SUMSETS WITH A MINIMUM NUMBER OF DISTINCT TERMS

Jagannath Bhanja
Department of Mathematics, Indian Institute of Information Technology, Design and Manufacturing, Kancheepuram, Chennai, India
jagannath@iiitdm.ac.in

Received: 5/7/24, Accepted: 2/1/25, Published: 2/21/25

Abstract

For a set A of k elements from an additive abelian group G and a positive integer $r \leq k$, we consider the set of elements of G that can be written as a sum of h elements of A with at least r distinct elements. We denote this set by $h^{(\geq r)}A$. The set $h^{(\geq r)}A$ generalizes the classical sumsets hA and $h\hat{}A$ for $r = 1$ and $r = h$, respectively. As the main result of this article, we give an upper bound for the minimum size of $h^{(\geq r)}A$ over $\mathbb{Z}_m$ for $m \geq 2$. Further, by an observation relating the sumsets hA, $h\hat{}A$, and $h^{(\geq r)}A$ we obtain the sharp lower bound on the size of $h^{(\geq r)}A$ and also characterize the set A for which the lower bound on the size of $h^{(\geq r)}A$ is tight over the groups $\mathbb{Z}$ and $\mathbb{Z}_p$, where p is a prime number.

1. Introduction

In this article, p stands for a prime number, θ for the golden ratio $\frac{1+\sqrt{5}}{2}$, G for an additive abelian group, $\mathbb{Z}$ for the group of integers, and $\mathbb{Z}_m$ for the group $\{0, 1, \ldots, m-1\}$, where m is a positive integer. For a given set A of integers, $|A|$ denotes the number of elements of A.

For a non-empty subset A of G and a positive integer h, let hA denote the set of elements of G that can be written as a sum of h elements of A, and $h\hat{}A$ denote the set of elements of G that can be written as a sum of h distinct elements of A. The sets hA and $h\hat{}A$ are called sumsets and restricted sumsets, respectively. One of the important problems in additive combinatorics is to estimate the sumsets hA and $h\hat{}A$ in terms of the size of A and the integer h. Such problems are known as direct problems. Some of the early results in this direction are the Cauchy-Davenport theorem [6, 7, 8] and the Erdős-Heilbronn conjecture (or Dias da Silva-Hamidoune theorem) [9].

DOI: 10.5281/zenodo.14907283

Theorem 1 (Cauchy-Davenport theorem [6, 7, 8]). *Let A be a non-empty k-element set in $\mathbb{Z}_p$. Then, for any positive integer h, we have*

$$|hA| \geq \min\{p, hk - h + 1\}.$$

Theorem 2 (Dias da Silva-Hamidoune theorem [9]). *Let A be a non-empty k-element set in $\mathbb{Z}_p$. Then, for any positive integer $h \leq k$, we have*

$$|h\hat{}A| \geq \min\{p, hk - h^2 + 1\}.$$

Another important problem in additive number theory is determining the structure of a set A given some information on the size of the sumsets. These are classified as inverse problems. Examples of such results are Vosper's theorem [21, 22], Nathanson's theorem [17], and Freiman's $3k - 4$ theorem [12].

Theorem 3 (Vosper's theorem [21, 22]). *Let A be a non-empty k-element set in $\mathbb{Z}_p$ with $k \geq 2$. If $h \geq 2$ and $|hA| = hk - h + 1 \leq p - 2$, then A is an arithmetic progression.*

Theorem 4 (Nathanson [17]). *Let A be a non-empty k-element set of integers with $k \geq 5$. If $2 \leq h \leq k-2$ and $|h\hat{}A| = hk - h^2 + 1$, then A is an arithmetic progression.*

Theorem 5 (Freiman's $3k-4$ theorem [12]). *Let $k \geq 3$. Let $A = \{a_0, a_1, \ldots, a_{k-1}\}$ be a set of integers such that $0 = a_0 < a_1 < \cdots < a_{k-1}$ and $d(A) = 1$. If $|2A| = 2k - 1 + b \leq 3k - 4$, then A is a subset of an arithmetic progression of length at most $k + b$.*

For recent results along this line, see [4, 5, 15, 16, 23].

In this paper, we consider a sumset that generalizes the sumsets hA and $h\hat{}A$ and also discuss the direct and inverse problems.

