Clay-Fields Conference on Additive Combinatorics, Number Theory, and Harmonic Analysis

On the exact structure of multidimensional sets with small doubling property

Yonutz V. Stanchescu
The Open University, Israel

April 5-13, 2008

1. Direct and inverse problems of additive and combinatorial number theory

Additive number theory is the study of sums of sets and we can distinguish two main lines of research.

In a *direct problem* of additive number theory we start with a particular known set A and attempt to determine the structure and properties of the h-folds sumset hA. These are the classical direct problems in additive number theory: Waring's problem, Goldbach conjecture...

As a counterbalance to this direct approach, an *inverse problem* in additive number theory is a problem in which we study properties of a set A, if some characteristic of the h-fold sumset hA is given.

Sumsets can be defined in any Abelian group G, for example in

- $\mathbb{Z}$
  the group of integers,

- $\mathbb{Z}/m\mathbb{Z}$
  the group of congruence classes modulo m,

- $\mathbb{Z}^n$
  the group of integer lattice points,

- $\mathbb{R}^d$
  the d-dimensional Euclidean space.

Freiman proposed an unifying “algorithm” for solving inverse additive problems:

- Step 1. Consider some (usually numerical) characteristic of the set under study.

- Step 2. Find an extremal value of this characteristic within the framework of the problem that we are studying.

- Step 3. Study the structure of the set when its characteristic is equal to its extremal value.

- Step 4. Study the structure of the set when its characteristic is near to its extremal value.

- Step 5. ....Continue, taking larger and larger neighborhoods for the characteristic.

Let us choose as characteristic the *cardinality of the sumset*:

$$2K = K + K,$$

or equivalently the "*measure of doubling*" :

$$\sigma = \frac{|K + K|}{|K|}.$$

We will examine in detail the **exact structure** of a finite set

$$K \subseteq G,$$

in the case of a torsion free Abelian group

$$G = \mathbb{Z}^n \quad \text{or} \quad G = \mathbb{R}^d,$$

assuming that the doubling constant is small.

REMARK: If σ is an *arbitrary* doubling constant, then *Freiman's fundamental result (1966)* asserts that such a set is a large subset of a multidimensional arithmetic progression; see also Freiman (1987), Bilu (1993), Ruzsa (1994), Nathanson (1996), or Tao and Vu (2006).

2. Small doubling property on the plane $\mathbb{Z}^2$

Let us describe some results concerning the structure of *planar sets* with small sumset.

We begin with the following basic inequality:

Theorem 1 (Freiman 1966). *If $\mathcal{K} \subseteq \mathbb{Z}^2$ lies on exactly $s \geq 2$ parallel lines, then*

$$|\mathcal{K}+\mathcal{K}| \geq (4-\frac{2}{s})|\mathcal{K}| - 2s + 1 \geq 3k - 3. \quad (1)$$

Moreover, using Freiman's $3k-4$ theorem we easily conclude that a planar set of lattice points $\mathcal{K} \subseteq \mathbb{Z}^2$ with

$$|\mathcal{K}+\mathcal{K}| < 3|\mathcal{K}| - 3$$

lies on a straight line and is contained in an arithmetic progression of no more than

$$v = |\mathcal{K}+\mathcal{K}| - |\mathcal{K}| + 1$$

terms. Step 2 is completely solved.

Therefore, a natural problem is to concentrate on the study of Steps 3 and 4.

We ask for the structure of a finite *planar set* of lattice points with small doubling $|\mathcal{K}+\mathcal{K}|$. As one can expect, this question is easier to answer when the cardinality $|\mathcal{K}+\mathcal{K}|$ is close to its minimal possible value $3|\mathcal{K}|-3$, and becomes much more complicated if we choose bigger values for $|\mathcal{K}+\mathcal{K}|$. To be more specific, we may ask the following

Problem.
Find the exact structure of planar sets of lattice points under the doubling hypothesis:

$$|\mathcal{K}+\mathcal{K}| < (4-\frac{2}{s+1})|\mathcal{K}|-(2s+1).$$

Let us examine the first case $s = 2$.

