Astérisque

GREGORY A. FREIMAN

Structure theory of set addition

Astérisque, tome 258 (1999), p. 1-33

<http://www.numdam.org/item?id=AST_1999__258__1_0>

Astérisque **258**, 1999, p. 1–33

STRUCTURE THEORY OF SET ADDITION

by

Gregory A. Freiman

Abstract. — We review fundamental results in the so-called structure theory of set addition as well as their applications to other fields.

1. 'Structure theory of set addition'[(1)] is a shorthand for a direction in the study of sets which extracts structures from sets for which some properties of their sums (or products in a non-abelian case) are known.

Here is an indication of what is meant by "structure". The first stage is to build an equivalence relation on sets. Then, by taking well chosen representatives of an equivalence class we are able to reveal its properties and thereby describe its structure (see, for example, the Definition and Theorem in §6).

2. This review is written in the following way. In §§3–8 we explain the main ideas. In §§9–12 we make some historical remarks. Then in §§13–19 we present several concrete problems in additive and combinatorial number theory, showing how new results may be obtained with the help of the described new approach. Further then in §§20–27 we try to show a diversity of fields where the ideas of "Structure Theory" may be applied. Finally in §§28–35 we discuss methods and problems. In the bibliography we include references to a wider spectrum of subjects which may be treated from the point of view of Structure Theory.

3. This approach to additive problems was originally given the name "Inverse problems of additive number theory". A series of nine papers under this heading was published in 1955–1964 (see [85], [86], [87], [88], [89], [90], [91], [92] and [98]).

4. I quote from my lecture in the Fourth All-Union Mathematical Congress, Leningrad, 3-12 July 1961 (see [84]):

1991 ***Mathematics Subject Classification.*** — 11 02, 11Z05.

Key words and phrases. — Structure theory of set addition, inverse problems of additive number theory, small doubling property, isomorphism of subsets.

(1)This paper is based on my review lecture given at the conference on *Structure theory of set addition* held at CIRM (Centre International des Rencontres Scientifiques), Luminy, Marseille, on 10 June 1993.

"The term *inverse problems of additive number theory* appeared in 1955 in two of my papers [85][(2)] and [86]. In [85] the following problem was studied. Let

$$a_1, a_2, \ldots, a_r, \ldots \tag{1}$$

be an unbounded, monotonically increasing sequence of positive numbers. To have an asymptotic formula

$$\log q(u) \sim Au^{\alpha}, \qquad \text{where } A > 0, 0 < \alpha < 1$$

it is necessary and sufficient that

$$n(u) \sim B(A, \alpha)u^{\alpha/1-\alpha}$$

where $n(u)$ is the number of terms of a sequence (1) not exceeding u, and $q(u)$ is the number of solutions of the inequality

$$a_1 n_1 + a_2 n_2 + \cdots \leq u.$$

In [86] the case

$$\log q(u) = Au^{\alpha} + O(u_1^{\alpha}), \qquad \text{where } 0 < \alpha_1 < \alpha,$$

was studied and an estimate of the error term in the asymptotic formula for $n(u)$ was obtained.

One can easily see that if $q(u)$ is known then (1) is determined in a unique way (see [85]). In 'direct' problems we study $q(u)$ when the sequence (1) is given; a particular case is the classical problem on the representation of positive integers as sums of an unlimited number of positive integers.

Thus a direct problem in additive number theory is a problem in which, given summands and some conditions, we discover something about the set of sums. An inverse problem in additive number theory is a problem in which, using some knowledge of the set of sums, we learn something about the set of summands.

Several cases of inverse problems were studied earlier; see [14] and [67].

Paul Erdős, in 1942, found an asymptotic formula for $n(u)$ when

$$\log p(u) \sim a\sqrt{u}$$

where $p(u)$ is the number of solutions of an equation

$$a_1 n_1 + a_2 n_2 + \cdots = u$$

where $\{a_i\}$ is some sequence of positive integers (see [67]).

