ON THE MINIMUM CARDINALITY OF GENERALIZED SUMSETS IN FINITE CYCLIC GROUPS

Jagannath Bhanja
Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Prayagraj, Uttar Pradesh, India
jagannathbhanja@hri.res.in

Received: 1/31/20, Revised: 10/3/20, Accepted: 12/20/20, Published: 2/1/21

Abstract

For a nonempty subset $\mathcal{A}$ of an abelian group $\mathcal{G}$, the *generalized sumset* $h^{(r)}\mathcal{A}$ consists of all sums of h elements of $\mathcal{A}$ with at most r repetitions for each element. In this paper, we generalize an earlier result of Bajnok on *restricted sumsets* $h^{(1)}\mathcal{A}$ in $\mathbb{Z}_n$ to generalized sumsets $h^{(r)}\mathcal{A}$ in $\mathbb{Z}_n$ for $1 \leq r \leq h$. More precisely, given positive integers h, r, k, we prove an upper bound for the minimum cardinality of $h^{(r)}\mathcal{A}$ when $\mathcal{A}$ runs through all k-subsets of $\mathbb{Z}_n$. This is done by exactly calculating $|h^{(r)}\mathcal{A}|$ for a very specific k-subset $\mathcal{A} = \mathcal{A}_d(n,k)$ of $\mathbb{Z}_n$.

1. Introduction

Let $\mathcal{G}$ be an abelian group written in additive notation. For a positive integer h and a nonempty finite subset $\mathcal{A}$ of $\mathcal{G}$, we let $h\mathcal{A}$ and $h^{\wedge}\mathcal{A}$ be the *h-fold sumset* and the *h-fold restricted sumset* of $\mathcal{A}$, respectively; that is, $h\mathcal{A}$ is the collection of all sums of h not-necessarily-distinct elements of $\mathcal{A}$, and $h^{\wedge}\mathcal{A}$ is the collection of all sums of h distinct elements of $\mathcal{A}$. Clearly, in every element of $h\mathcal{A}$ an element of $\mathcal{A}$ can appear at most h times, whereas it can appear at most once in every element of $h^{\wedge}\mathcal{A}$.

For given positive integers h, r with $r \leq h$, let $h^{(r)}\mathcal{A}$ be the collection of all sums of h elements of $\mathcal{A}$ with at most r repetitions for each element. The sumset $h^{(r)}\mathcal{A}$ denote the *generalized sumset* of $\mathcal{A}$. Clearly, $h^{(h)}\mathcal{A} = h\mathcal{A}$ and $h^{(1)}\mathcal{A} = h^{\wedge}\mathcal{A}$. Therefore, $h^{(r)}\mathcal{A}$ is a natural generalization of $h\mathcal{A}$ and $h^{\wedge}\mathcal{A}$.

For a positive integer k ($\leq |\mathcal{G}|$), let

$$\mu(\mathcal{G},k,h) := \min\{|h\mathcal{A}| : \ \mathcal{A} \subseteq \mathcal{G}, |\mathcal{A}| = k\},$$

$$\mu^{\wedge}(\mathcal{G},k,h) := \min\{|h^{\wedge}\mathcal{A}| : \ \mathcal{A} \subseteq \mathcal{G}, |\mathcal{A}| = k\},$$

and

$$\mu^{(r)}(\mathcal{G},k,h) := \min\{|h^{(r)}\mathcal{A}| : \ \mathcal{A} \subseteq \mathcal{G}, |\mathcal{A}| = k\}.$$

Given a nonempty subset $\mathcal{A}$ of a finite abelian group $\mathcal{G}$, one of the important problems in *additive number theory* is to find the minimum cardinality of its sumsets; that is, to find the exact value of the functions $\mu(\mathcal{G},k,h)$, $\mu^{\wedge}(\mathcal{G},k,h)$, and $\mu^{(r)}(\mathcal{G},k,h)$ in terms of $|\mathcal{G}|$, k, h, and/or r.

The study of $\mu(\mathcal{G},k,h)$ dates back to 1813, to one of the classical works of Cauchy [4], which gives the exact value of $\mu(\mathcal{G},k,h)$ in cyclic groups of prime order. Later, in 1935, Davenport [5] (see also [6]) rediscovered Cauchy's result. It is now known as the Cauchy-Davenport Theorem.

Theorem 1 (**Cauchy-Davenport Theorem [4–6]**). *Let $\mathcal{A}$ be a nonempty k-subset of the group $\mathbb{Z}_p$, where p is a prime number. Then*

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

This lower bound is tight for all values of k. Hence,

$$\mu(\mathbb{Z}_p,k,h) = \min\{p, hk-h+1\}.$$

After several important but partial results proved in this direction, Eliahou, Kervaire, and Plagne [8] (see also [12,13]) finally settled the general case by finding the exact value of $\mu(\mathcal{G},k,h)$ in arbitrary finite abelian groups.

Theorem 2 (**Eliahou, Kervaire, and Plagne [8]**). *Let n, k, and h be positive integers with $k \leq n$. For any abelian group $\mathcal{G}$ of order n, we have*

$$\mu(\mathcal{G},k,h) = \phi(n,k,h),$$

where

$$\phi(n,k,h) := \min\{(h\lceil k/d\rceil - h + 1)d : \ d \in D(n)\},$$

and $D(n)$ is the set of positive divisors of n.

If $n = p$ is a prime number, then $\phi(p,k,h) = \min\{p, hk-h+1\}$. Therefore, Theorem 2 is a generalization of the Cauchy-Davenport Theorem, i.e., Theorem 1.

