BOLYAI SOCIETY
MATHEMATICAL STUDIES, 11

Paul Erdős and his Mathematics. I,
Budapest, 2002, pp. 243–260.

Structure Theory of Set Addition II. Results and Problems

G. A. FREIMAN

1. Introduction

For a general introduction to the relevant background in additive number theory and structure theory of set addition, readers are referred to the review [15], of which this[1] is a continuation.

This paper is intended to promote further progress in the study of inverse problems in additive number theory and is aimed at mathematicians looking for new problems, particularly at young mathematicians.

In Section 2 I shall summarize some essential definitions and basic results from [15]. Then I shall give a detailed account of ten carefully chosen typical problems, including related ideas and results and suggest possible approaches. I shall also mention briefly new applications of structure theory in ergodic theory and commutative algebra and the results of W. T. Gowers [18].

2. Definitions and Basic Results

We consider a finite subset K of $\mathbb{Z}^n$ (and often of $\mathbb{Z}$) with cardinality $|K| = k$.

---

[1] This paper is based on my lecture "Additive Problems of Erdős and Structure Theory of Set Addition" given on July 8 at the conference "Paul Erdős and his Mathematics" held in Budapest, July 4–11, 1999.

We define $2K = K + K = \{x \,|\, x = a + b,\ a \in K,\ b \in K\}$. We say that K has the *small doubling property* if

$$|2K| < Ck,$$

where either C is a positive constant independent of k or $C = C(k)$ is a slowly increasing function. The number $|2K|/k$ is called *doubling coefficient* of K.

We shall need the notion of an *additive isomorphism* of one subset onto another (or, in the language of [15], of an $\mathcal{F}_2$-isomorphism). An additive isomorphism of $A \subset \mathbb{Z}^n$ onto $B \subset \mathbb{Z}^m$ is a bijection $\varphi : A \to B$ of A onto B such that for all a, b, c, d in A we have

$$\varphi(a) + \varphi(b) = \varphi(c) + \varphi(d) \quad \text{iff} \quad a + b = c + d.$$

If there exists an additive isomorphism of A onto B, we write $A \sim B$, and we note that $\sim$ is an equivalence relation.

A quantity which is invariant under additive isomorphism is called an *additive invariant.* For example, $|2K|$ and $|K - K|$ are additive invariants for $K \subset \mathbb{Z}^n$.

As no other types of isomorphism on subsets of $\mathbb{Z}^n$ will be used, we shall refer to additive isomorphisms simply as isomorphisms.

We also need the following concept. A *d-dimensional parallelepiped* is a subset D of $\mathbb{Z}^d$ of the form

$$D = \big\{ (x_1, x_2, \ldots, x_d) \,|\, x_i \in \mathbb{Z}, 0 \le x_i < h_i, h_i \ge 2, 1 \le i \le d \big\}$$

with cardinality $|D| = h_1 h_2 \ldots h_d$.

The "Main Theorem" of inverse additive number theory is discussed in Section 6 of [15]. The version of a proof due to Y. Bilu may be found in [2].

Main Theorem. *For all finite subsets $K \subset \mathbb{Z}$ for which $|2K| < Ck$, where the constant C does not depend on k, there exist $c = c(C)$ and D with $d \le [C - 1]$ and $|D| < ck$ such that $K \subset \varphi(D)$, where φ is an isomorphism.* ■

We also need the notion of dimension of a subset $K \subseteq \mathbb{Z}$.

For a given $K \subseteq \mathbb{Z}$, we consider the images $\varphi(K)$ under all isomorphisms $K \xrightarrow{\varphi} \mathbb{Z}^n$ for all $n \ge 1$. The dimension of any $\varphi(K)$ is the dimension of the smallest affine subspace containing it. The maximum dimension of $\varphi(K)$ for all such φ is called the *dimension* of K.

3. Sets of k Integers with $\log k$ as Doubling Coefficient

Problem 1. Study the structure of $K \subset \mathbb{Z}$ if

$$|2K| < k \log k. \tag{1}$$

In the case of (1) the doubling coefficient is at most $\log k$.

The structure of K that satisfies a small doubling condition of this type is described, for example, in papers of G. Freiman [13], Y. Bilu [2] and I. Ruzsa [20]. The best result, when the doubling coefficient is a small power of iterated logarithm was obtained by Ruzsa.

