}/q\mathbb{Z})^*$, λd also ranges over $(\mathbb{Z}/q\mathbb{Z})^*$

The unwrapped elements $\psi(\lambda d)$ range over $\{1 \dots q-1\}$.

The number of such elements divisible by p (i.e. $(*)$ happens) is obviously at most $\frac{q-1}{p}$.

Thus for each d, at most a proportion $\frac{1}{p}$ of possible choices of λ are "bad for d" in the sense that $(*)$ holds for some $a_1 \dots a_s a_1' \dots a_s'$ with

$d = a_1 + \dots + a_s - a_1' - \dots - a_s'$.

But there are only $|sA - sA|$ different choices of d.

This is, by <u>sumset estimates</u>, a set of size $\leq K^c_s |A|$.

Provided $p > |sA - sA|$ there is at least one good choice of λ (ie. good for all d), hence $(*)$ never happens for that λ. ∎

(5) <u>Ben Green</u> 10/5

<u>Corollary</u> Suppose $A \subseteq \mathbb{Z}$, $\delta[A] \leq K$.

Then $\exists$ subset $A' \subseteq A$, $|A'| \geq \frac{|A|}{8}$ which is Freiman 8-isomorphic to a subset of $\mathbb{Z}/p\mathbb{Z}$, for some $p \leq K^c |A|$.

Pf: Use preceding proposition and Bertrand's postulate. (always a prime between X and $2X$.) $\blacksquare$

<u>Digression</u>: Example

Heisenberg $\left\{ \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} : \begin{array}{l} 1 \leq x \leq \sqrt{p} \\ y, z \in \mathbb{Z}/p\mathbb{Z} \end{array} \right\}$

$|A \cdot A| \leq 2|A|$ but no good models for A or any large $A' \subseteq A$.

Meet Wed!