Definition 1. Let $A = \{a_1, a_2, \ldots, a_k\}$ be a non-empty finite set in G. Let $r \leq k$ be a positive integer. For integers $h \geq r$, we define

$$h^{(\geq r)}A := \left\{ \sum_{i \in I} x_i a_i : I \subset [1, k], |I| \geq r, x_i \geq 1 \text{ for all } i \in I, \text{ and } \sum_{i \in I} x_i = h \right\}.$$

Then $h^{(\geq r)}A = hA$ if $r = 1$ and $h^{(\geq r)}A = h\hat{}A$ if $r = h$.

Before we state our main result, we present some background on the problem.

In 2006, Plagne [19] (also see [10, 20]) extended the Cauchy-Davenport theorem to the group $\mathbb{Z}_m$ by finding the exact value of

$$\mu(\mathbb{Z}_m, k, h) = \min\{|hA| : A \subset \mathbb{Z}_m, |A| = k\}.$$

Theorem 6 (Plagne [19]). *Let m, k, h be positive integers with $k \leq m$. Then*

$$\mu(\mathbb{Z}_m, k, h) = \min\{(h \lceil k/d \rceil - h + 1)d : d \in D(m)\},$$

where $D(m)$ is the set of positive divisors of m.

Later, in 2016, Bajnok [3] considered the analogous function $\hat{\mu}(\mathbb{Z}_m, k, h) = \min\{|h\hat{\ }A| : A \subset \mathbb{Z}_m, |A| = k\}$ and proved an upper bound for $\hat{\mu}(\mathbb{Z}_m, k, h)$ by estimating the exact size of the set $h\hat{\ }A_d(m,k)$, where $h\hat{\ }A_d(m,k)$ is defined in the following way. For a fixed positive divisor d of m, consider the subgroup $H = \{0, m/d, \ldots, (d-1)(m/d)\}$ of $\mathbb{Z}_m$ of order d. Write $k = ud + v$ for some non-negative integers u, v with $1 \le v \le d$. Define

$$A_d(m,k) := \bigcup_{i=0}^{u-1} \Big\{ i + H \Big\} \bigcup \Big\{ u + j \cdot \frac{m}{d} : j = 0, 1, \ldots, v-1 \Big\}. \tag{1}$$

The following is the theorem of Bajnok.

Theorem 7 (Bajnok [3])**.** *Let h, k, and m be positive integers such that $k \le m$. Let d be a positive divisor of m. Let $A_d(m,k)$ be the set of k elements defined in (1). If $h = k$, then $|h\hat{\ }A_d(m,k)| = 1$, and if $h > k$, then $|h\hat{\ }A_d(m,k)| = 0$. For $1 \le h \le k-1$, let v and w be the positive remainders of k and h modulo d, respectively. Then*

$$|h\hat{\ }A_d(m,k)| = \begin{cases} \min\left\{m, \left(h\left\lceil \frac{k}{d}\right\rceil - h + 1\right)d, hk - h^2 + 1\right\} & \text{if } h \le \min\{v, d-1\}, \\ \min\{m, hk - h^2 + 1 - \delta_d\} & \text{otherwise,} \end{cases}$$

where

$$\delta_d = \begin{cases} (v-w)w - (d-1) & \text{if } w < v, \\ (d-w)(w-v) - (d-1) & \text{if } v < w < d, \\ d-1 & \text{if } v = w = d, \\ 0 & \text{otherwise.} \end{cases}$$

The main result of this paper is the following theorem along the lines of Theorem 7.

Theorem 8. *Let m, k, r be positive integers such that $r \le k \le m$. For a fixed positive divisor d of m, let $A_d(m,k) \subset \mathbb{Z}_m$ be a set of k elements defined in (1). Let v, w be the respective positive remainders of k, r modulo d. Then, for every integer $h > r$, we have*

$$|h^{(\ge r)}A_d(m,k)| = \begin{cases} \min\left\{m, \left(h\left\lceil \frac{k}{d}\right\rceil - h + 1\right)d, h(k-1) - r(r-1) + 1\right\} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } r \le \min\{v, d-1, k-1\} \\ \min\{m, h(k-1) - r(r-1) + 1 - \epsilon_d\} \qquad \text{otherwise,} \end{cases}$$

where

$$\epsilon_d = \begin{cases} (h-r)(v-1) + w(v-w) - (d-1) & \text{if } w < v \\ (h-r)(v-1) + (d-w)(w-v) - (d-1) & \text{if } v < w < d \\ (h-r)(v-1) - (d-1) & \text{otherwise.} \end{cases}$$

If we set $\mu^{(\geq r)}(\mathbb{Z}_m, k, h) := \min\{|h^{(\geq r)}A| : A \subset \mathbb{Z}_m, |A| = k\}$, analogous to the functions $\mu(\mathbb{Z}_m, k, h)$ and $\hat{\mu}(\mathbb{Z}_m, k, h)$, we obtain the following upper bound from Theorem 8:

$$\mu^{(\geq r)}(\mathbb{Z}_m, k, h) \leq \min\{|h^{(\geq r)}A_d(m, k)| : d \in D(m)\}. \tag{2}$$

2. Proof of Main Result

In this section we prove Theorem 8, for which we require the following lemma.