In contrast to $\mu(\mathcal{G},k,h)$, the function $\mu^{\wedge}(\mathcal{G},k,h)$ is not well settled in general finite abelian groups. The exact value of $\mu^{\wedge}(\mathcal{G},k,h)$ is known only in the cyclic groups of prime order. It was actually a conjecture of Erdős and Heilbronn [9] in 1964. In 1994, Dias da Silva and Hamidoune [7] proved this conjecture in its general form, that is, for all $h \geq 2$. They used some techniques from exterior algebra and representation theory. A year later the same conjecture was reproved by Alon, Nathanson, and Ruzsa [1, 2] using a more simple but powerful method, called the *polynomial method*.

Theorem 3 (**Dias da Silva and Hamidoune [7]**). *Let $\mathcal{A}$ be a nonempty k-subset of the group $\mathbb{Z}_p$, where p is a prime number. Then*

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

This bound is tight for all values of k. Therefore,

$$\mu^{\wedge}(\mathbb{Z}_p, k, h) = \min\{p, hk - h^2 + 1\}.$$

It is very difficult to find the exact value of $\mu^{\wedge}(\mathcal{G}, k, h)$ in general finite abelian groups, as in contrast to $\mu(\mathcal{G}, k, h)$, $\mu^{\wedge}(\mathcal{G}, k, h)$ depends on both cardinality and structure of the group $\mathcal{G}$.

In a recent study Bajnok [3] obtained an upper bound for the function $\mu^{\wedge}(\mathbb{Z}_n, k, h)$ by calculating the exact cardinality of a very specific set, which we define below.

For a given positive divisor d of n, we write k as $k = ud + v$ with $1 \le v \le d$, and set

$$\mathcal{A}_d(n,k) = \bigcup_{i=0}^{u-1} (i + \mathcal{H}) \bigcup \left\{ u + j \cdot \frac{n}{d} : \ j = 0, 1, \ldots, v-1 \right\}, \tag{1}$$

where $\mathcal{H} = \{0, n/d, \ldots, (d-1)(n/d)\}$ is the unique subgroup of order d in $\mathbb{Z}_n$. Clearly, $|\mathcal{A}_d(n,k)| = k$, and the set $\mathcal{A}_d(n,k)$ lies in exactly $\lceil k/d \rceil$ cosets of $\mathcal{H}$. Since $k \le n$, we have $u < n/d$. Thus, the set $\mathcal{A}_d(n,k)$ has k distinct elements.

Theorem 4 (Bajnok [3]). *Let n, k, and h be positive integers with $k \le n$. Let d be a positive divisor of n.*

If $h = k$, then $|h^{\wedge}\mathcal{A}_d(n,k)| = 1$, and if $h > k$, then $|h^{\wedge}\mathcal{A}_d(n,k)| = 0$.

For $1 \le h \le k-1$, let v and w be the positive remainders of k and h modulo d, respectively. Then

$$|h^{\wedge}\mathcal{A}_d(n,k)| = \begin{cases} \min\left\{n, \left(h\left\lceil \frac{k}{d} \right\rceil - h + 1\right) d, hk - h^2 + 1\right\} & \text{if } h \le \min\{v, d-1\}; \\ \min\{n, hk - h^2 + 1 - \delta_d\} & \text{otherwise}; \end{cases}$$

where δ_d is the correction term defined by

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

Thus, by setting

$$\phi^{\wedge}(n,k,h) := \min\{|h^{\wedge}\mathcal{A}_d(n,k)| : \ d \in D(n)\},$$

one has

$$\mu^{\wedge}(\mathbb{Z}_n, k, h) \le \phi^{\wedge}(n,k,h).$$

Turning now to the generalized sumset, $h^{(r)}\mathcal{A}$ was introduced by Mistri and Pandey [10] in 2014. They obtained the minimum cardinality of $h^{(r)}\mathcal{A}$ for all k, h, and r, when $\mathcal{A}$ is a finite set of k integers. A year later Monopoli [11] proved a similar result when $\mathcal{A}$ is a nonempty subset of the group $\mathbb{Z}_p$, where p is a prime number.

Theorem 5 (**Monopoli [11]**). *Let h and r be positive integers such that $h = mr+\epsilon$ with $0 \le \epsilon < r$. Let $\mathcal{A} \subseteq \mathbb{Z}_p$ be a nonempty set with $|\mathcal{A}| = k$ and $rk \ge h$. Then*

$$|h^{(r)}\mathcal{A}| \ge \min\{p, hk - m^2r + 1 - (2m+1)\epsilon\}.$$

This lower bound is tight for all values of h, r, and k, which can be seen by taking an arithmetic progression. Hence,

$$\mu^{(r)}(\mathbb{Z}_p, k, h) = \min\{p, hk - m^2r + 1 - (2m+1)\epsilon\}.$$

In this article we give an upper bound for the function $\mu^{(r)}(\mathbb{Z}_n, k, h)$ for all n, k, and h, which we obtain by exactly calculating $|h^{(r)}\mathcal{A}_d(n,k)|$. This computation is very similar to Bajnok's proof of Theorem 4. We use the following lemma of Bajnok (see Lemma 14, [3]) to achieve our results.

