On the Maximum Size of Zero-h-Sum-Free Sets In Finite Abelian Groups

Jacob Terkel

July 2021

Abstract

A zero-h-sum-free set is a subset of a group G such that no h (not necessarily distinct) elements in said subset sum to the identity element of G. In this paper, we investigate the question: "What is the largest possible size of a zero-h-sum-free set is a subset of a finite Abelian group G? Throughout this paper, we utilize ideas from Hamindoune, Plagne, Bajnok, and Matzke from a related topic as well as new ideas to answer this question for all cyclic G and a large portion of non-cyclic G for all h.

1 Introduction

First, we lay the groundwork for the contents of this paper

Definition 1. *An h-fold sumset of a set A, denoted as hA is the set of all sums of h not necessarily distinct elements in A.*

In [1] a very useful arithmetic function called "the v function" is utilized. In the realm of Additive Combinatorics, this function and variations of it appear quite often. This topic is no exception.

Definition 2. *The v function is defined as follows for positive integers g, n, h*

$$v_g(n,h) = \max\left\{\frac{n}{d}\left(\left\lfloor\frac{d-1-\gcd(d,g)}{h}+1\right\rfloor\right) \mid d \in D(n)\right\}$$

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

Regarding this function, we can utilize a specified version of a theorem of Bajnok's from [1] to assist us

Theorem 3. *(Theorem 4.4 from [1])*

$$v_h(n,h) = \begin{cases} \frac{n}{h}\cdot\max\left\{1+\frac{h-i}{\min(D_i(n,h))}\right\} \text{ for } i \in I(n,h) & I(n,h) \neq \emptyset \\ \left\lfloor\frac{n-1}{h}\right\rfloor & \text{Otherwise} \end{cases}$$

Where

$$D_i(n,h) = \{d \in D(n) \mid d = i \mod h, \gcd(d,h) < i\}$$

and

$$I(n,h) = \{i \in [0,h-1] \mid D_i(n,h) \neq \emptyset\}$$

Definition 4. *A set A is considered q-h-sum-free if and only if $q \notin hA$.*

Definition 5.

$$\tau(G,h,q) = \max\{|A| \mid A \in G, q \notin hA\}$$

In English, $\tau(G,h,q)$ is equal to the size of the largest q-h-sum-free subset of a group G.

Furthermore, when q is the identity element of G, we say that a q-h-sum-free subset of G is zero-h-sum-free, and we have the shorthand notation that $\tau(G,h,q) = \tau(G,h)$.

The objective of this paper is to determine as many values of $\tau(G,h)$ as we can. The next three statements below are give a brief summary with what is already known regarding $\tau(G,h)$.

Theorem 6. *(Theorem 13 from [5]) For prime p and and Abelian group G of order n*

$$\tau(G,p) = v_p(n,p)$$

(?)

* *Is not always true ($\mathbb{Z}_3^2$ for example), however my results do reinforce this for cyclic G, G of order n with at least one factor 2 mod* 3 *

Proposition 7. *(Corollary F.9 from [1]) For an Abelian group G of order n and exponent κ*

$$\frac{n}{\kappa} \cdot v_h(\kappa,h) \leq \tau(G,h) \leq v_1(n,h)$$

Theorem 8. *(Theorem F.12 from [1]) If n is relatively prime to h then $\tau(G,h) = v_1(n,h)$*

Below we will lay out some definitions which will be used in the proofs in subsequent sections.

Definition 9. *Let $\alpha_\tau(\mathbb{Z}_n,h,q)$ be equal to the largest q-h-sum-free arithmetic progression in $\mathbb{Z}_n$*

Definition 10. *Let $\gamma_\tau(\mathbb{Z}_n,h,q)$ be equal to the largest q-h-sum-free interval in $\mathbb{Z}_n$*

Below, we will list two results of Hamidoune and Plagne [2] which were especially helpful in this paper.

Theorem 11 (Theorem 2.1 from [2])**.** *Let A be a generating subset of an Abelian group G such that $|A| \leq \frac{|G|}{2}$ and $0 \in A$.*

Then there exists a subgroup of G, H where

$$|A+H| < \min(|G|, |H| + |A|)$$

and A/H is an arithmetic progression or a Vosper subset in G/H.