Lemma 1 (Bajnok [3]). *Let d and t be positive integers with $t \leq d-1$, and let $\ell \in \mathbb{Z}_d$. Then there is a t-element set $L = \{\ell_1, \ldots, \ell_t\}$ in $\mathbb{Z}_d$ for which $\ell_1 + \cdots + \ell_t = \ell$.*

Proof of Theorem 8. For a fixed positive divisor d of m, consider the subgroup $H = \{0, m/d, \ldots, (d-1)(m/d)\}$ of order d. Let $k = ud + v$ with $1 \leq v \leq d$, and

$$A_d(m, k) = \bigcup_{j=0}^{u-1} \left\{ j + H \right\} \bigcup \left\{ u + \ell \cdot \frac{m}{d} : \ell = 0, 1, \ldots, v-1 \right\}.$$

Since w is the positive remainder of r modulo d, we have $r = qd + w$ with some non-negative integer q. By definition every element of $h^{(\geq r)}A_d(m, k)$ is of the form

$$(j_1 + \cdots + j_h) + (\ell_1 + \cdots + \ell_h) \cdot \frac{m}{d}, \tag{3}$$

where $j_1, \ldots, j_h \in \{0, 1, \ldots, u\}$ and $\ell_1, \ldots, \ell_h \in \{0, 1, \ldots, d-1\}$, with the following two added conditions:

(i) when any of the j-indices equals u, the corresponding ℓ-index is at most $v-1$,

(ii) there are at least r distinct $j + \ell \cdot (m/d)$ in every sum of the form (3).

Let us denote the least value of $j_1 + \cdots + j_h$ in (3) by j_{min} and the largest value of $j_1 + \cdots + j_h$ in (3) by j_{max}. Then

$$j_{min} = (h - r + d) \cdot 0 + d \cdot 1 + d \cdot 2 + \cdots + d \cdot (q-1) + w \cdot q = q(r + w - d)/2.$$

On the other hand, to calculate j_{max} we consider the following four possible cases. If $q = 0$ and $w > v$, then $r = w > v$ and $1 \leq w - v \leq d - 1$. Therefore

$$j_{max} = (h - r + v) \cdot u + (w - v) \cdot (u - 1) = hu - r + v.$$

If $q = 0$ and $w \leq v$, then $r = w \leq v$. Therefore

$$j_{max} = h \cdot u = hu - r + w.$$

If $q \geq 1$ and $w > v$, then by writing $r = v + qd + (w - v)$, where $1 \leq w - v \leq d - 1$, we get

$$j_{max} = (h - r + v) \cdot u + d \cdot (u - 1) + \cdots + d \cdot (u - q) + (w - v) \cdot (u - q - 1).$$

After simplification we get

$$j_{max} = hu - r + vq - \frac{q(r + w - d)}{2} + v.$$

Finally, if $q \geq 1$ and $w \leq v$, then by writing $r = v + (q - 1)d + (d + w - v)$, where $1 \leq d + w - v \leq d$, we get

$$\begin{aligned} &j_{max} \\ &= (h - r + v) \cdot u + d \cdot (u - 1) + \cdots + d \cdot (u - q + 1) + (d + w - v) \cdot (u - q) \\ &= (h - r + v) \cdot u + d \cdot (u - 1) + \cdots + d \cdot (u - q) + (w - v) \cdot (u - q - 1) + (w - v) \\ &= hu - r + vq - \frac{q(r + w - d)}{2} + w. \end{aligned}$$

We can combine the above four possible values of j_{max} and write in the following unified form

$$j_{max} = hu - r + vq - \frac{q(r + w - d)}{2} + \min\{v, w\}.$$

Since $j = j_1 + \cdots + j_h$ can assume any integer value between j_{min} and j_{max}, the sumset $h^{(\geq r)} A_d(m, k)$ lies in exactly $\min\{m/d, j_{max} - j_{min} + 1\}$ cosets of H. Thus,

$$|h^{(\geq r)} A_d(m, k)| \leq \min\{m, (j_{max} - j_{min} + 1)d\}, \tag{4}$$

where after simplification we can write

$$(j_{max} - j_{min} + 1)d = h(k-1) - r(r-1) - (h-r)(v-1) - w(v-w) + d \cdot \min\{0, v-w\} + d.$$

Equation (4) gives an upper bound for the size of $h^{(\geq r)} A_d(m, k)$. However, to compute the exact value of $|h^{(\geq r)} A_d(m, k)|$ we need to consider the following three cases.