Lemma 1 (**Bajnok [3]**). *Let d and t be positive integers with $t \le d-1$, and let $j \in \mathbb{Z}_d$. Then there is a t-subset $J = \{j_1, \ldots, j_t\}$ of $\mathbb{Z}_d$ for which $j_1 + \cdots + j_t = j$.*

2. Main Results

Let $\mathcal{A}$ be a nonempty k-subset of $\mathbb{Z}_n$. Let h, r be positive integers with $r \le h$. Set $h = mr + \epsilon$, where $0 \le \epsilon < r$. So, by the definition of $h^{(r)}\mathcal{A}$ we have $|h^{(r)}\mathcal{A}| = 1$ if $h = rk$, and $|h^{(r)}\mathcal{A}| = 0$ if $h > rk$. Therefore, we assume that $1 \le h \le rk - 1$. This implies $1 \le m \le k-1$.

2.1. The case $\epsilon = 0$

Theorem 6. *Let n, k, h, m, and r be positive integers such that $k \le n$ and $h = mr$. For a fixed positive divisor d of n, let $\mathcal{A}_d(n,k)$ be the set defined in (1). Let v and w be the positive remainders of k and m modulo d, respectively. Then*

$$|h^{(r)}\mathcal{A}_d(n,k)| = \begin{cases} \min\{n, (h\lceil k/d\rceil - h + 1)d, hk - m^2r + 1\} & \text{if } m \le \min\{v, d-1\}; \\ \min\{n, hk - m^2r + 1 - \delta_d\} & \text{otherwise;} \end{cases} \tag{2}$$

where

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

Proof. Set

$$k = ud + v \text{ with } u = \left\lceil \frac{k}{d} \right\rceil - 1$$

and

$$m = qd + w \text{ with } q = \left\lceil \frac{m}{d} \right\rceil - 1,$$

where $u \geq 0$, $q \geq 0$, $1 \leq v \leq d$, and $1 \leq w \leq d$. Recall the set

$$\mathcal{A}_d = \mathcal{A}_d(n,k) = \bigcup_{i=0}^{u-1} (i + \mathcal{H}) \bigcup \left\{ u + j \cdot \frac{n}{d} : \ j = 0, 1, \ldots, v-1 \right\},$$

where $\mathcal{H} = \{0, n/d, \ldots, (d-1)(n/d)\}$.

Clearly, every element of $h^{(r)}\mathcal{A}_d$ is of the form

$$(i_1 + \cdots + i_h) + (j_1 + \cdots + j_h) \cdot \frac{n}{d},$$

where $i_1, \ldots, i_h \in \{0, 1, \ldots, u\}$ and $j_1, \ldots, j_h \in \{0, 1, \ldots, d-1\}$, with the added conditions

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

(ii) corresponding to one i-index we can have at most r same j-index.

The least value i_{min} of $i_1 + \cdots + i_h$ is

$$i_{min} = rd(0 + 1 + \cdots + (q-1)) + rqw = rq(m + w - d)/2.$$

To compute the largest value i_{max} of $i_1 + \cdots + i_h$ we consider the following four possible cases.

First, let $q = 0$ and $w > v$. Then $m = w > v$ and $1 \leq m - v \leq d - 1$. Thus,

$$i_{max} = ruv + r(m-v)(u-1) = r(mu - m + v).$$

Next, let $q = 0$ and $w \leq v$. Then $m = w \leq v$. Thus,

$$i_{max} = mru = r(mu - m + w).$$

Now, let $q \geq 1$ and $w > v$. By writing m as $m = v + dq + (w - v)$ we get

$$\begin{aligned} i_{max} &= ruv + r((u-1) + \cdots + (u-q))d + r(w-v)(u-q-1) \\ &= r(mu - m + qv - q(m + w - d)/2 + v). \end{aligned}$$

Finally, let $q \geq 1$ and $w \leq v$. Then $1 \leq d + w - v \leq d$. By writing m as $m = v + d(q-1) + (d + w - v)$ we get

$$\begin{aligned} i_{max} &= ruv + r((u-1) + \cdots + (u-q+1))d + r(d+w-v)(u-q) \\ &= r(mu - m + qv - q(m + w - d)/2 + w). \end{aligned}$$

All the above four cases can be written in the unified form

$$i_{max} = r(mu - m + qv - q(m + w - d)/2 + \min\{v, w\}).$$

Since $i = i_1 + \cdots + i_h$ can assume any integer value between i_{min} and i_{max}, the sumset $h^{(r)}\mathcal{A}_d$ lies exactly in $\min\{n/d, i_{max} - i_{min} + 1\}$ cosets of $\mathcal{H}$. This gives

$$|h^{(r)}\mathcal{A}_d| \le \min\{n, (i_{max} - i_{min} + 1)d\},$$

where

$$(i_{max} - i_{min} + 1)d = hk - m^2 r - r(v - w)w + rd \cdot \min\{0, v - w\} + d.$$

If $m = 1$, then $r = h$. Therefore,

$$h^{(r)}\mathcal{A}_d = h\mathcal{A}_d = \bigcup_{i=0}^{hu-1} (i + \mathcal{H}) \bigcup \left\{ hu + j \cdot \frac{n}{d} : \ j = 0, 1, \ldots, h(v-1) \right\}.$$

Hence,

$$\begin{aligned} |h^{(r)}\mathcal{A}_d| &= \min\{n, hud + \min\{d, hv - h + 1\}\} \\ &= \min\{n, (hu + 1)d, hk - h + 1\} \\ &= \min\{n, (h\lceil k/d \rceil - h + 1)d, hk - h + 1\}. \end{aligned}$$

This satisfies (2).

Now, assume that $2 \le m \le k - 1$. We compute $|h^{(r)}\mathcal{A}_d|$ in the following possible cases.

