PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 149, Number 10, October 2021, Pages 4073–4082
https://doi.org/10.1090/proc/15608
Article electronically published on July 16, 2021

A TIGHT STRUCTURE THEOREM FOR SUMSETS

ANDREW GRANVILLE AND ALED WALKER

(Communicated by Patricia L. Hersh)

Abstract. Let $A = \{0 = a_0 < a_1 < \cdots < a_{\ell+1} = b\}$ be a finite set of non-negative integers. We prove that the sumset NA has a certain easily-described structure, provided that $N \geqslant b - \ell$, as recently conjectured (see A. Granville and G. Shakan [Acta Math. Hungar. 161 (2020), pp. 700–718]). We also classify those sets A for which this bound cannot be improved.

1. Introduction

What are the possible postage costs that can be made up from an unlimited supply of 3 cent and 5 cent stamps? One cannot obtain $1c$, $2c$, $4c$, or $7c$ and it is a fun challenge to show that one can obtain n cents for every other positive integer n. In *the Frobenius postage stamp problem*, one asks the same question given an unlimited supply of a cent and b cent stamps, with $\gcd(a, b) = 1$.

The situation becomes more complicated if one may use at most N stamps. One can show that one can cover every integer amount up to $5N$ cents using at most N 3 and 5 cent stamps, other than $1, 2, 4$ and 7, as well as $5N - 3$ and $5N - 1$.

In the language of additive combinatorics, for a given finite set of integers A we wish to understand the structure of the sumset NA, where

$$NA := \{a_1 + \cdots + a_N : a_1, \ldots, a_N \in A\},$$

where the summands are not necessarily distinct. For simplicity we may assume without loss of generality that the smallest element of A is 0, and that the greatest common divisor of its elements is 1.[1] Since $0 \in A$ we have $A \subset 2A \subset \cdots \subset NA$, and so

$$\mathcal{P}(A) := \bigcup_{N=1}^{\infty} NA$$

is the set of all integers that are expressible as a finite sum of (not necessarily distinct) elements of A. Similarly, we define the exceptional set

$$\mathcal{E}(A) = \{n \geqslant 1 : n \notin \mathcal{P}(A)\}.$$

Received by the editors June 1, 2020, and, in revised form, October 12, 2020.
2020 *Mathematics Subject Classification.* Primary 11D07; Secondary 05A15, 05A17.
The first author was funded by the European Research Council grant agreement no. 670239, and by the Natural Sciences and Engineering Research Council of Canada (NSERC) under the Canada Research Chairs program. The second author was supported by a postdoctoral research fellowship at the Centre de Recherches Mathématiques, and is also a Junior Research Fellow at Trinity College Cambridge.

[1]Since if $A = g \cdot B + \tau$ then $NA = g \cdot NB + N\tau$, where $g \cdot B = \{gb : b \in B\}$.

In the setting of the original postage stamp problem, in this notation we have

$$\mathcal{E}(\{0,3,5\}) = \{1,2,4,7\}.$$

Let b denote the largest element of A so that $\{0,b\} \subset A \subset \{0,1,\ldots,b\}$ which implies that $NA \subset \{0,1,\ldots,bN\} \setminus \mathcal{E}(A)$. However, in the $A = \{0,3,5\}$ example there are exceptions other than $\mathcal{E}(A)$. Indeed, if $n \in NA$ then $bN - n \in N(b-A)$, where $b - A := \{b - a : a \in A\}$. Therefore $NA \cap (bN - \mathcal{E}(b-A)) = \emptyset$, and thus

$$NA \subset \{0,1,\ldots,bN\} \setminus (\mathcal{E}(A) \cup (bN - \mathcal{E}(b-A))).$$

Does equality hold in this expression? In our example $b - A = \{0,2,5\}$ and $\mathcal{E}(\{0,3,5\}) = \{1,3\}$ which explains the result above. It was shown in [1] that equality indeed holds for all $N \geq 1$ for all three element sets $A = \{0 < a < b\}$ where $(a,b) = 1$. If $A = \{0,1,b-1,b\}$ then equality does not hold for any $N \leq b-3$ since $\mathcal{E}(A) = \mathcal{E}(b-A) = \emptyset$ and $b - 2 \notin NA$ for such N.

Our main result gives an improved bound for the smallest N_0, such that we get equality above; that is, (1.1) for all $N \geq N_0$. This improved bound is "best possible" in several situations.

Theorem 1 (Main theorem)**.** *Let $A = \{0 = a_0 < a_1 < \cdots < a_{\ell+1} = b\}$ be a finite set of integers with* $\gcd(a_1,\ldots,a_{\ell+1}) = 1$ *and $\ell \geqslant 1$. If $N \geqslant b - \ell$ then*

$$NA = \{0,1,\ldots,bN\} \setminus (\mathcal{E}(A) \cup (bN - \mathcal{E}(b-A))). \tag{1.1}$$

A statement like Theorem 1 was first proved by Nathanson [3], but with the weaker bound $N \geqslant b^2(\ell+1)$. The bound was improved to $N \geqslant \sum_{a\in A,\, a\neq 0}(a-1)$ in [5], and then to $N \geqslant 2\lfloor \frac{b}{2} \rfloor$ in [1], where our bound $N \geq b - \ell$ was conjectured.