W. T. Gowers [18] has recently obtained a quantitative result for the density $\frac{k}{n}$ of a finite subset of integers in a segment $[1, n]$ such that this set contains four-term arithmetic progression. This result is obtained for densities that are characterized by a power of iterated logarithm. To obtain a density of order $\frac{1}{\log n}$ or, at least, some small power of it as in the result of Heath-Brown [19] in Roth problem on a set with a three-term arithmetic progression, it seems that we need a condition of type (1). This gives added importance to improving our understanding of the structure of sets with a small doubling property.

4. Sets of k Integers with $|2K|$ in $\left[3k - 3, \frac{10}{3}k - 5\right)$

Problem 2. Prove the following conjecture.

Let $K \subset \mathbb{Z}$ such that

$$|2K| = 3k - 3 + b,$$

where $0 \leq b < \frac{k}{3} - 2$. Then there exist a constant k_0, which does not depend on k, such that if $k > k_0$ then either $K \subset \mathcal{I}$, where $\mathcal{I}$ is an arithmetic progression such that

$$|\mathcal{I}| \leq 2k - 1 + 2b,$$

or

$$K \subset \varphi(D)$$

where $D \subset \mathbb{Z}^2$,

$$D = \left\{ (0,0), (1,0), \ldots, (k_1 - 1, 0),\ (0,1), (1,1), \ldots, (k_2 - 1, 1) \right\},$$
$$k_1 + k_2 \leq k + b,$$

$\varphi : D \to \mathbb{Z}$ is an isomorphism.

In other words, we have to prove that either K is a subset of an arithmetic progression $\mathcal{I}$ with $2k - 1 + 2b$ terms, or K is a part of a union of two arithmetic progressions $\mathcal{I}_1$ and $\mathcal{I}_2$ such that $|\mathcal{I}_1| + |\mathcal{I}_2| \leq k + b$, $\mathcal{I}_1$ and $\mathcal{I}_2$ have the same difference, and $2\mathcal{I}_1, \mathcal{I}_1 + \mathcal{I}_2$ and $2\mathcal{I}_2$ are pairwise disjoint.

The Main Theorem gives for $\mathcal{I}$ an estimate $|\mathcal{I}| < c_1 k$, where c_1 is a very large constant.

In Problem 2 we try to get the best possible estimate for $|\mathcal{I}|$.

Let us show first that the conclusion of the conjecture is false if the condition $b < \frac{k}{3} - 2$ is violated. Let us take $3 \mid k$, $b = \frac{k}{3} - 2$, $K = \left\{ 0, 1, \ldots, \frac{k}{3} - 1, c, c+1, \ldots, c + \frac{k}{3} - 1, 2c, 2c+1, \ldots, 2c + \frac{k}{3} - 1 \right\}$, $c > 2k$.

Clearly, $|2K| = \frac{10k}{3} - 5$ and K does not satisfy the conclusion of Problem 2.

The example

(2) $$K = \{0, 1, 2, \ldots, k-3, k+b-1, 2k+2b-2\}$$

with $b < \frac{k}{3} - 2$, for which dimension of K is one and $|2K| = 3k - 3 + b$, shows that the estimate for $|\mathcal{I}|$ conjected in Problem 2 cannot be improved.

We can generalize Example (2). Let s be an integer such that $2 \leq s \leq k - 1$. Take

(3)
$$K_{s,b} = \left\{ 0, 1, 2, \ldots, k-s, k-s+b, 2(k-s+b), 2^2(k-s+b), \ldots, 2^{s-2}(k-s+b) \right\},$$

where b is an integer such that $1 \leq b < k + 1 - s$. We have

(4) $$|2K_{s,b}| = sk - \frac{s^2+2}{2} + 1 + b.$$

We have constructed an example of a set K for which

(5) $$2k - 1 \leq |2K| \leq \frac{k^2 - k + 4}{2},$$

dimension of K is equal to one and K is contained in an arithmetic progression $\mathcal{I}_{s,b}$, where

$$|\mathcal{I}_{s,b}| = 2^{s-2}(k - s + b) + 1 \tag{6}$$

for $K = K_{s,b}$.

We can now formulate the following more general conjecture.

Conjecture. *Let $K_{s,b}$ be any set of integers for which (4) holds. Assume that there exists no arithmetic progression with $2^{s-2}(k - s + b) + 1$ terms that contains $K_{s,b}$. Then*

$$d(K_{s,b}) > 1$$

where $d(K)$ denotes the dimension of the set K.