Though, the Freiman's $(2^n - \epsilon)$ theorem gives a first indication on the structure of $\mathcal{K}$, still this is not so precise as the following

Theorem 2 (Freiman 1966, S. 1998)**.** *Let* $\mathcal{K} \subseteq \mathbb{Z}^2$ *be a finite of dimension* $\dim \mathcal{K} = 2$.

(i) $|\mathcal{K}| \geq 11$ *and* $|\mathcal{K} + \mathcal{K}| < \frac{10}{3}|\mathcal{K}| - 5$ *then* $\mathcal{K}$ *lies on two parallel lines.*

(ii) If $\mathcal{K}$ *lies on two parallel lines and*

$$|\mathcal{K} + \mathcal{K}| < 4|\mathcal{K}| - 6$$

then $\mathcal{K}$ *is included in two parallel arithmetic progressions with the same common having together no more than* $v = |2\mathcal{K}| - 2k + 3 \quad terms.$

This means that the total number of holes satisfies

$$h \leq |2\mathcal{K}| - (3k - 3).$$

FIGURE:

The following theorem incorporates Freiman's previous result as a particular case:

Theorem 3 (S. 1998). *Let $\mathcal{K}$ be a finite set of $\mathbb{Z}^2$ and $s \geq 1$ be a natural number. If $|\mathcal{K}|$ is sufficiently large, i.e. $k \geq O(s^3)$, and*

$$|\mathcal{K}+\mathcal{K}| < \left(4 - \frac{2}{s+1}\right)|\mathcal{K}| - (2s+1) \ , \qquad (2)$$

then there exist s parallel lines which cover the set $\mathcal{K}$.

This is a best possible result, because it cannot be improved by increasing the upper bound for $|\mathcal{K}+\mathcal{K}|$, or by reducing the number of lines that cover $\mathcal{K}$.

EXAMPLE: ...

The theorem is effective and recently Serra and Grynkiewicz obtained an explicit value for the constant $k_0(s) = 2s^2 + s + 1$. They also succeeded to extend the result for sums of different sets $A + B$:

Theorem 4 (Grynkiewicz and Serra 2007)**.** *Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{R}^2$ be finite subsets and $s \geq 1$ be a natural number.*

(i) If $\Big||\mathcal{A}| - |\mathcal{B}|\Big| \leq s + 1, |\mathcal{A}| + |\mathcal{B}| \geq 4s^2 + 2s + 1$ and

$$|\mathcal{A} + \mathcal{B}| < (2 - \frac{1}{s+1})(|\mathcal{A}| + |\mathcal{B}|) - (2s + 1)$$

then there exist $2s$ (not necessarily distinct) parallel lines which cover the sets $\mathcal{A}$ and $\mathcal{B}$.

(ii) If $|\mathcal{A}| > |\mathcal{B}| + s, |\mathcal{B}| \geq 2s^2 + \frac{s}{2}$ and

$$|\mathcal{A} + \mathcal{B}| < |\mathcal{A}| + (3 - \frac{2}{s+1})|\mathcal{B}| - (s + 1)$$

then there exist $2s$ (not necessarily distinct) parallel lines which cover the sets $\mathcal{A}$ and $\mathcal{B}$.

The next natural question is to consider a finite set $\mathcal{K}$ of lattice points on a plane having the *small doubling property*

$$|2\mathcal{K}| < (4 - \frac{2}{s+1})|\mathcal{K}| - (2s+1)$$

and ask for a reasonable estimate for the number of lattice points of a "minimal" parallelogram that covers the set $\mathcal{K}$.

