SUMS OF FINITE SETS OF INTEGERS, II

MEILYNN B. NATHANSON

Abstract. A fundamental result in additive number theory states that, for every finite set $A$ of integers, the $h$-fold sumset $hA$ has a very simple and beautiful structure for all sufficiently large $h$. Let $(hA)^{(t)}$ be the set of all integers in the sumset $hA$ that have at least $t$ representations as a sum of $h$ elements of $A$. It is proved that the set $(hA)^{(t)}$ has a similar structure.

1. Structure of sumsets.

G. H. Hardy and E. M. Wright [4, p. 361] clearly stated the general problem of additive number theory.

Suppose that $A$ or $a_1, a_2, a_3, \ldots$ is a given system of integers. Thus $A$ might contain all the positive integers, or the squares, or the primes. We consider all representations of an arbitrary positive integer $n$ in the form

$$n = a_{i_1} + a_{i_2} + \cdots + a_{i_s},$$

\ldots We denote by $r(n)$ the number of such representations. Then what can we say about $r(n)$?

Many classical problems are still unsolved. For example, we do not know what numbers are sums of four cubes.

Much recent work concerns sums of arbitrary sets of integers. The $h$-fold sumset of a set $A$ of integers is the set $hA$ consisting of all integers that can be represented as the sum of $h$ not necessarily distinct elements of $A$. Additive number theory studies $h$-fold sumsets. For every finite or infinite set $A$ of integers, we would like to know the structure of the sumsets $hA$ for small $h$ and, asymptotically, as $h$ goes to infinity. A fundamental theorem of additive number theory, published 50 years ago in [7][8], explicitly solves the asymptotic problem for finite sets of integers.

Define the interval of integers $[u, v] = \{ n \in \mathbb{Z} : u \leq n \leq v \}$. For every set $D$ and integer $w$, let $w - D = \{ w - d : d \in D \}$.

Theorem 1. Let $A = \{a_0, a_1, \ldots, a_k\}$ be a finite set of integers such that $0 = a_0 < a_1 < \cdots < a_k$ and $\gcd(A) = 1$.

Let

$$h_1 = (k - 1)(a_k - 1)a_k + 1.$$ 

There are nonnegative integers $c_1$ and $d_1$ and finite sets $C_1$ and $D_1$ with

$$C_1 \subseteq [0, c_1 - 2] \quad \text{and} \quad D_1 \subseteq [0, d_1 - 2].$$

2010 Mathematics Subject Classification. Primary 11B13. Secondary 11B34, 11D07.

Key words and phrases. Additive number theory; sumsets, representation functions.
such that
\[ hA = C_1 \cup [c_1, ha_k - d_1] \cup (ha_k - D_1) \]
for all \( h \geq h_1 \).

Thus, for \( h \) sufficiently large, the sumset \( hA \) consists of a long interval of consecutive integers, with a small initial fringe \( C_1 \) and small terminal fringe \( ha_k - D_1 \). This structure is rigid. In the sumset \((h + 1)A\), the length of the interval increases by \( a_k \), the initial fringe \( C_1 \) is unchanged, and the terminal fringe translates to the right by \( a_k \).

The integer \( FN_1(A) = c_1 - 1 \) is the Frobenius number of the set \( A \), that is, the largest number that cannot be represented as a nonnegative integral linear combination of elements of \( A \). This is often presented as the Frobenius coin problem: Find the largest amount that cannot be obtained using only coins with denominations \( a_1, \ldots, a_k \).

Smaller values for the number \( h_1 \) have been obtained by Wu, Chen, and Chen [10], Granville and Shakan [1], and Granville and Walker [2].

Let \( B \) be a finite set of integers with \( |B| \geq 2 \). If \( \min(B) = b_0 \) and \( \gcd(B - b_0) = d \), then the “normalized set”
\[ A = \left\{ \frac{b - b_0}{d} : b \in B \right\} \]
is a finite set of nonnegative integers with \( \min(A) = 0 \) and \( \gcd(A) = 1 \). We have
\[ hB = hb_0 + \{ dx : x \in hA \}. \]
for all positive integers \( h \). Thus, Theorem 1 describes the asymptotic structure of the sumsets of every finite set of integers.