5. Non-Commutative Case

The next problem invites a natural extension of the above ideas to non-commutative situation.

First we introduce an appropriate notion of isomorphism of pairs of sets.

The isomorphism of pairs of sets is defined as follows. Let G and G' be groups. A pair $A \subset G$ and $B \subset G$ is called isomorphic to a pair $A' \subset G'$ and $B' \subset G'$ if there exist bijections $A \overset{\varphi}{\longleftrightarrow} A'$ and $B \overset{\psi}{\longleftrightarrow} B'$ that induce a bijection $AB \overset{\gamma}{\longleftrightarrow} A'B'$. This means that if $a \in A$, $b \in B$, $c \in A$, $d \in B$ and $ab = cd$, then $\varphi(a)\psi(b) = \varphi(c)\psi(d)$ and, in a case when $ab \neq cd$, the last equality doesn't hold either.

Problem 3. Investigate the following conjecture.

Let G be a group (non-commutative in general). Let M and K be finite subsets of G, $m = |M|$, $k = |K|$, $k \leq m$. Let

$$|MK| = m + k - 1 + b, \tag{7}$$

where

$$0 \leq b < k - 2.$$

If G is a torsion-free group, there exist two elements a and b in G such that the sets $a^{-1}M$ and Kb^{-1} are contained in a pair $\mathcal{I}_1 \subset G$ and $\mathcal{I}_2 \subset G$ isomorphic to the pair $\mathcal{I}_1', \mathcal{I}_2' \subset \mathbb{Z}$, with

$$\mathcal{I}_1' = \{0, 1, 2, \dots, \ell_1 - 1\},$$

$$\mathcal{I}_2' = \{0, 1, 2, \dots, \ell_2 - 1\}$$

and

$$\ell_1 \leq m + b, \quad \ell_2 \leq k + b.$$

This result was proved in the case $b = 0$ by I. Brailovsky and G. Freiman [3], and we believe it should be true in general.

Remark. It seems that the conjectured result is valid also in the more general case when $m < cr$, where r is the minimal order of all elements of G different from one and c is a sufficiently small absolute constant that does not depend on G.

Roughly speaking, we can say that, under the small doubling condition (7), products of subsets of a noncommutative group behave as if the group is Abelian.

It is desirable to find under which condition of small doubling this is true.

A complete description of sets with small doubling was given by G. Elekes ([8] and [9]) for one important noncommutative group, the group of linear functions where the operation is composition.

6. Small Number of Collinear Points

Problem 4. Let $K \subset \mathbb{Z}^2$ such that no three points of K are collinear. Give a lower estimate for $|2K|$.

This problem was raised in the sixties but the only estimate known to me at this time is $|2K| \geq k(\log k)^{0.124}$ found by Y. Stanchescu [26]. He used results of D. R. Heath-Brown [19]. It is desirable to obtain a stronger and more direct result.

Why is this problem important? Suppose we succeeded in obtaining an estimate $|2K| \geq kf_2(k)$ in Problem 4. We know now that for every K, for which $|2K| < kf_2(k)$, there are three points of K on one line. This is the first step for describing the structure of K. Ask the same question about K with no more than three, four or s points on a line. From the case when s is a constant we can go to a situation when s is a function of k, say, $s = k^{\varepsilon}$, where $0 < \varepsilon < 1$, or to the case when $s = \delta k$ with δ a small positive constant. Now we can go to sets K when $K \subset \mathbb{Z}^n$, $n \geq 2$ and ask about the value of $|2K|$ when there are some restrictions on the number of points not only on lines but on planes including hyperplanes.

We now see that all these results, when obtained, will be helpful to have an advancement in the direction of Theorem 5.1 of Y. Bilu [2], p. 85, which is a very important part of the proof of the Main Theorem.

7. Exact Estimates

Problem 5. Find by elementary means the extremal estimates describing the structure of $K \subset \mathbb{Z}^2$, where $d(K) \geq 2$ and

$$|2K| < 4.5k.$$

Again we are asking about the structure of a set under a condition of small doubling. The special features of this case are that we seek *exact* estimates obtained with the help of *elementary* methods.

The first results of this type were those for $K \subset \mathbb{Z}$, for which $|2K| \leq 3k-3$ (see [15], page 3, [2], page 77). I also obtained results for $|2K| = 3k-2$, but the argument was extremely long and complicated and it was clear that the scope of a satisfactory elementary approach is limited to $|2K| \leq 3k-3$.

