The h-critical number and sumsets of nonbases of maximum size

Wout Jakob van der Meer

supervised by

Dr. Marta Pieropan

A thesis presented for the degree of

Bachelor in Mathematics

Department of Mathematics
Utrecht University
17-06-2024

Contents

Introduction

Let G be a finite abelian group of order $n \geq 2$. For any $h \geq 1$, and nonempty subsets $A_1, ..., A_h$ of G, the Minkowsi sum is defined as

$$A_1 + ... + A_h = \{a_1 + ... + a_h : a_1 \in A_1, ..., a_h \in A_h\}.$$

We write hA for the Minkowsi sum whenever $A_1 = A_2 = ... = A_h = A$.

A subset $A \subseteq G$ is called a basis of order h, or h-complete if $hA = G$. If $hA \neq G$ we say that A is a nonbasis of order h, or h-incomplete. As an example, let $G = \mathbb{Z}_3 \times \mathbb{Z}_6$ and $A = \{(0,0),(0,4)\}$. We find that

$$2A = \{(0,0),(0,4),(0,2)\} \neq G,$$

and therefore A is 2-incomplete. Note that $2A$ in this case is the subgroup $\{0\} \times \langle 2 \rangle$, where $\langle 2 \rangle$ is the subgroup of $\mathbb{Z}_6$ generated by 2. Since subgroups are closed under the operation of G, we find that $hA = 2A \neq G$ for every $h \geq 2$. So A is in this case h-incomplete for every $h \geq 1$.

The h-critical number $\chi(G,h)$ is defined as the smallest positive integer m such that all subsets $A \subseteq G$ such that $|A| \geq m$ are a basis of order h. In this bachelor thesis we provide the h-critical number for every h. We also discuss the possible sizes of hA when A is a nonbasis of order h of maximum size, so we look at $|hA|$ whenever $|A| = \chi(G,h) - 1$. We give a complete answer for $h = 2$ and $h = 3$.

This thesis is based on the work of B. Bajnok and P. P. Pach [1, 2]. We start off with several helpful results that will be used throughout the thesis. In the following section we determine $\chi(G,h)$ for each h, and after that we provide the size of sumsets of nonbases of maximum size for $h = 2$ and $h = 3$ respectively.

1. Preliminary results

In this section we provide several helpful results that will be useful later. We start off with a formal definition for the h-critical number.

Definition. For each finite abelian group G and $h \geq 1$, the h-critical number is defined as

$$\chi(G,h) = \min\{m \geq 1 : A \subseteq G, |A| \geq m \implies hA = G\}.$$

Note that for all h, we have $hG = G$, so $1 \leq \chi(G,h) \leq n$. Therefore $\chi(G,h)$ is well defined.

Definition. Let G be a finite abelian group, and let $\chi(G,h)$ be the h-critical number. Then

$$S(G,h) = \{|hA| : A \subset G, |A| = \chi(G,h) - 1, hA \neq G\}$$

is the set of sizes of sumsets of nonbases of maximum size.

Recall that for any subset A of G, the stabilizer subgroup H of A is defined as

$$H = \{g \in G : g + A = A\}.$$

Our next theorem is a result that follows from a paper published in 1953 by Martin Kneser [5]. It concerns the size of sumsets in relation to the stabilizer subgroup of the sumset. Additonally, another proof can be found in a paper by Matt DeVos [3].

Theorem 1.1 [5]. Let G be a finite abelian group. Let A, B be nonempty subsets of G, and let H be the stabilizer subgroup of $A + B$. Then

$$|A + B| \geq |A + H| + |B + H| - |H|.$$

Our next result is a corrolary which follows directly from Theorem 1.1.

Corollary 1.2. Let G be a finite abelian group. For $h \geq 1$, let $A_1, ..., A_h$ be nonempty subsets of G, and let H be the stabilizer subgroup of $A_1 + ... + A_h$. Then

$$|A_1 + ... + A_h| \geq |A_1| + ... + |A_h| - (h-1)|H|.$$

Proof. Note that since H is a group, it contains the identity element. Therefore, $|A_i + H| \geq |A_i|$ for all $1 \leq i \leq h$. We use induction on h. Let $h = 1$. Then

$$|A_1| \geq |A_1| - (1-1)|H| = |A_1|.$$

Now assume that the claim holds for some $h = k$. Let H be the stabilizer subgroup of $A_1 + ... + A_k + A_{k+1}$. Using Theorem 1.1 we conclude that

$$|A_1 + ... + A_k + A_{k+1}| \geq |A_1 + ... + A_k + H| + |A_{k+1} + H| - |H| \geq |A_1 + ... + A_k| + |A_{k+1}|$$
$$-|H| \geq |A_1| + ... + |A_k| - (k-1)|H| + |A_{k+1}| - |H| = |A_1| + ... + |A_{k+1}| - (k+1-1)|H|.$$

So for all $h \geq 1$ we have

$$|A_1 + ... + A_h| \geq |A_1| + ... + |A_h| - (h-1)|H|.$$

This completes our proof. □

Our next result is a simple application of Corollary 1.2.

Lemma 1.3. Let G be a finite abelian group, $h \geq 1$ and A a nonbasis of order h of maximum size, i.e. $|A| = \chi(G,h) - 1$. Let H be the stabilizer of hA. Then A and hA are unions of cosets of H. If A and hA consist respectively of k_1 and k_2 distinct cosets of H, we have

$$k_2 \geq hk_1 - h + 1.$$

Proof. We look at the set $A + H$. Since A is h-incomplete we have

$$h(A + H) = hA + H = hA \neq G.$$

Therefore $A + H$ is h-incomplete. Since A is h-incomplete of maximum size, we have $|A + H| \leq |A|$. However, H is a subgroup and contains the identity element, so $A \subseteq A + H$. Therefore

$$A = A + H = \bigcup_{a \in A} (a + H).$$

So A is a union of cosets of H. Similarly we see that hA is a union of cosets of H.

Let $|A| = k_1|H|$ and $|hA| = k_2|H|$. With Corollary 1.2 we find that

$$k_2|H| = |hA| \geq h|A| - (h-1)|H| = hk_1|H| - (h-1)|H|.$$

So $k_2 \geq hk_1 - h + 1$. □

Lemma 1.4. Let G be a finite abelian group and $h \geq 1$. Suppose that H is a subgroup of G of index d for some $d \geq 1$ and suppose that $\phi : G \to G/H$ is the canonical map. Let B be a subset of G/H, and let $A = \phi^{-1}(B)$. Then $|A| = \frac{n}{d} \cdot |B|$ and $|hA| = \frac{n}{d} \cdot |hB|$.

Proof. Let $g + H \in G/H$, and let $A_1 = \phi^{-1}(\{g + H\})$. Then A_1 is a subset of G, specifically it is a full coset of H, and therefore $|A_1| = \frac{n}{d}$.

We write $B = \{b_1, .., b_r\} \subseteq G/H$. Then $|\phi^{-1}(\{b_i\})| = \frac{n}{d}$ for all $1 \leq i \leq r$. Since

$$A = \bigcup_{1 \leq i \leq r} \phi^{-1}(\{b_i\}),$$

and all of those sets are pairwise disjoint, it follows that $|A| = \frac{n}{d} \cdot |B|$.

We will now show that $hA = \phi^{-1}(hB)$. We take an arbitrary $a_1 + ... + a_h \in hA$. Then

$$a_1 + ... + a_h \in \phi^{-1}(\{a_1 + ... + a_h + H\}) = \phi^{-1}(\{a_1 + H + ... + a_h + H\}) \subseteq \phi^{-1}(hB).$$

So $hA \subseteq \phi^{-1}(hB)$.

We take an arbitrary $b \in \phi^{-1}(hB)$. Then $b + H \in hB$, and therefore, $b + H = (b_1 + H) + ... + (b_h + H)$, where $b_1, ..., b_h \in A$. So $b = b_1 + ... + b_h \in hA$. So $\phi^{-1}(hB) \subseteq hA$. So $hA = \phi^{-1}(hB)$.

We write $hB = \{b_1, .., b_r\}$. Then $|\phi^{-1}(\{b_i\})| = \frac{n}{d}$ for all $1 \leq i \leq r$. Since

$$hA = \bigcup_{1 \leq i \leq r} \phi^{-1}(\{b_i\}),$$

and all of those sets are disjoint, it follows that therefore $|hA| = \frac{n}{d} \cdot |hB|$. □

We will now briefly discuss the fundamental theorem of finite abelian groups [4, p. 158-166]. This theorem states that every finite abelian group G is isomorphic to a direct product of finite cyclic groups. We write $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Then G has a unique type $(n_1, ..., n_r)$, where $r, n_1, .., n_r \in \mathbb{N}$ such that $n_1 \geq 2$ and $n_i | n_{i+1}$ for all $1 \leq i \leq r-1$, and

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}.$$

We say that r is the rank of G, and n_r the exponent of G. With this construction, G has a natural ordering, which we will define using the following lemma.

Lemma 1.5. Let $S = \{x \in \mathbb{Z} : 0 \leq x \leq n-1\}$. Then the function $\phi : G \to S$ given by

$$\phi((q_1, ..., q_r)) = \sum_{i=1}^{r} q_i n_{i+1} \cdots n_r$$

is a bijection.

Proof. We first show that ϕ is injective. Let $(a_1, ..., a_r), (b_1, ..., b_r) \in G$. Assume that $\phi((a_1, ..., a_r)) = \phi((b_1, ..., b_r))$, so

$$a_r + n_r \sum_{i=1}^{r-1} a_i n_{i+1} \cdots n_{r-1} = b_r + n_r \sum_{i=1}^{r-1} b_i n_{i+1} \cdots n_{r-1}.$$

Note that $a_r \leq n_r - 1$. We first look at the case where $n_r \sum_{i=1}^{r-1} a_i n_{i+1} \cdots n_{r-1} = 0$. Then it must be true that

$$n_r \sum_{i=1}^{r-1} b_i n_{i+1} \cdots n_{r-1} = 0,$$

since otherwise $\phi((b_1, ..., b_r)) \geq n_r > a_r = \phi((a_1, ..., a_r))$. So $a_r = b_r$, and $a_i = b_i = 0$ for all $i \geq 2$. So $(a_1, ..., a_r) = (b_1, ..., b_r)$.

Now assume that $n_r \sum_{i=1}^{r-1} a_i n_{i+1} \cdots n_{r-1} \geq n_r$ and that $a_r \neq b_r$. Then

$$a_r - b_r = n_r \left(\sum_{i=1}^{r-1} (a_i n_{i+1} \cdots n_{r-1} - b_i n_{i+1} \cdots n_{r-1}) \right).$$

However $-(n_r - 1) \leq a_r - b_r \leq n_r - 1$, and $a_r - b_r \neq 0$, so $n_r \nmid (a_r - b_r)$, so this is a contradiction. Therefore $a_r = b_r$. Now we have

$$a_{r-1} + n_{r-1} \sum_{i=1}^{r-2} a_i n_{i+1} \cdots n_{r-2} = b_{r-1} + n_{r-1} \sum_{i=1}^{r-2} b_i n_{i+1} \cdots n_{r-2},$$

and we can do the same thing to show that $a_{r-1} = b_{r-1}$. By induction it now follows that whenever $a_k = b_k$ for some $2 \leq k \leq r$, we have $a_{k-1} = b_{k-1}$. So $(a_1, ..., a_r) = (b_1, ..., b_r)$. So ϕ is injective.

We prove that ϕ is surjective by induction. First let $0 = m \in S$. We simply take $(0, ..., 0) \in G$

and it follows that $\phi((0,...,0)) = 0$. First note that

$$n-1 = n_1 \cdots n_r - 1 = n_1 \cdots n_r + (n_2 \cdots n_r - n_2 \cdots n_r) + ... + (n_r - n_r) - 1 = \sum_{i=1}^{r} (n_i - 1) n_{i+1} \cdots n_r.$$

So $\phi^{-1}(n-1) = (n_1 - 1, ..., n_r - 1)$. Now assume that for some $k \in S \setminus \{n-1\}$, there exists an element $(q_1, ..., q_r) \in G$ such that $k = \phi((q_1, ..., q_r))$. Since $k < n - 1$, there exists an $1 \leq j \leq r$ such that $q_j < n_j - 1$ and $q_i = n_i - 1$ for all $j \leq i \leq r$. So

$$k = \sum_{i=1}^{j} q_i n_{i+1} \cdots n_r + \sum_{i=j+1}^{r} (n_i - 1) n_{i+1} \cdots n_r.$$

Note that

$$\sum_{i=j+1}^{r} (n_i - 1) n_{i+1} \cdots n_r = \\ n_{j+1} \cdots n_r + (n_{j+2} \cdots n_r - n_{j+2} \cdots n_r) + ... + (n_r - n_r) - 1 = n_{j+1} n_{j+2} \cdots n_r - 1.$$

Therefore we find that

$$k+1 = \left(\sum_{i=1}^{j} q_i n_{i+1} \cdots n_r \right) + n_{j+1} n_{j+2} \cdots n_r = \left(\sum_{i=1}^{j-1} q_i n_{i+1} \cdots n_r \right) + (q_j + 1) n_{j+1} n_{j+2} \cdots n_r.$$

It follows that $k + 1 = \phi((q_1, ..., q_{j-1}, q_j + 1, 0, ..., 0))$. So ϕ is surjective, and therefore bijective. □

Now let $0 \leq m \leq n - 1$. Since ϕ is bijective, there exists an unique element $(q_1, ..., q_r)$ of G such that $\phi((q_1, ..., q_r)) = m$. We now introduce the ordering. Let $(a_1, ..., a_r), (b_1, ..., b_r) \in G$. Then $(a_1, ..., a_r) \leq (b_1, ..., b_r)$ if and only if

$$\phi((a_1, ..., a_r)) \leq \phi((b_1, ..., b_r)).$$

Note that with this ordering $(0, ..., 0)$ is the smallest element of G, while $(n_1 - 1, ..., n_r - 1)$ is the largest. If we assume that $q_r \geq 1$, the set of the first m elements of G is the set that ranges from the zero element to the element $(q_1, ..., q_{r-1}, q_r - 1)$. It can be formally defined as

$$\mathcal{I}(G, m) = \{g \in G : (0, ..., 0) \leq g \leq (q_1, ..., q_{r-1}, q_r - 1)\}.$$

We also introduce a variation of $\mathcal{I}(G, m)$, where the last element is replaced by the next one in the order. If we assume that $q_r \geq 3$, this set is given by:

$$\mathcal{I}^*(G, m) = \mathcal{I}(G, m - 1) \cup \{(q_1, ..., q_{r-1}, q_r)\}.$$

By considering these sets, we can straightforwardly determine the h-fold sumset of them, as long as $hq_i < n_i$ for all $1 \leq i \leq r$.