Where

Definition 12. *A set A is a Vosper subset of G if for any $X \subset G$ where $|X| \geq 2$*

$$|A+X| \geq \min(|G|-1, |A|+|X|)$$

Lemma 13 (Lemma 4.2 From [2])**.** *If B is a generating subset of G with $0 \in B$,*

$$|jB| \geq \min\left\{|G|, \left\lceil \frac{(j-1)|B|}{2} \right\rceil + |B|\right\}$$

In [2], Hamidoune and Plagne utilized these ideas, among others, to prove a theorem on (k,l)-sum-free sets (which we will not define in this paper, but curious readers should see Chapter G of [1]). We do the same, but for q-h-sum-free sets.

2 Results

Theorem 14. *Let $\delta = \gcd(n,h)$*

$$\gamma_\tau(\mathbb{Z}_d, h, q) = \left\lfloor \frac{d + q - 1 - \lceil \frac{1+q}{\delta} \rceil \cdot \delta}{h} \right\rfloor + 1$$

Theorem 15.

$$\max\left\{\alpha_\tau(\mathbb{Z}_d, h, q)\frac{n}{d} \mid d \in D(n)\right\} = \max\left\{\gamma_\tau(\mathbb{Z}_d, h, q)\frac{n}{d} \mid d \in D(n)\right\}$$

Specifically, it is important to recognize that

$$\max\left\{\alpha_\tau(\mathbb{Z}_d, h, 0)\frac{n}{d} \mid d \in D(n)\right\} = v_h(n,h)$$

and

$$v_h(n,h) \leq \max\left\{\alpha_\tau(\mathbb{Z}_d, h, q)\frac{n}{d} \mid d \in D(n)\right\}$$

Theorem 16. *For an Abelian group G with exponent κ, if A is a maximum cardinality q-h-sum-free subset of G, then one of the following holds*

- $|A| \leq \left\lfloor \frac{|G|}{h+2} \right\rfloor$ *or* $|A| = \frac{n}{\kappa} \cdot \max\left\{\gamma_\tau(\mathbb{Z}_d, h, q)\frac{\kappa}{d} \mid d \in D(\kappa)\right\}$ *and A is an arithmetic progression and there are no $a \in A$ such that $\langle A - a\rangle = G$.*
- $|A| \leq \left\lfloor \frac{|G|}{h} \right\rfloor$ *and and there is some $a \in A$ such that $\langle A - a\rangle = G$*
- $|A| = \frac{n}{\kappa} \cdot \max\left\{\gamma_\tau(\mathbb{Z}_d, h, q)\frac{\kappa}{d} \mid d \in D(\kappa)\right\}$ *and A is the union of arithmetic progressions.*

It easily follows that

Corollary 17. *For an Abelian group G of order n with exponent κ, and positive integer h*

$$\frac{n}{\kappa} \cdot v_h(\kappa, h) \leq \tau(G, h) \leq \max\left\{\left\lfloor \frac{n}{h} \right\rfloor, \frac{n}{\kappa} \cdot v_h(\kappa, h)\right\}$$

giving us

Corollary 18. *For an Abelian group G of order n with exponent κ, and positive integer h, if*

$$\frac{n}{\kappa} \cdot v_h(\kappa, h) \geq \left\lfloor \frac{n}{h} \right\rfloor$$

then

$$\tau(G, h) = \frac{n}{\kappa} \cdot v_h(\kappa, h)$$

Notably, this covers every cyclic G of order n with the exception of when h divides n, and n has no factors $d = i \mod h$ such that $i > \gcd(d, h)$.

Corollary 19. *For κ, the exponent of an Abelian group G of order n, if κ has any divisors $i \mod h$ where $i > \gcd(d, h)$ then $\tau(G, h) = v_h(\kappa, h) \cdot \frac{n}{\kappa}$*

Despite the above results being quite extensive, they are not complete. However, we can completely prove the cyclic case as follows

Theorem 20.

$$\tau(\mathbb{Z}_n, h) = v_h(n, h)$$

Notably, in [1], Bajnok conjectured the above Theorem.