The study of the case when K is on two parallel lines and $|2K| < 4k-6$ was completed by Y. Stanchescu [23]. He also studied the case when $|2K| < (4-\varepsilon)k$, $\varepsilon > 0$. Then K is on a finite number of parallel lines (see [23]) and he obtained a reasonable estimate for cardinality of a covering rectangle ($< 56k$).

The real break-through in our understanding began with the following remarkable result of Y. Stanchescu [22] about $K \subset \mathbb{Z}^2$ situated on three parallel lines.

Theorem. *Let* $K \subset \mathbb{Z}^2$ *and*

$$|2K| < 3.5k - 7.$$

If K lies on three parallel lines, then the convex hull of K is contained in three arithmetic progressions with the same common difference that have no more than

$$k + \frac{3}{4}\left(|2K| - \frac{10k}{3} + 5\right) \tag{8}$$

terms in their union. This upper bound is the best possible.

The proof appeared to be rather complicated and involved a study of different configurations. It was very startling that, almost for each configuration, an example was constructed showing that the estimate (8) cannot be improved. All this led to an understanding that exact estimates should exist in much wider situations than those already studied.

For the case when $K \subset \mathbb{Z}^2$ lies on $s \geq 3$ lines the following was conjectured.

Conjecture (Y. Stanchescu). *Let $K \subset \mathbb{Z}^2$, K lies on $s \geq 3$ parallel lines and*

$$|2K| = \left(4 - \frac{2}{s}\right)k - (2s-1) + b$$

where

$$0 \leq b < \frac{2k}{s(s+1)} - 2.$$

Then for the number of points H in a minimal convex hull covering K under isomorphism we have

$$H \leq k + \frac{s}{2(s-1)}b.$$

For corresponding results for $K \subset \mathbb{Z}^n$, $n \geq 3$, we can mention the papers of Y. Stanchescu [24] and [25], I. Ruzsa [21] and G. Freiman, B. Uhrin and A. Heppes [16].

8. Another Invariant

Problem 6. Let $K \subset \mathbb{Z}$, K a finite set,

$$M = \int_0^1 |S|^4 \, d\alpha, \tag{9}$$

where

$$S = \sum_{x \in K} e^{2\pi i \alpha x}. \tag{10}$$

Investigate the structure of K if the value of M is given.

We will explain first the arithmetical meaning of M and show that M is an additive invariant of K (as defined in Section 2 above).

We have

$$M = \int_0^1 S^2 \overline{S}^2 \, d\alpha = \sum_{\substack{x \in K \\ y \in K \\ z \in K \\ t \in K}} \int_0^1 e^{2\pi i \alpha (x-y-z+t)} \, d\alpha.$$

Denote by $u(a)$ the number of representations of a number a in the form $a = x - y$, $x \in K$, $y \in K$.

The number of solutions of the equation $x - y - (z - t) = 0$ under condition $x - y = z - t = a$ is equal to $u^2(a)$ and then $M = k^2 + 2M'$ where $M' = \sum_{a \in \mathbb{Z}_+} u^2(a)$.

M and M' are additive invariants.

As usual, the first question we ask is about the extremal values of M and M' and the sets with these extremal values.

The minimal value of M' is equal to $\frac{(k-1)k}{2}$ and the corresponding sets are Sidon sets that is sets where all nonzero differences are different.

If K is an arithmetic progression we have

$$M' = (k-1)^2 + (k-2)^2 + \ldots + 1 = \frac{(k-1)k(2k-1)}{6}$$

and

$$M = \frac{k(2k^2+1)}{3}. \tag{11}$$

It is not difficult to show that these values are maximal and achieved only if K is an arithmetic progression.

Let $K_s = \{a_0 < a_1 < \ldots < a_{s-1}\}$, $s \geq 1$ and

$$M'(K_s) \leq \frac{(s-1)s(2s-1)}{6}. \tag{12}$$

It can be checked that $M'(K_{s+1}) \le M'(K_s) + s^2$.

The differences $a_s - a_v = c_v$, $0 \le v \le s-1$, are those which are in K_{s+1} but not in K_s.