The bound "$N \geqslant b - \ell$" in Theorem 1 is tight, in that there are examples of sets A for which (1.1) does not hold when $N = b - \ell - 1$. In particular there are the following families:

- $A = \{0,1,\ldots,b\} \setminus \{a\}$ for some a in the range $2 \leqslant a \leqslant b-2$. Here $b - \ell - 1 = 1$ and $\mathcal{E}(A) = \mathcal{E}(b-A) = \emptyset$, but $a \notin A$, in contradiction to (1.1).
- $A = \{0,1,a+1,\ldots,b-1,b\}$, for some a in the range $2 \leqslant a \leqslant b-2$. Here $b - \ell - 1 = a - 1$ and $\mathcal{E}(A) = \mathcal{E}(b-A) = \emptyset$, but $a \notin (a-1)A$, contradicting (1.1).

The previous bounds of [5] and [1] were also tight for certain special values of ℓ and b, but our Theorem 1 is the first such bound for which tight examples exist for all $b \geqslant 4$ and for all ℓ in the range $2 \leqslant \ell \leqslant b-2$.

Moreover, it turns out that the families listed above are the only obstructions to improving Theorem 1:

Theorem 2. *Let $\ell \geqslant 1$ and $A = \{0 = a_0 < a_1 < \cdots < a_{\ell+1} = b\}$ be a finite set of integers with* $\gcd(a_1,\ldots,a_{\ell+1}) = 1$. *If $N \geqslant \max(1, b-\ell-1)$ then*

$$NA = \{0,1,\ldots,bN\} \setminus (\mathcal{E}(A) \cup (bN - \mathcal{E}(b-A))),$$

unless either A or $b - A$ is a set in one of the two families listed above.

Our goal in proving Theorems 1 and 2 was to establish tight bounds in the venerable Frobenius postage stamp problem. These bounds can now be applied to what we hope is a cornucopia of questions in additive combinatorics (for example, Corollary 1.8, Lemma 5.1, and Lemma 5.2 in [2]) where explicit tight bounds are needed.

Our methods also show that, if $b \geqslant 9$ and $\ell \geqslant 5$, then (1.1) holds for all $N \geqslant \max(1, b-\ell-2)$ unless A or $b-A$ belong to one of the two families listed above or one of the following new families:

- $A = \{0,1,b\} \cup (\{a+1,\dots,b-1\} \setminus \{d\})$ for some a in the range $2 \leqslant a \leqslant b-2$ and some d in the range $a+2 \leqslant d \leqslant b-1$, where $a \notin (a-1)A$;
- $A = \{0,1,\dots,b\} \setminus \{a,c\}$ for some $2 \leqslant a, c \leqslant b-2$, where $a \notin A$;
- $A = \{0,1,2,6,\dots,b\}$, where $5 \notin 2A$;
- $A = \{0,1,3,6,\dots,b\}$, where $5 \notin 2A$.

Indeed, our proofs are sufficiently flexible that one can go on and prove that (1.1) holds for all $N \geqslant \max(1, b-\ell-\Delta)$, for ever larger values of Δ, except in some explicit finite set of families of sets A, though the number of cases seems to grow prohibitively with Δ.

The final parts of the proofs of Theorems 1 and 2 come in Section 4. These will rely on a number of auxiliary lemmas and use some terminology from [1], all of which we will introduce in the preceding sections. There are a few families of examples, like $A = \{0, h, b-h, b\}$ with $(h,b)=1$, for which our general arguments for Theorems 1 and 2 fail, and for these examples we verify the theorems explicitly in Appendix A.

2. Placing elements in NA

Throughout we fix a set $A \subset \mathbb{Z}$ with minimum element 0 and maximum element b, where $A \setminus \{0,b\}$ has ℓ elements, and $\gcd(a : a \in A) = 1$. Let B be the reduction of $A \pmod b$ so that $|B| = \ell+1$, and its elements can be represented by $A \setminus \{b\}$.

For a in the range $1 \leqslant a \leqslant b-1$ we write

$$n_{a,A} := \min\{n \geqslant 1 : n \in \mathcal{P}(A),\ n \equiv a \pmod b\}$$

and

$$N_{a,A} := \min\{N \geqslant 1 : n_{a,A} \in NA\}, \text{ with } N_A^* := \max_{1 \leqslant a \leqslant b-1} N_{a,A}.$$

We always have $N_{a,A} \leq b-1$ for if not we write $n_{a,A} = a_1 + \cdots + a_N$ with each $a_i \in A$ and $N = N_{a,A}$. Then at least two of $b+1$ subsums

$$0, a_1, a_1+a_2, \dots, a_1+\cdots+a_b$$

must be congruent mod b, say $a_1+\cdots+a_i \equiv a_1+\cdots+a_j \pmod b$ with $i<j$, and then

$$a_1+\cdots+a_i+a_{j+1}\cdots+a_N \equiv a_1+\cdots+a_N = n_{a,A} \equiv a \pmod b,$$

contradicting the minimality of $n_{a,A}$.