Corollary 21.

$$\tau(\mathbb{Z}_n, h) = \max\left\{\alpha_\tau(\mathbb{Z}_d, h) \cdot \frac{n}{d} \mid d \in D(n)\right\}$$

This behavior is very interesting as it directly mirrors Bajnok's results in [4] and later his results with Matzke in [3].

3 Methods

First, we will determine the value of $\gamma_\tau(\mathbb{Z}_n, h, q)$. In this proof, we use very similar methods to those of Bajnok and Matzke in [3] for (k, l)-sum-free sets.

Proof of Theorem 14. Let $A \subset \mathbb{Z}_n$, and $A = [a, a+m-1]$ for some $a \in \mathbb{Z}_n$. We also know that

$$hA = [ha, ha + hm - h]$$

Thus, A can only be q-h-sum-free if and only if there exists some positive integer b for which

$$bn + q + 1 \leq ha$$

and

$$(b+1)n + q - 1 \geq ha + hm - h$$

Combined, these inequalities become

$$q + 1 \leq ha - bn \leq n + h - 1 - hm + q$$

$$\frac{1+q}{\delta} \leq \frac{ha - bn}{\delta} \leq \frac{n + h - 1 - hm + q}{\delta}$$

Where $\delta = \gcd(n, h)$.

The middle term is an integer, so this means we must have that

$$\left\lceil \frac{1+q}{\delta} \right\rceil \leq \frac{ha - bn}{\delta} \leq \frac{n + h + q - 1 - hm}{\delta}$$

$$\left\lceil \frac{1+q}{\delta} \right\rceil \leq \frac{n + h + q - 1 - hm}{\delta}$$

$$m \leq \left\lfloor \frac{n + q - 1 - \lceil \frac{1+q}{\delta} \rceil \cdot \delta}{h} \right\rfloor + 1$$

proving our claim. □

A relatively trivial but nonetheless important fact is that if A is q-h-sum-free in G then $A \times H$ is is $q \times \{0\}$-h-sum-free in $G \times H$ as well. This gives us that $\tau(\mathbb{Z}_n, h, q) \geq \max \left\{ \alpha_\tau(\mathbb{Z}_d, h, q) \cdot \frac{n}{d} | d \in D(n) \right\}$, a quantity which will be of great importance.

Before we continue to prove Theorem 15, we will prove a Lemma that will be utilized in that proof.

Lemma 22. *If neither or both of p and q are divisible by* $\gcd(n, h)$ *then*

$$\gamma_\tau(\mathbb{Z}_n, h, q) = \gamma_\tau(\mathbb{Z}_n, h, p)$$

Proof. By Theorem 14 a q-h-sum-free interval in $\mathbb{Z}_n$ has maximum size

$$\left\lfloor \frac{n+q-1-\left\lceil \frac{1+q}{\delta} \right\rceil \cdot \delta}{h} \right\rfloor + 1$$

Note that

$$q - \left\lceil \frac{1+q}{\delta} \right\rceil \cdot \delta$$

is equal to $r-\delta$ where r is the remainder of q when divided by δ, the greatest common divisor of n and h. Reexamining the expression for $\gamma_\tau(\mathbb{Z}_n, h, q)$ rewritten as

$$\left\lfloor \frac{n-1+r-\delta}{h} \right\rfloor + 1$$

gives us the following possibilities for a given n and h.

Case I: $n \bmod h > \delta$

If this is the case, then $n-\delta \geq 1 \mod h$, this gives us that

$$\gamma_\tau(\mathbb{Z}_n, h, q) \geq \left\lfloor \frac{n}{h} \right\rfloor + 1$$

Furthermore, because the maximum value of r is $\delta - 1$,

$$\gamma(\mathbb{Z}_n, h, q) \leq \left\lfloor \frac{n-2}{h} \right\rfloor + 1$$

which is equal to our lower bound unless n is 1 mod h, which cannot occur in this scenario. This means for all n and h that satisfy this scenario, $\gamma_\tau(\mathbb{Z}_n, h, q)$ is equal to $\left\lfloor \frac{n}{h} \right\rfloor + 1$ for all q.