`Case 1:` $r = k$. In this case $u = q$ and $v = w$. Therefore,

$$\begin{aligned} &|h^{(\geq r)} A_d(m, k)| \\ &= \min\{m, (j_{max} - j_{min} + 1)d\} \\ &= \min\{m, h(k - 1) - r(r - 1) - (h - r)(v - 1) - w(v - w) + d \cdot \min\{0, v - w\} \\ &\qquad + d\} \\ &= \min\{m, h(k - 1) - r(r - 1) - (h - r)(v - 1) + d\}. \end{aligned}$$

`Case 2:` $r = 1$. In this case $h^{(\geq r)}A_d(m,k)$ is simply $hA_d(m,k)$. So,

$$h^{(\geq r)}A_d(m,k) = \bigcup_{j=0}^{hu-1} \Big\{j + H\Big\} \bigcup \Big\{hu + \ell \cdot \frac{m}{d} : \ell = 0, 1, \ldots, h(v-1)\Big\}.$$

Hence,

$$\begin{aligned}
|h^{(\geq r)}A_d(m,k)| &= \min\{m, hud + \min\{d, hv - h + 1\}\} \\
&= \min\{m, (hu+1)d, h(ud+v) - h + 1\} \\
&= \min\{m, (h\lceil k/d\rceil - h + 1)d, h(k-1) + 1\} \\
&= \min\{m, (h\lceil k/d\rceil - h + 1)d, h(k-1) - r(r-1) + 1\}.
\end{aligned}$$

`Case 3:` $2 \leq r \leq k-1$. We divide the proof of this case into the following six possible subcases.
`Subcase 1:` Assume that $r \leq v$ and $r < d$. Then $q = 0$, $r = w < d$, and $r = w \leq v$. Therefore, $j_{min} = 0$ and $j_{max} = hu$. Thus, by Lemma 1, we get

$$\begin{aligned}
h^{(\geq r)}A_d(m,k) = \bigcup_{j=0}^{hu-1} \Big\{j + H\Big\} \bigcup \Big\{hu + \ell \cdot \frac{m}{d} : \ell = \frac{r(r-1)}{2}, \frac{r(r-1)}{2} + 1, \ldots, \\
h(v-1) - \frac{r(r-1)}{2}\Big\}.
\end{aligned}$$

Hence,

$$\begin{aligned}
|h^{(\geq r)}A_d(m,k)| &= \min\{m, hud + \min\{d, h(v-1) - r(r-1) + 1\}\} \\
&= \min\{m, (hu+1)d, hud + h(v-1) - r(r-1) + 1\} \\
&= \min\{m, (h\lceil k/d\rceil - h + 1)d, h(k-1) - r(r-1) + 1\}.
\end{aligned}$$

`Subcase 2:` Assume that $r = v = d$. Then $q = 0$ and $w = r = d$. This implies $j_{min} = 0$ and $j_{max} = hu$. Further, since $r = d$, $k = ud + v = (u+1)d$, and $r < k$, we have $u \geq 1$. Therefore,

$$\begin{aligned}
&h^{(\geq r)}A_d(m,k) \\
&= \Big\{\ell \cdot \frac{m}{d} : \ell = \frac{d(d-1)}{2}, \frac{d(d-1)}{2} + 1, \ldots, h(d-1) - \frac{d(d-1)}{2}\Big\} \bigcup_{j=1}^{hu-1} \Big\{j + H\Big\} \\
&\qquad \bigcup \Big\{hu + \ell \cdot \frac{m}{d} : \ell = \frac{d(d-1)}{2}, \frac{d(d-1)}{2} + 1, \ldots, h(d-1) - \frac{d(d-1)}{2}\Big\}.
\end{aligned}$$

Hence,

$$\begin{aligned}
|h^{(\geq r)}A_d(m,k)| &= \min\{m, (hu-1)d + 2 \cdot \min\{d, h(d-1) - d(d-1) + 1\}\} \\
&= \min\{m, (hu+1)d, (hu-1)d + 2(h-d)(d-1) + 2\}.
\end{aligned}$$