How many differences of K_s are equal to c_v for some given v (this number was denoted $u_{K_s}(c_v)$)? Take one of such differences $a_i - a_j = c_v = a_s - a_v$. We have here $a_i < a_s, i < s$. From this we obtain $a_v > a_j$ and $j < v$. Thus, j may take no more than v different values and so

$$u_{K_s}(c_v) \le v. \tag{13}$$

We have

$$M'(K_s) = \sum_{v=0}^{s-1} u^2_{K_s}(c_v) + \sum_{\substack{a\neq c_v\\ a>0}} u^2_{K_s}(a)$$

and therefore because of (12)

$$M'(K_{s+1}) = \sum_{v=0}^{s-1} \left(U_{K_s}(c_v)+1\right)^2 + \sum_{\substack{a\neq c_v\\ a>0}} u_{K_s}(a) \le M'(K_s) + 2\sum_{v=0}^{s-1} v + s$$

$$= M'(K_s) + s^2 \le \frac{s(s+1)(2s+1)}{6}.$$

When $M'(K) = \frac{(k-1)k(2k-1)}{6}$? Only in the case when induction reasoning uses equality in (13) for every s and v. The equality $u_{K_{k-1}}(c_{k-1}) = k-1$ occurs only if

$$a_{k-1} - a_{k-2} = a_{k-2} - a_{k-3} = \ldots = a_1 - a_0.$$

We have finished the first step of studying K for a given value of M. To continue, we have to gradually diminish values of M and M' and study the structure of K for these values.

9. Several Invariants

Problem 7. Investigate the structure of $K \subset \mathbb{Z}$ if values of $|2K|$ and M (as in (9)) are both given.

Some knowledge about the value of $|2K|$ gave us valuable information about the structure of K. It is clear that if we will know a value of an additional additive invariant (or several invariants) we will know more about K.

We have

$$\int_0^1 S^2 S_1 \, d\alpha = k^2$$

where

$$S = \sum_{x \in K} e^{2\pi i \alpha x}$$

and

$$S_1 = \sum_{x \in 2K} e^{-2\pi i \alpha x}$$

and we obtain using Cauchy–Schwartz inequality

$$k^4 \le \int_0^1 |S|^4 \, d\alpha \int_0^1 |S_1|^2 \, d\alpha = M|2K|. \tag{14}$$

If K is a set with a condition of small doubling $|2K| < Ck$ then, from (11) and results of Section 8, we obtain

$$\frac{k^3}{C} < M \le \frac{k(2k^2+1)}{3}. \tag{15}$$

We can take values of C a bit larger than the values for which the structure of K had been already studied, apply (14), and use the knowledge which gives (15) about M to learn more about the structure of K.

In Section 8, we introduced the value $u(a)$, the number of representations of a number a in the form $a = x - y$, $x \in K$, $y \in K$.

Define the order in the set of numbers $\{u(a)\}$ in the following way:

$$u_1 \geq u_2 \geq \ldots \geq u_s \geq \ldots \tag{16}$$

In the case when $u(a_1) = u(a_2)$ the order is defined arbitrarily.

The sequence of numbers (16) is a system of invariants. It was used in (10) to define M and to study K for the maximal value of M. We may continue in the same way and use (14) to study K in a case of condition (15). The greater the set of numbers we take from (16), the richer the information, but working with this set of numbers will be more difficult.

Begin with some simple examples. If $u_1 = k-1$ then K is an arithmetic progression. If $u_1 = k-2$ then K is a union of two arithmetic progressions with the same distance. The "$3k-3$ theorem" may be checked in this case directly.

Continuing the investigation in this way taking values $u_1 = k-3$, then $u_1 = k-4$, etc., introducing different vales u_2, u_3 etc., we will obtain richer examples of K and verify the conjectures of Section 2. Further study in this direction should lead to progress.

If $|2K| = 2k-1$ then $M = \frac{k(2k^2+1)}{3}$ and

$$M|2K| = \frac{4}{3}k^4 + O(k^3).$$

If $|2K| = \frac{k(k+1)}{2}$ then $M = 2k^2 - k$ and

$$M|2K| = k^4 + O(k^3).$$

We may think that $M|2K| \asymp k^4$ but this is not true.

Take[2] the union of two sets, each containing $\frac{k}{2}$ elements, where the first is an arithmetic progression and the second is a Sidon set. We then have $M|2K| \asymp k^5$.

We can ask about the extremal values of M for a given $|2K|$. Then we can investigate the structure of K for a given $|2K|$ and values of M which are close to these extremal values.