Case II: $n \bmod h = \delta$

In this case we have,

$$\gamma_\tau(\mathbb{Z}_n, h, q) = \frac{n-\delta}{h} + \left\lfloor \frac{r-1}{h} \right\rfloor + 1$$

However, for all q which $r \neq 0$, we have that

$$\gamma_\tau(\mathbb{Z}_n, h, q) = \frac{n-\delta}{h} + 1$$

And if $r = 0$, we have a slightly different case of

$$\gamma_\tau(\mathbb{Z}_n, h, q) = \frac{n-\delta}{h}$$

.

Case III: $n \bmod h = 0$

In the third and final scenario,

$$\gamma_\tau(\mathbb{Z}_n, h, q) = \frac{n}{h} + \left\lfloor \frac{r-1}{h} \right\rfloor$$

Similarly to Scenario II, if $r \neq 0$

$$\gamma_\tau(\mathbb{Z}_n, h, q) = \frac{n}{h}$$

and if r does happen to equal 0

$$\gamma_\tau(\mathbb{Z}_n, h, q) = \frac{n}{h} - 1$$

Note that these three scenarios encompass every possibility, as $n \mod h$ can only be less than δ if $n \mod h = 0$.

Across all three scenarios, it is seen that for a constant n and h, if q and p share divisibility (or lack thereof) by δ then

$$\gamma_\tau(\mathbb{Z}_n, h, q) = \gamma_\tau(\mathbb{Z}_n, h, p)$$

this completes the proof.

$\square$

Now, we will demonstrate that we only need to consider intervals when evaluating $\max\left\{\alpha_\tau(\mathbb{Z}_d, h, q) \cdot \frac{n}{d} | d \in D(n)\right\}$.

Proof of Theorem 15. In this proof, we will split arithmetic progressions in $\mathbb{Z}_n$ into two categories depending on whether the progression's common difference, d, is relatively prime to n or not.

First, we tackle when $\gcd(n, d) = 1$ **(Case A)**

Consider the set

$$A = \{a, a+d, a+2d, \cdots, a+(m-1)d\}$$

that is q-h-sum-free in $\mathbb{Z}_n$ where $\gcd(d, n) = 1$. Observe that

$$d^{-1} \cdot A = \{ad^{-1}, ad^{-1}+1, ad^{-1}+2, \cdots, ad^{-1}+(m-1)\}$$

is qd^{-1}-h-sum-free, and it is an interval. However, because d^{-1} is relatively prime to n, qd^{-1} is divisible by $\gcd(n, h)$ iff q is divisible by $\gcd(n, h)$. With this it follows from Lemma 22 that a q-h-sum-free arithmetic progression in $\mathbb{Z}_n$ of size m with a difference relatively prime to n exists iff $m \leq \gamma_\tau(\mathbb{Z}_n, h, q)$.

Now, we examine when d shares a divisor other than 1 with n.

We will split this into two sub-cases, **Case B1** and **Case B2**. We first examine **Case B1**: $\gcd(d, n) \neq 1$, and $\gcd(d, n)$ does not divide both h and q.

Let A be a q-h-sum-free arithmetic progression with differnce d where $c = \gcd(n, d) \neq 1$. A must be contained in a coset of H, the subgroup of $\mathbb{Z}_n$ with index c If c divides both q and h, then $q \in H$, and regardless of the coset of

H that is picked $h(H+a)=H$. As long as exactly one or neither of $c|h$ and $c|q$ hold, then there exists some coset of H has an h fold sumset without q. So, when it comes this this case, the largest $q-h$-sum-free arithmetic progression you can get has size $\frac{n}{c_1}$ where c_1 is the smallest divisor of n does not divide both h and q.