As $h \geq r+1 = d+1$ and $d \geq 1$, we have $(hu-1)d + 2(h-d)(d-1) + 2 \geq (hu+1)d$. Therefore,

$$|h^{(\geq r)}A_d(m,k)| = \min\{m, (hu+1)d\} = \min\{m, (h\lceil k/d \rceil - h + 1)d\}.$$

But, $(h\lceil k/d \rceil - h + 1)d = h(k-1) - r(r-1) - (h-r)(v-1) + d$, thus, we get

$$|h^{(\geq r)}A_d(m,k)| = \min\{m, h(k-1) - r(r-1) - (h-r)(v-1) + d\}.$$

`Subcase 3:` Assume that $r > v$, $w \neq d$, and $w \neq v$. Then, by Lemma 1, we have

$$h^{(\geq r)}A_d(m,k) = \bigcup_{j=j_{min}}^{j_{max}} \Big\{ j + H \Big\}.$$

Hence,

$$\begin{aligned}
&|h^{(\geq r)}A_d(m,k)| \\
&= \min\{m, (j_{max} - j_{min} + 1)d\} \\
&= \min\{m, h(k-1) - r(r-1) - (h-r)(v-1) - w(v-w) + d \cdot \min\{0, v-w\} \\
&\qquad + d\}.
\end{aligned}$$

`Subcase 4:` Assume that $r > v$, $w = d$, and $w \neq v$. Then $r = (q+1)d$ and $k = ud + v$ with $v < d$. This implies $j_{min} = \frac{q(q+1)d}{2}$ and $j_{max} = hu$. Thus,

$$\begin{aligned}
&h^{(\geq r)}A_d(m,k) \\
&= \Big\{ \frac{q(q+1)d}{2} + \ell \cdot \frac{m}{d} : \ell = \frac{(q+1)d(d-1)}{2}, \frac{(q+1)d(d-1)}{2} + 1, \ldots, \\
&\qquad \frac{(q+1)d(d-1)}{2} + (h-r)(d-1) \Big\} \bigcup_{j=\frac{q(q+1)d}{2}+1}^{hu} \Big\{ j + H \Big\}.
\end{aligned}$$

Hence,

$$\begin{aligned}
&|h^{(\geq r)}A_d(m,k)| \\
&= \min\{m, \min\{d, (h-r)(d-1)+1\} + (j_{\max} - j_{\min})d\} \\
&= \min\{m, (j_{\max} - j_{\min} + 1)d, (j_{\max} - j_{\min})d + (h-r)(d-1) + 1\} \\
&= \min\{m, h(k-1) - r(r-1) - (h-r)(v-1) + d, h(k-1) - r(r-1) \\
&\qquad - (h-r)(v-d) + 1\}.
\end{aligned}$$

Note that

$$h(k-1) - r(r-1) - (h-r)(v-1) + d \leq h(k-1) - r(r-1) - (h-r)(v-d) + 1$$

if and only if

$$(h-r)(d-1) \geq d-1.$$

As $h > r$, the latter inequality is true. Hence,

$$|h^{(\geq r)}A_d(m,k)| = \min\{m, h(k-1) - r(r-1) - (h-r)(v-1) + d\}.$$

`Subcase 5:` Assume that $r > v$, $w \neq d$, and $w = v$. Then $r = qd+v$ and $k = ud+v$ with $v = w < d$. This implies $j_{min} = q(r+w-d)/2$ and $j_{max} = hu-r+v-\frac{q(r-v-d)}{2}$. Thus,

$$\begin{aligned} &h^{(\geq r)}A_d(m,k) \\ &= \bigcup_{j=j_{\min}}^{j_{\max}-1}\left\{j+H\right\} \bigcup \left\{j_{max} + \ell\cdot\frac{m}{d} : \ell = \frac{d(d-1)q}{2} + \frac{v(v-1)}{2},\right. \\ &\qquad \left.\frac{d(d-1)q}{2} + \frac{v(v-1)}{2} + 1, \ldots, \frac{d(d-1)q}{2} + \frac{v(v-1)}{2} + (h-r)(d-1)\right\}. \end{aligned}$$

Hence,

$$\begin{aligned} &|h^{(\geq r)}A_d(m,k)| \\ &= \min\{m, (j_{\max} - j_{\min})d + \min\{d, (h-r)(d-1)+1\}\} \\ &= \min\{m, (j_{\max} - j_{\min}+1)d, (j_{\max} - j_{\min})d + (h-r)(d-1)+1\} \\ &= \min\{m, (j_{\max} - j_{\min}+1)d\} \\ &= \min\{m, h(k-1) - r(r-1) - (h-r)(v-1) + d\}. \end{aligned}$$