`Case 1.` Let $m \le v$ and $m < d$. This implies $i_{min} = 0$ and $i_{max} = mru = hu$. So, by Lemma 1, we have

$$\begin{aligned} h^{(r)}\mathcal{A}_d = &\bigcup_{i=0}^{hu-1} (i + \mathcal{H}) \\ &\bigcup \left\{ hu + j \cdot \frac{n}{d} : \ j = mr(m-1)/2, \ldots, mr(v-1) - mr(m-1)/2 \right\}. \end{aligned}$$

Hence,

$$\begin{aligned} |h^{(r)}\mathcal{A}_d| &= \min\{n, hud + \min\{d, mr(v-1) - mr(m-1) + 1\}\} \\ &= \min\{n, (hu + 1)d, hk - m^2 r + 1\} \\ &= \min\{n, (h\lceil k/d \rceil - h + 1)d, hk - m^2 r + 1\}. \end{aligned}$$

`Case 2.` Let $m = v = d$. Then $q = 0$ and $w = m = d$. This implies $i_{min} = 0$ and $i_{max} = mru = hu$. Since $m < k = ud + v = ud + m$, we have $u \ge 1$. Thus,

$$h^{(r)}\mathcal{A}_d = \left\{ \frac{mr(m-1)}{2} \cdot \frac{n}{d} \right\} \bigcup_{i=1}^{hu-1} (i + \mathcal{H}) \bigcup \left\{ hu + \frac{mr(m-1)}{2} \cdot \frac{n}{d} \right\}.$$

If $hu-1 \geq n/d$, then

$$|h^{(r)}\mathcal{A}_d| = n = \min\{n, hk - m^2r - m + 2\},$$

as

$$\begin{aligned} hk - m^2r - m + 2 &= mr(ud+v) - m^2r - m + 2 \\ &= mrud - m + 2 \\ &\geq d(n/d+1) - m + 2 \\ &= n + 2 \\ &> n. \end{aligned}$$

If $hu - 1 \leq n/d - 2$, then

$$|h^{(r)}\mathcal{A}_d| = (hu-1)d + 2 = hk - m^2r - m + 2 = \min\{n, hk - m^2r - m + 2\},$$

as $hk - m^2r - m + 2 = (hu-1)d + 2 \leq (n/d-2)d + 2 \leq n$.

Now, let $hu - 1 = n/d - 1$. Then

$$\begin{aligned} h^{(r)}\mathcal{A}_d &= \left\{ \frac{mr(m-1)}{2} \cdot \frac{n}{d} \right\} \bigcup_{i=1}^{hu-1} (i + \mathcal{H}) \bigcup \left\{ hu + \frac{mr(m-1)}{2} \cdot \frac{n}{d} \right\} \\ &= \bigcup_{i=1}^{n/d-1} (i + \mathcal{H}) \bigcup \left\{ j \cdot \frac{n}{d} : \ j = \frac{mr(m-1)}{2}, \frac{mr(m-1)}{2} + 1 \right\}. \end{aligned}$$

Therefore,

$$|h^{(r)}\mathcal{A}_d| = (n/d-1)d + 2 = (hu-1)d + 2 = hk - m^2r - m + 2.$$

Since $hk - m^2r - m + 2 = (n/d-1)d + 2 = n - (d-2)$ and $d = m \geq 2$, we get

$$|h^{(r)}\mathcal{A}_d| = hk - m^2r - m + 2 = \min\{n, hk - m^2r - m + 2\}.$$

`Case 3.` Let $m > v$, $w \neq d$, and $w \neq v$. So, by Lemma 1, we have

$$h^{(r)}\mathcal{A}_d = \bigcup_{i=i_{min}}^{i_{max}} (i + \mathcal{H}).$$

Hence,

$$\begin{aligned} |h^{(r)}\mathcal{A}_d| &= \min\{n, (i_{max} - i_{min} + 1)d\} \\ &= \min\{n, hk - m^2r - r(v-w)w + rd \cdot \min\{0, v-w\} + d\}. \end{aligned}$$

Case 4. Let $m > v$, $w = d$, and $w \neq v$. Then $m = (q+1)d$ and $k = ud + v$ with $1 \leq v < d$. So, by Lemma 1, we have

$$h^{(r)}\mathcal{A}_d = \{x_{min}\} \bigcup_{i=i_{min}+1}^{i_{max}} (i + \mathcal{H}),$$

where x_{min} is the sum of all elements of $\bigcup_{i=0}^{q}(i + \mathcal{H})$ with each element repeating exactly r-times. Hence,

$$|h^{(r)}\mathcal{A}_d| = \min\{n, (i_{max} - i_{min})d + 1\} = \min\{n, hk - m^2r + 1\}.$$

Case 5. Let $m > v$, $w \neq d$, and $w = v$. Then, Lemma 1 implies

$$h^{(r)}\mathcal{A}_d = \bigcup_{i=i_{min}}^{i_{max}-1} (i + \mathcal{H}) \bigcup \{x_{max}\},$$

where x_{max} is the sum of all elements of

$$\bigcup_{i=u-q}^{u-1} (i + \mathcal{H}) \bigcup \left\{ u + j \cdot \frac{n}{d} : j = 0, 1, \ldots, v - 1 \right\}$$

with each element repeating exactly r-times. Hence,

$$|h^{(r)}\mathcal{A}_d| = \min\{n, (i_{max} - i_{min})d + 1\} = \min\{n, hk - m^2r + 1\}.$$

Case 6. Let $m > v$ and $w = v = d$. So, by Lemma 1, we have

$$h^{(r)}\mathcal{A}_d = \{x_{min}\} \bigcup_{i=i_{min}+1}^{i_{max}-1} (i + \mathcal{H}) \bigcup \{x_{max}\},$$

where x_{min} and x_{max} are defined in Case 4 and Case 5, respectively.