Note that we only need to show that

$$\max\left\{\gamma_\tau(\mathbb{Z}_d,h,q)\frac{n}{d}\mid d\in D(n)\right\}\geq\left(\left\lfloor\frac{d_1+q-1-\left\lceil\frac{1+q}{\gcd(c_1,h)}\right\rceil\cdot\gcd(h,c_1)}{h}\right\rfloor+1\right)\cdot\frac{n}{c_1}\geq\frac{n}{c_1}$$

in order to prove that we can ignore **Case B1** when computing the value of $\max\left\{\alpha_\tau(\mathbb{Z}_d,h,q)\frac{n}{d}\right\}$.

Or equivalently,

$$c_1+q-1-\left\lceil\frac{1+q}{\gcd(c_1,h)}\right\rceil\cdot\gcd(h,c_1)\geq 0$$

$$c_1+q-1-\left\lceil\frac{1+q}{\gcd(c_1,h)}\right\rceil\cdot\gcd(h,c_1)\geq 0$$
$$\frac{c_1+q-1}{\gcd(h,c_1)}\geq\left\lceil\frac{1+q}{\gcd(c_1,h)}\right\rceil$$
$$\frac{c_1+q-1}{\gcd(h,c_1)}\geq\frac{1+q}{\gcd(c_1,h)}+1$$
$$\frac{c_1-2}{\gcd(h,c_1)}\geq 1$$
$$c_1-2\geq\gcd(h,c_1)$$

The only times this does not hold are $\gcd(c_1,h)=c_1$ or $c_1=2$.

However, the $c_1=2$ case is easily resolved as if this is true, either q or h must be odd, both of these result in $\frac{1+q}{\gcd(c_1,h)}$ being an integer, which slightly changes the above inequalities to be

$$\frac{c_1+q-1}{\gcd(h,c_1)}\geq\frac{1+q}{\gcd(c_1,h)}$$
$$c_1-2\geq 0$$

Thus easily resolving this would-be exception.

The second possible exception is when c_1 divides h. Starting again from

$$c_1+q-1-\left\lceil\frac{1+q}{\gcd(c_1,h)}\right\rceil\cdot\gcd(h,c_1)\geq 0$$

$$c_1+q-1-\left\lceil\frac{1+q}{c_1}\right\rceil\cdot c_1\geq 0$$

$$1+\frac{q-1}{c_1}\geq\left\lceil\frac{q+1}{c_1}\right\rceil$$

However, q cannot be divisible by c_1, as c_1 cannot divide both h and q. This gives us

$$1+\frac{q-1}{c_1}\geq\left\lceil\frac{q}{c_1}\right\rceil$$

$$\frac{q-1}{c_1}\geq\left\lfloor\frac{q}{c_1}\right\rfloor$$

Again, this always holds unless c_1 divides q, which we already mentioned cannot occur. This proves that we need not consider the **B1** case when determining the value of $\max\left\{\alpha_\tau(\mathbb{Z}_d,h,q)\cdot\frac{n}{d}|d\in D(n)\right\}$.

Now, for the final possibility: **Case B2**, when $\gcd(d,n)\neq 1$, and $\gcd(d,n)$ divides both h and q.

For cases where c ($\gcd(n,d)$) does divide both h and q, we have that for a q-h-sum-free arithmetic progression A that satisfies this, we have that $(q-A)\cap(h-1)A=\emptyset$. Furthermore, because c divides both h and q, $(h-1)A$ and $q-A$ are contained within the same coset of the subgroup with index c. This gives us

$$|q-A|+|(h-1)A|\leq\frac{n}{c}$$

because A is an arithmetic progression

$$|A|+(h-1)|A|-(h-1)+1\leq\frac{n}{c}$$

$$\frac{n/c-2}{h}+1\geq|A|$$

However, if we acknowledge that $|A|\geq 2$ (otherwise A is an interval) we reveal the following

$$\frac{n-2c}{ch}\geq 1$$

$$n/c-2\geq h$$

$$n-\frac{n}{c}-2\geq h$$

$$n-h-2\geq\frac{n}{c}$$

with this new information we can do the following

$$|A|\leq\left\lfloor\frac{n/c-2}{h}+1\right\rfloor\leq\left\lfloor\frac{n-h-2-2}{h}\right\rfloor+1=\left\lfloor\frac{n-4}{h}\right\rfloor\leq$$

$$\left\lfloor\frac{n-1}{h}\right\rfloor\leq\left\lfloor\frac{n+q-1-\left\lceil\frac{1+q}{\delta}\right\rceil\cdot\delta}{h}\right\rfloor+1$$

Thus, q-h-sum-free progressions in **Case B2** will always be smaller than the largest q-h-sum-free interval.