`Subcase 6:` Assume that $r > v$ and $w = v = d$. Then $r = (q+1)d$ and $k = (u+1)d$. Thus,

$$\begin{aligned} &h^{(\geq r)}A_d(m,k) \\ &= \left\{j_{\min} + \ell\cdot\frac{m}{d} : \ell = \frac{(q+1)d(d-1)}{2}, \ldots, \frac{(q+1)d(d-1)}{2} + (h-r)(d-1)\right\} \\ &\quad \bigcup_{j=j_{\min}+1}^{j_{\max}-1}\left\{j+H\right\} \bigcup \left\{j_{\max} + \ell\cdot\frac{m}{d} : \ell = \frac{(q+1)d(d-1)}{2}, \ldots,\right. \\ &\qquad\qquad \left.\frac{(q+1)d(d-1)}{2} + (h-r)(d-1)\right\}. \end{aligned}$$

Hence,

$$\begin{aligned}
&|h^{(\geq r)}A_d(m,k)| \\
&= \min\{m, (j_{\max} - j_{\min} - 1)d + 2 \cdot \min\{d, (h-r)(d-1)+1\}\} \\
&= \min\{m, (j_{\max} - j_{\min} + 1)d, (j_{\max} - j_{\min} - 1)d + 2(h-r)(d-1)+2\} \\
&= \min\{m, h(k-1) - r(r-1) - (h-r)(v-1) + d, h(k-1) - r(r-1) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad + (h-r-1)(d-1)+1\} \\
&= \min\{m, h(k-1) - r(r-1) - (h-r)(v-1) + d\}.
\end{aligned}$$

□

3. An Observation and its Consequences

Recall that in the introduction we defined the sumsets hA and $h\hat{}A$ for positive integers h. Here we add the convention that $0A = 0\hat{}A = \{0\}$. As every element of $h^{(\geq r)}A$ is a sum of h terms of A with at least r of them distinct, we have the following lemma.

Lemma 2. *Let A be a non-empty k-element set in G. Let r be a positive integer such that $r \leq k$. Then, for every positive integer $h \geq r$, we have*

$$h^{(\geq r)}A = (h-r)A + r\hat{}A. \tag{5}$$

We note that this lemma does not provide a simple proof of Theorem 8. However, we can use it to obtain some direct and inverse results for $h^{(\geq r)}A$ (see Theorems 9, 11, and 12). We can also use Lemma 2 to obtain a Freiman's $3k-4$ theorem-type result for $h^{(\geq r)}A$. We start with the following direct theorem.

Theorem 9. *Let k, r be positive integers with $r \leq k$. Then, for every positive integer $h \geq r$ and non-empty k-element set A in $\mathbb{Z}_p$, we have*

$$|h^{(\geq r)}A| \geq \min\{p, h(k-1) - r(r-1) + 1\}. \tag{6}$$

This lower bound is sharp.

To prove this theorem we shall use Theorem 1 together with the following theorem, which is another version of the Cauchy-Davenport theorem.

Theorem 10 ([18])**.** *Let A, B be non-empty subsets of $\mathbb{Z}_p$, where p is a prime number. Then*

$$|A+B| \geq \min\{p, |A| + |B| - 1\}.$$

Proof of Theorem 9. The case $k = 1$ is obvious. Assume that $k \geq 2$. By Lemma 2, we have $h^{(\geq r)}A = (h-r)A + r\hat{}A$. Then, by Theorem 10,

$$|h^{(\geq r)}A| = |(h-r)A + r\hat{}A| \geq \min\{p, |(h-r)A| + |r\hat{}A| - 1\}.$$

Now, by applying Theorem 1 on $(h-r)A$ and Theorem 2 on $r\hat{}A$, we obtain

$$\begin{aligned} |h^{(\geq r)}A| &\geq \min\{p, |(h-r)A| + |r\hat{}A| - 1\} \\ &\geq \min\{p, \min\{p, (h-r)(k-1)+1\} + \min\{p, r(k-r)+1\} - 1\} \\ &\geq \min\{p, (h-r)(k-1) + r(k-r) + 1\} \\ &= \min\{p, h(k-1) - r(r-1) + 1\}. \end{aligned}$$

This establishes the lower bound in Equation (6).

