Astérisque

VSEVOLOD F. LEV

The structure of multisets with a small number of subset sums

Astérisque, tome 258 (1999), p. 179-186
<http://www.numdam.org/item?id=AST_1999__258__179_0>

Astérisque **258**, 1999, p. 179–186

THE STRUCTURE OF MULTISETS WITH A SMALL NUMBER OF SUBSET SUMS

by

Vsevolod F. Lev

Abstract. — We investigate multisets of natural numbers with relatively few subset sums. Namely, let A be a multiset such that the number of distinct subset sums of A is bounded by a fixed multiple of the cardinality of A (that is, $|P(A)| \ll |A|$). We show that the set $P(A)$ of subset sums is then a union of a small number of arithmetic progressions sharing a common difference.

Similar problems were considered by G. Freiman (see [1]) and M. Chaimovich (see [2]). Unlike those papers, our conditions are stated in terms of the cardinality of the subset sums set $P(A)$ only and not on the largest element of the original multiset A.

The result obtained is nearly best possible.

1. Notation and definitions

By a *multiset* we mean a finite collection of natural numbers with repetitions allowed: $A = \{a_1, \ldots, a_k\}$, where $a_1 \leq \cdots \leq a_k$ are the elements of A. The number of appearances of an element will be called its *multiplicity.*

As with "normal" sets, $|A| = k$ is called the *cardinality* of A. The sum of all elements of the multiset is $\sigma(A) = a_1 + \cdots + a_k$, and its *subset sums set* is

$$P(A) = \{\varepsilon_1 a_1 + \cdots + \varepsilon_k a_k \colon 0 \leq \varepsilon_1, \ldots, \varepsilon_k \leq 1\}.$$

Notice that 0 and $\sigma(A)$ are both included in $P(A)$; generally, e belongs to $P(A)$ if and only if $\sigma(A) - e$ does.

Another useful notation:

$$A = \{a_1 \times k_1, \ldots, a_s \times k_s\},$$

meaning that $a_1 < \cdots < a_s$ are *distinct* elements of A with multiplicities $k_1, \ldots, k_s \geq 1$. In these terms, the cardinality of A is $|A| = k_1 + \cdots + k_s$, the sum of its elements is $\sigma(A) = k_1 a_1 + \cdots + k_s a_s$, and its subset sums set is

$$P(A) = \{\kappa_1 a_1 + \cdots + \kappa_s a_s \colon 0 \leq \kappa_1 \leq k_1, \ldots, 0 \leq \kappa_s \leq k_s\}.$$

1991 ***Mathematics Subject Classification.*** — 11P99, 11B75.
Key words and phrases. — Subset sums, small doubling, multisets.

2. The main result

The following theorem is our main result.

Theorem 1. — *Let A satisfy*

$$|P(A)| \leq C|A| - 4C^3, \tag{1}$$

where C is a natural number, and suppose that the cardinality of A is sufficiently large: $|A| \geq 8C^3$. Then $P(A)$ is a union of at most $C-1$ arithmetic progressions with the same common difference.

Theorem 1 (the proof of which will be given in Section 5) is somewhat unusual in describing the structure of the subset sums set $P(A)$ rather then the structure of the multiset A itself. As the reader will notice, this reflects the essence of the problem: one can change A substantially without affecting $P(A)$, and thus it seems impossible to describe the structure of A under any reasonable condition on $P(A)$.

I conjecture that (1) can be replaced by the weaker restriction

$$|P(A)| \leq C|A| - (C-1)^2. \tag{2}$$

The following examples show that inequality (2) cannot be further relaxed.

Example 1. — *Let $A = \{1 \times (k - C + 1), b \times (C - 1)\}$, where $k = |A|$ and b are sufficiently large. Then $P(A)$ is the union of C progressions*

$$\begin{gathered} 0, 1, \ldots, k - C + 1, \\ b, b+1, \ldots, b + (k - C + 1), \\ \cdots \\ (C-1)b, (C-1)b + 1, \ldots, (C-1)b + (k - C + 1), \end{gathered}$$

so that $|P(A)| = C(k - C + 2) = Ck - (C-1)^2 + 1$. However, $P(A)$ cannot be represented as a union of at most $C - 1$ arithmetic progressions with a common difference.

Example 2. — *Let $A = \{1 \times (C - 1), b \times (k - C + 1)\}$, where $k = |A|$ and b are sufficiently large. Then $P(A)$ is the union of C progressions*

$$\begin{gathered} 0, b, \ldots, (k - C + 1)b, \\ 1, 1 + b, \ldots, 1 + (k - C + 1)b, \\ \cdots \\ C - 1, C - 1 + b, \ldots, C - 1 + (k - C + 1)b, \end{gathered}$$

so that $|P(A)| = Ck - (C-1)^2 + 1$, and again $P(A)$ cannot be represented as a union of at most $C - 1$ arithmetic progressions with a common difference.

Note that in view of Lemma 2 below, the inequality $|P(A)| \geq |A| + 1$ is always true. Hence, the conditions of Theorem 1 are never satisfied for $C = 1$, and from now on we assume $C \geq 2$.

3. Small values of C

For A satisfying (1) (or even (2)) with small values of C ($C = 2, 3$) the structure of $P(A)$, as well as the structure of A itself, can be completely described.

