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].