Han, Kirfel, and Nathanson [3] extended Theorem 1 to linear forms of finite sets of integers. Khovanski˘ı [5, 6] and Nathanson [9] proved the exact polynomial growth of sums of finite sets of lattice points, and, more generally, of linear forms of finite subsets of any additive abelian semigroup.

2. Representation functions.

Let \( A \) be a set of integers. For every positive integer \( h \), the \( h \)-fold representation function \( r_{A,h}(n) \) counts the number of representations of \( n \) as the sum of \( h \) elements of \( A \). Thus,
\[ r_{A,h}(n) = \text{card} \left\{ (a_j, \ldots, a_{jh}) \in A^h : n = \sum_{i=1}^{h} a_j, \text{ and } a_j_1 \leq \cdots \leq a_{jh} \right\}. \]

Equivalently, if \( \mathbb{N}_0^A \) is the set of all sequences of nonnegative integers indexed by the elements of \( A \), then
\[ r_{A,h}(n) = \text{card} \left\{ (u_a)_{a \in A} \in \mathbb{N}_0^A : \sum_{a \in A} u_a a = n \text{ and } \sum_{a \in A} u_a = h \right\}. \]

For every positive integer \( t \), let \((hA)^{(t)} \) be the set of all integers \( n \) that have at least \( t \) representations as the sum of \( h \) elements of \( A \), that is,
\[ (hA)^{(t)} = \{ n \in \mathbb{Z} : r_{A,h}(n) \geq t \}. \]
The following result completely determines the structure of the sumsets \((hA)^{(t)} \) for all \( t \) and for all sufficiently large \( h \).
Theorem 2. Let $k \geq 2$, and let $A = \{a_0, a_1, \ldots, a_k\}$ be a finite set of integers such that

\[ 0 = a_0 < a_1 < \cdots < a_k \quad \text{and} \quad \gcd(A) = 1. \]

For every positive integer $t$, let

\[ h_t = (k-1)(ta_k - 1)a_k + 1. \]

There are nonnegative integers $c_t$ and $d_t$ and finite sets $C_t$ and $D_t$ with

\[ C_t \subseteq [0, c_t - 2] \quad \text{and} \quad D_t \subseteq [0, d_t - 2] \]

such that

\[ (hA)^{(t)} = C_t \cup [c_t, ha_k - d_t] \cup (ha_k - D_t) \]

for all $h \geq h_t$.

It is remarkable that the sumsets $(hA)^{(t)}$ have the same structure as the sumset $hA$.

3. Proof of Theorem 2

The proofs of the following lemmas are in Section 5.

Lemma 1. Let $A$ be a set of integers. For all positive integers $h$ and $t$,

\[ (hA)^{(t)} + A \subseteq ((h + 1)A)^{(t)}. \]

Lemma 2. Let $k \geq 2$ and let $A = \{a_0, a_1, \ldots, a_k\}$ be a finite set of integers with

\[ 0 = a_0 < a_1 < \cdots < a_k \quad \text{and} \quad \gcd(A) = 1. \]

For every positive integer $t$, let

\[ c'_t = (ta_k - 1) \sum_{j=1}^{k-1} a_j \]

and

\[ d'_t = (k-1)(ta_k - 1)a_k. \]

For every positive integer $h$,

\[ [c'_t, ha_k - d'_t] \subseteq (hA)^{(t)}. \]

We now prove Theorem 2

Proof. Let $t$ be a positive integer. Define $c'_t$ by (1) and $d'_t$ by (2). By Lemma 2, the set $(h_tA)^{(t)}$ contains the interval $[c'_t, h_t a_k - d'_t]$. Let $c_t$ and $d_t$ be the smallest integers such that

\[ [c'_t, h_t a_k - d'_t] \subseteq [c_t, h_t a_k - d_t] \subseteq (h_tA)^{(t)}. \]

Thus, $c_t \leq c'_t$ and $d_t \leq d'_t$. It follows that

\[ c_t - 1 \notin (h_tA)^{(t)} \quad \text{and} \quad h_t a_k - d_t + 1 \notin (h_tA)^{(t)}. \]