---

[2] I wish to thank the referee for proposing this example.

10. Tight Subsets

Unlike the previous problems, Problem 8 is one which would be difficult to approach on the basis of present knowledge. It would almost certainly require more detailed understanding of the structure of K. For this reason the formulation is necessarily somewhat vague.

Problem 8. For a finite set $K \subset \mathbb{Z}$ find a subset $K' \subset K$ such that the doubling coefficient $\frac{|2K'|}{|K'|}$ will be less than the doubling coefficient $\frac{|2K|}{k}$.

Take the set $K_{s,b}$ defined in (3). Let $s \to \infty$ and $s = o(k)$. Then from (4) we obtain an estimate $|2K_{s,b}| \sim sk$, and for the arithmetic progression $\mathcal{I}_{s,b}$ of minimal length containing $K_{s,b}$ we obtain from (8)

$$|\mathcal{I}_{s,b}| \asymp 2^s k.$$

Unfortunately, if $s > c \log k$ with c a large constant, the above estimate tells very little about the set K. However, K has a subset $K' = \{0, 1, \dots, k - s\}$ which has the doubling coefficient which is less than 2.

Another example gives us "$3k - 3$ theorem" (see [2]) where the doubling coefficient of K is close to 3 but there are subsets with the doubling coefficient close to 2.

Proposition 12 on page 541 of the paper of W. T. Gowers [18] gives a very important result in the same spirit. In a K with a large value of M he finds a subset with a small value of the invariant $|K - K|$.

11. Large Trigonometric Sums

Problem 9. Let $K \subset \mathbb{Z}$ be a finite set and

$$K \subset [0, \ell]. \tag{17}$$

For a trigonometric sum

$$S_K(\alpha) = \sum_{x \in K} e^{2\pi i \alpha x}$$

we take a set of α for which $|S_K(\alpha)|$ is large. Namely, we take a positive number $m < k$ and define

$$E_{K,m} = \{\alpha \in [0,1) \,|\, |S_K(\alpha)| \geq m\}.$$

We write $\mu_K(m) = \mu(E_{K,m})$, where μ is the Lebesgue measure on $[0,1]$. Also we set

$$\mu_k(m,\ell) = \max_{K\subset[0,\ell]} \mu_K(m).$$

The problem is to find the maximal value $\mu_k(m,\ell)$ and the set K which maximizes $\mu_K(m)$.

This problem was formulated in [15], Section 33, page 19. The motivation of introducing condition (17) is given there. We begin our study of K by taking small values of ℓ and gradually go to larger values of ℓ.

As an example, we consider the simple case when $m = 0.95k$ and $\ell = 1.5k$.

We will first show that when $\|\alpha\| > \frac{5}{k}$ we have $|S_K(\alpha)| < 0.95k$ and therefore for these values $\alpha \notin E_{K,m}$.

$$\begin{aligned}
|S_K(\alpha)| &= \left|\sum_{x=1}^{\ell} e^{2\pi i\alpha x} - \sum_{x\in[1,\ell]\setminus K} e^{2\pi i\alpha x}\right| \\
&\leq \left|\sum_{x=1}^{\ell} e^{2\pi i\alpha x}\right| + \left|\sum_{x\in[1,\ell]\setminus K} e^{2\pi i\alpha x}\right| \\
&\leq \left|\frac{\sin\pi\alpha\ell}{\sin\pi\alpha}\right| + \ell - k \\
&\leq \frac{1}{2\|\alpha\|} + \ell - k < \frac{k}{10} + 0.5k \\
&< 0.95k.
\end{aligned}$$

As the next step we will show that the estimate $|S_K(\alpha)| < 0.95k$ is valid also in the interval

$$\frac{1}{2\ell} \leq \alpha < \frac{5}{k} < \frac{8}{\ell}.$$

We will use the inequality

$$\operatorname{Re} e^{2\pi i\alpha x} = \cos 2\pi\alpha x \leq \cos\frac{\pi}{6} < 0.8661,$$

which holds if $\|\alpha x\| > \frac{1}{12}$.