More precisely, if $\mathcal{L}$ is a lattice generated by $\mathcal{K}$, we are interested in precise upper bounds for the number of points of $\mathcal{L}$ that lie in the convex hull of $\mathcal{K}$. Our main result asserts that $\mathcal{K}$ is located inside a parallelogram that lies on a few lines which are well filled:

Theorem 5 (S. 2007). *Let $s \geq 19$ be an integer and let $\mathcal{K}$ be a finite subset of $\mathbb{Z}^2$ that lies on exactly s parallel lines. If*

$$|2\mathcal{K}| < (4 - \frac{2}{s+1})|\mathcal{K}| - (2s+1),$$

then there is a lattice $\mathcal{L} \subseteq \mathbb{Z}^2$ and a parallelogram $\mathcal{P}$ such that

$$\mathcal{K} \subseteq (\mathcal{P} \cap \mathcal{L}) + v$$

and

$$|\mathcal{P} \cap \mathcal{L}| \leq 24\Big(|\mathcal{K} + \mathcal{K}| - 2|\mathcal{K}| + 1\Big),$$

for some $v \in \mathbb{Z}^2$.

Conjecture. We believe that for a best possible result, the constant factor 24 of Theorem 5 should be replaced by $\frac{1}{2}(1 + \frac{1}{s-1})$, i.e.

$$|\mathcal{P} \cap \mathcal{L}| \leq \frac{s}{2(s-1)}\Big(|\mathcal{K} + \mathcal{K}| - 2|\mathcal{K}| + 2s - 1\Big).$$

So far inequality this estimate has been proved only for $s = 2$ (Freiman 1966) and $s = 3$ (S. 1999).

3. Planar sets with no three collinear points on a line

Let $\mathcal{A} \subseteq \mathbb{Z}^2$ be a finite set, not containing any three collinear points. Freiman asked in 1966 for a lower bound for $|\mathcal{A}+\mathcal{A}|$. As a first step in the investigation of this problem we showed that $\frac{|\mathcal{A}\pm\mathcal{A}|}{|\mathcal{A}|}$ is unbounded, as $\lim |\mathcal{A}| = \infty$:

Theorem 6 (S.2002)**.** *Let $\mathcal{A} \subseteq \mathbb{Z}^2$ be a finite set of n lattice points. If $\mathcal{A}$ does not contain any three collinear points, then there is a positive absolute constant $\delta > 0$ such that*

$$|\mathcal{A} \pm \mathcal{A}| \gg n(\log n)^{\delta}. \tag{3}$$

The constant δ can be easily computed: for instance, any positive δ smaller than 0.125 will do.

There is an intimate connection between two seemingly unrelated problems:

(i) non-averaging sets of integers of ordet t
and
(ii) planar sets with no three points on a line.

Definition. *A finite set of integers $\mathcal{B} \subseteq \mathbb{Z}$ is called a non-averaging set of order t, if for every $1 \le m, n \le t$ the equation*

$$mX_1 + nX_2 = (m+n)X_3,$$

have no nontrivial solutions with $X_i \in \mathcal{B}$.

Let

$$s_t(n)$$

be the maximal cardinality of a *non-averaging set of order t* included in the interval $[1, n]$.

It is clear that a non-averaging set of order 1 is simply an integer set containing no arithmetic progressions. Bourgain's bound for Roth's theorem gives:

$$s_t(n) \leq s_1(n) = r_3(n) \ll \frac{n}{(\log n)^{\frac{1}{2}}}(\log\log n)^{\frac{1}{2}}.$$

Remark. We also obtained a *more exact* inequality, valid for sets $\mathcal{A} \subseteq \mathbb{Z}^2$ containing no $k-$terms arithmetic progressions: for every integer $t \geq 1$ we have

$$|\mathcal{A} \pm \mathcal{A}| \geq \frac{1}{2}|\mathcal{A}|\Big(\frac{n}{s_t(n)}\Big)^{\frac{1}{4t}}. \qquad (4)$$

We formulate the following:

Problem S. *Suppose that* $t \geq 1$ *is a fixed, positive, but rather large integer. Is it true that* $s_t(n) \ll \frac{n}{(\log n)^{4t}}$, *or at least* $s_t(n) \ll \frac{n}{(\log n)^{c}}$, *for a positive absolute constant* $c \geq \frac{1}{2}$*?*

