Doubling and Volume: on a conjecture of Freiman

Oriol Serra

Department of Mathematics
Universitat Politècnica de Catalunya, Barcelona

Additive Combinatorics in Bordeaux, April 2016
Joint work with G.A. Freiman

The Freiman–Ruzsa Theorem

Theorem (Freiman–Ruzsa)

Let $A \subset \mathbb{Z}$ be a finite set. If

$$|2A| \leq c|A|,$$

then A is contained in a d–dimensional arithmetic progression Q such that

$$|Q| \leq c'|A|$$

where d and c' depend only on c

Estimates of c'

Obtaining good estimates for c' is a significant problem.

Some results:

- $c' \leq (2d)^{exp\ exp\ exp\ (9c \log 2c)}$ (Freiman, 1988, Bilu 1999)
- $c' \leq exp(c^{c^c})$ (Ruzsa, 1994)
- $c' \leq exp(Kc^2(\log(c^3)))$ (Mei Chu-Chang, 2002)
- $c' \leq exp(O(c^{7/4} \log^3 c)$ (Sanders, 2008)
- $c' \leq exp(c \log c)$ (Konyagin, 2011)
- $c' \leq exp(c^{1+K(\log c)^{-1/2}})$ (Schoen, 2011)

One can not do better than $d \leq c-1$ and $c' = e^{O(c)}$: Schoen's estimation is essentially best possible.

Freiman conjecture: $c' = 2^{c-2}(k-c+b+1)$

Small doubling and structure: a quest for exact results

Let $A \subset \mathbb{Z}$ be a finite subset

We have

$$2|A| - 1 \leq |2A|$$

and equality holds iff A is an arithmetic progression.

Inverse problem: What is the structure of A if $|2A| \leq c|A|$?

Some Notation

$$A = \{a_0 < a_1 \cdots < a_{k-1}\} \text{ finite set of integers.}$$

- Doubling $2A = A + A = \{a + a' : a, a' \in A\}$.
- $T = |2A|$ cardinality of doubling.
- A is in normal form if $a_0 = 0$ and $\gcd(A) = 1$.

Freiman homomorphism and isomorphism

- G, H abelian groups, $A \subset G$, $B \subset H$ finite sets.
- $\phi : A \to B$ bijective is a Freiman–homomorphism if, for $a_i, a_j, a_k, a_l \in A$,

$$a_i + a_j = a_k + a_l \;\Rightarrow\; \phi(a_i) + \phi(a_j) = \phi(a_k) + \phi(a_l).$$

  If the implication is if and only if, then ϕ is a Freiman–isomorphism:

$$A \equiv_F B.$$

  F–isomorphic sets are indistinguishable with respect to additive structure.

- If $\phi : G \to H$ group isomorphism then ϕ is an F–isomorphism between any finite set $A \subset G$ and $\phi(A) \subset H$.
- Translations are F–isomorphisms.
- $A \subset \mathbb{Z}$ normal set, $A^{-} = -A + \max(A)$, the reverse of A, is normal set F–isomorphic to A.

Dimension and d–dimensional arithmetic progressions

- A d–dimensional arithmetic progression Q is a set of integers of the form

$$\begin{aligned} Q &= a + Q_1 + Q_2 + \cdots + Q_d \\ &= a + \{t_1 q_1 + \cdots + t_d q_d,\ 0 \le t_1 \le h_1 - 1, \ldots, 0 \le t_d \le h_d - 1\}, \end{aligned}$$