It was observed in [1] that

$$\mathcal{E}(A) = \bigcup_{a=1}^{b-1} \{n \geqslant 1 : n < n_{a,A},\ n \equiv a \pmod b\} \tag{2.1}$$

so that $\{0,1,\dots,bN\} \setminus (\mathcal{E}(A) \cup (bN - \mathcal{E}(b-A)))$ equals

$$\bigcup_{a=1}^{b-1} \{n : n_{a,A} \leqslant n \leqslant bN - n_{b-a,b-A},\ n \equiv a \pmod b\}.$$

Therefore the equality (1.1) holds if and only if the arithmetic progressions

$$\{n : n_{a,A} \leqslant n \leqslant bN - n_{b-a,b-A},\ n \equiv a \pmod b\}, \qquad 1 \leqslant a \leqslant b-1 \tag{2.2}$$

are contained in NA. Our first lemma shows that, under certain conditions on the sumset of B, elements of the arithmetic progressions in (2.2) do belong to NA.

Lemma 2.1. *Let a be in the range $1 \leqslant a \leqslant b-1$, let $k \geqslant 1$ and suppose that $|kB| \geqslant b - N_{a,A}$. Then $n_{a,A} + (k-1)b \in NA$ whenever $N \geqslant 2k + b - |kB| - 1$.*

Proof. Suppose that

$$n_{a,A} = a_1 + \cdots + a_L \text{ where } L := N_{a,A},$$

for some $a_i \in A$ not necessarily distinct. Consider then the set $\mathcal{M}$ of subsums

$$a_1 + \cdots + a_M, a_1 + \cdots + a_{M+1}, \ldots, a_1 + \cdots + a_L$$

where $M = N_{a,A} - (b - |kB|)$, where if $M = 0$ we consider the first (empty) sum to be equal to 0.

We make several observations. First, since $b \geqslant |kB| \geqslant b - N_{a,A}$ we have $N_{a,A} \geqslant M \geqslant 0$, so the construction of $\mathcal{M}$ is valid. Second, we observe that the members of $\mathcal{M}$ are distinct mod b by the definition of $n_{a,A}$. To justify this second part, we note that if two members of $\mathcal{M}$ were the same modulo b then there would be a subsum of $a_1 + \cdots + a_L$ congruent to 0 mod b, say $\sum_{s \in S} a_s$. Furthermore we know that $a_s \geqslant 1$ for all s, by the minimality of $N_{a,A}$. But then $n := n_{a,A} - \sum_{s\in S} a_s$ satisfies $n < n_{a,A}$, $n \equiv a \bmod b$, and $n \in \mathcal{P}(A)$, which contradicts the minimality of $n_{a,A}$.

Now $|\mathcal{M}| + |kB| \geqslant b+1$ and the elements of $\mathcal{M}$ are distinct mod b. Therefore, by the pigeonhole principle, there exists an integer $m \in [M, L]$ for which

$$a_1 + \cdots + a_m \in kB \mod b;$$

that is, there exists an integer i and $b_1, \ldots, b_k \in A \setminus \{b\}$ for which

$$a_1 + \cdots + a_m + ib = b_1 + \cdots + b_k.$$

We may extract some bounds for i. Indeed, note that $ib \leqslant a_1 + \cdots + a_m + ib = b_1 + \cdots + b_k < kb$ and so $i \leqslant k-1$. Also

$$n_{a,A} + ib = (a_1 + \cdots + a_m + ib) + (a_{m+1} + \cdots + a_L) = (b_1 + \cdots + b_k) + (a_{m+1} + \cdots + a_L) \in \mathcal{P}(A)$$

and so $i \geqslant 0$ by the minimality of $n_{a,A}$.

Therefore

$$\begin{aligned} n_{a,A} + (k-1)b &= (b_1 + \cdots + b_k) + (a_{m+1} + \cdots + a_L) + (k-1-i)b \\ &\in k(A \setminus \{b\}) + (N_{a,A} - m)A + (k-1-i)b \\ &\subset (k + (b - |kB|) + k - 1)A \subset NA, \end{aligned}$$

since $i \geqslant 0$ and $N_{a,A} - m \leqslant N_{a,A} - M = b - |kB|$. □

We will combine this lemma with some lower bounds on the growth of the sumset $|kB|$. Our main tool is Kneser's theorem [4, Theorem 5.5], which states that if U, V are subsets of a finite abelian group G then

$$|U + V| \geqslant |U + H| + |V + H| - |H|$$

where $H = H(U+V)$ is the *stabilizer* of $U+V$, defined in general by

$$H(W) := \{g \in G : g + W = W\}.$$

One notes in particular that $V + H$ is a union of cosets of H, so its size is a multiple of $|H|$. Therefore if $0 \in V$ but $V \not\subset H$ then $|V + H| - |H| \geqslant |H|$.