In the same paper another inverse problem was studied; if $q(u) \sim Cu^{2\alpha}$, where $q(u)$ is the number of solutions of an inequality

$$a_i + a_j \leq u,$$

(2)The reference numbers given accord with the bibliography of this paper and not the original text.

then

$$n(u) \sim C_1 u^{\alpha}.$$

In 1960 V. Tashbaev [252] studied the problem of estimating the error term for this inverse problem.

We will now explain how problems on the distribution of prime numbers are connected with inverse problems. If we define

$$q(u) = [e^u]$$

then $a_i = \log p_i$, where p_i denotes the i^{th} prime number. Thus the problem of the distribution of prime numbers may be treated as an inverse problem of additive number theory of the type described above. The study of inverse problems for different $q(u)$ close to $[e^u]$, and also of direct problems when $n(u)$ is close to e^u/u, may give some insight into the problem of the distribution of primes, in a way similar to that in which the behaviour of a function in the vicinity of a point may help to find its value at that point (see A.Beurling [14] and B.M.Bredichin [30], [31], [32] and [33]."

The results of Diamond (see [57], [58], [59], [60] and [61]) should of course be mentioned.

The treatment of prime distribution problems as inverse additive problems have not developed up to now. I still consider this approach very hopeful.

5. We pass on now to the study of additive problems with a fixed number of summands. The majority of papers mentioned in §3 treat the addition of two *equal* sets. The study of this particular case is usually sufficient to develop ideas, methods and results as well as their use in applications.

Let us start with $K \subseteq \mathbb{Z}$ with $|K| = k$. Define

$$2K = K + K = \{x \mid x = a_i + a_j, \quad a_i, a_j \in K\}.$$

We may ask the question what is the minimal cardinality of $2K$? Evidently,

$$|2K| \geq 2k - 1. \tag{2}$$

Suppose now that K is such that $|2K|$ is minimal i.e. $|2K| = 2k - 1$. What can be said about such a K? It is clear that,

$$|2K| = 2k - 1, \tag{3}$$

only if K is an arithmetic progression.

Suppose now that $|K + K|$ is not much greater than this minimal value. In that case we have the following result [87], describing the structure of K.

Theorem 1. — *Let K be a finite set, $K \subseteq \mathbb{Z}$. If*

$$|K + K| \leq 2k - 1 + b, \quad 0 \leq b \leq k - 3$$

then K is contained in an arithmetic progression of length $k + b$.

Further, suppose that we know that

$$|2K| < Ck, \tag{4}$$

where C is any given positive number, we may ask what then is the structure of K?

6. The theorem answering this question (we will quote it as a main theorem) was proved in a previously mentioned series of papers, expositions of it were given in [81] and [82], and an improved version of a proof was presented in [105]. We are citing here the result of Y. Bilu [16], where he studies a case when C in (4) is a slowly growing function of k.

Definition. — Let A and B be groups, and let $K \subset A$ and $L \subset B$. The map $\phi\colon K \to L$ is called an $\mathbb{F}_s$–homomorphism, if for any $x_1, \cdots, x_s$ and $y_1, \cdots, y_s$ in K we have

$$x_1 + \cdots + x_s = y_1 + \cdots + y_s \Rightarrow \phi(x_1) + \cdots + \phi(x_s) = \phi(y_1) + \cdots + \phi(y_s).$$

The $\mathbb{F}_s$–homomorphism ϕ is an $\mathbb{F}_s$–isomorphism if it is invertible and the inverse ϕ^{-1} is also an $\mathbb{F}_s$–homomorphism.