Since $w = v = d$, we get $(i_{max} - i_{min} - 1)d = hk - m^2r - d$. We consider the following three subcases.

Subcase (i). Let $k > n/mr + m$. Then $i_{max} - i_{min} - 1 > n/d - 1$. Since it is an integer, we get $i_{max} - i_{min} - 1 \geq n/d$. Thus,

$$|h^{(r)}\mathcal{A}_d| = n = \min\{n, hk - m^2r - d + 2\},$$

as $hk - m^2r - d + 2 = (i_{max} - i_{min} - 1)d + 2 \geq (n/d)d + 2 = n + 2 > n$.

Subcase (ii). Let $k < n/mr + m$. Then $i_{max} - i_{min} - 1 < n/d - 1$, and thus at most $n/d - 2$. Therefore,

$$|h^{(r)}\mathcal{A}_d| = (i_{max} - i_{min} - 1)d + 2 = hk - m^2r - d + 2 = \min\{n, hk - m^2r - d + 2\},$$

as $hk - m^2r - d + 2 = (i_{max} - i_{min} - 1)d + 2 \leq (n/d - 2)d + 2 = n - 2d + 2 \leq n$.

Subcase (iii). Let $k = n/mr + m$. Then $i_{max} - i_{min} = n/d$. So,

$$h^{(r)}\mathcal{A}_d = \{x_{min}\} \bigcup_{i=i_{min}+1}^{i_{max}-1} (i + \mathcal{H}) \bigcup \{x_{max}\}$$
$$= \bigcup_{i=i_{min}+1}^{i_{min}+n/d-1} (i + \mathcal{H}) \bigcup \{x_{min}, x_{max}\}.$$

From the definition, we have

$$x_{min} = \frac{rdq(q+1)}{2} + \frac{rd(d-1)(q+1)}{2} \cdot \frac{n}{d}$$

and

$$x_{max} = rud(q+1) - \frac{rdq(q+1)}{2} + \frac{rd(d-1)(q+1)}{2} \cdot \frac{n}{d}.$$

But,

$$ud = k - d = \frac{n}{mr} + m - d = \frac{n}{rd(q+1)} + dq.$$

This implies

$$x_{max} = \frac{rdq(q+1)}{2} + \left(\frac{rd(d-1)(q+1)}{2} + 1 \right) \cdot \frac{n}{d}.$$

We note that $x_{min} = x_{max}$ if and only if $d = 1$. Thus, if $d = 1$, then

$$|h^{(r)}\mathcal{A}_d| = \left(\frac{n}{d} - 1 \right) d + 1 = n = \min\{n, hk - m^2r - d + 2\},$$

as $hk - m^2r - d + 2 = n - d + 2 = n + 1 > n$. If $d \geq 2$, then

$$|h^{(r)}\mathcal{A}_d| = \left(\frac{n}{d} - 1 \right) d + 2 = n - d + 2 = \min\{n, hk - m^2r - d + 2\},$$

as $hk - m^2r - d + 2 = n - d + 2 \leq n$.

This completes the Case 6, and also completes the proof of the theorem. □

Remark 1. As a particular case of Theorem 6, for $r = 1$, we obtain Theorem 4.

Remark 2. When $n = p$ is a prime number, Theorem 6 gives

$$|h^{(r)}\mathcal{A}| \leq \min\{p, hk - m^2r + 1\}.$$

This upper bound is exactly the same as the lower bound obtained in Theorem 5, in the case $\epsilon = 0$.

2.2. The Case $\epsilon \geq 1$

Theorem 7. *Let n, k, h, m, and r be positive integers such that $k \leq n$ and $h = mr + \epsilon$ with $1 \leq \epsilon < r$. For a fixed positive divisor d of n, let $\mathcal{A}_d(n,k)$ be the set defined in (1). Let v and w be the positive remainders of k and m modulo d, respectively. Then*

$$|h^{(r)}\mathcal{A}_d(n,k)| = \begin{cases} \min\{n, (h\lceil k/d\rceil - h + 1)d, hk - m^2r + 1 - (2m+1)\epsilon\} & \text{if } m < v \leq d; \\ \min\{n, (h\lceil k/d\rceil - h + 1)d - \epsilon d\} & \text{if } m = v < d; \\ \min\{n, hk - m^2r + 1 - (2m+1)\epsilon - (m-1)(\epsilon - 1)\} & \text{if } m = v = d; \\ \min\{n, hk - m^2r + 1 - (2m+1)\epsilon - \delta_d\} & \text{if } m > v; \end{cases}$$

where

$$\delta_d = \begin{cases} r(v-w)w - (d-1) + (v - 2w - 1)\epsilon & \text{if } w < v \leq d, \\ r(d-w)(w-v) - (d-1) + (v - 2w + d - 1)\epsilon & \text{if } v < w < d, \\ -(d-1) + (v - 2w + d - 1)\epsilon & \text{if } v = w < d, \\ -(d-1) + (v - 2w + 2d - 1)\epsilon & \text{if } w = d. \end{cases}$$