Lemma 2.2. *Assume that $\ell \geqslant 2$. For all $k \geqslant 2$, $|kB| \geqslant \min(b, |(k-1)B| + 2)$.*

Proof. By Kneser's theorem we have

$$\begin{aligned}|kB| &\geqslant |(k-1)B + H(kB)| + |B + H(kB)| - |H(kB)|\\ &\geqslant |(k-1)B| + |B + H(kB)| - |H(kB)|.\end{aligned}$$

If $H(kB) = \mathbb{Z}/b\mathbb{Z}$ then $|kB| = b$ and we are done, so we may assume that $H(kB)$ is a proper subgroup of $\mathbb{Z}/b\mathbb{Z}$. Since B generates all of $\mathbb{Z}/b\mathbb{Z}$ we see that $B \not\subset H(kB)$ and so $|B + H(kB)| - |H(kB)| \geqslant |H(kB)|$. Therefore if $H(kB) \neq \{0\}$ then $|kB| \geqslant |(k-1)B| + 2$. If on the other hand we have $H(kB) = \{0\}$ then

$$|kB| \geqslant |(k-1)B| + |B| - 1 = |(k-1)B| + \ell \geqslant |(k-1)B| + 2$$

since $\ell \geqslant 2$. □

We make a deduction, phrased in a suitably general way so as to apply in the setting of both Theorems 1 and 2.

Corollary 2.1. *Assume that $\ell \geqslant 2$, and let $N = b - \ell - \Delta$ for some $\Delta \geqslant 0$. Let K be the smallest integer such that $K \geqslant 2$ and $|KB| \geqslant \min(b, 2K + \ell + \Delta - 1)$, and assume that $N \geqslant N_A^* + K - 2$. Then $n \in NA$ for all $n \leqslant bN/2$ with $n \notin \mathcal{E}(A)$.*

Proof. We will show that $n_{a,A} + kb \in NA$ for all $k < N/2$ and all a in the range $1 \leqslant a \leqslant b-1$, which implies the result, by (2.1).

Note that $N \geqslant N_A^* \geqslant N_{a,A}$. Therefore if $0 \leqslant k \leqslant N - N_{a,A}$ we have $n_{a,A} + kb \in N_{a,A}A + (N - N_{a,A})A = NA$, so without loss of generality we may assume that $k \geqslant N - N_{a,A} + 1$, so that $k + 1 \geqslant N - N_{a,A} + 2 \geqslant N - N_A^* + 2 \geqslant K$.

From Lemma 2.2 and induction, this means that

$$|(k+1)B| \geqslant \min(b, 2(k+1) + \ell + \Delta - 1).$$

Our goal is to apply Lemma 2.1 with k replaced by $k+1$ so we need to verify its hypotheses:

- If $|(k+1)B| = b$ then $|(k+1)B| \geqslant b - N_{a,A} \geqslant N - N_{a,A}$ trivially, and

$$2(k+1) + b - |(k+1)B| - 1 = 2k + 1 \leqslant N$$

  since $k < \frac{N}{2}$;
- Otherwise $|(k+1)B| \geqslant 2(k+1) + \ell + \Delta - 1$, and so we have both

$$2(k+1) + b - |(k+1)B| - 1 \leqslant b - \ell - \Delta = N$$

  and

$$|(k+1)B| \geqslant 2(N - N_{a,A} + 2) + \ell - 1 + \Delta \geqslant N + \ell + \Delta - N_{a,A} + 3 = b - N_{a,A} + 3$$

  as $N \geqslant N_{a,A}$.

Therefore Lemma 2.1 implies that $n_{a,A} + (k+1-1)b = n_{a,A} + kb \in NA$, as desired. □

3. Bounds on $|2B|$ and N_A^*

In order to use Corollary 2.1, two further bounds will be useful: a lower bound on $|2B|$ and an upper bound on N_A^*. We will achieve both of these objectives in this section (bar a few special cases which we will deal with separately).

Lemma 3.1. *Suppose that B is a subset of $\mathbb{Z}/b\mathbb{Z}$ which contains 0, generates all of $\mathbb{Z}/b\mathbb{Z}$, and has $\ell \geqslant 2$ non-zero elements. Then $|2B| \geqslant \min(b, \ell + 3)$. Moreover*

$|2B| \geqslant \min(b, \ell+4)$, *except in the following families of examples (where* $A = B \cup \{b\}$ *for later convenience):*

- $A = \{0 < h < 2h < b\}$ *with* $(h, b) = 1$*;*
- $A = \{0 < 2h - b < h < b\}$ *with* $(h, b) = 1$*;*
- $A = \{0 < h < b - h < b\}$ *with* $(h, b) = 1$*;*
- $A = \{0 < h, \frac{b}{2} < b\}$ *with* $(h, \frac{b}{2}) = 1$*;*
- $A = \{0 < h < h + \frac{b}{2} < b\}$ *with* $(h, \frac{b}{2}) = 1$*;*
- $A = \{0 < h < b/2 < h + \frac{b}{2} < b\}$ *with* $(h, \frac{b}{2}) = 1$*.*

Proof. We aim to prove that $|2B| \geqslant \min(b, \ell + 3 + \Delta)$ for $\Delta = 0$ or 1. By Kneser's theorem we have

$$|2B| \geqslant 2|B + H| - |H|,$$

where $H = H(2B)$. If $|H| = b$ then $|2B| = b$ and we are done.

If $H = \{0\}$ then we derive $|2B| \geqslant 2\ell+1 \geqslant \ell+3+\Delta$, provided $\ell \geqslant 2+\Delta$. Therefore we are done unless $\Delta = 1$ and $\ell = 2$ with $|2B| \leqslant 5$. In this case $B = \{0, h, k\}$ with $(h, k, b) = 1$ and at least two of $0, h, k, 2h, h + k, 2k$ must be congruent mod b. One obtains the first five families of examples in the result from a case-by-case analysis (letting $k = 2h, 2h - b, b - h, \frac{b}{2}$ and $h + \frac{b}{2}$, respectively).