Note that Freiman's question asks for a non trivial lower estimate of $|\mathcal{A}+\mathcal{A}|$ for a set $\mathcal{A} \subseteq \mathbb{Z}^2$ containing no three collinear points and in Problem S we want to estimate the density of a sequence of natural numbers $\mathcal{B}$, assuming that t *linear equations* does not hold for $\mathcal{B}$. Inequality (4) shows that any upper bound for $s_t(n)$, *better* than the trivial one $r_3(n)$ will lead to a corresponding sharpening of (3) and (4).

As regards lower bounds, we have:

Theorem 7 (S. 2002)**.**

(i) For every $t \geq 1$*, there is a positive constant* c_t *such that for every* n *one has*

$$s_t(n) \geq n \exp(-c_t \sqrt{\log n}).$$

(ii) There is no $\epsilon_0 > 0$ *such that the inequality*

$$|\mathcal{A} + \mathcal{A}| \gg |\mathcal{A}|^{1+\epsilon_0}$$

holds for every finite set $\mathcal{A} \subseteq \mathbb{Z}^2$ *containing no three collinear points.*

The proof uses Freiman's fundamental concept of isomorphism, Behrend's method and a result of Ruzsa about sets of integers containing no non-trivial three term arithmetic progressions.

A recent improvement of the lower bound (3), was obtained by T. Sanders (2006):

$$|\mathcal{A} + \mathcal{A}| \gg_\epsilon |\mathcal{A}|(\log |\mathcal{A}|)^{\frac{1}{3}-\epsilon}.$$

4. The simplest inverse problem for sums of sets in several dimensions

It is a well known fact that $|A+B| \geq |A|+|B|-1$ for every two finite sets A and B of $\mathbb{Z}^d$, equality being attained when A and B are arithmetic progressions with the same difference.

It is possible to obtain a much better estimate. The first result connecting geometry and additive properties is

Theorem 8 (Freiman 1966). *For every finite set $\mathcal{A} \subseteq \mathbb{Z}^d$ of affine dimension* $\dim \mathcal{A} = d$, *one has*

$$|\mathcal{A}+\mathcal{A}| \geq (d+1)|\mathcal{A}| - \frac{1}{2}d(d+1). \qquad (5)$$

This lower bound is tight, i.e. Step 2 is solved.

EXAMPLE:

Let us investigate now Step 3. What is the *exact structure* of multi-dimensional sets having the *smallest cardinality* of the sumset?

The following result is an analogue of the well known Vosper's theorem (1956), $\mathbb{Z}/p\mathbb{Z}$ being here replaced by the d-dimensional space $\mathbb{R}^d$.

Theorem 9 (S. 1998). *Let $\mathcal{A} \subseteq \mathbb{R}^n$ be a finite set such that* $\dim \mathcal{A} \geq d$ *and*

$$|\mathcal{A}+\mathcal{A}| = (d+1)|\mathcal{A}| - \frac{1}{2}d(d+1).$$

If $|\mathcal{A}| \neq d+4$, then $\mathcal{A}$ is a d-dimensional set and $\mathcal{A}$ consists of d parallel arithmetic progressions with the same common difference.

Moreover, if $|\mathcal{A}| = d+4$, then

$$\mathcal{A} = \{v_0, v_1, ..., v_d\} \cup \{2v_1, v_1+v_2, 2v_2\},$$

where v_i are the vertices of a d-dimensional simplex.

EXAMPLE:

Further developments:

Ruzsa (1994): If $|A| \geq |B|$ and $\dim(A+B) = d$, then

$$|A+B| \geq |A| + d|B| - \frac{d(d+1)}{2}.$$

Gardner and Gronchi (2001): If $|A| \geq |B|$ and $\dim(B) = d$, then

$$|A+B| \geq$$

$$\geq |A| + (d-1)|B| + \sqrt[d]{(|A|-d)^{d-1}(|B|-d)} - \frac{d(d-1)}{2}$$

Green and Tao (2006)
Suppose that $A \subseteq \mathbb{R}^m$ is a finite set which contains a parallelepiped $P = \{0,1\}^d \subseteq \mathbb{Z}^d \subseteq \mathbb{R}^m$.