Define the finite sets $C_t$ and $D_t$ by

\[ C_t = [0, c_t - 1] \cap (h_tA)^{(t)} \]

and

\[ h_t a_k - D_t = [h_t a_k - d_t + 1, h_t a_k] \cap (h_tA)^{(t)}. \]
Thus, if \( n \) (We must prove that and so \( r \) and so \( r \). Therefore, Because \( c \) This gives 4 MELVYN B. NATHANSON

We shall prove that \( n \) has at least 1. However, \( h \in A \), Lemma [3] gives

(5) \( (hA)^{(t)} \cup (hA)^{(t)} + a_k \subseteq (hA)^{(t)} + A \subseteq ((h + 1)A)^{(t)} \)

and so \( C_t \subseteq (hA)^{(t)} \subseteq ((h + 1)A)^{(t)} \).

Because \( c' \leq d' = h_t - 1 \leq h - 1 \) and \( a_k \geq 2 \), we have

\[
-c_t + d_t = c' + d' \leq 2d'_t \leq a_k(h_t - 1) \leq a_k(h - 1).
\]

Therefore,

\[
c_t + a_k \leq ha_k - d_t
\]

and

\[
[c_t, c_t + a_k] \subseteq [c_t, ha_k - d_t] \subseteq (hA)^{(t)} \subseteq ((h + 1)A)^{(t)}.
\]

By [5],

\[
[c_t + a_k, (h + 1)a_k - d_t] = a_k + [c_t, ha_k - d_t]
\]

\[
\subseteq a_k + (hA)^{(t)}
\]

\[
\subseteq ((h + 1)A)^{(t)}
\]

and

\[
(h + 1)a_k - D_t = a_k + (ha_k - D_t)
\]

\[
\subseteq a_k + (hA)^{(t)}
\]

\[
\subseteq ((h + 1)A)^{(t)}.
\]

Therefore,

\[
B^{(t)} = C_t \cup [c_t, (h + 1)a_k - d_t] \cup ((h + 1)a_k - D_t) \subseteq ((h + 1)A)^{(t)}.
\]

We must prove that \( B^{(t)} = ((h + 1)A)^{(t)} \).

We have \( A \subseteq [0, a_k] \) and

\[
((h + 1)A)^{(t)} \subseteq (h + 1)A \subseteq (h + 1)[0, a_k] = [0, (h + 1)a_k].
\]

Thus, if \( n \in ((h + 1)A)^{(t)} \setminus B^{(t)} \), then \( 0 \leq n \leq c_t - 1 \) or \( (h + 1)a_k - d_t + 1 \leq n \leq (h + 1)a_k \).

If \( n \in ((h + 1)A)^{(t)} \setminus B^{(t)} \) and \( n \leq c_t - 1 \), then

\[
n \notin C_t = [0, c_t - 1] \cap (hA)^{(t)}
\]

and so \( r_{A,h}(n) \leq t - 1 \). However, \( n \in ((h + 1)A)^{(t)} \) means \( r_{A,h+1}(n) \geq t \). Therefore, \( n \) has at least \( t \) representations as the sum of \( h + 1 \) elements of \( A \), but at most \( t - 1 \) representations as the sum of \( h \) elements of \( A \). It follows that \( n \) has at least one representation as the sum of \( h + 1 \) positive elements of \( A \), and so

\[
n \leq c_t - 1 \leq c' - 1 \leq h_t \leq h < (h + 1)a_1 \leq n
\]

which is absurd. Therefore, if \( n \in ((h + 1)A)^{(t)} \) and \( n < c_t \), then \( n \in C_t \subseteq B^{(t)} \).
If \( n \in ((h+1)A)^{(t)} \setminus B^{(t)} \) and \( n \geq (h+1)a_k - d_t + 1 \), then
\[
 n \notin (h+1)a_k - D_t
\]
and so
\[
 n - a_k \notin ha_k - D_t = [ha_k - d_t + 1, ha_k] \cap (hA)^{(t)}.
\]
Therefore, \( r_{A,h}(n-a_k) \leq t-1 \). However, \( n \in ((h+1)A)^{(t)} \) implies that \( r_{A,h+1}(n) \geq t \), and so there is at least one representation of \( n = a_{i_1} + \cdots + a_{i_{h+1}} \) with \( a_{i_j} \leq a_{k-1} \) for all \( j \in [1, h+1] \). It follows that
\[
 (h+1)a_k - d_t + 1 \leq n \leq (h+1)a_{k-1} \leq (h+1)(a_k - 1)
\]
and so
\[
 h_t \leq h \leq d_t - 2 \leq d'_t - 2 = h_t - 3
\]
which is absurd. Therefore,
\[
 n \in (h+1)a_k - D_t \subseteq B^{(t)}.
\]
It follows that \((h+1)A)^{(t)} = B^{(t)}\). This completes the proof. \( \square \)