Proposition 1.6. Let G be a finite abelian group of type $(n_1, ..., n_r)$. Let $0 \leq m \leq n - 1$, with unique integers $q_1, ..., q_r$, $0 \leq q_i \leq n_i - 1$, such that

$$m = \sum_{i=1}^{r} q_i n_{i+1} \cdots n_r.$$

Furthermore, let $h \geq 1$ such that $hq_i < n_i$ for all $1 \leq i \leq r$. Then

(1) If $q_r \geq 1$, then $|h\mathcal{I}(G,m)| = hm - h + 1$.

(2) If $q_r \geq 3$, then $|h\mathcal{I}^*(G,m)| = hm$.

Proof. Let $q_r \geq 1$, then $\mathcal{I}(G,m)$ is the set of elements from zero to the element $(q_1, ..., q_{r-1}, q_r - 1)$. Since $hq_i < n_i$ for all $1 \leq i \leq r$, it follows by induction that $h\mathcal{I}(G,m)$ is the set of elements from zero to the element $(hq_1, ..., hq_{r-1}, hq_r - h)$. Therefore, $h\mathcal{I}(G,m) = \mathcal{I}(G, hm - h + 1)$, and $|h\mathcal{I}(G,m)| = hm - h + 1$.

Let $q_r \geq 3$, then

$$\mathcal{I}^*(G,m) = \mathcal{I}(G, m-1) \cup (q_1, ..., q_{r-1}, q_r).$$

We deduce quickly that $h\{(q_1, ..., q_{r-1}, q_r)\} = \{(hq_1, ..., hq_{r-1}, hq_r)\} \subseteq h\mathcal{I}^*(G,m)$. We also find that

$$h\mathcal{I}(G, m-1) = \mathcal{I}(G, hm - 2h + 1) \subseteq h\mathcal{I}^*(G,m).$$

Note that $\mathcal{I}(G, hm-2h+1)$ is the set of elements from zero to $(hq_1, ..., hq_{r-1}, hq_r - 2h)$. We will use induction to show that for all $hq_r - 2h + 1 \leq q \leq hq_r - 2$, we have $(hq_1, ..., hq_{r-1}, q) \in h\mathcal{I}^*(G,m)$.

We take an arbitrary $0 \leq k \leq 2h - 3$. Assume that $(hq_1, ..., hq_{r-1}, hq_r - 2h + k) \in h\mathcal{I}^*(G,m)$. We will show that

$$(hq_1, ..., hq_{r-1}, hq_r - 2h + k + 1) \in h\mathcal{I}^*(G,m).$$

Since $(hq_1, ..., hq_{r-1}, hq_r - 2h + k) \in h\mathcal{I}^*(G,m)$, we know that $hq_r - 2h + k = a_1 + ... + a_h$, where $a_i \in \{0, ..., q_r - 2\} \cup \{q_r\}$ for each $1 \leq i \leq h$. We use proof by cases.

Case 1: Assume that there exists a $1 \leq i \leq h$ such that $a_i \leq q_r - 3$.
Then $(q_1, ..., q_{r-1}, a_i + 1) \in \mathcal{I}^*(G,m)$, and therefore

$$(hq_1, ..., hq_{r-1}, hq_r - 2h + k + 1) = (hq_1, ..., hq_{r-1}, 1 + \sum_{i=1}^{h} a_i) \in h\mathcal{I}^*(G,m).$$

Case 2: Let $1 \leq s \leq h$ and $1 \leq t \leq h$, with $s \neq t$ such that $a_s = a_t = q_r - 2$.
Assume that for all $i \in \{1, ..., h\}/\{s,t\}$, we have $a_i \in \{q_r - 2, q_r\}$. Note that

$$hq_r - 2h + k + 1 = 1 + a_s + a_t + \sum_{i \in \{1,...,h\}/\{s,t\}} a_i = (q_r - 3) + q_r + \sum_{i \in \{1,...,h\}/\{s,t\}} a_i.$$

So

$$(hq_1, ..., hq_{r-1}, hq_r - 2h + k + 1) \in h\mathcal{I}^*(G,m).$$

We have now distinguished all cases such that $0 \leq k \leq 2h - 3$. With our inductive process we conclude that for all $hq_r - 2h + 1 \leq q \leq hq_r - 2$, we have $(hq_1, ..., hq_{r-1}, q) \in h\mathcal{I}^*(G,m)$.

We will show that $(hq_1, ..., hq_{r-1}, hq_r - 1) \notin h\mathcal{I}^*(G,m)$. Assume the contrary. Than $hq_r - 1 = a_1 + ... + a_h$, where $a_i \in \{0, ..., q_r - 2\} \cup \{q_r\}$ for each $1 \leq i \leq h$. Note however, that

$$(h-1)q_r + q_r - 2 < hq_r - 1 < hq_r,$$

and therefore both of the following statements must be true.

a. For all $1 \leq i \leq h$, we have $a_i > q_r - 2$, so $a_i = q_r$ for all i.

b. There exists a $1 \leq i \leq h$ such that $a_i < q_r$.

This is a clear contradiction , so $(hq_1, ..., hq_{r-1}, hq_r - 1) \notin h\mathcal{I}^*(G, m)$.

Assume that there exists a $(b_1, ..., b_r) \in h\mathcal{I}^*(G, m)$ such that $(b_1, ..., b_r) > (hq_1, ..., hq_r)$. Then there exists some $1 \leq i \leq h$ such that $b_i > hq_i$ and $b_j = hq_j$ for all $1 \leq j < i$. But then $b_i = a_1 + ... + a_h$, where $0 \leq a_i \leq q_i$. Therefore $b_i \leq hq_i$, which is a contradiction.

We conclude that

$$h\mathcal{I}^*(G, m) = \mathcal{I}(G, hm - 1) \cup \{(hq_1, ..., hq_{r-1}, hq_r)\}.$$

So $|h\mathcal{I}^*(G, m)| = hm$. □

Remark.
It is easy to see why, in part (1) of Proposition 1.6, we have the requirement that $q_r \geq 1$: In this case the largest element of $\mathcal{I}(G, m)$ is $(q_1, ..., q_{r-1}, q_r - 1)$, which makes determining the set $h\mathcal{I}(G, m)$ manageable.

Thus it might be confusing why, for part (2), we have the requirement that $q_r \geq 3$:

$$\mathcal{I}^*(G, m) = \mathcal{I}(G, m - 1) \cup \{(q_1, ..., q_{r-1}, q_r)\},$$

so for $q_r = 2$ the largest element of $\mathcal{I}(G, m-1)$ would be $(q_1, ..., q_{r-1}, q_r - 2) = (q_1, ..., q_{r-1}, 0)$, which makes determining the set $\mathcal{I}^*(G, m)$ manageable. Note however, that in this case, for all $1 \leq k \leq h - 1$ we have

$$(hq_1, ..., hq_{r-1}, hq_r - 2h + 2k + 1) \notin h\mathcal{I}^*(G, m).$$

So

$$h\mathcal{I}^*(G, m) = \mathcal{I}(G, hm - 2h + 1) \cup \{(hq_1, ..., hq_{r-1}, hq_r - 2h + 2k) : 1 \leq k \leq h\}.$$

So $|h\mathcal{I}^*(G, m)| = hm - 2h + 1 + h = hm - h + 1$.

We will now introduce a corollary, which is a slight variation of Proposition 1.6.

Corollary 1.7. Let G be a finite abelian group, $1 \leq m \leq n$ and $h \geq 1$. Then

$$|h\mathcal{I}(G, m)| \leq hm - h + 1.$$

Proof. Let

$$m = \sum_{i=1}^{r} q_i n_{i+1} \cdots n_r.$$

If $q_r \geq 1$ and $hq_k < n_k$ for all $1 \leq k \leq r$, we apply Proposition 1.6 to obtain the result.

Assume that $q_r \geq 1$ and that there exist $1 \leq i \leq r$ such that $hq_i \geq n_i$, and k is the greatest of these. We find that

$$h\mathcal{I}(G, m) = \{g \in G : (0, ..., 0) \leq g \leq (hq_1, ..., hq_{k-1}, n_k - 1, hq_{k+1}, ..., hq_r - h)\}.$$

So it follows that

$$|h\mathcal{I}(G, m)| \leq hm - h + 1.$$

Assume that there exists a $1 \leq i \leq r$ such that $q_{i-1} \neq 0$ and $q_k = 0$ for all $i \leq k \leq r$. Then

$\mathcal{I}(G,m)$ is the set of elements from 0 up to $(q_1,...,q_{i-2},q_{i-1}-1,n_i-1,...,n_r-1)$. Therefore,

$$h\mathcal{I}(G,m)=\{g\in G:(0,...,0)\leq g\leq (hq_1,...,hq_{i-2},hq_{i-1}-h,n_i-1,...,n_r-1)\}.$$

So $|h\mathcal{I}(G,m)|\leq hm-h+1$.

Since we have distinguished all the cases, we conclude that

$$|h\mathcal{I}(G,m)|\leq hm-h+1.$$

This establishes our proof. □

2. The h-critical number

In this section we will work towards a result that gives us $\chi(G,h)$ for each h.

Let

$$\rho(G,m,h) = \min\{|hA| : A \subseteq G, |A| = m\}$$

and

$$u(n,m,h) = \min\{f_d : d|n\},$$

where n, m, h are positive integers and

$$f_d(m,h) = (h\lceil m/d\rceil - h + 1)d.$$

The following result will help us determine $\chi(G,h)$.

Lemma 2.1. Let n, m, h be positive integers such that $m \leq n$, and let G be a finite abelian group with $|G| = n$. Then

$$\rho(G,m,h) = u(n,m,h).$$

Proof. We first show that $\rho(G,m,h) \geq u(n,m,h)$. Let $A \subseteq G$ with $|A| = m$ such that $|hA| = \rho(G,m,h)$. Let H be the stabilizer subgroup of hA. Then by Corollary 1.2, it follows that

$$\rho(G,m,h) = |hA| \geq h|A| - (h-1)|H|.$$

Using Lemma 1.3, we know that $|A| = k_1|H|$ for some $k_1 \in \mathbb{N}$. Therefore

$$h|A| - (h-1)|H| = hk_1|H| - (h-1)|H| = (hk_1 - h + 1)|H| = f_{|H|} \geq u(n,m,h).$$

We will now show that $\rho(G,m,h) \leq u(n,m,h)$. Let $H \leq G$ be a subgroup. Let $\phi : G \to G/H$ be the canonical map. Note that since G is abelian, so is G/H. Let $r = \lceil m/|H|\rceil$. Using the notation in Proposition 1.6, we consider the set $\mathcal{I}(G/H, r)$. Note that $r \leq |G/H|$, since $m \leq n = |G/H||H|$, so $\frac{m}{|H|} \leq |G/H|$. So $\mathcal{I}(G/H, r)$ is well-defined. From Corollary 1.7, it follows that $|h\mathcal{I}(G/H, r)| \leq hr - h + 1$.