Then

$$|A+A| \geq 2^{d/2}|A|.$$

5. Exact Structure Results for Multidimensional Inverse Additive Problems

A natural question is to generalize Theorem 3 to the multidimensional case $d = \dim(\mathcal{K}) \geq 3$:

Assume that the doubling coefficient of the sum set $2\mathcal{K}$ is not much exceeding the minimal one, i.e.

$$d + 1 \leq \sigma = \frac{|2\mathcal{K}|}{|\mathcal{K}|} < \rho_d.$$

What can be said about the *exact structure* of $\mathcal{K}$? The expected result is: if

$$\rho_d = d + 1 + \frac{1}{3},$$

then the set K is contained in d "short" arithmetical progressions.

The problem was first solved for the first open case $d = 3$:

Theorem 10 (S. 2005)**.** *Let* $\mathcal{K}$ *be a finite subset of* $\mathbb{Z}^3$ *of affine dimension* $\dim \mathcal{K} = 3$.

(i) If $|\mathcal{K}| > 12^3$ *and*

$$|\mathcal{K} + \mathcal{K}| < \frac{13}{3}|K| - \frac{25}{3}$$

then $\mathcal{K}$ *lies on three parallel lines.*

(ii) If $\mathcal{K}$ *lies on three parallel lines and*

$$|\mathcal{K} + \mathcal{K}| < 5|\mathcal{K}| - 10,$$

then $\mathcal{K}$ *is contained in three arithmetic progressions with the same common difference, having together no more than*

$$v = |\mathcal{K} + \mathcal{K}| - 3|\mathcal{K}| + 6$$

terms.

The structure of $\mathcal{K}$ can be also be described for sets of dimension $d \geq 3$:

Theorem 11 (S. 2008). *Let $\mathcal{K} \subseteq \mathbb{Z}^d$ be a finite set of dimension $d \geq 2$.*

(i) If $k > 3 \cdot 4^d$ and

$$|\mathcal{K}+\mathcal{K}| < (d+\frac{4}{3})|\mathcal{K}| - c_d,$$

where $c_d = \frac{1}{6}(3d^2+5d+8)$, then $\mathcal{K}$ lies on d parallel lines.

(ii) If $\mathcal{K}$ lies on d parallel lines and

$$|\mathcal{K}+\mathcal{K}| < (d+2)|\mathcal{K}| - \frac{1}{2}(d+1)(d+2),$$

then $\mathcal{K}$ is contained in d parallel arithmetic progressions with the same common difference, having together no more than

$$v = |\mathcal{K}+\mathcal{K}| - d|\mathcal{K}| + \frac{1}{2}d(d+1) \quad terms.$$

These results are best possible and cannot be sharpened by reducing the quantity v or by increasing the upper bounds for $|\mathcal{K} + \mathcal{K}|$.

EXAMPLES:

We found that a similar inequality can be formulated for $d-$dimensional sets that have a small doubling coefficient $C_d = d + 2 - \frac{2}{s-d+3}$ (where $s \geq d$ is a positive integer). In this case we prove that $\mathcal{K}$ lies on no more than s parallel lines.

These results can be used to make Freiman's Main Theorem more precise.

In a joint work with Freiman (2008) we study the *exact structure* of d-dimensional sets satisfying the small doubling property

$$|2K| < (d + 2 - \epsilon)|K|.$$

6. Difference Sets

We will present now some results on difference sets in a d-dimensional Euclidean space. The need for lower estimates for $|\mathcal{A} - \mathcal{A}|$ in terms of $|\mathcal{A}|$ has been raised by Uhrin (1981), where the trivial $|\mathcal{A} - \mathcal{A}| \geq 2|\mathcal{A}| - 1$ is used to prove theorems sharpening the classical theorem of Minkowski-Blichfeldt in geometry of numbers.