Proof. Recall the notations

$$h = mr + \epsilon \text{ with } m = \left\lfloor \frac{h}{r} \right\rfloor,$$

$$k = ud + v \text{ with } u = \left\lceil \frac{k}{d} \right\rceil - 1,$$

and

$$m = qd + w \text{ with } q = \left\lceil \frac{m}{d} \right\rceil - 1,$$

where $m \geq 1$, $u \geq 0$, $q \geq 0$, $1 \leq \epsilon < r$, $1 \leq v \leq d$, and $1 \leq w \leq d$. Recall also that the set

$$\mathcal{A}_d = \mathcal{A}_d(n,k) = \bigcup_{i=0}^{u-1} (i + \mathcal{H}) \bigcup \left\{ u + j \cdot \frac{n}{d} : \ j = 0, 1, \ldots, v-1 \right\},$$

where $\mathcal{H} = \{0, n/d, \ldots, (d-1)(n/d)\}$.

Similar to the proof of Theorem 6, every element of $h^{(r)}\mathcal{A}_d$ is of the form

$$(i_1 + \cdots + i_h) + (j_1 + \cdots + j_h) \cdot \frac{n}{d},$$

where $i_1, \ldots, i_h \in \{0, 1, \ldots, u\}$ and $j_1, \ldots, j_h \in \{0, 1, \ldots, d-1\}$, with the added conditions

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

(ii) corresponding to one i-index we can have at most r same j-index.

We compute the least value i_{min} of $i_1 + \cdots + i_h$ in the following possible cases.

First, let $w < v$. Then $h = mr + \epsilon = rdq + rw + \epsilon$. Since $\epsilon < r \leq r(v - w)$, we get $rw + \epsilon < rv$. Therefore,

$$\begin{aligned} i_{min} &= rd(0 + 1 + \cdots + (q-1)) + (rw + \epsilon)q \\ &= rq((q-1)d + 2w)/2 + \epsilon q \\ &= rq(qd + w + w - d)/2 + \epsilon q \\ &= rq(m + w - d)/2 + \epsilon q. \end{aligned}$$

Next, let $w = v$. Then $h = mr + \epsilon = rdq + rw + \epsilon = rdq + rv + \epsilon$. If $v = d$, then

$$\begin{aligned} i_{min} &= rd(0 + 1 + \cdots + q) + \epsilon(q+1) \\ &= rq(q+1)d/2 + \epsilon(q+1) \\ &= rqm/2 + \epsilon(q+1) \\ &= rq(m + w - d)/2 + \epsilon(q+1). \end{aligned}$$

If $v < d$, then $rv + \epsilon < rv + r = r(v+1) \leq rd$. Therefore,

$$\begin{aligned} i_{min} &= rd(0 + 1 + \cdots + (q-1)) + (rv + \epsilon)q \\ &= rq((q-1)d + 2v)/2 + \epsilon q \\ &= rq(qd + v + v - d)/2 + \epsilon q \\ &= rq(m + v - d)/2 + \epsilon q \\ &= rq(m + w - d)/2 + \epsilon q. \end{aligned}$$

Finally, let $w > v$. If $w = d$, then

$$i_{min} = rd(0 + 1 + \cdots + q) + \epsilon(q+1) = rq(m + w - d)/2 + \epsilon(q+1).$$

If $w < d$, then $rw + \epsilon < r(d-1) + r = rd$. Therefore,

$$i_{min} = rd(0 + 1 + \cdots + (q-1)) + (rw + \epsilon)q = rq(m + w - d)/2 + \epsilon q.$$

The above three cases of i_{min} can be written in the unified form

$$i_{min} = \begin{cases} rq(m + w - d)/2 + \epsilon q & \text{if } w < d, \\ rq(m + w - d)/2 + \epsilon(q+1) & \text{if } w = d. \end{cases}$$

Now, we compute the largest value i_{max} of $i_1 + \cdots + i_h$ in the following possible cases.

First, let $q = 0$ and $w > v$. Then $m = w > v$ and $1 \leq m - v \leq d - 1$. Therefore,

$$h = mr + \epsilon = rw + \epsilon = rv + r(w - v) + \epsilon$$

with

$$r(w-v)+\epsilon < r(m-v)+r \le r(d-1)+r = rd.$$

Hence,

$$i_{max} = ruv + (r(w-v)+\epsilon)(u-1) = r(mu-m+v)+\epsilon(u-1).$$

Next, let $q=0$ and $w=v$. Then $m=w=v$ and $h=mr+\epsilon=rv+\epsilon$. Therefore,

$$i_{max} = ruv + \epsilon(u-1) = r(mu-m+v)+\epsilon(u-1).$$

Now, let $q=0$ and $w<v$. Then $m=w<v$ and $h=mr+\epsilon<(v-1)r+r=vr$. Thus,

$$i_{max} = (mr+\epsilon)u = r(mu-m+w)+\epsilon u.$$

Next, let $q\ge 1$ and $w>v$. Then $w-v+1\le d$. By writing m as $m=dq+w=v+dq+(w-v)$ we get $h=vr+dqr+(w-v)r+\epsilon$, with $(w-v)r+\epsilon<(w-v+1)r\le rd$. Thus,

$$\begin{aligned} i_{max} &= ruv + rd((u-1)+\cdots+(u-q)) + ((w-v)r+\epsilon)(u-q-1) \\ &= r(mu-m+vq-q(m+w-d)/2+v)+\epsilon(u-q-1). \end{aligned}$$