If \( A \) is a finite set of integers with \( \min(A) = 0 \) and \( \gcd(A) = 1 \), then \( FN_t(A) = c_t - 1 \) is the largest integer that does not have \( t \) representations as the sum of elements of \( A \). Equivalently, \( r_{A,h}(c_t - 1) < t \) for all \( h \geq 1 \). We have the increasing sequence
\[
 FN_1(A) \leq \cdots \leq FN_t(A) \leq FN_{t+1}(A) \leq \cdots
\]
There is no efficient algorithm to compute the numbers \( FN_t(A) \), and very little is known about them.

4. Symmetry.

Let \( A = \{a_0, a_1, \ldots, a_k\} \) be a finite set of integers with
\[
 0 = a_0 < a_1 < \cdots < a_k.
\]
The dual set
\[
 A^* = \max(A) - A = \{a_k - a_j : j \in [0, k]\}
\]
satisfies \( (A^*)^* = A \) and \( \gcd(A) = \gcd(A^*) \). Because \( ha_k = \max(hA) = \max(hA^*) \), we have
\[
 n = \sum_{j=1}^h a_{i_j} \in hA
\]
if and only if
\[
 ha_k - n = \sum_{j=1}^h (a_k - a_{i_j}) \in hA^*.
\]
Thus, \((hA)^* = hA^*\). Similarly,
\[
 ( (hA)^{(t)} )^* = (hA^*)^{(t)}
\]
for all positive integers \( h \) and \( t \). It follows that if
\[
 (hA)^{(t)} = C_t \cup [c_t, ha_k - d_t] \cup (ha_k - D_t),
\]
then
\[(hA^*)^{(t)} = \left((hA)^{(t)}\right)^* = (C_t \cup [c_t, ha_k - d_t] \cup (ha_k - D_t))^* = D_t \cup [d_t, ha_k - c_t] \cup (ha_k - C_t)].
\]

If \(A = A^*\), then \(c_t = d_t\) and \(C_t = D_t\).

5. Proofs of the lemmas.

Now we prove Lemmas \(\text{1}\) and \(\text{2}\) from Section \(\text{3}\).

Proof of Lemma \(\text{1}\). Let \(n \in (hA)^{(t)}\). Because \(r_{A,h}(n) \geq t\), for \(s \in [1,t]\) there are distinct sequences \((u_{a,s})_{a \in A}\) of nonnegative integers that satisfy
\[
\sum_{a \in A} u_{a,s}a = n \quad \text{and} \quad \sum_{a \in A} u_{a,s} = h.
\]

For all \(a, a' \in A\), let
\[
u'_{a,s} = \begin{cases} u_{a,s} & \text{if } a \neq a' \\ u_{a,s} + 1 & \text{if } a = a'. \end{cases}
\]

The sequences \((\nu'_{a,s})_{a \in A}\) are also distinct for \(s \in [1,t]\), and satisfy
\[
\sum_{a \in A} \nu'_{a,s}a = n + a' \quad \text{and} \quad \sum_{a \in A} \nu'_{a,s} = h + 1.
\]

It follows that \(r_{A,h+1}(n + a') \geq t\), and so \((hA)^{(t)} + a' \subseteq ((h+1)A)^{(t)}\) for all \(a' \in A\). This completes the proof.

\(\Box\)

Proof of Lemma \(\text{2}\). If \(ha_k < c'_t + d'_t\), then the interval \([c'_t, ha_k - d'_t]\) is empty and \((6)\) is true.

Let \(ha_k \geq c'_t + d'_t\) and \(n \in [c'_t, ha_k - d'_t]\).