Let $A = \phi^{-1}(\mathcal{I}(G/H, r))$. From Lemma 1.4 we know that $|A| = |H|\lceil m/|H|\rceil \geq m$. Therefore $|hA| \geq \rho(G,m,h)$, so

$$\rho(G,m,h) \leq |hA| = |H| \cdot |h\mathcal{I}(G/H, r)| \leq (h\lceil m/|H|\rceil - h + 1) \cdot |H|.$$

Since G is abelian, there exists a subgroup of order d for all divisors d of n. (This follows from the fundamental theorem of finite abelian groups.) Because of that, $\rho(G,m,h) \leq (h\lceil m/d\rceil - h+1) \cdot d$ for all $d \in \mathbb{N}$ such that $d|n$. So $\rho(G,m,h) \leq u(n,m,h)$. Since $\rho(G,m,h) \leq u(n,m,h)$ and $\rho(G,m,h) \geq u(n,m,h)$, we have

$$\rho(G,m,h) = u(n,m,h),$$

which concludes our proof. □

We write

$$v(n,h) = \max\left\{\left(\left\lfloor\frac{d-2}{h}\right\rfloor + 1\right)\frac{n}{d} : d|n\right\}.$$

With Lemma 2.1, we now have all the results we need to prove the following result:

Theorem 2.2. Let G be an abelian group with $|G| = n$, and let $h \geq 1$. Then

$$\chi(G,h) = v(n,h) + 1.$$

Proof. Recall that

$$\chi(G,h) = \min\{m \geq 1 : A \subseteq G, |A| \geq m \implies |hA| = n\}.$$

Therefore, we want to show that whenever $|A| = v(n,h) + 1$, we have $|hA| = n$, but that there exists a subset $A \subseteq G$ such that $|A| = v(n,h)$ and $|hA| < n$. This would show that any subset of size $v(n,h)+1$ is h-complete, and that $v(n,h)+1$ is the smallest positive integer with this property. From Lemma 2.1, we know that

$$\min\{|hA| : A \subseteq G, |A| = m\} = \rho(G,m,h) = u(n,m,h).$$

We will therefore show that

$$n > \min\{|hA| : A \subseteq G, |A| = v(n,h)\} = \rho(G, v(n,h), h) = u(n, v(n,h), h)$$

and that

$$n \leq \min\{|hA| : A \subseteq G, |A| = v(n,h)+1\} = \rho(G, v(n,h)+1, h) = u(n, v(n,h)+1, h).$$

We start with the first inequality. Let $d_0 | n$ such that

$$v(n,h) = \left(\left\lfloor \frac{d_0 - 2}{h} \right\rfloor + 1 \right) \frac{n}{d_0}.$$

Note that $u(n, v(n,h), h) \leq f_{n/d_0}(v(n,h),h)$, where

$$f_{n/d_0}(v(n,h),h) = \left(h \left\lceil \frac{\left(\left\lfloor \frac{d_0-2}{h} \right\rfloor + 1 \right) \frac{n}{d_0}}{\frac{n}{d_0}} \right\rceil - h + 1 \right) \frac{n}{d_0} = \left(h \left\lfloor \frac{d_0 - 2}{h} \right\rfloor + 1 \right) \frac{n}{d_0}.$$

Therefore it follows that

$$u(n, v(n,h), h) \leq f_{n/d_0}(v(n,h),h) = \left(h \left\lfloor \frac{d_0 - 2}{h} \right\rfloor + 1 \right) \frac{n}{d_0} \leq (d_0 - 1)\frac{n}{d_0} < n.$$

This completes the first inequality.

For the second inequality, we need to show that for any $d \in \mathbb{N}$ such that $d|n$, we have

$$f_d(v(n,h)+1,h) = \left(h \left\lceil \frac{\left(\left\lfloor \frac{d_0-2}{h} \right\rfloor + 1 \right) \frac{n}{d_0} + 1}{d} \right\rceil - h + 1 \right) d \geq n.$$

Note that $\frac{n}{d} | n$, so by our choice of d_0 we obtain

$$v(n,h) = \left(\left\lfloor \frac{d_0 - 2}{h} \right\rfloor + 1 \right) \frac{n}{d_0} \geq \left(\left\lfloor \frac{\frac{n}{d} - 2}{h} \right\rfloor + 1 \right) \frac{n}{n/d}.$$

Therefore

$$\frac{f_d(v(n,h)+1,h)}{d} = h\left\lceil\frac{\left(\left\lfloor\frac{d_0-2}{h}\right\rfloor+1\right)\frac{n}{d_0}+1}{d}\right\rceil - h+1 \geq h\left\lceil\frac{\left(\left\lfloor\frac{\frac{n}{d}-2}{h}\right\rfloor+1\right)\frac{n}{n/d}\cdot+1}{d}\right\rceil - h+1 =$$

$$h\left\lceil\left(\left\lfloor\frac{\frac{n}{d}-2}{h}\right\rfloor+1\right)+\frac{1}{d}\right\rceil - h+1 = h\left(\left\lfloor\frac{\frac{n}{d}-2}{h}\right\rfloor+2\right) - h+1 \geq$$

$$h\left(\frac{\frac{n}{d}-2}{h} - 1 + \frac{1}{h} + 2\right) - h + 1 = \frac{n}{d}.$$

So $f_d(v(n,h)+1,h) \geq n$ for all $d|n$. Therefore $n \leq u(n, v(n,h)+1, h) = \rho(G, v(n,h)+1, h)$. It follows that for any subset of G with size $v(n,h)+1$ is h-complete and that $v(n,h)+1$ is the smallest positive integer with this property. So $\chi(G,h) = v(n,h)+1$. $\square$

We will now prove a result that makes it easier to determine $\chi(G,h)$ for each h.

Lemma 2.3. Let $n \in \mathbb{N}$ and $h \geq 2$. For each $2 \leq i \leq h-1$, let $P_i(n)$ be the set of prime divisors of n that leave a remainder of i when divided by h, so

$$P_i(n) = \{p|n : p \text{ prime and } p \equiv i \pmod{h}\}.$$

Let I be the set of $2 \leq i \leq h-1$ such that $P_i(n) \neq \emptyset$, and for each $i \in I$ let p_i be the smallest element of $P_i(n)$. Then

$$v(n,h) = \begin{cases} \frac{n}{h}\max\left\{1+\frac{h-i}{p_i} : i \in I\right\} & \text{if } I \neq \emptyset; \\ \left\lfloor\frac{n}{h}\right\rfloor & \text{if } I = \emptyset. \end{cases}$$

Proof. We define

$$g(d) = \left(\left\lfloor\frac{d-2}{h}\right\rfloor+1\right)\frac{n}{d}.$$

Let $d_0|n$ such that $v(n,h) = g(d_0)$ and let $0 \leq i_0 \leq h-1$ such that $d_0 \equiv i_0 \pmod{h}$. We first prove two claims.

Claim 1: Assume that $i_0 \leq 1$. Then $g(d_0) = \lfloor\frac{n}{h}\rfloor$.

Proof of Claim 1: We write $d_0 = kh + i_0$. Since $i_0 - 2 < 0$, we have

$$v(n,h) = g(d_0) = \left(\left\lfloor\frac{kh+i_0-2}{h}\right\rfloor+1\right)\frac{n}{d_0} = (k-1+1)\frac{n}{d_0} = \frac{d_0-i_0}{d_0}\cdot\frac{n}{h} \leq \frac{n}{h}.$$

Also, we see that

$$v(n,h) \geq \left(\left\lfloor\frac{n-2}{h}\right\rfloor+1\right)\frac{n}{n} = \left(\left\lfloor\frac{n-2}{h}\right\rfloor+1\right) \geq \left\lfloor\frac{n}{h}\right\rfloor.$$

Since $\lfloor\frac{n}{h}\rfloor \leq v(n,h) \leq \frac{n}{h}$, we conclude that $\lfloor\frac{n}{h}\rfloor = v(n,h) = g(d_0)$, which proves the claim.

Claim 2: Let $i_0 \geq 2$. Then d_0 is prime.

Proof of claim 2: First, note that with this assumption $h \neq 2$, since that would imply that $2 \leq i_0 \leq 1$ which is a contradiction. So $h \geq 3$. Note that d_0 has at least one prime divisor

that leaves a remainder greater than 1 (mod h). Let p be the smallest prime divisor of d_0 such that $p \equiv i \pmod h$, for some $2 \le i \le h-1$.
We will show that

$$\frac{h-2}{p^2} < \frac{h-i}{p}.$$

If $p > h-2$, we have

$$\frac{h-2}{p^2} < \frac{h-2}{p(h-2)} = \frac{1}{p} \le \frac{h-i}{p},$$

since $i \le h-1$. Let $p \le h-2$. Since $p \equiv i \pmod h$, we have $i = p$, so

$$\frac{h-2}{p^2} = \frac{hp - h(p-1) - 2}{p^2} \le \frac{hp - (p+2)(p-1) - 2}{p^2} = \frac{h-p-1}{p} < \frac{h-p}{p} = \frac{h-i}{p}.$$

So

$$\frac{h-2}{p^2} < \frac{h-i}{p}.$$

Now assume that $i \neq i_0$. Then $\frac{d_0}{p} \not\equiv 1 \pmod h$, so $\frac{d_0}{p}$ has a prime divisor p' that leaves a remainder greater than 1 (mod h). Therefore $p' \ge p$, so $d_0 \ge p^2$. We find that

$$g(d_0) = \left(\left\lfloor \frac{d_0-2}{h} \right\rfloor + 1\right)\frac{n}{d_0} = \left(\frac{d_0-i_0}{h} + 1\right)\frac{n}{d_0} = \frac{n}{h}\left(1 + \frac{h-i_0}{d_0}\right) \le \frac{n}{h}\left(1 + \frac{h-2}{p^2}\right),$$

since $i_0 \ge 2$ and $d_0 \ge p^2$. Since $p \equiv i \pmod h$, and since $2 \le i \le h-1$, it follows that

$$\frac{n}{h}\left(1 + \frac{h-2}{p^2}\right) < \frac{n}{h}\left(1 + \frac{h-i}{p}\right) = \frac{n}{p}\left(\frac{p-i}{h} + 1\right) = \frac{n}{p}\left(\left\lfloor \frac{p-2}{h} \right\rfloor + 1\right) = g(p).$$

So $v(n,h) = g(d_0) < g(p)$. However $v(n,h) \ge g(d)$ for all divisors d of n, so this is a contradiction.
We conclude that $i = i_0$, and

$$v(n,h) = g(d_0) = \frac{n}{h}\left(1 + \frac{h-i_0}{d_0}\right) \le \frac{n}{h}\left(1 + \frac{h-i_0}{p}\right) = g(p).$$

Since $v(n,h) \ge g(p)$, we find that $g(d_0) = v(n,h) = g(p)$, so $d_0 = p$. So d_0 is prime, which completes the proof of our claim.

Now assume that $I = \emptyset$. Then for all $2 \le i \le h-1$, we know that n has no prime divisors congruent to $i \pmod h$. So all divisors of n are divisible by h or are congruent to $1 \pmod h$. Since $v(n,h) = g(d)$ for some $d|n$, we use the first claim and conclude that $v(n,h) = \lfloor \frac{n}{h} \rfloor$.

Assume that $I \neq \emptyset$. Note that

$$g(d_0) = \frac{n}{h}\left(1 + \frac{h-i_0}{d_0}\right) > \left\lfloor \frac{n}{h} \right\rfloor,$$

whenever $d_0 \equiv i_0 \pmod h$ with $2 \le i_0 \le h-1$.
Therefore, with our second claim we conclude that

$$v(n,h) = \max\{g(d) : d|n\} = \max\left\{ \left(\left\lfloor \frac{p-2}{h} \right\rfloor + 1\right)\frac{n}{p} : p|n \text{ and } p \text{ prime} \right\}.$$

Note that for two primes $p_1 \leq p_2$ such that $p_1 \equiv p_2 \equiv i \pmod{h}$, we have $g(p_1) \geq g(p_2)$, so

$$v(n,h) = \frac{n}{h} \max\left\{1 + \frac{h-i}{p_i} : i \in I\right\}.$$

This completes our proof. □

For each $h \in \mathbb{N}$, we can now determine the h-critical number without much effort, so we can now move on to the size of sumsets.

3. 2-fold sumsets

In this section we work out the case of $h = 2$. We first find the 2-critical number using previous results, and then determine the size of 2-fold sumsets of nonbases of maximum size.

Corollary 3.1. Let G be an abelian group of order n. Then we have

$$\chi(G,2) = \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

Proof. We know that $\chi(G,2) = v(n,2) + 1$. Using the notation in Theorem 2.3, we let I be the set of $2 \leq i \leq 1$ such that $P_i(n) \neq \emptyset$, therefore $I = \emptyset$. So

$$v(n,2) = \left\lfloor \frac{n}{2} \right\rfloor,$$

and

$$\chi(G,2) = v(n,2) + 1 = \left\lfloor \frac{n}{2} \right\rfloor + 1.$$

This completes the proof. □

Recall that the set of sizes of sumsets of nonbases of maximum size is given by

$$S(G,h) = \{|hA| : A \subset G, |A| = \chi(G,h) - 1, hA \neq G\}.$$

In the rest of this section, we work towards finding $S(G,2)$. We start with a result that will be of help later in a specific case.

Lemma 3.2. Let G be a finite abelian group with even order n, such that the exponent of G is not divisible by 4. Let $A \subseteq G$ with $A = \frac{n}{2}$. Then there exists a subgroup $H \leq G$ of order $|H| = \frac{n}{2}$ such that

$$|A \cap H| \neq |A \cap (G \setminus H)|.$$

Proof. Let $A \subseteq G$ with $|A| = \frac{n}{2}$. We assume, for contradiction, that each subgroup of order $\frac{n}{2}$ contains exactly half of the elements of A. We write $G = G_1 \times G_2$, where $|G_1|$ is odd and G_2 is of type $m_1, ..., m_t$, with all m_i even and not divisible by 4 for all $1 \leq i \leq t$. We call $C \subseteq G$ a projection of G if it is of the form $G_1 \times B_1 \times \cdots \times B_t$, and for each i either $B_i = \mathbb{Z}_{m_i}$ or B_i is a coset of the subgroup of index 2 in $\mathbb{Z}_{m_i}$. Therefore, each projection of G has size $\frac{n}{2^k}$, for some $0 \leq k \leq t$. Using our assumption, we will show the following:

If C is a projection of G of size $\frac{n}{2^k}$, then $|A \cap C| = \frac{n}{2^{k+1}}$.