With this, we have proven that **Case A** (and hence intervals alone) suffices when computing $\max\left\{\alpha_\tau(\mathbb{Z}_d, h, q) \cdot \frac{n}{d} \mid d \in D(n)\right\}$ meaning

$$\max\left\{\alpha_\tau(\mathbb{Z}_d, h, q) \cdot \frac{n}{d} \mid d \in D(n)\right\} = \max\left\{\gamma_\tau(\mathbb{Z}_d, h, q) \cdot \frac{n}{d} \mid d \in D(n)\right\}$$

□

Now, for the most important result thus far

Proof of Theorem 16. We will split this proof into three cases for a maximum size q-h-sum-free subset of G, A.

- **Case I:** There is no such element, a, in A where $\langle A - a\rangle = G$
- **Case II:** There exists $a \in A$ such that $\langle A - a\rangle = G$ and the subgroup H given by Theorem 11 has the property that $(A - a)/H$ is a Vosper subset in G/H
- **Case III:** There exists $a \in A$ such that $\langle A - a\rangle = G$ and the subgroup H given by Theorem 11 has the property that $(A - a)/H$ is an arithmetic progression in G/H

By Theorem 11, all $A \subset G$ with $|A| \leq \frac{|G|}{2}$ fall under one of these cases.

We will go in order

Case I: Assume that there exists no element $a \in A$ such that $\langle A - a\rangle = G$. If this is the case, for any $a \in A$ let $B = A - a$, B must be a generating subset of some subgroup, H of G, with cardinality at most $\frac{|G|}{2}$, thus by Lemma 13 we have that

$$|jB| \geq \min\left\{\frac{|G|}{2}, \left\lceil\frac{(j-1)|B|}{2}\right\rceil + |B|\right\}$$

We have that $q - A$ is disjoint from $(h-1)A$, and we will focus on when they are both contained in the same coset of H, as if they are contained in separate cosets of H, it is implied that $q \notin h(H + a)$ for some a, meaning $H + a$ itself is q-h-sum-free, and combined with the fact that A is maximum size, we would have $A = H + a$, and A is an arithmetic progression. Thus, either A is an arithmetic progression (in which case we consult Theorem 15) or $(h-1)A$ and $q - A$ must be disjoint in a single coset of H. If A is not an arithmetic progression then

$$\frac{|G|}{2} \geq \left\lceil\frac{(h-2)|B|}{2}\right\rceil + 2|B|$$

$$|G| \geq (h+2)|B|$$

This means that if A fits into Case I then either $|A| \leq \left\lfloor\frac{|G|}{h+2}\right\rfloor$ or A is an arithmetic progression. This brings us to our next case.

Case II:

If A is q-h-sum-free then $q - A$ must be disjoint from $(h-1)A$ or

$$|q - A| + |(h-1)A| \leq |G|$$

$$|A| + |(h-1)A| \leq |G|$$

Let $B = A - a$ for some $a \in A$ such that B generates G. Now, by Theorem 2.1 from [2] we can say there exists a subgroup of G, H, such that

$$|B + H| < \min(|G|, |H| + |B|)$$

If we split B into intersections of cosets of H labeled $B_1, B_2 \cdots B_r$, we get the following identities from [2].

