Astérisque

GREGORY A. FREIMAN
LEWIS LOW
JANE PITMAN

Sumsets with distinct summands and the Erdős-Heilbronn conjecture on sums of residues

Astérisque, tome 258 (1999), p. 163-172
<http://www.numdam.org/item?id=AST_1999__258__163_0>

Astérisque **258**, 1999, p. 163–172

SUMSETS WITH DISTINCT SUMMANDS AND THE ERDŐS-HEILBRONN CONJECTURE ON SUMS OF RESIDUES

by

Gregory A. Freiman, Lewis Low & Jane Pitman

Abstract. — Let S be a set of integers or of residue classes modulo a prime p, with cardinality $|S| = k$, and let T be the set of all sums of two distinct elements of S. For the integer case, it is shown that if $|T|$ is less than approximately $2.5k$ then S is contained in an arithmetic progression with relatively small cardinality. For the residue class case a result of this type is derived provided that $k > 60$ and $p > 50k$. As an application, it is shown that $|T| \geq 2k-3$ under these conditions. Earlier results of Freiman play an essential role in the proofs.

1. Introduction

1.1. Let Z be the set of all integers and let F_p be the finite field of residue classes modulo p, where p is a prime number. If A is a subset of Z or F_p (written $A \subset Z$ or $A \subset F_p$) we denote the cardinality of A by $|A|$. For a finite subset A of Z or F_p we shall consider $2A$, the set of all sums of two elements of A, and also $2^\wedge A$, the set of all sums of two *distinct* elements of A, that is,

$$\begin{aligned} 2A &= \{a+b : a,b \in A\}, \\ 2^\wedge A &= \{a+b : a,b \in A,\ a \neq b\}. \end{aligned}$$

1.2. Sums of elements from a set of integers. — First we consider the sumset $2A$ for $A \subset Z$. We write

$$A = \{a_0, a_1, \ldots, a_{k-1}\}, \quad k = |A|,$$

where

$$a_0 < a_1 < \cdots < a_{k-1}\ .$$

Since the $k-1$ sums $a_i + a_{i+1}$ and the k sums $a_i + a_i = 2a_i$ are all distinct we have

$$|2A| \geq 2k-1, \tag{1}$$

1991 ***Mathematics Subject Classification.*** — 11 B75, 11 B13.
Key words and phrases. — sumset, set addition, sums of residues.

and it is easily seen that equality holds if and only if A is an arithmetic progression (that is, the differences $a_{i+1} - a_i$ are all equal). Freiman [6, page 11] has proved the following more precise result (which will be used in Section 2 below).

***Theorem A* (Freiman).** — *Let $D \subset Z$. If $|2D| \leq 2|D| - 1 + C_1$, where $C_1 \leq |D| - 3$, then $D \subset L$, where L is an arithmetic progression such that*

$$|L| \leq |D| + C_1$$

(so that D is obtained by deleting at most C_1 terms from the arithmetic progression L).

1.3. Sums of elements from a subset of F_p. — Next we look at $2A$ for $A \subset F_p$ such that $|A| = k$. By analogy with (1) we have the following special case of the well-known Cauchy-Davenport theorem:

$$|2A| \geq \min(p, 2k - 1). \tag{2}$$

More detailed results have been obtained by various authors and Freiman [6, p.46] has used the above theorem on $2D$ for $D \subset Z$ to obtain the following result in the same vein for $A \subset F_p$.

***Theorem B* (Freiman).** — *Let $A \subset F_p$ such that*

$$|A| = k < p/35.$$

Suppose that $|2A| = 2k - 1 + b$, $b < 0.4k - 2$. Then $A \subset L$, where L is an arithmetic progression in F_p such that $|L| = k + b$.

1.4. Sums with distinct summands and the Erdős-Heilbronn conjecture

For $A \subset Z$ as in 1.2 above, the $k - 1$ sums $a_i + a_{i+1}$ and the $k - 2$ sums $a_i + a_{i+2}$ are all distinct and belong to $2^{\wedge}A$. Thus

$$|2^{\wedge}A| \geq 2k - 3, \tag{3}$$

and it can be checked that for $k \geq 5$ equality holds if and only if A is an arithmetic progression.

By analogy with the Cauchy-Davenport theorem (2), Erdős and Heilbronn conjectured in the 1960's (see Erdős and Graham [5]) that for $A \subset F_p$ such that $|A| = k$ we must have

$$|2^{\wedge}A| \geq \min(p, 2k - 3). \tag{4}$$

Although there is a short elementary proof of (2) (see, for example, Davenport [3]), the corresponding result for distinct summands seems to be more difficult. As discussed further below, the full conjecture (4) has been proved since 1993. The main published contribution prior to 1993 seems to be that of Mansfield [7], who proved the following theorem.

***Theorem* (Mansfield).** — *Let $A \subset F_p$ such that $|A| = k$. Then the Erdős-Heilbronn conjecture (4) is true if*

$$\text{either} \quad k \leq 11 \quad \text{or} \quad 2^{k-1} \leq p.$$

Our aim in this paper was to develop analogues for $2^{\wedge}A$ of Freiman's results on $2D$, both for $D \subset Z$ and for $A \subset F_p$, which would be strong enough for the purposes of proving (4) for a wider range, as well as being of independent interest.