We use induction over k. It is trivial that the claim holds for $k = 0$. For $k = 1$, we note that any projection of size $\frac{n}{2}$ is either a subgroup of index 2 or a coset of that subgroup, and by our assumption both contain $\frac{n}{4}$ elements of A. Now assume that the claim holds for $k - 1$ for some $1 \leq k - 1 \leq t$. We prove our claim for k. Because of the symmetry of the direct products of group, it suffices to only consider the projections in the set

$$S = \{G_1 \times B_1 \times \cdots \times B_t : |B_i| = \frac{n_i}{2} \text{ if } 1 \leq i \leq k \text{ and } |B_j| = n_i \text{ if } k + 1 \leq j \leq t\}.$$

We will now introduce Gray-code ordering of $\mathbb{Z}_2^k$, which we will define by induction. First, for $\mathbb{Z}_2$, let $0 < 1$. Now let $\mathbb{Z}_2^l$ have Gray-code ordering for some $1 \leq l \leq k - 1$ such that

$\mathbb{Z}_2^l = \{e_0, ..., e_{2^l-1}\}$, and $e_0 < ... < e_{2^l-1}$. Note that

$$\mathbb{Z}_2^{l+1} = \{\{0\} \times e_0, \{1\} \times e_0, \{0\} \times e_1, \{1\} \times e_1, ..., \{0\} \times e_{2^l-1}, \{1\} \times e_{2^l-1}\}.$$

We apply it with the following ordering:

$$\{0\} \times e_0 < \{0\} \times e_1 < ... < \{0\} \times e_{2^l-1}, \{1\} \times e_{2^l-1} < \{1\} \times e_{2^l-2} < ... < \{1\} \times e_0.$$

With this construction, we give $\mathbb{Z}_2^k = \{e_0, ..., e_{2^k-1}\}$ Gray-code ordering, and write

$$e_0 < e_1 < ... < e_{2^k-1}.$$

Here e_0 is the identity element, and e_j and e_{j+1} differ in exactly one position for each $0 \leq j \leq 2^k - 2$. Also, e_0 and e_{2^k-1} differ in exacly one position.

We now arrange the elements of S in a corresponding sequence

$$S = \{C_0, ..., C_{2^k-1}\}.$$

Here $C_j = G_1 \times B_1 \times \cdots \times B_t$, where for all $1 \leq i \leq k$, we have $B_i \leq \mathbb{Z}_{m_i}$ if and only if the i-th component of e_j is equal to 0, and otherwise $(\mathbb{Z}_{m_i} \setminus B_i) \leq \mathbb{Z}_{m_i}$. Of course we have $B_i = \mathbb{Z}_{m_i}$ whenever $k + 1 \leq i \leq t$.

Note that for all $0 \leq j \leq 2^k - 1$, we have $|C_j \cup C_{j+1}| = 2 \cdot \frac{n}{2^k} = \frac{n}{2^{k-1}}$, and $C_j \cup C_{j+1}$ is a projection of G. Therefore, by our inductive hypothesis, $|(C_j \cup C_{j+1}) \cap A| = \frac{n}{2^k}$.

Since $|(C_j \cup C_{j+1}) \cap A| = |(C_{j+1} \cup C_{j+2}) \cap A|$ it follows that, if $|C_0 \cap A| = s$, then $|C_j \cap A| = s$ if j is even, and $|C_j \cap A| = \frac{n}{2^k} - s$ if j is odd. Now note that

$$H = C_0 \cup C_2 \cup ... \cup C_{2^k-2}.$$

is a subgroup of G with index 2. So by our original assumption $|H \cap A| = \frac{n}{4}$. Now note that

$$H \cap A = (C_0 \cap A) \cup (C_2 \cap A) \cup ... \cup (C_{2^k-2} \cap A).$$

Therefore, $t \cdot \frac{2^k}{2} = \frac{n}{4}$, so $t = \frac{n}{2^{k+1}}$. So, by induction, for all $0 \leq k \leq t$, if C is a projection of G of size $\frac{n}{2^k}$, then $|A \cap C| = \frac{n}{2^{k+1}}$.

Now let C be a projection of G of size $\frac{n}{2^t}$. Then this result implies that $|A \cap C| = \frac{n}{2^{t+1}}$. However, all m_i are not divisible by 4, so $2^{t+1} \nmid n$, which is a contradiction, so our claim is false. Since we were only ably to prove the claim using our original assumption, the assumption is false, so $|A \cap H| \neq |A \cap (G \setminus H)|$. □

For determining $S(G, 2)$, we make a distinction between the cases where n is even and n is odd. We start with the case where n is even.

Theorem 3.3. Let G be a finite abelian group with $|G| = n$, where n is even. Let $(n_1, ..., n_r)$ be the unique type of G. If n_r is divisible by 4, then

$$S(G, 2) = \{n - \frac{n}{d} : d|n, 2|d\}.$$

If n_r is not divisible by 4, then

$$S(G, 2) = \{n - \frac{n}{d} : d|n, 2|d, d \neq 4\}.$$

Proof. Let A be a h-incomplete subset of G of maximum size. Using the notation of Lemma 1.3, let H denote the stabilizer subgroup of $2A$. Then A and $2A$ consist respectively of k_1 and k_2 cosets of H. Let d be the index of H. Since n is even, and $\chi(G,2) = \lfloor \frac{n}{2} \rfloor + 1$, we have

$$\frac{k_1 n}{d} = k_1|H| = |A| = \left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}.$$

So $2k_1 = d$, and therefore d is even. Using Lemma 1.3 again, we get

$$k_2 \geq 2k_1 - 2 + 1 = 2k_1 - 1 = d - 1.$$

Note that $k_2 \frac{n}{d} = |2A| < n$, so $d - 1 \leq k_2 < d$. So $k_2 = d - 1$, and

$$S(G,2) \subseteq \{n - \frac{n}{d} : d|n, 2|d\}.$$

Now let $4 \nmid n_r$. We show that $n - \frac{n}{4} \notin S(G,2)$. By Theorem 3.2, there exists a subgroup H of index 2 such that

$$|A \cap H| \neq |A \cap (G \setminus H)|.$$

Note that H has two cosets, namely H and $G \setminus H$, so we write $A = A_1 \cup A_2$, where $A_1 \subseteq H$, $A_2 \subseteq G \setminus H$. Without loss of generality we assume that $|A_1| > \frac{n}{4}$, so $2A_1 = H$. If $A_2 = \emptyset$, then $A = A_1$, so $|2A| = |2A_1| = \frac{n}{2} \neq \frac{3n}{4}$. Otherwise $|A_1 + A_2| \geq |A_1| > \frac{n}{4}$, so

$$|2A| \geq |2A_1| + |A_1 + A_2| > \frac{3n}{4}.$$

So $|2A| \neq \frac{3n}{4}$ and $\frac{3n}{4} \notin S(G,2)$.

We will now show that all other values are present in $S(G,2)$. Let A be a subgroup of index 2 of G, since subgroups are closed under the operation of G, we have $|2A| = |A| = \frac{n}{2}$. So $n - \frac{n}{2} = \frac{n}{2} \in S(G,2)$. Let $4|n_r$. We take the subgroup $H = \{\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_{r-1}} \times \mathbb{Z}_{\frac{n_r}{4}}\}$ of index 4 of G. Let $\phi : G \to G/H$ denote the canonical map. Note that

$$G/H = \{H, (0, ..., 0, 1) + H, (0, ..., 0, 2) + H, (0, ..., 0, 3) + H\},$$

and therefore $G/H \cong \mathbb{Z}_4$. We take the subset $B = \{H, (0, ..., 0, 1) + H\}$ of G/H, and note that $|2B| = 3$. Using Lemma 1.4, we let $A = \phi^{-1}(B)$, and find that $|A| = \frac{n}{4}|B| = \frac{n}{2}$, and

$$|2A| = \frac{n}{4}|2B| = \frac{3n}{4} = n - \frac{n}{4}.$$

So $n - \frac{n}{4} \in S(G,2)$ whenever $4 \nmid n_r$.

Now let $d|n$, with d even and $d > 4$. Using the notation in Lemma 1.4, let $H \leq G$ be of index d, and let $\phi : G \to G/H$ be the canonical map. We construct a subset B of G/H, such that $|B| = \frac{d}{2}$ and $|2B| = d - 1$. Let K be a subgroup of G/H of index 2. We define

$$B = (K \setminus \{k\}) \cup \{g\},$$

where $k \in K$ and $g \in (G/H) \setminus K$ are arbitrary elements. Note that $K = 2(K \setminus \{k\}) \subseteq 2B$, and $(g + K) \setminus \{k + g\} \subseteq B$. So $2B = (G/H) \setminus \{k + g\}$. Therefore $|2B| = d - 1$.

Let $A = \phi^{-1}(B)$. Then

$$|A| = \frac{n}{d}|B| = \frac{n}{d} \cdot \frac{d}{2} = \frac{n}{2},$$

and

$$|2A| = \frac{n}{d}|2B| = \frac{n}{d}(d-1) = n - \frac{n}{d},$$

which completes our proof. □

We will now determine $S(G, 2)$ for odd order.

Theorem 3.4. If $G \cong \mathbb{Z}_3, \mathbb{Z}_5$ or $\mathbb{Z}_3^2$, we have $S(G, 2) = \{n-2\}$. Otherwise, if G has odd order, we have $S(G, 2) = \{n-2, n-1\}$.

Proof. Let $A \subseteq G$ with $|A| = \chi(G, 2) - 1 = \frac{n-1}{2}$. Using the notation of Lemma 1.3, let H denote the stabilizer subgroup of $2A$. Then A and $2A$ consist respectively of k_1 and k_2 cosets of H. Let d be the index of H. Then

$$\frac{n-1}{2} = |A| = \frac{k_1 n}{d},$$

Which implies that $\frac{n}{d}$ divides $n-1$. Since $\frac{n}{d}|n$, this is only possible if $\frac{n}{d} = 1$, so $n = d$ and $k_1 = \frac{n-1}{2}$. Therefore

$$|2A| = k_2 \geq 2k_1 - 2 + 1 = n - 2.$$

Since $|2A| < n$, we have $S(G, 2) \subseteq \{n-2, n-1\}$.

Since $|G|$ is odd, G is of type $(n_1, ..., n_r)$ for $r, n_1, ..., n_r \in \mathbb{N}$ with n_k odd for all k. Then

$$\frac{n-1}{2} = \sum_{k=1}^{r} \frac{n_k - 1}{2} n_{k+1} \cdots n_r.$$

This can be realized by noting that

$$\sum_{k=1}^{r} (n_k - 1) n_{k+1} \cdots n_r = n - \frac{n}{n_1} + \frac{n}{n_1} - \frac{n}{n_1 n_2} + \frac{n}{n_1 n_2} - ... - n_r + n_r - 1 = n - 1.$$

Since $n_i | n_{i+1}$ for all $1 \leq i \leq r-1$, we have $n_r \geq 3$. So $\frac{n_r - 1}{2} \geq 1$. Using the notation of Proposition 1.6, we have

$$|2\mathcal{I}(G, \frac{n-1}{2})| = \frac{2(n-1)}{2} - 2 + 1 = n - 2.$$

So $n - 2 \in S(G, 2)$. Similarly, if $\frac{n_r - 1}{2} \geq 3$ we have

$$|2\mathcal{I}^*(G, \frac{n-1}{2})| = \frac{2(n-1)}{2} = n - 1.$$

So $n - 1 \in S(G, 2)$ whenever $n_r \geq 7$.

That leaves us with $\mathbb{Z}_3^r$ and $\mathbb{Z}_5^s$. For $r \geq 3$, we take

$$A = \left(\mathcal{I}\left(\mathbb{Z}_3^r, \frac{n-1}{2}\right) \setminus \{(1, 1, ..., 1, 0, 2, 2)\}\right) \cup \{(1, 1, ..., 1, 2, 0, 0)\}.$$

We then find that

$$2A = \mathbb{Z}_3^r \setminus \{(2, 2, ..., 2)\}.$$

For $s \geq 2$, we take

$$B = (\mathcal{I}(\mathbb{Z}_5^r, \frac{n-1}{2} \setminus \{(2, 2, ..., 2, 1, 4)\}) \cup \{(2, 2, ..., 2, 3, 0)\}.$$

We then find

$$2B = \mathbb{Z}_5^r \setminus \{(4, 4, ..., 4)\}.$$

For $G \cong \mathbb{Z}_3, \mathbb{Z}_5$ or $\mathbb{Z}_3^2$, it can be verified that $n - 1 \notin S(G, 2)$.
Therefore $S(G, 2) = \{n - 2\}$ if $G \cong \mathbb{Z}_3, \mathbb{Z}_5$ or $\mathbb{Z}_3^2$, and for all other groups G of odd order we have $S(G, 2) = \{n - 2, n - 1\}$. □

We have now determined $S(G, 2)$ for all G. In the next section we will consider $h = 3$.

4. 3-fold sumsets

In this section we determine $S(G,h)$ for $h=3$. Once again we first give the h-critical number.

Corollary 4.1. Let G be an abelian group of order n. Then

$$\chi(G,3)=\begin{cases}\left(1+\frac{1}{p}\right)\frac{n}{3}+1 & \text{if } n \text{ has prime divisors congruent to } 2 \pmod 3,\\ & \text{and } p \text{ is the smallest such divisor;}\\ \left\lfloor\frac{n}{3}\right\rfloor+1 & \text{otherwise.}\end{cases}$$

Proof. Note that $\chi(G,3)=v(n,3)+1$. Using the notation of Lemma 2.3, let

$$P_2(n)=\{p|n : p \text{ prime and } p\equiv 2 \pmod 3\}.$$

We then have

$$v(n,3)=\begin{cases}\left(1+\frac{1}{p}\right)\frac{n}{3} & \text{if } P_2(n)\neq\emptyset,\\ & \text{and } p \text{ is the smallest element of } P_2(n);\\ \left\lfloor\frac{n}{3}\right\rfloor+1 & \text{if } P_2(n)=\emptyset.\end{cases}$$

This completes the proof. □

We will now determine $S(G,3)$ by giving several theorems distinguishing all the possible cases.