Let $P \subset \mathbb{Z}^n$ be given by

$$P = \{0, \ldots, b_1 - 1\} \times \cdots \times \{0, \ldots, b_n - 1\}.$$

We have $|P| = b_1 \ldots b_n$. In this paper we will call P an *n–dimensional parallelepiped.*

Theorem 2. — *Let $K \subset \mathbb{Z}$ and suppose that*

$$|K + K| < \sigma k \tag{5}$$

where

$$k = |K| \geq k_0(\sigma) = \frac{[\sigma][\sigma + 1]}{2([\sigma + 1] - \sigma)} + 1\,,$$

then there exists an n–dimensional parallelepiped, P, such that $n \leq [\sigma - 1]$ and $|P| < ck$, where c depends only on σ and s and there also exists a map $\phi\colon P \to \mathbb{Z}$ which is such that $P \to \phi(P)$ is an $\mathbb{F}_s$–isomorphism while $K \subset \phi(P)$.

Let us now return to §1. The equivalence relation that we talked about there, is now seen to be $\mathbb{F}_s$–isomorphism. A representative of an equivalence class is an n–dimensional parallelepiped, P. We now understand that K, a subset of the one-dimensional space $\mathbb{R}$, has, in fact, a multidimensional structure, being a dense subset of an n-dimensional set P (i.e. $\phi^{-1}(K) \subset P$). Consider the numbers

$$a = \phi\big((0, \ldots, 0)\big),\ a_1 = \phi\big((1, 0, \ldots, 0)\big) - a,\ \ldots,\ a_n = \phi\big((0, 0, \ldots, 1)\big) - a.$$

Then,

$$\phi(P) = \{a + a_1 x_1 + a_2 x_2 + \cdots + a_n x_n, \text{ with } 0 \leq x_i \leq b_i - 1\}\,.$$

Imre Rusza has called such a set $\phi(P)$ a generalized arithmetic progression of rank n. He gave a new and shorter proof, based on new ideas, of the main theorem together with an important generalization; in this the summands A and B may be different, although however the condition $|A| = |B|$ is required (see [233]). His generalization to the case of subsets of abelian groups is to be found in [238].

7. We can now describe an "algorithm" for solving an inverse additive problem, by the following steps.

(i) Choose some (usually numerical) characteristic of the set under study.
(ii) Find an extremal value of this characteristic within the framework of the problem that we are studying.
(iii) Study the structure of the set when its characteristic is equal to its extremal value.
(iv) Study the structure of a set when its characteristic is near to its extremal value.
(v) (vi),... continue, taking larger and larger neighbourhoods for the characteristic.

From estimates obtained by Yuri Bilu it follows that in (5) we can take, for σ, the following very slowly growing function of k,

$$\sigma = c \log\log\log\log k.$$

It will be very important to study the cases

$$\sigma = (\log k)^c \tag{6}$$

and

$$\sigma = k^\varepsilon,\ \varepsilon > 0, \tag{7}$$

even if ε is a very small number.

Here to simplify this extremely difficult problem a little, it is better to take $|rK|$ as a characteristic value, where r is a fixed, positive, but rather large, integer. So our condition is now

$$|rK| < k^{1+\varepsilon}$$

which is much stronger than (5); rK contains k^r sums, but no more than $k^{1+\varepsilon}$ of them are different.

8. I have here added a playful description of the comparative difficulty of the problems discussed, which should not be taken too literally. To prove (2) took one minute. Condition (3) was studied in three minutes. The proof of the theorem of §5 together with the description of K under the condition $|2K| = 3k - 3$ took one month. Proof of the main theorem took five years. I will be very happy if we will see results for (6) in the next thirty years but I am not certain that for (7) we will have satisfactory results even in the next hundred years.

9. L. Schnirelman [242] was one of the first who passed from studying fixed sets to studying general additive properties. Schnirelman introduced the notion of the density of a sequence.

Definition. — Let $A = (a_1, a_2, \dots, a_n, \dots)$ be an increasing sequence of positive integers and further let,

$$A(x) = \big|\{y \in A \mid 0 < y \leq x\}\big|,$$

and

$$d(A) = \inf_{x \in \mathbb{N}} A(x)/x\,.$$

The number $d(A)$ is called the *Schnirelman density* of the sequence A (see step (i) of §7).