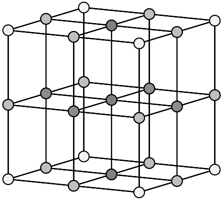
where Q_i is an arithmetic progression with difference q_i with length h_i. Its volume is

$$vol(Q) = h_1 \cdots h_d.$$

The arithmetic progression Q is proper if

$$|Q| = vol(Q).$$

$\{0, 1, 2\} + \{0, 5, 10\} + \{0, 13, 26\}$



Dimension and d–dimensional arithmetic progressions

- A d–dimensional arithmetic progression Q is a set of integers of the form

$$\begin{aligned} Q &= a + Q_1 + Q_2 + \cdots + Q_d \\ &= a + \{t_1 q_1 + \cdots + t_d q_d,\ 0 \le t_1 \le h_1 - 1, \ldots, 0 \le t_d \le h_d - 1\}, \end{aligned}$$

  where Q_i is an arithmetic progression with difference q_i with length h_i. Its volume is

$$vol(Q) = h_1 \cdots h_d.$$

  The arithmetic progression Q is proper if

$$|Q| = vol(Q).$$

- G abelian group, $A \subset G$ finite set.
- The dimension of A is the largest d for which there is $B \subset \mathbb{Z}^d$ such that
  - $B \equiv_F A$, and
  - B is d–dimensional (not contained in a proper hyperplane of $\mathbb{Z}^d$.)

Volume

- $A \subset G$ finite set.
- The Additive Volume $vol(A)$ of a finite set $A \subset G$ is the smallest cardinality of the convex hull of an F–isomorphic copy of A in $\mathbb{Z}^d$, $d = \dim(A)$.
- For given k and T, $vol(k, T)$ is the maximum volume among all sets with cardinality k and doubling T.
- A set $A \subset \mathbb{Z}$ is extremal if

$$vol(A) = vol(|A|, |2A|)$$

Parametrization of doubling

For each $T \in [2k, \binom{k}{2}+2]$ there are unique

$$c = c(k,T) \in [2, k-1] \text{ and } b = b(k,T) \in [1, k-c-1]$$

such that

$$T = T(k,c,b) = ck - \binom{c+1}{2} + b + 1.$$

If $A \subset \mathbb{Z}$ has cardinality k and doubling

$$T = |2A| \in I_c = \left[ck - \binom{c+1}{2} + 2, (c+1)k - \binom{c+2}{2} + 1\right]$$

then the doubling constant of A is c.

c	2	2	2	3	4	$k-2$
b	1	2	$k-3$	1	1	1
T	$2k$	$2k+1$	$3k-4$	$3k-3$	$4k-7$	$\binom{k}{2}+2$

Freiman Conjecture for the maximum volume

Conjecture (Freiman, 2008)

Let $A \subset \mathbb{Z}$ *with* $k = |A|$ *and*

$$|2A| = T = ck - \binom{c+1}{2} + b + 1$$

Then

$$vol(A) \leq \mu(k, T),$$

with

$$\mu(k, T) = 2^{c-2}(k + 1 - c + b)$$

that is,

$$vol(k, T) = \mu(k, T)$$

Freiman Conjecture for the maximum volume

The conjecture holds for $c = 2$: The $(3k-4)$–Theorem.

Theorem (Freiman, 1959)

Let $A \subset \mathbb{Z}$. *If*

$$T = 2k - 1 + b \leq 3k - 4$$

then

$$vol(A) \leq k - 1 + b.$$

- For each $T \in [2k-1, 3k-4]$ there are extremal sets A with cardinality k and doubling T.

$$\bullet\ \underbrace{\circ\ \circ\ \circ}_{b}\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet$$

- If $T \geq 3k - 3$ $(c \geq 3)$ a new picture appears:

$$\bullet\ \bullet\ \bullet\ \circ\ \circ\ \circ\ \circ\ \bullet\ \bullet\ \bullet \rightarrow \begin{array}{cc} \bullet & \bullet \\ \bullet & \bullet \\ \bullet & \bullet \end{array}$$

Freiman Conjecture for the maximum volume

The value for the maximum is tight: $vol(k, T) \geq \mu(k, T)$

if $A \subset \mathbb{Z}$ has doubling $T = T(k, c, b)$ and $vol(A) = \mu(k, T)$, then

- $D(A) = A \cup \{2 \max(A)\}$, and
- $D_x(A) = 2 \cdot A \cup \{x\}$, $x \in 2A \setminus A$ odd

have doubling $T' = T(k+1, c+1, b) = T + k$ and volume $\mu(k+1, T') = 2\mu(k, T)$

For every k and T one can construct sets with doubling T and volume $\mu(k, T)$ starting with a set under the $(3k-4)$–Theorem.