1. If $(i,j) \neq (1,1)$ $|B_i| + |B_j| \geq |H| + 1$
2. $kB = (k(B+H) \setminus (kB_1 + H)) \cup (kB_1)$

Assume that B/H is a Vosper subset, if this is the case then $|B/H| \geq 3$, this means $|B| \geq |B_1| + |B_2| + |B_3|$, and with

$$|B| + |(h-1)B| \leq |G|$$

we have

$$|B_1| + |B_2| + |B_3| + |(h-1)(B+H)| - |H| + |B_1| \leq |G|$$

and because of $|B_i| + |B_j| \geq |H| + 1$ we now have

$$|(h-1)(B+H)| + |H| < |G|$$

Which gives us that $|h(B/H)| < |G/H| - 1$ thus, we have that for any $X \subset G/H$ where $|X| \geq 2$, $|B/H + X| \geq |B/H| + |X|$ which in turn gives us

$$|(h-1)(B+H)| \geq (h-1)|B+H|$$

and because

$$|(h-1)B| \geq |(h-1)(B+H)| - |(h-1)B_1 + H| + |(h-1)B_1| \geq$$

$$(h-1)|B+H| - |H| + |B_1| \geq (h-1)|B|$$

we now have

$$|(h-1)B| \geq (h-1)|B|$$

which gives us

$$|B| + (h-1)|B| \leq |G|$$

$$\frac{|G|}{h} \geq |B| = |A|$$

This results in the conclusion that if A is a set which falls into Case II, then $|A| \leq \left\lfloor \frac{|G|}{h} \right\rfloor$

Case III:

Lastly we tackle a similar situation to Case II, but B/H is an arithmetic progression instead. because B/H is an arithmetic progression containing 0 and B/H is also a generating subset of G/H, H must be cyclic, which means that we only need to consider cyclic subgroups of G when determining what subgroups of G are able to contain the arithmetic progressions, this means if A fits into Case III then we consult Theorem 15 and we have that

$$|A| = \frac{n}{\kappa} \cdot \max\left\{\gamma_\tau(\mathbb{Z}_d, h, q)\frac{\kappa}{d} \mid d \in D(\kappa)\right\}$$

. This completes our proof.

□

Now, we will finish the cyclic case However, the following lemmas will be of use

Lemma 23.

$$\tau(\mathbb{Z}_n, h, q) = \tau(\mathbb{Z}_n, h, a)$$

where $\tau(\mathbb{Z}_n, h, q)$ *is equal the the largest* $A \subset \mathbb{Z}_n$ *such that* $q \notin hA$ *and* $a \in \langle h\rangle + q$

Proof. This proof is simple. A set $A \subset \mathbb{Z}_n$ is q-h-sum-free in $\mathbb{Z}_n$ iff

$$q \notin hA$$

$$q \notin hA \iff q + hx \notin h(A - x)$$

□

A second lemma is as follows

Lemma 24. *If* $v_h(n, h) = \left\lfloor \frac{n-1}{h} \right\rfloor$ *then for any divisor of* n*,* d

$$v_h(d, h) = \left\lfloor \frac{d-1}{h} \right\rfloor$$

This easily follows from Theorem 3.

Proof of Theorem 20. Let A be a zero-h-sum-free subset of $\mathbb{Z}_n$ for n divisible by h, and $v_h(n, h) = \left\lfloor \frac{n-1}{h} \right\rfloor$

Let $H < \mathbb{Z}_n$ be a subgroup of index f where f is a prime divisor of h. Let $K_i = H - i$, and $A_i = K_i \cap A$.

Let $B_i = A_i + i$. B_i is contained in H, which is isomorphic to $\mathbb{Z}_{\frac{n}{f}}$. Therefore, by Lemma 23 if $h \cdot i \in hB_i$, then $0 \in hA_i$. However, because $H \cong \mathbb{Z}_{\frac{n}{f}}$, we have

$$|A_i| \leq \tau\left(\mathbb{Z}_{\frac{n}{f}}, h, \frac{hi}{f}\right)$$

By Theorem 15 we have that for $\delta = \gcd(d, h)$

$$|A_i| \leq \max\left\{\left\lfloor\frac{d + \frac{hi}{f} - 1 - \left\lceil\frac{1+\frac{hi}{f}}{\delta}\right\rceil \cdot \delta + h}{h}\right\rfloor\frac{n}{fd}, \left\lfloor\frac{n}{fh}\right\rfloor \mid d \in D\left(\frac{n}{f}\right)\right\}$$