It can be stated that the sharper estimation for $|\mathcal{A} - \mathcal{A}|$ we have, the sharper results in geometry of numbers can be proved.

Let $\mathcal{A} \subseteq \mathbb{R}^d$ be a finite set and (as Step 1 of Freiman's algorithm requires) we choose as numerical characteristic the cardinality of the difference set $\mathcal{A} - \mathcal{A}$.

The following inequality is analogous to (5):

Theorem 12 (Freiman-Heppes-Uhrin 1989). *If* $\dim \mathcal{A} \geq 1$, *then*

$$|\mathcal{A} - \mathcal{A}| \geq (d+1)|\mathcal{A}| - \frac{1}{2}d(d+1). \qquad (6)$$

This immediately yields that if

- $d = 1$ and $\mathcal{A} \subseteq \mathbb{R}$, then $|\mathcal{A} - \mathcal{A}| \geq 2|\mathcal{A}| - 1$

and if

- $d = 2$ and $\mathcal{A} \subseteq \mathbb{R}^2$, then $|\mathcal{A} - \mathcal{A}| \geq 3|\mathcal{A}| - 3$.

These two inequalities cannot be strengthened. However, the lower bound (6) is not exact for dimension $d = 3$.

Freiman-Heppes-Uhrin (1989) and Ruzsa (1994) conjectured that the "correct" lower bound for $\dim \mathcal{A} = 3$ is

$$|\mathcal{A} - \mathcal{A}| \geq 4.5|\mathcal{A}| - 9 \ . \qquad (7)$$

This conjecture is correct and (7) is a best possible lower bound for $|\mathcal{A} - \mathcal{A}|$:

Theorem 13 (S. 1998). *Let $\mathcal{A}$ be a finite set of $\mathbb{R}^3$ and let $\{e_1, e_2, e_3\}$ be the standard basis of $\mathbb{R}^3$.*

(i) If $\dim \mathcal{A} = 3$, *then* $|\mathcal{A} - \mathcal{A}| \geq 4.5|\mathcal{A}| - 9$.

(ii) Equality is attained if and only if $\mathcal{A}$ is a union of four parallel arithmetic progressions: $\mathcal{A} = \{0, e_1, e_2, e_1 + e_2\} + \{0, e_3, 2e_3, ..., ke_3\}$.

For 2-dimensional sets the situation is similar:

Theorem 14 (S. 1998). *Let $\mathcal{D}$ be a finite set in $\mathbb{R}^2$ of affine dimension* $\dim \mathcal{D} = 2$. *Then* $|\mathcal{D} - \mathcal{D}| = 3|\mathcal{D}| - 3$, *if and only if $\mathcal{D}$ consists of two parallel arithmetic progressions with the same number of elements and the same common difference.*

This solves Steps 2 and 3 of Freiman's algorithm: it gives the structure of 2 and 3 dimensional sets having the smallest cardinality of the difference set.

Let us give now a short description of the multidimensional case $d \geq 4$.

Let s_d be the maximal positive number for which the inequality

$$|\mathcal{A} - \mathcal{A}| \geq s_d|\mathcal{A}| - t_d$$

holds for every finite set $\mathcal{A}$ of affine dimension $\dim \mathcal{A} = d$.