Freiman Conjecture for the maximum volume

Beyond $3k-4$

- Freiman: $3k-3, 3k-2$
- Hamidoune, Plagne: $3k-3, 3k-2$ (isoperimetric method)
- Grynkiewicz, Serra: $3k-3, 3k-2$ (Kemperman Structure Theorem)
- Jin $(3+\epsilon)k$ (nonstandard analysis)

Main result

Theorem (Freiman, Serra)

Let A be a chain with $k = |A|$ and $T = |2A|$. Then

$$\max(A) = \mu(k, T).$$

Theorem (Freiman, Serra)

Let A be an extremal set with $k = |A|$ and $T \leq 4k - 8$. Then

$$vol(A) \leq \mu(k, T).$$

Chains

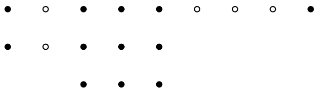
A normalized 1–dimensional extremal set A is a chain if there is a sequence

$$A_3 \subset A_4 \subset \cdots \subset A_k = A$$

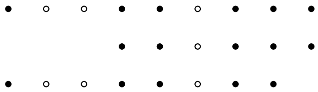
such that

- A_i is (isomorphic to) a 1–dimensional extremal set with cardinality i, $3 \leq i \leq k$,
- A_i is obtained from A_{i+1} by deleting $\max(A_{i+1})$ or $\min(A_{i+1})$.

A chain:



An extremal set not a chain



not extremal

2–dimensional

Chains

A normalized 1–dimensional extremal set A is a chain if there is a sequence

$$A_3 \subset A_4 \subset \cdots \subset A_k = A$$

such that

- A_i is (isomorphic to) a 1–dimensional extremal set with cardinality i, $3 \leq i \leq k$,
- A_i is obtained from A_{i+1} by deleting $\max(A_{i+1})$ or $\min(A_{i+1})$.

$\mathcal{C}$ class of chains.

$$vol_{\mathcal{C}}(k, T) = \max\{\max(A) : A \text{ chain}, k = |A|, T = |2A|\}$$

Theorem

$$vol_{\mathcal{C}}(k, T) = \mu(k, T)$$

Computation of dimension

Basic additive relations: $A = \{a_1, \dots, a_k\}$ finite set in an additive group

$$a_i + a_j = a_r + a_s,\ a_i, a_j, a_r, a_s \in A,\ \{a_i, a_j\} \neq \{a_r, a_s\}.$$

Basic relations in $\mathbb{R}^k = \langle e_1, \dots, e_k \rangle$:

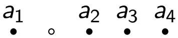
$$a_i + a_j = a_r + a_s \to v(i,j,r,s) = e_i + e_j - e_r - e_s$$

Theorem (Konyagin, Lev)

The additive dimension of a set A satisfies

$$\dim(A) = k - 1 - \lambda(A),$$

where $\lambda(A) = \dim\langle v(i,j,r,s) : a_i + a_j = a_r + a_s \rangle$.



$$a_1 + a_4 = 2a_2 \ \to (1, -2, 0, 1)$$
$$a_2 + a_4 = 2a_3 \ \to (0, 1, -2, 1)$$
$$\lambda(A) = 2,\ \dim(A) = 1$$

Computation of dimension

Basic additive relations: $A = \{a_1, \dots, a_k\}$ finite set in an additive group

$$a_i + a_j = a_r + a_s,\ a_i, a_j, a_r, a_s \in A,\ \{a_i, a_j\} \neq \{a_r, a_s\}.$$

Basic relations in $\mathbb{R}^k = \langle e_1, \dots, e_k \rangle$:

$$a_i + a_j = a_r + a_s \to v(i,j,r,s) = e_i + e_j - e_r - e_s$$

Theorem (Konyagin, Lev)

The additive dimension of a set A satisfies

$$\dim(A) = k - 1 - \lambda(A),$$

where $\lambda(A) = \dim\langle v(i,j,r,s) : a_i + a_j = a_r + a_s \rangle$.