Now we may assume that $2 \leqslant |H| \leqslant b - 1$. If B is not a union of H-cosets then $|B + H| \geqslant |B| + 1 = \ell + 2$. Also, since B generates $\mathbb{Z}/b\mathbb{Z}$ and $|H| \neq b$ we have $B \not\subset H$, and so $|B + H| \geqslant 2|H|$. Thus

$$|2B| \geqslant |B + H| + (|B + H| - |H|) \geqslant \ell + 2 + |H| \geqslant \ell + 4.$$

Finally assume that B is the union of r H-cosets with $r \geqslant 2$, so that

$$|2B| \geqslant (2r - 1)|H| = (2 - \tfrac{1}{r})|B| = (2 - \tfrac{1}{r})(\ell + 1).$$

This is at least $\ell + 3 + \Delta$ unless $\ell < \frac{r}{r-1}(1 + \frac{1}{r} + \Delta)$, where $r, \ell \geq 2$ and r is a proper divisor of $\ell + 1$, and so $\ell \neq 2$ or 4. For $\Delta = 0$ this implies $\ell < 3$, which is impossible. If $\Delta = 1$ the inequality implies $\ell < 2 + \frac{3}{r-1} \leq 5$, so that the only possibility is $\ell = 3$ and $r = 2$, so that $|H| = 2$. Therefore b is even, $H = \{0, \frac{b}{2}\}$ and we obtain the sixth family of examples. □

We now present some bounds on N_A^*.

Lemma 3.2. *Suppose that* $2 \leqslant \ell \leqslant b - 2$*. Then we have* $N_A^* \leqslant b - \ell - 1$*, except when:*

- $A = \{0, 1, \ldots, b\} \setminus \{a\}$ *for some* a *in the range* $1 \leqslant a \leqslant b - 1$*, in which case* $N_{a,A} = 2$ *and* $N_A^* = 2 = b - \ell$*; or when*
- $A = \{0, 1, a + 1, \ldots, b - 1, b\}$ *for some* a *in the range* $2 \leqslant a \leqslant b - 2$*, in which case* $n_{a,A} = a \times 1$*,* $N_{a,A} = a = b - \ell$ *and* $N_A^* = b - \ell$*.*

Proof. Choose some a in the range $1 \leqslant a \leqslant b - 1$, and let $n_{a,A} = a_1 + \cdots + a_L$ where $L := N_{a,A}$, with each $a_i \in A$. All subsums are non-zero mod b, as both $n_{a,A}$ and L are minimal (see the proof of Lemma 2.1 for a longer explanation of this fact). Furthermore a subsum with more than one element cannot be congruent mod b to an element of B else we can replace that subsum by the single element, contradicting the minimality of L. Hence the residue classes mod b of

$$a_1 + a_2, \ldots, a_1 + \cdots + a_L \tag{3.1}$$

are all distinct and do not belong to $B \mod b$. This yields $L-1$ distinct residue classes of $(\mathbb{Z}/b\mathbb{Z}) \setminus B$, and so $N_{a,A} \leqslant b-\ell$. Therefore either $N_A^* \leqslant b-\ell-1$, in which case we are done, or we are in a case where $N_{a,A} = b-\ell$.

If $N_{a,A} = b-\ell$ then the displayed values (3.1) yield all the residue classes of $(\mathbb{Z}/b\mathbb{Z}) \setminus B$. This is also true if we list the a_i in a different order, so we can swap a_2 and a_3 and find that $a_1 + a_2 \equiv a_1 + a_3 \pmod b$ (as this element is the only difference between the two lists). Thus $a_2 = a_3$. But this is true for any ordering of the a_i's, so $n_{a,A}$ is given by $L = N_{a,A}$ copies of some $h \in A$. Therefore

$$A = \{0, 1, \ldots, b\} \setminus \{(2h)_b, (3h)_b, \ldots, (Lh)_b\}, \tag{3.2}$$

where $(t)_b$ denotes the least positive residue of $t \pmod b$, and $a \equiv Lh \pmod b$.

We split into two cases according to the value of the greatest common divisor (h, b). If $(h, b) > 1$ then $1 \in A$ (since $1 \not\equiv 0 \mod (h, b)$). Therefore $n_{a,A} = a = Lh$. Moreover $a-1 \in A$ (since $a-1 \equiv -1 \not\equiv 0 \mod (h, b)$) and $a = (a-1)+1$ implies that $N_{a,A} \leqslant 2$. But $N_{a,A} = b-\ell \geq 2$, and so $\ell = b-2$. Hence $A = \{0, 1, \ldots, b\} \setminus \{a\}$.