As is easily shown, we can assume without loss of generality that $S_K(\alpha)$ is real. Then

$$(18)\quad \left|S_K(\alpha)\right| = \left|\sum_{x\in K} \cos 2\pi\alpha x\right| \le \frac{1}{2}\left|\left\{x \,\middle|\, \|\alpha x\| \ge \frac{1}{6}\right\}\right| + \cos\frac{\pi}{6}\left|\left\{x \,\middle|\, \frac{1}{12} \le \|\alpha x\| < \frac{1}{6}\right\}\right| + \left|\left\{x \,\middle|\, \|\alpha x\| < \frac{1}{12}\right\}\right|.$$

Take an interval I of the length d. How many integers x are there such that $\alpha x \in I$? It is easy to show that this number is equal to $\frac{d}{\alpha} + O(1)$.

If the numbers αx are on a segment of length 1 we have $\frac{1}{6\alpha} + O(1)$ such numbers with the additional condition $\|\alpha x\| \le \frac{1}{12}$, and $\frac{1}{6\alpha} + O(1)$ numbers with the condition $\frac{1}{12} \le \|\alpha x\| < \frac{1}{6}$.

We now study the case when

$$(19)\qquad \frac{u}{\ell} \le \alpha \le \frac{u+1}{\ell},$$

where $u \in \mathbb{Z}$, $2 \le u \le 7$.

Because of (19) and (17), we have $0 \le \alpha x < u + 1$ and we obtain

$$(20)\qquad \left|\left\{x \,\middle|\, \|\alpha x\| < \frac{1}{12}\right\}\right| \le \frac{u+1}{6\alpha} + O(1),$$

$$(21)\qquad \left|\left\{x \,\middle|\, \frac{1}{12} \le \|\alpha x\| < \frac{1}{6}\right\}\right| \le \frac{u+1}{6\alpha} + O(1).$$

Using (20) and (21) we obtain in (18)

$$\begin{aligned}\left|S_K(\alpha)\right| &\le \frac{1}{2}\left(k - \frac{u+1}{3\alpha}\right) + \frac{u+1}{6\alpha}\cos\frac{\pi}{6} + \frac{u+1}{6\alpha} + O(1)\\ &< \frac{k}{2} + \frac{u+1}{6\alpha}\cos\frac{\pi}{6}\\ &< 0.95k.\end{aligned}$$

The case $\frac{1}{2\ell} \le \alpha \le \frac{2}{\ell}$ may be studied in the same way and we omit this computation. (Because of $\left|S(\alpha)\right| = \left|S(-\alpha)\right|$ the case $-\frac{8}{\ell} \le \alpha \le -\frac{1}{2\ell}$ is also covered.)

If

$$0 \le \alpha \le \frac{1}{2\ell} \tag{22}$$

the arguments of the numbers $e^{2\pi i\alpha x}$ with x in K are all in an angle less than π. For an arithmetic progression K_{ap} we will have $|S_{K_{ap}}(\alpha)| \ge |S_K(\alpha)|$ for every α in (22), as shown, for example, in Besser [1], page 50.

An advancement to the values $|S| \simeq 0.5k$ and $\ell \simeq 3k$ would already give an interesting application.

To avoid difficulties arising when ℓ is large, we propose the following variant of Problem 9.

Let $K \subset \mathbb{Z}$ be a finite set and m a positive number, $m < k$.

Let

$$E_{K,m} = \{\alpha \in [0,1) \mid |S_K(\alpha)| \ge m\}.$$

Denote

$$\mathcal{I}_{K,m} = \int_{E_{K,m}} |S_K(\alpha)|\, d\alpha.$$

The problem is to find the maximal value of $\mathcal{I}_{K,m}$ and the set K for which this value is obtained.

12. Erdős Additive Problems

Problem 10. Describe the structure of sum-free sets and prove the hypothesis about their number.

We recall that the set of integers $A \subset [1,n]$ is called sum-free if $A \cap (A+A) = \emptyset$. Paul Erdős conjectured that the number of sum-free sets is $O(2^{\frac{n}{2}})$.

The use of very simple inverse additive results has already led to substantial progress in Problem 10 (see [14], [7]). The same tools gave advancement in other Erdős additive combinatorial problems (see [4], [5] and [15]). It is clear that the use of results in Inverse Problems provide a general method to treat Erdős additive problems.

13. Applications

Applications of structure theory to various topics were discussed in [15], Sections 21–27, pp. 9–15. Recently new applications to Ergodic theory, Commutative algebra and Combinatorics have appeared (see [6], [17] and W. T. Gowers [18]).

14. Concluding Remarks

Each of the problems sketched above could open up a significant research direction. I hope that some of my readers will take up the challenge.