If $A_3 \subset A_4 \subset \cdots A_k = A$ is a chain,

$$|2A_i| \leq |2A_{i-1}| + (i-1) \ \text{ and } \quad \max(A_i^*) \leq 2\max(A_{i-1}^*)$$

A^* normalization of A.

Structure of Chains

A set $A = \{0 = a_0 < a_1 < \cdots < a_{k-1}\}$ is stable if

$$2A \cap [0, a_{k-1}] = A.$$

A is right–stable if its reflexion A^- is stable.

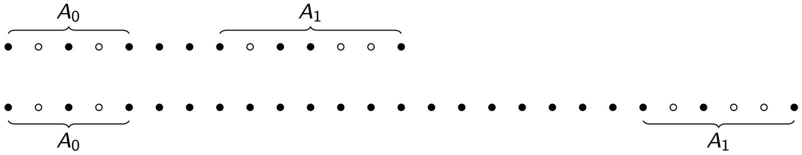
Theorem (Freiman (2009))

Let A be an extremal set with $|2A| \leq 3k - 4$.
There are A_0 stable set, P segment and A_1 right–stable set such that

$$A = A_0 \circ P \circ A_1,$$

where $X \circ Y = X \cup (\max(X) + Y)$ denotes concatenation.
Moreover

$$2A = A_0 \circ P' \circ A_1.$$



Structure of Chains

A set $A = \{0 = a_0 < a_1 < \cdots < a_{k-1}\}$ is stable if

$$2A \cap [0, a_{k-1}] = A.$$

A is right–stable if its reflexion A^- is stable.

Theorem (Freiman (2009))

Let A be an extremal set with $|2A| \leq 3k - 4$.
There are A_0 stable set, P segment and A_1 right–stable set such that

$$A = A_0 \circ P \circ A_1,$$

where $X \circ Y = X \cup (\max(X) + Y)$ denotes concatenation.
Moreover

$$2A = A_0 \circ P' \circ A_1.$$

- A stable if $2A \cap [0, \max(A)] = A$ and $1, \max(A) - 1 \notin A$

Structure of Chains

A set $A = \{0 = a_0 < a_1 < \cdots < a_{k-1}\}$ is stable if

$$2A \cap [0, a_{k-1}] = A.$$

A is right–stable if its reflexion A^- is stable.

Theorem (Freiman (2009))

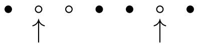
Let A be an extremal set with $|2A| \leq 3k-4$.
There are A_0 stable set, P segment and A_1 right–stable set such that

$$A = A_0 \circ P \circ A_1,$$

where $X \circ Y = X \cup (\max(X) + Y)$ denotes concatenation.
Moreover

$$2A = A_0 \circ P' \circ A_1.$$

- A stable if $2A \cap [0, \max(A)] = A$ and $1, \max(A) - 1 \notin A$
- If A is stable then $|A \cap [0, x]| \leq \lceil \frac{x+1}{2} \rceil$.



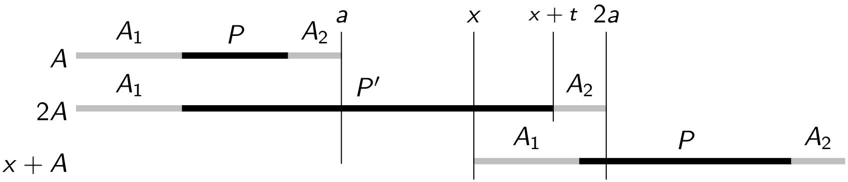
Chain extension

Lemma

Let $A = A_0 \circ P \circ A_2$ *be an extremal set with* $|2A| \leq 3|A| - 4$.