Now, because h divides n

$$|A_i| \leq \max\left\{\left\lfloor\frac{d - 1 - \gcd(h, d) + h}{h}\right\rfloor\frac{n}{fd}, \left\lfloor\frac{n}{fh}\right\rfloor \mid d \in D\left(\frac{n}{f}\right)\right\}$$

This however is equal to

$$|A_i| \leq \max\left\{v_h\left(\frac{n}{f}, h\right), \left\lfloor\frac{n}{fh}\right\rfloor\right\}$$

By Lemma 24, we have that

$$|A_i| \leq \max\left\{\left\lfloor\frac{n-f}{fh}\right\rfloor, \left\lfloor\frac{n}{fh}\right\rfloor\right\}$$

$$|A_i| \leq \left\lfloor\frac{n}{fh}\right\rfloor$$

Now, assume that there exists a k such that

$$\tau(\mathbb{Z}_k, h) = \left\lfloor\frac{k-1}{h}\right\rfloor$$

and let f be some divisor h such that kf is divisible by h and $v_h(kf, h) \leq \frac{kf}{h}$

Now, let A be a zero-h-sum-free set in $\mathbb{Z}_{kf}$. Using the above notation, we have that

$$A = A_0 \uplus A_1 \uplus \cdots \uplus A_{f-1}$$

Because we already have that $\tau(\mathbb{Z}_k, h) = \lfloor\frac{k-1}{h}\rfloor$, we can combine this with $|A_i| \leq \lfloor\frac{k}{h}\rfloor$ we arrive at

$$|A| \leq \left\lfloor\frac{k-1}{h}\right\rfloor + (f-1)\left\lfloor\frac{k}{h}\right\rfloor \leq \frac{kf-1}{h}$$

$$|A| \leq \left\lfloor \frac{kf-1}{h} \right\rfloor$$

Thus, we have that for

$$\tau(\mathbb{Z}_k, h) = \left\lfloor \frac{k-1}{h} \right\rfloor$$

and a divisor of h, f, that has the property that $v_h(kf, h) \leq \frac{kf}{h}$

$$\tau(\mathbb{Z}_k, h) = \left\lfloor \frac{k-1}{h} \right\rfloor \Longrightarrow \tau(\mathbb{Z}_{kf}, h) \leq \left\lfloor \frac{kf-1}{h} \right\rfloor$$

We can use induction on the above with the base cases being values of k such that $\lfloor \frac{k}{h} \rfloor = \lfloor \frac{k-1}{h} \rfloor = v_h(k, h)$ (for every factor of k, d, we have $\gcd(d, k) \geq i \mod k$, and k is not divisible by h), which one can see by consulting Theorem 3, would cover all the cyclic cases not covered by Corollary 18, proving our claim.

□

4 Next Steps

While the results obtained above are extensive, they are not complete. There are still some remaining cases, so it is natural to offer the following very challenging problem.

Problem 25. *Find $\tau(G, h)$ for the remaining non-cyclic G.*

In addition I also have other questions regarding the nature of zero-h-sum-free sets themselves

Problem 26. *Classify all zero-h-sum-free $A \subset G$ where $|A| = \tau(G, h)$*

Problem 27. *Classify all zero-h-sum-free $A \subset G$ where $hA = G \setminus \{0\}$*

Problem 28. *Classify all* maximal *zero-h-sum-free $A \subset G$, ie. if $A \subseteq B$ and $0 \notin hB$ then $B = A$.*

References

[1] B. Bajnok Additive Combinatorics A Menu of Research Problems *CRC Press, Boca Raton,* 2018, p.284,

[2] Y. Hamidoune and A. Plagne A new critical pair theorem applied to sum-free sets in Abelian groups

[3] B. Bajnok and R. Matzke The Maximum Size of (k, l)-Sum-Free Sets in Cyclic Groups

[4] B. Bajnok On The Maximum Size of a (k,l)-Sum-Free Subset of an Abelian Group

[5] P. Francis, G. Slevin, P. Szanto Research Papers in Mathematics Vol. 23, Gettysburg College