10. Define

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

and denote

$$\alpha = d(A),\ \beta = d(B),\ \gamma = d(A + B)\,.$$

Schnirelman proved that

$$\gamma \geq \alpha + \beta - \alpha\beta\,.$$

L. Schnirelman and E. Landau conjectured in 1932 and Mann [178] has proved in 1942 that

$$\gamma \geq \alpha + \beta\,. \tag{8}$$

11. The famous $\alpha + \beta$ theorem of Mann cannot be improved. Take a sequence

$$A = \{0, 1, \ldots, r, l + 1, l + 2, \ldots, l + r, 2l + 1, 2l + 2, \ldots, 2l + r, \ldots\}$$

It is clear that if $r \leq l$ then,

$$\alpha = d(A) = r/l\,.$$

However if $2r < l$ then

$$\gamma = d(2A) = 2r/l = 2\alpha\,.$$

But for $A = B$ we always have from (8) that $\gamma \geq 2\alpha$. So step 2 of §7 is now completed.

Thus Mann has entirely solved the problem of increase of the density under summation of sequences. Its solution took ten years. Khinchine [151] writes in his book:

> "The problem has become 'fashionable'. Scientific societies proposed a prize for its solution. My friends from England wrote me in 1935 that half of English mathematicians tried to solve it, putting aside all other obligations"

When Mann had solved the problem, the interest in these subjects disappeared. But what about proving the inequality $\gamma \geq 3\alpha$? Or, equivalently, what are the sequences A for which $\gamma < 3\alpha$? These questions were not asked.

12. However, Schnirelman density is not a good characteristic. Take $A = \{2, 3, 4, \ldots\}$. For this sequence we have $A(1) = 0$ and $d(A) = 0$. We feel, however, that the value 1 would be more appropriate for a density. So we arrive at a notion of an asymptotic density:

$$\underline{d}(A) = \liminf_{x \to \infty} A(x)/x\,.$$

In 1953 Martin Kneser [153] proved an analog of the $\alpha + \beta$ theorem for asymptotic densities. He described the structure of A and B in the case when

$$\underline{d}(A) + \underline{d}(B) < \underline{d}(A + B)\,.$$

Recently Yuri Bilu analysed the case when

$$\underline{d}(A + A) \leq \sigma \underline{d}(A)\,,$$

where $\sigma \in [2, 5/2]$.

To prove his theorem Kneser had to consider, for some positive integer g, sets of residues A and B modulo g for which

$$|A + B| = |A| + |B| - 1\,.$$

Cauchy [38] and Davenport [50] have proved that if $A \subseteq \mathbb{Z}_p$ and $B \subseteq \mathbb{Z}_p$, where p is a prime, then

$$|A+B| \geq \min\big(p,\ |A|+|B|-1\big)\,.$$

This inequality is analogous to (8).

Vosper [257] proved that if $A, B \subseteq \mathbb{Z}_p$, $|A|+|B|-1 \leq p-2$ and $\min(|A|,|B|) \geq 2$ then from $|A+B| = |A|+|B|-1$ it follows that A and B are arithmetic progressions in $\mathbb{Z}_p$ with the same difference.

Theorems of Kneser, Cauchy-Davenport and Vosper were amongst the first results giving solutions of inverse additive problems.

13. We may ask, are there any applications of the ideas and results described in §§4–8? For an answer to this question we turn now to the extremal combinatorial problems of Paul Erdős.

We begin with the problem raised by Erdős and Freud [68]. Fix some positive integer, ℓ. Denote by A a set of x natural numbers, $\{a_1, a_2, \ldots, a_x\}$, with $1 \leq a_1 < a_2 < \cdots < a_x \leq \ell$. Take the set, $A_0 = \{3, 6, 9, \ldots, 3\left[\frac{\ell}{3}\right]\}$. For each subset $B \subset A_0$ the sum of elements in B, the *subset sum*, is divisible by 3 and thus not equal to any power of 2. In this case $|A_0| = \left[\frac{\ell}{3}\right]$.