If $A_x = A \cup \{x\}$ *is extremal with* $|2A_x| > 3|A_x| - 4$, *then* x *is even and*

$$x \geq \ell(A_1) + \ell(A_2) - 2 \text{ and } |A_1 \cap (t + A_2) \cap [0, 2a - x]| = \left\lceil \frac{2a-x+1}{2} \right\rceil.$$



Chain extension

Lemma

Let $A = A_0 \circ P \circ A_2$ *be an extremal set with* $|2A| \le 3|A| - 4$.

If $A_x = A \cup \{x\}$ *is extremal with* $|2A_x| > 3|A_x| - 4$, *then* x *is even and*

$$x \ge \ell(A_1) + \ell(A_2) - 2 \text{ and } |A_1 \cap (t + A_2) \cap [0, 2a - x]| = \left\lceil \frac{2a-x+1}{2} \right\rceil.$$

The last condition can only hold if both A_1 and A_2 are 2–progressions. Otherwise $x = 2a$.

Lemma

If the only extension of an extremal set A *is* $A' = A \cup 2\max(A)$ *then the same happens with* A'.

Structure of Chains

Theorem

Let A be a chain. Then,

$$vol_{\mathcal{C}}(A) = \mu(|A|, |2A|).$$

Moreover, there is a subchain $B = B_0 \circ P \circ B_1$ with $|2B| \leq 3|B| - 4$ such that

$$A = D^t(B)$$

unless B_0, B_1 are both 2–progressions.

$$\bullet\ \circ\ \circ\ \circ\ \circ\ \circ\ \underbrace{\bullet\ \circ\ \circ\ \bullet\ \bullet\ \bullet\ \bullet}_{B}\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \circ\ \bullet$$

$$\bullet\ \circ\ \circ\ \circ\ \circ\ \circ\ \bullet\ \circ\ \circ\ \circ\ \underbrace{\bullet\ \bullet\ \bullet\ \circ\ \bullet\ \circ\ \bullet}_{B}\ \circ\ \circ\ \circ\ \bullet$$

Theorem applies to chains with $|2A| \leq \binom{|A|+1}{2} - |A| + 2$

Beyond chains: a $(4k-8)$–theorem

Theorem

Let A be an extremal set with $T \leq 4k-8$. Then,

$$vol(A) = \mu(k, T).$$

Moreover, A is 1–dimensional.

Dimension descent

Largest volume occurs for 1–dimensional sets.

Theorem

Let A be 2-dimensional set with cardinality k and doubling $T = T(A)$.

There is a 1–dimensional set B and an injective Freiman homomorphism $\phi : A \to B$ such that

$$T(B) < T(A) \text{ and } Vol(B) > Vol(A).$$

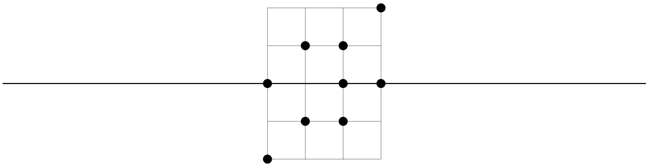
Dimension descent

Lemma

Let $A \subset \mathbb{Z}^d$ be a d–dimensional set and $\phi : \mathbb{Z}^d \to \mathbb{Z}^m$ a group homomorphism. If ϕ is injective on A then

(i) $\dim(\phi(A)) \leq \dim(A)$, *and*

(ii) $T(\phi(A)) \leq T(A)$.