Because \(\gcd(A) = \gcd(a_1, \ldots, a_k) = 1\), there exist integers \(x'_1, \ldots, x'_k\) such that
\[
n = \sum_{j=1}^{k} x'_j a_j
\]

and so
\[
n \equiv \sum_{j=1}^{k-1} x'_j a_j \pmod{a_k}.
\]

For all integers \(s\), the interval \([{(s-1)a_k, sa_k - 1}]\) is a complete set of representatives for the congruence classes modulo \(a_k\). It follows that, for all \(j \in [1, k - 1]\) and \(s \in [1, t]\), there exist unique integers
\[(s)\]

such that
\[
x'_j \equiv x_{j,s} \pmod{a_k}.
\]

Therefore,
\[
n \equiv \sum_{j=1}^{k-1} x_{j,s} a_j \pmod{a_k}.
\]
There is a unique integer $x_{k,s}$ such that

$$n = \sum_{j=1}^{k} x_{j,s}a_j. \tag{7}$$

The inequality

$$\sum_{j=1}^{k-1} x_{j,s}a_j \leq \sum_{j=1}^{k-1} (sa_k - 1)a_j \leq (ta_k - 1)\sum_{j=1}^{k-1} a_j = c'_t \leq n$$

implies

$$x_{k,s}a_k = n - \sum_{j=1}^{k-1} x_{j,s}a_j \geq 0.$$ 

Thus, $x_{k,s} \geq 0$ for all $s \in [1,t]$, and so (7) is a nonnegative integral linear combination of elements of $A$.

We have

$$x_{k,s}a_k \leq n \leq ha_k - d'_t = ha_k - (k-1)(ta_k - 1)a_k$$

and so

$$x_{k,s} \leq h - (k-1)(ta_k - 1).$$

Therefore,

$$\sum_{i=1}^{k} x_{i,s} = \sum_{i=1}^{k-1} x_{i,s} + x_{k,s}$$

$$\leq (k-1)(sa_k - 1) + h - (k-1)(ta_k - 1)$$

$$= h - (k-1)(t-s)a_k$$

$$\leq h$$

and $n \in hA$. It follows from (6) that, for $s \in [1,t]$, the $k$-tuples

$$(x_{1,s}, x_{2,s}, \ldots, x_{k-1,s}, x_{k,s})$$

are distinct, and so the representations (7) are distinct. Therefore, $r_{A,h}(n) \geq t$ and

$$[c'_t, ha_k - d'_t] \subseteq (hA)^{(t)}.$$

This proves Lemma 2. \hfill \Box

**References**

[1] Granville, A., Shakan, G. (2020). The Frobenius postage stamp problem and beyond. arXiv:2003.04075

[2] Granville, A., Walker, A. (2020). A tight structure theorem for sumsets. arXiv:2006.01041

[3] Han, S.-P., Kirfel, C., Nathanson, M. B. (1998). Linear forms in finite sets of integers. Ramanujan J. 2(1-2): 271–281.

[4] Hardy, G. H., Wright, E. M. (2008). *An Introduction to the Theory of Numbers*, 6th ed. Oxford: Oxford Univ. Press.

[5] Khovanskii, A. G. (1992). The Newton polytope, the Hilbert polynomial and sums of finite sets. Funktsional. Anal. i Prilozhen. 26(4): 57–63, 96.

[6] Khovanskii, A. G. (1995). Sums of finite sets, orbits of commutative semigroups and Hilbert functions. Funktsional. Anal. i Prilozhen. 29(2): 36–50, 95.

[7] Nathanson, M. B. (1972). Sums of finite sets of integers. Amer. Math. Monthly. 79(9): 1010–1012.

[8] Nathanson, M. B. (1996). *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. Graduate Texts in Mathematics, vol. 165. New York: Springer-Verlag.
[9] Nathanson, M. B. (2000). Growth of sumsets in abelian semigroups. *Semigroup Forum*. 61(1): 149–153.

[10] Wu, J.-D., Chen, F.-J., Chen, Y.-C. (2011). On the structure of the sumsets. *Discrete Math.* 311(6): 408–412.

Lehman College (CUNY), Bronx, NY 10468

E-mail address: melvyn.nathanson@lehman.cuny.edu