However if we take $|A| > \left[\frac{\ell}{3}\right]$ then for sufficiently large ℓ there exist $B \subset A$ and $s \in \mathbb{N}$ such that $\sum\limits_{a_i \in B} a_i = 2^s$. This was proved in [70]. E. Lipkin [167] proved that, for sufficiently large ℓ, a set of maximal cardinality, none of whose subset sums is equal to a power of two, must be exactly the set A_0.

The desired result was achieved with the help of analytical methods. However, there was a difficulty — how to apply them to prove a result which is valid for some integer, say, $\left[\frac{\ell}{3}\right]+1$, but is not valid for an integer which is one less. To cope with this, some conditions were formulated, so that when satisfied an analytical treatment could be used. The case where these conditions were not fulfilled was treated as an inverse additive problem. The structure of such sets was thus determined and it then became possible to finish the proof. (For more details, see §28.)

One might think that the problem of representing powers of two by subset sums is rather special, even artificial and therefore not that interesting. But, Paul Erdős knows how to ask questions. Ideas developed in order to solve the problem explained here, have turned out to be sufficient to solve a wide range of problems in Integer Programming, see §23 and [41]–[44].

14. In the framework of the problem of the previous section we may ask the following questions.

1) Let $|A| > \left[\frac{\ell}{3}\right]$. What is the minimal cardinality $|B|$ of $B \subset A$, whose subset sum is equal to some power of 2?
2) What is the minimal number of summands required in the representation of a power of 2, if equal summands are allowed?

These questions were asked and answered in a paper of M. Nathanson and A. Sárkőzy [201]. The sufficient number of summands required was estimated to be at most 30360 and 3503, respectively. Using the Theorem of §5 it appeared to be possible to improve these estimates to 8 and 6, respectively (see [104]). We will here briefly

explain the main ideas. If we apply the Theorem of §5 to some set $A \subset [1, \ell]$, then under doubling the number of elements is multiplied, roughly, by 3 and the length of the segment where the sum $2A$ is situated is multiplied by 2. So, the density is multiplied, roughly, by $\frac{3}{2}$. After the doubling is repeated twice, the density of $4A$ will be $\geq \frac{1}{3} \cdot \frac{3}{2} \cdot \frac{3}{2} = \frac{3}{4}$. One more doubling (or more accurately summing $4A + 2A$) will give a long interval, in $8A$ (or even in $6A$), containing then some power of 2.

Noga Alon gave a simple example showing that 4 summands in the case of different and 3 summands in a case of possibly repeating summands are not, in general, sufficient. Recently, Vsevolod Lev [160] found the exact number of summands, in a case of possibly repeating ones. He showed that four summands are sufficient.

The following questions are of interest.

1) For given $|A|$ and s, find, $f(|A|, \ell, s)$, the minimum over all sets $A \subset [1, \ell]$ of order $|A|$, of the maximal length arithmetic progression contained in sA.
2) For given $|A|$ and L, find, $f(|A|, \ell, L)$, the maximum over all sets $A \subset [1, \ell]$ of order $|A|$, of the minimum number of summands, s, such that sA contains an arithmetic progression of length L.

15. Denote by $s^\wedge A$ the set of integers which can be written as a sum of s pairwise distinct elements from A. The set A is called *admissible* if, and only if, $s \neq t$ implies that $s^\wedge A$ and $t^\wedge A$ have no element in common.

E.G. Straus [247] showed that the set $\{N - k + 1, N - k + 2, \dots, N\}$ is admissible if, and only if, $k \leq 2\sqrt{N + \frac{1}{4}} - 1$. He proved that for any admissible set $A \subset [1, N]$ we have $|A| \leq (4/\sqrt{3} + o(1))\sqrt{N}$. The constant involved was slightly reduced by P. Erdős, J-L. Nicolas and A. Sárkőzy (cf. [75]). In the paper of J-M. Deshouillers and G. Freiman [52] (see also [51]) Erdős' conjecture was proved, at least when N is sufficiently large.