1.5. Results obtained. — In Section 2 we use simple combinatorial arguments together with Freiman's theorem on $2D$ for $D \subset Z$ to prove the following theorem.

Theorem 1. — *Let D be a set of k integers for which*

$$|2^{\wedge}D| \leq 2k - 3 + C,$$

where

$$0 \leq C \leq \frac{1}{2}(k-5).$$

Then D is contained in an arithmetic progression L such that

$$|L| \leq k + 2C + 2.$$

In Section 3 we use Theorem 1 and arguments based on trigonometric sums to prove the main result of the paper, which is as follows.

Theorem 2. — *Let $A \subset F_p$ such that*

$$|A| = k < \frac{p}{50}, \quad k > 60.$$

Suppose that

$$|2^{\wedge}A| \leq 2k - 3 + C,$$

where $C < 0.06k$. Then $A \subset L$, where L is an arithmetic progression in F_p such that

$$|L| \leq k + 2C + 2.$$

As a corollary, we will show that for $A \subset F_p$ such that $|A| = k$ the Erdős-Heilbronn conjecture (4) is true if

$$k < \frac{p}{50}, \quad k > 60. \tag{5}$$

Pybus [10] told us that he had obtained a proof of a version of the Erdős-Heilbronn conjecture based on different ideas. More recent work by others, including proofs of the full conjecture, will be discussed in Section 4 at the end of the paper.

1.6. Isomorphisms. — We note that the sumsets $2A$ and $2^{\wedge}A$ can be considered for any set A with addition. If A and B are two sets, each with an addition, and $\phi : A \to B$ is a bijection, we call ϕ an isomorphism if and only if

$$\phi(a) + \phi(b) = \phi(c) + \phi(d) \Leftrightarrow a + b = c + d.$$

We call A and B as above *isomorphic* if such an isomorphism exists, in which case we have

$$|2A| = |2B| \quad \text{and} \quad |2^{\wedge}A| = |2^{\wedge}B|.$$

We shall use the fact that affine transformations of Z or F_p are isomorphisms.

2. Sums of distinct elements from a set of integers

2.1. In this section we consider a set of integers A such that $|A| = k$ and use notation as at the beginning of section 1.2, together with some further vocabulary as follows. We note that $2^\wedge A$ is isomorphic to the set

$$\{\tfrac{1}{2}(a_i + a_j) : 1 \leq i < j \leq n\}$$

and it is helpful to think geometrically in terms of the points a_i and the mid-points of pairs a_i, a_j $(i < j)$. We shall say that a_i is *representable* if and only if a_i coincides with one of the mid-points, that is

$$2a_i \in 2^\wedge A.$$

We shall call a sum $a_i + a_{i+s}$ with $s \geq 1$ an *s-step sum*, and we recall that the 1-step and 2-step sums are all distinct. For $s \geq 1$, an s-step sum will be called *new* if and only if it is not equal to any j-step sum with $1 \leq j < s$. All 1-step and 2-step sums are new, but for $s \geq 3$ an s-step sum is not necessarily new. We shall use the notations

$$\begin{aligned} k_1 = k_1(A) &= \text{total number of } \textit{new } s\text{-step sums with } s \geq 3, \\ k_2 = k_2(A) &= \text{number of } a_j\text{'s which are } \textit{representable.} \end{aligned}$$

If an s-step sum $a_i + a_{i+s}$ is not new, then for some j, k such that $i < j < j+k < i+s$ we must have

$$a_i + a_{i+s} = a_j + a_{j+k}$$

and hence

$$0 < a_j - a_i = a_{i+s} - a_{j+k}\ .$$

We therefore consider the associated *difference set*

$$\mathcal{D}(a_i, a_{i+s}) = (a_{i+1} - a_i, a_{i+2} - a_{i+1}, \ldots, a_{i+s} - a_{i+s-1}).$$

Our proof of Theorem 1 will be based on the following lemma.

Lemma. — *For $A \subset Z$ such that $|A| = k$, $k \geq 5$, let k_1, k_2 be the number of new s-step sums with $s \geq 3$ and the number of representable elements of A as defined above. Then*

$$k_1 + k_2 \geq k - 4. \tag{6}$$

Proof. — Consider a particular subscript i such that $0 \leq i \leq k - 5$. If $a_i + a_{i+3}$ is not new we must have

$$\mathcal{D}(a_i, a_{i+3}) = (x, y, x)$$

for some $x, y > 0$, and so

$$\mathcal{D}(a_i, a_{i+4}) = (x, y, x, z)$$

for some z. If $z = x$ or $z = x + y$ then a_{i+3} is a mid-point and so is representable, while if $z \neq x$ and $z \neq x + y$ then $a_i + a_{i+4}$ is new. Thus at least one of the following three statements holds:

(i) $a_i + a_{i+3}$ is new; (ii) $a_i + a_{i+4}$ is new; (iii) a_{i+3} is representable.