On sumsets of nonbases of maximum size

Béla Bajnok[1*], Péter Pál Pach[2†,‡]

[*]Department of Mathematics, Gettysburg College, Gettysburg, PA 17325, USA
[†]Department of Computer Science and Information Theory, Budapest University of Technology and Economics, Műegyetem rkp. 3., H-1111 Budapest, Hungary.
[‡]MTA-BME Lendület Arithmetic Combinatorics Research Group, ELKH, Műegyetem rkp. 3., H-1111 Budapest, Hungary.

The full version of this work will be published elsewhere.

Abstract

Let G be a finite abelian group. A nonempty subset A in G is called a basis of order h if $hA = G$; when $hA \neq G$, it is called a nonbasis of order h. Our interest is in all possible sizes of hA when A is a nonbasis of order h in G of maximum size; we provide the complete answer when $h = 2$ or $h = 3$.

1 Introduction

Let G be a finite abelian group of order $n \geq 2$, written in additive notation. For a positive integer h, the *Minkowski sum* of nonempty subsets $A_1, \ldots, A_h$ of G is defined as

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

When $A_1 = \cdots = A_h = A$, we simply write hA, which then is the collection of sums of h not-necessarily-distinct elements of A.

We say that a nonempty subset A of G is *h-complete* (alternatively, a *basis of order h*) if $hA = G$; while, if hA is a proper subset of G, we say that A is *h-incomplete*. The *h-critical number* $\chi(G, h)$ of G is defined as the smallest positive integer m for which all m-subsets of G are h-complete; that is:

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

It is easy to see that for all G and h we have $hG = G$, so $\chi(G, h)$ is well defined. The value of $\chi(G, h)$ is now known for every G and h—see [1, 2].

The following question then arises naturally: What can one say about the size of hA if A is an h-incomplete subset of maximum size in G? Namely, we aim to determine the set

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

In this paper we attain the complete answer to this question for $h = 2$ and $h = 3$. For $h = 2$, we find that the situation is greatly different for groups of even and odd order.

Theorem 1. *Let G be an abelian group of order n.*

[1]Email: bbajnok@gettysburg.edu.
[2]Email: ppp@cs.bme.hu. Research of P. P. P. is supported by the Lendület program of the Hungarian Academy of Sciences (MTA) and by the National Research, Development and Innovation Office NKFIH (Grant Nr. K124171 and K129335).

1. *When n is even, the maximum size of a 2-incomplete subset of G is $n/2$, and the elements of $S(G,2)$ are of the form $n - n/d$ where d is some even divisor of n; in fact all such integers are possible, with the exception that $3n/4$ arises only when the exponent of G is divisible by 4.*

2. *When n is odd, the maximum size of 2-incomplete subsets of G is $(n-1)/2$; furthermore, when G is of order 3, 5, or is noncyclic and of order 9, then $S(G,2) = \{n-2\}$, and for all other groups of odd order we have $S(G,2) = \{n-2, n-1\}$.*

For $h = 3$ we separate three cases.

Theorem 2. *Let G be an abelian group of order n.*

1. *When n has prime divisors congruent to 2 mod 3, and p is the smallest such prime, the maximum size of a 3-incomplete subset is $(p+1)n/(3p)$, and we have $S(G,3) = \{n - n/p\}$.*

2. *When n is divisible by 3 but has no divisors congruent to 2 mod 3, then the maximum size of a 3-incomplete subset is $n/3$, and the elements of $S(G,3)$ are of the form $n - n/d$ or $n - 2n/d$ where d is some divisor of n that is divisible by 3; furthermore, all such integers are possible, with the exceptions of $2n/3$ and $n - 2n/d$ when the highest power of 3 that divides d is more than the highest power of 3 that divides the exponent of G.*

3. *In the case when all divisors of n are congruent to 1 mod 3, then the maximum size of a 3-incomplete subset is $(n-1)/3$, and $S(G,3) = \{n-3, n-1\}$, unless G is an elementary abelian 7-group, in which case $S(G,3) = \{n-3\}$.*

We should note that the three cases addressed in Theorem 2 are the same as those used while studying sumfree sets—see [3] and [4]; in fact, the maximum size of a 3-incomplete set in G agrees with the maximum size of a sumfree set in G when G is cyclic.