We may now assume that $(h, b) = 1$. Then $n_{a,A} = Lh$, so that

$$a \equiv Lh \equiv ((L+j)h)_b + ((b-j)h)_b$$

for $1 \leq j \leq \ell-1$. Since $L = b-\ell$ we have both $L+1 \leqslant L+j \leqslant b-1$ and $L+1 \leqslant b-j \leqslant b-1$. Therefore by (3.2) we have $((L+j)h)_b \in A$ and $((b-j)h)_b \in A$ for each j. Thus

$$((L+j)h)_b + ((b-j)h)_b \in \mathcal{P}(A) \text{ and } n_{a,A} \leq ((L+j)h)_b + ((b-j)h)_b < b+b = 2b.$$

Therefore

$$((L+j)h)_b + ((b-j)h)_b = Lh \text{ or } Lh+b.$$

If $((L+j)h)_b + ((b-j)h)_b = Lh = n_{a,A}$ then $N_{a,A} \leqslant 2$. Since $N_{a,A} = b-\ell \geq 2$ we conclude that $N_{a,A} = 2$ and $\ell = b-2$, and so $A = \{0, 1, \ldots, b\} \setminus \{a\}$ again.

Otherwise $Lh < b$ and $((L+j)h)_b + (-jh)_b = Lh+b$ for all j in the range $1 \leqslant j \leqslant \ell-1$. This means that for all such j we have

$$b > ((L+j)h)_b = Lh + (b - (-jh)_b) > Lh. \tag{3.3}$$

This implies that $((L+j)h)_b = (L+j)h$ for all j in the range $1 \leqslant j \leqslant \ell-1$. Indeed, suppose for contradiction that j in that range is minimal such that $((L+j)h)_b < (L+j)h$. Then $((L+j-1)h)_b = (L+j-1)h < b$, by the assumption of minimality if $j \geqslant 2$, or by (3.3) if $j = 1$. So $((L+j)h)_b < h \leqslant Lh$. This is a contradiction to (3.3).

Choosing $j = \ell-1$ in the equation $((L+j)h)_b = (L+j)h$ we deduce that $(b-1)h < b$ and so $h = 1$. Therefore $A = \{0, 1, a+1, \ldots, b-1, b\}$ with $a = L = b-\ell$ and so $2 \leqslant a \leqslant b-2$. Thus we have established that $N_A^* \leqslant b-\ell-1$ except when A has one of the two special forms listed in the statement of the lemma. □

4. Proofs of Theorems 1 and 2

The result [1, Theorem 4] showed that (1.1) holds for all $N \geqslant 1$ when $\ell = 1$ (and so it holds for all $N \geqslant b-\ell$). Furthermore, (1.1) holds for trivial reasons if $\ell = b-1$, i.e. if $A = \{0, 1, \ldots, b\}$. So without loss of generality may assume $2 \leqslant \ell \leqslant b-2$ in these two proofs.

Proof of Theorem 1. We have $N_A^* \leqslant b-\ell$ by Lemma 3.2, and $|2B| \geqslant \min(b, \ell+3)$ by Lemma 3.1. Taking $\Delta = 0$ and $K = 2$ in Corollary 2.1, we deduce that if $N = b-\ell$ then $n \in NA$ for all $n \leqslant bN/2$ with $n \notin \mathcal{E}(A)$. Applying the same argument with the set A replaced by the set $b-A$ we conclude that if $N=b-\ell$ then $m \in N(b-A)$ for all $m \leqslant bN/2$ with $m \notin \mathcal{E}(b-A)$.

So, if $1 \leqslant n < bN$ and $n \notin (\mathcal{E}(A) \cup (bN - \mathcal{E}(b-A)))$ then either $1 \leqslant n \leqslant bN/2$, in which case $n \in NA$ by the applying the first argument to n, or $bN/2 \leqslant n < bN$, in which case $n \in NA$ by applying the second argument to $m = bN - n$. Since $bN \in NA$ for trivial reasons, we have established (1.1) for $N = b - \ell$.

The result [1, Lemma 2] established that if (1.1) holds for some $N_0 \geqslant N_A^*$ then it holds for all $N \geqslant N_0$. So (1.1) holds for all $N \geqslant b-\ell$, and Theorem 1 is proved. □

Proof of Theorem 2. Following the proof of Theorem 1, we have $N_A^* \leqslant b-\ell-1$ except in the two exceptional cases of Lemma 3.2, and $|2B| \geqslant \min(b, \ell+4)$ except in the six exceptional cases of Lemma 3.1. Outside these exceptional cases, the proof then follows analogously to the proof of Theorem 1, taking $\Delta = 1$ and $K = 2$ in Corollary 2.1.

It remains to consider the exceptional cases. All of the exceptional cases in Lemma 3.2 are excluded in the statement of Theorem 2, except for when A or $b-A$ equals $\{0, 2, 3, \ldots, b\}$. In this instance, $\mathcal{E}(A) = \{1\}$ or $\mathcal{E}(b-A) = \{1\}$, respectively, and (1.1) manifestly holds for all $N \geqslant 1 = b - \ell - 1$.