Theorem 4.2. Let G be a finite abelian group with $|G|=n$. Assume that n has prime divisors congruent to 2 (mod 3), and that p is the smallest of these. Then

$$S(G,3)=\left\{n-\frac{n}{p}\right\}.$$

Proof. Let A be a 3-incomplete subset of maximum size of G. With the notation of Lemma 1.3, let H be the stabilizer subgroup of $3A$. Let A and $3A$ consist respectively of k_1 and k_2 cosets of H. Let d denote the index of H. Then by Corollary 4.1,

$$\frac{(p+1)n}{3p}=|A|=\frac{k_1 n}{d}.$$

So $k_1=\frac{(p+1)d}{3p}$, which implies that $p|d$, since $p\nmid\frac{p+1}{3}$. Then we have

$$k_2\geq 3k_1-3+1=\frac{dp+d}{p}-2=d+\left(\frac{d}{p}-2\right)\geq d-1,$$

with equality if and only if $d=p$. We find that

$$n>|3A|=\frac{k_2 n}{d}\geq\frac{(d-1)n}{d}.$$

Therefore $d>k_2\geq d-1$. We conclude that $k_2=d-1$, and $d=p$. So $|3A|=\frac{(p-1)n}{p}=n-\frac{n}{p}$. It follows that

$$S(G,3)=\left\{n-\frac{n}{p}\right\}.$$

This concludes our proof. □

Next we look at the case where n is divisible by 3, and has no prime divisors that are congruent to $2 \pmod 3$.

Theorem 4.3. Let G be a finite abelelian group of order n, with exponent n_r. Assume that $3|n$, and n has no prime divisors congruent to $2 \pmod 3$. For any $t \geq 1$, let

$$\nu_3(t) = \max\{m \geq 0 : 3^m = t\}.$$

Then

$$S(G,3) = \{n - \frac{n}{d} : d|n, 3|d, d \neq 3\} \cup \{n - \frac{2n}{d} : d|n, 1 \leq \nu_3(d) \leq \nu_3(n_r)\}.$$

With n_r denoting the exponent of G.

Proof. By Corollary 4.1, we have $\chi(G,3) = \frac{n}{3} + 1$. Let A be a subset of G with $|A| = \frac{n}{3}$. We show the result using five claims.

Claim 1: $S(G,3) \subseteq \{n - \frac{cn}{d} : d|n, 3|d, c = 1,2\}$.

Proof of Claim 1: With the notation of Lemma 1.3, let H be the stabilizer subgroup of $3A$. Let A and $3A$ consist respectively of k_1 and k_2 cosets of H. Let d denote the index of H. Then

$$\frac{n}{3} = |A| = \frac{k_1 n}{d},$$

so $3k_1 = d$, and $3|d$. Furthermore, we have

$$k_2 \geq 3k_1 - 3 + 1 = d - 2.$$

So

$$n > |3A| = \frac{k_2 n}{d} \geq \frac{(d-2)n}{d}.$$

Therefore, $k_2 = d - 2$ or $k_2 = d - 1$, from which our claim follows.

Claim 2: Let $d|n$, $3|d$, and $d \neq 3$. Then $n - \frac{n}{d} \in S(G,3)$.

Proof of Claim 2: Using the notation in Lemma 1.4, let $H \leq G$ be of index d, and let $\phi : G \to G/H$ be the canonical map. We construct a subset B of G/H, such that $|B| = \frac{d}{3}$ and $|3B| = d - 1$. Let K be a subgroup of G/H of index 3. We define

$$B = (K \setminus \{k\}) \cup \{g\},$$

where $k \in K$ and $g \in (G/H) \setminus K$ are arbitrary elements. Note that d has no divisors congruent to $2 \pmod 3$, since d divides n. Therefore $6 \nmid d$, and $d \geq 9$. It follows that $d = 3 + 6k$ for some $k \in \mathbb{N}$, and

$$|K \setminus \{k\}| = \frac{d}{3} - 1 = 2k \geq k + 1 = \left\lfloor \frac{d}{6} \right\rfloor + 1 = \chi(K,2).$$

So $2(K \setminus \{k\}) = K$, and $3(K \setminus \{k\}) = K$. So

$$3B = 3(K \setminus \{k\}) \cup (2(K \setminus \{k\}) + g) \cup ((K \setminus \{k\}) + 2g) = G \setminus \{k + 2g\}.$$

So $|3B| = d - 1$. Using the notation of Lemma 1.4, let $A = \phi^{-1}(B)$. Then $|A| = \frac{n}{d}|B| = \frac{n}{3}$, and

$$|3A| = \frac{n}{d}|3B| = n - \frac{n}{d}.$$

This concludes the proof of our claim.

Claim 3: $\frac{2n}{3} \notin S(G,3)$.

Proof of Claim 3: Let H be the stabilizer subgroup of $3A$. With the notation of Lemma 1.3, let A and $3A$ consist respectively of k_1 and k_2 cosets of H. Let d denote the index of H. Assume that $|3A| = \frac{2n}{3}$. Just like before, we see that $3k_1 = d$, and $k_2 \geq d-2$. We find

$$\frac{2n}{3} = \frac{k_2 n}{d} \geq n - \frac{2n}{d}.$$

So $d \leq 6$. Note however, that $3|d$ and d has no divisors congruent to 2 (mod 3). So $d = 3$. Therefore $k_1 = 1$, and A is a coset of H. This implies that $3A$ is also a coset of H, so $k_2 = 1$. It follows that $|3A| = \frac{n}{3}$, which is a clear contradiction. So $\frac{2n}{3} \notin S(G,3)$.

Claim 4: Let $d|n$ such that $\nu_3(d) > \nu_3(n_r)$. Then $n - \frac{2n}{d} \notin S(G,3)$.

Proof of Claim 4: Assume, for contradiction, that $|A| = \frac{n}{3}$ and $|3A| = n - \frac{2n}{d}$. With the notation of Lemma 1.3, let H be the stabilizer subgroup of $3A$. Let $A, 3A$ consist respectively of k_1, k_2 cosets of H. Let d_1 denote the index of H. Then $3k_1 = d_1$, and

$$n - \frac{2n}{d} = |3A| = \frac{k_2 n}{d_1},$$

so $d_1 - \frac{2d_1}{d} = k_2 \geq 3k_1 - 2 = d_1 - 2$. Therefore $d|2d_1$, but $d \geq d_1$. This implies that $d = d_1$ or $d = 2d_1$. However, d is odd since all prime divisors are odd, so $d \neq 2d_1$. So $d = d_1$.

Let $\phi : G \to G/H$ be the canonical map. We write $G' = G/H$ and $B = \phi(A)$. Using Lemma 1.4 we get $|G/H| = d$, $|B| = \frac{d}{3}$ and $|3B| = d-2$. Let $\{x,y\} = G' \setminus (3B)$. We will show that the stabilizer subgroup H of $3B$ is trivial. For the sake of contradiction, let $g \in H$ such that g is not the identity element. Assume that $x - g \notin 3B$. Then $x - g = y$, since $x - g \neq x$. Note that $y - g \neq y$, while $y - g \neq y + g = x$. Therefore $y - g \in 3B$, while $g + y - g = y \notin 3B$. This is a contradiction, so the stabilizer subgroup of $3B$ contains only the identity element and is trivial.

Since the stabilizer of $3B$ is trivial, so is the stabilizer of $2B$. By Corollary 1.2 it follows that $|2B| \geq 2|B| - 1$, so

$$|G' \setminus (2B)| = |G'| - |2B| \leq |G'| - 2|B| + 1 = \frac{d}{3} + 1.$$

Note that $x - B \not\subseteq 2B$, and therefore $x - B \subseteq G' \setminus (2B)$ and similarly $y - B \subseteq G' \setminus (2B)$. Since $|x - B| = |y - B| = \frac{d}{3}$, we know that

$$|(x - B) \cup (y - B)| \geq \frac{d}{3} - 1.$$

Now let $l = x - y$, $K = \langle l \rangle$, and $|K| = k$. Then

$$|B \cap (B + l)| = |(x - B) \cap (y - B)| \geq |B| - 1.$$

So either $|B \cap (B + l)| = |B|$ or $|B \cap (B + l)| = |B| - 1$.

Let $|B \cap (B + l)| = |B|$. Then $B + l = B$. We write $B = \{b_1, ..., b_{\frac{d}{3}}\}$. Let $1 \leq i \leq \frac{d}{3}$. Then there exists some $1 \leq j \leq \frac{d}{3}$ such that $l + b_i = b_j$. Therefore, $b_i, b_i + l, b_i + 2l, ..., b_i + (k-1)l$ are distinct elements of B. It follows that B is a union of cosets of K.

We say that some subset $C \subseteq G$ is an arithmetic progression of difference l and size r if

$$C = \{g + jl : r_0 \leq j \leq r_0 + r - 1\},$$

for some $0 \leq r_0 \leq k - r$. Note that C is a coset of K if and only if $r = k - 1$. Let $|B \cap (B + l)| = |B| - 1$. Let $g \in B \setminus B + l$. Then $g, g + l, ..., g + (k - 1)l$ are distinct elements of B, while $B + l$ is a union of arithmetic progressions, each of difference l and all of them size k.

Either way, we conclude that B is a union of arithmetic progressions, each of difference l and at most one of them size less than k. Note that K is a subgroup generated by a single element, therefore $K \cong \mathbb{Z}_k$, and $k|n_r$. Since $\nu_3(d) > \nu_3(n_r)$, we have $n_r|\frac{d}{3}$, so $k||B|$. Therefore B is a union of full cosets of K, and so is $3B$. So $d-2$ is divisible by k, and d is divisible by k. Thus $k \leq 2$, but k is odd since all prime divisors of n are not congruent to 2 (mod 3). So $k = 1$, which is a contradiction if $x \neq y$. So $n - \frac{2n}{d} \notin S(G, 3)$.

Claim 5: Let $d|n$ such that $1 \leq \nu_3(d) \leq \nu_3(n_r)$. Then $n - \frac{2n}{d} \in S(G, 3)$.

Proof of Claim 5: Let G be of type $(n_1, ..., n_r)$. Note that $d = 3^{\nu_3(d)} p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, where for all $1 \leq i \leq k$, $p_i \equiv 1 \pmod 3$ is prime and $r_i \in \mathbb{N}$. Therefore, we can find positive integers $d_1, ..., d_r$ with the following properties:

a. $d_j|n_j$ for each $1 \leq j \leq r$, and $3^{\nu_3(d)}|d_r$.

b. $d_1 d_2 \cdots d_r = d$.

c. $d_j \equiv 1 \pmod 3$ for each $1 \leq j \leq r - 1$.

We then have

$$\frac{d}{3} = \frac{d_r}{3} + \sum_{k=1}^{r-1} \frac{d_k - 1}{3} d_{k+1} \cdots d_r.$$

This can be realised by noting that

$$d = d_1 d_2 \cdots d_r = d_1 d_2 \cdots d_r - d_2 \cdots d_r + d_2 \cdots d_r - ... - d_r + d_r = d_r + \sum_{k=1}^{r-1} (d_k - 1) d_{k+1} \cdots d_r.$$

Now let H be a subgroup of G of type $(\frac{n_1}{d_1}, ..., \frac{n_r}{d_r})$. Then $K = G/H$ is of type $(d_1, ..., d_r)$. Let $\phi : G \to K$ be the corresponding canonical map. With the notation of Proposition 1.6, we see that

$$|h\mathcal{I}(K, \frac{d}{3})| = d - 2.$$

Let $A = \phi^{-1}(\mathcal{I}(K, \frac{d}{3}))$. By Lemma 1.4, it follows that $|A| = \frac{n}{d}\frac{d}{3} = \frac{n}{3}$. Also

$$|3A| = \frac{n}{d}(d - 2) = \frac{n - 2n}{d}.$$

This concludes the proof of our claim.

Using every claim, we quickly realize that

$$S(G, 3) = \{n - \frac{n}{d} : d|n, 3|d, d \neq 3\} \cup \{n - \frac{2n}{d} : d|n, 1 \leq \nu_3(d) \leq \nu_3(n_r)\},$$

which concludes our proof. $\square$

We will now distinguish the case where all divisors of n are congruent to 1 (mod 3) using two theorems.

Theorem 4.4. *Let G be a finite abelian group of order n. Assume that all divisors of n are congruent to 1 (mod 3), and that $G \not\cong \mathbb{Z}_7^r$ for all $r \geq 1$. Then*

$$S(G,3) = \{n-3, n-1\}.$$

Proof. By Corollary 4.1, we have $\chi(G,3) = \frac{n-1}{3} + 1$. Let $A \subseteq G$ such that $|A| = \frac{n-1}{3}$. We show the result using three claims.

Claim 1: $S(G,3) \subseteq \{n-3, n-2, n-1\}$.

Proof of Claim 1: Using the notation of Lemma 1.3, let H be the stabilizer subgroup of $3A$ with index d, and let A and hA consist respectively of k_1 and k_2 cosets of H. Then $\frac{d(n-1)}{3} = k_1 n$, so $n | \left(d \cdot \frac{n-1}{3}\right)$. Note that $\gcd(n, \frac{n-1}{3}) = 1$, since the greatest common divisor must divide both n and $n-1$. Therefore we can apply Euclids lemma, from which it follows that $n|d$. Therefore $n = d$ and $k_1 = \frac{n-1}{3}$. By Lemma 1.3, we have

$$|3A| = \frac{k_2 n}{d} = k_2 \geq 3k_1 - 2 = n - 3.$$

Since $|3A| < n$, we conclude that $S(G,3) \subseteq \{n-3, n-2, n-1\}$.