Choose a prime number p and positive integers h, r, k such that $r \leq \min\{h, k\}$ and $h(k-1) - r(r-1) + 1 \leq p$. Let $A = [1, k] \subset \mathbb{Z}_p$. Then

$$h^{(\geq r)}A \subset [(h-r+1)\cdot 1 + 2 + 3 + \cdots + r, (h-r+1)\cdot k + (k-1) + (k-2) + \cdots + (k-r+1)].$$

Therefore,

$$|h^{(\geq r)}A| \leq h(k-1) - r(r-1) + 1.$$

This upper bound together with Equation (6) shows that $|h^{(\geq r)}A| = h(k-1) - r(r-1) + 1$. Hence, the lower bound in Equation (6) is sharp. □

The following theorem gives the structure of set A for which the bound in Theorem 9 is tight.

Theorem 11. *Let k, r be positive integers with $k \geq 2$ and $r \leq k$. Let $h \geq r+2$ be a positive integer and A be a non-empty k-element set in $\mathbb{Z}_p$ with*

$$|h^{(\geq r)}A| = h(k-1) - r(r-1) + 1 \leq p - 2.$$

Then A is an arithmetic progression.

Proof. As any set of two elements is an arithmetic progression, we shall assume that $k \geq 3$. Observe that

$$\begin{aligned} \max\{(h-r)(k-1)+1, r(k-r)+1\} &\leq (h-r)(k-1) + r(k-r) + 1 \\ &= h(k-1) - r(r-1) + 1 \\ &\leq p - 2. \end{aligned}$$

As it is given that

$$|h^{(\geq r)}A| = h(k-1) - r(r-1) + 1,$$

from the proof of Theorem 9, we obtain

$$|(h-r)A| = \min\{p, (h-r)(k-1)+1\} = (h-r)(k-1) + 1 \leq p - 2.$$

Then, Theorem 3 implies that the set A is an arithmetic progression. □

One can prove the following theorem using similar arguments as in Theorem 9 and Theorem 11.

Theorem 12. *Let k, r be positive integers with $r \leq k$. Then for every positive integer $h \geq \max\{r, 2\}$ and non-empty k-element set A of integers, we have*

$$|h^{(\geq r)}A| \geq h(k-1) - r(r-1) + 1. \tag{7}$$

Furthermore, if $|h^{(\geq r)}A| = h(k-1) - r(r-1) + 1$ and

1. *$k \geq 2$ in case $h \geq r+2$,*
2. *$k \geq 5$ and $2 \leq r \leq k-2$ in case $h = r$ or $h = r+1$,*

then A is an arithmetic progression.

From Theorem 12 it follows that the set A is an arithmetic progression if the lower bound for $|h^{(\geq r)}A|$ is tight. A natural question that arises here is: up to what deviation from the lower bound in Theorem 12 can one cover the set A inside a "small" arithmetic progression? To answer such a question, one possible way is to express the size of $h^{(\geq r)}A$ in terms of the size of $(h-1)^{(\geq r)}A$ or lower order sumsets. Theorem 14 is one such result in this direction, which directly follows from Lemma 2 and the following theorem of Lev [13].

Theorem 13 (Lev [13])**.** *Let $k \geq 3$. Let $A = \{a_0, a_1, \ldots, a_{k-1}\}$ be a set of integers such that $0 = a_0 < a_1 < \cdots < a_{k-1}$ and $\gcd(A) = 1$. Then, for $h \geq 2$, we have*

$$|hA| \geq |(h-1)A| + \min\{a_{k-1}, h(k-2) + 1\}.$$

Theorem 14. *Let r, k be positive integers such that $k \geq 3$ and $r \leq k$. Let $A = \{a_0, a_1, \ldots, a_{k-1}\}$ be a set of k integers such that $0 = a_0 < a_1 < \cdots < a_{k-1}$ and $\gcd(A) = 1$. Then, for $h \geq r+2$, we have*

$$|h^{(\geq r)}A| \geq |r\hat{}A| + |(h-r-1)A| + \min\{a_{k-1}, (h-r)(k-2) + 1\}.$$

4. Further Remarks

Another sumset that may come immediately to the reader's mind is the sumset $h^{(\leq r)}A$, which contains those elements of the group G that are the sum of h elements of A with at most r distinct elements. The sumset hA is a special case of $h^{(\leq r)}A$ for $r = h$.