Our methods are completely elementary, with Kneser's Theorem as the main tool. In Section 2 we review some standard terminology and notations and prove some auxiliary results, then in Section 3 we sketch the proof of Theorem 1 in the case when the order of the group is even.

2 Preliminaries

Here we present a few generic results that come useful in our proofs. We will use the following version of Kneser's Theorem.

Theorem 3 (Kneser's Theorem; [5])**.** *If $A_1, \ldots, A_h$ are nonempty subsets of a finite abelian group G, and H is the stabilizer subgroup of $A_1 + \cdots + A_h$ in G, then*

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

Our first lemma is a simple application of Kneser's Theorem:

Lemma 4. *Suppose that G is a finite abelian group and that h is a positive integer. Let A be an h-incomplete subset of maximum size in G, and let H denote the stabilizer of hA in G. Then both A and hA are unions of full cosets of H; furthermore, if A and hA consist of k_1 and k_2 cosets of H, respectively, then*

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

We will also use the following observation:

Lemma 5. *Suppose that G is a finite abelian group of order n and that h is a positive integer. Let H be a subgroup of G of index d for some $d \in \mathbb{N}$, and let ϕ be the canonical map from G to G/H. Suppose further that B is a subset of G/H, and set $A = \phi^{-1}(B)$. Then $|A| = \frac{n}{d} \cdot |B|$ and $|hA| = \frac{n}{d} \cdot |hB|$.*

Our next result takes advantage of the fact that the elements of a finite abelian group have a natural ordering. We review some background and introduce a useful result.

When G is cyclic and of order n, we identify it with $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. More generally, G has a unique *type* $(n_1, \ldots, n_r)$, where r and $n_1, \ldots, n_r$ are positive integers so that $n_1 \geq 2$, n_i is a divisor of n_{i+1} for $i = 1, \ldots, r-1$, and

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

here r is the *rank* of G and n_r is the *exponent* of G.

The above factorization of G allows us to arrange the elements in lexicographic order and then consider the 'first' m elements in G. Namely, suppose that m is a nonnegative integer less than n; we then have unique integers $q_1, \ldots, q_r$, so that $0 \leq q_k < n_k$ for each $1 \leq k \leq r$, and

$$m = \sum_{k=1}^{r} q_k n_{k+1} \cdots n_r.$$

For simplicity, we assume $q_r \geq 1$, in which case the first m elements in G range from the zero element to $(q_1, \ldots, q_{r-1}, q_r - 1)$ and thus form the set

$$\mathcal{I}(G, m) = \bigcup_{k=1}^{r} \{q_1\} \times \cdots \times \{q_{k-1}\} \times \{0, 1, \ldots, q_k - 1\} \times \mathbb{Z}_{n_{k+1}} \times \cdots \times \mathbb{Z}_{n_r}.$$

The advantage of considering these initial sets is that their h-fold sumsets are also initial sets. Indeed, assuming for simplicity that $hq_k < n_k$ for each k, we find that $h\mathcal{I}(G, m)$ consists of the elements from the zero element to $(hq_1, \ldots, hq_{r-1}, hq_r - h)$, and thus

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

We will also employ a slight modification of $\mathcal{I}(G, m)$ where its last element is replaced by the next one in the lexicographic order. To avoid degenerate cases, we further assume that $q_r \geq 3$, in which case we have

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

an easy calculation shows that

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

We can summarize these calculations, as follows.

Proposition 6. *Suppose that the finite abelian group G is of type $(n_1, \ldots, n_r)$. Let $0 \leq m < n$, and let $q_1, \ldots, q_r$ be the unique integers with $0 \leq q_k < n_k$ for each $1 \leq k \leq r$ for which*

$$m = \sum_{k=1}^{r} q_k n_{k+1} \cdots n_r.$$

Let h be a positive integer for which $hq_k < n_k$ for each $1 \leq k \leq r$. Then for the m-subsets $\mathcal{I}(G, m)$ and $\mathcal{I}^*(G, m)$ of G we have the following:

1. *If $q_r \geq 1$, then $|h\mathcal{I}(G, m)| = hm - h + 1$.*
2. *If $q_r \geq 3$, then $|h\mathcal{I}^*(G, m)| = hm$.*

3 Sketch of the proof for two-fold sumsets

In this section we outline the proof of Theorem 1 in the case when the order of the group is even: Theorem 9.