Claim 2: $\{n-3, n-1\} \subseteq S(G,3)$.

Proof of Claim 2: Let G be of type $(n_1, ..., n_r)$. Note that for each $1 \leq i \leq r$, we have $n_i \equiv 1$ (mod 3), and therefore

$$\frac{n-1}{3} = \sum_{k=1}^{r} \frac{n_k - 1}{3} n_{k+1} \cdots n_r.$$

Note that all divisors of n_r are congruent to 1 (mod 3), and that $n_r \neq 7$, so $n_r \geq 13$, and therefore $\frac{n_r-1}{3} \geq 3$. By Proposition 1.6 we have $|h\mathcal{I}(G, \frac{n-1}{3})| = n-3$, and $|h\mathcal{I}^*(G, \frac{n-1}{3})| = n-1$. So $\{n-3, n-1\} \subseteq S(G,3)$.

Claim 3: $n-2 \notin S(G,3)$.

Proof of Claim 3: Assume that $|3A| = n-2$, while $|A| = \frac{n-1}{3}$. We write $3A = G \setminus \{x, y\}$, with some $x, y \in G$, $x \neq y$. Let d be the size of the stabilizer subgroup of $3A$. With Lemma 1.3, we see that $d | \frac{n-1}{3}$, thus $d|(n-1)$, and that $d|(n-2)$. Therefore $d = 1$ and the stabilizer subgroup is trivial. It follows that the stabilizer of $2A$ is also trivial, and with Corollary 1.2 we get $|2A| \geq 2|A| - 1$. It follows that

$$|G \setminus 2A| = |G| - |2A| \leq |G| - 2|A| + 1 = n - \frac{2n-2}{3} + 1 = |A| + 2.$$

Note that $x - A \subseteq G \setminus 2A$, since otherwise $x \in 3A$. Similarly $y - A \subseteq G \setminus 2A$. Since $|x-A| = |A| = |y-A|$, and since $(x-A) \cup (y-A) \subseteq G \setminus 2A$, we get $|(x-A) \cap (y-A)| \geq |A| - 2$, since otherwise we would have

$$|A| + 2 < |(x-A) \cup (y-A)| \leq |G \setminus 2A| \leq |A| - 2,$$

which is a contradiction. Now let $l = x - y$, $K = \langle l \rangle$ and $|K| = k$. Note that

$$|A \cap (A + l)| = |(x-A) \cap (y-A)| \geq |A| - 2.$$

Therefore A is a union of arithmetic progressions, with difference l, and at most two of them have size less than k. Now note that $k|n$, therefore $k \equiv 1 \pmod 3$ and $km = n$ for some $m \in \mathbb{N}$, so

$$|A| - \frac{k-1}{3} = \frac{n-1}{3} - \frac{k-1}{3} = \frac{km-k}{3} = k\frac{m-1}{3}.$$

So $k|(|A| - \frac{k-1}{3})$, and therefore $|A| \equiv \frac{k-1}{3} \pmod k$. This leaves us with the following cases which we will all contradict.

Case 1: A is a union of full cosets of K, and one arithmetic progression of size $\frac{k-1}{3}$.

Case 2: A is a union of full cosets of K, and two disjoint arithmetic progression in different cosets. The sizes of these sets add up to $\frac{k-1}{3}$ or $k + \frac{k-1}{3}$.

Case 3: A is a union of full cosets of K, and two disjoint arithmetic progression in the same coset. The sizes of these sets add up to $\frac{k-1}{3}$.

For Case 1, let $C = \{g + jl : r_0 \leq j \leq r_0 + \frac{k-1}{3} - 1\}$ be the arithmetic progression. Then

$$3C = \{3g + jl : 3r_0 \leq j \leq 3r_0 + k - 4\}$$

We conclude that $|3C| = k - 3$, so $|3A| \equiv k - 3 \pmod k$, since $3A$ is for the rest made up of full cosets. However, $|3A| = n - 2 \equiv k - 2 \pmod k$, so this is a contradiction.

For Case 2, let $B_1, B_2 \subseteq G$ be two arithmetic progressions in different cosets, respectively of size r_1 and r_2. We write

$$B_1 = \{b_1 + m_1 l : s_1 \leq m_1 \leq s_1 + r_1 - 1\}, \quad B_2 = \{b_2 + m_2 l : s_2 \leq m_2 \leq s_2 + r_2 - 1\},$$

for some $b_1, b_2 \in G$ with $b_1 \neq b_2$ $0 \leq s_1 \leq k - r_1$ and $0 \leq s_2 \leq k - r_2$. We find that

$$3B_1 \subseteq 3b_1 + K, \quad 2B_1 + B_2 \subseteq 2b_1 + b_2 + K, \quad B_1 + 2B_2 \subseteq b_1 + 2b_2 + K, \quad 3B_2 \subseteq 3b_2 + K.$$

We find that all these sets are within distinct cosets of K. Note that $|3B_1| = 3r_1 - 2$, $|2B_1 + B_2| = 2r_1 + r_2 - 2$, $|B_1 + 2B_2| = r_1 + 2r_2 - 2$ and $|3B_2| = 3r_2 - 2$. We assume that $r_1 + r_2 = \frac{k-1}{3}$. Then each of these sets has size less than k, and therefore

$$|3B_1| + |2B_1 + B_2| + |B_1 + 2B_2| + |3B_2| = 6(r_1 + r_2) - 8 = 2k - 10.$$

Note that

$$n - 2 = |3A| \equiv |3B_1| + |2B_1 + B_2| + |B_1 + 2B_2| + |3B_2| \pmod k,$$

and therefore $n - 2 \equiv 2k - 10 \equiv -10 \pmod k$, so $n + 8 \equiv 0 \pmod k$, while $k|n$. This implies that $k|8$, and since $k \equiv 1 \pmod 3$ and $k > 1$ we know that $k = 4$. This implies however that $2|n$, which is a contradiction since all divisors of n are congruent to $1 \pmod 3$.

Now we assume that $r_1 + r_2 = k + \frac{k-1}{3}$. Assume without loss of generality that $r_1 \geq r_2$. Then

$$3r_1 - 2 \geq 2r_1 + r_2 - 2 \geq r_1 + 2r_2 - 2 = k + \frac{k-1}{3} + r_2 - 2 \geq k.$$

Therefore $|3B_1| \geq |2B_1 + B_2| \geq |B_1 + 2B_2| \geq k$. So $3B_1, 2B_1 + B_2, B_1 + 2B_2$ are subsets of cosets of K with size at least k. It follows that they have size k. Now assume that

$3r_2 - 2 = |3B_2| < k$. Then

$$n - 2 = |3A| \equiv 3r_2 - 2 \pmod{k}.$$

Note however, that $k \nmid 3r_2$, because otherwise $k = 3r_2$ since $3r_2 - 2 < k$ and $k \geq 7$. But this contradicts $3 \nmid k$. Therefore $k \nmid 3r_2$ while $k|n$, so this is a contradiction. Now assume that $3r_2 - 2 \geq k$. Then $n - 2 \equiv 0 \pmod{k}$, and since $k > 1$ we have $k = 2$ which is a contradiction. This completes our second case.

We now look at Case 3. Let B_1, B_2 be two disjoint arithmetic progressions that are in the same coset, with $|B_1| + |B_2| = \frac{k-1}{3}$. Note that since K is cyclic, $K \cong \mathbb{Z}_k$. Let I_1, I_2 be two disjoint arithmetic progressions in $\mathbb{Z}_k$ with $|I_1| + |I_2| = \frac{k-1}{3}$. We will show that $|3(I_1 \cup I_2)| \neq k - 2$. Without loss of generality, we assume that

$$I_1 = \{0, 1, ..., r_1 - 1\}, \quad I_2 = \{s, s + 1, ..., s + r_2 - 1\},$$

for some $r_1, r_2, s \in \mathbb{Z}_k$ such that $r_1 + r_2 = \frac{k-1}{3}$, $r_1 \geq r_2$ and $r_1 + 1 \leq s \leq k - r_2 - 1$. We also assume that $s \leq \frac{k-1}{3} + r_1$ which interests the two gaps between I_1 and I_2. This makes it so that

$$|\{r_1, r_1 + 1, ..., s - 1\}| \leq |\{s + r_2, s + r_2 + 1, ..., k - 1\}|.$$

We can assume this without loss of generality since the case $s < \frac{k-1}{3} + r_1$ is equivalent to the case $s > \frac{k-1}{3} + r_1$. The set $|3(I_1 \cup I_2)| \neq k - 2$ is now a union of the following sets:

$$\begin{aligned} 3I_1 &= \{0, 1, ..., 3r_1 - 3\}, \\ 2I_1 + I_2 &= \{s, s + 1, ..., s + 2r_1 + r_2 - 3\}, \\ I_1 + 2I_2 &= \{2s, 2s + 1, ..., 2s + r_1 + 2r_2 - 3\}, \\ 3I_2 &= \{3s, 3s + 1, ..., 3s + 3r_2 - 3\}. \end{aligned}$$

We distinguish three subcases to show that $|3(I_1 \cup I_2)| \neq k - 2$.

Subcase 1: Let $r_1 + 1 \leq s \leq \frac{k-1}{3} + r_2 - 2$. Since $r_1 + r_2 = \frac{k-1}{3}$ and $r_2 \leq r_1$ we then obtain the following inequalities:

$$\begin{aligned} s &\leq \tfrac{k-1}{3} + r_2 - 2 = r_1 + 2r_2 - 2 \leq 3r_1 - 2, \\ 2s &\leq s + \tfrac{k-1}{3} + r_2 - 2 = s + r_1 + 2r_2 - 2 \leq s + 2r_1 + r_2 - 2, \\ 3s &\leq 2s + \tfrac{k-1}{3} + r_2 - 2 = 2s + r_1 + 2r_2 - 2, \\ k - 1 &= 3r_1 + 3r_2 \leq 3s + 3r_2 - 3. \end{aligned}$$

It follows that $3I_1 \cup (2I_1 + I_2) \cup (I_1 + 2I_2) \cup 3I_2 = \mathbb{Z}_k$, and therefore $|3(I_1 \cup I_2)| = k \neq k - 2$. So this is a contradiction.

Subcase 2: Let $\frac{k-1}{3} + r_2 - 1 \leq s \leq \frac{k-1}{3} + r_1 - 2$. Then

$$\begin{aligned} s &\leq \tfrac{k-1}{3} + r_1 - 2 = 2r_1 + r_2 - 2 \leq 3r_1 - 2, \\ 2s &\leq s + \tfrac{k-1}{3} + r_1 - 2 = s + 2r_1 + r_2 - 2. \end{aligned}$$

So $3I_1 \cup (2I_1 + I_2) \cup (I_1 + 2I_2) = \{0, 1, ..., 2s + r_1 + 2r_2 - 3\}$. Now we have

$$2s + r_1 + 2r_2 - 3 \geq \frac{2k - 2}{3} + 2r_2 - 2 + r_1 + 2r_2 - 3 = k + 3r_2 - 6 \geq k - 3.$$

If either of these inequalities is a strict inequality, we have $3I_1 \cup (2I_1 + I_2) \cup (I_1 + 2I_2) = \mathbb{Z}_k \setminus \{k-1\}$ or $3I_1 \cup (2I_1 + I_2) \cup (I_1 + 2I_2) = \mathbb{Z}_k$, so $|3(I_1 \cup I_2)| > k - 2$. If both inequalities are equalities, then $r_2 = 1, s = \frac{k-1}{3}$ and $r_1 = \frac{k-4}{3}$. Therefore $3I_2 = \{k-1\}$. So $3(I_1 \cup I_2) = \mathbb{Z}_k \setminus \{k-2\}$, and $|3(I_1 \cup I_2)| \neq k-2$.

Subcase 3: Let $\frac{k-1}{3} + r_1 - 1 \leq s$. Note that from our assumption, $s \leq \frac{k-1}{3} + r_1$ and that $r_1 \geq \frac{k-1}{6}$. First we look at the case where $r_1 \geq \frac{k-1}{6} + 1$. Then $s \leq \frac{k-1}{3} + r_1 \leq 2r_1 - 2 + r_1 = 3r_1 - 2$. Therefore

$$3I_1 \cup (2I_1 + I_2) = \{0, 1, ..., s + 2r_1 + r_2 - 3\}.$$

If $s + r_1 \geq \frac{2k-2}{3} + 2$, we have

$$s + 2r_1 + r_2 - 3 \geq \frac{2k-2}{3} + 2 + \frac{k-1}{3} - 3 = k-2,$$

so $\mathbb{Z}_k \setminus \{k-1\} \subseteq 3(I_1 \cup I_2)$ and $|3(I_1 \cup I_2)| \geq k-1$. If $s + r_1 \leq \frac{2k-2}{3} + 1$, then

$$\frac{2k-2}{3} + 1 \geq s + r_1 \geq \frac{k-1}{3} + 2r_1 - 1.$$

This is equivalent to $\frac{k-1}{6} + 1 \geq r_1$, but $\frac{k-1}{6} + 1 \leq r_1$, so $\frac{k-1}{6} + 1 = r_1$ and $s = \frac{k-1}{2}$. We conclude that $3I_1 \cup (2I_1 + I_2) = \{0, 1, ..., s + 2r_1 + r_2 - 3\} = \{0, ..., k-3\}$, while $k-1 \in I_1 + 2I_2$. So $|3(I_1 \cup I_2)| \geq k-1 > k-2$. So this is a contradiction.