Let $A = \{a_1, a_2, \ldots, a_k\}$ be a set of k integers. Then for any positive integer h the sumset hA contains at least the following $hk - h + 1$ elements written in an increasing order:

$$\begin{aligned} &ha_1 < (h-1)a_1 + a_2 < \cdots < a_1 + (h-1)a_2 < \\ &ha_2 < (h-1)a_2 + a_3 < \cdots < a_2 + (h-1)a_3 < \\ &\vdots \\ &ha_{k-1} < (h-1)a_{k-1} + a_k < \cdots < a_{k-1} + (h-1)a_k < \\ &ha_k. \end{aligned}$$

Observe that to get the minimum number of elements (which is $hk - h + 1$) in the sumset $hA = h^{(\leq h)}A$, we only required elements in hA which are sums of at most two distinct elements of A (see the list of elements above). Thus, the sumset $h^{(\leq r)}A$ contains at least $hk - h + 1$ distinct elements for all $r \geq 2$. Therefore, we ask the following question for integers $r \geq 2$.

Question 1. Is it always the case that the minimum size of both the sumsets hA and $h^{(\leq r)}A$ are the same in any abelian group G, where the minimum runs over the subsets of G of size (say) k?

Acknowledgement. The author thanks Professor Georges Grekos and the anonymous referee for reading the article carefully, pointing out some typos, and making suggestions that improved the presentation of the article.

References

[1] N. Alon, M. B. Nathanson, and I. Ruzsa, Adding distinct congruence classes modulo a prime, *Amer. Math. Monthly* **102** (1995), 250-255.

[2] N. Alon, M. B. Nathanson, and I. Ruzsa, The polynomial method and restricted sums of congruence classes, *J. Number Theory* **56** (1996), 404-417.

[3] B. Bajnok, On the minimum cardinality of restricted sumsets in cyclic groups, *Acta Math. Hungar.* **148** (1) (2016), 228-256.

[4] J. Bhanja, T. Komatsu, and R. K. Pandey, Direct and inverse problems for restricted signed sumsets in integers, *Contrib. Discrete Math.* **16** (1) (2021), 28-46.

[5] J. Bhanja and R. K. Pandey, Direct and inverse theorems on signed sumsets of integers, *J. Number Theory* **196** (2019), 340-352.

[6] A. L. Cauchy, Recherches sur les nombres, *J. Éc. polytech. Math.* **9** (1813), 99-116.

[7] H. Davenport, On the addition of residue classes, *J. Lond. Math. Soc.* **10** (1935), 30-32.

[8] H. Davenport, A historical note, *J. Lond. Math. Soc.* **22** (1947), 100-101.

[9] J. A. Dias da Silva and Y. O. Hamidoune, Cyclic space for Grassmann derivatives and additive theory, *Bull. Lond. Math. Soc.* **26** (1994), 140-46.

[10] S. Eliahou, M. Kervaire, and A. Plagne, Optimally small sumsets in finite Abelian groups, *J. Number Theory* **101** (2003), 338-348.

[11] P. Erdős and H. Heilbronn, On the addition of residue classes mod p, *Acta Arith.* **9** (1964), 149-159.

[12] G. A. Freiman, *Foundations of a Structural Theory of Set Addition* (in Russian), Kazan: Kazan Gos. Ped. Inst, 1966.

[13] V. F. Lev, Structure theorem for multiple addition and the Frobenius problem, *J. Number Theory* **58** (1996), 79-88.

[14] V. F. Lev, Restricted set addition in groups I: The classical setting, *J. Lond. Math. Soc.* **62** (2000), 27-40.

[15] R. K. Mistri and R. K. Pandey, A generalization of sumsets of set of integers, *J. Number Theory* **143** (2014), 334-356.

[16] F. Monopoli, A generalization of sumsets modulo a prime, *J. Number Theory* **157** (2015), 271-279.

[17] M. B. Nathanson, Inverse theorems for subset sums, *Trans. Amer. Math. Soc.* **347** (1995), 1409-1418.

[18] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

[19] A. Plagne, Optimally small sumsets in groups, I. The supersmall sumset property, the $\mu_G^{(k)}$ and the $\nu_G^{(k)}$ functions, *Unif. Distrib. Theory* **1** (1) (2006), 27-44.

[20] A. Plagne, Optimally small sumsets in groups, II. The hypersmall sumset property and restricted addition, *Unif. Distrib. Theory* **1** (1) (2006), 111-124.

[21] A. G. Vosper, The critical pairs of subsets of a group of prime order, *J. Lond. Math. Soc.* **31** (1956), 200-205.

[22] A. G. Vosper, Addendum to "The critical pairs of subsets of a group of prime order", *J. Lond. Math. Soc.* **31** (1956), 280-282.

[23] Q. H. Yang and Y. G. Chen, On the cardinality of general h-fold sumsets, *European J. Combin.* **47** (2015), 103-114.