The Freiman-Ruzsa Theorem

Let G be an (additive) abelian group. If $A \subseteq G$ is a finite set we may consider the sumset $A+A = \{a+a' : a, a' \in A\}$.

Trivial Bounds: $|A| \leq |A+A| \leq \min\{\frac{1}{2}|A|(|A|+1), |G|\}$.

One would expect that the upper bound should be attained (or nearly attained) whenever A has no "special additive structure".

For example, it is certainly attained when $A = \{1, 3, 3^2, \ldots, 3^{n-1}\}$ (say).

Clarifying what exactly is meant by "special additive structure" is a deep, important and interesting question. Specifically, one is interested in describing as carefully as one can the structure of non-empty finite sets A for which $\underbrace{|A+A| \leq K|A| \text{ for some } K \in \mathbb{R}^+}_{\text{We say "A has doubling at most } K\text{"}}$.

Examples

1. • If A is a finite subgroup H of G, then $|A+A| = |A|$. The same is also true if A is some coset of H.

   • If $A \subseteq H$ with $|A| = \delta|H|$, then $A+A \subseteq H$ and $|A+A| \leq \delta^{-1}|A|$.

② Suppose $G = \mathbb{Z}$

- If A is a (finite) arithmetic progression P, then $|A+A| = 2|A|-1 \leq 2|A|$.

Again if $A \subseteq P$ with $|A| = \delta|P|$, then $|A+A| \leq 2\delta^{-1}|A|$.

More generally, we may consider so-called (d-dimensional) <u>generalized arithmetic progressions</u> (GAP), namely sets of the form

$$P = \{ x_0 + \sum_{j=1}^{d} \ell_j x_j : 0 \leq \ell_j \leq L_j \}.$$

We say that a GAP, P, is <u>proper</u> if $|P| = \prod_{j=1}^{d} L_j$. (i.e. all elements distinct)

- If A is a proper GAP P of dimension d, then $|A+A| \leq 2^d|A|$

Again, if $A \subseteq P$ with $|A| = \delta|P|$, then $|A+A| \leq 2^d\delta^{-1}|A|$.

<u>Exercise 1</u>

③ Finally, one can combine any of these examples.

- If $A_1 \subseteq G_1$ and $A_2 \subseteq G_2$ with $|A_1+A_1| \leq K_1|A_1|$ & $|A_2+A_2| \leq K_2|A_2|$, then $A_1 \times A_2 \subseteq G_1 \times G_2$ satisfies $|(A_1\times A_2)+(A_1\times A_2)| \leq K_1K_2|A_1\times A_2|$.

* It turns out, qualitatively at least, that the three examples above provide a complete description of sets with small doubling in abelian groups. *

This was established first in the case $G = \mathbb{Z}$ by Freiman in 1973.

Freiman's Theorem (Qualitative Form)

Let $A \subseteq \mathbb{Z}$ be finite and satisfy $|A+A| \leq K|A|$, then A is contained inside a GAP P of dimension d with $d \leq f_1(K)$ and $|P| \leq f_2(K)|A|$.

Remark on Quantitative Bounds

- We establish this result with $f_1(K) = K^{100}$ and $f_2(K) = e^{K^{100}}$.
- Best known bounds are currently due to Tom Sanders (2010), he establish the result with $f_1(K) = K\log^c K$ and $f_2(K) = e^{K\log^c K}$.

Note that $\mathbb{Z}$ has <u>no</u> interesting subgroups so only example 2 was relevant here. At the other extreme (groups with bounded torsion) we have the following result of Ruzsa (which has a short elegant proof).

Theorem (Freiman's Theorem for Torsion Groups)

Suppose $A \subseteq G$, that every element in G has order at most r, and that $|A+A| \leq K|A|$, then A is contained within a coset of some subgroup H of G with $|H| \leq K^2 r^{K^4} |A|$.

In 2007 (Ruzsa's result is from 1999) Green and Ruzsa combined these two results to get a result valid for all abelian groups.

Theorem (Freiman's Theorem for Abelian Groups)

Let $A \subseteq G$ finite, with $|A+A| \leq K|A|$, then $\exists$ coset progression $H+P$, where H is a finite subgroup of G and P is a GAP of dimension d, such that $A \subseteq H+P$ with $d \leq f_1(K)$ and $|H||P| \leq f_2(K)|A|$.

Remark on Quantitative Bounds:

- Green and Ruzsa obtained $f_1(K) = O(K^{4+o(1)})$ & $f_2(K) = e^{f_1(K)}$.
- Best known bounds are again due to Sanders, who showed

$$f_1(K) \leq C K \log^c K \quad \& \quad f_2(K) = e^{CK\log^c K}.$$

In a sense, these bounds are best possible up to the value of C, since if $A = \{1, 10, 10^2, \dots, 10^{K-1}\}$ (say) then A cannot be efficiently covered by any GAP of dimension less that $K-1$, and any GAP of dimension d has size at least 2^d. (This observation was already made by Ruzsa).

Polynomial Freiman-Ruzsa Conjecture

Let $A \subseteq G$ finite with $|A+A| \leq K|A|$, then A can be K^C-covered by a d-dimensional (centred) convex coset progression P with

$e^{c\log^c K}$ ''

$$d \leq C\log K \quad \text{and} \quad |P| \leq K^C|A|.$$

$\log^c K$ '' $e^{c\log^c K}$ ''

Sander's result corresponds to