Regarding the exceptional cases from Lemma 3.1, the example $A = \{0, 1, b-1, b\}$ is excluded from Theorem 2. We will prove that equation (1.1) holds for $N \geqslant b-\ell-1$ for all of the other exceptional cases from Lemma 3.1 (in the five cases of Section A.1, and in Case 6 of Appendix A). This completes the proof of Theorem 2. □

Appendix A. A catalogue of exceptional cases

A.1. **Resolving the five exceptional families of A for which $|A| = 4$ and $|2B| \leqslant 5$.** A key tool will be [1, Corollary 2], which showed that if $n \equiv a \pmod b$ and $n_{a,A} \leqslant n \leqslant bN - n_{b-a,b-A}$ then $n \in NA$ for all $N \geqslant 1$ if and only if $N_{a,A} = \frac{1}{b}(n_{a,A} + n_{b-a,b-A})$ for all a.

Case 1. If $A = \{0 < a < 2a < b\}$ with $(a,b) = 1$, then (1.1) holds for all $N \geqslant 1$.

Proof. Let $A' := b - A = \{0 < 2a' - b < a' < b\}$ with $a' = b - a$. For $1 \leqslant k \leqslant (b-1)/2$ we have $n_{2ka,A} = 2k \times a = k \times 2a$ while $n_{b-2ka,b-A} = n_{2ka',A'} = k \times (2a' - b)$; in the range $0 \leqslant k \leqslant (b-2)/2$, we have $n_{(2k+1)a,A} = a + k \times 2a$ while $n_{b-(2k+1)a,b-A} = n_{(2k+1)a',A'} = a' + k \times (2a' - b)$. So $N_{2ka,A} = k$ and $N_{(2k+1)a,A} = k+1$, and so for all $1 \leqslant r \leqslant b-1$ we have $N_{r,A} = \frac{1}{b}(n_{r,A} + n_{b-r,b-A})$. Thus [1, Corollary 2] shows (1.1) holds for all $N \geqslant 1$. □

Case 2. If $A = \{0 < 2a - b < a < b\}$ with $(a,b) = 1$, then (1.1) holds for all $N \geqslant 1$.

Proof. This follows from the previous case by symmetry. □

Case 3. If $A = \{0 < a, \frac{b}{2} < b\}$ with $(a, \frac{b}{2}) = 1$, then (1.1) holds for all $N \geqslant 1$.

Proof. Here $b - A = \{0 < b-a, \frac{b}{2} < b\}$ is of the same form. By performing a simple case analysis, we deduce that for $1 \leqslant k < \frac{b}{2}$ we have $n_{ka,A} = k \times a$ and $n_{b-ka,b-A} = n_{k(b-a),b-A} = k \times (b-a)$, while for $0 \leqslant k < \frac{b}{2}$ we have $n_{ka+\frac{b}{2},A} = k \times a + \frac{b}{2}$ and $n_{\frac{b}{2}-ka,b-A} = n_{k(b-a)+\frac{b}{2},A} = k \times (b-a) + \frac{b}{2}$. Then (1.1) holds for all $N \geqslant 1$ by [1, Corollary 2], as described above. □

Case 4. If $A = \{0 < h < b-h < b\}$ with $(h,b) = 1$ then (1.1) holds for all $N \geqslant b-1-h$. In particular if $h \neq 1$ then (1.1) holds for all $N \geqslant b-3 = b-\ell-1$.

Proof. If $a \not\equiv 0 \pmod b$ then the summands in $n_{a,A}$ are either all h or all $b-h$ since if we had both we could remove one of each, contradicting minimality. Therefore

$$N_{kh,A} = \begin{cases} k \\ b-k \end{cases} \quad \text{and } n_{kh,A} = \begin{cases} kh & \text{if } 1 \leqslant k < b-h \\ (b-k)(b-h) & \text{if } b-h \leqslant k \leqslant b-1. \end{cases} \tag{A.1}$$

If $k \leqslant h$ then $n_{kh,A} = kh$ and $n_{b-kh,b-A} = n_{k(b-h),A} = k \times (b-h)$. Then the structure (1.1), restricted to the arithmetic progression $n \equiv kh \pmod b$, follows from [1, Corollary 2].

If $h < k \leqslant \frac{b}{2}$ then $n_{kh,A} = kh$ and $n_{b-kh,b-A} = n_{(b-k)h,A} = (b-k)h$. Therefore we wish to show that if n is in the range $kh \leqslant n \leqslant Nb - (b-k)h = kh + (N-h)b$ and $n \equiv kh \pmod b$ then $n \in NA$ (as long as $N \geqslant b-1-h$).

If we write $n = k \times h + j \times b$ for $j \in [0, N-k]$ then this covers such n with $kh \leqslant n \leqslant kh+(N-k)b$; and if we write $n = (b-k)\times(b-h)+i\times b$ for $i \in [0, N+k-b]$ then we cover such n with $kh+(b-k-h)b \leqslant n \leqslant kh+(N-h)b$. Together these two ranges cover the entire range of n, provided $b-k-h \leqslant N-k+1$. This inequality holds, since $N \geqslant b-1-h$.

To deal with the remaining arithmetic progressions $kh \pmod b$ for $k > \frac{b}{2}$ we note that $NA = bN - NA$, and so the result follows from the above using the arithmetic progression $-kh \pmod b$. □

Case 5. If $A = \{0 < a < a+\frac{b}{2} < b\}$ with $(a, \frac{b}{2}) = 1$ then (1.1) holds for all $N \geqslant \frac{b}{2}$.