What can one say about s_d ?
The exact value of s_d is known only for $d = 1$, $d = 2$ and $d = 3$ and Ruzsa conjectured

Conjecture. (Ruzsa, 1994) For every $d \geq 4$ we have

$$s_d = 2d - 2 + \frac{2}{d}.$$

EXAMPLES :

The following upper bound for s_d is true:

Theorem 15 (S. 2001)**.** *For every integer* d*,* $d \geq 2$ *one has*

$$s_d \leq 2d - 2 + \frac{1}{d-1} \ .$$

This readily disproves Ruzsa's conjecture. Moreover, in view of inequality (7) and Theorem 15, it seems that the equality $s_d = 2d-2+\frac{1}{d-1}$ is true for every $d \geq 2$. Thus, we suggest the following:

Conjecture 16 (S. 2001)**.** *For every finite set* $\mathcal{A}$ *of affine dimension* $\dim \mathcal{A} = d \geq 2$*, one has*

$$|\mathcal{A} - \mathcal{A}| \geq (2d - 2 + \frac{1}{d-1})|\mathcal{A}| - (2d^2 - 4d + 3).$$

Of course, in view of Theorem 15, if the above inequality is true, then is best possible.

EXAMPLES for dimension 2, 3 and 4...

7. Finite Abelian groups

Similar questions can be asked for any group G. A short and incomplete list of results for

$$G = \mathbf{F}_p, G = (\mathbf{F}_2)^d, G = \mathbb{Z}/n\mathbb{Z}$$

will show that additive questions in finite abelian groups are generally more difficult than analogous problems in $\mathbb{Z}$.

• Consider for the beginning sums of *congruence classes modulo a prime* p. Take two finite sets A and B in $\mathbf{F}_p$ and choose as characteristic the *cardinality of the sum*

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

Then the solution of Step 2 is Cauchy-Davenport theorem:

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

The answer to Step 3 is given by Vosper's theorem (1956), which classify those pairs A, B of sets of residues for which equality holds in Cauchy-Davenport inequality.

The next natural question is to consider Step 4 and to analyze the case when the cardinality of the sum is not much exceeding its extremal value.

Freiman (1966), generalized Vosper's theorem for sumsets of the form $A + A$ in $\mathbf{F}_p$, by describing the structure of A in the case

$$|2A| < c|A| - 3,$$

with $c < 2.4$; either $|A|$ is large or the set A is located in a short arithmetic progression.

This has been recently extended to any c by Green and Ruzsa (2006), using the rectification principle of Freiman and Bilu-Lev-Ruzsa (1998).

• For sumsets in *vector spaces over finite fields,* Eliahou and Kervaire proved in (1998) that

$$|A+B| \geq \min\left\{p^t\left(\lceil\frac{|A|}{p^t}\rceil+\lceil\frac{|B|}{p^t}\rceil-1\right) : 0 \leq t \leq d\right\},$$

for every two sets A and B included in $(\mathbf{F}_p)^d$. Step 2 is solved.

Deshouillers-Hennecart-Plagne gave in (2004) an answer to Steps 3 and 4 by obtaining a structure theorem under the assumption

$$A \subseteq \mathbf{F}_2^d, |A+A| = c|A|, 1 \leq c < 4.$$

In this instance the set A is contained in a coset $a+H$ of order at most $\frac{|A|}{u(c)}$ where $u(c) > 0$ is an explicit function depending only c.

• Recently Step 5 was solved by Ruzsa and Green (2008), not only for $G = \mathbf{F}_p^d$, but also for *commutative torsion groups:*

If A is a subset of a commutative group G of exponent r and if

$$|A + A| < k|A|,$$

then A is contained in a coset of a subspace of size no more than

$$k^2 r^{2k^2-2}.$$

• Let G is an *arbitrary Abelian group.*
Kneser (1953) gave a deep generalization of Cauchy-Davenport's theorem:

Let A and B be two finite subsets of an Abelian group G. One has

$$|A+B| \geq |A| + |B| - |H|,$$

where H is the stabilizer of $A+B$.

Important results concerning the equality case in Kneser's theorem are due to Kemperman (1960) and Lev (1999).

In a step beyond Kneser's theorem, Deshouillers and Freiman (2003) proved a structural result for the cyclic group

$$G = \mathbb{Z}/n\mathbb{Z}$$

assuming that

$$|A+A| < 2.04|A|$$

and $|A|$ sufficiently small.