Next, let $q\ge 1$ and $w=v$. Then $m=dq+v$ and $h=vr+dqr+\epsilon$. Therefore,

$$\begin{aligned} i_{max} &= ruv + rd((u-1)+\cdots+(u-q)) + \epsilon(u-q-1) \\ &= r(mu-m+vq-q(m+w-d)/2+v)+\epsilon(u-q-1). \end{aligned}$$

Finally, let $q\ge 1$ and $w<v$. Then $1\le d+w-v\le d-1$. By writing m as $m=v+d(q-1)+(d+w-v)$ we get $h=vr+(q-1)dr+(d+w-v)r+\epsilon$, with $(d+w-v)r+\epsilon<(d-1)r+r=rd$. Thus,

$$\begin{aligned} i_{max} &= ruv + rd((u-1)+\cdots+(u-q+1)) + ((d+w-v)r+\epsilon)(u-q) \\ &= r(mu-m+vq-q(m+w-d)/2+w)+\epsilon(u-q). \end{aligned}$$

All the above six possible values of i_{max} can be written in the unified form

$$i_{max} = \begin{cases} r(mu-m+vq-q(m+w-d)/2+w)+\epsilon(u-q) & \text{if } w<v, \\ r(mu-m+vq-q(m+w-d)/2+v)+\epsilon(u-q-1) & \text{if } w\ge v. \end{cases}$$

Since $i=i_1+\cdots+i_h$ can assume any integer value between i_{min} and i_{max}, the sumset $h^{(r)}\mathcal{A}_d$ lies exactly in $\min\{n/d, i_{max}-i_{min}+1\}$ cosets of $\mathcal{H}$. This implies

$$|h^{(r)}\mathcal{A}_d| \le \min\{n, (i_{max}-i_{min}+1)d\}.$$

Note that, if $w = d$, then

$$\begin{aligned}
&(i_{max} - i_{min} + 1)d \\
&= \left(mru - mr + rvq - \frac{mrq}{2} + rv + \epsilon(u - q - 1) - \frac{mrq}{2} - \epsilon(q + 1) + 1\right) d \\
&= mrud - mr(q + 1)d + rv(q + 1)d + \epsilon ud - \epsilon(2q + 2)d + d \\
&= (mr + \epsilon)ud - m^2 r + mrv + d - \epsilon(2q + 2)d \\
&= (mr + \epsilon)(ud + v) - m^2 r - \epsilon v + d - \epsilon(2q + 2)d \\
&= hk - m^2 r + d - \epsilon((2q + 2)d + v).
\end{aligned}$$

If $w < d$, then

$$\begin{aligned}
&(i_{max} - i_{min} + 1)d \\
&= \begin{cases} hk - m^2 r - r(v - w)w + d - \epsilon(2qd + v) & \text{if } w < v, \\ hk - m^2 r - r(w - v)(d - w) + d - \epsilon((2q + 1)d + v) & \text{if } w \geq v. \end{cases}
\end{aligned}$$

Now we are ready to compute $|h^{(r)}\mathcal{A}_d|$.

`Case 1:` Let $m = v < d$. Then $q = 0$ and $m = w = v < d$. This implies $i_{min} = 0$ and $i_{max} = ruv + \epsilon(u - 1) = mru + \epsilon(u - 1) = hu - \epsilon$. So, by Lemma 1, we have

$$h^{(r)}\mathcal{A}_d = \bigcup_{i=0}^{hu-\epsilon} (i + \mathcal{H}).$$

Hence,

$$\begin{aligned}
|h^{(r)}\mathcal{A}_d| &= \min\{n, (hu - \epsilon + 1)d\} \\
&= \min\{n, (hu + 1)d - \epsilon d\} \\
&= \min\{n, (h\lceil k/d\rceil - h + 1)d - \epsilon d\}.
\end{aligned}$$

`Case 2:` Let $m < v \leq d$. Then $q = 0$ and $m = w$. This implies $i_{min} = 0$ and $i_{max} = (mr + \epsilon)u = hu$. So, by Lemma 1, we have

$$\begin{aligned}
h^{(r)}\mathcal{A}_d = &\bigcup_{i=0}^{hu-1} (i + \mathcal{H}) \bigcup \\
&\left\{hu + j \cdot \frac{n}{d} : \ j = \frac{mr(m-1)}{2} + \epsilon m, \ldots, mr(v-1) - \frac{mr(m-1)}{2} + \epsilon(v - m - 1)\right\}.
\end{aligned}$$

Hence,

$$\begin{aligned}
|h^{(r)}\mathcal{A}_d| &= \min\{n, hud + \min\{d, mr(v - m) + (v - 2m - 1)\epsilon + 1\}\} \\
&= \min\{n, (hu + 1)d, hk - m^2 r - (2m + 1)\epsilon + 1\} \\
&= \min\{n, (h\lceil k/d\rceil - h + 1)d, hk - m^2 r + 1 - (2m + 1)\epsilon\}.
\end{aligned}$$

Case 3: Let $m = v = d$. Then $q = 0$ and $w = m = v = d$. This implies $i_{min} = \epsilon$ and $i_{max} = mru + \epsilon(u-1) = hu - \epsilon$. So, by Lemma 1, we have

$$h^{(r)}\mathcal{A}_d = \bigcup_{i=\epsilon}^{hu-\epsilon} (i + \mathcal{H}).$$

If $hu - 2\epsilon + 1 \geq n/d$, then

$$\begin{aligned} |h^{(r)}\mathcal{A}_d| &= n \\ &= \min\{n, hk - m^2r + (1-3\epsilon)m\} \\ &= \min\{n, hk - m^2r + 1 - (2m+1)\epsilon - (m-1)(\epsilon-1)\}, \end{aligned}$$

as

$$\begin{aligned} hk - m^2r + (1-3\epsilon)m &= (mr+\epsilon)(ud+v) - m^2r + (1-3\epsilon)m \\ &= mrud + \epsilon ud + (1-2\epsilon)m \\ &= mrud + \epsilon ud + (1-2\epsilon)d \\ &= (hu - 2\epsilon + 1)d \\ &\geq n. \end{aligned}$$