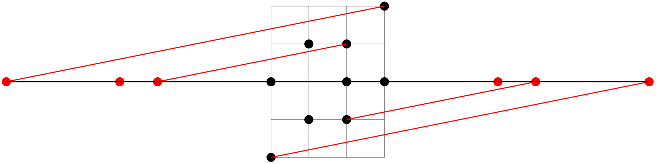
Dimension descent

Lemma

Let $A \subset \mathbb{Z}^d$ be a d–dimensional set and $\phi : \mathbb{Z}^d \to \mathbb{Z}^m$ a group homomorphism. If ϕ is injective on A then

(i) $\dim(\phi(A)) \leq \dim(A)$, *and*

(ii) $T(\phi(A)) \leq T(A)$.



A projection can be found such that $dim(\phi(A)) = 1$ and $vol(\phi(A)) > vol(A)$.

A $(4k-8)$–theorem

Theorem

Let A be an extremal set with $T \leq 4k-8$. Then,

$$vol(A) = \mu(k, T).$$

Moreover A is 1–dimensional.

- Proved if $T \leq 3k-4$ and if A is a chain.
- If $T \geq 3k-3$ and A is not a chain, find a sequence $A_i \subset A_{i+1} \subset \cdots \subset A$ of 1–dimensional sets where A_i is not extremal and A_{i+1} is extremal: one shows that $\max(A_{i+1}) = \mu(|A_i|, |2A_i|)$.

Some applications: the Freiman–Vosper Theorem

Theorem (Freiman)

Let $A \subset \mathbb{Z}/p\mathbb{Z}$ with $|A| \leq p/35$ and $|2A| \leq (5/2)|A|$. Then A is covered by an arithmetic progression of length at most $|2A| - |A| + 1$.

Some applications: the Freiman–Vosper Theorem

Theorem (Freiman)

Let $A \subset \mathbb{Z}/p\mathbb{Z}$ with $|A| \leq p/35$ and $|2A| \leq (5/2)|A|$. Then A is covered by an arithmetic progression of length at most $|2A| - |A| + 1$.

Conjecture (Bilu, Lev Ruzsa; Serra, Zémor)

Let $A \subset \mathbb{Z}/p\mathbb{Z}$ with $k = |A|$. If

$$|2A| = 2k - 1 + b,\ 0 \leq b \leq \min\{k-3, p/2 - k - 1\}$$

then A is contained in a progression with length at most $k + b$.

- Vosper–Freiman theorem. Improved to $|A| \leq p/10$ by Rødseth.
- $b = 1$ (Hamidoune–Rødseth)
- $|A| \leq 10^{-180}p$ (Green and Ruzsa: rectification)
- $|2A| \leq (2+\epsilon)p$ (Serra and Zémor: isoperimetric method and rectification)

Some applications: the Freiman–Vosper Theorem

Theorem (Freiman)

Let $A \subset \mathbb{Z}/p\mathbb{Z}$ *with* $|A| \leq p/35$ *and* $|2A| \leq (5/2)|A|$. *Then* A *is covered by an arithmetic progression of length at most* $|2A| - |A| + 1$.

Conjecture (Bilu, Lev Ruzsa; Serra, Zémor)

Let $A \subset \mathbb{Z}/p\mathbb{Z}$ *with* $k = |A|$. *If*

$$|2A| = 2k - 1 + b,\ 0 \leq b \leq \min\{k - 3, p/2 - k - 1\}$$

then A *is contained in a progression with length at most* $k + b$.

Theorem (Freiman, Rué, Serra, Spiegel)

The BLR conjecture holds for 1*–dimensional sets.*

Final remarks

- Is it possible to prove the Freiman conjecture for $c = f(|A|)$?
- The Freiman–Ruzsa theorem is extended to abelian groups: the Green–Ruzsa theorem. Can the structure of extremal sets be given in this case?
- The knowledge of structure of extremal sets will be helpful in many of the applications of Freiman theorem. How relevant will it be?
- Some steps in the extension of Freiman–Ruzsa theorem to nonabelian groups (approximate groups) rely on the Freiman–Ruzsa theorem for the integers. How relevant can the structure of extremal sets be in that step?