15.

I am deeply grateful to Dr. Jane Pitman for her invaluable help in the final stage of writing this review.

References

[1] A. Besser, Sets of integers with large trigonometric sums, *Asterisque,* **258** (1998), 35–76.

[2] Y. Bilu, Structure of sets with small sumset, *Asterisque,* **258** (1998), 77–108.

[3] L. V. Brailovsky and G. A. Freiman, Groups with small cardinality of the cubes of their two-element subsets, *Ann. New York Acad. Sci.,* **410** (1983), 75–82.

[4] J.-M. Deshouillers and G. A. Freiman, On an additive problem of Erdős and Straus I, *Israel J. Math.,* **92** (1995), No. 1–3, 33–43.

[5] J.-M. Deshouillers and G. A. Freiman, On an additive problem of Erdős and Straus II, *Asterisque,* **258** (1998), 141–148.

[6] J-M. Deshouillers, G. Freiman and A. Yudin, An application of Structure Theory of Set Addition to a question in Ergodic Theory, to appear.

[7] J.-M., Deshouillers, G. A. Freiman, V. Sós and M. Temkin, On the structure of sum-free sets 2, *Asterisque,* **258** (1998), 149–161.

[8] G. Elekes, Linear combinatorics I, *Combinatorica,* **17** (1997), 447–458.

[9] G. Elekes, Linear combinatorics II, *Combinatorica,* **18** (1998), 13–25.

[10] G. A. Freiman, The addition of finite sets I, *Izv. Vysš. Učebn. Zaved. Matematica,* **6(13)** (1959), 202–213 (Russian).

[11] G. A. Freiman, Inverse problems in additive number theory VII. On the addition of finite sets IV. The method of trigonometric sums, *Izv. Vysš. Učebn. Zaved. Matematica,* **6(31)** (1962), 131–134 (Russian).

[12] G. A. Freiman, Foundations of a structural theory of set addition, in: *Translations of Mathematical Monographs,* **37**, Amer. Math. Soc., Providence, R.I. (1973).

[13] G. A. Freiman, What is the structure of K if $K+K$ is small? in: *Lecture Notes in Mathematics,* **1240**, Springer-Verlag (New York, 1987), pp. 109–134.

[14] G. A. Freiman, On the structure and the number of sum-free sets, *Asterisque,* **209** (1992), 195–203.

[15] G. A. Freiman, Structure Theory of Set Addition, *Asterisque,* **258** (1999), 1–33.

[16] G. A. Freiman, A. Heppes and B. Uhrin, A lower estimation for the cardinality of finite difference sets in $\mathbb{R}^n$, in: *Coll. Math. Soc. J. Bolyai,* **51**, North-Holland and Bolyai Társulat (Budapest, 1989), pp. 125–139.

[17] G. Freiman and A. Geroldinger, An addition theorem and its arithmetical application, *Journal of Number Theory,* **85** (2000), 59–73.

[18] W. T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, *GAFA, Geom. Funct. Anal.*, Vol. **8** (1998), 529–551.

[19] D. R. Heath-Brown, Integer sets containing no arithmetic progression, *J. London Math. Soc. (2),* **35** (1987), 385–394.

[20] I. Z. Ruzsa, Generalized arithmetical progressions and sumsets, *Acta Math. Hungar.*, **65** (1994), 379–388.

[21] I. Z. Ruzsa, Sums of sets in several dimensions, *Combinatorica,* **14** (1994), 485–490.

[22] Y. Stanchescu, On the structure of sets of lattice points in the plane with small doubling property, *Asterisque,* **258** (1999), 217–240.

[23] Y. Stanchescu, On the structure of sets with small doubling property on the plane I, *Acta Arithmetica,* **[83] 2** (1998), 127–141.

[24] Y. Stanchescu, On the simplest inverse problem for sums of lattice points, *Combinatorica,* **18** (1998), 139–149.

[25] Y. Stanchescu, On finite difference sets, *Acta Math. Hungar.*, **79(1-2)** (1998), 123–138.

[26] Y. Stanchescu, Planar sets containing no three collinear points and non-averaging sets of integers, *Discrete Mathematics* (submitted).

Gregory A. Freiman

Tel Aviv University
School of Mathematical Sciences
Sackler Faculty of Exact Sciences
Ramat Aviv 69978
Israel

e-mail: grisha@tau.ac.il