Now we look at the case where $r_1 = \frac{k-1}{6} = r_2$. Then

$$\frac{k-3}{2} = \frac{k-1}{3} + r_1 - 1 \leq s \leq \frac{k-1}{3} + r_1 \leq \frac{k-1}{2}.$$

Therefore $s = \frac{k-3}{2}$ or $s = \frac{k-1}{2}$. Assume that $s = \frac{k-3}{2}$. We find that

$$\begin{aligned} 3I_1 &= \{0, ..., \tfrac{k-3}{2} - 2\}, \\ 2I_1 + I_3 &= \{\tfrac{k-3}{2}, ..., k-5\}, \\ I_1 + 2I_2 &= \{k-3, ..., k + \tfrac{k-3}{2} - 5\}, \\ 3I_2 &= \{\tfrac{k-3}{2} - 3, ..., k-8\}. \end{aligned}$$

For $k = 7$, this means that $3(I_1 \cup I_2) = \{0, 2, 4, 6\}$, so $|3(I_1 \cup I_2)| \neq k-2$. We now look at the elements that are not in these sets. When $k > 7$, we find that $\frac{k-3}{2} - 1 \in 3I_2$, and $\frac{k-3}{3} - 4 \in 3I_1$. For $1 \leq i \leq 7$ and $i \neq 4$, we have $k - i \in 2I_1 + I_2$ or $k - i \in I_1 + 2I_2$, while $k-4$ is not present in any of these sets. We conclude that $3(I_1 \cup I_2) = \mathbb{Z}_k \setminus \{k-4\}$.
Let $s = \frac{k-1}{2}$. We find that

$$\begin{aligned} 3I_1 &= \{0, ..., \tfrac{k-1}{2} - 3\}, \\ 2I_1 + I_3 &= \{\tfrac{k-1}{2}, ..., k-4\}, \\ I_1 + 2I_2 &= \{k-1, ..., k + \tfrac{k-1}{2} - 4\}, \\ 3I_2 &= \{\tfrac{k-1}{2} - 1, ..., k-5\}. \end{aligned}$$

We look at the elements that are not in these sets. We find that $\frac{k-1}{2} - 1 \in 3I_2$, and $\frac{k-1}{2} - 3 \in 3I_1$. Furthermore $k-4 \in 2I_1 + I_2$, while $k-1 \in I_1 + 2I_2$. We find that $\frac{k-1}{2} - 2, k-3, k-2 \notin 3(I_1 \cup I_2)$, so $3(I_1 \cup I_2) = \mathbb{Z}_k \setminus \{\frac{k-1}{2} - 2, k-3, k-2\}$.
So for each two disjoint arithmetic progressions $I_1, I_2 \subseteq \mathbb{Z}_k$ with $|I_1| + |I_2| = \frac{k-1}{3}$ we have $|3(I_1 \cup I_2)| \neq k-2$. Since $K \cong \mathbb{Z}$, we can find such I_1, I_2 such that $|3(B_1 \cup B_2)| = |3(I_1 \cup I_2)| \neq k-2$. This completes our proof for Case 3. Since we have distinguished all the cases, it follows

that $n-2 \notin S(G,3)$. Using all our claims, we obtain

$$S(G,3) = \{n-3, n-1\}.$$

This completes our proof. $\square$

The only groups left to treat are $\mathbb{Z}_7^r$ for $r \in \mathbb{N}$. We have distinguished this case because part (2) of Proposition 1.6 can not be applied. Since the type is $(7, ..., 7)$, we find that

$$\chi(\mathbb{Z}_7^r, 3) - 1 = \frac{n-1}{3} = \sum_{k=1}^{r} q_k n_{k+1} \cdots n_r = \sum_{k=1}^{r} 2n_{k+1} \cdots n_r.$$

So $q_r = 2 < 3$, and part (2) is not applicable.

Theorem 4.5. Let $G \cong \mathbb{Z}_7^r$ for some $r \in \mathbb{N}$. Then

$$S(G,3) = \{n-3\}.$$

Proof. We first prove the following claim.
Claim. Let $r \in \mathbb{N}$, and let 0 denote the identity element of $G = \mathbb{Z}_7^r$. Let A be a subset of G such that $|A| = \frac{7^r-1}{3}$ and $0 \notin 3A$. Then there is an ascending chain of subgroups

$$\{0\} = H_0 < H_1 < \cdots < H_r = G$$

and elements $a_0, a_0' \in H_1$, $a_k \in H_{k+1} \setminus H_k$ for $1 \le k \le r-1$, such that

$$A = \{a_0, a_0'\} \cup \bigcup_{k=1}^{r-1} (\{a_k, 2a_k\} + H_k).$$

Proof of Claim: First, we show that $\mathbb{Z}_7^r$ has $\frac{7^r-1}{6}$ subgroups of index 7. We identify with the r-dimiensional vector space over $\mathbb{Z}_7$. For any $1 \le k \le r$, the number of k-dimensional subspaces is given by the Gaussian binomial coefficient [6]

$$\binom{r}{k}_7 = \frac{(1-7^r)(1-7^{r-1})\cdots(1-7^{r-k+1})}{(1-7^k)(1-7^{k-1})\cdots(1-7)}.$$

Now note that the number of subgroups of $\mathbb{Z}_7^r$ with index 7 is equal to the number of $(r-1)$-dimensional subspaces of the r-dimensional vector space over $\mathbb{Z}_7$. Therefore, we find that the number of subgroups of index 7 is

$$\binom{r}{r-1}_7 = \frac{(1-7^r)(1-7^{r-1})\cdots(1-7^2)}{(1-7^{r-1})(1-7^{k-1})\cdots(1-7)} = \frac{1-7^r}{1-7} = \frac{7^r-1}{6}.$$

Let $A \subseteq \mathbb{Z}_7^r$ such that $|A| = \frac{7^r-1}{3}$ and $0 \notin A$. We show that for any subgroup H of G we have $|A \cap H| = \frac{|H|-1}{3}$. By Corollary 4.1 we have

$$\chi(H,3) = \frac{|H|-1}{3} + 1.$$

Note that $|A \cap H| \le \frac{|H|-1}{3}$, since otherwise we have $H \subseteq A$, which contradicts $0 \notin 3A$. So we need to show that $|A \cap H| \geq \frac{|H|-1}{3}$. This holds trivially for $|H| = 1$. For $|H| = 7$, observe that the collection of *pierced lines*

$$\{H \setminus \{0\} : H \leq G, |H| = 7\}$$

forms a partition of $G \setminus \{0\}$. Note that G has $\frac{7^r-1}{6}$ subgroups of order 7. Since every element $g \in \mathbb{Z}_7^r \setminus \{0\}$ has order 7, $\langle g \rangle$ is a unique subgroup of order 7. By not counting the identity element, we obtain $\frac{7^r-1}{6}$ subgroups of order 7. For each such subgroup H, we have $|A \cap (H \setminus \{0\})| = |A \cap H| \leq \frac{|H|-1}{3} = 2$. Now assume that there exists some subgroup H of order 7 of G, such that $|H \cap A| < 2$. Then

$$\frac{7^r - 1}{3} = |A| = |A \cap (G \setminus \{0\})| = \bigcup_{H \leq g, |H|=7} |A \cap (H \setminus \{0\})| < 2 \left(\frac{7^r - 1}{6} \right),$$

which is a clear contradiction, so $|A \cap H| = 2 = \frac{|H|-1}{3}$ for all subgroups H of size 7. Note that for every subgroup H of G, $H \setminus \{0\}$ is the disjoint union of $\frac{|H|-1}{6}$ pierced lines, each of size $7 - 1 = 6$. It follows that

$$|A \cap H| = 2 \left(\frac{|H| - 1}{6} \right) = \frac{|H| - 1}{3}.$$

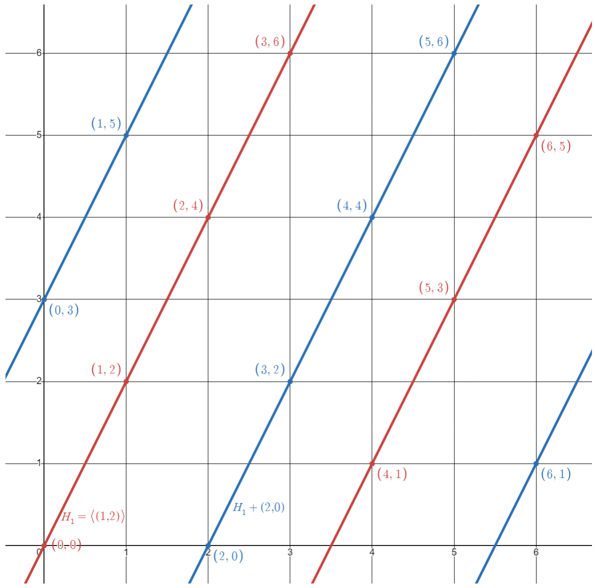
We are now ready to prove our claim. For $r = 1$, we have $\{0\} = H_0 < H_1 = \mathbb{Z}_7$. Let $A \subseteq \mathbb{Z}_7$ with $|A| = 2$. We pick $a_0, a_0' \in A$ and find that $A = \{a_0, a_0'\}$, which completes this case.

We consider $r = 2$. Let A be a subset of $\mathbb{Z}_7^2$ of size $\frac{7^2-1}{3} = 16$, and let $0 \notin 3A$. Let $H \leq G$ with index 7. We show that there are at most two distinct cosets of H that contain 3 or more elements of A. Assume for contradiction that cosets C_1, C_2, C_3 each contain at least 3 elements of A. Then $\chi(G/H, 3) = \chi(\mathbb{Z}_7, 3) = 3$, so any subset of G/H of size 3 is 3-complete. Since $\{C_1, C_2, C_3\} \subseteq G/H$ has size 3, we find that $3\{C_1, C_2, C_3\} = G/H$. Since $H \in G/H$ we can find (not necessarily distinct) indices $i, j, k \in \{1, 2, 3\}$ such that $C_i + C_j + C_k = H$. We write $A_i = A \cap C_i$, $A_j = A \cap C_j$, $A_k = A \cap C_k$, and let K be the stabilizer subgroup of $A_1 + A_2 + A_3$ in H. Since K is a subgroup of H, and $|H| = 7$, we know that either $|K| = 7$ or K is trivial. Note that $0 \notin A$, so $0 \notin A_i + A_j + A_k$, and that the sizes of these sets are all greater or equal to 3. Therefore $K \neq H$, so K is trivial. Then by Corollary 1.2 we have

$$6 \geq |A_i + A_j + A_k| \geq |A_i| + |A_j| + |A_k| - 2|K| = |A_i| + |A_j| + |A_k| - 2 \geq 7,$$

which is a clear contradiction. So there are at most two distinct cosets of H that contain 3 or more elements of A.

Next we show that there exists a subgroup H of $\mathbb{Z}_7^2$ of order 7 such that one of its cosets contains at least 4 elements of A. Assume the contrary. Then for each subgroup H of order 7, two cosets contain 3 elements of A, while five cosets contain 2 elements of A, since $3 \cdot 2 + 2 \cdot 5 = 16 = |A|$. We identify $\mathbb{Z}_7^2$ with the 2-dimensional vector space over $\mathbb{Z}_7$. Then every subgroup of G of order 7 corresponds to a unique normal vector through $(0, 0)$, unique up to nonzero scalar multiplication. For example, lets look at $H_1 = \langle (1, 2) \rangle$. We find that this subgroup and its coset $H_1 + (2, 0)$ corresponds to the following lines in the 2-dimensional vector space over $\mathbb{Z}_7$:



We define an *affine line* as a coset of a subgroup of order 7. We find that the group G/H is the set of affine lines corresponding to the lines parallel to H in the 2-dimensional vector space over $\mathbb{Z}_7$. For every $g \in G$, there exists a subgroup of G containing g, so there exists an unique affine line containing $(0, 0)$ and g. Therefore, we find that for every two elements $g_1, g_2 \in G$, there exists a unique affine line that contains both g_1 and g_2. We now look at the set

$$S = \{(C, a, a') : C \text{ is an affine line in } G; a, a' \in C \cap A; a \neq a'\}.$$

After arbitrarily choosing $a, a' \in A$ such that $a \neq a'$, there exists a unique affine line that contains both a and a'. Therefore $|S| = |A| \cdot (|A| - 1) = 240$.
On the other hand, there are $\frac{7^r-1}{6} = \frac{7^2-1}{6} = 8$ subgroups of order 7. We partitioning the 56 affine lines into 8 parallel classes depending on which subgroup they correspond to. For each of these classes, two affine lines contain 3 elements of A, while five affine lines contain 2 elements of A. Therefore, for each class the number of suitable pairs a, a' is $6+6+2+2+2+2+2 = 22$, so $240 = |S| = 8 \cdot 22 = 176$, which is a contradiction.
So there exists a subgroup H of $\mathbb{Z}_7^2$ of order 7 such that one of its cosets contains at least 4 elements of A. We choose $c \in G \setminus H$, and let $C_i = ic + H$ for $0 \leq i \leq 6$ be the distinct cosets of H. Let $A_i = C_i \cap A$. Note that $|A \cap H| = \frac{|H|-1}{3} = 2$, so $|A_0| = 2$. We may assume without loss of generality that $|A_1| = \max\{|A_i|\}$, so $|A_1| \geq 4$. Let $i, j, k \in \{0, ..., 6\}$ such that $i + j + k \equiv 0 \pmod 7$, and assume that none of A_i, A_j or A_k is the emptyset. We show that and $|A_i| + |A_j| + A_k| \leq 8$. Assume the contrary. Note that $C_i + C_j + C_k = c(i+j+k) + H = H$, so $A_i + A_j + A_k \subseteq H$. Also, the stabilizer subgroup K of $A_i + A_j + A_k$ is either trivial or H, but $0 \notin A_i + A_j + A_k$, while $A_i + A_j + A_k \neq \emptyset$. So K is trivial. We conclude from Corollary 1.2 that

$$|A_i + A_j + A_k| \geq |A_i| + |A_j| + A_k| - 2|K| \geq 9 - 2 = 7.$$

So $A_i + A_j + A_k = H$, and $0 \in A_i + A_j + A_k$, which is a contradiction, so $|A_i| + |A_j| + A_k| \leq 8$ whenever A_i, A_j, A_k are not empty. We then find the following results:

- If $A_5 \neq \emptyset$, we find that $8 \geq 2|A_1| + |A_5| \geq 8 + |A_5|$, which implies that $A_5 = \emptyset$.
- If $A_6 \neq \emptyset$, we have $8 \geq |A_0| + |A_1| + |A_6| = 2 + |A_1| + |A_6|$. Note that if $|A_1| \geq 6$, we must have that $A_6 = \emptyset$, meaning that $A_6 \leq \max\{0, 6 - A_1\}$.