The critical number $\chi(G,2)$ is as follows.

Proposition 7. *For any abelian group G of order n we have*

$$\chi(G,2) = \lfloor n/2 \rfloor + 1.$$

We now turn to finding

$$S(G,2) = \{|2A| \ : \ A \subset G,\ |A| = \lfloor n/2 \rfloor\ ,\ 2A \neq G\}.$$

Our proof builds on the following result that may be of independent interest.

Theorem 8. *Let G be a finite abelian group of even order whose exponent is not divisible by 4, and suppose that A is a subset of G of size $|A| = n/2$. Then G has a subgroup H of order $n/2$ for which*

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

We note that the claim of Theorem 8 may be false in groups with exponent divisible by 4. For example, in $\mathbb{Z}_2 \times \mathbb{Z}_4$, the set $\mathbb{Z}_2 \times \{0,1\}$ intersects all three subgroups in two elements.

We are now ready to determine $S(G,2)$. Here we present the proof in the case when n is even.

Theorem 9. *If the exponent of G is divisible by 4, then*

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

if the exponent of G is even but not divisible by 4, then

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

Proof: Using the notations of Lemma 4, we have $|A| = n/2 = k_1 n/d$ where d is the index of the stabilizer subgroup of $2A$. This implies that d is even and $k_1 = d/2$; using Lemma 4 again yields $k_2 \geq d-1$ and thus $|2A| = k_2 n/d$ equals n or $n - n/d$. Therefore, we have

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

When the exponent of G is congruent to 2 mod 4, then we can rule out $d = 4$, as follows. By Theorem 8, G has a subgroup H of index 2 for which $H \cap A$ and $(G \setminus H) \cap A$ have different sizes; let $A = A_1 \cup A_2$ where A_1 and A_2 are subsets of different cosets of H. Without loss of generality, we assume that $|A_1| > n/4$, and thus $2A_1 = H$. If A_2 were to be empty, then A is a full coset of H, and thus $|2A| = n/2 \neq 3n/4$. Otherwise, $|A_1 + A_2| \geq |A_1| > n/4$, which implies that $|2A| \geq |2A_1| + |A_1 + A_2| > 3n/4$.

What remains is the proof that all remaining values arise as sumset sizes. This is clearly true when $d = 2$, or when $d = 4$ and the exponent of G is divisible by 4. Suppose now that d is an even divisor of n and $d > 4$. According to Lemma 5, it suffices to prove that every group K of order d contains some subset B of size $d/2$ for which $|2B| = d - 1$. Let H be any subgroup of index 2 in K, and set $B = (H \setminus \{h\}) \cup \{g\}$, where h and g are arbitrary elements of H and $K \setminus H$, respectively. Since $|H \setminus \{h\}| = d/2 - 1 > d/4$, we get $2(H \setminus \{h\}) = H$ and thus $2B = G \setminus \{h + g\}$. Therefore, $|2B| = d - 1$, and our proof is complete. □

References

[1] B. Bajnok. "The h-critical number of finite Abelian groups". In: *Unif. Distrib. Theory* 10.2 (2015), pp. 93–115.

[2] B. Bajnok. *Additive combinatorics*. Discrete Mathematics and its Applications (Boca Raton). A menu of research problems. CRC Press, Boca Raton, FL, 2018, pp. xix+390. DOI: 10.1201/9781351137621.

[3] P. H. Diananda and H. P. Yap. "Maximal sum-free sets of elements of finite groups". In: *Proc. Japan Acad.* 45 (1969), pp. 1–5.

[4] B. Green and I. Z. Ruzsa. "Sum-free sets in abelian groups". In: *Israel J. Math.* 147 (2005), pp. 157–188. DOI: 10.1007/BF02785363.

[5] M. Kneser. "Abschätzung der asymptotischen Dichte von Summenmengen". In: *Math. Z.* 58 (1953), pp. 459–484. DOI: 10.1007/BF01174162.

[6] V. F. Lev. "Stability result for sets with $3A \neq \mathbb{Z}_5^n$". In: *J. Combin. Theory Ser. A* 157 (2018), pp. 334–348. DOI: 10.1016/j.jcta.2018.03.008.