Theorem 3. — *There exists an integer N_0 such that for any integer $N \geq N_0$ and any admissible subset $A \subset [1, N]$ we have,*

$$|A| \leq 2\sqrt{N + \frac{1}{4}} - 1 .$$

The proof was obtained with the help of methods of the type quoted in §5.

16. Let $A \subset [1, n]$. If $A \cap (A + A) = \varnothing$, the set A is called sum-free. P. Erdős and P.J. Cameron conjectured that for the number I_n of sum-free sets we have,

$$I_n = O(2^{n/2}) . \tag{9}$$

The typical example of sum-free set $A \subset [1, n]$ is the set $\{1, 3, 5, \dots\}$ of odd numbers. We can show that $[\frac{n+1}{2}]$ is the maximal cardinality of a sum-free set.

In G. Freiman [101] and the paper of J-M. Deshouillers, G. Freiman, V. Sos and M. Temkin [54], the problem of structure of sum-free sets was raised and studied. It was solved in the case of large cardinality of A, namely, when $|A| > 0.4\ell - c$, where c is some positive constant. An example of such a structure is one in which all the elements of A are congruent to 2 or 3 modulo 5.

The structure of A having been found, the estimate (9) for this class of A, now follows immediately. An open question is to describe the structure of A for smaller cardinalities.

17. In the paper of G. Freiman, L. Low and J. Pitman [106], the following conjecture of Erdős and Heilbronn [73] is proved for sufficiently large primes. *For $A \subset \mathbb{Z}_p$, where p is a prime, $|A| = k < p/50$ and $k > 60$, we have*

$$|A + A| \geq 2k - 3 .$$

Also, the structure of A was described in the case when $|A + A| < 2.06k - 3$. The conjecture of Erdős and Heilbronn was proved independently by J.A. Dias da Silva and Y.O. Hamidoune, see [246].

18. In the paper of A. Yudin [261], an example of large sets of integers, A, was constructed for which

$$|A + A| < |A - A|^c$$

where $c = 0.756$. The previous example [113] gave only $c = 0.89$. In [113] the estimate $c \geq 0.75$ was proved. The result of A. Yudin puts the important additive characteristic,

$$\liminf \frac{\log |A + A|}{\log |A - A|} = \alpha ,$$

in a very narrow interval, $0.75 \leq \alpha \leq 0.756$, and allows one to begin to study the structure of sets with values of c which are close to α. Possibly the example of Yudin is not far from an extremal structure (look at §7).

19. In the paper of E. Lipkin [169], the Diderich conjecture [62] was studied. We now describe the conjecture. Let G be a finite Abelian group, $A \subset G$ with $0 \notin A$. Let A^* denote the set of subset sums of the set A. G.T. Diderich called the minimal number n such that, if $|A| \geq n$ then $A^* = G$, the *critical number*, $c(G)$ of the group G.

Let G be an Abelian group of odd order $|G| = ph$ where p is the least prime divisor of $|G|$ and h is a composite integer. Diderich conjectured, and E. Lipkin proved for $G = \mathbb{Z}_q$ when q is sufficiently large, that

$$c(G) = p + h - 2 .$$

20. In §§21–27 we will give a few examples of problems in different fields which may be looked at and treated as Structure Theory problems. These examples will be chosen from Additive Number Theory (§21), Combinatorial Number Theory (§22), Integer Programming (§23), Probability Theory (§24), Coding Theory (§25), Group Theory (§26) and Mathematical Statistics (§27). Our aim is not so much to enumerate these problems as to show how ideas and methods of Structure Theory may influence their solution and to show their interdependence. Not many examples are chosen and they do not cover the whole stock of related problems.

21. Additive Number Theory. We now present a paper (see [109]) of G. Freiman, H. Halberstam and I.Z. Ruzsa. This paper confronts the problem of how to show that, starting from some set of integers A, the set rA contains an arithmetic progression of integers of length, L, and difference, d.