- If $A_3 \neq \emptyset$, we have $|A_1| + 2|A_3| \leq 8$, and thus $|A_3| \leq 4 - \frac{|A_1|}{2}$.
- If A_2 and A_4 are not empty, then $|A_2| + |A_4| \leq 8 - |A_1| \leq |A_1|$, since $4 \leq |A_1|$. If A_2 or A_4 is empty, this holds trivially since $|A_1| \leq 7$.

With these results, we have

$$16 = |A| = |A_0| + |A_1| + |A_3| + |A_5| + |A_6| + (|A_2| + |A_4| \leq \\ 2 + |A_1| + 4 - \tfrac{|A_1|}{2} + 0 + \max\{0, 6 - |A_1|\} + |A_1|.$$

This is equivalent with

$$20 \leq 3|A_1| + 2\max\{0, 6 - |A_1|\}.$$

Now assume that $|A_1| \leq 5$. Then we find that $20 \leq 15 + 2 = 17$, which is a contradiction. So $|A_1| \geq 6$, and therefore $20 \leq 3|A_1|$, and $|A_1| = 7$. Then our previous inequalities yield $A_3 = A_6 = \emptyset$, and therefore $16 = |A| = |A_0| + |A_1| + |A_2| + |A_4| = 9 + |A_2| + |A_4|$. So if A_2, A_4 are both not empty we have $7 = |A_2| + |A_4| \leq 8 - |A_1| = 1$. It follows either A_2 or A_4 is empty, and the other is a full coset. Assume without loss of generality that $A_2 = C_2$.
We now set $H_1 = H$, $\{a_0, a_0'\} = A_0$, and $a_1 = c$. Then

$$A = A_0 \cup C_1 \cup C_2 = \{a_0, a_0'\} \cup (\{a_1, 2a_1\} + H_1),$$

which completes our proof for the case $r = 2$.

We will now use induction to show that the claim holds for $r \geq 3$. Assume that the statement holds for $r - 1$, so for each subset B of size $\frac{7^{r-1}-1}{3}$ with $0 \notin 3B$ there is an ascending chain of subgroups of G

$$\{0\} = H_0 < H_1 < \cdots < H_{r-1}$$

and elements $a_0, a_0' \in H_1$, $a_k \in H_{k+1} \setminus H_k$ for $1 \leq k \leq r - 2$, such that

$$B = \{a_0, a_0'\} \cup \bigcup_{k=1}^{r-2} (\{a_k, 2a_k\} + H_k).$$

Recall that if a group G has type $(n_1, ..., n_s)$, then s is the rank of G. We say that a *flat of type* K is a coset of a subgroup K of rank $r - 2$ in $\mathbb{Z}_7^r$. We count the number of flats contained in A as follows. Note that $0 \notin A$, and therefore subgroups are not contained in A. So each flat F in A is no subgroup. Therefore $F = g + K$ for some subgroup K of rank $r - 2$, and some $g \notin K$. Since g has order 7, F generates a unique subgroup $\langle F \rangle$ of index 7. We know that $|\langle F \rangle \cap A| = \frac{\langle F \rangle - 1}{3} = \frac{7^{r-1}}{3}$. Since $\langle F \rangle \cap A$ is a subset of size $\frac{7^{r-1}}{3}$, we find that by our induction hypotheses $\langle F \rangle \cap A$ consists of two full flats and a part of a third, all of the same type. Therefore, $\langle F \rangle \cap A$ does not contain a third flat of any type, and thus contains a total of two flats. Since there are $\frac{7^r-1}{6}$ subgroups of index 7 in G, we find that A contains $2 \cdot \frac{7^r-1}{6} = \frac{7^r-1}{3}$ flats. We call these A-flats.
Note that not all A-flats are of the same type. Each subgroup of rank $r - 2$ has 49 cosets, of which at most 48 are in A since $0 \notin A$. Whenever $r \geq 3$, we find that $\frac{7^r-1}{3} \geq 114 > 48$, so there exist A-flats of different types. Let F_1 and F_2 be A-flats of types K_1 and K_2 respectively, with $K_1 \neq K_2$. We write $H = K_1 + K_2$. Note that H is a subgroup of G of index 7, since $K_1 + K_2 = G$ implies that $2F_1 + F_2 = G$, which contradicts $3A \neq G$. Let F be an arbitrary A-flat of type K. Then $K \leq H$, since otherwise $K + H = G$, so $F + F_1 + F_2 = G$, which contradicts $3A \neq G$. So H contains every subgroup of rank $r - 2$ that has a flat in A.
Now let $c \in G \setminus H$. The cosets of H are then given by $C_i = ic + H$ for $0 \leq i \leq 6$. Since

H contains every subgroup of rank $r-2$ that has a flat in A, every A-flat is contained entirely in one of the seven cosets of H. Let $\mathcal{F}_i$ be the union of A-flats in C_i. Note that $H \cap A$ is a subgroup of size $\frac{7^{r-1}-1}{3}$, so by our inductive hypothesis, H contains 2 A-flats, and they are of the same type. However, there has to be at least one coset of H that has at least two A-flats of different types: since all flats of the same type are disjoint, each coset of H contains at most 7 A-flats of the same type, and we have more than $2+6\cdot 7=44$ A-flats. Without loss of generality, assume that C_1 contains at least two different types of A-flats. Note that the sum of two flats of different types is an entire coset of H. Indeed, if g_1+K_3 and g_2+K_4 are flats of different types K_3 and K_4 respectively, then their sum is $g_1+g_2+K_3+K_4$, and since $K_3, K_4 \leq H$ we have $K_3+K_4=H$, so this is a coset of H. Therefore, $\mathcal{F}_6=\emptyset$, since otherwise $\mathcal{F}_0+\mathcal{F}_1+\mathcal{F}_6=C_0=H$, contradicting $0 \notin 3A$. Similarly, since $1+3+3 \equiv 1+1+5 \equiv 1+2+4 \equiv 0 \pmod 7$, we get $\mathcal{F}_3=\mathcal{F}_5=\emptyset$, and at least one of $\mathcal{F}_2$ or $\mathcal{F}_4$ is empty. So either $C_0 \cup C_1 \cup C_2$ or $C_0 \cup C_1 \cup C_4$ contain all A-flats. Assume without loss of generality that $C_0 \cup C_1 \cup C_2$ contains all A-flats. Note that $H \cong \mathbb{Z}_7^{r-1}$ has $\frac{7^{r-1}}{6}$ subgroups of index 7, and each coset of H contains at maximum 7 A-flats of the same type, so each coset of H has at maximum $7\cdot\frac{7^{r-1}}{6}$ A-flats. Since C_0 contains 2 A-flats, C_1 and C_2 must both contain $7\cdot\frac{7^{r-1}}{6}$ A-flats, since $2+2\cdot 7\cdot\frac{7^{r-1}}{6}=\frac{6}{3}+\frac{7^r-7}{3}=\frac{7^r-1}{3}$, which is the amount of A-flats. Note that if a cost of H contains 7 A-flats of the same type, then it is the disjoint union of these A-flats. Since C_1 and C_2 both contain 7 A-flats of the same type, we find that $A=(A\cap H)\cup C_1\cup C_2=(A\cap H)\cup(c+H)\cup(2c+H)$. Since $|A\cap H|=\frac{7^{r-1}-1}{3}$ we can apply the inductive hypothesis, so there is an ascending chain of subgroups

$$\{0\}=H_0<H_1<\cdots<H_{r-1}<H_r=G$$

and elements $a_0, a_0' \in H_1$, $a_k \in H_{k+1}\setminus H_k$ for $1 \leq k \leq r-2$, such that

$$A\cap H=\{a_0,a_0'\}\cup\bigcup_{k=1}^{r-2}(\{a_k,2a_k\}+H_k).$$

Note that $a_{r-2}\in H$, since otherwise we get $a_{r-2}+H_{r-2}\nsubseteq H$ while $a_{r-2}+H_{r-2}\subseteq H\cap A$. So $a_{r-2}\in H\setminus H_{r-2}$, and therefore $H_{r-1}=H$. When then choose $a_{r-1}=c$ and find that

$$A=(A\cap H)\cup(c+H)\cup(2c+H)=\{a_0,a_0'\}\cup\bigcup_{k=1}^{r-1}(\{a_k,2a_k\}+H_k).$$

This completes the proof of our claim.

Now let $A\subseteq G$ be 3-incomplete, so of size $\frac{n-1}{3}=\frac{7^r-1}{3}$. Since A is 3-incomplete, we know that $3A\neq G$. Let $g\in G\setminus 3A$. Note that each element of G has order 7, so $7\cdot g=0$. We let $B=2g+A$. Then $3B=6g+3A$, and since $g\notin 3A$ and since inverses are unique, we have $6\cdot g+g=7\cdot g=0\notin 3B$. Note that $|B|=|A|$, while $|3B|=|3A|$. With our claim we let

$$B=\{b_0,b_0'\}\cup\bigcup_{k=1}^{r-1}(\{b_k,2b_k\}+H_k)$$

for $H_0<\cdots<H_r$, $b_0,b_0'\in H_1$ and $b_k\in H_{k+1}\setminus H_k$ for $1\leq k\leq r-1$. Now note that $3(\{b_k,2b_k\}+H_k)=\{3b_k,4b_k,5b_k,6b_k\}+H_k$ for each k. Also, whenever $i>j$ we have $b_j,2b_j\in H_i$, and $H_j\subseteq H_i$, so

$$(\{b_i,2b_i\}+H_i)+2(\{b_j,2b_j\}+H_j)=(H_i+2\{b_j,2b_j\}+H_j)+\{b_i,2b_i\}=H_i+\{b_i,2b_i\}.$$

So $H_k + \{b_k, 2b_k\} \subseteq 3B$ for each k. Similarly, since $b_0, 2b_0 \in H_k$ for each k, we have $\{b_0, 2b_i\} + \{b_k, 2b_k\} + H_k = \{b_k, 2b_k\} + H_k$. We conclude that

$$3B = \{3b_0, 3b_0', 2b_0 + b_0', b_0 + 2b_0'\} \cup \bigcup_{k=1}^{r-1} (\{b_k, 2b_k, 3b_k, 4b_k, 5b_k, 6b_k\} + H_k).$$

Note that all these sets are disjoint. Therefore

$$|3B| = 4 + \sum_{k=1}^{r-1} 6 \cdot 7^k = 6 \cdot \sum_{k=0}^{r-1} 7^k - 2 = 6 \cdot \frac{1 - 7^r}{1 - 7} - 2 = 7^r - 3.$$

Note that $|3A| = |3B| = 7^r - 3$. We conclude that for each subset A of $\mathbb{Z}_7^r$ of size $\frac{7^r - 1}{3}$ we have $|3A| = 7^r - 3 = n - 3$. So $S(G, 3) = \{n - 3\}$. $\square$

Conclusion

In conclusion, we have determined the h-critical number for every $h \geq 1$, and the set of sizes of sumsets of nonbases of maximum size for $h = 2$ and $h = 3$. It is likely that it is more work to determining this set for greater h, since it is probable that more cases would have to be distinguished, based on Lemma 2.3.

This thesis was heavily inspired the work of B. Bajnok and P. P. Pach [1, 2]. Specifically, the lemmas and theorems concerning h-critical number are based on a paper by Béla Bajnok [1], while the sizes of sumsets of nonbases of maximum size for $h = 2$ and $h = 3$ are based on a paper by Béla Bajnok and Péter Pál Pach [2]. Results that I have provided myself include the proofs for Corollary 1.2, Lemma 1.4, Lemma 1.5, Proposition 1.6, Corollary 1.7, and Lemma 2.1.

References

[1] Béla Bajnok. The h-critical number of finite Abelian groups. *Unif. Distrib. Theory*, 10(2):93–115, 2015.

[2] Béla Bajnok and Péter Pál Pach. On sumsets of nonbases of maximum size. *European Journal of Combinatorics*, 2023.

[3] Matt DeVos. A short proof of Kneser's addition theorem for Abelian groups. In *Combinatorial and additive number theory—CANT 2011 and 2012*, volume 101 of *Springer Proc. Math. Stat.*, pages 39–41. Springer, New York, 2014.

[4] David Steven Dummit and Richard Martin Foote. *Abstract Algebra*, volume 3. Wiley, 2003.

[5] Martin Kneser. Abschätzung der asymptotischen dichte von summenmengen. *Mathematische Zeitschrift*, 58:459–484, 1953.

[6] John Konvalina. Generalized binomial coefficients and the subset–subspace problem. *Advances in Applied Mathematics*, 21(2):228–240, 1998.