Proof. Note first that $b - A = \{0 < \frac{b}{2} - a < b-a < b\}$, which is of the same form as A. The proof splits into four subcases, which we will deal with in two sets of two.

If $1 \leqslant k \leqslant \frac{b}{2}$ with k even then $n_{ka,A} = k \times a$ and $n_{b-ka,b-A} = k \times (\frac{b}{2} - a)$. Therefore, from (2.2), we wish to represent all $n \equiv ka \pmod b$ with $ka \leqslant n \leqslant ka + b(N - \frac{k}{2})$ by an element in NA.

If $1 \leqslant k \leqslant \frac{b}{2}$ with k odd then $n_{ka,A} = k \times a$ and $n_{b-ka,b-A} = (k-1) \times (\frac{b}{2} - a) + (b-a)$, so we wish to represent $n \equiv ka \pmod b$ with $ka \leqslant n \leqslant ka + b(N - \frac{k+1}{2})$ by an element in NA.

We let

$$n = (k-2i) \times a + 2i \times (a + \tfrac{b}{2}) + j \times b = ka + (i+j)b$$

for $0 \leqslant 2i \leqslant k$ and $0 \leqslant j \leqslant N-k$. We have $n \in (k+j)A \subset NA$, and we obtain the full range of n in each case, provided $N \geqslant k$. This is satisfied if $N \geqslant \frac{b}{2}$.

If $1 \leqslant k < \frac{b}{2}$ with k odd then $n_{ka+\frac{b}{2},A} = (k-1) \times a + (a + \frac{b}{2})$ and $n_{\frac{b}{2}-ka,b-A} = k \times (\frac{b}{2} - a)$, so we wish to represent $n \equiv ka + \frac{b}{2} \pmod b$ with

$$ka + \tfrac{b}{2} \leqslant n \leqslant ka + \tfrac{b}{2} + b(N - \tfrac{k+1}{2})$$

by an element of NA.

If $1 \leqslant k < \frac{b}{2}$ with k even then $n_{ka+\frac{b}{2},A} = (k-1) \times a + (a + \frac{b}{2})$ and $n_{\frac{b}{2}-ka,b-A} = (k-1) \times (\frac{b}{2} - a) + (b-a)$, so we wish to represent $n \equiv ka + \frac{b}{2} \pmod b$ with $ka + \frac{b}{2} \leqslant n \leqslant ka + \frac{b}{2} + b(N - 1 - \frac{k}{2})$ by an element of NA.

We let

$$n = (k-2i-1) \times a + (2i+1) \times (a + \tfrac{b}{2}) + j \times b = ka + \tfrac{b}{2} + (i+j)b$$

for $0 \leqslant 2i+1 \leqslant k$ and $0 \leqslant j \leqslant N-k$. We have $n \in (k+j)A \subset NA$, and we obtain the full range provided $N \geqslant k$. This is satisfied if $N \geqslant \frac{b}{2}$. □

A.2. **Resolving the exceptional cases in which $H(2B) \neq \{0\}$.**

Case 6. If $A = \{0 < a < \frac{b}{2} < a + \frac{b}{2} < b\}$ with b even and $(a, \frac{b}{2}) = 1$ then (1.1) holds for $N \geqslant \frac{b}{2} - 1$.

Proof. If $A' := \{0 < a < a + b/2 < b\}$ then $\mathcal{P}(A) = \mathcal{P}(A') \cup \{n \geqslant 0 : n \equiv b/2 \pmod{b}\}$, and $\mathcal{P}(b-A) = \mathcal{P}(b-A') \cup \{n \geqslant 0 : n \equiv b/2 \pmod{b}\}$. From the proof of Case 5, we see that (1.1) holds provided $N \geqslant \frac{b}{2} - 1$ except possibly for the residue class $n \equiv b/2 \pmod{b}$.

However, since $n_{b/2,A} = n_{b/2,b-A} = b/2$, [1, Corollary 2] finishes the matter. □

Acknowledgment

The authors would like to thank George Shakan for helpful communications.

References

[1] A. Granville and G. Shakan, *The Frobenius postage stamp problem, and beyond*, Acta Math. Hungar. **161** (2020), no. 2, 700–718, DOI 10.1007/s10474-020-01073-y. MR4131939

[2] G. Iyer, O. Lazarev, S. J. Miller, and L. Zhang, *Generalized more sums than differences sets*, J. Number Theory **132** (2012), no. 5, 1054–1073, DOI 10.1016/j.jnt.2011.10.006. MR2890526

[3] M. B. Nathanson, *Sums of finite sets of integers*, Amer. Math. Monthly **79** (1972), 1010–1012, DOI 10.2307/2318072. MR304305

[4] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006, DOI 10.1017/CBO9780511755149. MR2289012

[5] J.-D. Wu, F.-J. Chen, and Y.-G. Chen, *On the structure of the sumsets*, Discrete Math. **311** (2011), no. 6, 408–412, DOI 10.1016/j.disc.2010.11.014. MR2799890

Département de mathématiques et de statistique, Université de Montréal, CP 6128 succ. Centre-Ville, Montréal, Québec H3C 3J7, Canada

Email address: andrew@dms.umontreal.ca

Trinity College, Cambridge CB2 1TQ, England

Email address: aw530@cam.ac.uk