We begin with some basic properties of subset sums set. First, we estimate by how much $|P(A)|$ increases if one adds an element to A.

Lemma 1. — *Let $A = \{a_1 \times k_1, \ldots, a_s \times k_s\}$, $A^+ = A \cup \{a\}$, and suppose that A contains at least $i-1$ different elements less then a (that is, $a > a_{i-1}$ unless $i = 1$). Then*

$$|P(A^+)| \geq |P(A)| + i.$$

Proof. — $P(A^+)$ contains all the elements of $P(A)$, as well as the i additional elements

$$\sigma(A) + a, \sigma(A) + a - a_1, \ldots, \sigma(A) + a - a_{i-1}.$$

□

As a direct corollary, we obtain a lower-bound estimate for $|P(A)|$.

Lemma 2. — *The cardinality of the subset sums set $P(A)$ of the multiset*

$$A = \{a_1 \times k_1, \ldots, a_s \times k_s\}$$

satisfies

$$|P(A)| \geq 1 + k_1 + 2k_2 + \cdots + sk_s.$$

In particular, $|P(A)| \geq 1 + |A|$.

Proof. — The assertion is obviously true for $|A| = 1$, and we use induction on $|A|$. Denote by A^- the multiset obtained by removing from A its largest element a_s. Applying Lemma 1, we obtain then

$$\begin{aligned} |P(A)| &\geq |P(A^-)| + s \geq (1 + k_1 + 2k_2 + \cdots + s(k_s - 1)) + s \\ &= 1 + k_1 + 2k_2 + \cdots + sk_s. \end{aligned}$$

□

It follows from Lemma 2 that a multiset A with relatively small value of $|P(A)|$ has at least one element with large multiplicity.

Lemma 3. — *Let $A = \{a_1 \times k_1, \ldots, a_s \times k_s\}$, and let $k_0 = \max_{1 \leq i \leq s} k_i$ be the maximal multiplicity of an element of A. Then*

$$k_0 > \frac{k^2}{2|P(A)|}.$$

Proof. — For $1 \leq i \leq s$ we have:

$$\begin{aligned} |P(A)| &\geq 1 + k_1 + 2k_2 + \cdots + ik_i + (i+1)(k_{i+1} + \cdots + k_s) \\ &> (i+1)k - (k_i + 2k_{i-1} + \cdots + ik_1) \\ &\geq (i+1)k - \frac{1}{2}i(i+1)k_0. \end{aligned}$$

The resulting estimate

$$|P(A)| > (i+1)k - \frac{1}{2}i(i+1)k_0$$

also holds for $i > s$, as in this case the expression in the right-hand side, considered as a function of real i, has a negative derivative:

$$k - \frac{1}{2}(2i+1)k_0 < k - sk_0 \leq 0.$$

Hence,

$$k_0 > \frac{2}{i}\left(k - \frac{|P(A)|}{i+1}\right)$$

for every $i = 1, 2, \ldots$ We choose i under the condition

$$2\frac{|P(A)|}{k} - 1 \leq i < 2\frac{|P(A)|}{k}.$$

Then

$$\frac{2}{i} > \frac{k}{|P(A)|}, \quad \frac{|P(A)|}{i+1} \leq \frac{k}{2},$$

and so

$$k_0 > \frac{k}{|P(A)|} \cdot \frac{k}{2} = \frac{k^2}{2|P(A)|}.$$

□

We now construct multisets whose subset sums sets have a particularly simple structure.

Example 3. — *Let $A = \{a_1, \ldots, a_k\}$ be a multiset such that*

i) $a_2, \ldots, a_k \equiv 0 \pmod{a_1}$;

ii) $a_{i+1} \leq a_1 + \cdots + a_i$ for $i = 1, \ldots, k-1$.

Then $P(A)$ is an arithmetic progression: $P(A) = \{0, a_1, 2a_1, \ldots, \sigma(A)\}$.

This easily follows by induction on k: if $A^- = \{a_1, \ldots, a_{k-1}\}$, then

$$\begin{aligned} P(A) &= P(A^-) \cup (a_k + P(A^-)) \\ &= \{0, a_1, \ldots, \sigma(A^-)\} \cup \{a_k, a_k + a_1, \ldots, a_k + \sigma(A^-)\} \\ &= \{0, a_1, \ldots, \sigma(A)\}, \end{aligned}$$

since $a_k \leq \sigma(A^-)$ and $a_k + \sigma(A^-) = \sigma(A)$.

Proposition 1. — *Any multiset A, satisfying $|P(A)| \leq 2|A| - 1$ (that is satisfying (2) with $C = 2$) has the structure, described in Example 3.*

Proof. — Suppose, on the contrary, that there exists an index $2 \leq i \leq k$ for which either $a_i \not\equiv 0 \pmod{a_1}$ or $a_i > a_1 + \cdots + a_{i-1}$; we assume, moreover, that i is the *minimum* index with this property. Then, writing $A_j = \{a_1, \ldots, a_j\}$ $(j = 1, \ldots, k)$ and applying Lemma 2, we obtain

$$|P(A_i)| = 2|P(A_{i-1})| \geq 2i$$