If $hu - 2\epsilon + 1 \leq n/d - 1$, then

$$\begin{aligned} |h^{(r)}\mathcal{A}_d| &= (hu - 2\epsilon + 1)d \\ &= hk - m^2r + (1-3\epsilon)m \\ &= hk - m^2r + 1 - (2m+1)\epsilon - (m-1)(\epsilon-1) \\ &= \min\{n, hk - m^2r + 1 - (2m+1)\epsilon - (m-1)(\epsilon-1)\}, \end{aligned}$$

as

$$\begin{aligned} hk - m^2r + 1 - (2m+1)\epsilon - (m-1)(\epsilon-1) &= (hu - 2\epsilon + 1)d \\ &\leq (n/d - 1)d \\ &= n - d \\ &< n. \end{aligned}$$

Case 4: Let $m > v$, $w \neq d$, and $w \neq v$. Then, Lemma 1 implies

$$h^{(r)}\mathcal{A}_d = \bigcup_{i=i_{min}}^{i_{max}} (i + \mathcal{H}).$$

Hence,

$$
\begin{aligned}
&|h^{(r)}\mathcal{A}_d| \\
&= \min\{n, (i_{max} - i_{min} + 1)d\} \\
&= \begin{cases} \min\{n, hk - m^2r - r(v-w)w + d - \epsilon(2qd + v)\} & \text{if } w < v, \\ \min\{n, hk - m^2r - r(w-v)(d-w) + d - \epsilon((2q+1)d + v) & \text{if } w > v. \end{cases} \\
&= \begin{cases} \min\{n, hk - m^2r - (2m+1)\epsilon - r(v-w)w + d - (v - 2w - 1)\epsilon\} & \text{if } w < v, \\ \min\{n, hk - m^2r - (2m+1)\epsilon - r(v-w)(w-d) + d - (v - 2w + d - 1)\epsilon & \text{if } w > v. \end{cases}
\end{aligned}
$$

`Case 5:` Let $m > v$, $w = d$, and $w \neq v$. Then $h = (q+1)d + \epsilon$ and $k = ud + v$ with $1 \leq v < d$. So, by Lemma 1, we have

$$h^{(r)}\mathcal{A}_d = \bigcup_{i=i_{min}}^{i_{max}} (i + \mathcal{H}).$$

Hence,

$$
\begin{aligned}
|h^{(r)}\mathcal{A}_d| &= \min\{n, (i_{max} - i_{min} + 1)d\} \\
&= \min\{n, hk - m^2r + d - \epsilon((2q+2)d + v)\} \\
&= \min\{n, hk - m^2r - (2m+1)\epsilon + d - (v - 2w + 2d - 1)\epsilon\}.
\end{aligned}
$$

`Case 6:` Let $m > v$, $w \neq d$, and $w = v$. Then, Lemma 1 implies

$$h^{(r)}\mathcal{A}_d = \bigcup_{i=i_{min}}^{i_{max}} (i + \mathcal{H}).$$

Hence,

$$
\begin{aligned}
|h^{(r)}\mathcal{A}_d| &= \min\{n, (i_{max} - i_{min} + 1)d\} \\
&= \min\{n, hk - m^2r + d - \epsilon((2q+1)d + v)\} \\
&= \min\{n, hk - m^2r - (2m+1)\epsilon + d - (v - 2w + d - 1)\epsilon\}.
\end{aligned}
$$

`Case 7:` Let $m > v$ and $w = v = d$. By Lemma 1, we have

$$h^{(r)}\mathcal{A}_d = \bigcup_{i=i_{min}}^{i_{max}} (i + \mathcal{H}).$$

Hence,

$$
\begin{aligned}
|h^{(r)}\mathcal{A}_d| &= \min\{n, (i_{max} - i_{min} + 1)d\} \\
&= \min\{n, hk - m^2r + d - \epsilon((2q+2)d + v)\} \\
&= \min\{n, hk - m^2r - (2m+1)\epsilon + d - (v - 2w + 2d - 1)\epsilon\}.
\end{aligned}
$$

This completes the proof of the theorem. □

As an analogue of the function $\phi(n,k,h)$ and $\phi^{\wedge}(n,k,h)$, let us define the function

$$\phi^{(r)}(n,k,h) := \min\{|h^{(r)}\mathcal{A}_d(n,k)| : \ d \in D(n)\}.$$

So, by Theorem 6 and Theorem 7, we have

$$\mu^{(r)}(\mathbb{Z}_n,k,h) \leq \phi^{(r)}(n,k,h).$$

Acknowledgement. The author would like to thank the anonymous referee for his/her valuable and constructive comments, that helped the author to present the paper in a better form.

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] A. L. Cauchy, Recherches sur les nombres, *J. École Polytech.* **9** (1813), 99-116.

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

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

[7] J. A. Dias da Silva and Y. O. Hamidoune, Cyclic space for Grassmann derivatives and additive theory, *Bull. Lond. Math. Soc.* **26** (1994), 140-146.

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

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

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

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

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

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